4

CHAPTER FOUR

General Network Security

Objectives

This chapter covers the following Cisco-specific objectives for the “Identify security threats to a network and describe general methods to mitigate those threats” section of both the 640-802 CCNA and 640-822 ICND1 exams:

- **Describe today’s increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats**
- **Explain general methods to mitigate common security threats to network devices, hosts, and applications**
- **Describe the functions of common security appliances and applications**
- **Describe security recommended practices including initial steps to secure network devices**

Outline

Study Strategies

- Read the information presented in this chapter, paying special attention to tables, Notes, and Exam Alerts.
- Read the objectives at the beginning of the chapter.
- Review each class of attack.
- Name the specific attacks that comprise each class.
- Describe security threat mitigation techniques.
- Familiarize yourself with the Cisco devices that assist with general network security.
- Complete the Challenges and the Exercises at the end of the chapter.

Introduction

Information technology has evolved and provides countless resources for everyday people to create, maintain, and utilize data. If you have ever seen or read *Spiderman*, you have likely heard the quote "With great power comes great responsibility." Information is power, so it is vitally important to implement safeguards on your LAN and WAN to protect data from hackers. Everyone with a computer is susceptible and should be cautious with important private details such as credit card information. I have worked in the networking department at several types of companies, including a health-care company. Imagine if a hacker were to obtain patient medical records or a list of social security numbers from the human resources database. A company must follow special guidelines to ensure data privacy, which ties directly to network security. To make sure that companies adhere to security guidelines, annual audits are performed on their networks to identify potential weaknesses.

Even though network security has been a hot topic since the advent of computer networking, it is a new set of objectives on the CCENT and CCNA exams. To prepare yourself for the exams, you must know what classes of attack are common today, how to mitigate those attacks, and what features or hardware Cisco offers to assist in protecting your network. This chapter begins with a discussion of prevalent classes of attack.

Classes of Attack

Objective:

- Describe today's increasing network security threats and explain the need to implement a comprehensive security policy to mitigate the threats

Any number of motives could inspire an attacker; two motives that we touched on already are financial gain and gathering intelligence. A hacker may also simply enjoy the thrill of successfully breaking into someone's network. There are documented cases of hackers who intentionally attacked government systems simply to prove that it could be done and therefore gain notoriety.

This section discusses three classes of attack that are commonly found in today's network environment:

- Access attacks
- Reconnaissance attacks
- Denial of service (DoS) attacks

Each class has various more-specific subcategories of attack methods that will be covered in greater detail.

TIP

The three common classes of attack are access, reconnaissance, and DoS.

Access Attacks

An access attack is just what it sounds like: an attempt to access another user account or network device through improper means. If proper security measures are not in place, the network may be left vulnerable to intrusion. A network administrator is responsible for ensuring that only authorized users access the network. Unauthorized attacks are attempted via four means, all of which try to bypass some facet of the authentication process: password attacks, trust exploitation, port redirection, and man-in-the-middle attacks.

TIP

The four types of access attacks are password attacks, trust exploitation, port redirection, and man-in-the-middle attacks.

Password Attacks

Nowadays, it seems as if you need a password for everything. I have so many passwords that I find it hard to keep track. Although it might sound like a good idea to keep your passwords simple or to write them down, both practices are highly discouraged. The goal is to make it harder for someone to find or guess your password; therefore, password integrity is necessary. That being said, an attacker might attempt a login with false credentials. It is also important to note that not all attackers are external users. Many recorded instances of attempted and/or successful attacks have come from internal company employees.

There are alternatives to passwords, such as Terminal Access Controller Access Control System (TACACS) or Remote Authentication Dial-In User Service (RADIUS), both of which manage access to network hardware. Passwords are fast becoming as obsolete as rabbit-ear antennas or dialup Internet connections.

Cisco equipment is shipped from the factory with a standard configuration. When the device is turned on, the setup program prompts for a password and leaves all but the enable secret password in plain text. It is the responsibility of the recipient to update the password information before deploying the device on a network. Changing passwords every time an employee leaves the company or in a given time period (every 90 days) would also help protect login credentials.

Trust Exploitation

Trust exploitation can occur in one of two ways:

- Reliance on the trust a client has in a server
- Reliance on the trust the server has in the client

For example, most companies have a part of their network that lies between the wide-open Internet and the corporate internal network. This in-between part of the network is called the demilitarized zone (DMZ). Servers that communicate from the DMZ and the internal network may have a trust relationship established. The internal devices may be set up to trust information that is received from a DMZ server. An attacker can then compromise the DMZ server and initiate a connection to the internal network. This is an example of phishing. When the trust that the server has in a client is exploited, this is an example of session hijacking.

Port Redirection

Port redirection is a form of trust exploitation in which the untrustworthy source uses a machine with access to the internal network to pass traffic through a port on the firewall or access control list (ACL). The port in question normally denies traffic, but with redirection the attacker can bypass security measures and open a tunnel for communication.

Man-in-the-Middle Attacks

A man-in-the-middle attack happens when a hacker eavesdrops or listens for network traffic and intercepts a data transmission. After the transmission is intercepted, the untrustworthy host can position itself between the two communicating hosts, interpret the data, and steal information from the packets sent. The hacker can also take over the session and reformat the packets to send information to either or both communicating parties. In this situation, it is possible for the hacker to capture credentials, hijack a session, or instigate a DoS attack.

Data sessions are more vulnerable when the packets are left in clear-text format and can be read without additional decryption by the human eye. Proper data encryption, with the use of an encryption protocol, makes the captured data useless.

Challenge

In this challenge, write down the four types of access attacks.

1.
2.
3.
4.

Reconnaissance Attacks

When I hear the word reconnaissance, I think of a military reconnaissance mission. The soldier is sent out to gather important information about an area of interest. The same holds true for a reconnaissance attack on a computer network. The hacker surveys a network and collects data for a future attack. Important information that can be compiled during a reconnaissance attack includes the following:

- Ports open on a server
- Ports open on a firewall
- IP addresses on the host network
- Hostnames associated with the IP addresses

As with access attacks, there are four main subcategories or methods for gathering network data:

- Packet sniffers (also known as network monitors)
- Ping sweeps
- Port scans
- Information queries

TIP

The four common tools used for reconnaissance attacks are packet sniffers, ping sweeps, port scans, and information queries.

Packet Sniffers

A packet sniffer may also be called a network analyzer, packet analyzer, or Ethernet sniffer. The packet sniffer may be either a software program or a piece of hardware with software installed in it that captures traffic sent over the network, which is then decoded and analyzed by the sniffer. Network administrators install monitors on dedicated machines or on their workstations when needed. A common software program available today is Wireshark, formerly known as Ethereal.

Ping Sweeps

As you may recall, ping enables you to validate that an IP address exists and can accept requests by sending an echo request and then waiting for an echo reply. A ping sweep tool can send an echo request to numerous host IP addresses at the same time to see which host(s) respond(s) with an echo reply.

NOTE

Refer to Chapter 1, “Standard Internetworking Models,” for a review of ping, which uses ICMP.

Port Scans

A port scanner is a software program that surveys a host network for open ports. Because ports are associated with applications, the hacker can use the port and application information to determine a way to attack the network. As mentioned, these programs can be used by a third party to audit a network as well as being used by a hacker for malicious intent.

As mentioned in Chapter 1, it is extremely important that you know the prevalent applications and their matching port numbers. Table 4.1 reviews the applications that use TCP, and Table 4.2 reviews UDP-based applications.

TABLE 4.1 Applications Using TCP

Application	Port Number(s)
FTP	20, 21
Telnet	23
SMTP	25
DNS (zone transfers)	53
HTTP	80
POP3	110
NNTP	119
HTTPS	443

TABLE 4.2 Applications Using UDP

Application	Port Number(s)
DHCP	67, 68
DNS (name resolution)	53
TFTP	69
NTP	123
SNMP	161

Information Queries

Information queries can be sent via the Internet to resolve hostnames from IP addresses or vice versa. One of the most commonly used queries is nslookup. You can use nslookup by opening a Windows or Linux command prompt (CMD) window on your computer and entering `nslookup` followed by the IP address or hostname that you are attempting to resolve.

Here are a couple sample CMD commands:

```
C: nslookup www.cisco.com
C: nslookup 198.133.219.25
```

A multitude of websites offer an nslookup tool.

Challenge

In this challenge, write down the four common tools we discussed for gathering information for a reconnaissance attack.

1.

2.

3.

4.

Denial of Service (DoS) Attacks

DoS attacks are often implemented by a hacker as a means of denying a service that is normally available to a user or organization. For example, users might be denied access to email as the result of a successful DoS attack. IP spoofing can be used as part of a DoS attack or man-in-the-middle attack and occurs when a valid host IP address is assumed by an attacking system. This provides a way to bypass the trust a machine has in another machine.

Although it has long since been patched, a DoS attack called the ping of death occurred when an ICMP echo request packet larger than 65,535 bytes was sent to a target destination, causing it to overflow, crash, and/or reboot. A current example of a DoS attack is a teardrop, which can cause a system to crash by running the CPU up to 100%. Teardrop sends in thousands of tiny fragments with overlapping offsets.

DoS can also be in the form of a distributed DoS (DDoS) attack, TCP SYN attack, or smurf attack.

Distributed DoS (DDoS)

With distributed DoS, multiple systems are compromised to send a DoS attack to a specific target. The compromised systems are commonly called zombies or slaves. As a result of the attack, the targeted system denies service to valid users. Figure 4.1 illustrates a DDoS attack.

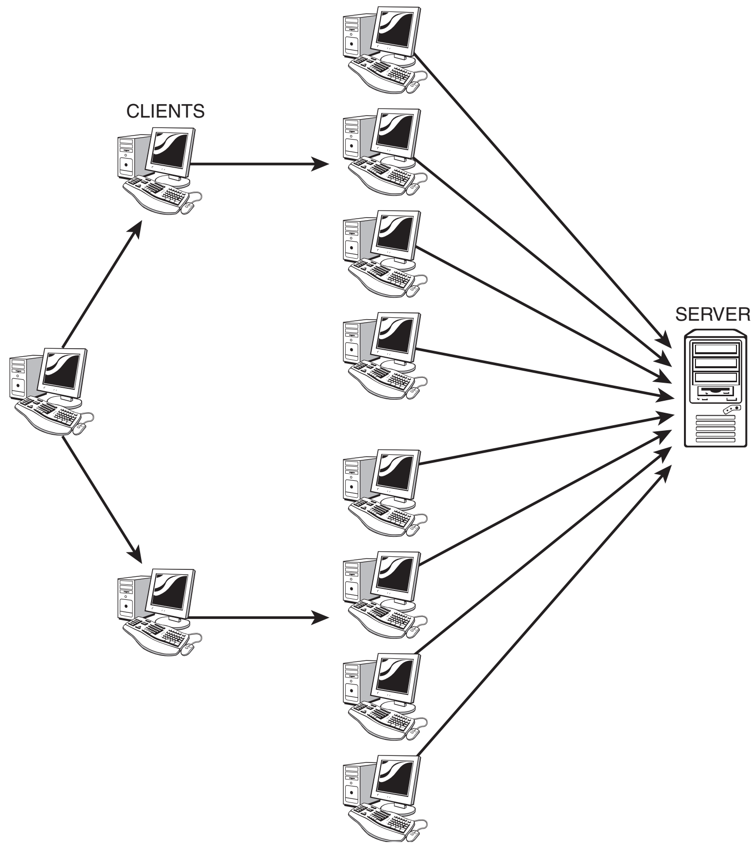

FIGURE 4.1 DDoS attack.

TCP SYN

You may recall from Chapter 1 that a TCP session is established with the use of a three-way handshake, which involves the following steps:

1. A "connection agreement" segment is sent to the recipient, asking to synchronize systems. This step is associated with the bit name SYN.
2. The second and third segments acknowledge the request to connect and determine the rules of engagement. Sequencing synchronization is requested of the receiving device. A two-way connection is established. This step is associated with the bit name SYN-ACK.
3. A final segment is sent as an acknowledgment that the rules have been accepted and a connection has been formed. This step is associated with the bit name ACK.

Figure 4.2 illustrates a proper TCP session.

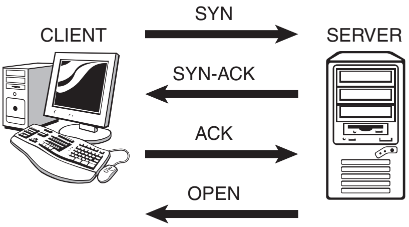

FIGURE 4.2 TCP session establishment.

In a TCP SYN attack, a SYN request is sent to a device with a spoofed source IP address. The attacking system does not acknowledge the resulting SYN-ACK, which causes the session connection queues to fill up and stop taking new connection requests. TCP intercept can be configured on a router to block a TCP SYN attack. This enables the router to terminate any sessions that have not been established within an allotted time frame.

Smurf Attack

With a smurf attack, multiple broadcast ping requests are sent to a single target from a spoofed IP address. Figure 4.3 illustrates a smurf attack. Adding the `no ip directed-broadcast` command to a router might help mitigate a potential smurf attack.

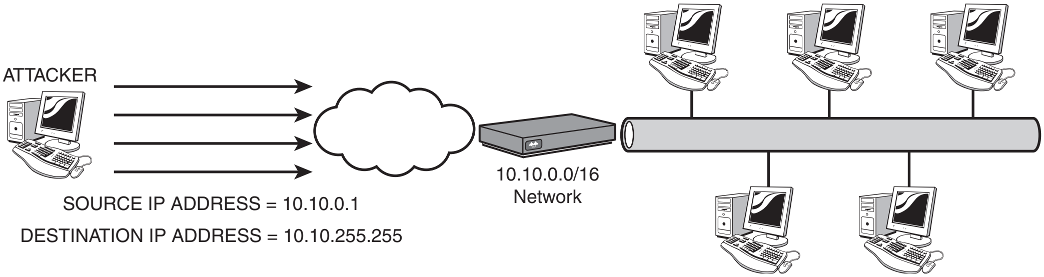
ATTACKER
SOURCE IP ADDRESS = 10.10.0.1
DESTINATION IP ADDRESS = 10.10.255.255
10.10.0.0/16
Network

FIGURE 4.3 Smurf attack.

Challenge

In this challenge, write down the three DoS attacks that we reviewed in this chapter.

1.
2.
3.

Mitigating Network Threats

Objectives:

- Explain general methods to mitigate common security threats to network devices, hosts, and applications
- Describe the functions of common security appliances and applications
- Describe security recommended practices including initial steps to secure network devices

By definition, to mitigate is to lessen in force or intensity. Now that you are familiar with the various classes of attack, let's discuss what actions you can take to lessen the impact of an attack on a network. Keep in mind that we already went over some common mitigation techniques, such as password integrity, password encryption, TCP intercept, and `no ip directed-broadcast`. We will continue this chapter with a general overview of additional recommended practices and security measures. Our discussion includes the following mitigation techniques:

- Authentication, Authorization, and Accounting (AAA)
- Cisco access control lists (ACLs)
- Cisco Internetwork Operating System (IOS) secure management features
- Encryption protocols
- Security appliances and applications

AAA

Commonly called "triple A," AAA is a group of three services that are used to increase network security:

- **Authentication:** Identifies a user by login and password.
- **Authorization:** Determines what a user is allowed to do.
- **Accounting:** Assembles and sends usage information (such as logging).

AAA works in conjunction with TACACS or RADIUS to provide a secure network connection with a record of user activities.

Cisco ACLs

An access list is an ordered list of `permit` and `deny` statements that can be applied on a Cisco device to effectively determine whether a packet will be permitted or denied access to the network. A properly configured access list can help block most of the attack methods described in this chapter:

- IP spoofing
- TCP SYN attacks
- Smurf attacks
- ICMP and traceroute

Cisco IOS Secure Management Features

I mentioned earlier that it is the responsibility of the network administrator to configure Cisco equipment with a new password before deployment. You can take this a step further by performing some initial steps to secure Cisco equipment within the IOS. Configuring the following features on your Cisco device helps create a secure network environment:

- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- Syslog
- Network Time Protocol (NTP)

SSH

SSH is a data transmission protocol that uses strong authentication and an encrypted tunnel to ensure secure communications between an SSH client and the SSH server. SSH uses TCP port number 22 for connectivity.

SNMP

SNMP is a management protocol that monitors the network and manages configurations by collecting statistics to analyze network performance and ensure network security. It is best to use SNMP version 3, which provides cryptographic authentication and management traffic encryption. SNMP uses UDP port number 161 for connectivity.

Syslog

With syslog, log messages are collected from the Cisco device and are sent to a syslog server to keep record of any network occurrences. For syslog to work properly, NTP must be configured. Each logged message has an associated severity level. Syslog uses UDP port number 514 for connectivity. Table 4.3 lists the severity levels in order, with 0 representing the most critical message.

TABLE 4.3 Syslog Severity Levels

Security Level	Description
0	Emergency
1	Alert
2	Critical
3	Error
4	Warning
5	Notification
6	Informational
7	Debugging

NTP

NTP is a protocol that synchronizes clocks on the local network to provide accurate local time on the user system. As with SNMP version 3, NTP version 3 is preferred because of the ability to provide cryptographic authentication and management traffic encryption. NTP uses UDP port number 123 for connectivity.

Encryption Protocols

Unencrypted data can be easily read by internal or external threats to a network. This is the case when data is left in clear-text format. To help prevent an attack, it is important to encrypt or encode data. Here are three key encryption protocols:

- **SSH:** A data transmission protocol that uses strong authentication and an encrypted tunnel to ensure secure communications between an SSH client and the SSH server.
- **Internet Protocol Security (IPsec):** Consists of a set of protocols that were developed to secure the transfer of packets above the Network layer (Layer 3) of the OSI model.
- **Secure Socket Layer (SSL):** A protocol that provides a secure channel between two devices at the Application layer (Layer 7) of the OSI model. Asymmetric encryption and certificates are used to exchange a session key. Data is encrypted using that key and a block cipher. HTTPS is an example of an SSL secure transaction.

Security Appliances and Applications

The following are security devices used to mitigate security vulnerabilities:

- **Firewall:** A firewall can be either software or hardware that is installed to separate a trusted network from a less-trusted network, such as the Internet.
- **Intrusion Prevention System (IPS):** IPS is an active device that is inline with the traffic path on a network. An IPS listens promiscuously to all incoming traffic to

identify attacks. It works with the firewall to modify rule templates to block traffic from the attacker address(es) while the attack is still in progress.

- **Intrusion Detection System (IDS):** IDS is a passive device that may not be inline with the traffic path on a network. An IDS also listens promiscuously to all incoming traffic to record and generate alerts and issue TCP resets if necessary.

REVIEW BREAK

Because so many possible mitigation techniques exist, let's go over them all in a quick review. Table 4.4 lists and describes each method.

TABLE 4.4 Security Mitigation Techniques

Mitigation Method	Description
AAA	A group of three services (authentication, authorization, and accounting) that are used in conjunction with TACACS or RADIUS to provide a secure network connection with a record of user activities.
Cisco ACL	An ordered list of `permit` and `deny` statements that can be applied on a Cisco device to effectively determine whether a packet will be permitted or denied access to the network.
SSH	A data transmission protocol that uses strong authentication and an encrypted tunnel to ensure secure communications between an SSH client and the SSH server. SSH protects otherwise-vulnerable services such as Telnet, news, and mail.
SNMP	A management protocol that monitors the network and manages configurations by collecting statistics to analyze network performance and ensure network security.
Syslog	Log messages are collected from the Cisco device and are sent to a syslog server to keep records of any network occurrences.
NTP	A protocol that synchronizes clocks on the local network to provide accurate local time on the user system.
IPsec	A set of protocols that were developed to secure the transfer of packets at the Network layer (Layer 3) of the OSI model.
SSL	A protocol that provides a secure channel between two devices at the Application layer (Layer 7) of the OSI model.
Firewall	Either software or hardware that is installed to protect a network from outside networks, such as the Internet.
IPS	An active device that is inline with the traffic path on a network. An IPS listens promiscuously to all incoming traffic to identify attacks, which the system can then block.
IDS	A passive device that may not be inline with the traffic path on a network. An IDS also listens promiscuously to all incoming traffic to generate alerts and issue TCP resets if necessary.

Chapter Summary

After reading through this chapter, you should have a general understanding of the types of security threats that are prevalent in our high-tech, information-driven society and various ways to mitigate those threats. A responsible network administrator must be aware of these possible attacks to protect the network from any form of security breach. Cisco offers built-in security management features that can be configured before the equipment is installed on the local network. It is also possible to purchase additional hardware and software to enhance overall security. The Cisco catalog includes IOS versions of firewall, IPS, IPsec VPN, and SSL VPN. You also have a variety of network security appliances to choose from, depending on the size and needs of your particular company.

Key Terms

- Access attack
- Reconnaissance attack
- Denial of service (DoS) attack
- Password attack
- Trust exploitation
- Port redirection
- Man-in-the-middle attack
- Packet sniffer
- Port scan
- Ping sweep
- Information query
- IP spoofing
- Ping of death
- Teardrop attack
- Distributed DoS attack
- TCP SYN attack
- Smurf attack
- Authentication, Authorization, and Accounting (AAA)
- Access control list (ACL)

- Secure Shell (SSH)
- Simple Network Management Protocol (SNMP)
- SYSLOG
- Network Time Protocol (NTP)
- Internet Protocol Security (IPsec)
- Secure Socket Layer (SSL)
- Firewall
- Intrusion Prevention System (IPS)
- Intrusion Detection System (IDS)

Apply Your Knowledge

Exercise

4.1 Mitigation Methods

Based on the Cisco-provided exam objectives, you may need to “explain general methods to mitigate common security threats to network devices, hosts, and applications” on the CCNA exam. In this exercise, list the eleven mitigation methods that were covered in this chapter, and write a brief description of each one. You may refer to Table 4.4 to check your answers.

Estimated Time: 20 minutes

1. ___________ ____

2. ___________ ____

3. ___________ ____

4. ___________ ____

5. ___________ ____

6. ___________ ____

7. ___________ ____

8. ___________ ____

9. __________ ____

10. __________ ____

11. __________ ____

Review Questions

1. Define trust exploitation.
2. Describe a TCP SYN attack.
3. What are the three services that make up AAA?
4. What can a Cisco ACL help mitigate?
5. List the similarities and differences between an IPS and IDS.

Exam Questions

1. What are the three common classes of attack?

   ○ **A.** Access attack

   ○ **B.** DoS attack

   ○ **C.** Smurf attack

   ○ **D.** Reconnaissance attack

2. Which of the following are types of access attacks? (Choose three)

   ○ **A.** Trust exploitation

   ○ **B.** TCP SYN attack

   ○ **C.** Port redirection

   ○ **D.** Man-in-the-middle

3. Which of the following are tools that can be used for a reconnaissance attack? (Choose three)

   ○ **A.** Port redirection

   ○ **B.** Ping sweep

   ○ **C.** Port scan

   ○ **D.** Packet sniffer

4. Which of the following are types of DoS attacks? (Choose three)

❍ **A.** Smurf attack

❍ **B.** Packet sniffer

❍ **C.** DDoS

❍ **D.** TCP SYN attack

5. What command can be configured on a Cisco device to mitigate smurf attacks?

❍ **A.** `ip tcp intercept`

❍ **B.** `ip directed-broadcast`

❍ **C.** `no ip directed-broadcast`

❍ **D.** `no ip tcp intercept`

6. When a valid host IP address is assumed by an attacking system, it is called ________________.

❍ **A.** Filtering

❍ **B.** Ping of death

❍ **C.** IP spoofing

❍ **D.** Teardrop attack

7. What do the three A's in AAA stand for?

❍ **A.** Authentication, authorization, advertising

❍ **B.** Authorization, accounting, activating

❍ **C.** Authentication, accounting, activating

❍ **D.** Authentication, authorization, accounting

8. Which protocol uses TCP port 22?

❍ **A.** SSL

❍ **B.** SSH

❍ **C.** SNMP

❍ **D.** NTP

9. Which of the following are Cisco IOS secure management features? (Choose three)

❍ **A.** Syslog

❍ **B.** SSH

❍ **C.** AAA

❍ **D.** SNMP

10. Which protocol provides a secure channel between two devices at the Application layer (Layer 7) of the OSI model?

❍ **A.** SSL

❍ **B.** IPsec

❍ **C.** SNMP

❍ **D.** NTP

Answers to Review Questions

1. Trust exploitation occurs when a device or group of devices on a shared segment erroneously trusts information that has been provided by an untrustworthy source.

2. In a TCP SYN attack, a SYN request is sent to a device with a spoofed IP address. The attacking system does not acknowledge the resulting SYN-ACK, which causes the session connection queues to fill up and stop taking new connection requests.

3. Authentication identifies a user by login and password. Authorization determines what a user is allowed to do by putting together a list of attributes. Accounting assembles and sends usage information.

4. IP spoofing
TCP SYN attacks
Smurf attacks
ICMP and traceroute

5. Both IPS and IDS listen promiscuously to all incoming traffic. IPS is an active device that is inline with the traffic path. It can identify attacks and block them in the system. IDS is a passive device that may not be inline with the path of traffic. IDS can also generate alerts and send TCP resets when necessary.

Answers to Exam Questions

1. **A, B, D.** The three common classes of attack are access attack, reconnaissance attack, and DoS attack. Answer C is not a class of attack, but rather a type of DoS attack.

2. **A, C, D.** Trust exploitation, port redirection, and man-in-the-middle are all types of access attacks. Answer B is incorrect because a TCP SYN attack is a form of DoS attack.

3. **B, C, D.** Ping sweeps, port scans, and packet sniffers are all tools that can be utilized for a reconnaissance attack. Answer A is incorrect because port redirection is a type of access attack.

4. **A, C, D.** Smurf attacks, DDoS attacks, and TCP SYN attacks are all types of DoS attacks. Answer B is incorrect because a packet sniffer is a tool used for a reconnaissance attack.

5. **C.** The `no ip directed-broadcast` command can be configured on a Cisco device to block smurf attacks. Answers A and D are incorrect because they are related to the TCP SYN attack. Answer B is incorrect because it does not contain the keyword `no`.

6. **C.** When a valid host IP address is assumed by an attacking system, it is called IP spoofing. Answer A is incorrect because filtering is used to filter traffic. Answer B is incorrect because the ping of death is when an ICMP echo request packet that is larger than 65,535 bytes is sent to a target destination, causing it to overflow, crash, and/or reboot. Answer D is incorrect because a teardrop attack happens when the Offset field of the TCP header is changed.

7. **D.** AAA stands for authentication, authorization, and accounting. Answer A is incorrect because advertising is not a service of AAA. Answers B and C are incorrect because activating is not a service of AAA.

8. **B.** SSH uses TCP port 22. Answer A is incorrect because SSL uses TCP port 443. Answer C is incorrect because SNMP uses UDP port 161. Answer D is incorrect because NTP uses UDP port 123.

9. **A, B, D.** Syslog, SSH, and SNMP are all Cisco IOS secure management features. Answer C is incorrect because AAA consists of a group of three services that are used in conjunction with an authentication server and a software service such as TACACS or RADIUS to provide a secure network connection with a record of user activities.

10. **A.** SSL is a protocol that provides a secure channel between two devices at the Application layer (Layer 7) of the OSI model. Answer B is incorrect because IPsec functions at Layer 3 of the OSI model. Answer C is incorrect because SNMP is a management protocol that monitors the network and manages configurations. Answer D is incorrect because NTP is a protocol that synchronizes clocks on the local network to provide accurate local time on the user system.

Suggested Readings and Resources

1. "A Beginner's Guide to Network Security," http://www.cisco.com/warp/public/cc/so/neso/sqso/beggu_pl.pdf.

2. List of Cisco Security products, http://www.cisco.com/en/US/products/hw/vpndevc/index.html.