Chapter 1: Fundamentals of Security

Exam Objectives

- **Types of attacks**
- **Physical security**
- **Authentication and authorization**
- **Data protection**

One of the most important skills to have if you're going to support networked systems or systems connected to the Internet is the fundamental skill involved in securing systems and networks. If you aren't working in a networked environment, you can apply these same skills to your customers with home Internet machines. The bottom line is that you need a solid understanding of network security in today's day and age.

I remember when a close friend of mine had his Web site totally replaced by a hacker. My friend's Web site files were replaced with inappropriate content, and he wondered how on earth someone had hacked his server. It seems amazing now, but back then (which was around 1994), a lot of companies didn't use firewalls because they weren't aware of the risks involved in having a computer connected directly to the Internet. Back then, people thought, "I have a password on the administrator account, so I am secure."

In this chapter, I introduce you to the basic concepts and terminology used to help secure an environment. Be sure to read this chapter carefully and make sure you understand the topics. Have fun with this topic area — it is very exciting!

Identifying Types of Attacks

If I had to define *hacker,* I would say that a hacker is someone who has the technical expertise to bypass the security of a network or operating system. A hacker also knows how to use features of a piece of software or hardware to gain access to restricted areas of a network and how to use those features against you and your system. For example, Windows 2000 servers have Web server software installed by default, and with that Web server installed, anyone in the world can view or delete files on the hard drive of the server — and the hackers know this!

There are two types of hackers:

- **White-hat hackers** try to “hack” or break software or hardware for the purpose of understanding how to protect the environment from black-hat hackers. These are the good guys.
- **Black-hat hackers** are people who break into a system or network for malicious reasons or for personal gain. The reasons could be for financial gain, bragging rights, or revenge.

Hackers use a number of different types of attacks to hack into a network or operating system. Sometimes one attack can lay the groundwork for a future or different type of attack, meaning that the initial attack doesn’t seem all that dangerous, but it is used in the future to gain unauthorized access. This section outlines some of the most popular types of attacks that can happen in networking environments today.

Social engineering attacks

A *social engineering attack* occurs when a hacker tries to obtain information or gain access to a system through social contact with a user. Typically, the hacker poses as someone else and tries to trick a user into divulging personal or corporate information that allows the hacker access to a system or network.

For example, a hacker could call your company’s phone number, which is listed in the phone book, and pretend to be technical support for your company, telling the user who answers the phone that a new application has been deployed on the network and in order for the application to work, the user’s password must be reset. After the password is reset to what the hacker wants, he may “verify” with the user the credential that the user uses. A user who isn’t educated on social engineering may divulge important information without thinking.

A social engineering attack is an attack performed by a hacker where he tries to trick a user or administrator into divulging sensitive information through social contact. Once the sensitive information is obtained, the hacker can then use that information to compromise the system or network.

This example may sound unrealistic, but it happens all the time. If you work for a small company, you might not experience a social engineering attack, but for large companies, it is extremely possible that a social engineering attack would be successful if the company doesn’t educate its users. A large company usually has the IT staff or management located at the head office, but most branch locations have never talked to IT management, so those branch employees won't recognize the voices of the IT folks. A hacker could impersonate someone from the head office, and the user at the branch office would never know the difference.

There are a number of popular social engineering attacks scenarios — and network administrators are just as likely to be social engineering victims as "regular" employees, so they need to be aware. Here are some popular social engineering scenarios:

- **Hacker impersonates IT administrator:** In this example, the hacker calls or e-mails an employee and pretends to be the network administrator. The hacker tricks the employee into divulging a password or even resetting the password.
- **Hacker impersonates user:** In this example, the hacker calls or e-mails the network administrator and pretends to be a user who forgot her password, asking the administrator to reset her password for her.
- **Hacker e-mails program:** The hacker typically e-mails all the users on a network, telling them about a security bug in the operating system and that they need to run the `update.exe` file that is attached to the e-mail. In this example, the `update.exe` is the attack — it opens the computer up so that the hacker can access the computer.

TIP

Educate your users never to run a program that has been e-mailed to them. Most software vendors, such as Microsoft, state that they will never e-mail a program to a person — they will e-mail the URL to an update, but it is up to the person to go to the URL and download it. A great book to learn more on the process a hacker takes to compromise a systems is Kevin Beaver's *Hacking For Dummies, 2nd Edition*.

Network-based attacks

A *network-based attack* uses networking technologies or protocols to perform the attack. There are a number of different types of network-based attacks, the most popular of which are mentioned in the following sections.

Password attacks

There are a number of different types of password attacks. For example, a hacker could perform a *dictionary attack* against the most popular user accounts found on networks. With a dictionary attack, hackers use a program that typically uses two text files:

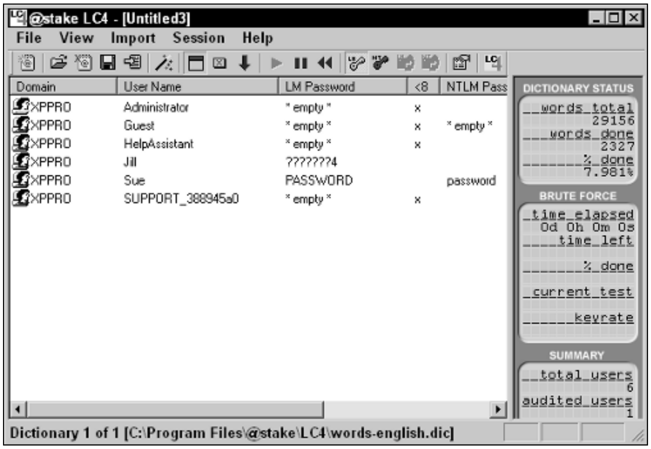
- One text file contains the most popular user accounts found on networks, such as administrator, admin, and root.
- The second text file contains a list of all the words in the dictionary, and then some.

The program then tries every user account in the user account file with every word in the dictionary file, attempting to determine the password for the user account.

To protect against a dictionary attack, be sure employees use strong passwords that mix letters and numbers. This way, their passwords aren't found in the dictionary. Also, passwords are normally case sensitive, so educate users on the importance of using both lowercase and uppercase characters. The hacker would not only have to guess the password, but also the combination of upper- and lowercase characters.

Also remind users that words found in *any* dictionary are unsafe for passwords. This means avoiding not only English words, but also French, German, Hebrew . . . even Klingon!

Hackers can also perform a *brute force attack*. With a brute force attack, instead of trying to use words from a dictionary, the hacker uses a program that tries to figure out your password by trying different combinations of characters. Figure 1-1 shows a popular password-cracking tool known as LC4. Tools like this are great for network administrators to audit how strong their users' passwords are.



Domain	User Name	LM Password	<8	NTLM Pass
XPPRO	Administrator	* empty *	x	
XPPRO	Guest	* empty *	x	* empty *
XPPRO	HelpAssistant	* empty *	x	
XPPRO	Jill	???????4		
XPPRO	Sue	PASSWORD		password
XPPRO	SUPPORT_388945a0	* empty *	x	

DICTIONARY STATUS
words total 29156
words done 2327
% done 7.981%

BRUTE FORCE
time elapsed 0d 0h 0m 0s
time left
% done
current test
keyrate

SUMMARY
total users 6
audited users 1

Dictionary 1 of 1 [C:\Program Files\@stake\LC4\words-english.dic]

Figure 1-1: Cracking passwords with LC4.

Remember that to protect against password attacks users should use strong passwords, which is a password made up of letters, numbers, symbols, has a mix of upper- and lowercase characters, and a minimum length of 6 characters.

Denial of service

Another popular network attack is a *denial of service (DoS)* attack. A denial of service attack can come in many forms and is designed to cause a system to be so busy that it cannot service a real request from a client, essentially overloading the system and shutting it down.

For example, if I have an e-mail server, and a hacker attacks the e-mail server by flooding the server with e-mail messages, causing it to be so busy that it cannot send anymore e-mails for me, then I have been denied the service the system was created for.

There are a number of different types of DoS attacks. For example, there is *the ping of death.* The ping of death is when a hacker continuously pings your system, and your system is so busy sending replies that it cannot do its normal function.

Spoofing

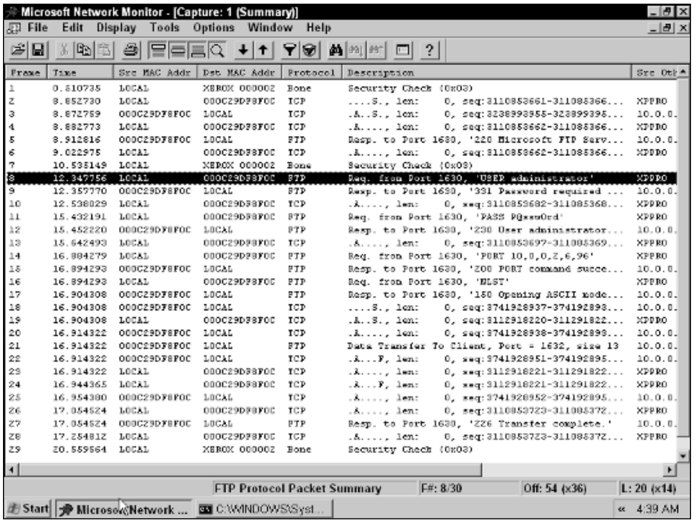
Spoofing is a type of attack in which a hacker modifies the source address of a network packet. A *packet* is a piece of information that is sent out on the network. This packet includes the data being sent but also has a header section that contains the source address (where the data is coming from) and the destination address (where the data is headed). If the hacker wants to change who the packet looks like it is coming from, the hacker modifies the source address of the packet.

An example of a spoof attack is the smurf attack. A *smurf attack* is a combination of a denial of service and spoofing. Here's how it works:

1. The hacker pings a large number of systems but modifies the source address of the packet so that the ping request looks like it is coming from a different system.
2. All systems that were pinged reply to the modified source address — an unsuspecting victim.
3. The victim's system (most likely a server) receives so many replies to the ping request that it is overwhelmed with traffic, causing it to be unable to answer any other request from the network.

Eavesdropping attack

An *eavesdropping attack* is when a hacker uses some sort of packet sniffer program that allows him to see all the traffic on the network. Hackers use *packet sniffers* to find out login passwords or to monitor activities. Figure 1-2 shows Microsoft Network Monitor, a program that monitors network traffic by displaying the contents of the packets.



```
Frame  Time       Src MAC Addr  Dst MAC Addr  Protocol  Description                                       Src Oth
1      0.810735   LOCAL         XEROX 000002  None      Security Check (0x03)
2      8.852730   LOCAL         000C29DF8F0C  TCP       ....S., len:    0, seq:3110853661-311085366...  XPPRO
3      8.872759   000C29DF8F0C  LOCAL         TCP       .A..S., len:    0, seq:3238993955-323899395...  10.0.0.
4      8.882773   LOCAL         000C29DF8F0C  TCP       .A...., len:    0, seq:3110853662-311085366...  XPPRO
5      8.912816   000C29DF8F0C  LOCAL         FTP       Resp. to Port 1630, '220 Microsoft FTP Serv...  10.0.0.
6      9.022975   LOCAL         000C29DF8F0C  TCP       .A...., len:    0, seq:3110853662-311085366...  XPPRO
7      10.535149  LOCAL         XEROX 000002  None      Security Check (0x03)
8      12.347756  LOCAL         000C29DF8F0C  FTP       Req. from Port 1630, 'USER administrator'       XPPRO
9      12.357770  000C29DF8F0C  LOCAL         FTP       Resp. to Port 1630, '331 Password required ...  10.0.0.
10     12.538029  LOCAL         000C29DF8F0C  TCP       .A...., len:    0, seq:3110853682-311085368...  XPPRO
11     15.432191  LOCAL         000C29DF8F0C  FTP       Req. from Port 1630, 'PASS P@ssw0rd'            XPPRO
12     15.452220  000C29DF8F0C  LOCAL         FTP       Resp. to Port 1630, '230 User administrator...  10.0.0.
13     15.642493  LOCAL         000C29DF8F0C  TCP       .A...., len:    0, seq:3110853697-311085369...  XPPRO
14     16.884279  LOCAL         000C29DF8F0C  FTP       Req. from Port 1630, 'PORT 10,0,0,2,6,96'       XPPRO
15     16.894293  000C29DF8F0C  LOCAL         FTP       Resp. to Port 1630, '200 PORT command succe...  10.0.0.
16     16.894293  LOCAL         000C29DF8F0C  FTP       Req. from Port 1630, 'NLST'                     XPPRO
17     16.904308  000C29DF8F0C  LOCAL         FTP       Resp. to Port 1630, '150 Opening ASCII mode...  10.0.0.
18     16.904308  000C29DF8F0C  LOCAL         TCP       ....S., len:    0, seq:3741928937-374192893...  10.0.0.
19     16.904308  LOCAL         000C29DF8F0C  TCP       .A..S., len:    0, seq:3112918220-311291822...  XPPRO
20     16.914322  000C29DF8F0C  LOCAL         TCP       .A...., len:    0, seq:3741928938-374192893...  10.0.0.
21     16.914322  000C29DF8F0C  LOCAL         FTP       Data Transfer To Client, Port = 1632, size 13   10.0.0.
22     16.914322  000C29DF8F0C  LOCAL         TCP       .A...F, len:    0, seq:3741928951-374192895...  10.0.0.
23     16.914322  LOCAL         000C29DF8F0C  TCP       .A...., len:    0, seq:3112918221-311291822...  XPPRO
24     16.944365  LOCAL         000C29DF8F0C  TCP       .A...F, len:    0, seq:3112918221-311291822...  XPPRO
25     16.954380  000C29DF8F0C  LOCAL         TCP       .A...., len:    0, seq:3741928952-374192895...  10.0.0.
26     17.054524  LOCAL         000C29DF8F0C  TCP       .A...., len:    0, seq:3110853723-311085372...  XPPRO
27     17.054524  000C29DF8F0C  LOCAL         FTP       Resp. to Port 1630, '226 Transfer complete.'    10.0.0.
28     17.254812  LOCAL         000C29DF8F0C  TCP       .A...., len:    0, seq:3110853723-311085372...  XPPRO
29     20.559564  LOCAL         XEROX 000002  None      Security Check (0x03)

FTP Protocol Packet Summary    F#: 8/30    Off: 54 (x36)    L: 20 (x14)
```

Figure 1-2: Using Network Monitor to analyze FTP logon traffic.

Notice in Figure 1-2 that the highlighted packet (frame 8) shows someone logging on with a username of `administrator`; in frame 11, you can see that this user has typed the password `P@ssw0rd`. In this example, the hacker now has the username and password of a network account by eavesdropping on the conversation!

Man-in-the middle

While an eavesdropping attack involves the hacker reviewing information, a *man-in-the-middle attack* involves the hacker monitoring network traffic but also intercepting the data, modifying the data, and then sending the modified result out. The person the packet is destined for never knows that the data was altered in transit.

Session hijacking

A *session hijack* is similar to a man-in-the-middle attack, but instead of the hacker intercepting the data, altering it, and sending it to whomever it was destined for, the hacker simply hijacks the conversation, known as a *session,* and then impersonates one of the parties. The other party has no idea he is not communicating with the original partner.

FOR THE EXAM

Ensure that you are familiar with the different types of network-based attacks for the A+ exams.

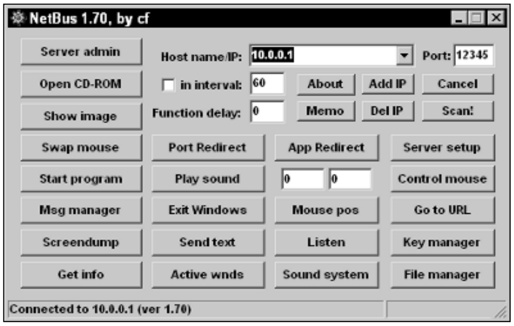
Software-based attacks

Just as there are a number of different types of network attacks, there are a number of software attacks as well. A *software attack* is an attack through software that a user runs. The most popular software attacks are mentioned in the sections that follow.

Trojan horse

A *Trojan horse* is a piece of software that a user is typically tricked into running on the system, and when the software runs, it does something totally different than what the user expected it to do. For example, a typical Trojan horse attack is with a program called NetBus. NetBus is an example of a Trojan horse program that is sent as a file called `patch.exe`. The user receiving the file, typically through an e-mail, believes that the file will fix a security issue. The problem is that `patch.exe` is a Trojan horse, and when that horse starts running, it opens the computer up to allow a hacker to connect to the system.

The hacker then uses a client program, like the one shown in Figure 1-3, to connect to the system and start messing with the computer. The hacker can do things like launch other programs, flip your screen upside-down, eject your CD-ROM tray, watch your activity, and modify or delete files!



NetBus 1.70, by cf

Host name/IP: 10.0.0.1 Port: 12345

□ in interval: 60

Function delay: 0

Connected to 10.0.0.1 (ver 1.70)

Figure 1-3: Using NetBus to control a user's computer.

Virus

A *virus* is a program that causes harm to your system. Typically, viruses are spread through e-mails and are included in attachments such as word processing documents and spreadsheets. The virus can do any of a number of things — it can delete files from your system, modify the system configuration, or e-mail all your contacts in your e-mail software. To prevent viruses, you should install antivirus software and not open any file attachments that arrive in your e-mail that you are not expecting.

Worm

A *worm* is a virus that does not need to be activated by someone opening the file. The worm is *self-replicating,* meaning that it spreads itself from system to system, infecting each computer. To protect against a worm, you should install a firewall. A *firewall* is a piece of software or hardware that prevents someone from entering your system.

Logic bomb

A *logic bomb* is malicious software that could run every day, but the software was designed to wreak havoc on your system on a certain date and time. The scary thing about logic bombs is that they seem like useful software until the day the programmer decides it will become malicious!

Understanding Physical Security

You should implement security in many places. One of the most overlooked areas is physical security. *Physical security* has nothing to do with software; it refers to how you protect your environment and systems by making sure that a person cannot physically access the system. For example, many companies use a numeric keypad to secure the entrance to a facility. In order to get into the facility, you must enter a valid combination on the keypad in order to open the door. Figure 1-4 shows a numeric keypad lock used to enforce physical security.

Another example of physical security is the server room. Most server room doors are locked with a numeric padlock or a key. In order to get access to the server room, you need the key or the correct number for the keypad. Higher-security server rooms sometimes even require fingerprint or retinal scans from anyone trying to enter the room.

The benefit of locking your servers in the server room is that hackers cannot boot off a bootable CD-ROM, which could bypass the operating system entirely. After they have bypassed the operating system, they typically can bypass a lot of the security because they have booted to a totally different operating system.

TIP

You can apply security best practices like the ones used by companies with their servers to your home systems. For example, to help secure your home system you may want to prevent booting from a CD-ROM so that an unauthorized person cannot try to bypass your Windows security.

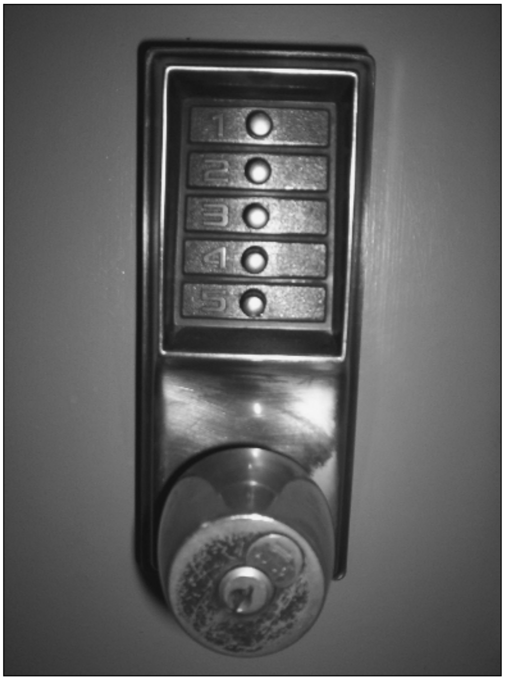


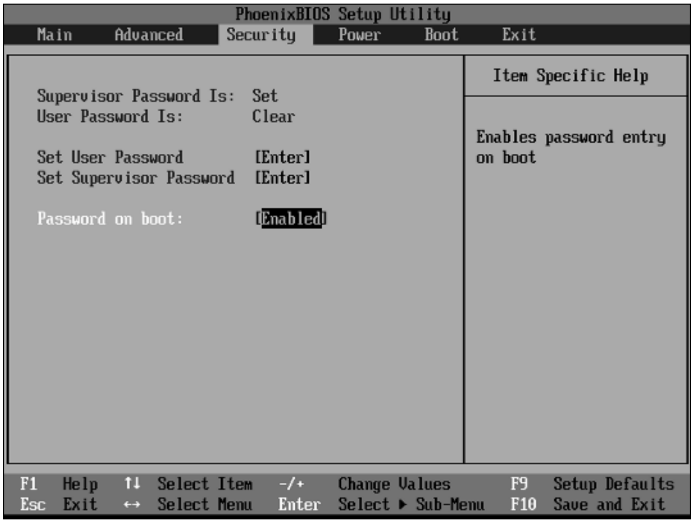
Figure 1-4: A numeric keypad used to enforce physical security.

In order to protect your systems, follow these physical security best practices:

- **Server placement:** Lock your servers in a room that only a select few individuals have the key for.
- **Disable boot devices:** You can help secure the systems by disabling the ability to boot from a floppy disk or CD-ROM in the CMOS setup on the systems.
- **Set CMOS password:** Because most hackers know how to go to CMOS and enable booting from CD-ROM, you want to make sure that you set a password on CMOS so that a hacker cannot modify your CMOS settings. Figure 1-5 shows a CMOS password being enabled.

  TIP

  Check out Book II, Chapter 4, to get the lowdown on reconfiguring your CMOS settings.
- **Disable network ports:** To ensure that a hacker doesn't enter your office, plug into the network, and then start performing a number of network attacks, ensure that network ports in lobbies and front entrances are disabled unless an administrator enables them.



```
                      PhoenixBIOS Setup Utility
  Main    Advanced    Security    Power    Boot    Exit

  Supervisor Password Is:  Set               Item Specific Help
  User Password Is:        Clear
                                             Enables password entry
  Set User Password        [Enter]           on boot
  Set Supervisor Password  [Enter]

  Password on boot:        [Enabled]

F1   Help  ↑↓  Select Item   -/+    Change Values        F9   Setup Defaults
Esc  Exit  ↔   Select Menu   Enter  Select ▶ Sub-Menu    F10  Save and Exit
```

Figure 1-5: Enabling the CMOS password.

✦ **Lockdown cable:** A *lockdown cable* is a cable that you connect to laptops, projectors, and other types of office equipment that locks the device to a table or desk — unless unlocked. Figure 1-6 shows a lockdown cable being used to secure a laptop. A lockdown cable usually connects to a hole in the side of the computer equipment that usually has a picture of a lock next to it.

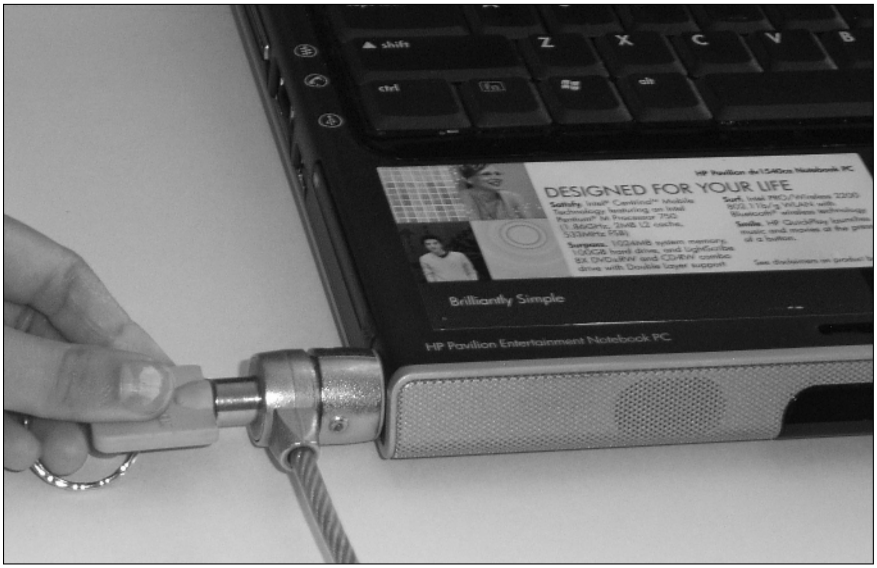


Figure 1-6: A lockdown cable is used to secure computer equipment to a desk.

Remembering ways to physically secure your systems will help you with the security portion of the A+ exam. Be sure to place critical systems in locked rooms and lock down equipment that is accessible by the public.

Understanding Authentication and Authorization

After you have physically secured your environment, you then want to focus on the people who access your systems and network. The next step after implementing physical security is to ensure that persons who have entered your server room or have a connection to a network port are authorized to log on to the network. Logging onto the network is known as *authentication.*

Authentication

Authentication is the process of proving one's identity to the network environment. Typically, authentication involves typing a username and password on a system before you are granted access, but you could also use biometrics to be authenticated. *Biometrics* are the use of one's unique physical characteristics, such as a fingerprint or the blood vessels in one's retina, to prove one's identity. Figure 1-7 shows a fingerprint reader that is used to scan your fingerprint in order to log on.

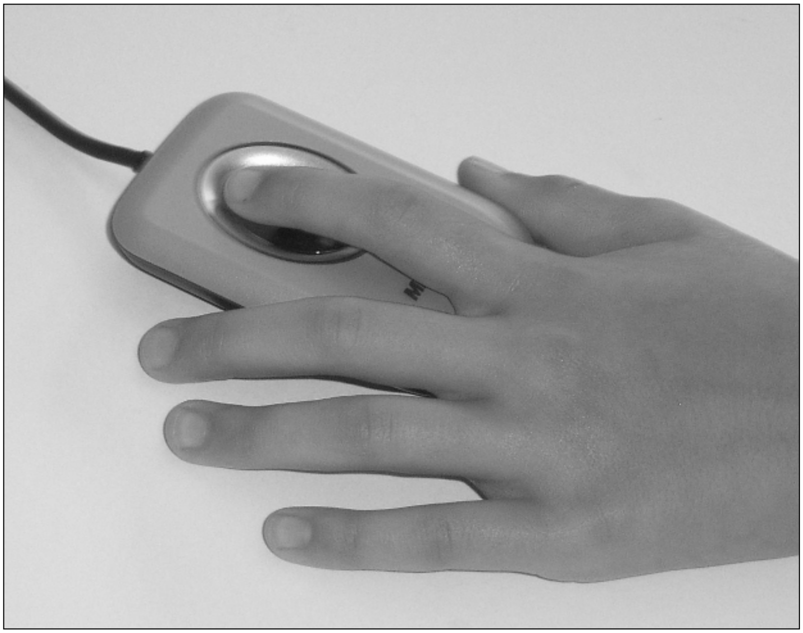


Figure 1-7: A fingerprint reader is an example of biometrics used for authentication.

Here's a quick look at what happens when you log on to your system with a username and password. When you type a username and password to log on to a system, that username and password are verified against a database, known as the *user account database,* which has a list of the usernames and passwords that are allowed to access the system. If the username and password you type are in the user account database, you are allowed to access the system — otherwise, you get an error message and aren't allowed to access the system.

The name of the account database that stores the usernames and passwords is different depending on the environment. In a Microsoft network, the account database is known as the *Active Directory Database* and resides on a server known as a *domain controller* (shown in Figure 1-8).

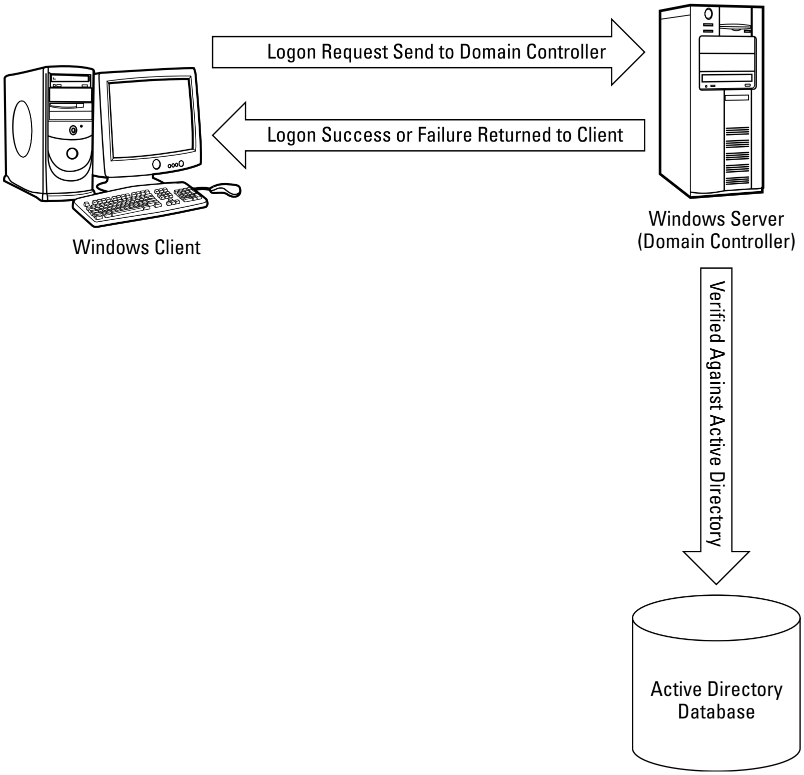

Logon Request Send to Domain Controller
Logon Success or Failure Returned to Client
Windows Client
Windows Server
(Domain Controller)
Verified Against Active Directory
Active Directory
Database

Figure 1-8: Logging on to Active Directory in a Microsoft network environment.

Generating the access token

When you log on to a Microsoft network environment, the username and password you type are placed in a logon request message that is sent to the domain controller to be verified against the Active Directory Database. If the username and password that you have typed are correct, then an access token is generated for you. An *access token* is a piece of information that identifies you and is associated with everything you do on the computer and network. The access token contains your user account information and any groups you are a member of. When you try to access a resource on the network, the user account and group membership in the access token are compared against the permission list of a resource. If the user account in the access token or one of the groups contained in the access token are also contained in the permission list, then you are granted access to the resource — if not, you get an access-denied message.

If you don't have a server-based network environment and you are simply running Windows 2000 Professional or Windows XP, when you log on, the logon request is sent to the local computer — to an account database known as the *Security Accounts Manager (SAM)* database. When you log on to the SAM database, an access token is generated as well, and that helps the system determine what files you can access.

Smart card

Another type of logon supported by network environments today is the use of a smart card. A *smart card* is a small, ATM card–like device that contains your account information. You insert the smart card into a smart card reader that is connected to a computer, and then you enter the PIN (Personal Identification Number) associated with the smart card. This is an example of securing an environment by forcing someone to not only have the card but also know the PIN.

Strong passwords

It's really hard to talk about authentication without talking about ensuring that users create strong passwords. A *strong password* is a password that is very difficult for hackers to guess or crack because it contains a mix of upper- and lowercase characters, contains a mix of numbers and letters, and is a minimum of six characters long.

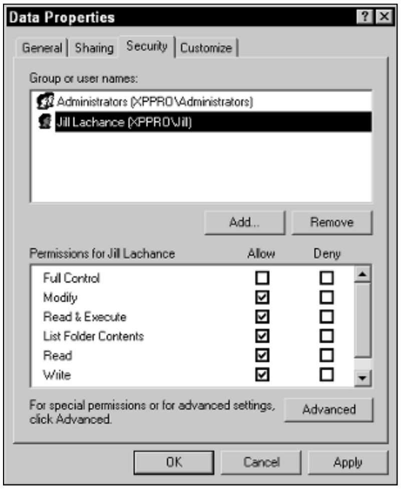
Authorization

After a user has logged on and an access token is created, the user may start trying to access resources such as files and printers. In order to access a file, folder, or printer on the network, the user must be authorized to access the resource. *Authorization* is the process of giving a user permission to access a resource. Do not confuse authentication and authorization — you must be first authenticated to the network, and once authenticated, you can then access the resources you have been authorized for.

Using Strong Passwords

A number of years ago, I had a coworker who was always trying to get me to guess his passwords. He thought I had some magical trick or program that was cracking them, but all I was doing was guessing his passwords. I remember one time he changed it and I couldn't guess it, until one night we were at a social function for work and all he talked about were the Flyers hockey team. I remember sitting there thinking, "I bet that's his password." Sure enough, the next day at work, I tried `flyers` as his password, and it worked. Now the lesson here is that he should have at least mixed the case of the word *flyers* to make something like `flYeRs`, or even better, thrown a symbol in there by replacing the "s" with a "$." I would have had a much harder time trying to guess his password if he had used `flYeR$` instead. This is an example of a strong password.

In order to authorize access to a resource, you set permissions on the resource. For example, if you want to allow Jill to access the accounting folder, you need to give Jill permission to the accounting folder, as shown in Figure 1-9.



Group or user names:

Administrators (XPPRO\Administrators)
Jill Lachance (XPPRO\Jill)

Permissions for Jill Lachance	Allow	Deny
Full Control	☐	☐
Modify	☑	☐
Read & Execute	☑	☐
List Folder Contents	☑	☐
Read	☑	☐
Write	☑	☐

For special permissions or for advanced settings, click Advanced.

Figure 1-9: Using permissions to authorize which users are allowed to access the resource.

In Figure 1-9, you can see that the Administrators and Jill have access to the resource. No one else is authorized to access the resource. You find out how to set permissions in the next chapter, but for now, make sure you understand the difference between authentication and authorization.

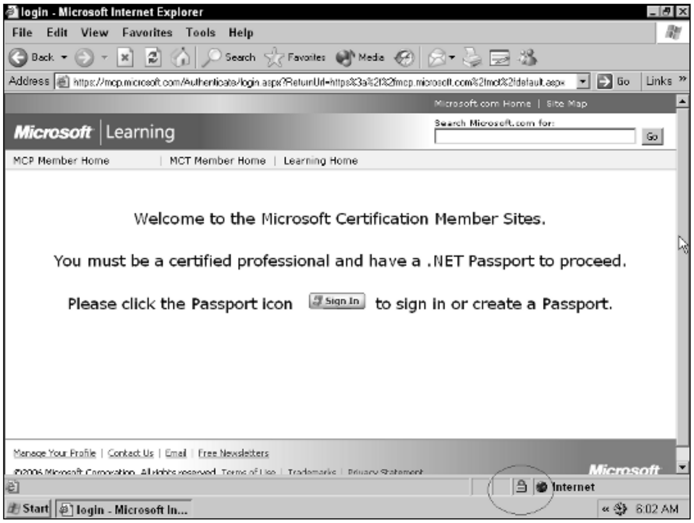
Methods of Securing Transmissions

After you have authenticated users and authorized them to access certain parts of the network, you should then consider methods of securing information while it travels along the network cable.

Most network communication is sent along the network wire in *cleartext,* meaning that anyone connected to your network can read the information. But if the information is traveling across the Internet, anyone can view that information if it is passed in cleartext.

Most Internet protocols, such as HTTP, send information in cleartext, and it is up to the people who set up the servers that use these Internet protocols to encrypt the information before it is released to the Internet. *Encrypting* the information means that the information is run through a mathematical calculation that generates an altered version of the information, known as a *result.* For example, the words "Glen Clarke" could be encrypted to look like "7y3i s3fk4r." This is encrypted information, and if anyone intercepts and views it when it is traveling across the wire, the information means nothing to him or her.

A great example is if you were to type your credit card number into a Web site. You don't want that credit card number to be viewed as you send it from your client computer to the server, so be sure that the Web site you enter the credit card number into is encrypting the traffic. You can tell by the lock icon that appears in the Web browser, as shown in Figure 1-10.


login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Go
Links
Microsoft.com Home | Site Map
Microsoft | Learning
Search Microsoft.com for:
Go
MCP Member Home | MCT Member Home | Learning Home
Sign In
Manage Your Profile | Contact Us | Email | Free Newsletters
©2006 Microsoft Corporation. All rights reserved. Terms of Use | Trademarks | Privacy Statement
Microsoft
Internet
Start
login - Microsoft In...
6:02 AM

Address https://mcp.microsoft.com/Authenticate/login.aspx?ReturnUrl=https%3a%2f%2fmcp.microsoft.com%2fmct%2fdefault.aspx

Welcome to the Microsoft Certification Member Sites.

You must be a certified professional and have a .NET Passport to proceed.

Please click the Passport icon Sign In to sign in or create a Passport.

Figure 1-10: Identifying a secure site by locating the lock in Internet Explorer.

It is important for the A+ exam that you understand popular methods of encrypting traffic. You can use a number of technologies, such as

- **Secure Sockets Layer (SSL):** SSL is a protocol that is used to encrypt different types of Internet traffic. For example, you could use SSL to encrypt HTTP traffic by applying a digital certificate to the Web site. The *digital certificate* contains the key that is used to encrypt and decrypt the traffic.
- **Internet Protocol Security (IPSec):** IPSec is a protocol that can encrypt all TCP/IP traffic between systems. As a network administrator, you configure IPSec on the server and the clients with the same key, which is used to encrypt and decrypt network traffic. Due to the configuration, it is an unlikely solution for a Web site but is a great way to encrypt traffic on your network.
- **Virtual Private Network (VPN):** A VPN allows a user to connect across the Internet to a remote network, typically her office network, and send information between her system and the office network securely. The information is secured because the VPN technology used creates an encrypted tunnel between the user and the office network — any data that travels through the tunnel is encrypted.

The preceding sections touch on a number of places that require security. Here's a quick overview of the security steps I've discussed so far:

- You should secure your office environment first from physical access by unauthorized persons.
- You should set up a system for authentication, which is the idea that users must log on to the network.
- After users log on to the network, they must be authorized to access resources.
- When you allow someone to access resources, make sure that you encrypt the traffic while it is in transit, especially if the information is transmitted outside your own network.

Don't Forget about Data Protection

In this section, you find out about how to secure your data environment from a hacker or malicious user. When securing your systems, you want to protect the systems from a person who damages information or systems with or without intent. You want to be sure to secure your environment from hackers, but at the same time, you want to protect your systems from users on the network who may cause damage without meaning to. Accidents can always happen, so be sure to prevent accidents from happening by following the best practices in the following sections.

Destroying data

Most office environments have strict policies in place to help secure confidential information. Shredding paper documents that contain personal or confidential information is a no-brainer, and computerized data should be no different. It is important for the company to have strict guidelines on how to destroy data that resides on computer hard drives. Destroying data that resides on a computer hard disk typically involves shredding the computer hard drive with a huge shredding machine — or destroying the drive another way such as sanding the platters down to nothing.

I have talked to some customers who used to destroy drives by driving spikes through them, but what they found was that the data around the hole that the spike put in the drive could still be read! These customers now disintegrate the drive in a huge "shredder," while other customers sand the drives right down to nothing. Either way, if securing the data is a concern, make sure to physically destroy the disk that contains the data.

Instead of destroying the drives, some companies use a shredder *application* that writes a bunch of 1s to the drive, thereby overwriting the previous data. These applications typically overwrite the drive a number of times because hackers can retrieve the data from disk even after it has been overwritten a few times. If you are purchasing shredding software, be sure to investigate how many overwrite operations the software performs. I recommend using software that overwrites at least 7 times.

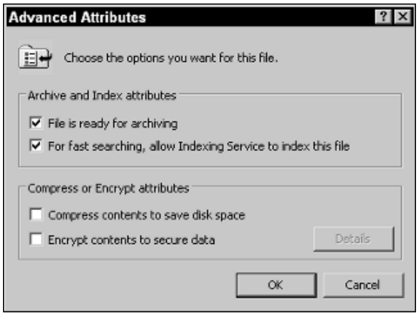
Backing up data

A big part of securing the data environment is not only setting the permissions but also ensuring that you create a good backup and restore strategy. It is important to identify which files are critical to the operation of the business and should be backed up. You also want to be familiar with all types of information used by your company. For example, you may depend on e-mail, so you want to make sure you back up your e-mail server along with any files that exist in shared folders. If your company stores important data in databases, you want to make sure that you back up those databases as well.

Backup review

You can find out more about backups in Book VII, Chapter 3, but for the exam here are some of the key points you need to remember:

When you perform a backup, the operating system keeps track of which files have been changed since the last backup by setting the *archive bit.* The archive bit is an attribute of the file that tells the system that the file has changed. To view the archive bit within Windows XP, right-click the file and choose Properties. In the Properties dialog box, click the Advanced button — the Advanced Attributes dialog box appears (shown in Figure 1-11).



Choose the options you want for this file.

Archive and Index attributes

☑ File is ready for archiving

☑ For fast searching, allow Indexing Service to index this file

Compress or Encrypt attributes

☐ Compress contents to save disk space

☐ Encrypt contents to secure data

Figure 1-11: Viewing the archive bit in Windows XP.

The first option, File Is Ready for Archiving, is the archive bit. When this check box is checked it means that the file needs to be backed up because it has changed.

Before you perform a backup, you must first decide what type of backup to perform. Each backup type deals with the archive bit a little differently. There are three major types of backup, which are discussed below:

- **Full backup:** A full backup copies any files that you select, whether the archive bit is set or not, and clears the archive bit on any file that is backed up — essentially recording the fact that the file has been backed up.
- **Differential backup:** A differential backup copies any files that have changed, but it doesn't clear the archive bit; thus, there is no record that the files have been backed up. The benefit is that the next time you do the backup, the files will be backed up again because the archive bit has not been cleared. As far as the operating system is concerned, the file has not been backed up since it was changed.
- **Incremental:** An incremental backup copies any file that has changed and then clears the archive bit on any files that are backed up. So if a file is copied during an incremental backup, because the backup process clears the archive bit, the file won't be backed up during subsequent incremental backups unless the file changes again.

For the exam, be familiar with the difference between a full backup, incremental backup, and differential backup. Also know which backup types clear the archive bit.

Tape rotation and offsite storage

You want to make sure that you take the time to rotate tapes so that the same tape is not being used all the time. You also want to make sure that you store a backup offsite in case of a disaster such as flood or fire. It is important that you are able to recover the system no matter what happens.

Test restore operations

As a last point with backup strategy best practices, you want to ensure that you test restorations frequently to ensure that you can recover information from backup without any problem. You don't want to find out that the backups are bad when management is hanging over your shoulder waiting for the company network to come back online! Be sure to perform regular test restorations.

Implementing RAID solutions

To help secure your data, you not only want to make sure you have good backups, but you also want to ensure that you are implementing some form of a *RAID* solution. *RAID (Redundant Array of Inexpensive Disks)* is covered in detail in Book II, Chapter 5, so in this section, I review the different types of RAID volumes supported in Windows 2000 Server and Windows Server 2003 and ensure that you understand that RAID solutions are a way of helping secure data.

RAID is a way of storing duplicated data on multiple disks so that if one disk goes down, the data is still available to the users because other disks in the RAID array have a copy of the data. The benefit of RAID over backups is that with the RAID solution, the user never knows that a drive has failed because the other drive is supplying all the data. You still need the backups in case both drives fail or some disaster happens, like a flood or fire — destroying the system and all of its drives.

There are a number of different types of RAID solutions. The ones provided by the Windows Server operating systems are as follows:

- **RAID Level 0:** Also known as a *striped volume* in Windows, RAID Level 0 writes different parts of the data to different disks at the same time. The benefit of a striped volume is that you get a performance benefit by writing the data at the same time to two different disks, essentially taking less time to read or write to the file. Note that the data is split between both drives, and there is no duplication — which means that this is not really a redundant solution.
- **RAID Level 1:** Also known as *a mirrored volume* in Windows. A mirrored volume duplicates the data stored on one disk to another disk. If one disk fails, then the other disk has a copy of the data.

- **RAID Level 5:** Also known as a *RAID 5 volume* in Windows. A RAID 5 volume requires a minimum of three drives and writes to all drives in the solution like a striped volume. A RAID 5 volume is different than a striped volume in the sense that it does store redundant data, known as parity data, on one of the disks. The redundant data is used to calculate the missing data when a disk goes missing, ensuring that users can still retrieve the data without noticing a problem.

Ensure that you are comfortable with the RAID levels when preparing for the exam. Check out Book II, Chapter 5, to learn how to create volumes in Windows 2000, XP, and Server 2003.

Getting an A+

This chapter introduces you to a number of security-related terms that you need to understand before taking your first A+ exam. The following are some key points to remember when preparing for the exam:

- *Authentication* is the process of proving your identity to the network, while *authorization* is the process of determining whether you are allowed to access a resource or not after you have been authenticated.
- Hackers take many different approaches to compromise a system. You should ensure that you protect your environment from both network-based and software-based attacks and that physical security is in place.
- A *denial of service* (DoS) is an attack on a system or network that prevents the system or network from performing its regular function.
- *Social engineering* is a popular type of attack that involves the hacker compromising security by tricking an employee through social contact. The social engineer might entice the user to divulge confidential information or may trick the user into running a program that does harm to the system.
- You secure network traffic by *encrypting* traffic between two systems by using technologies such as SSL and IPSec. Administrators typically use SSL to encrypt Web traffic and IPSec to encrypt internal or VPN traffic.
- Securing your data involves not only protecting resources with permissions but also protecting your data by following proper data destruction procedures and backup strategies and creating redundant disk solutions.

Prep Test

1 **What type of attack involves the hacker tricking a user through social contact?**

A ❍ Password attack
B ❍ Eavesdrop attack
C ❍ Man-in-the middle attack
D ❍ Social engineering attack

2 **What type of attack involves the hacker using a packet sniffer and trying to view confidential information traveling over the network?**

A ❍ Password attack
B ❍ Eavesdrop attack
C ❍ Man-in-the-middle attack
D ❍ Social engineering attack

3 **What type of attack involves the hacker causing your system or network to become unresponsive to valid requests?**

A ❍ DoS attack
B ❍ Eavesdrop attack
C ❍ Man-in-the-middle attack
D ❍ Password attack

4 **What type of RAID volume duplicates the data fully on two disks?**

A ❍ Striped volume
B ❍ Mirrored volume
C ❍ RAID 5 volume
D ❍ RAID Level 0

5 **What type of attack involves the hacker capturing network traffic, altering the data, and sending it on to its destination?**

A ❍ Password attack
B ❍ Eavesdrop attack
C ❍ Man-in-the-middle attack
D ❍ Social engineering attack

6 **What type of software-based attack involves a program performing an unexpected function at a certain date or time?**

A ❍ Virus
B ❍ Worm
C ❍ DoS
D ❍ Logic bomb

7 **You wish to ensure that a hacker cannot boot off a CD-ROM or floppy disk to bypass the operating system; what should you do?**

A ❍ Set a password in Windows.
B ❍ Disable the CD-ROM and floppy as bootable devices in CMOS. Also put a password on CMOS.
C ❍ Disconnect the CD-ROM and floppy drive.
D ❍ Ensure that the CD-ROM and floppy are first in the boot order — before the hard disk.

8 **What type of RAID volume stripes the data across all disks but also contains parity information used to recalculate missing data?**

A ❍ Striped volume
B ❍ Mirrored volume
C ❍ RAID 5 volume
D ❍ RAID Level 0

9 **What should you purchase for each laptop to help protect it from theft?**

A ❍ Flash drive
B ❍ Driver disk
C ❍ A Doberman pinscher
D ❍ Lockdown cable

10 **What type of authentication device requires you to know the PIN when you place the card into the reader?**

A ❍ Fingerprint scanner
B ❍ Smart card
C ❍ Biometric device
D ❍ Retinal scanner

11 **Which of the following are forms of biometrics? (Select all that apply.)**

A □ Fingerprint scan
B □ Smart card
C □ Username and password
D □ Retinal scan

12 **What type of software-based attack involves a virus spreading itself from system to system without needing to be activated by a user?**

A ○ Trojan
B ○ Worm
C ○ DoS
D ○ Logic bomb

13 **What type of backup copies the files that have changed and does not clear the archive bit?**

A ○ Full backup
B ○ Incremental backup
C ○ Differential backup
D ○ Copy

14 **What technology is typically used to encrypt traffic between a Web server and Web browser?**

A ○ DoS
B ○ IPSec
C ○ Smart card
D ○ SSL

15 **In high-security environments, what should you do with old hard drives?**

A ○ Donate them to charity
B ○ Recycle them
C ○ Physically destroy them
D ○ Drive a spike through them

16 **Which of the following is the strongest password?**

A ○ `thisisalongpassword`
B ○ `P@ssw8rd`
C ○ `password`
D ○ `StrongPassword`

17 **Where should your company's servers be located?**

A ○ At the front door
B ○ In a manager's office
C ○ At the reception desk
D ○ In a locked room

18 **What technology is used to encrypt all TCP/IP traffic?**

A ❍ DOS
B ❍ IPSec
C ❍ Smart card
D ❍ SSL

19 **What type of attack involves the hacker modifying the source address of the packet?**

A ❍ Spoof attack
B ❍ Eavesdrop attack
C ❍ Man-in-the middle attack
D ❍ Social engineering attack

20 **When is an access token generated?**

A ❍ Only during logon
B ❍ During logon and automatically every 90 minutes
C ❍ When the system is turned on
D ❍ When the system is turned on and automatically every 90 minutes

Answers

1 **D.** Social engineering is a type of hack that involves contacting victims through phone or e-mail and tricking them into doing something that compromises company security. *See "Social engineering attacks."*

2 **B.** An eavesdropping attack is when a hacker monitors network traffic to try to capture information that could be useful in another attack. *Review "Eavesdropping attack."*

3 **A.** A denial of service (DoS) attack is when a hacker consumes all of the system's processing power or bandwidth so that it is unable to perform its normal job. *Check out "Denial of service."*

4 **B.** A mirrored volume is used to create a full duplicate of the data on two different disks. *Peruse "Implementing RAID solutions."*

5 **C.** A man-in-the-middle attack is when the hacker captures data traveling on the wire, alters the data, and sends it to the person it was originally destined for. The parties involved have no idea they are dealing with altered information. *Take a look at "Man-in-the-middle."*

6 **D.** A logic bomb is placed in the code of the program so that on a certain date, the program harms the system. Before that triggered date, the program runs normally and offers benefits to the user. *Peek at "Logic bomb."*

7 **B.** Ensure that a hacker cannot boot off a CD-ROM or floppy disk by disabling them as bootable devices in CMOS. Also be sure to set a CMOS password so that hackers cannot easily enter CMOS and change the boot settings. *Look over "Understanding Physical Security."*

8 **C.** A RAID 5 volume spreads the data across a number of disks and then calculates parity information, which is used to generate missing data when a disk fails. *Study "Implementing RAID solutions."*

9 **D.** A lockdown cable is used to secure the laptop to a desk to help prevent the laptop from being stolen. *Refer to "Understanding Physical Security."*

10 **B.** A smart card is a small credit card–like authentication device that is inserted into a smart card reader. After the card is inserted into the reader, the user then types a PIN to be authenticated. *Examine "Smart card."*

11 **A, D.** Biometric devices involve authenticating a user through the user's unique physical characteristics. Fingerprint scans and retinal scans are popular biometric authentication methods. *See "Authentication."*

12 **B.** A worm is a self-replicating virus that bounces from system to system. You can use a firewall to stop the worm from replicating to your system. *Review "Worm."*

13 **C.** A differential backup only backs up the files that have changed since the last full backup and then does not clear the archive bit. *Check out "Backup review."*

14 **D.** Secure Socket Layer (SSL) is used to encrypt Web traffic. You can identify whether or not you are on a secure Web site by looking for the lock icon at the bottom of the screen. *Peruse "Methods of Securing Transmissions."*

15 **C.** You want to make sure that you physically destroy the drives if securing data is critical to the business. *Take a look at "Destroying data."*

16 **B.** `P@ssw8rd` is the strongest password listed because it a) is more than six characters long, b) it has a mix of upper- and lowercase characters, and c) it is a mix of numbers, letters, and symbols. *Peek at "Strong passwords."*

17 **D.** You should keep your servers in a locked room. You want to make sure that you physically secure your systems, along with all the other security measures. *Look over "Understanding Physical Security."*

18 **B.** Internet Protocol Security (IPSec) is used to secure all TCP/IP traffic. *Study "Methods of Securing Transmissions."*

19 **A.** A spoof attack is when the hacker modifies the source address, trying to hide the origin of the packet. *Refer to "Spoofing."*

20 **A.** The access token is generated only during logon. *Examine "Generating the access token."*