

# Chapter 1

## Extending OSI to Network Security

### Solutions in this chapter:

- Our Approach to This Book
- Common Stack Attacks
- Mapping the OSI Model to the TCP/IP Model
- The Current State of IT Security
- Using the Information in this Book

- ☑ Summary
- ☑ Solutions Fast Track
- ☑ Frequently Asked Questions

## 2 Chapter 1 • Extending OSI to Network Security

# Introduction

“Everything old becomes new again.” The goal of this chapter is to take the well-known Open Systems Interconnect (OSI) model and use it to present security topics in a new and unique way. While each of the subsequent chapters focuses on one individual layer, this chapter offers a high-level overview of the entire book.

# Our Approach to This Book

This book is compiled of issues and concerns that security professionals must deal with on a daily basis. We look at common attack patterns and how they are made possible. Many attacks occur because of poor protocol design; others occur because of poor programming or lack of forethought when designing code. Finally, the tools that are useful for identifying and analyzing exploits and exposures are discussed—the tools you will return to time and time again.

## WARNING

Many of the tools discussed in this book can be used by both security professionals *and* hackers. Always make sure you have the network owner’s permission before using any of these tools, which will save you from many headaches and potential legal problems.

# Tools of the Trade

The following sections examine “protocol analyzers” and the Intrusion Detection Systems (IDSes), which are the two main tools used throughout this book.

# Protocol Analyzers

*Protocol analyzers* (or *sniffers*) are powerful programs that work by placing the host system’s network card into *promiscuous mode*, thereby allowing it to receive all of the data it sees in that particular collision domain. *Passive sniffing* is performed when a user is on a *hub*. When using a hub, all traffic is sent to all ports; thus, all a security professional or attacker has to do is start the sniffer and wait for someone on the same collision domain to begin transmitting data. A *collision domain* is a network segment that is shared but not bridged or switched; packets collide because users are sharing the same bandwidth.

Sniffing performed on a switched network is known as *active sniffing*, because it switches segment traffic and knows which particular port to send traffic to. While this feature adds much needed performance, it also raises a barrier when attempting to sniff all potential

switched ports. One way to overcome this impediment is to configure the switch to mirror a port. Attackers may not have this capability, so their best hope of bypassing the functionality of the switch is through *poisoning* and *flooding* (discussed in subsequent chapters).

Sniffers operate at the data link layer of the OSI model, which means they do not have to play by the same rules as the applications and services that reside further up the stack. Sniffers can capture everything on the wire and record it for later review. They allow user's to see all of the data contained in the packet. While sniffers are still a powerful tool in the hands of an attacker, they have lost some of their mystical status as many more people are using encryption.

The sniffer used in this book is called Ethereal, which is free and works well in both a Windows and a Linux environment. (Chapter 3 provides a more in-depth review of how to install and use Ethereal.) If you're eager to start using Ethereal, more details about the program can be found at [www.ethereal.com](http://www.ethereal.com). (Ethereal's name has been changed to Wireshark.)

## Intrusion Detection Systems

Intrusion detection systems (IDSes) play a critical role in protecting the Information Technology (IT) infrastructure. Intrusion detection involves monitoring network traffic, detecting attempts to gain unauthorized access to a system or resource, and notifying the appropriate individuals so that counteractions can be taken. The ability to analyze vulnerabilities and attacks with a sniffer and then craft a defense with an IDS is a powerful combination. The IDS system used in this book is Snort, which can be used with both Linux and Windows and has industry wide support.

### NOTE

Intrusion detection has a short history. In 1983, Dr. Dorothy Denning began developing the first IDS, which would be used by the U.S. government to analyze the audit trails of government mainframe systems.

Snort is a freeware IDS developed by Martin Roesch and Brian Caswell. It's a lightweight, network-based IDS that can be set up on a Linux or Windows host. While the core program uses a Command Line Interface (CLI), graphical user interfaces (GUIs) can also be used. Snort operates as a network sniffer and logs activity that matches predefined signatures. Signatures can be designed for a wide range of traffic, including Internet Protocol (IP), Transmission Control Protocol (TCP), User Datagram Protocol (UDP), and Internet Control Message Protocol (ICMP).

Snort consists of two basic parts:

- **Header** Where the rules "actions" are identified
- **Options** Where the rules "alert messages" are identified

To learn more about Snort, go to [www.Snort.org](http://www.Snort.org).

## 4 Chapter 1 • Extending OSI to Network Security

## Organization of This Book

This book is arranged in the same manner as the layers of the OSI model, which was developed to provide organization and structure to the world of networking. In 1983, the International Organization for Standardization (ISO) and the International Telegraph and Telephone Consultative Committee (CCITT) merged documents and developed the OSI model, which is based on a specific hierarchy where each layer builds on the output of each adjacent layer (see *ISO 7498*). Today, it is widely used as a guide for describing the operation of a networking environment, and also serves as a teaching model for hacks, attacks, and defenses.

The OSI model is a protocol stack where the lower layers deal primarily with hardware, and the upper layers deal primarily with software. The OSI model's seven layers are designed so that control is passed down from layer to layer. The seven layers of the OSI model are shown in Table 1.1

**Table 1.1** The Seven-Layer OSI Model

Layer	Responsibility
Application	Application support such as File Transfer Protocol (FTP), Telnet, and Hypertext Transfer Protocol (HTTP)
Presentation	Encryption, Server Message Block (SMB), American Standard Code for Information Interchange (ASCII), and formatting
Session	Data flow control, startup, shutdown, and error detection/correction
Transport	End-to-end communications, UDP and TCP services
Network	Routing and routable protocols such as IP and Open Shortest Path First (OSPF). Path control and best effort at delivery
Data link	Network interface cards, Media Access Control (MAC) addresses, framing, formatting, and organizing data
Physical	Transmission media such as twisted-pair cabling, wireless systems, and fiber-optic cable

The OSI model functions as follows:

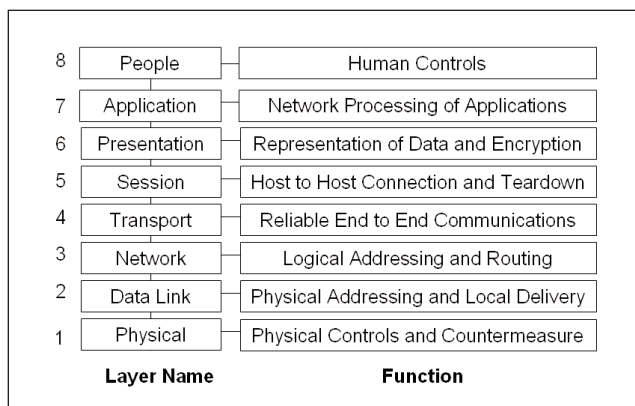
1. Information is introduced into the application layer and passed down until it ends up at the physical layer.
2. Next, it is transmitted over the physical medium (i.e., wire, coax, or wireless) and sent to the target device.
3. Once at the target device, it proceeds back up the stack to the application layer.

For this book, an eighth layer has been added to the OSI model that is called the “people” layer (or “social” layer). Figure 1.1 shows the eight layers and interprets the services of each.

**NOTE**

While the OSI model is officially seven layers, for the purposes of this book an additional layer (layer 8 [the “people” layer]) has been added to better address the different hacks and attacks that can occur in a networked environment.

**Figure 1.1** Hack the Stack’s Eight Layers



## The People Layer

Layer 8 is known as the *people layer*, and while not an official layer of the OSI model, it is an important consideration; therefore, it has been added to the OSI model for this book. People are often the weakest link. We can implement the best security solutions known at the lower layers of the OSI model and still be vulnerable through people and employees. Social engineering, phishing, phreaking, and dumpster diving are a few of the ways these attacks can be carried out.

### Notes from the Underground...

#### Phreaking in the Early Years

Hacking phone systems (or *phreaking*) predates computer hacking by many years. Phreakers used to use a variety of techniques to manipulate the phone system in order to make free phone calls. One early technique was called “blue boxing,” which worked by replicating the tones used to switch long distance

Continued

[www.syngress.com](http://www.syngress.com)

## 6 Chapter 1 • Extending OSI to Network Security

phone calls. In those days, the phone company used the same channel for switching that it used for voice communication. Blue boxing received its name because the first of these illegal devices recovered by the phone company were in blue plastic cases. One key element of the blue box was its ability to produce a 2600 hertz tone, which could be used to bypass the phone company's billing system and allow users to make free long distance phone calls.

Even if the phreaker lacked the ability to construct a blue box, all was not lost. In the early 1970s, it was discovered that the toy whistles given away in Capt-n-Crunch cereal could produce the same frequency tone. Anyone could use the whistle to signal a new call and then dial anywhere in the world for free.

### The Application Layer

Layer 7 is known as the *application layer*. Recognized as the official top layer of the OSI model, this layer serves as the window for application services. Layer 7 is not the actual application, but rather the channel through which applications communicate.

### The Presentation Layer

Layer 6 is known as the *presentation layer*. The main purpose of the presentation layer is to deliver and present data to the application layer. This data must be formatted so that the application layer can understand and interpret it. The presentation layer is responsible for items such as:

- Encryption and decryption of messages
- Compression and expansion of messages, format translation
- Handling protocol conversion

### The Session Layer

Layer 5 is known as the *session layer*. Its purpose is to allow two applications on different computers to establish and coordinate a session. It is also responsible for managing the session while information and data are being moved. When a data transfer is complete, the session layer tears down the session. Session-layer protocols include:

- Remote Procedure Call (RPC)
- Structured Query Language (SQL)

### The Transport Layer

Layer 4 is known as the *transport layer*. Whereas the application, presentation, and session layers are primarily concerned with data, the transport layer is focused on *segments*.

Depending on the application protocol being used, the transport layer can send data either quickly *or* reliably. Transport layer responsibilities include end-to-end error recovery and flow control. The two primary protocols found on this layer include:

- **TCP** A connection-oriented protocol; provides reliable communication using handshaking, acknowledgments, error detection, and session teardown
- **UDP** A connectionless protocol; offers speed and low overhead as its primary advantage

## The Network Layer

Layer 3 is known as the *network layer*, which is tied to software and deals with packets. The network layer is the home of the IP, which offers best effort at delivery and seeks to find the best route from the source to the target network. Network-layer components include:

- Routers
- Stateless inspection/packet filters

## The Data Link Layer

Layer 2 is known as the *data link layer* and is focused on traffic within a single local area network (LAN). The data link layer formats and organizes the data before sending it to the physical layer. Because it is a physical scheme, hard-coded Mandatory Access Control (MAC) addresses are typically used. The data link layer organizes the data into frames. When a frame reaches the target device, the data link layer strips off the data frame and passes the data packet up to the network layer. Data-link-layer components include:

- Bridges
- Switches
- Network Interface Card (NIC)
- MAC addresses

## The Physical Layer

Layer 1 of the OSI model is known as the *physical layer*. Bit-level communication takes place at layer 1. Bits have no defined meaning on the wire; however, the physical layer defines how long each bit lasts and how it is transmitted and received. Physical layer components include copper cabling, fiber cabling, wireless system components, and Ethernet hubs. The physical layer in this book has been extended to include:

## 8 Chapter 1 • Extending OSI to Network Security

- Perimeter security
- Device Security
- Identification and authentication

# Common Stack Attacks

A range of exploits can be launched in any stack-based system. For this book, we followed the stack-based approach of arranging the various attacks into a logical order for discussion of the risks and potential solutions. Let's look at some of the attacks and the layers where they can be found.

## The People Layer

One of the biggest threats at this layer is *social engineering*, because it targets people. Some organizations spend a fortune on technical controls but next to nothing on training and educating employees on security processes and procedures. Attackers use various techniques (e.g., trust) to trick individuals into complying with their wishes. As with other types of attacks, the bulk of the work of a social engineering attack is doing the reconnaissance and laying the groundwork. The attack itself usually takes on one of the following angles:

- **Diffusion of Responsibility** I know the policy is not to give out passwords, but I will take responsibility for this.
- **Identification** We both work for the same company; this benefits everyone.
- **Chance for Ingratiation** This is a win-win situation. The company is going to reward you for helping me in this difficult situation.
- **Trust Relationships** Although I am new here, I am sure I have seen you in the break room.
- **Cooperation** Together we can get this done.
- **Authority** I know what the policy is; I drafted those policies and I have the right to change them.

Another threat at the people layer is *dumpster diving*. Many companies throw out an amazing amount of stuff (e.g., old hardware, software, post-it pads, organizational charts, printouts of names and passwords, source code, memos and policy manuals). All of these items offer a wealth of information to an attacker.

## The Application Layer

Most of the applications listed in this section are totally insecure because they were written for a different time. At the beginning of the networked world, most systems were mainframes

that were locked in government and business buildings. There were no Category 5 cables interconnecting every office in the building, and no open wireless access points were being broadcast from the apartment next door. Suppressing passwords and other critical information on the monitor was considered robust enough to protect information and data. Here's a short list of some of the insecure applications and high-level protocols:

- **FTP** FTP is a TCP service that operates on ports 20 and 21 and is used to move files from one computer to another. Port 20 is used for the data stream, and transfers the data between the client and the server. Port 21 is the control stream, and is used to pass commands between the client and the FTP server. Attacks on FTP target misconfigured directory permissions and compromised or sniffed cleartext passwords. FTP is one of the most commonly hacked services.
- **Telnet** Telnet is a TCP shell service that operates on port 23. Telnet enables a client at one site to establish a session with a host at another site. The program passes the information typed at the client's keyboard to the host computer system. While Telnet can be configured to allow anonymous connections, it should also be configured to require usernames and passwords. Unfortunately, even then, Telnet sends them in cleartext. When a user is logged in, he or she can perform any allowed task.
- **Simple Mail Transfer Protocol (SMTP)** This application is a TCP service that operates on port 25, and is designed to exchange electronic mail between networked systems. Messages sent through SMTP have two parts: an address header and the message text. All types of computers can exchange messages with SMTP. *Spoofing* and *spamming* are two of the vulnerabilities associated with SMTP.
- **Domain Name Service (DNS)** This application operates on port 53, and performs address translation. DNS converts fully qualified domain names (FQDNs) into a numeric IP address and converts IP addresses into FQDNs. DNS uses UDP for DNS queries and TCP for zone transfers. DNS is subject to poisoning and if misconfigured, can be solicited to perform a full zone transfer.
- **Trivial File Transfer Protocol (TFTP)** TFTP operates on port 69, and is a connectionless version of FTP that uses UDP to reduce overhead and reliability. It does so without TCP session management or authentication, which can pose a big security risk. It is used to transfer router configuration files and to configure cable modems. People hacking those cable modems are known as *uncappers*.
- **Hypertext Transfer Protocol (HTTP)** HTTP is a TCP service that operates on port 80. HTTP helped make the Web the popular service that it is today. The HTTP connection model is known as a *stateless connection*. HTTP uses a request response protocol where a client sends a request and a server sends a response. Attacks that exploit HTTP can target the server, browser, or scripts that run on the browser. Nimda is an example of the code that targeted a Web server.

## 10 Chapter 1 • Extending OSI to Network Security

- **Simple Network Management Protocol (SNMP)** SNMP is a UDP service that operates on ports 161 and 162, and was designed to be an efficient and inexpensive way to monitor networks. The SNMP protocol allows agents to gather information (e.g., network statistics) and report back to their management stations. Some of the security problems that plague SNMP are caused by the fact that community strings are passed as cleartext and the default community strings (public/private) are well known. SNMP version 3 is the most current and offers encryption for more robust security.

### The Session Layer

There is a weakness in the security controls at the presentation and *session layers*. Let's look at the Windows NT LanMan (NTLM) authentication system. Originally developed for Windows systems and then revised for Windows NT post service pack 2 systems, this security control proved to be an example of weak encryption (i.e., many passwords encrypted with this system could be cracked in less than 1 second because of the way Microsoft stored the hashed passwords). An NTLM password is uppercase, padded to 14 characters, and divided into seven character parts. The two hashed results are concatenated and stored as a LAN Manager (LM) hash, which is stored in the SAM. The session layer is also vulnerable to attacks such as *session hijacking*. Network Basic Input/Output System (NetBIOS) is another service located in this area of the stack. (Subsequent chapters go into greater detail regarding the various types of encryption (e.g., hashing).

NetBIOS was developed for IBM and adopted by Microsoft, and has become an industry standard. It allows applications on different systems to communicate through the LAN. On LANs, hosts using NetBIOS systems identify themselves using a 15-character unique name. Since NetBIOS is non-routable, Microsoft adapted it to run over Transmission Control Protocol/Internet Protocol (TCP/IP). NetBIOS is used in conjunction with SMB, which allows for the remote access of shared directories and files. This key feature of Windows makes file and print sharing and the Network Neighborhood possible. It also introduced other potential vulnerabilities into the stack by giving attackers the ability to enumerate systems and gather user names and accounts, and share information. Almost every script kiddie and junior league hacker has exploited the *net use* command.

### The Transport Layer

The *transport layer* is rife with vulnerabilities, because it is the home of UDP and TCP. Because UDP is connectionless, it's open for attackers to use for a host of denial of service (DoS) attacks. It's also easy to spoof and requires no confirmation. TCP is another used and abused protocol. Port scanning and TCP make the hacker trade possible. Before a hacker can launch an attack, he or she must know what is running and what to target. TCP makes this possible. From illegal flag settings, NULL, and XMAS, to more common synchronous (SYN) and reset (RST) scans, TCP helps attackers identify services and operating systems.

At the network level are services such as IP and ICMP. IPv4 has no security services built in, which is why Secure Internet Protocol (IPSec) (a component of IPv6) was developed. Without IPSec, IP can be targeted for many types of attacks (e.g., DOS), abused through source routing, and tricked into zombie scanning “IPID Scan.” While ICMP was developed for diagnostics and to help with logical errors, it is also the target of misuse. ICMP can be used to launch Smurf DoS attacks or can be subverted to become a covert channel with programs such as Loki.

## The Data Link Layer

The dangers are real at the *data link layer*. Conversion from logical to physical addressing must be done between the network and data link layers. Address Resolution Protocol (ARP) resolves logical to physical addresses. While critical for communication, it is also used by attackers to bypass switches and monitor traffic, which is known as *ARP poisoning*. Even without ARP poisoning, passive sniffing can be a powerful tool if the attacker positions himself or herself in the right place on the network.

## The Physical Layer

An attacker gaining access to the telecommunications closet, an open port in the conference room, or an unused office, could be the foothold needed to breach the network or, even worse, gain physical access to a server or piece of equipment. It’s a generally accepted fact that if someone gains physical access to an item, they can control it. The Cisco site provides a page that explains how to reset the password and gain entry into a Cisco device ([www.cisco.com/warp/public/474/pswdrec\\_2500.html](http://www.cisco.com/warp/public/474/pswdrec_2500.html)). Figure 1.2 lists each layer of the stack and many of the common attacks and vulnerabilities found at those layers.

### WARNING

Logical controls are of little value if no physical controls are put in place (i.e., the best logical controls are of little value if an attacker can walk in and reboot a server or gain physical access of the SAM and its passwords).

## Notes from the Underground...

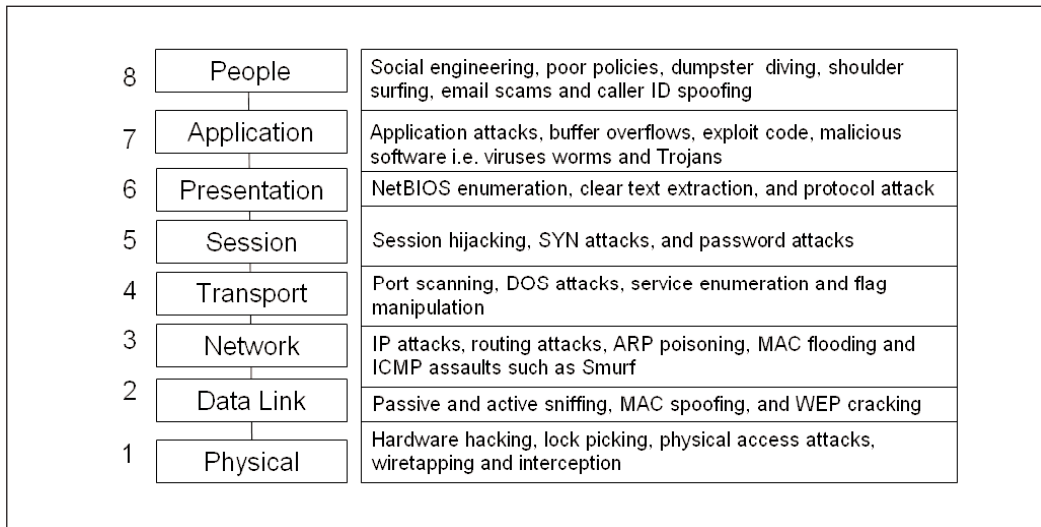
### The Importance of Physical Controls

Current and past U.S. military veterans recently learned the value of physical security controls when it was revealed that the personal details of as many as 26.5 million veterans were lost, even though the Department of Veterans Affairs had security measures in place.

On May 3, 2006, several items were stolen from a Veterans Affairs information security specialist's home. Among the items stolen were a laptop and a small external hard drive containing the unencrypted names, birthdates, and social security numbers of almost 26.5 million veterans. While the theft was reported that same day, what remains unclear is why the security specialist took such sensitive data home, which was in clear violation of existing policy.

Even though the laptop and data were eventually recovered, it does not negate the breach of confidentiality or the fact that stronger security controls should have been used.

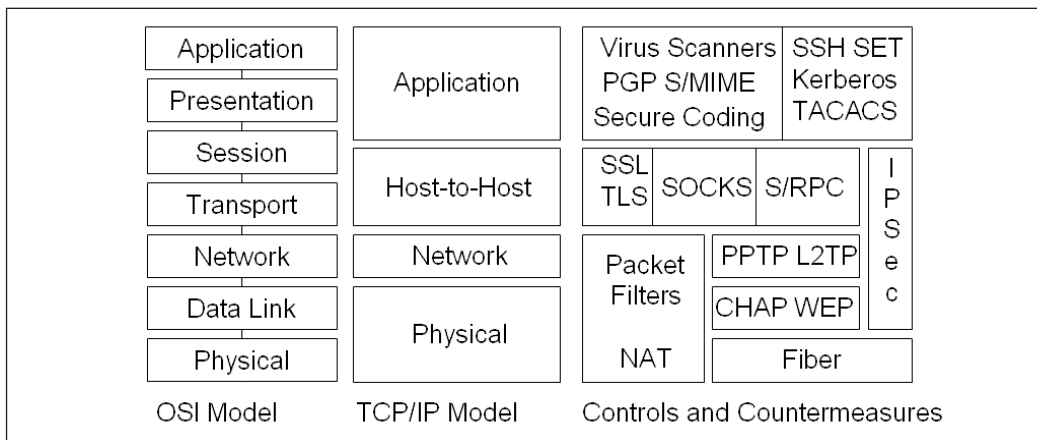
**Figure 1.2** Stack Attacks and Vulnerabilities



## Mapping OSI to TCP/IP

Although the OSI model proved itself as a teaching model, it was never fully adopted. The Department of Defense (DoD), funder of the original Advanced Research Projects Agency Network (ARPANET) research, implemented the TCP/IP model, which became the foundation of the Internet as we know it today. TCP/IP is similar to the OSI model, but consists of only four layers, which include the *physical layer*, the *network layer*, the *host-to-host layer*, and the *application layer*. Figure 1.3 illustrates the relationship of the OSI model to the TCP/IP model and shows some primary defenses that can be used to make the stack more secure.

**Figure 1.3** The OSI Model, TCP/IP Model, and Common Countermeasures



A wide range of protective mechanisms are shown at the various layers. The reason why so many countermeasures were developed can be traced to the early development of TCP/IP, which was originally developed as a flexible, fault tolerant network; security was not the driving concern. The network was designed to these specifications to withstand a nuclear strike that might destroy key routing nodes. The designers of this original network never envisioned the Internet used today; therefore, many TCP/IP protocols and applications are insecure. Security controls like IPsec are add-ons to the original protocol suite.

### NOTE

Layering defensive techniques on top of one another is known as *defense in depth*. This technique seeks to delay and deter attackers by buying time and delaying the ultimate succession of the attack. It is designed so that if one security control fails, it is unlikely that the same attack will penetrate the next layer.

## Countermeasures Found in Each Layer

Security countermeasures are the controls used to protect the confidentiality, integrity, and availability of data and information systems. There is a wide array of security controls available at every layer of the stack. Overall security can be greatly enhanced by adding additional security measures, removing unneeded services, hardening systems, and limiting access (discussed in greater detail throughout the book and introduced in this section).

- **Virus Scanners** Antivirus programs can use one or more techniques to check files and applications for viruses. While virus programs didn't exist as a concept until 1984, they are now a persistent and perennial problem, which makes maintaining antivirus software a requirement. These programs use a variety of techniques to scan and detect viruses, including signature scanning, heuristic scanning, integrity checks, and activity blocking.
- **Pretty Good Privacy (PGP)** In 1991, Phil Zimmerman initially developed PGP as a free e-mail security application, which also made it possible to encrypt files and folders. PGP works by using a public-private key system that uses the International Data Encryption Algorithm (IDEA) algorithm to encrypt files and e-mail messages.
- **Secure Multipurpose Internet Mail Extensions (S/MIME)** S/MIME secures e-mail by using X.509 certificates for authentication. The Public Key Cryptographic Standard is used to provide encryption, and can work in one of two modes: *signed* and *enveloped*. Signing provides integrity and authentication. Enveloped provides confidentiality, authentication, and integrity.
- **Privacy Enhanced Mail (PEM)** PEM is an older e-mail security standard that provides encryption, authentication, and X.509 certificate-based key management.
- **Secure Shell (SSH)** SSH is a secure application layer program with different security capabilities than FTP and Telnet. Like the two aforementioned programs, SSH allows users to remotely log into computers and access and move files. The design of SSH means that no cleartext usernames/passwords can be sent across the wire. All of the information flowing between the client and the server is encrypted, which means network security is greatly enhanced. Packets can still be sniffed but the information within the packets is encrypted.
- **Secure Electronic Transmission (SET)** SET is a protocol standard that was developed by MasterCard, VISA, and others to allow users to make secure transactions over the Internet. It features digital certificates and digital signatures, and uses of Secure Sockets Layer (SSL).
- **Terminal Access Controller Access Control System (TACACS)** Available in several variations, including TACACS, Extended TACACS (XTACACS), and

TACACS+. TACACS is a centralized access control system that provides authentication, authorization, and auditing (AAA) functions.

- **Kerberos** Kerberos is a network authentication protocol created by the Massachusetts Institute of Technology (MIT) that uses secret-key cryptography and facilitates single sign-on. Kerberos has three parts: a client, a server, and a trusted third party (Key Distribution Center [KDC] or AS) to mediate between them.
- **SSL** Netscape Communications Corp. initially developed SSL to provide security and privacy between clients and servers over the Internet. It's application-independent and can be used with HTTP, FTP, and Telnet. SSL uses Rivest, Shamir, & Adleman (RSA) public key cryptography and is capable of client authentication, server authentication, and encrypted SSL connection.
- **Transport Layer Security (TLS)** TLS is similar to SSL in that it is application-independent. It consists of two sublayers: the *TLS record protocol* and the *TLS handshake protocol*.
- **Windows Sockets (SOCKS)** SOCKS is a security protocol developed and established by Internet standard *RFC 1928*. It allows client-server applications to work behind a firewall and utilize their security features.
- **Secure RPC (S/RPC)** S/RPC adds an additional layer of security to the RPC process by adding Data Encryption Standard (DES) encryption.
- **IPSec** IPSec is the most widely used standard for protecting IP datagrams. Since IPSec can be applied below the application layer, it can be used by any or all applications and is transparent to end users. It can be used in *tunnel mode* or *transport mode*.
- **Point-to-point Tunneling Protocol (PPTP)** Developed by a group of vendors including Microsoft, 3Com, and Ascend, PPTP is comprised of two components: the *transport* that maintains the virtual connection and the *encryption* that insures confidentiality. PPTP is widely used for virtual private networks (VPNs).
- **Challenge Handshake Authentication Protocol (CHAP)** CHAP is an improvement over previous authentication protocols such as Password Authentication Protocol (PAP) where passwords are sent in cleartext. CHAP uses a predefined secret and a pseudo random value that is used only once (i.e., a hash is generated and transmitted from client to server). This facilitates security because the value is not reused and the hash cannot be reversed-engineered.
- **Wired Equivalent Privacy (WEP)** While not perfect, WEP attempts to add some measure of security to wireless networking. It is based on the RC4 symmetric encryption standard and uses either 64-bit or 128-bit keys. A 24-bit Initialization Vector (IV) is used to provide randomness; therefore, the "real key"

## 16 Chapter 1 • Extending OSI to Network Security

may be no more than 40 bits long. There have been many proven attacks based on the weaknesses of WEP.

- **Wi-Fi Protected Access (WPA)** WPA was developed as a replacement for WEP. It delivers a more robust level of security. WPA uses Temporal Key Integrity Protocol (TKIP), which scrambles the keys using a hashing algorithm and adds an integrity-checking feature that verifies that the keys haven't been tampered with. Next, WPA improves on WEP by increasing the IV from 24 bits to 48 bits. WPA also prevents rollover (i.e., key reuse is less likely to occur). Finally, WPA uses a different secret key for each packet.
- **Packet Filters** Packet filtering is configured through access control lists (ACLs). ACL's allow rule sets to be built that will allow or block traffic based on header information. As traffic passes through the router, each packet is compared to the rule set and a decision is made whether the packet will be permitted or denied.
- **Network Address Translation (NAT)** Originally developed to address the growing need for intrusion detection (ID) addresses, NAT is discussed in *RFC 1631*. NAT can be used to translate between private and public addresses. Private IP addresses are those considered non-routable (i.e., public Internet routers will not route traffic to or from addresses in these ranges).
- **Fiber Cable** The type of transmission media used can make a difference in security. Fiber is much more secure than wired alternatives and unsecured wireless transmission methods.
- **Secure Coding** It is more cost-effective to build secure code up front than to try and go back and fix it later. Just making the change from C to a language such as .NET or CSharp can have a big security impact. The drive for profits and the additional time that QA for security would introduce, causes many companies to not invest in secure code.

## The Current State of IT Security

According to [www.Cert.org](http://www.Cert.org), in the year 2000 there were 1,090 vulnerabilities reported, in 2001 there were 2,437, and in 2005 that number climbed to 5,990. With such an increase in the number of known vulnerabilities, it's important to consider how we got to this current state. There is also real value in studying the past to try and learn from our mistakes and prevent them in the future. What follows is a somewhat ordered look at the history of security.

## Physical Security

Long before any other type of security was created, *physical security* existed. The Egyptians used locks more than 2,000 years ago. If information was important, it was carved in stone or later written on paper.

When information was transmitted or moved from one location to another, it was usually done with armed guards. The only way for the enemy to gain the information was to physically seize it. The loss of information usually meant the loss of critical assets, because knowledge is power. Even when information was not in transit, many levels of protection were typically used to protect it, including guards, walls, dogs, moles, and fences.

## Communications Security

All of the concerns over physical security made early asset holders concerned about the protection of their assets. Think about it: one mistake in transit meant that your enemy was now in control of vital information. There had to be a way to protect information in transit and in storage beyond physical storage.

A means of security was found in the discovery of *encryption*, which meant that the confidentiality of information in-transit could be ensured. Encryption dates to the Spartans, who used a form of encryption known as Skytale. The Hebrews used a basic cryptographic system called ATBASH that worked by replacing each letter used with another letter the same distance away from the end of the alphabet (e.g., “A” would be sent as a Z and “B” would be sent as a “Y”). More complicated substitution ciphers were developed throughout the middle ages as individuals became better at breaking simple encryption systems. In the ninth century, Abu al-Kindi published what is considered to be the first paper that discusses how to break cryptographic systems. It is titled “A Manuscript on Deciphering Cryptographic Messages,” and deals with using frequency analysis to break cryptographic codes.

After the first part of the twentieth century, the science of encryption and cryptography moved more quickly because the US government and the National Security Agency (NSA) became involved. One of the key individuals that worked with the NSA in its early years was William Frederick Friedman, who is considered one of the best cryptologists of all time. Mr. Friedman helped break the encryption scheme used by the Japanese. Many of his inventions and cryptographic systems were never patented, because they were considered so significant that the release of any information about them would aid the enemy.

## Signal Security

While encryption provided another level of needed security, history shows that it wasn't always enough. Systems like telephones were known to be vulnerable; at the same time, work began on a system to intercept electronic emissions from other systems. This developed into the TEMPEST program, a US-led initiative designed to develop shielding for equipment to make it less vulnerable to signal theft.

## 18 Chapter 1 • Extending OSI to Network Security

The problem of *signal security* repeated itself when the first cordless phones were released. The early cordless phones had no security. If you and your neighbor had the same frequency or you had a scanner, your conversations were easy to intercept. Early cell phones were also easily intercepted.

Luckily, there have been advances in signal security such as *spread spectrum* technology, which was pioneered by the military. This technology is implemented in two different methods: *direct-sequence spread spectrum (DSSS)* and *frequency-hopping spread spectrum (FHSS)*. These systems of transmission provide security and improved reliability.

## Computer Security

*Computer security* is focused on secure computer operations. The *protection ring* model provides the operating system with various levels at which to execute code or restrict access. It provides much greater granularity than a system that operates in user and privileged mode. As you move toward the outer bounds of the model, the numbers increase and the level of trust decreases.

Another advancement in computer security was in the development of computer security models based on confidentiality and integrity. The Bell LaPadula model was one of the first and was designed to protect the confidentiality of information. The Clark-Wilson model was the first integrity model, and differed from previous models because it was developed with the intention to be used for commercial activities. Clark Wilson dictates that the separation of duties must be enforced, subjects must access data through an application, and auditing is required.

Bell LaPadula, Clark Wilson, and others led the US government to adopt standards to measure these computer security controls. One of the first of these standards to be developed was the Trusted Computing System Evaluation Criteria (TCSEC) (also known as the “Orange Book”). The Orange Book defines the confidentiality of computer systems according to the following scale:

- **A: Verified Protection** The highest security division
- **B: Mandatory Security** Has mandatory protection of the TCB
- **C: Discretionary Protection** Provides discretionary protection of the TCB
- **D: Minimal Protection** Failed to meet any of the standards of A, B, or C; has no security controls

## Network Security

While *network security* has long been a concern, the advent of the Internet and the growth of e-commerce have increased the need. Most home users no longer use slow dial-up connections; they use DSL or cable Internet. Not only is there increased bandwidth, but many of these systems are always turned on, which means that attackers can benefit from the bandwidth available to these users to launch attacks.

The need for network security was highlighted by the highly successful attacks such as Nimda, Code Red, and SQL Slammer. Nimda alone is believed to have infected more than 1.2 million computers. Once a system was infected, Nimda scanned the hard drive once every 10 days for e-mail addresses, which were used to send copies of itself to other victims. Nimda used its own internal mail client, making it difficult for individuals to determine who sent the infected e-mail. Nimda also had the capability to add itself to executable files to spread itself to other victims. Exploits such as these highlight the need for better network security.

Organizations are responding by implementing better network security. Firewalls have improved. Many companies are moving to intrusion prevention systems (IPS), and antivirus and e-mail-filtering products have become must-have products. However, these systems don't prevent crime; they simply move the criminal down to other unprotected sites. The same analogy can be applied to network security. While some organizations have taken the threat seriously and built adequate defenses, many others are still unprotected. All of the virus infections, dangers of malicious code, and DoS zombies are simply relocated to these uncaring users.

## Information Security

Where does this leave us? Physical security is needed to protect our assets from insiders and others who gain access. Communication security is a real requirement as encryption offers a means to protect the confidentiality and integrity of information in storage and in transit. Signal security gives us the ability to prevent others from intercepting and using signals that emanate from our facility and electronic devices. Computer security provides us the ability to trust our systems and the operating systems on which they are based. It provides the functionality to control who has read, write, execute, or full control over our data and informational resources. Network security is another key component that has grown in importance as more and more systems have connected to the Internet. This means there is a need for availability, which can be easily attacked. The Distributed Denial of Service (DDoS) attacks against Yahoo and others in 2000 are good examples of this.

None of the items discussed by themselves are enough to solve all security risks. Only when combined together and examined from the point of information security can we start to build a complete picture. In order for information security to be successful, it also requires senior management support, good security policies, risk assessments, employee training, vulnerability testing, patch management, good code design, and so on.

## Using the Information in This Book

This book is designed to demonstrate vulnerabilities, defenses, and countermeasures. Therefore it can be used as a tool to better understand common flaws and also for testing and better security for the IT infrastructure. Security is about finding a balance, because all systems have limits. No one person or company has unlimited funds to secure everything, therefore, they can't always take the most secure approach. This requires risk management.

## 20 Chapter 1 • Extending OSI to Network Security

Security professionals can use this book to assess their network and help in the process of decision-based security, risk acceptance, avoidance, and reduction.

# Vulnerability Testing

Different types of security tests can be performed, ranging from those that merely examine policy (audit) to those that attempt to hack in from the Internet and mimic the activities of true hackers (penetration testing). The process of *vulnerability testing* includes a systematic examination of an organization's network, policies, and security controls. The purpose is to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of potential security measures, and confirm the adequacy of such measures after implementation.

### WARNING

When performing vulnerability tests, never exceed the limits of your authorization. Every assignment has rules of engagement, which not only include what you are authorized to target, but also the extent that you are authorized to control or target such systems.

While you may be eager to try out some of the tools and techniques you find in this book, make certain that you receive written approval before beginning. Proper authorization through documented means is a critical event in the testing process. Before any testing begins, you need to receive approval in writing. Even basic vulnerability testing tools like Nessus can bring down a computer system.

# Security Testing

There are a variety of ways that an organization's IT infrastructure can be probed, analyzed, and tested. Some common types of tests are:

- **Security Audits** This review seeks to evaluate how closely a policy or procedure matches the specified action. Are security policies actually used and adhered to? Are they sufficient?
- **Vulnerability Scanning** Tools like Nessus and others can be used to automatically scan single hosts or large portions of the network to identify vulnerable services and applications.
- **Ethical Hacks (Penetration Testing)** Ethical hacks seek to simulate the types of attacks that can be launched across the Internet. They can target HTTP, SMTP, SQL, or any other available service.

- **Stolen Equipment Attack** This simulation is closely related to physical security and communication security. The goal is to see what information is stored on company laptops and other easily accessible systems. Strong encryption is the number one defense for stolen equipment attacks. Otherwise attackers will probably be able to extract critical information, usernames, and passwords.
- **Physical Entry** This simulation seeks to test the organization's physical controls. Systems such as doors, gates, locks, guards, Closed Circuit Television (CCTV), and alarms are tested to see if they can be bypassed.
- **Signal Security Attack** This simulation is tasked with looking for wireless access points and modems. The goal is to see if these systems are secure and offer sufficient authentication controls.
- **Social Engineering Attack** Social engineering attacks target an organization's employees and seeks to manipulate them in order to gain privileged information. Proper controls, policies and procedures, and user education can go a long way in defeating this form of attack.

Many methodologies can be used to help perform these security tests. One well-known open-sourced methodology is the Open Source Security Testing Methodology Manual (OSSTMM). The OSSTMM divides security reviews into six key points known as sections:

- Physical Security
- Internet Security
- Information Security
- Wireless Security
- Communications Security
- Social Engineering

Other documents that are helpful when assessing security include *NIST 800-42*, *NIST 800-26*, *OCTAVE*, and *ISO 17799*.

## Finding and Reporting Vulnerabilities

If your security testing is successful, you will probably find some potential vulnerabilities that need be fixed. Throughout the security testing process you should be in close contact with management to keep them abreast of your findings. There shouldn't be any big surprises dropped on management at the completion of the testing. Keep them in the loop. At the conclusion of these assessment activities, you should report on your initial findings before you develop a final report. You shouldn't be focused on solutions at this point, but on what you found and its potential impact.

**22 Chapter 1 • Extending OSI to Network Security**

Keep in mind that people don't like to hear about problems. Many times, administrators and programmers deny that a problem exists or that the problem is of any consequence. There have been many stories about well-meaning security professional being threatened with prosecution after reporting vulnerabilities. If you feel you must report a vulnerability in a system other than your own, [www.cert.org](http://www.cert.org) has developed a way to report these anonymously. While this step does not guarantee anonymity, it does add a layer of protection. This form can be found at [www.cert.org/reporting/vulnerability\\_form.txt](http://www.cert.org/reporting/vulnerability_form.txt).

**Tools & Traps...****Reporting Vulnerabilities May Get You More Than You Bargained For**

Eric McCarty thought he was doing the right thing when he tried to report a vulnerability in a Web-based system at the University of Southern California. The University did not see it the same way and turned the case over to the FBI. Even when they appeared at Mr. McCarty's home, he still thought he had nothing to worry about.

Those thoughts quickly turned to dread when he was informed that he was being charged with one count of computer intrusion. What is unfortunate but true is that whenever you do something unnecessary (e.g., reporting a vulnerability), the asset's owners start to wonder why. Any people exposing vulnerabilities on systems that they don't own or control may quickly find themselves accused of being a hacker. The end result is that many researchers are now advising individuals to walk away and not report vulnerabilities, because it is not worth the risk.

## Summary

This chapter introduced “hack the stack.” The goal of this chapter was to show a new way of looking at vulnerabilities and security controls. The concept is that the basic stack model is something that most people in the business are familiar with. Therefore programmers, security professionals, and network administrators can start to put these critical issues into perspective. Security is a continually changing, multifaceted process that requires you to build a multilayered defense-in-depth model. The stack concept demonstrates that defense can be layered at levels throughout the process. Physical protection, data link access controls, secure host-to-host connection mechanisms, and well-written hardened applications together provide the assurance needed for robust security.

## Solutions Fast Track

### Our Approach to the Book

- ☑ This book approaches vulnerabilities and exploits in a layer-by-layer manner
- ☑ It examines exploits and also countermeasures that can be used to secure systems
- ☑ It looks inside the operation of the protocols. What does the tool do? How does it manipulate the application or protocol?

### Common Stack Attacks

- ☑ **Social Engineering** One of the most efficient attacks, because it bypasses stack-based controls and targets the user, which allows the attacker to bypass the most stringent logical controls.
- ☑ **Poor Coding** Applications are not like vehicles or other consumer products. If you get a defective one there will be no massive recalls or huge consumer lawsuits. You'll be forced to wait for a patch and hope it doesn't introduce other problems into the network.
- ☑ **Weak Applications** Too many people use weak applications such as FTP and Telnet, which were never designed for the situations they are used in today.

### Mapping the OSI Model to the TCP/IP Model

- ☑ While the OSI model is great for learning, it was never fully implemented.
- ☑ TCP/IP comprises of four layers that map closely to the OSI model. The same security issues apply to each.

## 24 Chapter 1 • Extending OSI to Network Security

- ☑ TCP/IP was never designed for security. It was developed to be a flexible, fault-tolerant set of protocols that wouldn't suffer from a single point of failure.

### The Current State of IT Security

- ☑ The number of vulnerabilities continues to increase each year. In 2005, almost 6,000 were reported.
- ☑ Security is evolving. At one point in history, physical security was the paramount concern. However, computers changed this focus and the reliance on networked communications changed it again.
- ☑ Security requires defense in depth. With so many potential attack vectors, security professionals must set up multiple layers of security and many different defenses to protect informational assets.

### Using the Information in this Book

- ☑ This book can be used to help increase the security of the applications, data, and systems under your control
- ☑ A better understanding of the underlying functionality of key protocols and services can help you choose better security solutions.
- ☑ Security is about balance. It means finding the right level of protection balanced against the value of the asset and its importance to the organization.

## Frequently Asked Questions

The following Frequently Asked Questions, answered by the authors of this book, are designed to both measure your understanding of the concepts presented in this chapter and to assist you with real-life implementation of these concepts. To have your questions about this chapter answered by the author, browse to [www.syngress.com/solutions](http://www.syngress.com/solutions) and click on the “Ask the Author” form.

**Q:** Why develop a hacking book based on the OSI model?

**A:** It's a common model that is known to everyone. There are many books that list one security tool after another. Anyone can use a tool, but to understand what the tool does and how it works allows for a higher level of learning.

**Q:** Why do you list Ethereal as one of the most important tools a security professional can use?

**A:** Because it allows you to examine what is happening at the wire level. Being able to examine packets as they traverse the network can help you understand the functionality of attacks and exploits.

**Q:** What is the most important tool a security professional has?

**A:** Knowledge. Having the ability to really know how the protocols work adds a higher level of understanding.

**Q:** Has the state of network security improved?

**A:** Yes, but it's a game of cat and mouse. As security increases, so do the attacks that hackers launch.

**Q:** What is the value of dividing up security into groups such as physical, communication, and network?

**A:** Attacks can come from many angles. Any of the security documentation you examine, such as the OSSTMM or ISO17799, divides the IT infrastructure into various sub-groups. This helps break down and organize the complexity and number of tests that must be performed to ensure good security.

**26 Chapter 1 • Extending OSI to Network Security**

**Q:** Why write a book that can be used by hackers?

**A:** Hackers already have the knowledge. It's important to put it into the hands of security professionals.

**Q:** Do you really see danger in someone reporting vulnerabilities?

**A:** Yes. If it is not a system under your control you must be very careful of what you are doing. It's easy to run afoul of specific laws and regulations. It's best to get signed consent before performing any tests.