CHAPTER 1

Vulnerabilities, Threats, and Attacks

Upon completion of this chapter, you should be able to answer the following questions:

- What are the basics concepts of network security?
- What are some common network security vulnerabilities and threats?
- What are security attacks?
- What is the process of vulnerability analysis?

Key Terms

This chapter uses the following key terms. You can find the definitions in the glossary at the end of the book.

Unstructured threats	page 20
Structured threats	page 20
External threats	page 20
Internal threats	page 21
Hacker	page 21
Cracker	page 21
Phreaker	page 21
Spammer	page 21
Phisher	page 21
White hat	page 21
Black hat	page 21
Dictionary cracking	page 28
Brute-force computation	page 28
Trust exploitation	page 28
Port redirection	page 29
Man-in-the-middle attack	page 30
Social engineering	page 30
Phishing	page 30

The Internet continues to grow exponentially. Personal, government, and business applications continue to multiply on the Internet, with immediate benefits to end users. However, these network-based applications and services can pose security risks to individuals and to the information resources of companies and governments. Information is an asset that must be protected. Without adequate network security, many individuals, businesses, and governments risk losing that asset.

Network security is the process by which digital information assets are protected.

The goals of network security are as follows:

- Protect confidentiality
- Maintain integrity
- Ensure availability

With this in mind, it is imperative that all networks be protected from threats and vulnerabilities for a business to achieve its fullest potential.

Typically, these threats are persistent because of vulnerabilities, which can arise from the following:

- Misconfigured hardware or software
- Poor network design
- Inherent technology weaknesses
- End-user carelessness
- Intentional end-user acts (that is, disgruntled employees)

This chapter provides an overview of essential network security concepts, common vulnerabilities, threats, attacks, and vulnerability analysis.

Note

It is highly recommended that you study the commands covered in the chapters using the labs and the Command Reference (Cisco Security Appliance Command Reference Guide, Version 7.0, at http://www.cisco.com/application/pdf/en/us/guest/products/ps5317/c2001/ccmigration_09186a008018e5f2.pdf; and Cisco IOS Security Command Reference, Release 12.3, at http://www.cisco.com/application/pdf/en/us/guest/products/ps5317/c2001/ccmigration_09186a008018e5f2.pdf).

Not all required commands are covered in sufficient detail in the text alone. Successful completion of this course requires a thorough knowledge of command syntax and application.

Introduction to Network Security

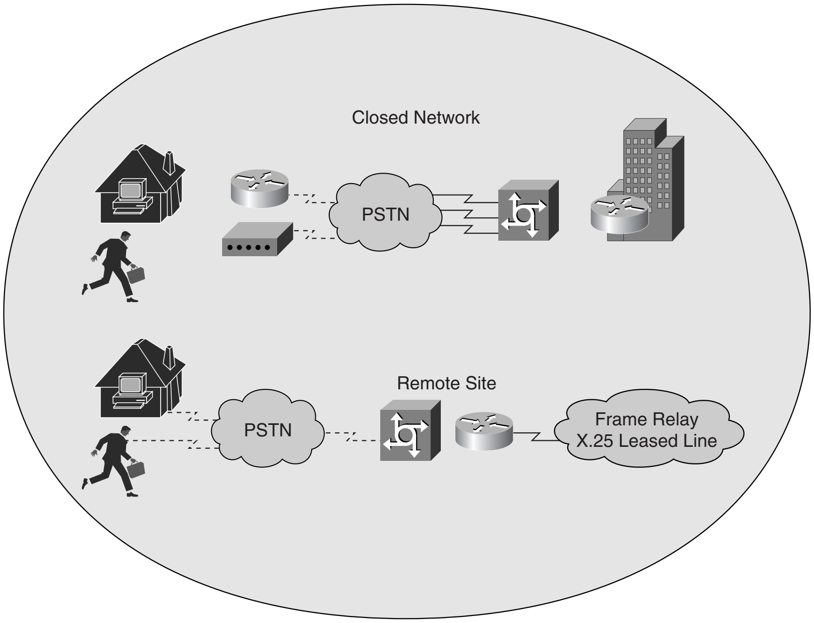
This chapter consists of an overview of what network security is all about. The sections that follow cover the following aspects of network security:

- The need for network security
- Identifying potential risks to network security
- Open versus closed security models
- Trends driving network security
- Information security organizations

The Need for Network Security

Security has one purpose: to protect assets. For most of history, this meant building strong walls to stop the enemy and establishing small, well-guarded doors to provide secure access for friends. This strategy worked well for the centralized, fortress-like world of mainframe computers and closed networks, as seen in Figure 1-1.

Figure 1-1 Closed Network



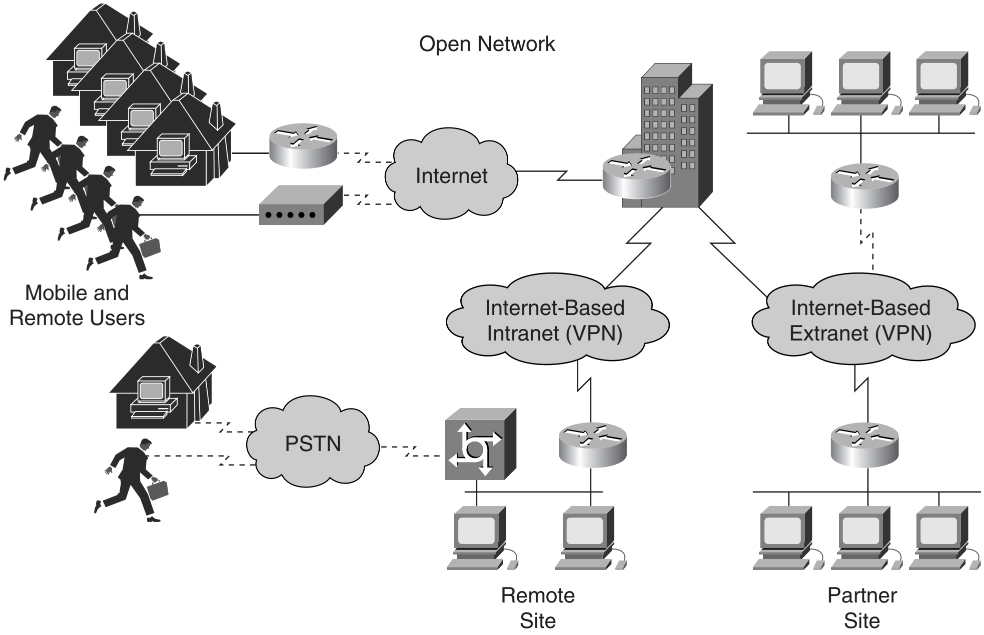
The closed network typically consists of a network designed and implemented in a corporate environment and provides connectivity only to known parties and sites without connecting to public networks. Networks were designed this way in the past and thought to be reasonably secure because of no outside connectivity.

With the advent of personal computers, LANs, and the wide-open world of the Internet, the networks of today are more open, as shown in Figure 1-2.

As e-business and Internet applications continue to grow, the key to network security lies in defining the balance between a closed and open network and differentiating the good guys from the bad guys.

With the increased number of LANs and personal computers, the Internet began to create untold numbers of security risks. Firewall devices, which are software or hardware that enforce an access control policy between two or more networks, were introduced. This technology gave businesses a balance between security and simple outbound access to the Internet, which was mostly used for e-mail and web surfing.

Figure 1-2 Open Network: The Network Today



This balance was short-lived as the use of extranets began to grow, which connected internal and external business processes. Businesses were soon realizing tremendous cost savings by connecting supply-chain management and enterprise resource planning systems to their business partners, and by connecting sales-force automation systems to mobile employees, and by providing electronic commerce connections to business customers and consumers. The firewall began to include intrusion detection, authentication, authorization, and vulnerability-assessment systems. Today, successful companies have again struck a balance by keeping the enemies out with increasingly complex ways of letting friends in.

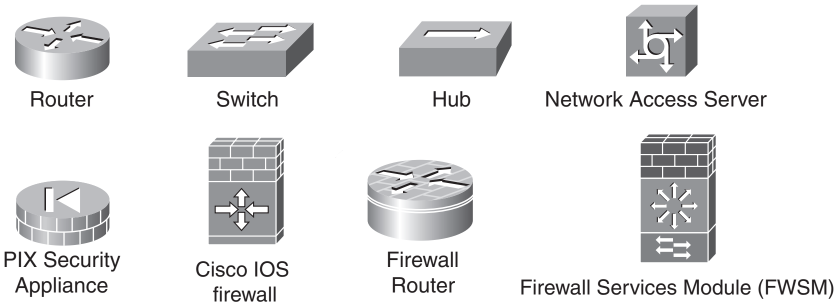
Most people expect security measures to ensure the following:

- Users can perform only authorized tasks.
- Users can obtain only authorized information.
- Users cannot cause damage to the data, applications, or operating environment of a system.

The word *security* means protection against malicious attack by outsiders (and by insiders). Statistically, there are more attacks from inside sources. Security also involves controlling the effects of errors and equipment failures. Anything that can protect against an attack will probably prevent random misfortunes, too.

Throughout this book, many definitions, acronyms, and logical device symbols dealing with security are introduced (see Figure 1-3). Refer to the glossary for further explanation when encountering unknown terms and acronyms. For a complete listing of all the graphic symbols in this book, see the Introduction.

Figure 1-3 Several Graphic Symbols Used in This Book



Lab 1.1.1 Student Lab Orientation

In this lab, you review the lab bundle equipment and gain an understanding of the security pod technology and the pod naming and addressing scheme. You then load a Cisco IOS Firewall image and the default lab configurations. After that, you cable the standard lab topology and, finally, test connectivity.

Identifying Potential Risks to Network Security

A risk analysis should identify the risks to the network, network resources, and data. The intent of a risk analysis is to identify the components of the network, evaluate the importance of each component, and then apply an appropriate level of security. This analysis helps to maintain a workable balance between security and required network access. The key is to identify what needs to be secured and at what cost. More money and assets would be allocated ensuring the security of a high-priced automobile versus an old junker, for example.

Asset Identification

Before the network can be secured, you must identify the individual components that make up the network. You need to create an asset inventory that includes all the network devices and endpoints, such as hosts and servers.

Vulnerability Assessment

After you have identified the network components, you can assess their vulnerabilities. These vulnerabilities could be weaknesses in the technology, configuration, or security policy. Any vulnerability you discover must be addressed to mitigate any threat that could take advantage of the vulnerability. Vulnerabilities can be fixed by various methods, including applying software patches, reconfiguring devices, or deploying countermeasures, such as firewalls and antivirus software. Many websites list the vulnerabilities of network components, and the manufacturers of operating systems and components that list vulnerabilities of their products sponsor many websites.

Threat Identification

A threat is an event that can take advantage of vulnerability and cause a negative impact on the network. Potential threats to the network need to be identified, and the related vulnerabilities need to be addressed to minimize the risk of the threat.

Open Versus Closed Security Models

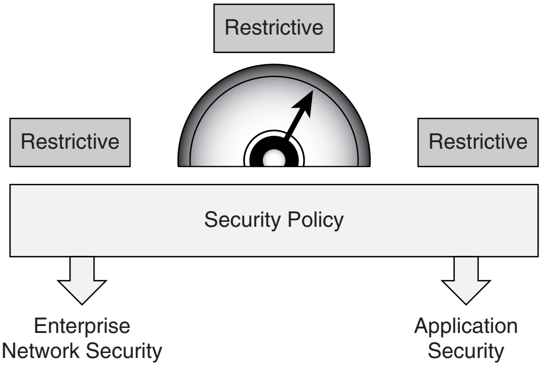
With all security designs, some trade-off occurs between user productivity and security measures. The goal of any security design is to provide maximum security with minimum impact on user access and productivity. Some security measures, such as network data encryption, do not restrict access and productivity. On the other hand, cumbersome or unnecessarily redundant verification and authorization systems can frustrate users and prevent access to critical network resources. Remember that the network is a tool designed to enhance production. If the security measures that are put in place become too cumbersome, they will actually detract rather then enhance productivity.

Networks used as productivity tools should be designed so that business needs dictate the security policy. A security policy should not determine how a business operates. Because organizations are constantly subject to change, security policies must be systematically updated to reflect new business directions, technological changes, and resource allocations.

Security policies vary greatly in design. Three general types of security models are open, restrictive, and closed. Some important points are as follows (see Figure 1-4):

- Security model can be open or closed as a starting point.
- Choose the best end-to-end mix of security products and technology to implement the model.
- Application-level security can include Secure Sockets Layer (SSL) technology.

Figure 1-4 Network Security Policies



Like security models, many devices can be classified as open, restrictive, or closed. For example, routers and switches are typically open devices, allowing high functionality and services by default. On the other hand, a firewall is typically a closed system that does not allow any services until they are switched on. Server operating systems can fall into any of the three categories, depending on the vendor. It is important to understand these principles when deploying these devices.

Open Access

An open security model is the easiest to implement, as shown in Figures 1-5 and 1-6. Few security measures are implemented in this design. Administrators configure existing hardware and software basic security capabilities. Firewalls, virtual private networks (VPNs), intrusion detection systems (IDSs), and other measures that incur additional costs are typically not implemented. Simple passwords and server security become the foundation of this model. If encryption is used, it is implemented by individual users or on servers.

Figure 1-5 Open Security Policy

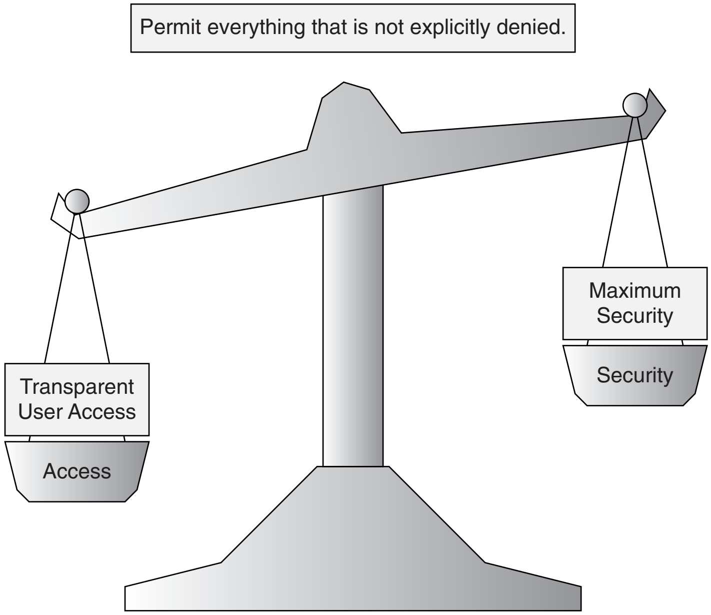
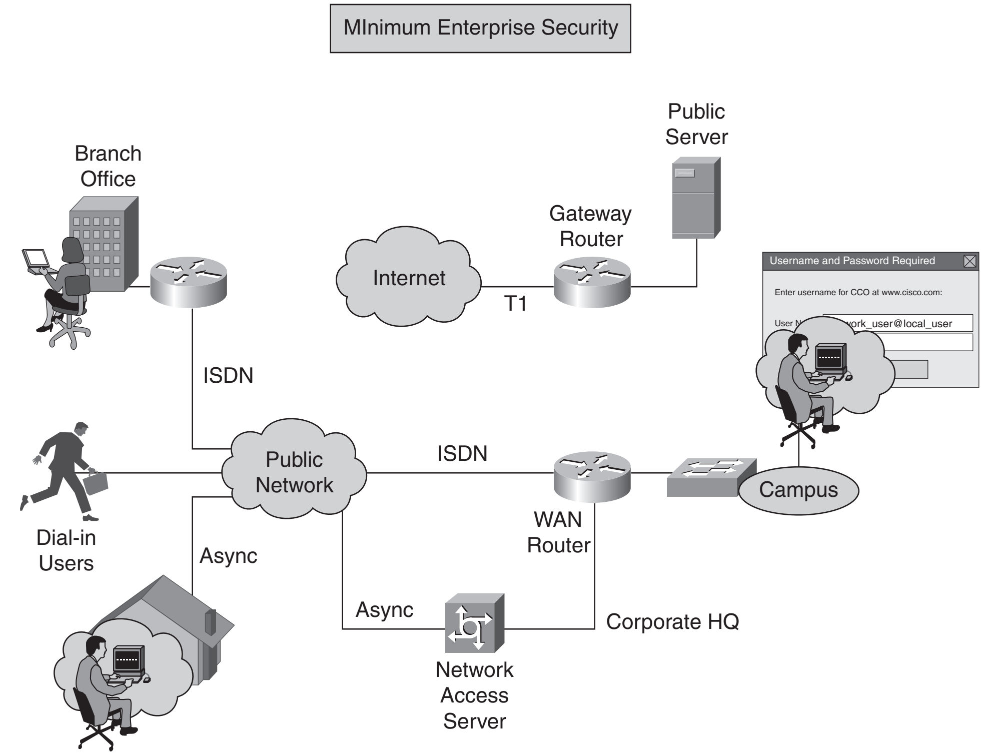


Figure 1-6 Open Security Policy Topology



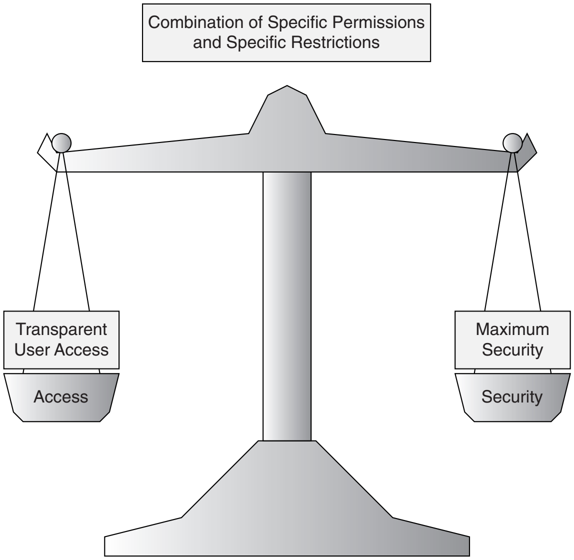
This model assumes that the protected assets are minimal, users are trusted, and threats are minimal. However, this does not exclude the need for data backup systems in most open security policy scenarios. LANs that are not connected to the Internet or public WANs are more likely to implement this type of model.

This type of network design gives users free access to all areas. When security breaches occur, they are likely to result in great damage and loss. Network administrators are usually not held responsible for network breaches or abuse.

Restrictive Access

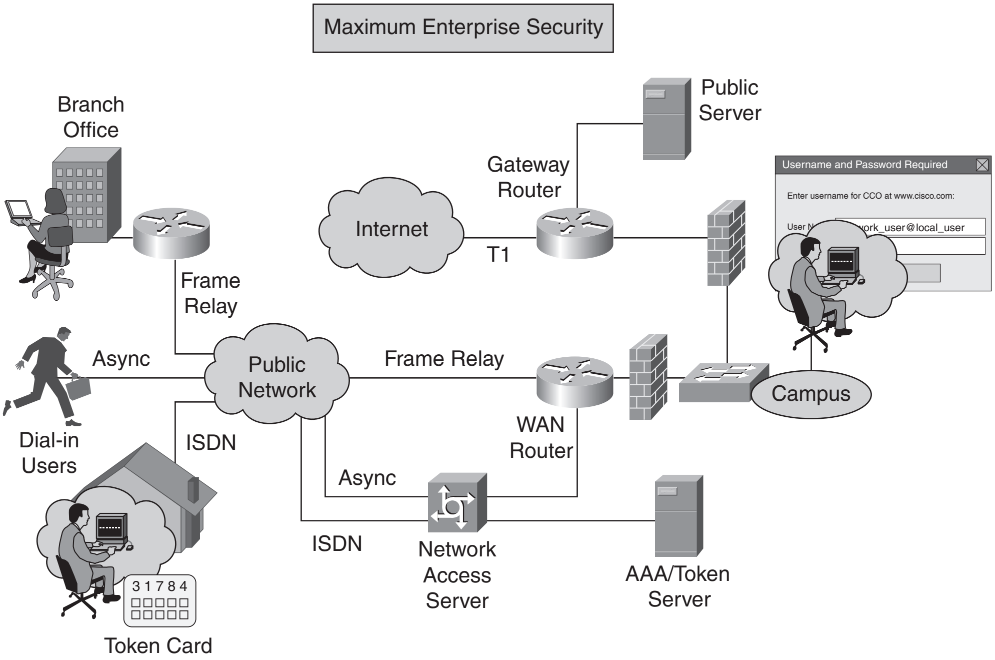
A restrictive security model is more difficult to implement, as shown in Figures 1-7 and 1-8. Many security measures are implemented in this design. Administrators configure existing hardware and software for security capabilities in addition to deploying more costly hardware and software solutions such as firewalls, VPNs, IDSs, and identity servers. Firewalls and identity servers become the foundation of this model.

Figure 1-7 Restrictive Security Policy


Combination of Specific Permissions and Specific Restrictions
Transparent User Access
Access
Maximum Security
Security

This model assumes that the protected assets are substantial, some users are not trustworthy, and that threats are likely. LANs that are connected to the Internet or public WANs are more likely to implement this type of model. Ease of use for users diminishes as security tightens.

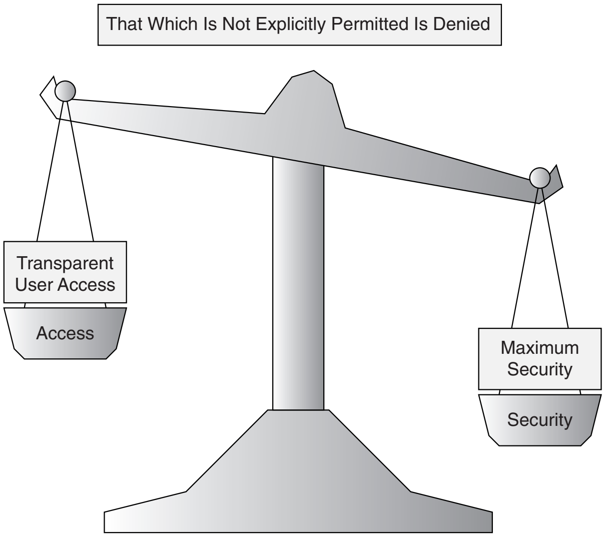
Figure 1-8 Restrictive Security Policy Topology



Closed Access

A closed security model is most difficult to implement. All available security measures are implemented in this design. Administrators configure existing hardware and software for maximum-security capabilities in addition to deploying more costly hardware and software solutions such as firewalls, VPNs, IDSs, and identity servers, as shown in Figures 1-9 and 1-10.

Figure 1-9 Closed Security Policy



The closed security model assumes that the protected assets are premium, all users are not trustworthy, and that threats are frequent. User access is difficult and cumbersome. Network administrators require greater skills and more time to administer the network. Furthermore, companies require a higher number of and better trained network administrators to maintain this tight security.

In many corporations and organizations, these administrators are likely to be unpopular while implementing and maintaining security. Network security departments must clarify that they only implement the policy, which is designed, written, and approved by the corporation. Politics behind the closed security model can be monumental. In the event of a security breach or network outage, network administrators might be held more accountable for problems.

Trends Driving Network Security

As in any fast-growing industry, changes are to be expected. The types of potential threats to network security are always evolving. If the security of the network is compromised, there could be serious consequences, such as loss of privacy, theft of information, and even legal liability. Figure 1-11 illustrates several threats and their potential consequences.

Figure 1-10 Closed Security Policy Topology

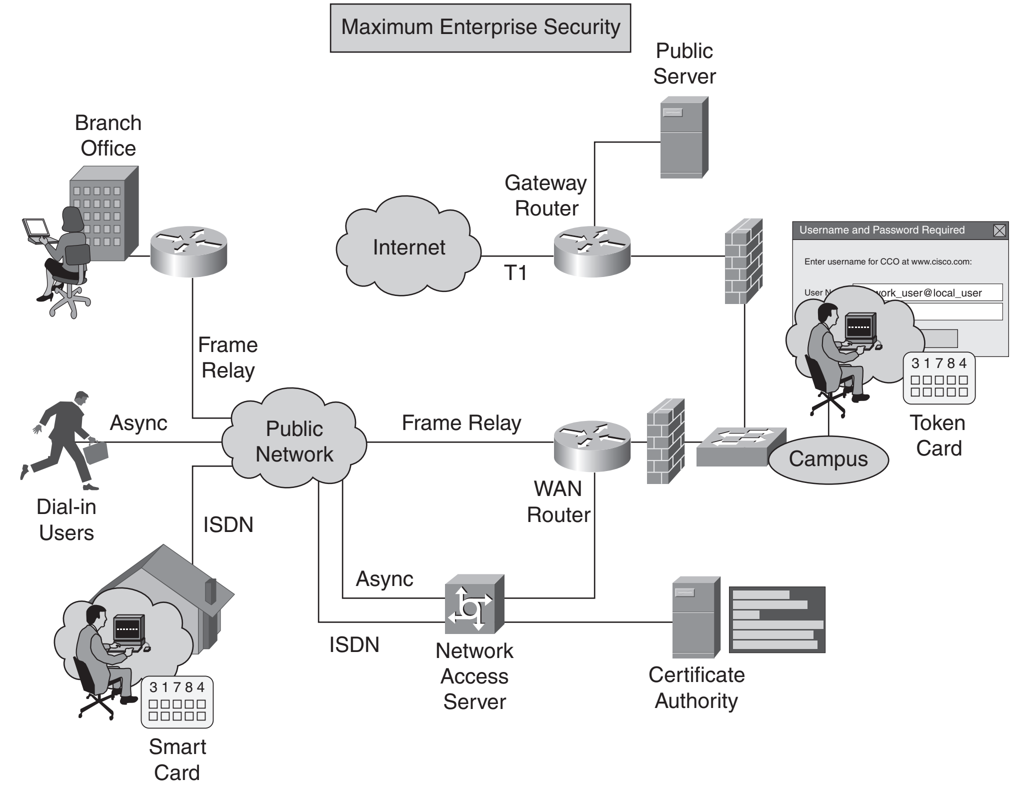
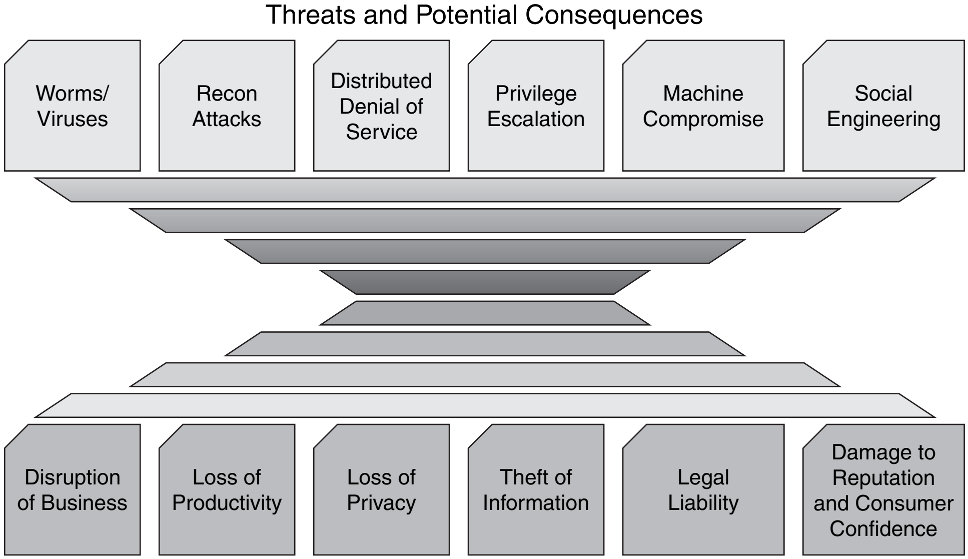


Figure 1-11 Threats and Potential Consequences



Legal Issues and Privacy Concerns

For many businesses today, one of the biggest reasons to create and follow a security policy is compliance with the law. Any business is potentially liable should a hacker or a virus take down the operation. Similarly, if a business is running a publicly held e-business and a catastrophic attack seriously impairs the business, a lawsuit is possible.

Legal liability in such cases is likely to depend on what prevention technologies and practices are available and on whether these technologies and practices are reasonably cost-effective to implement. As a result, showing due diligence will mean everything from implementing technologies such as firewalls, intrusion-detection tools, content filters, traffic analyzers, and VPNs to having best practices for continuous risk assessment and vulnerability testing. Of course, litigation is not the only legal consideration that e-businesses face today. Lawmakers concern over the lack of Internet security, particularly where it hampers rights to privacy, is growing.

Due diligence is the part of the legal equation in which the technology person researches the vulnerabilities, threats, and risks. This process determines the countermeasures that are available and gives that information to the executives, who then make the decisions based on the four mitigation strategies available:

- Transfer the risk (insurance)
- Reduce the risk (apply a mitigation)
- Accept the risk (understanding that the risk might occur and if it does the company will shoulder the loss)
- Reject the risk (it has not happened to us before, so we don't believe it will happen to use in the future)

This process is called due care on the management side: What would a prudent person do in that situation?

In 1998, the European Union passed the comprehensive Data Privacy Directives that provide consumers with strong control over their personal data. Many countries outside the United States have adopted the equivalent of these privacy principles. In the United States, more than 1000 privacy-related bills were introduced in state legislatures in 1999 and 2000, and numerous bills are currently pending.

In the United States, education, financial services, government, and health care are currently scrambling to meet federally mandated guidelines for network security and privacy. In financial services, there is the Gramm-Leach-Blilely (GLB) Act, which was passed in 1999. The GLB Act erased long-standing antitrust laws that prohibited banks, insurance companies, and securities firms from merging and sharing information with one another. The idea was that smaller firms would then be able to pursue acquisitions and alliances that would help drive competition against many of the larger financial institutions. Included in that law were several consumer privacy protections. Namely, companies must tell their customers what sorts of data they plan to share and with whom and then give customers a chance to opt out of that data sharing. The law required banks to send those notices to customers by July 1, 2001.

The U.S. government is contending with the Government Information Security Reform Act (passed in October 2002), which directs federal agencies to increase security plans for their computer systems. Representatives from the General Accounting Office (GAO) and other organizations recently told Congress that, despite this legislation, federal agencies are still falling short of dealing with key security issues.

On the health-care side, the Health Insurance Portability and Accountability Act of 1996 (HIPAA) requires the U.S. Department of Health and Human Services to develop a set of national standards for health-care transactions and provide assurance that the electronic transfer of confidential patient information will be as safe as or safer than paper-based patient records. Compliance with HIPAA is estimated to cost the health-care industry $4 billion annually.

The Family Educational Rights and Privacy Act (FERPA) is a federal law designed to protect the privacy of a student's education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. When an individual requests student information from a university, the university must respond in accordance with FERPA guidelines. The Department of Education's FERPA guidelines act as the foundation.

Finally, many education institutions in the United States must comply with the Children Internet Protection Act (CIPA) if they want to receive any form of U.S. federal funding.

Wireless Access

The increasing use of wireless LAN connections and the rapid rise of Internet access from cell phones in Europe and Asia are requiring entirely whole new approaches to security. Radio frequency (RF) connections do not respect firewalls the way wired connections do. Moreover, the slow processors, small screens, and nonexistent keyboards on cell phones and personal digital assistants (PDAs) challenge many of the standard approaches to access, authentication, and authorization.

The Need for Speed

The number of broadband connections to the Internet from homes is exceeding projections. Many businesses are finding that multiple T1 or E1 connections to the Internet no longer suffice. Current software-based security approaches have problems scaling to OC-1 and higher ratings.

IT Staffing Shortages

The IT staffing shortage is especially evident in the security field. To solve this problem, many enterprises are increasingly outsourcing day-to-day security management tasks. The application service provider (ASP) business model will become increasingly common in the security world. Therefore, security solutions will need to be more manageable in this outsourced model. Clearly, there is a demand for skilled network security professionals.

ISO/IEC 17799

ISO/IEC 17799, *Information technology—Code of practice for information security management*, is an information security standard that is published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC 17799 is intended to be a common basis and practical guideline for developing organizational security standards and effective security management practices.

ISO/IEC 17799 was originally published in 2000 and was revised and republished in 2005. ISO/IEC 17799 is based on the British Standard (BS7799). The 2005 revision of ISO/IEC 17799 is made up of the following 11 sections:

- Security policy
- Organization of information security
- Asset management
- Human resources security
- Physical and environmental security
- Communications and operations management
- Access control
- Information systems acquisition, development, and maintenance
- Information security incident management
- Business continuity management
- Compliance

Information Security Organizations

Many organizations provide useful information for security professionals. These organizations provide information on detecting and responding to both established and emerging information security threats. Information about operating system weaknesses, best practices for security, and security training and certification information is also available. Independent security evaluations have arisen to provide organizations with an unbiased and objective review of security products. For example, Common Criteria, Federal Information Processing Standards Publication 140 (FIPS 140), and International Computer Security Association (ICSA) are some of the independent certifications and evaluations.

CERT/CC

The CERT Coordination Center (CERT/CC) is a reporting center for Internet security issues. The CERT/CC plays a major role in coordinating responses to Internet security threats. The CERT/CC is located at the Software Engineering Institute (SEI) operated by Carnegie Mellon University.

US-CERT

The United States Computer Emergency Readiness Team (US-CERT) is a partnership between the Department of Homeland Security and the public and private sectors. US-CERT was established in 2003 to protect the nation's Internet infrastructure by coordinating defense against and responses to Internet security threats.

US-CERT is responsible for the following:

- Analyzing and reducing cyber threats and vulnerabilities
- Disseminating cyber threat warning information
- Coordinating incident-response activities

SANS Institute

The SysAdmin, Audit, Network, Security (SANS) Institute was established in 1989 as a cooperative research and education organization. The SANS Institute develops and maintains research documents about various aspects of information security. These documents are available at no cost. SANS also operates the Internet Storm Center, an early warning system for Internet security issues.

ISC^2

The International Information Systems Security Certification Consortium, Inc. (ISC^2) is a nonprofit organization that maintains a collection of industry best practices for information security. The ISC^2 has created five certifications that align to these best practices, the Systems Security Certified Practitioner (SSCP), and the Certified Information Systems Security Professional (CISSP). There are two Focus certifications that one can take after the CISSP, and then there is the new Certification and Accreditation Professional (CAP) certification.

Common Criteria

The Common Criteria is an international standard for evaluating IT security. It was developed by a consortium of 14 countries to replace a number of existing country-specific security assessments and was intended to establish a single high-quality standard for international use. Although there are seven security levels defined for the Common Criteria evaluation process, Evaluation Assurance Level 4 (EAL4) is the highest universal evaluation level implemented under the Common Criteria today. Table 1-1 describes each EAL.

Table 1-1 Evaluation Assurance Levels

EAL Level	Description
EAL1	Minimal level of independently assured security
EAL2	Low to moderate level of independently assured security
EAL3	Moderate level of independently assured security
EAL4	Moderate to high level of independently assured security
EAL5-7	Specific requirements, yet to be implemented. Needed only in the most restrictive government environments

FIPS

The Federal Information Processing Standard (FIPS) 140 is a U.S. and Canadian government standard that specifies security requirements for cryptographic modules. FIPS 140 has four levels of assurance: Level 1 is the lowest, and Level 4 is the most stringent. Each level builds upon the one below it, so a Level 2 certification means that a product meets the requirements for both Level 1 and Level 2. Table 1-2 describes each FIPS security level.

Table 1-2 FIPS Security Levels

Level	Description
Level 1	Lowest level of security requirements specified for a cryptographic module
Level 2	Level 1 plus tamper-evident coatings or seals, locks on removable covers or doors
Level 3	Level 2 plus detecting and responding to attempts at physical access, use, or modification of the cryptographic module
Level 4	Highest level of security useful for operation in physically unprotected environments

ICSA

ICSA Labs tests firewalls against a standard set of functional and assurance criteria elements. ICSA Labs is presently testing firewalls against the Modular Firewall Product Certification Criteria Version 4.0. ICSA also test VPN devices for IP Security (IPsec) interoperability. IPsec interoperability testing validates a product or set of products that use cryptography to provide effective security services. ICSA certification exists to provide a set of measurable, public-domain standards for commercial security products.

Introduction to Vulnerabilities, Threats, and Attacks

When discussing network security, the three common terms used are as follows:

- **Vulnerability**—A weakness that is inherent in every network and device. This includes routers, switches, desktops, servers, and even security devices themselves.
- **Threats**—The people eager, willing, and qualified to take advantage of each security weakness, and they continually search for new exploits and weaknesses.
- **Attacks**—The threats use a variety of tools, scripts, and programs to launch attacks against networks and network devices. Typically, the network devices under attack are the endpoints, such as servers and desktops.

The sections that follow discuss vulnerabilities, threats, and attacks in further detail.

Vulnerabilities

Vulnerabilities in network security can be summed up as the "soft spots" that are present in every network. The vulnerabilities are present in the network and individual devices that make up the network.

Networks are typically plagued by one or all of three primary vulnerabilities or weaknesses:

- Technology weaknesses
- Configuration weaknesses
- Security policy weaknesses

The sections that follow examine each of these weaknesses in more detail.

Technological Weaknesses

Computer and network technologies have intrinsic security weaknesses. These include TCP/IP protocol weaknesses, operating system weaknesses, and network equipment weaknesses. Table 1-3 describes these three weaknesses.

Table 1-3 Network Security Weaknesses

Weakness	Description
TCP/IP protocol weaknesses	HTTP, FTP, and ICMP are inherently insecure. Simple Network Management Protocol (SNMP), Simple Mail Transfer Protocol (SMTP), and SYN floods are related to the inherently insecure structure upon which TCP was designed.
Operating system weaknesses	The UNIX, Linux, Macintosh, Windows NT, 9x, 2K, XP, and OS/2 operating systems all have security problems that must be addressed. These are documented in the CERT archives at http://www.cert.org.
Network equipment weaknesses	Various types of network equipment, such as routers, firewalls, and switches, have security weaknesses that must be recognized and protected against. These weaknesses include the following: Password protection Lack of authentication Routing protocols Firewall holes

Configuration Weaknesses

Network administrators or network engineers need to learn what the configuration weaknesses are and correctly configure their computing and network devices to compensate. Table 1-4 lists some common configuration weaknesses.

Table 1-4 Configuration Weaknesses

Weakness	How the Weakness Is Exploited
Unsecured user accounts	User account information might be transmitted insecurely across the network, exposing usernames and passwords to snoopers.
System accounts with easily guessed passwords	This common problem is the result of poorly selected and easily guessed user passwords.
Misconfigured Internet services	A common problem is to turn on JavaScript in web browsers, enabling attacks by way of hostile JavaScript when accessing untrusted sites. IIS, Apache, FTP, and Terminal Services also pose problems.
Unsecured default settings within products	Many products have default settings that enable security holes.

Table 1-4 Configuration Weaknesses *continued*

Weakness	How the Weakness Is Exploited
Misconfigured network equipment	Misconfigurations of the equipment itself can cause significant security problems. For example, misconfigured access lists, routing protocols, or SNMP community strings can open up large security holes. Misconfigured or lack of encryption and remote-access controls can also cause significant security issues, as can the practice of leaving ports open on a switch (which could allow the introduction of noncompany computing equipment).

Security Policy Weaknesses

Security policy weaknesses can create unforeseen security threats. The network can pose security risks to the network if users do not follow the security policy. Table 1-5 lists some common security policy weaknesses and how those weaknesses are exploited.

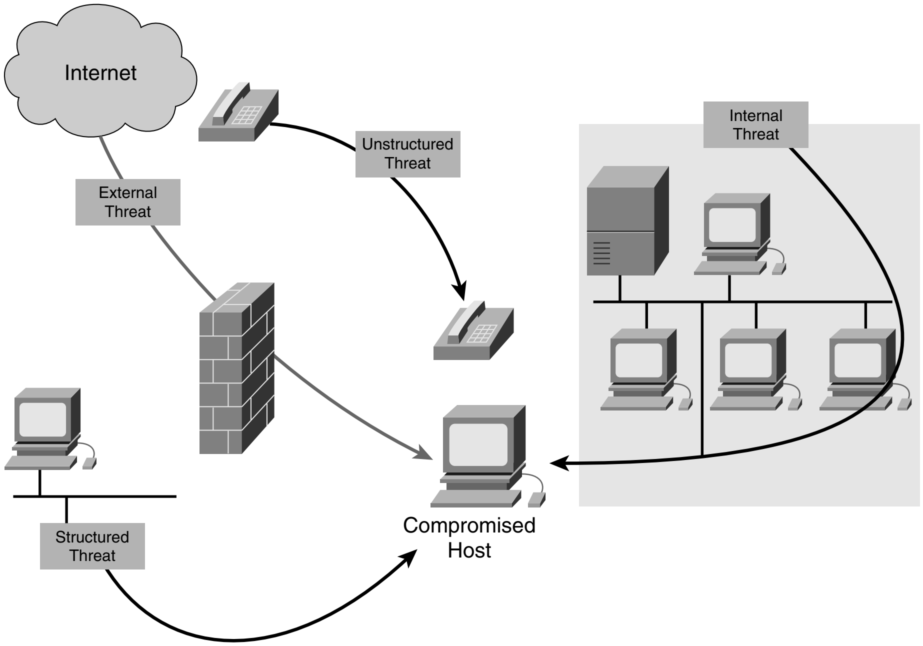
Table 1-5 Security Policy Weaknesses

Weakness	How the Weakness Is Exploited
Lack of written security policy	An unwritten policy cannot be consistently applied or enforced.
Politics	Political battles and turf wars can make it difficult to implement a consistent security policy.
Lack of continuity.	Poorly chosen, easily cracked, or default passwords can allow unauthorized access to the network.
Logical access controls. not applied	Inadequate monitoring and auditing allow attacks and unauthorized use to continue, wasting company resources. This could result in legal action or termination against IT technicians, IT management, or even company leadership that allows these unsafe conditions to persist. Lack of careful and controlled auditing can also make it hard to enforce policy and to stand up to legal challenges for “wrongful termination” and suits against the organization.
Software and hardware installation and changes do not follow policy.	Unauthorized changes to the network topology or installation of unapproved applications create security holes.
Disaster recovery plan nonexistent.	The lack of a disaster recovery plan allows chaos, panic, and is confusion to occur when someone attacks the enterprise.

Threats

There are four primary classes of threats to network security, as Figure 1-12 depicts. The list that follows describes each class of threat in more detail.

Figure 1-12 Variety of Threats



- ***Unstructured threats***—Unstructured threats consist of mostly inexperienced individuals using easily available hacking tools such as shell scripts and password crackers. Even unstructured threats that are only executed with the intent of testing and challenging a hacker's skills can still do serious damage to a company. For example, if an external company website is hacked, the integrity of the company is damaged. Even if the external website is separate from the internal information that sits behind a protective firewall, the public does not know that. All the public knows is that the site is not a safe environment to conduct business.
- ***Structured threats***— Structured threats come from hackers who are more highly motivated and technically competent. These people know system vulnerabilities and can understand and develop exploit code and scripts. They understand, develop, and use sophisticated hacking techniques to penetrate unsuspecting businesses. These groups are often involved with the major fraud and theft cases reported to law enforcement agencies.
- ***External threats***—External threats can arise from individuals or organizations working outside of a company. They do not have authorized access to the computer systems or network. They work their way into a network mainly from the Internet or dialup access servers.

- ***Internal threats***—Internal threats occur when someone has authorized access to the network with either an account on a server or physical access to the network. According to the FBI, internal access and misuse account for 60 percent to 80 percent of reported incidents.

As the types of threats, attacks, and exploits have evolved, various terms have been coined to describe different groups of individuals. Some of the most common terms are as follows:

- ***Hacker***—Hacker is a general term that has historically been used to describe a computer programming expert. More recently, this term is commonly used in a negative way to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.

- ***Cracker***—Cracker is the term that is generally regarded as the more accurate word that is used to describe an individual who attempts to gain unauthorized access to network resources with malicious intent.

- ***Phreaker***—A phreaker is an individual who manipulates the phone network to cause it to perform a function that is normally not allowed. A common goal of phreaking is breaking into the phone network, usually through a payphone, to make free long-distance calls.

- ***Spammer***—A spammer is an individual who sends large numbers of unsolicited e-mail messages. Spammers often use viruses to take control of home computers to use these computers to send out their bulk messages.

- ***Phisher***—A phisher uses e-mail or other means in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords. The phisher masquerades as a trusted party that would have a legitimate need for the sensitive information.

- ***White hat***—White hat is a term used to describe individuals who use their abilities to find vulnerabilities in systems or networks and then report these vulnerabilities to the owners of the system so that they can be fixed.

- ***Black hat***—Black hat is another term for individuals who use their knowledge of computer systems to break into systems or networks that they are not authorized to use.

Attacks

Four primary classes of attacks exist:

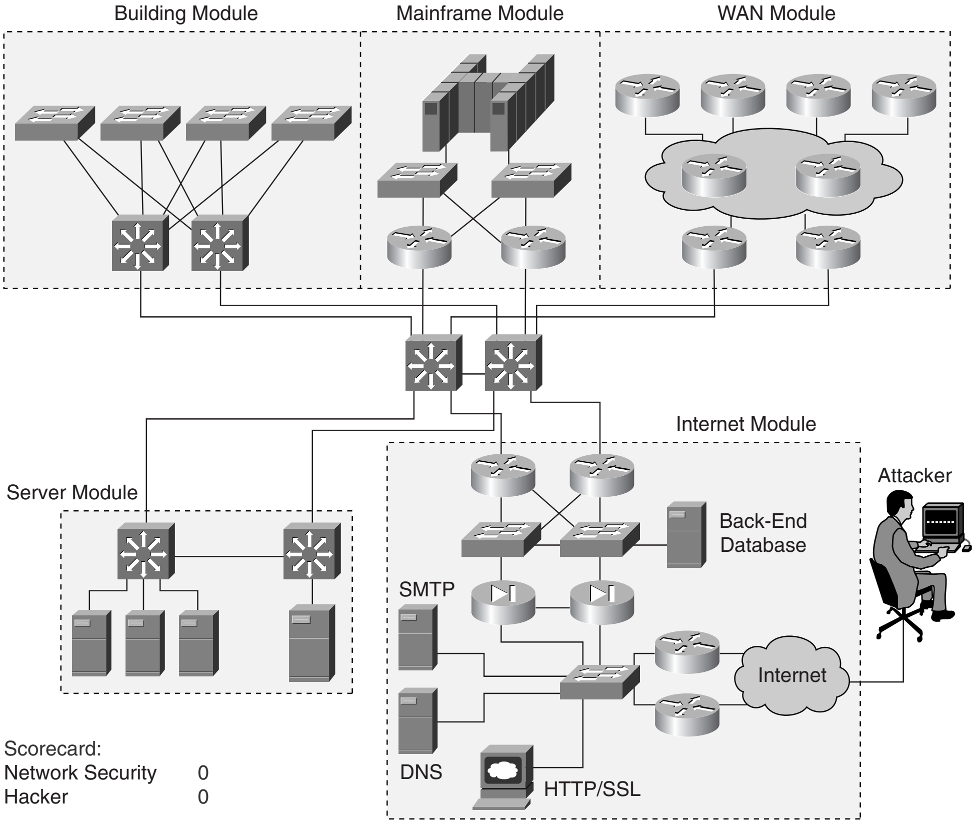
- Reconnaissance
- Access
- Denial of service
- Worms, viruses, and Trojan horses

The sections that follow cover each attack class in more detail.

Reconnaissance

Reconnaissance is the unauthorized discovery and mapping of systems, services, or vulnerabilities (see Figure 1-13). It is also known as information gathering and, in most cases, it precedes an actual access or denial-of-service (DoS) attack. Reconnaissance is somewhat analogous to a thief casing a neighborhood for vulnerable homes to break into, such as an unoccupied residence, easy-to-open doors, or open windows.

Figure 1-13 Reconnaissance



Access

System access is the ability for an unauthorized intruder to gain access to a device for which the intruder does not have an account or a password. Entering or accessing systems to which one does not have authority to access usually involves running a hack, script, or tool that exploits a known vulnerability of the system or application being attacked.

Denial of Service (DoS)

Denial of service implies that an attacker disables or corrupts networks, systems, or services with the intent to deny services to intended users. DoS attacks involve either crashing the system or slowing it down to the point that it is unusable. But DoS can also be as simple as deleting or corrupting information. In most cases, performing the attack simply involves running a hack or script. The attacker does not need prior access to the target because a way to access it is all that is usually required. For these reasons, DoS attacks are the most feared.

Worms, Viruses, and Trojan Horses

Malicious software is inserted onto a host to damage a system; corrupt a system; replicate itself; or deny services or access to networks, systems or services. They can also allow sensitive information to be copied or echoed to other systems.

Trojan horses can be used to ask the user to enter sensitive information in a commonly trusted screen. For example, an attacker might log in to a Windows box and run a program that looks like the true Windows logon screen, prompting a user to type his username and password. The program would then send the information to the attacker and then give the Windows error for bad password. The user would then log out, and the correct Windows logon screen would appear; the user is none the wiser that his password has just been stolen.

Even worse, the nature of all these threats is changing—from the relatively simple viruses of the 1980s to the more complex and damaging viruses, DoS attacks, and hacking tools in recent years. Today, these hacking tools are powerful and widespread, with the new dangers of self-spreading blended worms such as Slammer and Blaster and network DoS attacks. Also, the old days of attacks that take days or weeks to spread are over. Threats now spread worldwide in a matter of minutes. The Slammer worm of January 2003 spread around the world in less than 10 minutes.

The next generations of attacks are expected to spread in just seconds. These worms and viruses could do more than just wreak havoc by overloading network resources with the amount of traffic they generate, they could also be used to deploy damaging payloads that steal vital information or erase hard drives. Also, there is a strong concern that the threats of tomorrow will be directed at the very infrastructure of the Internet.

Attack Examples

Several types of attacks are used today, and this section looks at a representative sample in more detail.

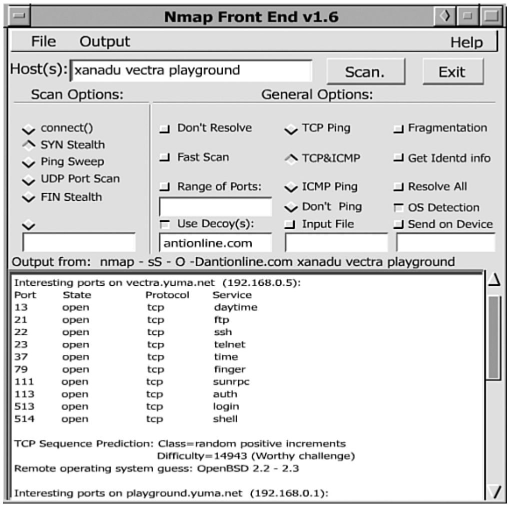
Reconnaissance Attacks

Reconnaissance attacks can consist of the following:

- Packet sniffers
- Port scans
- Ping sweeps
- Internet information queries

A malicious intruder typically ping sweeps the target network to determine which IP addresses are alive. After this, the intruder uses a port scanner, as shown in Figure 1-14, to determine what network services or ports are active on the live IP addresses. From this information, the intruder queries the ports to determine the application type and version, and the type and version of operating system running on the target host. Based on this information, the intruder can determine whether a possible vulnerability exists that can be exploited.

Figure 1-14 Nmap



Host(s): xanadu vectra playground

Scan Options:

- ○ connect()
- ● SYN Stealth
- ○ Ping Sweep
- ○ UDP Port Scan
- ○ FIN Stealth
- ○

General Options:

- □ Don't Resolve
- □ Fast Scan
- □ Range of Ports:
- ☑ Use Decoy(s): antionline.com
- ○ TCP Ping
- ● TCP&ICMP
- ○ ICMP Ping
- ○ Don't Ping
- □ Input File
- □ Fragmentation
- □ Get Identd info
- □ Resolve All
- ☑ OS Detection
- □ Send on Device

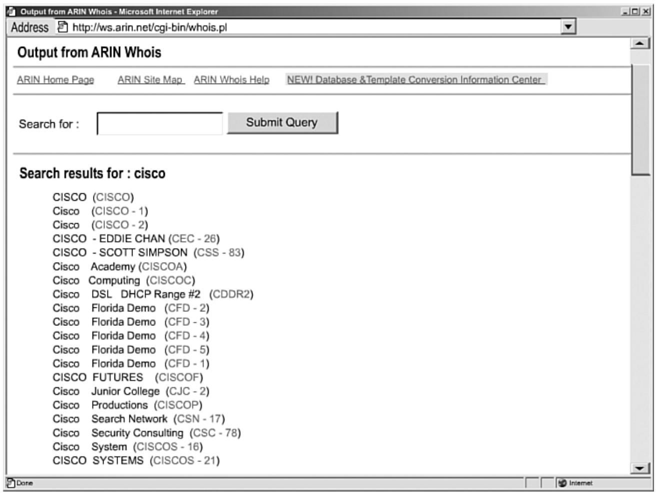
Output from: nmap - sS - O -Dantionline.com xanadu vectra playground

```
Interesting ports on vectra.yuma.net  (192.168.0.5):
Port      State           Protocol      Service
13        open            tcp           daytime
21        open            tcp           ftp
22        open            tcp           ssh
23        open            tcp           telnet
37        open            tcp           time
79        open            tcp           finger
111       open            tcp           sunrpc
113       open            tcp           auth
513       open            tcp           login
514       open            tcp           shell

TCP Sequence Prediction: Class=random positive increments
                         Difficulty=14943 (Worthy challenge)
Remote operating system guess: OpenBSD 2.2 - 2.3

Interesting ports on playground.yuma.net  (192.168.0.1):
```

Using, for example, the Nslookup and Whois software utilities (see Figure 1-15), an attacker can easily determine the IP address space assigned to a given corporation or entity. The **ping** command tells the attacker what IP addresses are alive.

Network snooping and packet sniffing are common terms for *eavesdropping*. Eavesdropping is listening in to a conversation, spying, prying, or snooping. The information gathered by eavesdropping can be used to pose other attacks to the network.

Figure 1-15 ARIN Whois


Output from ARIN Whois - Microsoft Internet Explorer
Address http://ws.arin.net/cgi-bin/whois.pl
Submit Query
Done
Internet

Output from ARIN Whois

ARIN Home Page ARIN Site Map ARIN Whois Help NEW! Database &Template Conversion Information Center

Search for :

Search results for : cisco

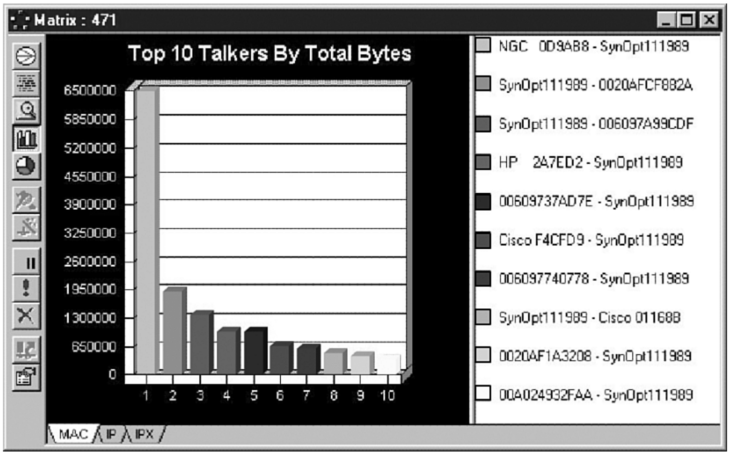
CISCO (CISCO)
Cisco (CISCO - 1)
Cisco (CISCO - 2)
CISCO - EDDIE CHAN (CEC - 26)
CISCO - SCOTT SIMPSON (CSS - 83)
Cisco Academy (CISCOA)
Cisco Computing (CISCOC)
Cisco DSL DHCP Range #2 (CDDR2)
Cisco Florida Demo (CFD - 2)
Cisco Florida Demo (CFD - 3)
Cisco Florida Demo (CFD - 4)
Cisco Florida Demo (CFD - 5)
Cisco Florida Demo (CFD - 1)
CISCO FUTURES (CISCOF)
Cisco Junior College (CJC - 2)
Cisco Productions (CISCOP)
Cisco Search Network (CSN - 17)
Cisco Security Consulting (CSC - 78)
Cisco System (CISCOS - 16)
CISCO SYSTEMS (CISCOS - 21)

An example of data susceptible to eavesdropping is SNMP Version 1 community strings, which are sent in clear text. An intruder could eavesdrop on SNMP queries and gather valuable data on network equipment configuration. Another example is the capture of usernames and passwords as they cross a network.

Types of Eavesdropping

A common method for eavesdropping on communications is to capture TCP/IP or other protocol packets and decode the contents using a protocol analyzer or similar utility, as shown in Figure 1-16.

Figure 1-16 Protocol Analyzer


Matrix : 471
Top 10 Talkers By Total Bytes
6500000
5850000
5200000
4550000
3900000
3250000
2600000
1950000
1300000
650000
0
1
2
3
4
5
6
7
8
9
10
NGC 0D9AB8 - SynOpt111989
SynOpt111989 - 0020AFCF882A
SynOpt111989 - 006097A99CDF
HP 2A7ED2 - SynOpt111989
00609737AD7E - SynOpt111989
Cisco F4CFD9 - SynOpt111989
006097740778 - SynOpt111989
SynOpt111989 - Cisco 01168B
0020AF1A3208 - SynOpt111989
00A024932FAA - SynOpt111989
MAC
IP
IPX

Two common uses of eavesdropping are as follows:

- **Information gathering**—Network intruders can identify usernames, passwords, or information carried in the packet such as credit card numbers or sensitive personal information.
- **Information theft**—Network eavesdropping can lead to information theft. The theft can occur as data is transmitted over the internal or external network. The network intruder can also steal data from networked computers by gaining unauthorized access. Examples include breaking into or eavesdropping on financial institutions and obtaining credit card numbers. Another example is using a computer to crack a password file.

Tools Used to Perform Eavesdropping

The following tools are used for eavesdropping:

- Network or protocol analyzers
- Packet capturing utilities on networked computers

Methods to Counteract Eavesdropping

Three of the most effective methods for counteracting eavesdropping are as follows:

- Implementing and enforcing a policy directive that forbids the use of protocols with known susceptibilities to eavesdropping
- Using encryption that meets the data security needs of the organization without imposing an excessive burden on the system resources or the users
- Using switched networks

Encrypted Data for Protection Against Reconnaissance Attacks

Encryption provides protection for data susceptible to eavesdropping attacks, password crackers, or manipulation. Some benefits of data encryption are as follows:

- Almost every company has transactions, which, if viewed by an eavesdropper, could have negative consequences. Encryption ensures that when sensitive data passes over a medium susceptible to eavesdropping, it cannot be altered or observed.
- Decryption is necessary when the data reaches the router or other termination device on the far-receiving LAN where the destination host resides.
- By encrypting after the UDP or TCP headers, so that only the IP payload data is encrypted, Cisco IOS network-layer encryption allows all intermediate routers and switches to forward the traffic as they would any other IP packets. Payload-only encryption allows flow switching and all access list features to work with the encrypted traffic just as they would with plain text traffic, thereby preserving desired quality of service (QoS) for all data.

Most encryption algorithms can be broken and the information can be revealed if the attacker has enough time, desire, and resources. A realistic goal of encryption is to make obtaining the information too work-intensive to be worth it to the attacker.

Access Attacks

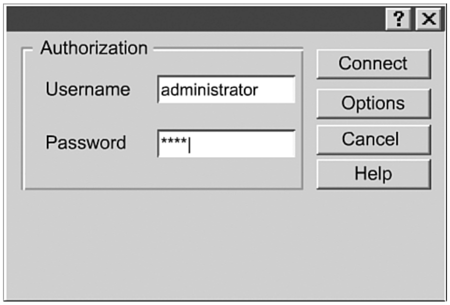
Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information. Access attacks can consist of the following:

- Password attacks
- Trust exploitation
- Port redirection
- Man-in-the-middle attacks
- Social engineering
- Phishing

Password Attacks

Password attacks can be implemented using several methods, including brute-force attacks, Trojan horse programs, IP spoofing, and packet sniffers. Although packet sniffers and IP spoofing can yield user accounts and passwords, password attacks usually refer to repeated attempts to identify a user account, password, or both (see Figure 1-17 for an illustration of an attempt to attack using the administrator's profile). These repeated attempts are called brute-force attacks.

Figure 1-17 Password Attack Example



Username administrator

Password ****

Often a brute-force attack is performed using a program that runs across the network and attempts to log in to a shared resource, such as a server. When an attacker gains access to a resource, he has the same access rights as the user whose account has been compromised. If this account has sufficient privileges, the attacker can create a back door for future access, without concern for any status and password changes to the compromised user account. In fact, not only would the attacker have the same rights as the exploited, he could attempt privilege escalation.

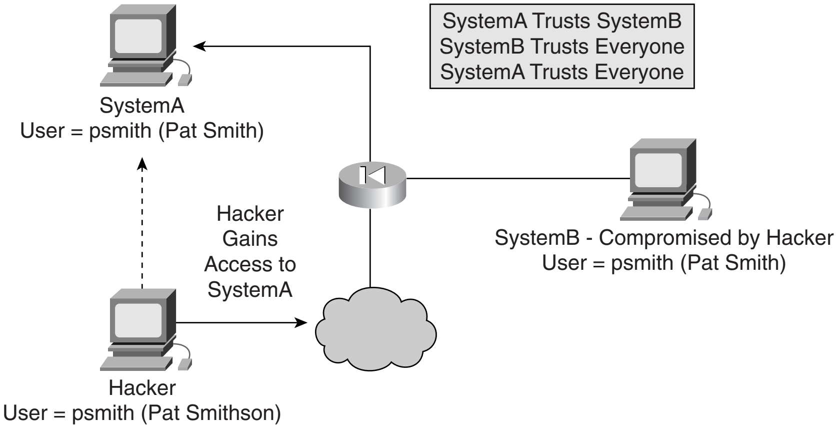
The following are the two methods for computing passwords:

- ***Dictionary cracking***—All of the words in a dictionary file are computed and compared against the possible users' password. This method is extremely fast and finds simple passwords.
- ***Brute-force computation***—This method uses a particular character set, such as A to Z, or A to Z plus 0 to 9, and computes the hash for every possible password made up of those characters. It always computes the password if that password is made up of the character set you have selected to test. The downside is that time is required for completion of this type of attack.

Trust Exploitation

Although it is more of a technique than a hack itself, ***trust exploitation***, as shown in Figure 1-18 refers to an attack in which an individual takes advantage of a trust relationship within a network. The classic example is a perimeter network connection from a corporation. These network segments often house Domain Name System (DNS), SMTP, and HTTP servers. Because all these servers reside on the same segment, the compromise of one system can lead to the compromise of other systems because these systems usually trust other systems attached to the same network.

Figure 1-18 Trust Exploitation


SystemA Trusts SystemB
SystemB Trusts Everyone
SystemA Trusts Everyone
SystemA
User = psmith (Pat Smith)
Hacker
Gains
Access to
SystemA
SystemB - Compromised by Hacker
User = psmith (Pat Smith)
Hacker
User = psmith (Pat Smithson)

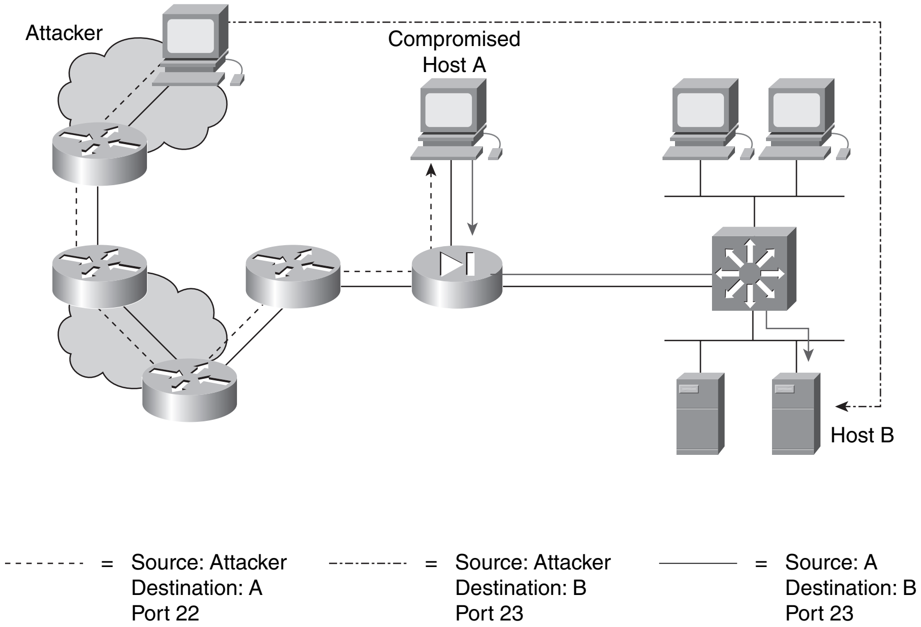
Another example is a system on the outside of a firewall that has a trust relationship with a system on the inside of a firewall. When the outside system is compromised, it can take advantage of that trust relationship to attack the inside network. Another form of an access attack involves privilege escalation. Privilege escalation occurs when a user obtains privileges or rights to objects that were not assigned to the user by an administrator. Objects can be files, commands, or other components on a network device. The intent is to gain access to information or execute unauthorized procedures. This information is used to gain administrative privileges to a system or device. They use these privileges to install sniffers, create backdoor accounts, or delete log files.

Trust exploitation-based attacks can be mitigated through tight constraints on trust levels within a network. Systems on the outside of a firewall should never be absolutely trusted by systems on the inside of a firewall. Such trust should be limited to specific protocols and should be authenticated by something other than an IP address where possible.

Port Redirection

Port redirection attacks, as shown in Figure 1-19, are a type of trust exploitation attack that uses a compromised host to pass traffic through a firewall that would otherwise be dropped. Consider a firewall with three interfaces and a host on each interface. The host on the outside can reach the host on the public services segment, but not the host on the inside. This publicly accessible segment is commonly referred to as a demilitarized zone (DMZ). The host on the public services segment can reach the host on both the outside and the inside. If hackers were able to compromise the public services segment host, they could install software to redirect traffic from the outside host directly to the inside host. Although neither communication violates the rules implemented in the firewall, the outside host has now achieved connectivity to the inside host through the port redirection process on the public services host. An example of an application that can provide this type of access is Netcat.

Figure 1-19 Protocol Analyzer


Attacker
Compromised Host A
Host B
- - - - - - - = Source: Attacker Destination: A Port 22
-·-·-·-·- = Source: Attacker Destination: B Port 23
——— = Source: A Destination: B Port 23

Port redirection can be mitigated primarily through the use of proper trust models, which are network specific (as mentioned earlier). Assuming a system under attack, a host-based IDS can help detect a hacker and prevent installation of such utilities on a host.

Man-in-the-Middle Attacks

A ***man-in-the-middle attack*** requires that the hacker have access to network packets that come across a network. An example could be someone who is working for an Internet service provider (ISP) and has access to all network packets transferred between the ISP network and any other network.

Such attacks are often implemented using network packet sniffers and routing and transport protocols. The possible uses of such attacks are theft of information, hijacking of an ongoing session to gain access to private network resources, traffic analysis to derive information about a network and its users, denial of service, corruption of transmitted data, and introduction of new information into network sessions.

Man-in-the-middle attack mitigation is achieved by encrypting traffic in an IPsec tunnel, which would allow the hacker to see only cipher text.

Social Engineering

The easiest hack (***social engineering***) involves no computer skill at all. If an intruder can trick a member of an organization into giving over valuable information, such as locations of files, and servers, and passwords, the process of hacking is made immeasurably easier.

Perhaps the simplest, but a still-effective attack is tricking a user into thinking one is an administrator and requesting a password for various purposes. Users of Internet systems frequently receive messages that request password or credit card information to "set up their account" or "reactivate settings." Users of these systems must be warned early and frequently not to divulge sensitive information, passwords or otherwise, to people claiming to be administrators. In reality, administrators of computer systems rarely, if ever, need to know the user's password to perform administrative tasks. However, even social engineering might not be necessary—in an Infosecurity survey, 90 percent of office workers gave away their password in exchange for a cheap pen.

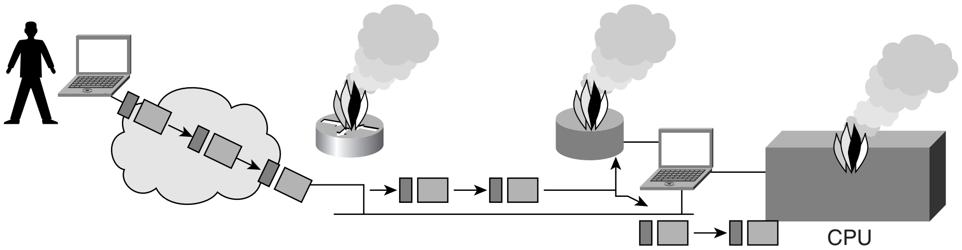
Phishing

Phishing is a type of social-engineering attack that involves using e-mail or other types of messages in an attempt to trick others into providing sensitive information, such as credit card numbers or passwords. The phisher masquerades as a trusted party that has a seemingly legitimate need for the sensitive information. Frequent phishing scams involve sending out spam e-mails that appear to be from common online banking or auction sites. These e-mails contain hyperlinks that appear to be legitimate but actually cause users to visit a phony site set up by the phisher to capture their information. The site appears to belong to the party that was faked in the e-mail, and when users enter their information it is recorded for the phisher to use.

Denial-of-Service (DoS) Attacks

Certainly the most publicized form of attack, DoS attacks are also among the most difficult to completely eliminate. Even within the hacker community, DoS attacks are regarded as trivial and considered bad form because they require so little effort to execute. Still, because of their ease of implementation and potentially significant damage, DoS attacks deserve special attention from security administrators. If you are interested in learning more about DoS attacks, researching the methods employed by some of the better-known attacks can be useful. DoS attacks take many forms. Ultimately, they prevent authorized people from using a service by using up system resources, as shown in Figure 1-20.

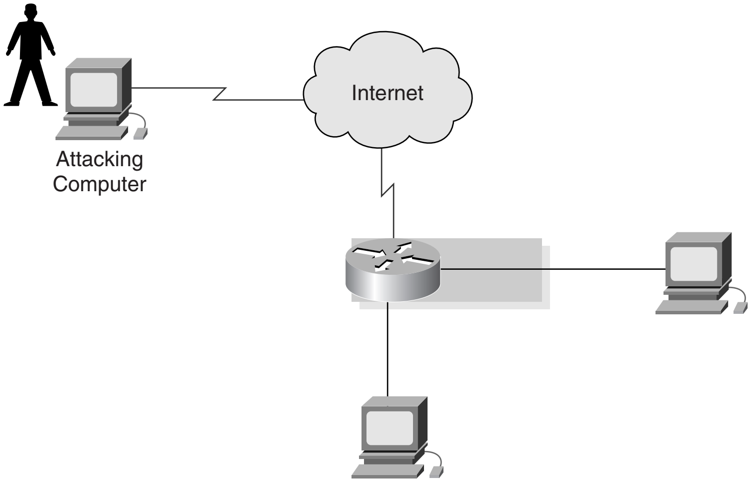
Figure 1-20 Denial of Service



The following are some examples of common DoS threats:

- **Ping of death**—This attack modifies the IP portion of the header, indicating that there is more data in the packet than there actually is, causing the receiving system to crash, as shown in Figure 1-21.

Figure 1-21 Ping of Death



- **SYN flood attack**— This attack randomly opens up many TCP ports, tying up the network equipment or computer with so many bogus requests that sessions are thereby denied to others. This attack is accomplished with protocol analyzers or other programs.

  The SYN flood attack sends TCP connections requests faster than a machine can process them. The SYN flood attack follows these steps:

  – An attacker creates a random source address for each packet.

  – The SYN flag set in each packet is a request to open a new connection to the server from the spoofed IP address.

  – A victim responds to spoofed IP address, and then waits for confirmation that never arrives (waits about three minutes).

  – The victim's connection table fills up waiting for replies.

  – After the table fills up, all new connections are ignored.

  – Legitimate users are ignored, too, and cannot access the server.

  – When the attacker stops flooding the server, it usually goes back to normal state (SYN floods rarely crash servers).

  Newer operating systems manage resources better, making it more difficult to overflow tables, but still are vulnerable.

  The SYN flood can be used as part of other attacks, such as disabling one side of a connection in TCP hijacking, or by preventing authentication or logging between servers.

- **Packet fragmentation and reassembly**—This attack exploits a buffer–overrun bug in hosts or internetworking equipment.

- **E-mail bombs**—Programs can send bulk e-mails to individuals, lists, or domains, monopolizing e-mail services.

- **CPU hogging**—These attacks constitute programs such as Trojan horses or viruses that tie up CPU cycles, memory, or other resources.

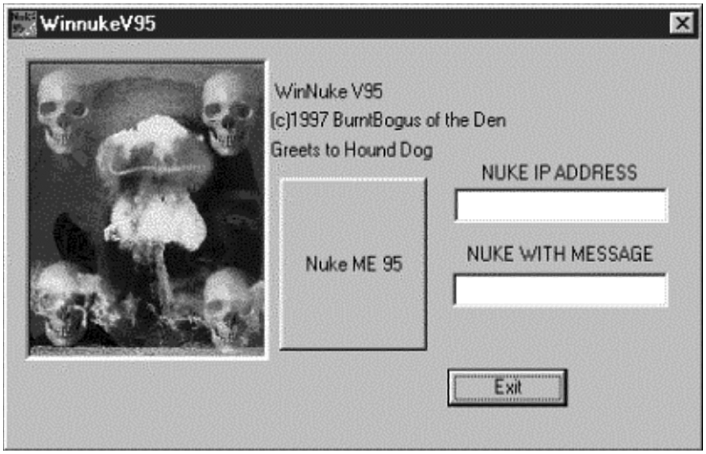
- **Malicious applets**—These attacks are Java, JavaScript, or ActiveX programs that act as Trojan horses or viruses to cause destruction or tie up computer resources.

- **Misconfiguring routers**—Misconfiguring routers to reroute traffic disables web traffic.

- **The chargen attack**—This attack establishes a connection between UDP services, producing a high character output. The host chargen service is connected to the echo service on the same or different systems, causing congestion on the network with echoed chargen traffic.

- **Out-of-band attacks such as WinNuke**— These attacks send out-of-band data to port 139 on Windows 95 or Windows NT machines. The attacker needs the victim's IP address to launch this attack, as shown in Figure 1-22.

Figure 1-22 WinNuke



- **DoS**—DoS can occur accidentally because of misconfigurations or misuse by legitimate users or system administrators.
- **Land.c**—This program sends a TCP SYN packet that specifies the target host address as both source and destination. The program also uses the same port (such as 113 or 139) on the target host as both source and destination, causing the target system to stop functioning.
- **Teardrop.c**—In this attack, the fragmentation process of the IP is implemented in such a way that reassembly problems can cause machines to crash.
- **Targa.c**—This attack is a multiplatform DoS attack that integrates bonk, jolt, land, nestea, netear, syndrop, teardrop, and WinNuke all into one exploit.

Masquerade/IP Spoofing Attacks

With a masquerade attack, the network intruder can manipulate TCP/IP packets by IP spoofing, falsifying the source IP address, thereby appearing to be another user. The intruder assumes the identity of a valid user and gains that user's access privileges by IP spoofing. IP spoofing occurs when intruders create IP data packets with falsified source addresses.

During an IP spoofing attack, an attacker outside the network pretends to be a trusted computer. The attacker may either use an IP address that is within the range of IP addresses for the network or use an authorized external IP address that is trusted and provides access to specified resources on the network.

Normally, an IP spoofing attack is limited to the injection of data or commands into an existing stream of data passed between a client and server application or a peer-to-peer network connection. The attacker simply does not worry about receiving any response from the applications.

To enable bidirectional communication, the attacker must change all routing tables to point to the spoofed IP address. Another approach the attacker could take is to simply not worry about receiving any response from the applications.

If attackers manage to change the routing tables, they can receive all the network packets that are addressed to the spoofed address, and reply just as any trusted user can. Like packet sniffers, IP spoofing is not restricted to people who are external to the network.

Some tools used to perform IP spoofing attacks are as follows:

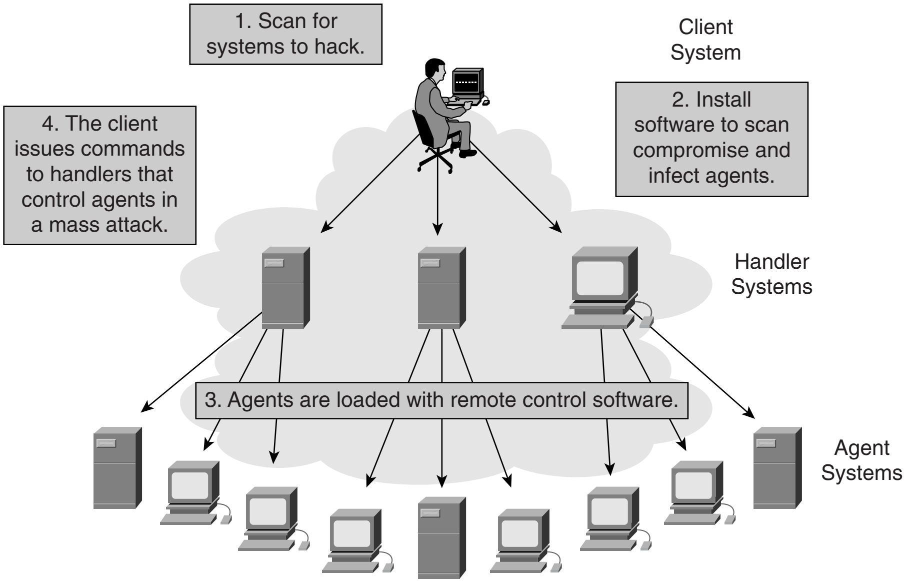
- Protocol analyzers, also called password sniffers
- Sequence number modification
- Scanning tools that probe TCP ports for specific services, network or system architecture, and the operating system

After obtaining information through scanning tools, the intruder looks for vulnerabilities associated with those entities.

Distributed Denial-of-Service Attacks

Distributed denial-of-service attacks (DDoS) attacks are designed to saturate network links with spurious data. This data can overwhelm an Internet link, causing legitimate traffic to be dropped. DDoS uses attack methods similar to standard DoS attacks but operates on a much larger scale. Typically hundreds or thousands of attack points attempt to overwhelm a target, as shown in Figure 1-23.

Figure 1-23 DDos Attack


1. Scan for systems to hack.
Client System
2. Install software to scan compromise and infect agents.
4. The client issues commands to handlers that control agents in a mass attack.
Handler Systems
3. Agents are loaded with remote control software.
Agent Systems

Examples of DDoS attacks include the following:

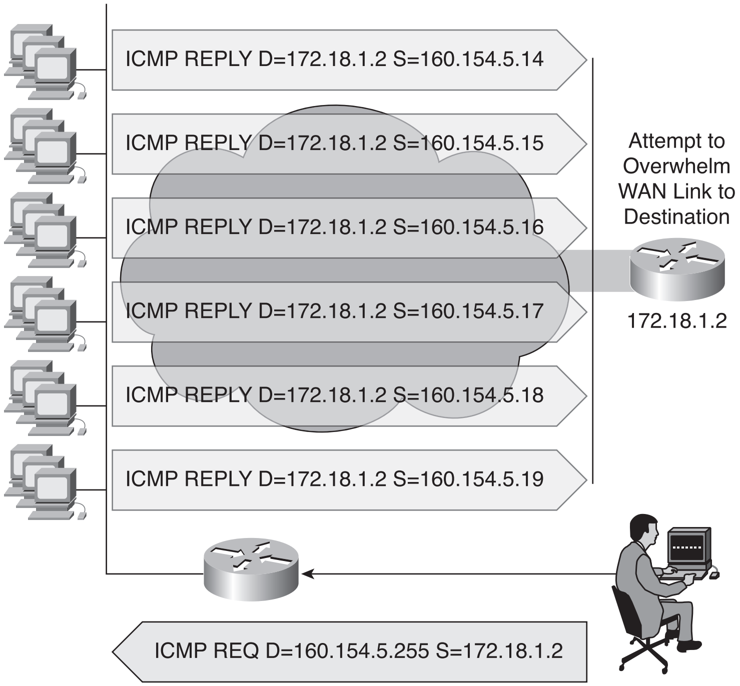
- Smurf
- Tribe Flood Network (TFN)
- Stacheldraht

The sections that follow describe each of these DDoS attacks in more detail.

Smurf Attacks

The Smurf attack starts with a perpetrator sending a large number of spoofed ICMP echo, or ping, requests to broadcast addresses, hoping that these packets will be magnified and sent to the spoofed addresses, as shown in Figure 1-24. If the routing device delivering traffic to those broadcast addresses performs the Layer 3 broadcast-to-Layer 2 broadcast function, most hosts on that IP network will each reply to the ICMP echo request with an ICMP echo reply, multiplying the traffic by the number of hosts responding. On a multi-access broadcast network, there could potentially be hundreds of machines replying to each echo packet.

Figure 1-24 Smurf Attack


ICMP REPLY D=172.18.1.2 S=160.154.5.14
ICMP REPLY D=172.18.1.2 S=160.154.5.15
ICMP REPLY D=172.18.1.2 S=160.154.5.16
ICMP REPLY D=172.18.1.2 S=160.154.5.17
ICMP REPLY D=172.18.1.2 S=160.154.5.18
ICMP REPLY D=172.18.1.2 S=160.154.5.19
Attempt to Overwhelm WAN Link to Destination
172.18.1.2
ICMP REQ D=160.154.5.255 S=172.18.1.2

Assume the network has 100 hosts and that the attacker has a T1 link. The attacker sends a 768-kbps stream of ICMP echo, or ping packets, with a spoofed source address of the victim, to the broadcast address of the “bounce site.” These ping packets hit the bounce site broadcast network of 100 hosts, and each takes the packet and responds to it, creating 100 outbound ping replies. A total of 76.8 Mbps of bandwidth is used outbound from the bounce site after the traffic is multiplied. This is then sent to the victim, or the spoofed source of the originating packets.

Turning off directed broadcast capability in the network infrastructure prevents the network from being used as a bounce site.

Tribe Flood Network (TFN)

Tribe Flood Network (TFN) and Tribe Flood Network 2000 (TFN2K) are distributed tools used to launch coordinated DoS attacks from many sources against one or more targets. A TFN attack can generate packets with spoofed source IP addresses. An intruder instructing a master to send attack instructions to a list of TFN servers or daemons carries out a DoS attack using a TFN network. The daemons then generate the specified type of DoS attack against one or more target IP addresses. Source IP addresses and source ports can be randomized, and packet sizes can be altered. Use of the TFN master requires an intruder-supplied list of IP addresses for the daemons.

Stacheldraht Attack

Stacheldraht, German for "barbed wire," combines features of several DoS attacks, including TFN. It also adds features such as encryption of communication between the attacker and Stacheldraht masters and automated update of the agents. There is an initial mass-intrusion phase, in which automated tools are used to remotely root-compromise large numbers of systems to be used in the attack. This is followed by a DoS attack phase, in which these compromised systems are used to attack one or more sites. Figure 1-25 illustrates a Stacheldraht attack.

Lab 1.3.4 Vulnerabilities and Exploits

In this lab, you examine the use of common network mapping tools, hacking programs, and scripts on a LAN and across a WAN. Where vulnerabilities are discovered, propose a fix or solution to the problem.

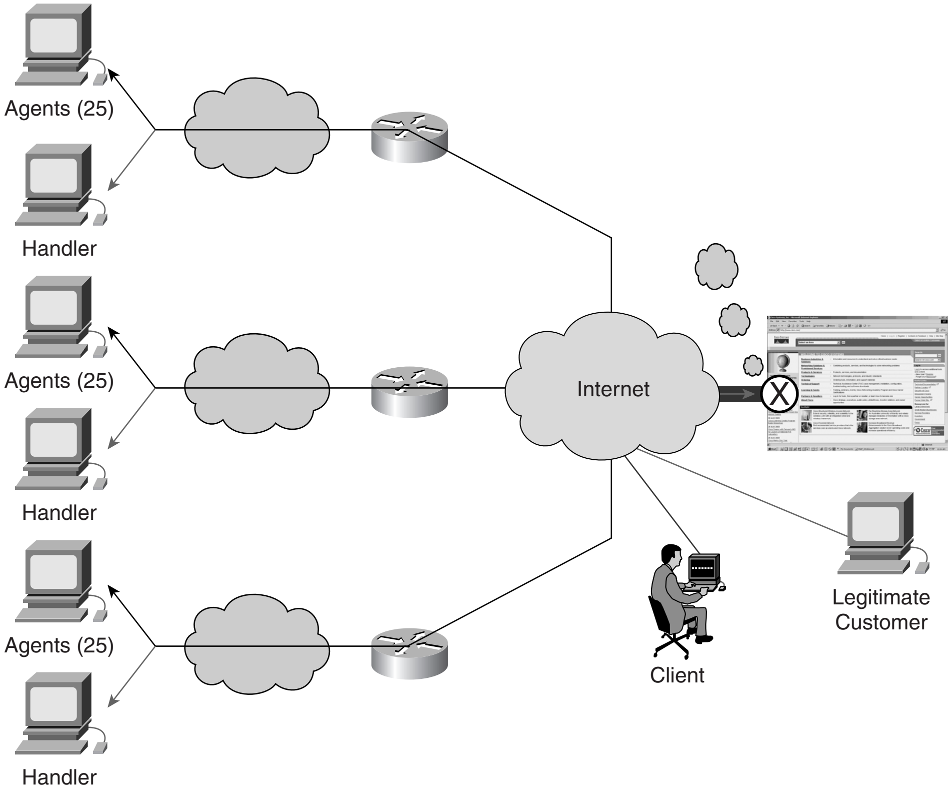
Malicious Code

The primary vulnerabilities for end-user workstations are worm, virus, and Trojan horse attacks. A worm executes arbitrary code and installs copies of itself in the infected computer's memory, which infects other hosts. A virus is malicious software that is attached to another program to execute a particular unwanted function on a user's workstation. A Trojan horse differs only in that the entire application was written to look like something else, when in fact it is an attack tool. Examples of attack types include the following:

- **Trojan horse**—An application written to look like something else that in fact is an attack tool

- **Worm**—An application that executes arbitrary code and installs copies of itself in the memory of the infected computer, which then infects other hosts
- **Virus**—Malicious software that is attached to another program to execute a particular unwanted function on the user workstation

Figure 1-25 Stacheldraht Attack



Worms

The anatomy of a worm attack is as follows:

1. **The enabling vulnerability**—A worm installs itself using an exploit vector on a vulnerable system.
2. **Propagation mechanism**—After gaining access to devices, a worm replicates and selects new targets.
3. **Payload**—After the device is infected with a worm, the attacker has access to the host—often as a privileged user. Attackers could use a local exploit to escalate their privilege level to administrator.

Typically, worms are self-contained programs that attack a system and try to exploit a specific vulnerability in the target. Upon successful exploitation of the vulnerability, the worm copies its program from the attacking host to the newly exploited system to begin the cycle again. A virus normally requires a vector to carry the virus code from one system to another. The vector can be a word processing document, an e-mail message, or an executable program. The key element that distinguishes a computer worm from a computer virus is that human interaction is required to facilitate the spread of a virus.

Worm attack mitigation, as shown in Figure 1-26, requires diligence on the part of system and network administration staff. Coordination between system administration, network engineering, and security operations personnel is critical in responding effectively to a worm incident. The following are the recommended steps for worm attack mitigation:

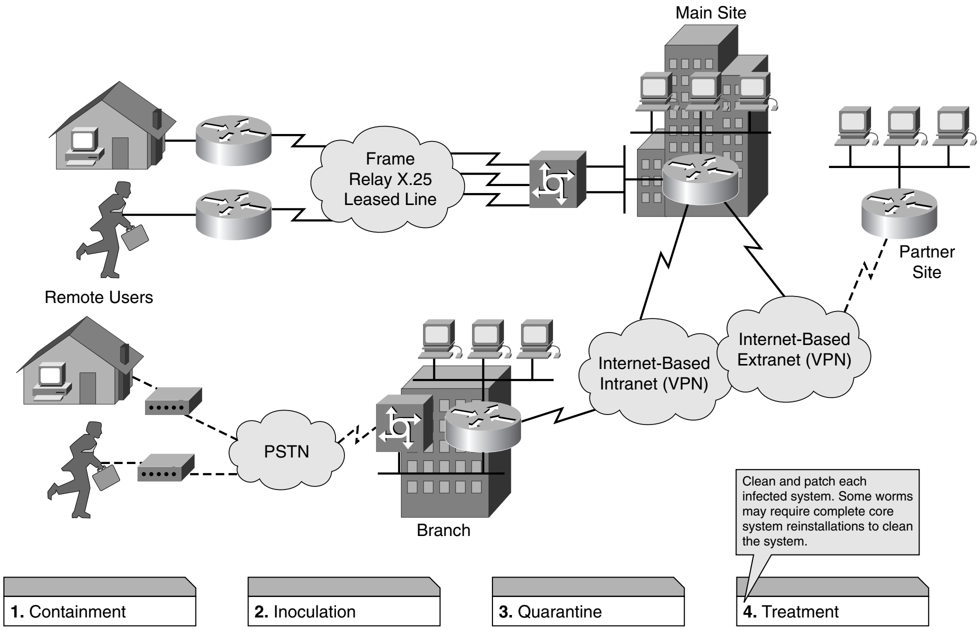
Step 1. Containment

Step 2. Inoculation

Step 3. Quarantine

Step 4. Treatment

Figure 1-26 Worm Attack Mitigation


Main Site
Frame Relay X.25 Leased Line
Partner Site
Remote Users
Internet-Based Intranet (VPN)
Internet-Based Extranet (VPN)
PSTN
Branch
Clean and patch each infected system. Some worms may require complete core system reinstallations to clean the system.
1. Containment
2. Inoculation
3. Quarantine
4. Treatment

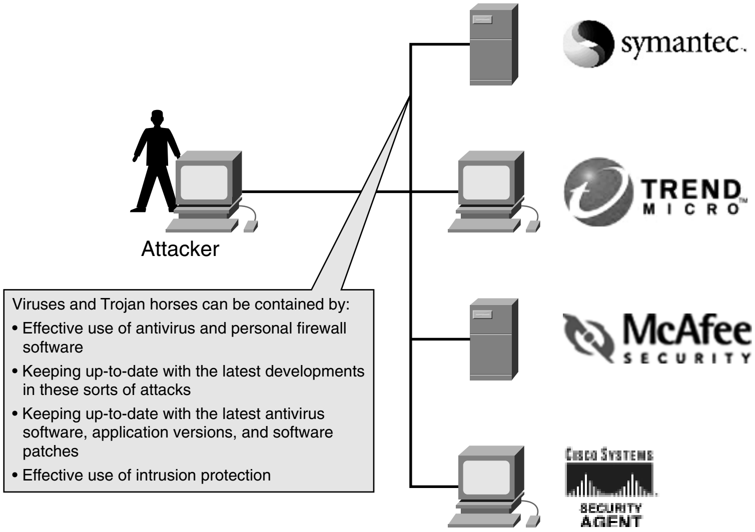
Viruses and Trojan Horses

Viruses are malicious software that is attached to another program to execute a particular unwanted function on a user's workstation. An example of a virus is a program that is attached to command.com (the primary interpreter for Windows systems) that deletes certain files and infects any other versions of command.com that it can find.

A Trojan horse differs only in that the entire application was written to look like something else, when in fact it is an attack tool. An example of a Trojan horse is a software application that runs a simple game on the user's workstation. While the user is occupied with the game, the Trojan horse mails a copy of itself to every user in the user's address book. The other users receive the game and then play it, thus spreading the Trojan horse.

These kinds of applications can be contained through the effective use of antivirus software at the user level and potentially at the network level, as depicted by Figure 1-27. Antivirus software can detect most viruses and many Trojan horse applications and prevent them from spreading in the network. Keeping current with the latest developments in these sorts of attacks can also lead to a more effective posture against these attacks. As new virus or Trojan applications are released, enterprises need to keep current with the latest antivirus software and application versions.

Figure 1-27 Virus and Trojan Horse Attack Mitigation



Viruses and Trojan horses can be contained by:

- Effective use of antivirus and personal firewall software
- Keeping up-to-date with the latest developments in these sorts of attacks
- Keeping up-to-date with the latest antivirus software, application versions, and software patches
- Effective use of intrusion protection

Vulnerability Analysis

Before adding new security solutions to an existing network, you need to identify the current state of the network and organizational practices to verify their current compliance with the requirements. This analysis also provides you with the opportunity to identify possible improvements and the potential need to redesign a part of the system or to rebuild a part of the system from scratch to satisfy the requirements. This analysis can be broken down into the following steps:

1. Policy identification
2. Network analysis
3. Host analysis

The remainder of this chapter looks at each of these steps in more depth and at some analysis tools.

Policy Identification

If a security policy exists, the designer should analyze it to identify the security requirements, which will influence the design of the perimeter solution. Initially, the designer should examine two basic areas of the policy:

- The policy should identify the assets that require protection. This helps the designer provide the correct level of protection for sensitive computing resources and to identify the flow of sensitive data in the network.
- The policy should identify possible attackers. This gives the designer insight into the level of trust assigned to internal and external users, ideally identified by more-specific categories such as business partners, customers of an organization, and outsourcing IT partners.

The designer should also be able to evaluate whether the policy was developed using correct risk-assessment procedures. For example, did the policy development include all relevant risks for the organization and not overlook important threats? The designer should also reevaluate the policy mitigation procedures to determine whether they satisfactorily mitigate expected threats. This ensures that the policy, which the designer will work with, is current and complete.

Organizations that need a high level of security assurance will require defense-in-depth mechanisms to be deployed to avoid single points of failure. The designer also needs to work with the organization to determine how much investment in security measures is acceptable for the resources that require protection.

The result of policy analysis will be as follows:

- The evaluation of policy correctness and completeness
- Identification of possible policy improvements, which need to be made before the security implementation stage

Network Analysis

Many industry best practices, tools, guides, and training are available to help secure network devices. These include tools from Cisco, such as AutoSecure and Cisco Output Interpreter, and from numerous web resources. Third-party resources include the U.S. National Security Agency (NSA) Cisco Router Security Recommendation Guides and the Center for Internet Security (CIS) Router Audit Tool (RAT) for auditing Cisco router and PIX Security Appliance configuration files.

Cisco AutoSecure

The Cisco AutoSecure feature is enabled from a Cisco IOS Security command-line interface (CLI) command, as shown in Table 1-6. AutoSecure enables rapid implementation of security policies and procedures to ensure secure networking services. It enables a "one-touch" device lockdown process, simplifying the security configuration of a router and hardening the router configuration. This feature simplifies the security process, thus lowering barriers to the deployment of critical security functionality.

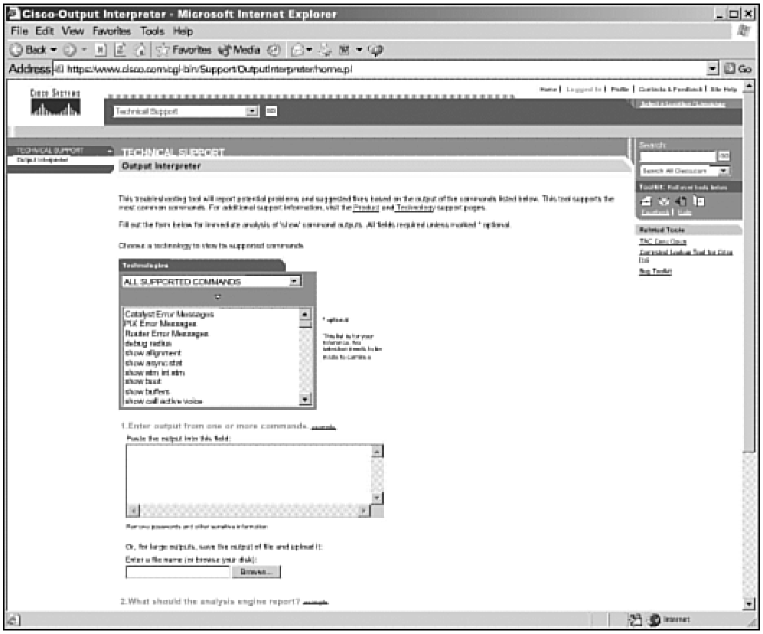
Table 1-6 AutoSecure

Command	Description
auto secure [**management** | **forwarding**] [**no-interact**]	Secures the management and forwarding planes of the router. Applying the **management** keyword dictates that only the management plane will be secured. Applying the **forwarding** keyword dictates that only the forwarding plane will be secured. The **no-interact** option dictates that the user will not be prompted for any interactive configurations.
show auto secure config	Displays all configurations commands that have been added as part of the AutoSecure configuration.

Cisco Output Interpreter

The Cisco Output Interpreter (see Figure 1-28) is a troubleshooting tool that report potential problems by analyzing supported **show** command output. The Output Interpreter is available at the Cisco website to users with a valid Cisco.com.

Figure 1-28 Output Interpreter


Cisco-Output Interpreter - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Favorites Media
Address https://www.cisco.com/cgi-bin/Support/OutputInterpreter/home.pl
Go
Cisco Systems
Technical Support
TECHNICAL SUPPORT
Search
Related Tools
Technologies
ALL SUPPORTED COMMANDS
Browse...

Output Interpreter

This troubleshooting tool will report potential problems and suggested fixes based on the output of the commands listed below. This tool supports the most common commands. For additional support information, visit the Product and Technology support pages.

Fill out the form below for immediate analysis of 'show' command outputs. All fields required unless marked * optional.

Choose a technology to view its supported commands.

Catalyst Error Messages
PIX Error Messages
Router Error Messages
debug radius
show alignment
show async stat
show atm int atm
show buat
show buffers
show call active voice

* optional

1.Enter output from one or more commands.

Paste the output into this field:

Remove passwords and other sensitive information

Or, for large outputs, save the output of file and upload it:

Enter a file name (or browse your disk):

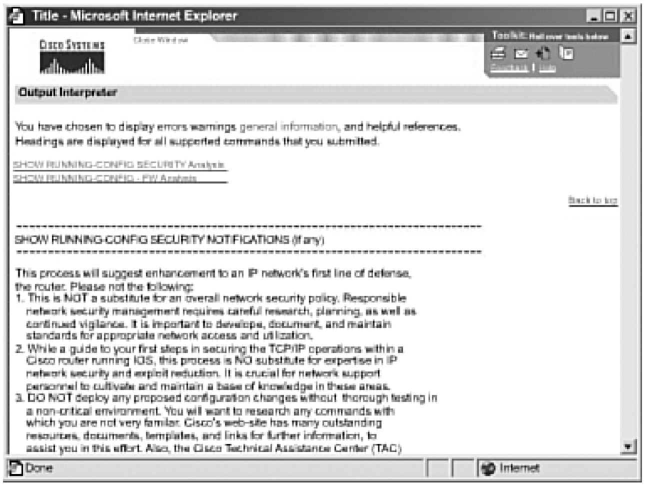
2.What should the analysis engine report?

Output Interpreter supports the following functionality:

- Displays **show** command output from a router, switch, or PIX Security Appliance. A list of supported **show** commands is available at the Output Interpreter site.
- Displays error messages generated by a router, switch, or PIX Security Appliance. The error or log messages can be copied and pasted from a router, switch, or PIX Security Appliance into the Output Interpreter.
- Decodes and analyzes a router or switch **stack trace** for any possible bugs. Copy and paste the **show version** command output followed by traceback or stack trace and alignment data.
- Can convert the **apply**, **conduit**, and **outbound** statements of a PIX Security Appliance configuration to equivalent **access-list** statements. Copy and paste **show tech-support** or **write terminal** command output of the PIX Security Appliance.
- Decodes and analyzes the Configuration Register. Copy and paste the **show version** or **show tech-support** command output into the Output Interpreter.

Figure 1-29 shows an example of the output of the Output Interpreter.

Figure 1-29 Output Interpreter Results



Output Interpreter

You have chosen to display errors warnings general information, and helpful references.
Headings are displayed for all supported commands that you submitted.

SHOW RUNNING-CONFIG SECURITY Analysis
SHOW RUNNING-CONFIG - FW Analysis

Back to top

```
--------------------------------------------------------------------------------
SHOW RUNNING-CONFIG SECURITY NOTIFICATIONS (if any)
--------------------------------------------------------------------------------

This process will suggest enhancement to an IP network's first line of defense,
the router. Please not the following:
1. This is NOT a substitute for an overall network security policy. Responsible
   network security management requires careful research, planning, as well as
   continued vigilance. It is important to develope, document, and maintain
   standards for appropriate network access and utilization.
2. While a guide to your first steps in securing the TCP/IP operations within a
   Cisco router running IOS, this process is NO substitute for expertise in IP
   network security and exploit reduction. It is crucial for network support
   personnel to cultivate and maintain a base of knowledge in these areas.
3. DO NOT deploy any proposed configuration changes without thorough testing in
   a non-critical environment. You will want to research any commands with
   which you are not very familar. Cisco's web-site has many outstanding
   resources, documents, templates, and links for further information, to
   assist you in this effort. Also, the Cisco Technical Assistance Center (TAC)
```

National Security Agency (NSA) Cisco Router Security Configuration Guides

The Router Security Configuration Guide (RSCG) contains principles and guidance for secure configuration of IP routers, with detailed instructions for Cisco Systems routers (http://www.nsa.gov/snac/routers/cisco_scg-1.1b.pdf). The RSCG was used extensively in the development of the Cisco Router Security course. This guide was developed in response to numerous questions and requests for assistance received by the NSA System and Network Attack Center (SNAC). The topics covered in the guide were selected on the basis of customer interest, community consensus, and the SNAC's background in securing networks. The RSCG is a large, detailed, yet readable and accessible document. It is supplemented with an Executive Summary Card, a quick checklist for securing your Cisco router.

Routers direct and control much of the data flowing across computer networks. The RSCG provides technical guidance intended to help network administrators and security officers improve the security of their networks. Using the information presented here, you can configure your routers to control access, resist attacks, shield other network components, and even protect the integrity and confidentiality of network traffic.

The goal for this guide is a simple one: improve the security provided by routers on U.S. government operational networks.

The RSCG document is only a guide to recommended security settings for IP routers, particularly routers running Cisco IOS Software Release 11 and 12. It is not meant to replace well-designed policy or sound judgment. The guide does not address site-specific configuration issues. Care must be taken when implementing the security steps specified in this guide. Ensure that all security steps and procedures chosen from this guide are thoroughly tested and reviewed prior to implementing them on an operational network.

Cisco IOS XR Software

Cisco IOS XR Software, a new member of the Cisco IOS family, is a unique self-healing and self-defending operating system designed for always-on operation while scaling system capacity up to 92 Tbps. Cisco IOS XR powers the Cisco Carrier Routing System, enabling the foundation for network and service convergence today while providing investment protection for decades to come.

Cisco Router Audit Tool (RAT)

The CIS RAT is based on the CIS Benchmark for Cisco IOS routers, a consensus-based best practice guideline for hardening Cisco routers. Version 2.2 of the RAT tool can be used to score both Cisco IOS routers and PIX Security Appliances. The RAT is available for the Windows or UNIX operating systems. Example 1-1 shows a sample RAT output display. The RAT downloads configurations of devices to be audited (optionally) and then checks them against the settings defined in the benchmark.

Example 1-1 Cisco RAT Sample Output

```
C:\CIS\RAT\bin>rat Austin1.text
Auditing Austin1.text...
Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/common.conf/
Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/cis-level-1.conf/
Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/cis-level-2.conf/
Checking: Austin1.txt
done checking Austin1.txt.
Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/common.conf/
Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/cis-level-1.conf/
Parsing: /C:\CIS\RAT/etc/configs/cisco-ios/cis-level-2.conf/
ncat_report: writing Austin1.txt.ncat_fix.txt.
ncat_report: writing Austin1.txt.ncat_report.txt.
ncat_report: writing Austin1.html.
ncat_report: writing rules.html  (cisco-ios-benchmark.html).
ncat_report: writing all.ncat_fix.txt.
ncat_report: writing all.ncat_report.txt.
ncat_report: writing all.html.

C:\CIS\RAT\bin>
```

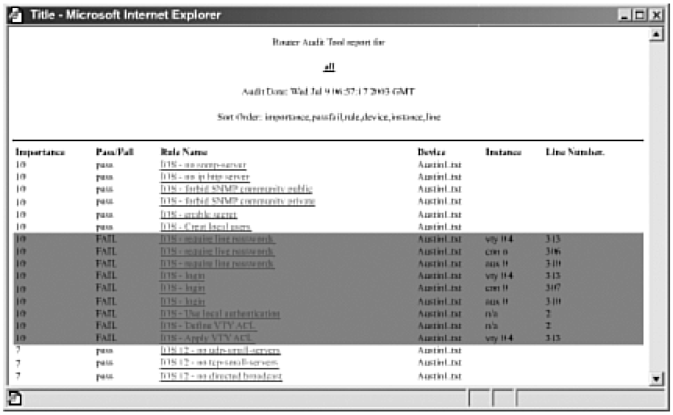
For each configuration examined, the RAT produces a report listing the following:

- A list of each rule checked with a pass/fail score
- A raw overall score

- A weighted overall score (1–10)
- A list of commands that will correct problems identified

The RAT produces a composite report listing all rules (settings) checked on all devices (and an overall score) and recommendations for improving the security of the router, as shown in Figure 1-30.

Figure 1-30 CIS RAT Report



Router Audit Tool report for

all

Audit Date: Wed Jul 9 06:57:17 2003 GMT

Sort Order: importance,pass/fail,rule,device,instance,line

Importance	Pass/Fail	Rule Name	Device	Instance	Line Number
10	pass	IOS - no snmp-server	Austin1.txt		
10	pass	IOS - no ip http server	Austin1.txt		
10	pass	IOS - forbid SNMP community public	Austin1.txt		
10	pass	IOS - forbid SNMP community private	Austin1.txt		
10	pass	IOS - enable secret	Austin1.txt		
10	pass	IOS - Creat local users	Austin1.txt		
10	FAIL	IOS - require line passwords	Austin1.txt	vty 0 4	313
10	FAIL	IOS - require line passwords	Austin1.txt	con 0	306
10	FAIL	IOS - require line passwords	Austin1.txt	aux 0	310
10	FAIL	IOS - login	Austin1.txt	vty 0 4	313
10	FAIL	IOS - login	Austin1.txt	con 0	307
10	FAIL	IOS - login	Austin1.txt	aux 0	310
10	FAIL	IOS - Use local authentication	Austin1.txt	n/a	2
10	FAIL	IOS - Define VTY ACL	Austin1.txt	n/a	2
10	FAIL	IOS - Apply VTY ACL	Austin1.txt	vty 0 4	313
7	pass	IOS 12 - no udp-small-servers	Austin1.txt		
7	pass	IOS 12 - no tcp-small-servers	Austin1.txt		
7	pass	IOS 12 - no directed broadcast	Austin1.txt		

Host Analysis

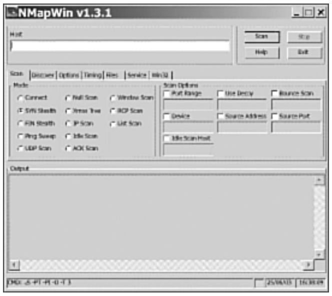
The hosts that are on the network need to be considered when designing a network security solution. Determining the role in the network of each host will help to decide the steps that will be taken to secure it. The network could have many user workstations, and multiple servers that need to be accessed from both inside and outside of the network.

The types of applications and services that are running on the hosts need to be identified, and any network services and ports that are not necessary should be disabled or blocked. All operating systems should be patched as needed. Antivirus software should be installed and kept current. Some servers may be assigned static routable IP addresses to be accessible from the Internet. These hosts in particular should be monitored for signs of malicious activity.

Many tools are available to test host security. Most tools have been developed on a UNIX or Linux platform, and some of them have now been ported to other operating systems. Two of the most common tools are as follows:

- **Network Mapper (Nmap)**—Nmap is a popular free tool used for security scanning and auditing. It can rapidly perform a port scan of a single host or a range of hosts. Nmap was originally written to be run on UNIX systems, and it is now available for use on Microsoft Windows platforms, as shown in Figure 1-31.
- **Nessus**—Nessus is a vulnerability scanner that is available for UNIX and Microsoft Windows platforms. New vulnerability testing capabilities can be added to Nessus through the installation of modular plug-ins. Nessus includes a built-in port scanner, or it can be used along with Nmap. When the Nessus scan is finished, a report is created. This report displays the results of the scan and provides steps to mitigate vulnerabilities.

Figure 1-31 NMAP for Windows



Analysis Tools

Many tools are available to help to determine vulnerabilities in endpoint devices, such as network hosts and servers. You can obtain these tools from either the company that creates the operating system or a third party. In many cases, these tools are free. The sections that follow describe some of the most commonly used analysis tools.

Knoppix STD

Knoppix Security Tools Distribution (STD) is a Linux LiveCD distribution that contains many valuable security tools. The LiveCD is a bootable CD-ROM that contains the Linux operating system, along with software applications, that can be run from memory without installation on the hard drive. After the LiveCD is ejected from the CD-ROM drive, the system can be rebooted to return to the original operating system. Knoppix STD contains many useful features, such as the following:

- Encryption tools
- Forensics tools
- Firewall tools
- Intrusion detection tools
- Network utilities
- Password tools
- Packet sniffers
- Vulnerability assessment tools
- Wireless tools

Many additional versions of LiveCD are available. If one distribution does not support a particular system or piece of hardware, it might be necessary to try another distribution. Most LiveCD releases are available as free downloads that the end user can burn to a CD.

Microsoft Baseline Security Analyzer

You can use the Microsoft Baseline Security Analyzer (MBSA) to scan hosts running Windows 2000, Windows XP, and Windows Server 2003 operating systems to determine potential security risks. MBSA scans for common system misconfigurations and missing security updates. MBSA includes both a graphical interface and a CLI that can perform local or remote scans. After a system scan, the MBSA provides a report outlining potential vulnerabilities and the steps required to correct them. This tool is available as a free download from Microsoft.

Summary

This module introduced the needs, trends, and goals of network security. The exponential growth of networking has led to increased security risks. Many of these risks are due to hacking, device vulnerabilities, and improper uses of network resources. Awareness of the various weaknesses and vulnerabilities is critical to the success of modern networks. Security professionals who can deploy secure networks are in high demand.

The four primary threats to network security include unstructured threats, structured threats, external threats, and internal threats. To defend against threats, an understanding of the common methods of attack must be established, including reconnaissance, access, DoS, and malicious code.

Responses to security issues range from ignoring the problem to excessive spending on security devices and solutions. Neither approach will succeed without a good, sound policy, and highly skilled security professionals.

Check Your Understanding

Complete all the review questions listed here to test your understanding of the topics and concepts in this chapter. Answers are listed in Appendix A, "Check Your Understanding Answer Key."

1. Which of the following is not a primary network security goal?

   a. Assure the availability of corporate data

   b. Maintain integrity of corporate data

   c. Protect against denial-of-service attacks

   d. Protect the confidentiality of corporate data

2. What is the method of mapping a network called?

   a. Eavesdropping

   b. Reconnaissance

   c. Sniffing

   d. Discovery

3. Which security model would describe a CISCO PIX Appliance with a basic configuration without access control lists or conduits?

   a. Open access

   b. Hybrid access

   c. Closed access

   d. Restrictive access

4. What is a low-technology method of acquiring information for future network attacks?

   a. Man-in-the-middle

   b. Social engineering

   c. Back doors

   d. Masquerade

   e. Graffiti

5. Which will introduce an inconspicuous back door into a host?

   a. Trojan horse

   b. TCP session hijacker

   c. LophtCrack

   d. Packet sniffer

6. Which of the following would not be considered an attack?

a. Trust exploitation

b. Man-in-the-middle

c. Access control

d. Port redirection

7. What is data manipulation an attack on?

a. Confidentiality

b. Integrity

c. Authentication

d. Access

8. What would not be considered part of the security policy?

a. Remote access

b. Access control

c. Employee comfort

d. Password length

9. Which of the following is not likely to cause a denial-of-service attack?

a. SYN flood

b. Power outage

c. Buffer overflow

d. Access violation

10. A protocol analyzer can be used to do which of the following?

a. Determine the contents of a packet

b. Analyze the inside of a switch

c. Determine the layers of the OSI model

d. Rearrange the sequence numbers