SECOND EDITION

Principles of Computer Security

CompTIA Security+™ and Beyond

VINCENT NESTLER
CompTIA Security+

GREGORY WHITE, PH.D.

WM. ARTHUR CONKLIN, PH.D.
CompTIA Security+, CISSP®

appendix A

Objectives Map: CompTIA Security+

Topic	Chapter(s)
1.0 Systems Security	
1.1 Differentiate among various systems security threats.	
Privilege escalation	15
Virus	15, 16
Worm	15, 16
Trojan	15, 16
Spyware	15, 16
Spam	15, 16
Adware	15, 16
Rootkits	15
Botnets	15
Logic bomb	15
1.2 Explain the security risks pertaining to system hardware and peripherals.	
BIOS	10
USB devices	10
Cell phones	10
Removable storage	10
Network attached storage	10
1.3 Implement OS hardening practices and procedures to achieve workstation and server security.	
Hotfixes	10, 14
Service packs	10, 14
Patches	10, 14
Patch management	10, 14
Group policies	14
Security templates	14
Configuration baselines	14
1.4 Carry out the appropriate procedures to establish application security.	
ActiveX	17
Java	17
Scripting	17
Browser	17
Buffer overflows	17, 18

Topic	Chapter(s)
Cookies	17
SMTP open relays	17, 18
Instant messaging	16, 17
P2P	17
Input validation	17, 18
Cross-site scripting (XSS)	17
1.5 Implement security applications.	
HIDS	13
Personal software firewalls	10, 13
Antivirus	10, 13
Anti-spam	10, 13
Popup blockers	10, 13
1.6 Explain the purpose and application of virtualization technology.	
	10
2.0 Network Infrastructure	
2.1 Differentiate between the different ports & protocols, their respective threats and mitigation techniques.	
Antiquated protocols	11
TCP/IP hijacking	11, 15
Null sessions	15
Spoofing	15
Man-in-the-middle	15
Replay	15
DOS	15
DDOS	15
Domain Name Kiting	15
DNS poisoning	15
ARP poisoning	15
2.2 Distinguish between network design elements and components.	
DMZ	9
VLAN	9
NAT	9
Network interconnections	9
NAC	10
Subnetting	9
Telephony	3, 10
2.3 Determine the appropriate use of network security tools to facilitate network security.	
NIDS	10, 13
NIPS	10, 13
Firewalls	10, 13

Topic	Chapter(s)
Proxy servers	10, 13
Honeypot	10, 13
Internet content filters	13
Protocol analyzers	10, 13
2.4 Apply the appropriate network tools to facilitate network security.	
NIDS	10, 13
Firewalls	10, 13
Proxy servers	10, 13
Internet content filters	13
Protocol analyzers	10, 13
2.5 Explain the vulnerabilities and mitigations associated with network devices.	
Privilege escalation	10
Weak passwords	10
Back doors	10
Default accounts	10
DOS	10
2.6 Explain the vulnerabilities and mitigations associated with various transmission media.	
Vampire taps	10
2.7 Explain the vulnerabilities and implement mitigations associated with wireless networking.	
Data emanation	3, 12
War driving	12
SSID broadcast	12
Blue jacking	12
Bluesnarfing	12
Rogue access points	12
Weak encryption	12
3.0 Access Control	
3.1 Identify and apply industry best practices for access control methods.	
Implicit deny	1
Least privilege	1, 18, 19
Separation of duties	1, 19
Job rotation	1
3.2 Explain common access control models and the differences between each.	
MAC	1, 11, 22
DAC	1, 11, 22
Role & Rule based access control	1, 11, 22
3.3 Organize users and computers into appropriate security groups and roles while distinguishing between appropriate rights and privileges.	
	2, 11, 22

Topic	Chapter(s)
3.4 Apply appropriate security controls to file and print resources.	
	2, 22
3.5 Compare and implement logical access control methods.	
ACL	2, 11, 22
Group policies	2, 11, 22
Password policy	2, 4, 22
Domain password policy	2, 11, 22
User names and passwords	2, 4, 22
Time of day restrictions	2, 22
Account expiration	2, 4, 22
Logical tokens	2, 11, 22
3.6 Summarize the various authentication models and identify the components of each.	
One, two and three-factor authentication	11
Single sign-on	11, 22
3.7 Deploy various authentication models and identify the components of each.	
Biometric reader	3, 11
RADIUS	11
RAS	11
LDAP	11
Remote access policies	11
Remote authentication	11
VPN	11
Kerberos	11
CHAP	11
PAP	11
Mutual	11
802.1x	11
TACACS	11
3.8 Explain the difference between identification and authentication (identity proofing).	
	11
3.9 Explain and apply physical access security methods.	
Physical access logs/lists	8
Hardware locks	8
Physical access control – ID badges	8
Door access systems	8
Man-trap	8
Physical tokens	8
Video surveillance – camera types and positioning	8
4.0 Assessments & Audits	
4.1 Conduct risk assessments and implement risk mitigation.	
	14

Topic	Chapter(s)
4.2 Carry out vulnerability assessments using common tools.	
Port scanners	14
Vulnerability scanners	14
Protocol analyzers	14
OVAL	17
Password crackers	15
Network mappers	14
4.3 Within the realm of vulnerability assessments, explain the proper use of penetration testing versus vulnerability scanning.	
	14
4.4 Use monitoring tools on systems and networks and detect security-related anomalies.	
Performance monitor	14
Systems monitor	14
Performance baseline	14
Protocol analyzers	14
4.5 Compare and contrast various types of monitoring methodologies.	
Behavior-based	13
Signature-based	13
Anomaly-based	13
4.6 Execute proper logging procedures and evaluate the results.	
Security application	14
DNS	14
System	14
Performance	14
Access	14
Firewall	13
Antivirus	14
4.7 Conduct periodic audits of system security settings.	
User access and rights review	2, 19
Storage and retention policies	19
Group policies	19
5.0 Cryptography	
5.1 Explain general cryptography concepts.	
Key management	5, 6, 7
Steganography	5
Symmetric key	5
Asymmetric key	5
Confidentiality	5
Integrity and availability	5

Topic	Chapter(s)
Non-repudiation	5
Comparative strength of algorithms	5
Digital signatures	5
Whole disk encryption	5
Trusted Platform Module (TPM)	5
Single vs. Dual sided certificates	5, 6
Use of proven technologies	5
5.2 Explain basic hashing concepts and map various algorithms to appropriate applications.	
SHA	5, 23
MD5	5, 23
LANMAN	5
NTLM	5
5.3 Explain basic encryption concepts and map various algorithms to appropriate applications.	
DES	5
3DES	5
RSA	5
PGP	5
Elliptic curve	5
AES	5
AES256	5
One time pad	5
Transmission encryption (WEP TKIP, etc.)	5, 7
5.4 Explain and implement protocols.	
SSL/TLS	5,
S/MIME	5, 7, 16
PPTP	5, 7, 11
HTTP vs. HTTPS vs. SHTTP	5, 7
L2TP	5, 11
IPSEC	5, 7, 11
SSH	5, 11
5.5 Explain core concepts of public key cryptography.	
Public Key Infrastructure (PKI)	6, 16
Recovery agent	6
Public key	6
Private keys	6
Certificate Authority (CA)	6
Registration	6
Key escrow	6
Certificate Revocation List (CRL)	6
Trust models	6

Topic	Chapter(s)
5.6 Implement PKI and certificate management.	
Public Key Infrastructure (PKI)	6, 16
Recovery agent	6
Public key	6
Private keys	6
Certificate Authority (CA)	6
Registration	6
Key escrow	6
Certificate Revocation List (CRL)	6
6.0 Organizational Security	
6.1 Explain redundancy planning and its components.	
Hot site	19
Cold site	19
Warm site	19
Backup generator	19
Single point of failure	19
RAID	19
Spare parts	19
Redundant servers	19
Redundant ISP	19
UPS	19
Redundant connections	19
6.2 Implement disaster recovery procedures.	
Planning	19
Disaster recovery exercises	19
Backup techniques and practices – storage	19
Schemes	19
Restoration	19
6.3 Differentiate between and execute appropriate incident response procedures.	
Forensics	19, 23
Chain of custody	19, 23
First responders	19, 23
Damage and loss control	19, 23
Reporting – disclosure of	19, 23
6.4 Identify and explain applicable legislation and organizational policies.	
Secure disposal of computers	2
Acceptable use policies	2, 19
Password complexity	2, 4
Change management	2, 19
Classification of information	2, 19

Topic	Chapter(s)
Mandatory vacations	2, 4, 19
Personally Identifiable Information (PII)	2, 25
Due care	2, 19
Due diligence	2, 19
Due process	2, 19
SLA	2, 19
Security-related HR policy	2, 4
User education and awareness training	2, 4
6.5 Explain the importance of environmental controls.	
Fire suppression	3, 8
HVAC	3, 8
Shielding	3, 8
6.6 Explain the concept of and how to reduce the risks of social engineering.	
Phishing	2, 4
Hoaxes	2, 4
Shoulder surfing	2, 4
Dumpster diving	2, 4
User education and awareness training	2, 4

appendix B

About the CD

The CD-ROM included with this book comes complete with MasterExam, the electronic version of the book, and Session #1 of LearnKey's online training. The software is easy to install on any Windows 2000/XP/Vista computer and must be installed to access the MasterExam feature. You may, however, browse the electronic book directly from the CD without installing the software. To register for LearnKey's online training or the bonus MasterExam, simply click the Bonus MasterExam link on the main launch page and follow the directions to the free online registration.

System Requirements

Software requires Windows 2000 or higher and Internet Explorer 6.0 or above and 20MB of hard disk space for full installation. The electronic book requires Adobe Reader. To access the online training from LearnKey, you must have Windows Media Player 9 or higher and Adobe Flash Player 9 or higher.

LearnKey Online Training

Clicking the LearnKey Online Training link will allow you to access online training from Osborne.OnlineExpert.com. The first session of this course is provided at no charge. Additional session for this course and other courses may be purchased directly from www.LearnKey.com or by calling 800-865-0165.

The first time that you click the LearnKey Online Training link, you will be required to complete a free online registration. Follow the instructions for a first-time user. Please make sure to use a valid e-mail address.

Installing and Running MasterExam

If your computer CD-ROM drive is configured to autorun, the CD-ROM will automatically start up when you insert the disc. From the opening screen, you may install MasterExam by clicking the MasterExam link. This will begin the installation process and create a program group named LearnKey. To run MasterExam, select Start | All Programs | LearnKey | MasterExam. If the autorun feature did not launch your CD, browse to the CD drive and click the LaunchTraining.exe icon.

MasterExam

MasterExam provides you with a simulation of the actual exam. The number of questions, the type of questions, and the time allowed are intended to be an accurate representation of the exam environment. You have the option to take an open-book exam, including hints, references, and answers, a closed-book exam, or the timed MasterExam simulation.

When you launch MasterExam, a digital clock display will appear in the bottom-right corner of your screen. The clock will continue to count down to zero unless you choose to end the exam before the time expires.

Electronic Book

The entire contents of the textbook are provided as a PDF. Adobe Reader has been included on the CD.

Help

A help file is provided through the Help button on the main page in the lower-left corner. Individual help features are also available through MasterExam and LearnKey's online training.

Removing Installation(s)

MasterExam is installed to your hard drive. For best results removing the program, select the Start | All Programs | LearnKey | Uninstall option to remove MasterExam.

Technical Support

For questions regarding the content of the electronic book or MasterExam, please visit www.mhprofessional.com or e-mail customer.service@mcgraw-hill.com. For customers outside the 50 United States, e-mail international_cs@mcgraw-hill.com.

LearnKey Technical Support

For technical problems with the software (installation, operation, installation removal) and for questions regarding LearnKey online training content, please visit www.learnkey.com, e-mail techsupport@learnkey.com, or call toll free 800-482-8244.

chapter 1

Introduction and Security Trends

Security is mostly a superstition. It does not exist in nature, nor do the children of men as a whole experience it. Avoiding danger is no safer in the long run than outright exposure. Life is either a daring adventure or nothing.

—Helen Keller

In this chapter, you will learn how to

- **List and discuss recent trends in computer security**
- **Describe simple steps to take to minimize the possibility of an attack on a system**
- **Describe various types of threats that exist for computers and networks**
- **Discuss recent computer crimes that have been committed**

Why should we be concerned about computer and network security? All you have to do is turn on the television or read the newspaper to find out about a variety of security problems that affect our nation and the world today. The danger to computers and networks may seem to pale in comparison to the threat of terrorist strikes, but in fact the average citizen is much more likely to be the target of an attack on their own personal computer, or a computer they use at their place of work, than they are to be the direct victim of a terrorist attack. This chapter will introduce you to a number of issues involved in securing your computers and networks from a variety of threats that may utilize any of a number of different attacks.

The Security Problem

Fifty years ago, few people had access to a computer system or network, so securing them was a relatively easy matter. If you could secure the building that these early, very large systems were housed in, you could secure the data and information they stored and processed. Now, personal computers are ubiquitous and portable, making them much more difficult to secure physically, and are often connected to the Internet, putting the data they contain at much greater risk of attack or theft. Similarly, the typical computer user today is not as technically sophisticated as the typical computer user 50 years ago. No longer are computers reserved for use by scientists and engineers; now, even children who are barely able to read can be taught to boot a computer and gain access to their own favorite games or educational software.

Fifty years ago companies did not conduct business across the Internet. Online banking and shopping were only dreams in science fiction stories. Today, however, millions of people perform online transactions every day. Companies rely on the Internet to operate and conduct business. Vast amounts of money are transferred via networks, in the form of either bank transactions or simple credit card purchases. Wherever there are vast amounts of money, there are those who will try to take advantage of the environment to conduct fraud or theft. There are many different ways to attack computers and networks to take advantage of what has made shopping, banking, investment, and leisure pursuits a simple matter of "dragging and clicking" for many people. Identity theft is so common today that most everyone knows somebody who's been a victim of such a crime, if they haven't been a victim themselves. This is just one type of criminal activity that can be conducted using the Internet. There are many others and all are on the rise.

Tech Tip

Historical Security

Computer security is an ever-changing issue. Fifty years ago, computer security was mainly concerned with the physical devices that made up the computer. At the time, these were the high-value items that organizations could not afford to lose. Today, computer equipment is inexpensive compared to the value of the data processed by the computer. Now the high-value item is not the machine, but the information that it stores and processes. This has fundamentally changed the focus of computer security from what it was in the early years. Today the data stored and processed by computers is almost always more valuable than the hardware.

Security Incidents

By examining some of the computer-related crimes that have been committed over the last 20 or so years, we can better understand the threats and security issues that surround our computer systems and networks. Electronic crime can take a number of different forms but the ones we will examine here fall into two basic categories: crimes in which the computer was the target, and incidents in which a computer was used to perpetrate the act (for example, there are many different ways to conduct bank fraud, one of which uses computers to access the records that banks process and maintain).

We will start our tour of computer crimes with the 1988 Internet worm (Morris worm), one of the first real Internet crime cases. Prior to 1988 criminal activity was chiefly centered on unauthorized access to computer systems and networks owned by the telephone company and companies which provided dial-up access for authorized users. Virus activity also existed prior to 1988, having started in the early 1980s.

The Morris Worm (November 1988)

Robert Morris, then a graduate student at Cornell University, released what has become known as the Internet worm (or the Morris worm). This was the first large-scale attack on the Internet, though it appears doubtful that

Morris actually intended that his creation cause the impact that it did at the time. The worm infected roughly 10 percent of the machines then connected to the Internet (which amounted to approximately 6000 infected machines) and caused an estimated $100 million in damage, though this number has been the subject of wide debate. The worm carried no malicious payload, the program being obviously a “work in progress,” but it did wreak havoc because it continually reinfected computer systems until they could no longer run any programs. The worm took advantage of known vulnerabilities in several programs to gain access to new hosts and then copied itself over. Morris was eventually convicted under Title 10 United States Code Section 1030 for releasing the worm and was sentenced to three years’ probation, a $10,000 fine, and 400 hours of community service.

Citibank and Vladimir Levin (June–October 1994)

Starting about June of 1994 and continuing until at least October of the same year, a number of bank transfers were made by Vladimir Levin of St. Petersburg, Russia. By the time he and his accomplices were caught, they had transferred an estimated $10 million. Eventually all but about $400,000 was recovered. Levin reportedly accomplished the break-ins by dialing into Citibank’s cash management system. This system allowed clients to initiate their own fund transfers to other banks. An estimated $500 billion was transferred daily during this period, so the amounts transferred by Levin were very small in comparison to the overall total on any given day. To avoid detection, he also conducted the transactions at night in Russia so that they coincided with normal business hours in New York. Levin was arrested in London in 1995 and, after fighting extradition for 30 months, eventually was turned over to U.S. authorities, was tried, and was sentenced to three years in jail. Four accomplices of Levin plead guilty to conspiracy to commit bank fraud and received lesser sentences.

Kevin Mitnick (February 1995)

Kevin Mitnick’s computer activities occurred over a number of years during the 1980s and 1990s. He was arrested in February 1995 (not his first arrest on computer criminal charges) for federal offenses related to what the FBI described as a 2½-year computer hacking spree. He eventually pled guilty to four counts of wire fraud, two counts of computer fraud, and one count of illegally intercepting a wire communication and was sentenced to 46 months in jail. In the plea agreement, Mitnick admitted to having gained unauthorized access to a number of different computer systems belonging to companies such as Motorola, Novell, Fujitsu, and Sun Microsystems. He described using a number of different “tools” and techniques, including social engineering, sniffers, and cloned cellular telephones. Mitnick also admitted to having used stolen accounts at the University of Southern California to store proprietary software he had taken from various companies. He also admitted to stealing e-mails and impersonating employees of targeted companies in order to gain access to the software he was seeking.

Omega Engineering and Timothy Lloyd (July 1996)

On July 30, 1996, a software “time bomb” went off at Omega Engineering, a New Jersey–based manufacturer of high-tech measurement and control instruments. Twenty days earlier, Timothy Lloyd, a computer network program designer, had been dismissed from the company after a period of growing tension between Lloyd and management at Omega. The program that ran on July 30 deleted all of the design and production programs for the company, severely damaging the small firm and forcing the layoff of 80 employees. The program was eventually traced back to Lloyd, who had left it in retaliation for his dismissal. In May of 2000, a federal judge sentenced Lloyd to 41 months in prison and ordered him to pay more than $2 million in restitution.

Worcester Airport and "Jester" (March 1997)

In March of 1997, airport services to the FAA control tower as well as the emergency services at the Worcester Airport and the community of Rutland, Massachusetts, were cut off for a period of six hours. This disruption occurred as a result of a series of commands sent by a teenage computer "hacker" who went by the name "Jester." The individual had gained unauthorized access to the "loop carrier system" operated by NYNEX, a New England telephone company. Loop carrier systems are programmable remote computer systems used to integrate voice and data communications. Jester was eventually caught and ordered to pay restitution to the telephone company, as well as complete 250 hours of community service.

Tech Tip

Intellectual Curiosity

In the early days of computer crime, much of the criminal activity centered on gaining unauthorized access to computer systems. In many early cases, the perpetrator of the crime did not intend to cause any damage to the computer but was instead on a quest of "intellectual curiosity"—trying to learn more about computers and networks. Today the ubiquitous nature of computers and networks has eliminated the perceived need for individuals to break into computers to learn more about them. While there are still those who dabble in hacking for the intellectual challenge, it is more common today for the intellectual curiosity to be replaced by malicious intent. Whatever the reason, today it is considered unacceptable (and illegal) to gain unauthorized access to computer systems and networks.

Solar Sunrise (February 1998)

In January of 1998, relations between Iraq and the United States again took a turn for the worse and it appeared as if the United States might take military action against Iraq. During this period of increased tension and military preparation, a series of computer intrusions occurred at a number of U.S. military installations. At first the military thought that this might be the start of an information warfare attack—a possibility the military had been discussing since the early 1990s. Over 500 domain name servers were compromised during the course of the attacks. Making it harder to track the actual origin of the attacks was the fact that the attackers made a number of "hops" between different systems, averaging eight different systems before arriving at the target. The attackers eventually turned out to be two teenagers from California and their mentor in Israel. The attacks, as it turned out, had nothing to do with the potential conflict in Iraq.

The Melissa Virus (March 1999)

Melissa is the best known of the early macro-type viruses that attach themselves to documents for programs that have limited macro programming capability. The virus, written and released by David Smith, infected about a million computers and caused an estimated $80 million in damages. Melissa, which clogged networks with the traffic it generated and caused problems for e-mail servers worldwide, was attached to Microsoft Word 97 and Word 2000 documents. If the user opened the file, the macro ran, infecting the current host and also sending itself to the first 50 addresses in the individual's e-mail address book. The e-mail sent contained a subject line stating "Important Message From" and then included the name of the individual who was infected. The body of the e-mail message contained the text "Here is that document you asked for … don't show anyone else ;-)." The nature of both the subject line and the body of the message usually generated enough user curiosity that many people opened the document and thus infected their system, which in turn sent the same message to 50 of their acquaintances. As a final action, if the minute of the current hour when the macro was run matched the day of the month, the macro inserted "Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here." into the current document. Smith, who plead guilty, was ultimately fined $5000 and sentenced to 20 months in jail for the incident. Because the macro code is easy to modify, there have been many variations of the Melissa virus. Recipients could avoid infection by Melissa simply by not opening the attached file.

The Love Letter Virus (May 2000)

Also known as the "ILOVEYOU" worm and the "Love Bug," the Love Letter virus was written and released by a Philippine student named Onel de Guzman. The virus was spread via e-mail with the subject line of "ILOVEYOU." Estimates of the number of infected machines worldwide have been as high as 45 million, accompanied by a possible $10 billion in damages (it should be noted that figures like these are extremely hard to verify or calculate). Similar to the Melissa virus, the Love Letter virus spread via an e-mail attachment, but in this case, instead of utilizing macros, the attachments were VBScript programs. When the receiver ran the attachment, it searched the system for files with specific extensions in order to replace them with copies of itself. It also sent itself to everyone in the user's address book. Again, since the receiver generally knew the sender, most individuals opened the attachment without questioning it. de Guzman ultimately was not convicted for releasing the worm because the Philippines, at the time, did not have any laws denoting the activity as a crime. Again, recipients avoided infection from the virus simply by not opening the attachments.

The Code Red Worm (2001)

On July 19, 2001, over 350,000 computers connected to the Internet were infected by the Code Red worm. This infection took only 14 hours to occur. The cost estimate for how much damage the worm caused (including variations of the worm released on later dates) exceeded $2.5 billion. The vulnerability exploited by the Code Red worm had been known for a month. The worm took advantage of a buffer-overflow condition in Microsoft's IIS web servers. Microsoft released a patch for this vulnerability and made an official announcement of the problem on June 18, 2001. The worm itself was "memory resident," so simply turning off an infected machine eliminated it. Unfortunately, unless the system was patched before being reconnected to the Internet, chances were good that it would soon become reinfected. Though the worm didn't carry a malicious payload designed to destroy data on the infected system, on some systems, the message "Hacked by Chinese" was added to the top-level page for the infected host's web site. If the date on the infected system was between the 1st and the 19th of the month, the worm would attempt to infect a random list of IP addresses it generated. If the date was between the 20th and the 28th of the month, the worm stopped trying to infect other systems and instead attempted to launch a denial-of-service (DoS) attack against a web site owned by the White House. After the 28th, the worm would lay dormant until the 1st of the next month. This date scheme actually ended up helping to eliminate the worm, because soon after it was released on the 19th, the worm stopped trying to infect systems. This provided a period of time when systems could be rebooted and patched before they were infected again.

Adil Yahya Zakaria Shakour (August 2001–May 2002)

On March 13, 2003, 19-year-old Adil Yahya Zakaria Shakour plead guilty to a variety of crimes, including unauthorized access to computer systems and credit card fraud. Shakour admitted to having accessed several computers without authorization, including a server at Eglin Air Force Base (where he defaced the web site), computers at Accenture (a Chicago-based management consulting and technology services company), a computer system at Sandia National Laboratories (a Department of Energy facility), and a computer at Cheaptaxforms.com. Shakour admitted to having obtained credit card and personal information during the break-in of Cheaptaxforms.com and having used it to purchase items worth over $7000 for his own use. Shakour was sentenced to one year and one day in federal prison and a three-year term of supervised release, and was ordered to pay $88,000 in restitution.

The Slammer Worm (2003)

On Saturday, January 25, 2003, the Slammer worm (also sometimes referred to as the Slammer virus) was released. It exploited a buffer-overflow vulnerability in computers running Microsoft's SQL Server or Microsoft SQL Server Desktop Engine. Like the vulnerability in Code Red, this weakness was not new and, in fact, had been discovered in July of 2002; Microsoft issued a patch for the vulnerability before it was even announced. Within the first 24 hours of Slammer's release, the worm had infected at least 120,000 hosts and caused network outages and the disruption of airline flights, elections, and ATMs. At its peak, Slammer-infected hosts were generating a reported 1TB of worm-related traffic *every second*. The worm doubled its number of infected hosts every 8 seconds. It is estimated that it took less than ten minutes to reach global proportions and infect 90 percent of the possible hosts it could infect. Once a machine was infected, the host would start randomly selecting targets and sending packets to them to attempt infection at a rate of 25,000 packets per second. Slammer did not contain a malicious payload. The problems it caused were a result of the massively overloaded networks, which could not sustain the traffic being generated by the thousands of infected hosts. The worm sent its single packet to a specific UDP port, 1434, which provided an immediate fix to prevent further network access. Thus, the response of administrators was to quickly block all traffic to UDP port 1434, effectively curbing the spread of the worm to new machines.

Tech Tip

Speed of Virus Proliferation

The speed at which the Slammer virus spread served as a wakeup call to security professionals. It drove home the point that the Internet could be adversely impacted in a matter of minutes. This in turn caused a number of professionals to rethink how prepared they needed to be in order to respond to virus outbreaks in the future. A good first step is to apply patches to systems and software as soon as possible. This will often eliminate the vulnerabilities that the worms and viruses are designed to target.

U.S. Electric Power Grid (1997–2009)

In April 2009, Homeland Security Secretary Janet Napolitano told reporters that the United States was aware of attempts by both Russia and China to break into the U.S. electric power grid, map it out, and plant destructive programs that could be activated at a later date. She indicated that these attacks were not new and had in fact been going on for years. One article in the *Kansas City Star*, for example, reported that in 1997 the local power company, Kansas City

Power and Light, saw perhaps 10,000 attacks for the entire year. In contrast, in 2009 the company has been experiencing 10 to 20 attacks every second. While none of these attacks is credited with causing any significant loss of power, the attacks nonetheless highlight the fact that the nation's critical infrastructures are viewed as potential targets by other nations. In the event of some future conflict, the United States could expect to experience a cyber attack on the cyber infrastructures that operate its critical systems.

Try This

Software Patches

One of the most effective measures security professionals can take to address attacks on their computer systems and networks is to ensure that all software is up-to-date in terms of vendor-released patches. Many of the outbreaks of viruses and worms would have been much less severe if everybody had applied security updates and patches when they were released. For the operating system that you use, use your favorite web browser to find what patches exist for the operating system and what vulnerabilities or issues they were created to address.

Conficker (2008–2009)

In late 2008 and early 2009, security experts became alarmed when it was discovered that millions of systems attached to the Internet were infected with the Downadup worm. Also known as Conficker, the worm was first detected in November 2008 and was believed to have originated in Ukraine. Infected systems were not initially damaged beyond having their antivirus solution updates blocked. What alarmed experts was the fact that infected systems could be used in a secondary attack on other systems or networks. Each of these infected systems was part of what is known as a *bot network* and could be used to cause a DoS attack on a target or be used for the forwarding of spam e-mail to millions of users. It was widely believed that this network of subverted systems would be activated on April 1, 2009, and would result in the widespread loss of data and system connectivity. As it turned out, very little damage was done on that date, though millions of dollars were spent in responding to the millions of infected systems.

Fiber Cable Cut (2009)

On April 9, 2009, a widespread phone and Internet outage hit the San Jose area in California. This outage was not the result of a group of determined hackers gaining unauthorized access to the computers that operate these networks, but instead occurred as a result of several cuts in the physical cables that carry the signals. A cable being cut is not an unusual occurrence; backhoes have been responsible for many temporary interruptions in telephone service in the past decade. What was unusual, and significant, about this incident was that the cuts were deliberate. A manhole cover had been removed to allow the attacker(s) to gain access to the cables underground. The cuts resulted in a loss of all telephone, cell phone, and Internet service for thousands of users in the San Jose area. Emergency services such as 911 were also affected, which could have had severe consequences. What is important to take away from this incident is the fact that the infrastructures that our communities, states, and the nation rely on can also be easily attacked using fairly simple physical techniques and without a lot of technical expertise.

Threats to Security

The incidents described in the previous section provide a glimpse into the many different threats that face administrators as they attempt to protect their computer systems and networks. There are, of course, the normal natural disasters that organizations have faced for years. In today's highly networked world, however, new threats have developed that we did not have to worry about 50 years ago.

There are a number of ways that we can break down the various threats. One way to categorize them is to separate threats that come from outside of the organization from those that are internal. Another is to look at the various levels of sophistication of the attacks, from those by "script kiddies" to those by "elite hackers." A third is to examine the level of organization of the various threats, from unstructured threats to highly structured threats. All of these are valid approaches, and they in fact overlap each other. The following sections examine threats from the perspective of where the attack comes from.

Viruses and Worms

While your organization may be exposed to viruses and worms as a result of employees not following certain practices or procedures, generally you will not have to worry about your employees writing or releasing viruses and worms. It is important to draw a distinction between the writers of malware and those who release them. Debates over the ethics of writing viruses permeate the industry, but currently, simply writing them is not considered a criminal activity. A virus is like a baseball bat; the bat itself is not evil, but the inappropriate use of the bat (such as to smash a car's window) falls into the category of criminal activity. (Some may argue that this is not a very good analogy since a baseball bat has a useful purpose—to play ball—but viruses *have* no useful purpose. In general, this is true but in some limited environments, such as in specialized computer science courses, the study and creation of viruses can be considered a useful learning experience.)

By far, viruses and worms are the most common problem that an organization faces because literally thousands of them have been created and released. Fortunately, antivirus software and system patching can eliminate the largest portion of this threat. Viruses and worms generally are also nondiscriminating threats; they are released on the Internet in a general fashion and aren't targeted at a specific organization. They typically are also highly visible once released, so they aren't the best tool to use in highly structured attacks where secrecy is vital. This is not to say that the technology used in virus and worm propagation won't be used by highly organized criminal groups, but its use for what these individuals are normally interested in accomplishing is limited. The same cannot be said for terrorist organizations, which generally want to create a large impact and have it be highly visible.

Tech Tip

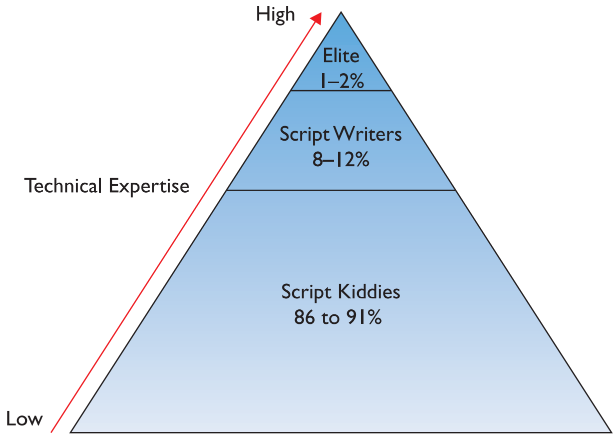
Malware

Viruses and worms are just two types of threats that fall under the general heading of malware. *The term malware comes from "malicious software," which describes the overall purpose of code that falls into this category of threat. Malware is software that has a nefarious purpose, designed to cause problems to you as an individual (for example, identity theft) or your system. More information on the different types of malware is provided in Chapter 15.*

Intruders

The act of deliberately accessing computer systems and networks without authorization is generally referred to as **hacking**, with individuals who conduct this activity being referred to as **hackers**. The term hacking also applies to the act of exceeding one's authority in a system. This would include authorized users who attempt to gain access to files they aren't permitted to access or who attempt to obtain permissions that they have not been granted. While the act of breaking into computer systems and networks has been glorified in the media and movies, the physical act does not live up to the Hollywood hype. Intruders are, if nothing else, extremely patient, since the process to gain access to a system takes persistence and dogged determination. The attacker will conduct many preattack activities in order to obtain the information needed to determine which attack will most likely be successful. Generally, by the time an attack is launched, the attacker will have gathered enough information to be very confident that the attack will succeed. If it doesn't, the attacker will gather additional information and take a different approach (though launching the first attack may alert security personnel). Generally, attacks by an individual or even a small group of attackers fall into the **unstructured threat** category. Attacks at this level generally are conducted over short periods of time (lasting at most a few months), do not involve a large number of individuals, have little financial backing, and are accomplished by insiders or outsiders who do not seek collusion with insiders.

Intruders, or those who are attempting to conduct an intrusion, definitely come in many different varieties and have varying degrees of sophistication (see Figure 1.1). At the low end technically are what are generally referred to as **script kiddies**, individuals who do not have the technical expertise to develop scripts or discover new vulnerabilities in software but who have just enough understanding of computer systems to be able to download and run scripts that others have developed. These individuals generally are not interested in attacking specific targets, but instead simply want to find any organization that may not have patched a newly discovered vulnerability for which the script kiddie has located a script to exploit the vulnerability. It is hard to estimate how many of the individuals performing activities such as probing networks or scanning individual systems are part of this group, but it is undoubtedly the fastest growing group and the vast majority of the "unfriendly" activity occurring on the Internet is probably carried out by these individuals.



• **Figure 1.1** Distribution of attacker skill levels

At the next level are those people who are capable of writing scripts to exploit known vulnerabilities. These individuals are much more technically competent than script kiddies and account for an estimated 8 to 12 percent of malicious Internet activity. At the top end of this spectrum are those highly technical individuals, often referred to as **elite hackers**, who not only have the ability to write scripts that exploit vulnerabilities but also are capable of discovering new vulnerabilities. This group is the smallest of the lot, however, and is responsible for, at most, only 1 to 2 percent of intrusive activity.

Insiders

It is generally acknowledged by security professionals that insiders are more dangerous in many respects than outside intruders. The reason for this is simple—insiders have the access and knowledge necessary to cause immediate damage to an organization. Most security is designed to protect against outside intruders and thus lies at the boundary between the organization and the rest of the world. Insiders may actually already have all the access they need to perpetrate criminal activity such as fraud. In addition to unprecedented access, insiders also frequently have knowledge of the security systems in place and are better able to avoid detection. Attacks by insiders are often the result of employees who have become disgruntled with their organization and are looking for ways to disrupt operations. It is also possible that an "attack" by an insider may be an accident and not intended as an attack at all. An example of this might be an employee who deletes a critical file without understanding its critical nature.

Employees are not the only insiders that organizations need to be concerned about. Often, numerous other individuals have physical access to company facilities. Custodial crews frequently have unescorted access throughout the facility, often when nobody else is around. Other individuals, such as contractors or partners, may have not only physical access to the organization's facilities but also access to computer systems and networks.

Tech Tip

The Inside Threat

One of the hardest threats that security professionals will have to address is that of the insider. Since employees already have access to the organization and its assets, additional mechanisms need to be in place to detect attacks by insiders and to lessen the ability of these attacks to succeed.

Criminal Organizations

As businesses became increasingly reliant upon computer systems and networks, and as the amount of financial transactions conducted via the Internet increased, it was inevitable that criminal organizations would eventually turn to the electronic world as a new target to exploit. Criminal activity on the Internet at its most basic is no different from criminal activity in the physical world. Fraud, extortion, theft, embezzlement, and forgery all take place in the electronic environment.

One difference between criminal groups and the "average" hacker is the level of organization that criminal elements employ in their attack. Criminal groups typically have more money to spend on accomplishing the criminal activity and are willing to spend extra time accomplishing the task provided the level of reward at the conclusion is great enough. With the tremendous amount of money that is exchanged via the Internet on a daily basis, the level of reward for a successful attack is high enough to interest criminal elements. Attacks by criminal organizations usually fall into the **structured threat** category, which is characterized by a greater amount of planning, a longer period of time to conduct the activity, more financial backing to accomplish it, and possibly corruption of, or collusion with, insiders.

Terrorists and Information Warfare

As nations have increasingly become dependent on computer systems and networks, the possibility that these essential elements of society might be targeted by organizations or nations determined to adversely affect another nation has become a reality. Many nations today have developed to some extent the capability to conduct **information warfare**. There are several definitions for information warfare, but a simple one is that it is warfare conducted against the information and information processing equipment used by an adversary. In practice, this is a much more complicated subject, because information not only may be the target of an adversary, but also may be used as a weapon. Whatever definition you use, information warfare falls into the **highly structured threat** category. This type of threat is characterized by a much longer period of preparation (years is not uncommon), tremendous financial backing, and a large and organized group of attackers. The threat may include attempts not only to subvert insiders but also to plant individuals inside of a potential target in advance of a planned attack.

An interesting aspect of information warfare is the list of possible targets available. We have grown accustomed to the idea that, during war, military forces will target opposing military forces but will generally attempt to destroy as little civilian infrastructure as possible. In information warfare, military forces are certainly still a key target, but much has been written about other targets, such as the various infrastructures that a nation relies on for its daily existence. Water, electricity, oil and gas refineries and distribution, banking and finance, telecommunications—all fall into the category of **critical infrastructures** for a nation. Critical infrastructures are those whose loss would have severe repercussions on the nation. With countries relying so heavily on these infrastructures, it is inevitable that they will be viewed as valid targets during conflict. Given how dependent these infrastructures are on computer systems and networks, it is also inevitable that these same computer systems and networks will be targeted for a cyber attack in an information war.

Another interesting aspect of information warfare is the potential list of attackers. As mentioned, several countries are currently capable of conducting this type of warfare. Nations, however, are not the only ones that can conduct information, or cyber, warfare. Terrorist organizations can also accomplish this. Such groups fall into the category of highly structured threats since they too are willing to conduct long-term operations, have (in some cases) tremendous financial support, and often have a large following. Reports out of Afghanistan related stories of soldiers and intelligence officers finding laptop computers formerly owned by members of al-Qaeda that contained information about various critical infrastructures in the United States. This showed that terrorist organizations not only were targeting such infrastructures, but were doing so at an unexpected level of sophistication.

Tech Tip

Information Warfare

Once only the concern of governments and the military, information warfare today can involve many other individuals. With the potential to attack the various civilian-controlled critical infrastructures, security professionals in nongovernmental sectors today must also be concerned about defending their systems against attacks by agents of foreign governments.

Security Trends

The biggest change that has occurred in security over the last 30 years has been the change in the computing environment from large mainframes to a highly interconnected network of much smaller systems (smaller is a relative term here because the computing power of desktop computers exceeds the power of many large mainframes of 30 years ago). What this has meant for security is a switch from an environment in which everything was fairly contained and people operated in a closed environment to one in which access to a computer can occur from almost anywhere on the planet. This has, for obvious reasons, greatly complicated the job of the security professional.

The type of individual who attacks a computer system or network has also evolved over the last 30 years. There was, of course, the traditional intelligence service operator paid by a particular country to obtain secrets from other government computer systems. These people still exist. What has increased dramatically is the number of nonaffiliated intruders. As discussed earlier, the rise of the "script kiddie" has greatly multiplied the number of individuals who probe organizations looking for vulnerabilities to exploit. This is actually the result of another recent trend: as the level of sophistication of attacks has increased, the level of knowledge necessary to exploit vulnerabilities has decreased. This is due to the number of automated tools that have been created that allow even novice attackers to exploit highly technical and complex vulnerabilities. The resulting increase in network attacks has been reflected in a number of different studies conducted by various organizations in the industry.

One of the best-known security surveys is the joint survey conducted annually by the Computer Security Institute (CSI) and the FBI (this survey, *CSI Computer Crime and Security Survey*, can be obtained from www.gocsi.com). The respondents, who normally number over 500 individuals, come from all walks of life: government, academia, and industry. Over the last several years, the percentage of organizations that have experienced security incidents has slowly declined (from 46 percent in 2007 to 43 percent in 2008). This decline has been seen in the most frequent type of incidents experienced (viruses, insider abuse, laptop theft, and unauthorized access) which have remained the same for the last four years. Only four types of attacks showed any increase from 2007 to 2008 (unauthorized access, theft/loss of proprietary information, misuse of web applications, and DNS attacks).

One of the most interesting and oft-repeated statistics from the survey is the average loss experienced by organizations due to specific types of security incidents. The average loss as a result of theft of proprietary information, for example, hit a high of $6.57 million in 2002 but was only $2.70 million in 2003 before rising to $6.03 million in 2006 and then dropping again to $5.69 million in 2007. Financial fraud plunged from $4.63 million in 2002 to $328,000 in 2003 before rising to $2.56 million in 2006 and then skyrocketing to $21.12 million in 2007. While it is tempting to assume that this means we, as a community, are becoming more secure (and there is indeed some indication that organizations are doing a better job of securing their systems), the reality is that these figures reflect the difficulty in quantifying the actual state of Internet security and of producing accurate results. While we all like to use figures such as those from the CSI/FBI survey, the truth of the matter is that these numbers likely don't accurately portray the state of current security. They are, however, the most reliable ones we have.

Avenues of Attack

There are two general reasons a particular computer system is attacked: either it is specifically targeted by the attacker, or it is an opportunistic target. In the first case, the attacker has chosen the target not because of the hardware or software the organization is running but for another reason, perhaps a political reason. An example of this type of attack would be an individual in one country attacking a government system in another. Alternatively, the attacker may be targeting the organization as part of a **hacktivist** attack. An example, in this case, might be an attacker who defaces the web site of a company that sells fur coats because the attacker feels that using animals in this way is unethical. Perpetrating some sort of electronic fraud is another reason a specific system might be targeted. Whatever the reason, an attack of this nature is decided upon before the attacker knows what hardware and software the organization has.

The second type of attack, an attack against a target of opportunity, is conducted against a site that has software that is vulnerable to a specific exploit. The attackers, in this case, are not targeting the organization; instead, they have learned of a vulnerability and are simply looking for an organization with this vulnerability that they can exploit. This is not to say that an attacker might not be targeting a given sector and looking for a target of opportunity in that sector, however. For example, an attacker may desire to obtain credit card or other personal information and may search for any exploitable company with credit card information in order to carry out the attack.

Targeted attacks are more difficult and take more time than attacks on a target of opportunity. The latter simply relies on the fact that with any piece of widely distributed software, there will almost always be somebody who has not patched the system (or has not patched it properly) as they should have.

The Steps in an Attack

The steps an attacker takes in attempting to penetrate a targeted network are similar to the ones that a security consultant performing a penetration test would take.

First, the attacker gathers as much information about the organization as possible. There are numerous ways to do this, including studying the organization's own web site, looking for postings on newsgroups, or consulting resources such as the U.S. Securities and Exchange Commission's (SEC) EDGAR web site (www.sec.gov/edgar.shtml). A number of different financial reports are available through the EDGAR web site that can provide information about an organization that is useful for an attack—particularly a social engineering attack. The type of information that the attacker wants includes IP addresses, phone numbers, names of individuals, and what networks the organization maintains. This step is known as "profiling" or "reconnaissance." Commands such as *whois* are useful in this step for obtaining information on IP blocks and DNS server addresses. An even more common tool that is useful in gathering data is a traditional web search engine such as Google.

Typically, the next step, which is the first step in the technical part of an attack, is to determine what target systems are available and active. This step moves us from profiling to actual scanning and is accomplished with methods such as a **ping sweep**, which simply sends a "ping" (an ICMP echo request) to the target machine. If the machine responds, it is reachable. The next step is often to perform a **port scan**. This will help identify which ports are open, thus giving an indication of which services may be running on the target machine. Determining the operating system (known as *OS fingerprinting*) that is running on the target machine, as well as specific application programs, follows, along with determining the

Try This

Security Tools

Numerous tools are available on the Internet to conduct the initial reconnaissance activity described in this chapter. Examples include *Nmap* and *superscan*. Most security professionals recommend that security administrators run these tools against their own systems in order to see what attackers will see when they inevitably run the same, or similar, tools against the network. Using your favorite search engine, see what open source security tools you can find. Do the same for commercial security tools. If you have access to a closed network that you can play with, you may want to download some of the tools and try them to see how they work and what information they supply.

sample content of Principles of Computer Security: CompTIA Security+ and Beyond [With CDROM] (Official Comptia Guide)

- **Success pdf, azw (kindle), epub, doc, mobi**
- read The Syntax of French (Cambridge Syntax Guides)
- The Sign of Four pdf, azw (kindle)
- click Witch Heart (Elemental Witches, Book 3)
- Barriers and Openings to a New Socialist Internationalism: South African Histories, Strategies and Narratives pdf, azw (kindle), epub, doc, mobi
- download Lectures on the Forces of Matter: And Their Relations to Each Other

- http://diy-chirol.com/lib/Fodor-s-England-2014--With-the-Best-of-Wales.pdf
- http://reseauplatoparis.com/library/The-Syntax-of-French--Cambridge-Syntax-Guides-.pdf
- http://www.satilik-kopek.com/library/Y---Y---Girls-of--60s-French-Pop.pdf
- http://www.gateaerospaceforum.com/?library/Thinking-Kids--Math--Grade-1.pdf
- http://www.rap-wallpapers.com/?library/Theodore-Boone--The-Activist--Theodore-Boone--Book-4-.pdf
- http://twilightblogs.com/library/The-Crane-Wife.pdf