CHAPTER 9

Network Forensics

Information in This Chapter:

- Networking Fundamentals
- Types of Networks
- Network Security Tools
- Network Attacks
- Incident Response
- Network Evidence & Investigations

INTRODUCTION

It seems like hardly a day goes by that a major company or government entity isn't reporting a significant network intrusion of some kind. Take Fidelity National Information Services Inc. (FIS), for example. The Jacksonville processor of prepaid credit cards reported that an international criminal enterprise stole $13 million in a single day during 2011. They disclosed the theft in their first-quarter earnings statement released on May 3, 2011. The hackers executed a highly planned and well-coordinated operation involving ATMs from around the world along with stolen prepaid credit cards (Krebs). FIS is just one of many victims of crimes like this.

What began as a subculture motivated simply by overcoming the challenge hacking presented has now evolved into a much more sinister and significant threat, so much so that it's now a critical matter of national security. So much of the nation's critical infrastructure is reliant upon digital networks and devices. There is certainly no shortage of high-profile targets. These include governmental agencies, the power grid, and the financial and health care industries. This threat now comprises nation-states, organized criminal enterprises, terrorists, as well as individuals.

The private sector bears a significant portion of the responsibility in defending these networks. So, how does digital forensics figure into all this? Digital forensics can play a couple of roles:

Network investigations have some inherent hurdles that don't come into play in an investigation focusing on a stand-alone computer. Unlike a single machine,

The Basics of Digital Forensics. DOI: 10.1016/B978-1-59749-661-2.00009-7

data (evidence) could be spread across multiple machines or devices. To further complicate things, they could also be spread across a geographically expansive area. The sheer amount of data that could be involved presents another challenge. Depending on the size of the organization and its network, the volume of data could reach truly astronomical proportions.

Hackers have many attack options at their disposal when it comes to attacking a network. The attacks can be quite sophisticated or astoundingly simple. Some attacks rely on vulnerabilities in the technology; others rely on the weaknesses found in people. Software is one example of a weakness in the technology. Flaws in the software are found in the underlying code. These flaws are identified by software developers, security professionals, or others. Hackers then develop exploits to take advantage of the vulnerability. Hopefully, the software developer will take notice and fix the issue sooner rather than later. These normally come in the form of a "patch." This is a constant struggle that never seems to end.

Human weakness also contributes to a hacker's success in a number of ways. First, people are inclined to use weak passwords. They tend to be either too short or too predictable. For example, they use the names of their pets or children or they use actual words that can be found in the dictionary. Finally, even if the password was strong, they could leave the password written down very near the computer. Second, unsuspecting users can fall prey to a **social engineering** attack.

Social Engineering

In a social engineering attack, an authorized user is persuaded by an unauthorized individual into divulging sensitive information. Common attacks include hackers posing as employees, customers, or security consultants.

These various attacks can also be conducted in combination, leveraging the vulnerabilities of both the technology and the people who control it.

NETWORK FUNDAMENTALS

Networking or linking computers together has some distinct advantages. Sharing resources and collaboration are just two such benefits.

A network has some basic necessities that are required regardless of its size or purpose. The first is some type of connection between computers or devices. This connection can be a physical one (such as via an Ethernet cable) or wireless. Next, the network must have an established way to communicate. This common language, or set of rules, is known as a protocol. **Transmission Control Protocol/Internet Protocol (TCP/IP)** is a very commonly used network protocol and is also the one used on the Internet.

To lay the foundation, we'll start by defining and identifying the various types of networks in common use today. By far, the most common type of network encountered in a commercial setting is client/server. In a **client/server network**, each computer on the network is assigned one of these two roles. Clients are utilized by end-users, such as the workstation on your desk. These machines request files, services, and information from servers. Servers, by contrast, store and provide files, services, and information to multiple clients. In essence, you can have one server sharing files with hundreds of clients. They have much more control on the network. Servers tend to function in specific role(s). File servers, e-mail servers, and print servers are but a few examples.

The other network configuration commonly in use is known as **peer-to-peer (P2P)**. As the name suggests, all machines on the network can/do function as both clients and servers. P2P networks are seldom used in a commercial setting. File sharing is the predominant use of P2P networks. Music, movies, and software are some of the more commonly shared files. Unfortunately, P2P is also a major conduit for not only pirated music, video, and software, but child pornography as well. This is a major problem not only in the United States but worldwide as well.

Now that we have a basic understanding of how networks are organized, let's take a look at how these networks can be classified.

Network Types

The **Local Area Network** or LAN is generally considered the smallest office network. It comprises computers and devices in a single office or building. The **Wide Area Network (WAN)** is larger, sometimes significantly so. A WAN consists or LANs at different locations. The WAN can be spread across great distances. Other network types include **MANs (Metropolitan Area Network**), **PANs (Personal Area Networks**), **CANs (Campus Area Networks)**, and **GANs (Global Area Networks**).

In contrast to the Internet is an intranet. A company's intranet is private, and access to it is limited. Intranets are routinely used for file sharing, communication, and so on. An intranet functions like the Internet, using web browsers and typically the same protocol (TCP/IP).

On a network that uses the TCP/IP protocol, each computer or device on the network has a unique identifier or address known as an **IP address**. An IP address is used to deliver messages and data to its proper destination, functioning much like a street address. There are two versions of IP addressing we need to be concerned with: version 4 and version 6. IPv4 is being phased out because of the relatively small number of addresses when compared to the staggering numbers of devices and computers on the Internet. We're simply running out of addresses. IPv4 offers in the neighborhood of about four billion different IP addresses. It is being replaced by IPv6. IPv6, by contrast, provides for all intents and purposes a limitless number of addresses (Microsoft Corporation).

An IPv4 address is made up of four numbers that are separated by periods. Each of these four numbers, called octets, can range from 0 to 255. A typical IPv4 address would look like this: 198.122.55.16. An IPv6 address would look like this:

2008:0eb3:29a2:0000:0000:8c1d:0967:7256.

As a comparison, if you wrote an IPv6 address using IPv4 notation, it would look like this:

65535.65535.65535.65535.65535.65535.65535.65535 (Nikkel, 2007)

IP addresses can be static or dynamic. A static address is normally fixed and doesn't change. In contrast, a dynamic address changes on a regular basis. For example, certain Internet Service Providers (ISPs) use dynamic IP addressing. Here, each time you log on, the network assigns you an IP address from a pool of addresses that are currently unassigned. This enables a provider to service a large number of customers within the fixed number of IP addresses that they control. This works because not all of their subscribers will be online at any given time.

Data on a network can travel in different ways. **Packet switching** is used on the Internet and many other networks. Packet switching breaks the data into small chunks called packets. These packets then travel the network to their final destination using IP addressing.

Each packet is structured in a uniform manner. Individual packets are comprised of three parts; the header, payload, and footer. The header contains the addressing information, identifying the sender and receiver's IP address. Next, the packet identifies itself relative to the total number of packets. Something like "I'm packet 26 out 234." Then comes the payload itself. Finally, the packet is concluded with a footer or trailer. The trailer tells the receiver that this is the end of the packet. It also conducts a cyclical redundancy check (CRC). The CRC is a sum of all the ones in the packet. If the numbers don't match, the receiving computer will automatically resend the request. It's is used to verify the integrity of the packet. Figure 9.1 depicts the organization of a TCP/IP packet.

Networks routinely consist of hardware beyond just computers and servers. These devices are also important from an investigative perspective in that they can contain valuable evidence.

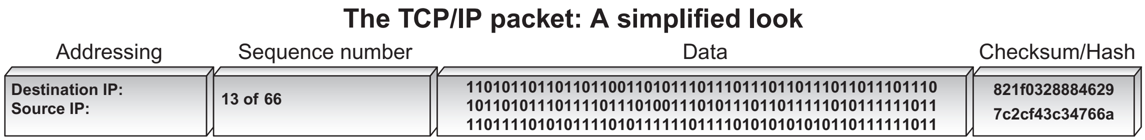

FIGURE 9.1
A typical IP packet. Illustration courtesy of Jonathan Sisson.

A gateway is a network point that acts as an entrance to another network (TechTarget, 2000). A bridge, by contrast, is used to connect two networks using the same protocol. Routers direct data, using the IP address, on the network to their final destination.

NETWORK SECURITY TOOLS

Regarding security, the best (and most realistic) approach is to prepare in terms of "when" there is an intrusion as opposed to "if" there is an intrusion. Working on the assumption that you will be able to keep each and every committed hacker out is just not realistic. Does that mean organizations should only take minimal measures to protect their networks, focusing more resources on response rather than prevention? Absolutely not. A robust perimeter defense should always be employed, the scope of which is normally dictated by the available budget and personnel needed to run it.

Fortunately, there are many hardware and software tools available that can help protect our networks. These tools not only serve to prevent a successful attack, they can also contain information of investigative value. Let's examine a couple of these tools.

A **firewall** is "a set of related programs, located at a network gateway server, that protects the resources of a private network from users from other networks" (TechTarget, 2000). The firewall acts as a filter for both inbound and outbound network traffic. It decides whether or not to allow the traffic to pass after carefully examining the network packets.

The purpose of an **Intrusion Detection System (IDS)** is to detect attacks from both outside and inside an organization. The IDS typically monitors a network looking for a pattern of recognized network attacks as well as unusual system and user actions and activity (TechTarget, 2000). Snort is a well-known open-source network intrusion detection system **(NIDS).** Snort operates as a **sniffer**, watching the network in real time and firing off alerts should a potential problem be identified (TechTarget, 2002).

NETWORK ATTACKS

There are many different ways to hack and/or attack a network. These attacks change at something akin to "warp" speed, resulting in a constant strain on the security industry. Below are just some of the attacks in use today.

Distributed Denial of Service (DDoS)—This attack uses massive numbers of compromised computers to attack a lone system. The attacking computers overwhelm the target with huge numbers of messages and requests. The target simply can't deal with this large volume of inbound traffic and eventually buckles, shutting down. The "army" of attacking computers are known as a "botnet," comprising individual compromised systems called "zombies."

Identity Spoofing (IP Spoofing)—An attacker can forge or "spoof" a valid or "known" IP addresses to gain access to a targeted network.

Man-In-The-Middle-Attack—In this attack, the hacker inserts himself between you and the person or entity you are communicating with. Your communications can then be monitored, altered, or deleted. This can also enable the attacker to impersonate you.

Social Engineering—Social engineering is one of the most effective attacks at the hacker's disposal. Social engineering is often described as obtaining protected information by way of a "trick" or a "con." TechTarget defines social engineering this way: "a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures" (TechTarget, 2001). Legendary hacker Kevin Mitnick made wide use of this technique with tremendous success (Mitnick, 2011).

Here is just one of many such examples of Mitnick's success: Mitnick calls up the network operations center of a cell phone company during a snowstorm. After befriending one of the operators, he asks them: "I left my SecureID card on my desk. Will you fetch it for me?" Of course, the network operators are too busy to do that, so they do the next best thing: They read it to him over the phone, giving him access to their network. Once inside, Mitnick steals source code belonging to the company. In this instance, Mitnick was able to "prove" his identity by telling the network operators his office number, the department where he worked, and the name of his supervisor—all information that the attacker had gleaned from previous phone calls to the company (Garfinkel, 2002).

In 2011, Verizon Business, the United States Secret Service (USSS), and the Dutch National High Tech Crime Unit (NHTCU) issued an interesting joint report after analyzing some eight hundred security incidents. These incidents were investigated by one or more of these organizations. As part of their report, they identified the most common hacking methods used in these incidents. These include:

- Exploitation of backdoor or command/control channel.
- Exploitation of default or guessable credentials.
- Brute force and dictionary attacks.
- Footprinting and fingerprinting.
- Use of stolen login credentials.

Some, like exploiting default passwords or the use of stolen credentials, are pretty self-explanatory. Others, like the command/control channel exploit and footprinting bear a little further explanation. Exploiting a command and control channel or backdoor allows an attacker to avoid security countermeasures. This enables the attacker to avoid detection. **Footprinting** or **fingerprinting** is an automated process by an attacker to scan for open ports or services (Verizon Business Global LLC & United States Secret Sevice, 2011).

Network security must focus on threats not only outside the firewall, but behind it as well. Internal attacks, such as those launched by disgruntled employees, can be devastating. Lets take a look at two such attacks.

ALERT!

Inside Threat

It's important to recognize the fact that threats come from not only outside of an organization, but inside as well. Preventative measures must account for both possibilities. An inside threat has a significant advantage in that it can bypass much of the security measures that are in place.

An application developer, who lost his IT sector job as a result of company downsizing, expressed his displeasure at being laid off just prior to the Christmas holidays by launching a systematic attack on his former employer's computer network. Three weeks following his termination, the insider used the username and password of one of his former coworkers to gain remote access to the network and modify several of the company's Web pages, changing text and inserting pornographic images. He also sent each of the company's customers an e-mail message advising that the web site had been hacked. Each e-mail message also contained that customer's usernames and passwords for the web site. An investigation was initiated, but it failed to identify the insider as the perpetrator. A month and a half later, he again remotely accessed the network, executed a script to reset all network passwords, and changed four thousand pricing records to reflect bogus information. This former employee ultimately was identified as the perpetrator and prosecuted. He was sentenced to serve five months in prison and two years on supervised probation, and ordered to pay $48,600 restitution to his former employer (Keeney, Cappelli, Kowalski, Moore, Shimeall, & Rogers, 2005).

A system administrator, angered by his diminished role in a thriving defense manufacturing firm whose computer network he alone had developed and managed, centralized the software that supported the company's manufacturing processes on a single server, and then intimidated a coworker into giving him the only backup tapes for that software. Following the system administrator's termination for inappropriate and abusive treatment of his coworkers, a logic bomb previously planted by the insider detonated, deleting the only remaining copy of the critical software from the company's server (Keeney, Cappelli, Kowalski, Moore, Shimeall, & Rogers, 2005). The company estimated the cost of damage in excess of $10 million, which led to the layoff of some eighty employees (Keeney, Cappelli, Kowalski, Moore, Shimeall, & Rogers, 2005).

INCIDENT RESPONSE

Organizations have to be able to respond when the breach occurs. Having a plan along with the tools and personnel to effectively respond can go a long way in mitigating the damage.

The National Institute of Standards and Technology (NIST) outlined the incident response life cycle in their *Computer Security Incident Handling Guide*. We can use this to walk us through an incident from beginning to end. The phases are: preparation, prevention, detection and analysis containment, eradication and recovery, and postincident activity (Scarphone, Grance, & Masone, 2008).

Preparation—Preparation is key for organizations to respond quickly and effectively to any network security event. There are many steps an entity can take during the preparation phase. Planning is obviously one such step. A network's defenses should also be assessed and tested at regular intervals in order to identify vulnerabilities.

Proactive measures must be taken to prevent intrusions. Some of the preventative actions that can be taken include patching systems (keeping software up-to-date), host security (hardening individual computers), network security (securing the perimeter of the network), and conducting user awareness and training. Finally, having well-thought-out policies, procedures, and guidelines adds significantly to an organization's preparedness.

Detection and Analysis—Detecting a security incident presents a significant challenge. Today's sophisticated attacks can mask themselves as "normal" network activity. Vigilance and a painstaking attention to detail are needed by network security personnel in order to improve their odds of catching an attack. It also helps them reach a proper conclusion after conducting their analysis. It's a well-known fact that Intrusion Detection Systems produce large numbers of false positives. As such, the security team must be capable of accurately sifting through data. What does an attack look like? That can be a little tough to describe. To better identify suspicious activity, it's best to get an accurate picture of what is "normal" network traffic or activity is for the organization. Some of the potential signs of an attack include antivirus software alerts, abnormally slow Internet connectivity, and abnormalities in network traffic.

Containment, Eradication, and Recovery—When a breach occurs, it must be controlled in order to minimize its impact. Left unchecked, the fallout from an attack could grow exponentially. How to contain the incident varies based on the type of incident being faced. Some containment options include shutting down the compromised system, disconnecting it from the network, or disabling some functionality. Once the attack has been identified and contained, steps could be required to remove any potentially dangerous components such as malicious code or compromised accounts.

Postincident Activity—Unfortunately, this valuable step is often overlooked. A postincident review represents a missed opportunity for the organization as a whole and its personnel to improve. A typical postincident review seeks to answer questions such as:

- What did we get right?
- What did we get wrong?
- Are our policies and procedures adequate and effective?
- Do we have the necessary resources to effectively respond?
- What, if anything, would we do differently?

Responding to a security breach effectively requires diverse skill sets. As part of an incident response plan, an organization should form a computer Incident Response Team. This multidisciplinary team should bring all of the skills necessary to manage the incident to the table. Some of the skills needed to respond include representatives from management, information security, IT support, legal, public affairs/media relations, and others (Scarphone, Grance, & Masone, 2008). Someone with digital forensics capabilities should be part of the team. Many times digital forensics resources do not exist within the company itself. In these instances this function would have to be outsourced. If this is indeed the situation, this resource should be identified well in advance of an actual incident.

NETWORK EVIDENCE AND INVESTIGATIONS

A hacker's attack typically follows a path both to and through the targeted network. As such, the potential exists to locate evidence all along the route. "Tracking" the intruder, therefore, is a critical step in the process of finding and identifying them. It is to our advantage to identify, follow, and examine as much of this trail as we can.

Our examination should include as many of the in-between or intermediary devices as possible. These intermediary devices, such as routers and servers, can hold valuable information and shouldn't be overlooked. Routers can be both an evidentiary source as well as a target for hackers. As a critical part of a network, they often serve as a valuable goal for hackers. If they can compromise a router, they can gain a significant foothold. A challenge with routers as a source of evidence is their volatility. You may recall from Chapter 2 that volatile memory requires constant electrical power to maintain its contents. Unplugging or rebooting the device will likely result in a loss of potential evidence. This will in all likelihood require a "live" examination of the device while it's running. The best advice is to handle with care and treat it as you would any other piece of volatile memory.

Digital evidence is digital evidence, regardless of its source. The fundamental principles and procedures of preservation and collection still apply.

LOG FILES

Many devices and computers in a network generate logs of events and activities. As such, log files serve as a primary source of evidence in network investigations. There are several different types of log files. Some of the logs of interest include authentication, application, operating system, and the firewall log. An **authentication log** identifies the account (and IP address) connected to a particular event.

Application logs record the date and time as well as the application identifier. The date/time stamps indicate when the application was started and how long it was used. **Operating system** logs track system reboots as well as the use of different devices. The operating system logs are useful in recognizing patterns of activity as well as anomalies (unusual occurrences) in the network.

Device logs such as those generated by routers and firewalls are also worth examining. We'll look at router logs more in just a second (Vacca & Rudolph, 2011).

There are some things to keep in mind with log files. Log files can change or disappear pretty rapidly. They can be purged at regular intervals to help keep storage space free. There's also a good chance that not all of the relevant logs will be in your possession. Attacks that originate outside of your organization will pass through devices under the control of a third party, such as an Internet Service Provider (ISP). These logs may have to be subpoenaed, which can take some time. ISPs won't likely hang onto these logs forever. They likely have document retention and destruction policies in place controlling what gets kept and for how long. Lacking a clear need or reason to keep it, those logs will be destroyed.

The router logs can contain much information of interest. Some of the things we can uncover are:

Requested Uniform Resource Locators (URLs)
Server Name
Server IP Address
Client's URL
Client IP Address
Who logged in and when

When attempting to collect evidence from a router, it's very important to minimize any interaction. Instead of accessing the router through the network itself, it's a better option to go through the router's console. Remember, our objective is to observe and record what we find, not to alter or change anything. To that end, we should avoid any command that could potentially modify any of the data. A configuration command, for example, is one that should be avoided. The "show" command is a much better option. Here are a couple of examples of "show" commands:

>(router name)#show clock detail—Displays the system time
>(router name)#show users—Displays the users that have access to the router

NETWORK INVESTIGATIVE TOOLS

The actual traffic (packets) moving on the network can hold some valuable clues. There are several tools, called "sniffers," available that can capture and analyze network traffic. Some of these tools include:

Wireshark (www.wireshark.org)
NetIntercept (http://www.niksun.com/product.php?id=16)
Netwitness Investigator (http://www.netwitness.com/products-services/investigator)
Snort (http://www.snort.org/)

Capturing network traffic can yield some great clues. For instance, we can determine what files have been stolen, what commands were executed, as well as any malicious payload that was delivered. From a legal perspective, it's important to realize that monitoring network traffic in certain instances can be considered wiretapping (Casey, 2009).

Network Investigation Challenges

Identifying the responsible hacker is by no stretch a simple task. There are many impediments along the way that can keep the attacker's identity hidden. The suspect can "spoof" his or her real IP address, potentially sending investigators on a wild goose chase. Along the same lines, the hacker can channel his or her attack through many intermediate servers scattered across the globe.

Logs can be a great source of evidence, but only if they are actually there for us to examine. Sometimes the logging function is disabled to start with, meaning that no logs were even generated. Time presents another concern. If the breach is discovered too late, then there is a significant chance that any logs maintained by an outside entity (an ISP, for example) will be destroyed pursuant to their retention and destruction policy. Hackers can also intentionally delete relevant logs during their attack, effectively covering their tracks. Lastly, jurisdiction can create a substantial obstacle. The attacker's trail can literally traverse state, national, and international boundaries. Different legal jurisdictions, especially international ones, can have wildly different requirements for obtaining this sort of information. Different countries may also have very different views of cybercrime in general, which can result in a lack of cooperation (Morris, 2005).

ADDITIONAL RESOURCES

Training and Research

Training and research are a must in the world of digital forensics. Established in 1989, the SANS Institute is one of the leading institutions meeting this critical need. They offer a wide array of courses and resources covering both information security and digital forensics. In addition, they offer many certifications that are accepted throughout the industry. They also have a strong presence on Twitter.

http://www.sans.org/
http://computer-forensics.sans.org/blog
@SANSInstitute
@sansforensics

SUMMARY

Network security should be a huge concern to all of us. Our networks and PCs are under near constant attack from lone hackers, organized criminals, and foreign countries. Cybercrime, cyberwar, and cyberterrorism are major problems threatening not only our countries and companies, but our personal computers as well. Networks represent a far greater challenge, from a forensic standpoint.

They vary wildly in size and complexity. There are several tools to help us protect our critical network infrastructure, including firewalls and intrusion detection systems. Smart organizations plan ahead for security breaches, enabling them to respond efficiently and effectively, minimizing the damage and increasing the odds that they can identify the perpetrator(s).

References

Bowden, M. (2011). *Worm: The First Digital World War*. New York: Atlantic Monthly Press.

Casey, E. (2009). *Handbook of Digital Forensics and Investigation*. Burlington, MA: Academic Press.

Casey, E. (2011). *Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet*. Waltham, MA: Academic Press.

Conrad, E., Misenar, S., & Feldman, J. (2010). *CISSP Study Guide*. Burlington, MA: Elsevier.

Garfinkel, S. (2002, October 7). *Kevin Mitnick and Anti-Social Engineering*. Retrieved November 9, 2011, from CSOOnline.com: http://www.csoonline.com/article/217395/kevin-mitnick-and-anti-social-engineering-

Hadnagy, C. (2011). *Social Engineering: The Art of Human Hacking*. Indianapolis: Wiley.

Krebs, B. (n.d.). *Coordinated ATM Heist Nets Thieves $13M*. Retrieved September 19, 2011, from: http://krebsonsecurity.com/2011/08/coordinated-atm-heist-nets-thieves-13m/

Keeney, M., Kowalski, E., Cappelli, D., Moore, A., Shimeall, T., and Rogers, S. (2005, May). *Insider threat study: Computer sabotage in critical infrastructure sectors. United States Secret Service and CERT program*. Report available at http://www.secretservice.gov

Maggiora, P. D., & Doherty, J. (2003). *Cisco Networking Simplified*. Indianapolis: Cisco Press.

McClure, S., Scambray, J., & Kurtz, G. (2009). *Hacking Exposed: Network Security Secrets and Solutions*. New York: McGraw-Hill.

Microsoft Corporation. (n.d.). *IPv6*. Retrieved September 17, 2011, from: http://technet.microsoft.com/en-us/network/bb530961.aspx

Mitnick, K. (2011). *Ghost in the Wires: My Adventures as the World's Most Wanted Hacker*. New York: Little, Brown and Company.

Morris, D. A. (2005, May 3). *Tracking a Computer Hacker*. Retrieved September 19, 2011, from: http://www.justice.gov/criminal/cybercrime/usamay2001_2.htm

Nikkel, B. J. (2007). *An Introduction to Investigating IPv6 Networks*. Digital Investigation: The International Journal of Digital Forensics and Incident Response Vol. 4, No. 2. Oxford, England: Elsevier.

Poulsen, K. (2011). *Kingpin: How One Hacker Took Over the Billion-Dollar Cybercrime Underground*. New York: Crown.

Prowell, S., Kraus, R., & Borkin, M. (2010). *Seven Deadliest Network Attacks*. Burlington, MA: Syngress.

Scarphone, K., Grance, T., & Masone, K. (2008). *Computer Security Incident Handling Guide*. National Institute of Standards and Technology, Computer Security Division. Gaithersburg, TN: National Institute of Standards & Technology.

TechTarget. (2000, August). *Intrusion Detection (ID)*. Retrieved September 17, 2011, from: http://searchmidmarketsecurity.techtarget.com/definition/intrusion-detection

TechTarget. (2000, October). *Firewall*. Retrieved September 17, 2011, from: http://searchsecurity.techtarget.com/definition/firewall

TechTarget. (2001, March). *Social Engineering*. Retrieved September 18, 2011, from: http://searchsecurity.techtarget.com/definition/social-engineering

TechTarget. (2002, January). *Snort*. Retrieved September 17, 2011, from: http://searchmidmarketsecurity.techtarget.com/definition/Snort

Vacca, J. R., & Rudolph, K. (2011). *System Forensics, Investigation, and Response*. Sudbury, MA: Jones and Bartlett Learning.

Verizon Business Global LLC, & United States Secret Sevice. (2011). *2011 Data Breach Investigations Report*. Ashburn New York: Verizon Business Global LLC.