# Chapter 1: Fundamentals of Security

## Exam Objectives

- **Types of attacks**
- **Physical security**
- **Authentication and authorization**
- **Data protection**
- **Prevention methods and best practices**
- **Incident response**

One of the most important skills to have if you are going to support networked systems or systems connected to the Internet is the capability of securing systems and networks. And even if you are not 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.

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 (circa 1994), a lot of companies did not use firewalls because they were not 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 as you will be tested on security topics on the A+ exams. Have fun with this topic area — it is very exciting!

## Identifying Types of Attacks

To me, a hacker is someone with the technical expertise to bypass the security of a network or an OS. A hacker knows how to use features of a piece of software or hardware to gain access to restricted areas of a network and then how to use those features against you and your system. For example, most Web sites connect to a database behind the scenes so that you can get a list of products when you visit their site. A hacker knows how to input data into the site to manipulate your database server into executing the code that the hacker wants to execute — and this happens because the hacker understands the technologies being used.

The two types of hackers are

- **White-hat hackers,** who try to "hack" or break software or hardware so as to understand how to protect the environment from black-hat hackers. These are the good guys.
- **Black-hat hackers** 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 an OS. Sometimes an attack lays the groundwork for a future or different type of attack: that is, the initial attack does not 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 calls your company's phone number, listed in the phone book, and poses as a technical support person for your company. He tells the user who answers the phone that a new application has been deployed on the network, and for the application to work, the user's password must be reset. After the password is reset to what the hacker wants, he might "verify" with the user the credential that the user uses. A user who is not educated on social engineering might divulge important information without thinking.

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

This example might sound unrealistic, but it happens all the time. If you work for a small company, you might not experience a social engineering attack. In a large corporate environment, though, it is extremely possible that a social engineering attack would be successful if the company does not 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 would not 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.** 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.** 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 OS and that they need to run the `update.exe` file 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: Instead, 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 system is Kevin Beaver's *Hacking For Dummies,* 2nd Edition (Wiley).

## Phishing

Phishing is a type of social engineering that involves the hacker sending you an e-mail that is impersonating a site such as a bank or an online site like eBay. The e-mail message typically tells you that a pressing matter exists, such as a security compromise with your account, and that you need to log on to your account to verify your transactions. The e-mail message gives you a link to use to navigate to the site, but instead of navigating to the real site, the hacker is leading you to a fake site that he or she has created. This fake site looks like the real site, but when you type in your username and password, the hacker captures that information and then uses it to access your account on the real site!

It is important to educate employees about phishing attacks and know that they should not click the link that is available in the e-mail message. Navigate to the site manually through the browser by typing the URL yourself.

## Shoulder surfing

Shoulder surfing is another type of social engineering attack where someone hangs out behind you and watches what you type on the keyboard. The person is hoping to discover sensitive information such as a password. The key to protect against shoulder surfing is to educate employees and inform them that they should never type sensitive information while someone is looking over their shoulder or at their screen.

## Network-based attacks

A *network-based attack* uses networking technologies or protocols to perform the attack. Here are the most popular types.

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

### 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:

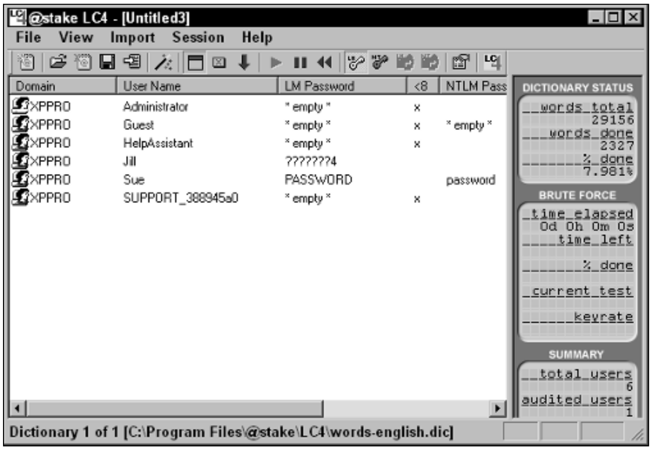
- One text file contains the most popular user accounts found on networks, such as administrator, admin, and root.
- The second text file contains a list of all the words in the English dictionary, and then some. You can also get dictionary files for different languages.

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 are not found in the dictionary. Also, passwords are normally case sensitive, so educate users on the importance of using both lowercase and uppercase characters. That way, a hacker not only has to guess the password but also the combination of uppercase 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.

To protect against password attacks, users should use strong passwords, which is a password comprising of letters, numbers, and symbols with a mix of uppercase and lowercase characters and a minimum length of six characters.

## Denial of service

Another popular network attack is a *denial of service (DoS)* attack, which 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, say you 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. You have been denied the service that the system was created for.

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

TIP

To protect against denial of service attacks you should have a firewall installed and also keep your system patched.

### Spoofing

*Spoofing* is a type of attack in which a hacker modifies the source address of a network *packet,* which 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.

There are three major types of spoofing — MAC spoofing, IP spoofing, and e-mail spoofing. MAC spoofing is when the hacker alters the source MAC address of the packet, IP spoofing is when the hacker alters the source IP address in a packet, and e-mail spoofing is when the hacker alters the source e-mail address to make the e-mail look like it came from someone other than the hacker.

An example of a spoof attack is the smurf attack, which is a combination of a denial of service and spoofing. Here is how it works:

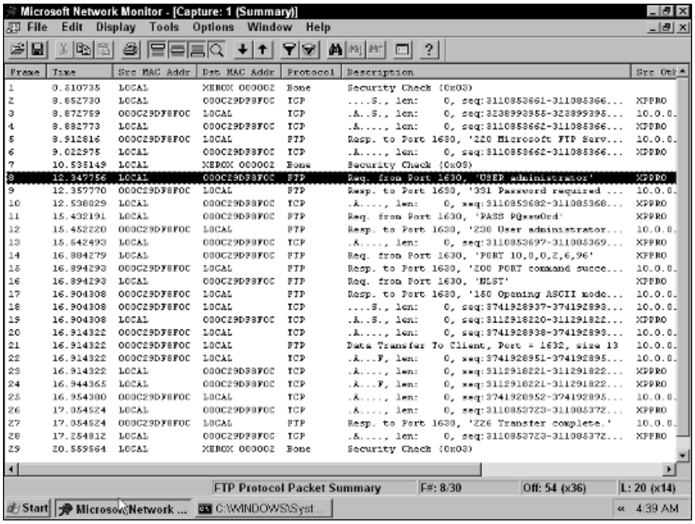
1. The hacker pings a large number of systems but modifies the source address of the packet so that the ping request looks like it is coming from a different system.
2. All systems that were pinged reply to the modified source address — an unsuspecting victim.
3. The victim's system (most likely a server) 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.

TIP

To protect against spoof attacks you can implement encryption and authentication services on the network.

## Eavesdropping attack

An *eavesdropping attack* occurs when a hacker uses some sort of packet sniffer program 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.


Microsoft Network Monitor - [Capture: 1 (Summary)]
File Edit Display Tools Options Window Help
Start
Microsoft Network ...
C:\WINDOWS\Syst...
4:39 AM

```
Frame Time       Src MAC Addr  Dst MAC Addr  Protocol Description                                     Src Oth
1     0.510735   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!

TIP

To protect against eavesdrop attacks you should encrypt network traffic.

## Man-in-the-middle

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

TIP

To protect against man-in-the-middle attacks you should restrict access to the network and implement encryption and authentication services on the network.

### 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 — a *session* — and then impersonates one of the parties. The other party has no idea that he is communicating with someone other than the original partner.

TIP

To protect against session hijacking attacks you should restrict access to the network and implement encryption and authentication services on the network.

### Wireless attacks

There are a number of different attacks against wireless networks that you should be familiar with. Hackers can crack your wireless encryption if you are using a weak encryption protocol such as WEP. Hackers can also spoof the MAC address of their system and try to bypass your MAC address filters. Also, there are wireless scanners such as Kismet that can be used to discover wireless networks even though SSID broadcasting is disabled.

TIP

To protect against wireless attacks you should implement encryption protocols such as WPA2 and use an authentication server such as a RADIUS server for network access. For more information on wireless check out Book VIII, Chapter 2.

## Software-based attacks

Just as there are a number of different types of network attacks, there are a number of software attacks as well. As you can likely guess, a *software attack* comes through software that a user runs. The most popular software attacks are mentioned in the sections that follow, and you should be familiar with them for the A+ exams.

### SQL injection

An *SQL injection attack* occurs when the hacker sends `Transact SQL` statements (statements that manipulate a database) into an application so that the application will send those statements to the database to be executed. If the application developer does not validate data inputted in the application, the hacker can modify the data or even delete it. The hacker can potentially manipulate the OS through the application that sends the input to the database.

### Buffer overflow

A very popular type of attack today is a *buffer overflow attack,* which involves the hacker sending more data to a piece of software than it is expecting. The information sent to an application is typically stored in an area of memory (a *buffer*). When more data than expected is sent to the application, the information is stored in memory beyond the allocated buffer. If the hacker can go beyond the allocated buffer, he can run the code. This code executes in the context of the user account associated with the software that was hacked — normally an administrative account!

TIP

To protect against buffer overflow attacks, you should keep the system and its applications patched.

## Malicious software (malware)

Malicious software, also known as malware, is any software that does harm to the system, such as a virus or spyware. In the following sections, you will get an overview of the different types of malicious software, but be sure to review Book IV, Chapter 3 for more information on malware!

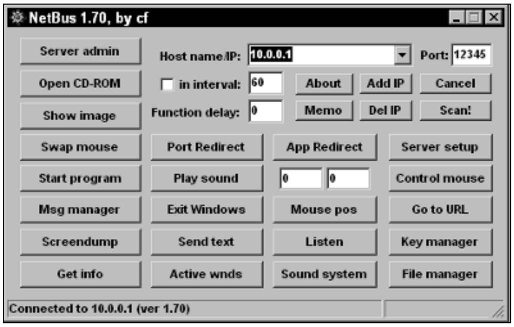
### Virus

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: delete files from your system, modify the system configuration, or e-mail all your contacts in your e-mail software. To prevent viruses, install antivirus software and do not open any file attachments that arrive in your e-mail inbox that you are not expecting.

### Trojan horse

A *Trojan horse* is 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, NetBus (an older attack) is an example of a Trojan horse program 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!



Host name/IP: 10.0.0.1 Port: 12345

□ in interval: 60

Function delay: 0

0 0

Connected to 10.0.0.1 (ver 1.70)

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

## Rootkit

A rootkit is malicious software installed on your system by the hacker that gives the hacker unauthorized access to the system at a later time. You find out more about rootkits in Book IX, Chapter 3.

## 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!

## Spyware and adware

Spyware is a type of malicious software that when installed on your system, monitors your activity, including Internet activity. Adware is software that after being installed on your system, will pop up with ads promoting different products and websites. Be sure to install spyware protection and adware protection on your system to prevent such software from running on your computer.

A term sometimes used by security professionals to describe software that performs unwanted actions is *grayware.* Grayware encompasses malicious software such as adware and spyware. Be sure to have malware protection software loaded on your system to protect against forms of grayware.

TIP

To protect against malicious software such as a virus, Trojan horse, worm, and a logic bomb, you should use a firewall and keep your virus definitions up to date. To find out more about malicious software, check out Book IX, Chapter 3.

## Understanding Physical Security

You should implement security in many places, and one of the most overlooked areas is physical security. *Physical security* has nothing to do with software; rather, it covers 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 entrance to a facility. To get into the facility, users must enter a valid combination to open the door.

Another example of physical security is the server room. Most server room doors are locked with a numeric padlock or a key. 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 a hacker cannot boot off a bootable CD-ROM, which could bypass the OS entirely. After a hacker bypasses the OS, he typically can bypass a lot of the security by booting to a totally different OS.

A big part of physical security is locking doors to prevent unauthorized access to certain areas of the building, but in high-secure environments, that is not enough because of tailgaiting! *Tailgaiting* is when an employee unlocks a door and enters the facility, and an unauthorized person slips through the door with him. To prevent tailgaiting, the company should use a *mantrap,* which is two locked doors that someone must pass through to gain access to the facility. The hook is that the second door does not open until the first door is locked again. This allows the employee to be aware of who is entering the facility with him before unlocking the second door.

TIP

You can apply enterprise security best practices to your home systems. For example, to help secure your home system, you might want to prevent booting from a CD-ROM so that an unauthorized person cannot try to bypass your Windows security.

## BIOS settings

You can set a number of settings in your system BIOS to help control the security of the system. Be sure to investigate the BIOS settings on your system to see what security settings you can enable on the system. Here are some popular BIOS/CMOS settings to aid in physical security:

- **Drive lock:** Drive lock (a popular feature with laptops) is a hard disk specification used to protect access to the drive. To protect access to the drive, there are two drive lock passwords: a user password and a master password. The user password is used by the user wanting to access the system; the master password is used to reset the user password if the user forgets the password. Do not confuse drive lock passwords that prevent booting from the drive with the general CMOS passwords for the system. If the user password and master password are forgotten or lost, the drive is useless.
- **Passwords:** You can set a power-on password in CMOS to limit who can use the system. If the power-on password is forgotten, it can typically be erased via a jumper on the motherboard or by taking the battery off the motherboard and putting it back in.
- **Intrusion detection:** Most systems have intrusion detection features that can be enabled through the BIOS that will notify you if the cover is taken off the system. This is designed to alert you if someone opens the cover and takes internal components.
- **TPM:** The *Trusted Platform Module* (TPM) is a chip on computer hardware used to store cryptography keys that are typically used to encrypt data. A TPM chip can also be used to authenticate a device because it contains a unique key that identifies the chip, or hardware device. Most computers today have a TPM chip, and a number of software solutions (such as Windows Vista Bit Locker) can use the TPM chip to encrypt the contents of the drive.

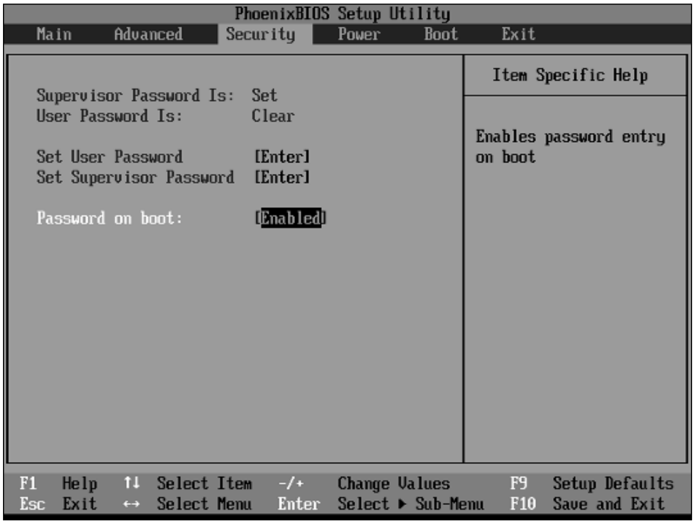
## Best practices

To protect your systems, follow these physical security best practices:

- **Secure server placement.** Lock your servers in a room for which only a select few individuals have the key.
- **Lock the workstation.** When you leave your system, get in the habit of locking your workstation. A locked workstation can only be unlocked by yourself or the network administrator. This will prevent other users from accessing the system while you are away.

- **Disable boot devices.** Disable 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, make sure that you set a password on CMOS so that a hacker cannot modify your CMOS settings. Figure 1-4 shows a CMOS password being enabled.

  Check out Book II, Chapter 4, to get the lowdown on reconfiguring your CMOS settings.



```
Supervisor Password Is:  Set
User Password Is:        Clear

Set User Password        [Enter]
Set Supervisor Password  [Enter]

Password on boot:        [Enabled]
```

Enables password entry on boot

**Figure 1-4:** Enabling the CMOS password.

- **Disable network ports.** To prevent a hacker from entering your office, plugging into the network, and performing a number of network attacks, ensure that network ports, or jacks, in lobbies and front entrances are disabled unless an administrator enables them.
- **Use a lockdown cable.** Use a *lockdown cable* to tether laptops, projectors, and other types of office equipment to a table or desk. Figure 1-5 shows a lockdown cable being used to secure a laptop. A lockdown cable usually connects to a special hole in the side of the computer equipment (look for a picture of a lock next to it).

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.

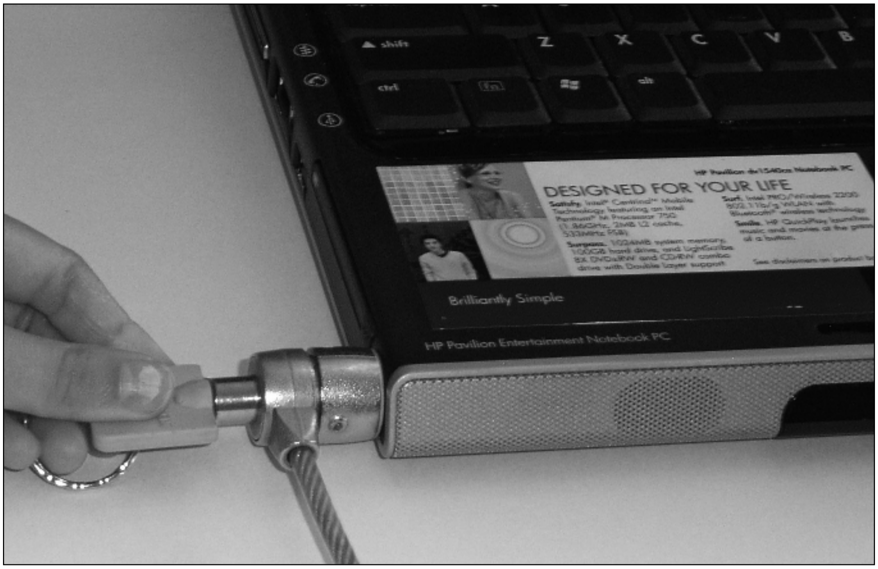


**Figure 1-5:** A lockdown cable is used to secure computer equipment to a desk.

# Understanding Authentication and Authorization

After you physically secure your environment, focus on the people who access your systems and network. The next step after implementing physical security is to ensure that persons who enter your server room or have a connection to a network port are authorized to log on to the network. Logging onto the network is *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* is using one's unique physical characteristics, such as a fingerprint or the blood vessels in one's retina, to prove one's identity. Figure 1-6 shows a fingerprint reader used to scan your fingerprint when logging on.

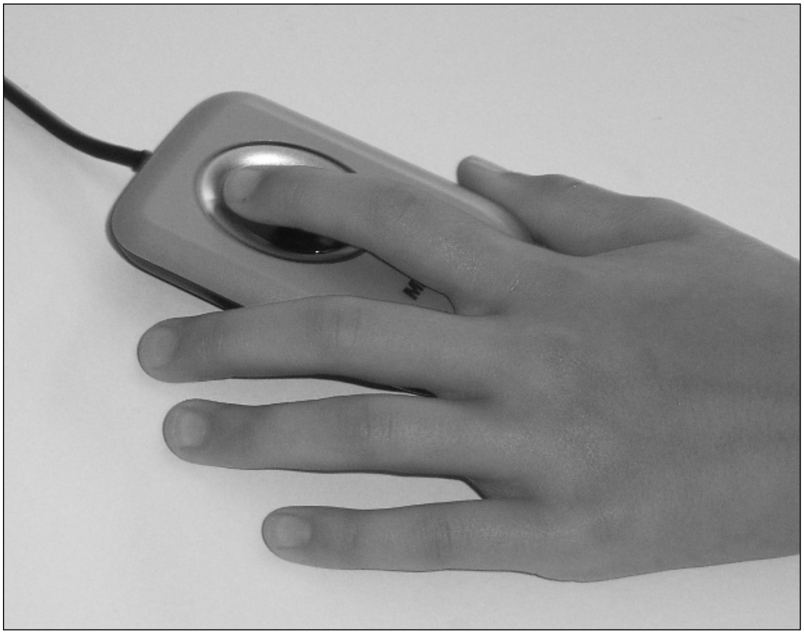


**Figure 1-6:** A fingerprint reader is an example of biometrics used for authentication.

Here is 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 — the *user account database* — which has a list of the usernames and passwords 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 are not allowed access.

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 the *Active Directory Database* and resides on a server known as a *domain controller* (shown in Figure 1-7).

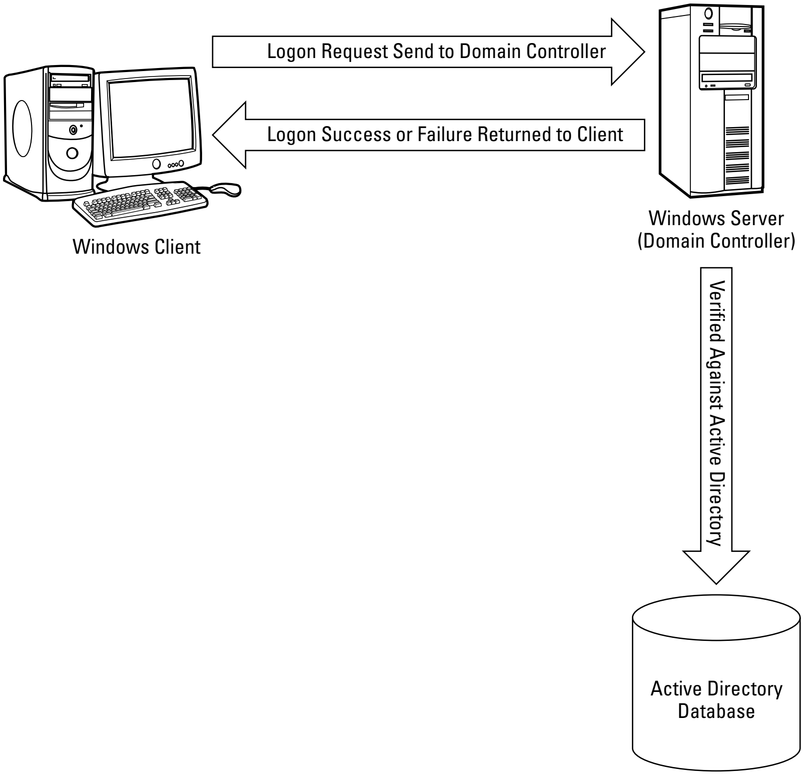

Logon Request Send to Domain Controller
Logon Success or Failure Returned to Client
Windows Client
Windows Server
(Domain Controller)
Verified Against Active Directory
Active Directory
Database

**Figure 1-7:** 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 typed are correct, 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 of which you are a member. 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, you are granted access to the resource. If not, you get an access-denied message.

If you do not have a server-based network environment and you are simply running Windows XP or Windows 7, 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.

### Other authentication objects

When implementing authentication systems, you have a number of different ways that you can prove someone's identity or that he belongs in the environment. The most common method to authenticate someone to a system is with a username and password, but the following items outline some other methods of authenticating employees:

- **Badges:** High-secure environments require all personnel, including employees and contractors, to wear identification badges at all times to identify that employee. These badges may also use different colors, which are a flag identifying different parts of the building that the employee is allowed to be in. Some badges have magnetic strips that store authentication information and are used to swipe before gaining access to the building.
- **Key fobs:** A key fob is a small authentication hardware device that connects to an employee's keychain. The device is used in the authentication process by generating a random number that the employee who possesses the key fob must enter as part of the authentication process. The random number is synchronized with an authentication device.
  A key fob is also a device that is used to gain access to a building by having the employee swipe the key fob past a scanner.
- **RFID badge:** RFID (radio frequency ID) badges use radio frequency to submit authentication information to RFID access points as the employee approaches the facility or different areas of the facility. The benefit of the RFID badge is that the employee is not required to swipe any kind of card because the RFID signal is picked up by the access point.

- **RSA token:** An RSA token is a device, also called a key fob, that is used in authentication by generating a random number that the user carrying the token, usually on his or her keychain, would use along with his or her password.
- **Privacy filters:** Privacy filters are placed on computer screens so that to see the information on the screen, you have to be directly in front of the screen. The privacy filter is similar in concept to a window blind that sits on top of your computer screen and prevents someone lurking around you from seeing the information on the screen.

### Strong passwords

It is 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 uppercase and lowercase characters, contains a mix of numbers and letters, and is a minimum of six characters long.

### Single sign-on

Single sign-on (SSO) is an authentication term you should be familiar with for the certification exams. SSO is the principle that you should be able to log on to the network with your username and password and then be given access to a number of different resources such as files, printers, and your e-mail using that one username and password. The opposite of an SSO environment is when you have to supply a username and password for each different resource that you access. Microsoft's Active Directory environment is an example of a single sign-on environment.

## Using strong passwords

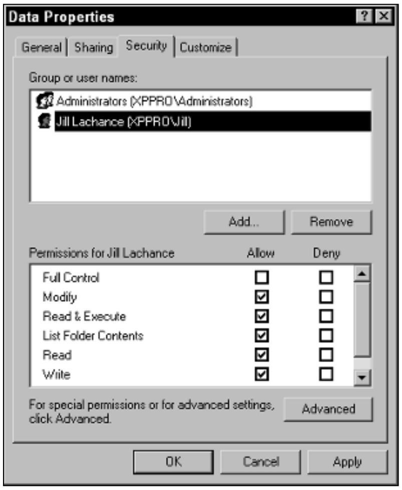
A number of years ago, I had a co-worker who was always trying to get me to guess his passwords. He thought I had some magical trick or program that was cracking them, but all I was doing was guessing his passwords. I remember one time he changed it, and I could not guess it until one night when we were at a social function for work and all he talked about were the Flyers hockey team. I remember sitting there thinking, "I bet that is 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 "$." I would have had a much harder time trying to guess his password if he had used `flYeR$` or `f1YeR$` instead. This is an example of a strong password.

## Authorization

After a user logs on and an access token is created, the user may start trying to access resources such as files and printers. 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 or the right to perform an OS task. Do not confuse authentication and authorization: You must be first authenticated to the network; then, after authentication, you can access the resources you have been authorized for.

### Permissions

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 1-8.



Data Properties

General | Sharing | Security | Customize

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 1-8:** Using permissions to authorize which users are allowed to access the resource.

In Figure 1-8, 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.

### Rights

In the Windows world, there is a difference between permissions and rights. As you can read in earlier sections, permission is your level of access to a resource. Comparatively, a right is your privilege to perform an OS task. For example, you can be assigned the right to change the time on the computer.

Other examples of rights are the right to do backups or the right to log on to the system.

To learn more about how to set permissions and rights, check out Book IX, Chapter 2.

## Methods of Securing Transmissions

After you authenticate users and authorize 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: a *result.* For example, the words `Glen Clarke` could be encrypted to look like `7y3i s3fk4r`. If anyone intercepts such encrypted information and views it while it is traveling across the wire, the information would mean nothing.

Here is a real-world example. You type your credit card number on a Web site, but you certainly do not want that credit card number to be viewed while you send it from your client computer to the server. You want to be sure that the Web site where you enter the credit card number encrypts the traffic. You can tell by the lock icon that appears in the Web browser, as shown in Figure 1-9.

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

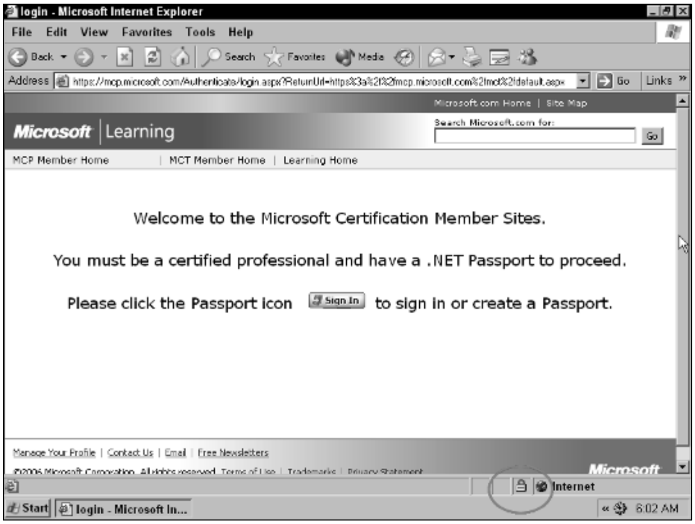
- **Secure Sockets Layer (SSL):** This protocol is used to encrypt different types of Internet traffic. For example, you could use SSL to encrypt HTTP traffic by applying a digital certificate to the Web site. The *digital certificate* contains the key that is used to encrypt and decrypt the traffic.
- **Internet Protocol Security (IPSec):** This protocol 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 or digital certificates,

which are used to encrypt and decrypt network traffic. Because of 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 is a quick overview of the security steps that I have discussed so far:

- Secure your office environment first from physical access by unauthorized persons.
- 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.


login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Search
Favorites
Media
Address
Go
Links
Microsoft.com Home | Site Map
Microsoft | Learning
Search Microsoft.com for:
Go
MCP Member Home | MCT Member Home | Learning Home
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 1-9:** Identifying a secure site by locating the lock in Internet Explorer.

# Do Not 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 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 with personal or confidential information is a no-brainer, and computerized data should be no different. A company needs strict guidelines on how to properly destroy data that resides on computer hard drives.

### Low-level format versus standard format

When looking to replace a system, recycle it, or donate it to charity, it is critical that you erase all the company data from the drive. Most people look to formatting the drive as a method of erasing the data from the drive, but depending on the type of format you do, the data may actually not be erased. The following are different types of formats that can be performed:

- **Low-level format (LLF):** A low-level format is performed on the drive at the manufacturer and is responsible for setting up the tracks and sectors on the disk. Low-level formats are normally not done by the administrator or user. You need the LLF program to perform such an operation, which is typically only available to the manufacturer of the drive.
- **High-level format (HLF):** The high-level format is responsible for setting up the file system on the drive and creating allocation tables such as the file allocation table (FAT) and the directory entry table.
- **Quick format:** A quick format is the term for the format operation you can perform to “erase” the contents from the drive. It is called a quick format because it doesn’t actually erase the data; it simply deletes the entries from the directory entry table (which is a listing of files that exist).

### Hard drive sanitation

When it comes to erasing the data from the drive, also known as *sanitizing* the drive, it is not enough to perform a format of the drive because formatting the drive does not actually erase the data from the sectors, and someone determined to discover your information can use a forensics tool to view deleted data on the drive. You must use a drive-wiping program, also known as a shredding application, which actually overwrites the contents on the sectors of the drives many times to ensure that the company data no longer exists.

I use a program called *Secure Wipe,* from the Forensics Acquisition Utilities (FAU), to overwrite and sanitize a drive, which you can download from `http://gmgsystemsinc.com/fau`. After you downloaded FAU, you can run the secure wipe program by navigating to a command prompt (to the FAU directory) and then type the following command to securely erase a drive (I am erasing the F: drive in this example):

```
wipe \\.\f:
```

You will notice that the program overwrites the contents of the drive three times, the first time writing all FFs to the drive, the second time writing random bits, and the third time writing null values (nothing).

### Hard drive destruction

Many highly secure environments do not want to risk the fact that the program used to erase the contents of the drive did not work as expected, so they opt to have the hard drives removed from any system being decommissioned and then physically destroy the drives through one of the following methods:

- **Shredder:** Destroying data that resides on a computer hard drive 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.
- **Drill:** I have talked to some customers who used to destroy drives by drilling 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. Other customers sand the drives down to nothing. Either way, if securing the data is a concern, make sure to *physically destroy* the entire drive that contains the data.
- **Electromagnetic:** Because the data is stored magnetically on the disk, you could destroy the data from the drive by using a very strong magnet to magnetically corrupt the data on the drive into an unreadable format.
- **Degaussing tool:** You can use a degaussing tool to magnetically randomize the data stored on the drive to prevent the data from being readable.

### Hard drive recycling

What do you do with your hard drive when you get an upgrade or replacement drive? Well, you could pass the hard drive on to someone else who needs the drive, or you could have the drive recycled. After all, a number of useful parts are on the drive, such as the hard drive platters and the magnets.

However, be aware of the risk of passing your drive over to someone! Companies concerned with corporate security and data privacy will likely opt to destroy the drive instead of recycling because of the risk of having private data lifted off the drive.

### Destroying paper documents

Not only should you be concerned with the company data that is stored on hard drives electronically, but you should also watch for security issues surrounding confidential data in hard copy format. A business must have paper shredders that are used by employees to shred documents before recycling or placing in the garbage.

Also watch for situations where employees are writing passwords on paper and leaving the paper in an unsecure location. Be sure to educate employees on the importance of not writing passwords on paper.

Make sure that you secure physical documents by having all confidential documents in hard-copy format locked in filing cabinets. Ensure that the filing cabinets are in secure areas where you can control who has physical access to those cabinets.

## Backing up data

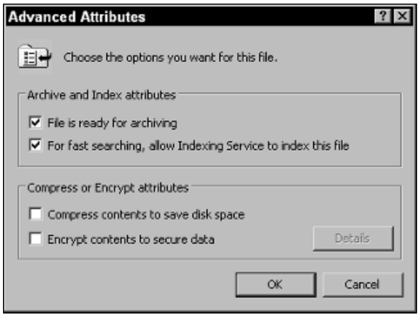
A big part of securing the data environment is not only setting the permissions but also ensuring that you create a good backup and restore strategy. Identify which files are critical to the operation of the business and should be backed up. You also want to be familiar with all types of information used by your company. For example, you might depend on e-mail, so make sure that you back up your e-mail server along with any files in shared folders. If your company stores important data in databases, 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 OS 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 or Windows 7, right-click the file and choose Properties. In the Properties dialog box, click the Advanced button.

The first option in the Advanced Attributes dialog box that appears — File Is Ready for Archiving — is the archive bit. (See Figure 1-10.) When this check box is selected, it means that the file needs to be backed up because it has changed.



Advanced Attributes

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 1-10:** Viewing the archive bit in Windows.

Before you perform a backup, decide what type of backup to perform. Each backup type deals with the archive bit a little differently. Here are the three major types of backup:

- **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:** Copies any files that have changed, but it does not 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 OS is concerned, the file has not been backed up since it was changed.
- **Incremental:** Copies any file that has changed and then clears the archive bit on any files that are backed up. Thus, if a file is copied during an incremental backup, because the backup process clears the archive bit, the file will not be backed up during subsequent incremental backups unless the file changes again.

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

### Tape rotation and offsite storage

Take the time to rotate tapes so that the same tape is not 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 test restorations frequently to ensure that you can recover information from backup without any problem. You do not 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, not only do you want to 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 6, so in this section I review the different types of RAID volumes supported in Windows servers 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; 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 using RAID instead of 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. ***Note:*** You still need the backups, though, in case both drives fail, or some disaster happens, like a flood or fire, destroying the system and all of its drives.

A number of different types of RAID solutions are available. The ones provided by the Windows Server OSes 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, the other disk has a copy of the data.

Book IX Chapter 1

Fundamentals of Security

- **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 — *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.

FOR THE EXAM

Be comfortable with the RAID levels when preparing for the exam. Check out Book II, Chapter 6, to see how to create volumes in Windows.

## Data encryption

Encrypting data converts information to an unreadable format so that if folks gain access to the data, they cannot understand it. In the cryptography world, encryption is described as changing plain text to cipher text. As you can likely intuit, decryption converts cipher text to plain text.

There are a number of ways to encrypt data on the hard drive:

- **EFS:** The Encrypting File System (EFS) is a feature of NTFS and can be enabled through the file properties. After the file is encrypted, it can be read only by authorized persons. To read more about EFS, check out Book V, Chapter 4.
- **Bit Locker:** Instead of encrypting data at the file level with EFS, you can have Windows encrypt the entire partition or volume, which protects all data on the partition, including the Windows OS, the Registry, and the data. With Bit Locker, data is encrypted by using keys stored in a TPM chip or a USB drive, depending upon how Bit Locker has been configured.
- **Third-party software:** You can also use third-party software to encrypt data. For example, you can use the free program TrueCrypt (`www.truecrypt.org`) to encrypt all your data into a TrueCrypt file and then copy the file to a USB flash drive.

## Compliance and classification

Part of securing your computing environment is understanding how to protect the business from disclosure of information and by ensuring the business is compliant with government and industry regulations that surround computing and data.

### Compliance

Data compliance is the concept of protecting the data from information leaks and ensuring recoverability of information by following government regulations and industry regulations. For example, if you are in the health industry, you must be compliant with the Health Insurance Portability and Accountability Act (HIPAA), which requires that health records and patient information be secured and kept private.

Companies are also required to protect customer information as outlined by the Privacy Act. Companies are no longer allowed to share customer information with other businesses, including contact information such as e-mail addresses and phone numbers.

Another example of data compliance is ensuring that your company has taken the correct steps and implemented the correct controls to adhere to the Sarbanes-Oxley Act, which outlines that the company must be able to prove that adequate auditing controls have been put in place in case an incident requires review of internal information, such as company e-mails.

WARNING!

If you are the security manager for your company, be sure to spend time researching which government regulations and industry regulations your company falls under. With your list of regulations in hand, then you can determine the steps you need to take to be compliant.

### Classification

Part of securing company information is through data classification, which assigns a level of sensitivity to information, such as Confidential or Top Secret. After the level of sensitivity is assigned to the information, the necessary controls are put in place to protect that classification of information.

Each data classification has specific security measures that need to be implemented to keep it secure. For example, a company might decide that top secret information cannot leave the “top secret” system — say, by disabling the ports on the system that typically would allow connecting a removable drive.

REMEMBER

Data classification is assigned to the information based on the value of the information to the organization. Each classification level is designed to indicate whether the information is to be kept private or is available for public release. The following are examples of classification levels:

- Top secret, secret, and unclassified
- Confidential, official use only, and public
- Highly confidential, proprietary, internal use, and public

# Prevention Methods and Best Practices

A company can take a number of different steps to help improve the security posture of the organization. In the following sections, you review important methods of improving different aspects of security.

## Physical security

Physical security was discussed earlier in the chapter, and it is a big part of any company's security strategy. It is important to ensure that you have servers, routers, and other network equipment locked in a server room.

In highly secure environments, ensure that you have fences around the perimeter of the property, with only one entrance that all persons must pass through. In most high-secure environments, security guards are at the entrance, controlling who gains access to the facility. After people are inside the facility, you can control access to different areas of the building with swipe cards or other authentication devices.

When configuring a system for security, be sure to configure BIOS passwords to control who can change the BIOS settings on the system. Also, modify the boot order of the system so that someone cannot boot from a CD or DVD. If employees can boot from another operating system, they may be able to bypass the security of the system.

## Digital security

You can take a number of different steps to improve digital security. First ensure that you have software installed on the system to protect you against malicious software. All systems should have antivirus and antispyware software installed.

You should also ensure that firewall software is installed on the system to protect the system from unwanted traffic. Hackers can exploit the system by simply sending a few commands to the system, so it is important that you control what can reach your system. All current versions of Windows have built-in firewall software that can be enabled.

Ensure that you configure strong passwords on your user accounts so that no one can guess or crack your passwords. Passwords should meet the following requirements:

- Minimum of eight characters
- Mix of uppercase and lowercase characters

- Contain a number and symbol
- Not be related to the username in any way

You should also ensure that you secure the files and printers on a system with permissions. In Windows, we call these the NTFS permissions, which control who can access what files and what level of access employees should get. For example, you can specify that Bob gets access to the employee handbook document, but that he only gets read access, not write (modify) access!

## User education

As a security professional within the organization, it is important to educate the user on security incidents that could occur if best practices are not followed. Educate users on concepts such as tailgaiting and social engineering attacks so that they are comfortable with how to handle such incidents.

Also educate users on password security best practices. Ensure that users know not to write down their passwords or share them with other employees, and make sure that they know how to change their password.

## Principle of least privilege

One of the fundamental principles of security is the principle of least privilege, which means that when you give someone permission to a resource or the rights to perform a task, ensure that you always give the minimum privileges necessary. For example, if you need Bob to change the time on the computer, you could put him in the Administrators group or you could just give him the Change System Time right. The proper choice is to give him the Change System Time right because placing Bob in the Administrators group accomplishes the goal but also allows Bob to modify every other aspect of the system.

## Workstation security best practices

You have a number of best practices to follow when you look at security best practices for workstations. The following list outlines some security best practices that you can follow to help secure the client systems on a network:

- **Setting strong passwords:** Ensure that passwords are complex passwords, meaning that they should contain a mix of uppercase and lowercase letters, numbers, and symbols.
- **Requiring passwords:** Ensure that you require passwords for someone to gain access to a workstation or a mobile device.

- **Restricting user permissions:** Ensure that you are following the principle of least privilege by making sure that employees only have user-level access to the system. Employees do not need administrative access to the system.
- **Changing default usernames:** All Windows systems have a username of "administrator" by default. It is important to rename that account to hide the account name and make it harder for someone to log on as administrator.
- **Disabling guest account:** Most operating systems have a guest account that can be used to connect to the system without needing an actual username and password. Ensure that the guest account is disabled on all systems so that a username and password are required to access the system.
- **Requiring a screen saver password:** Be sure to have a screen saver kick in after a small period of inactivity (5 or 10 minutes). Also make sure that a password is required to use the system after the screen saver has become active. This limits who can use the system if an employee leaves the system temporarily.
- **Disabling autorun:** If you disable autorun on the system, you have a bit of protection against an employee using a CD/DVD with malicious software from automatically executing.

## Introduction to Incident Response

*Incident response* is how you respond to security incidents within the organization. It is critical that you have an incident response procedure in place so that when a security incident occurs, employees know how to report the incident and the security officers know how to handle the incident.

A *security incident* could be an employee noticing that her account has been locked out, a system that has been infected with a virus, or a user who receives a phishing e-mail, or it could be related to a user accessing prohibited content or performing prohibited activity on the network. You will respond to each of these incidents in different ways.

### The first response

Although each type of incident will be handled in a different way, the overall process is similar with all security incidents. Handling a security incident starts with the first responder. The role of the first responder is as follows:

- **Identify:** The first step in handling an incident is to identify that the incident has occurred and to contain that incident. For example, when looking at logs, you notice that Sue has been surfing inappropriate content, so you contain the incident by blocking her system from Internet access.
- **Report through proper channels:** When an incident has been identified, all employees should understand how to report the incident. For example, an end user should know who he should report a security incident to as well as to the network administrators. Typically the user may report a problem to the network administrator, and upon looking into the problem, if the network administrator notices that the problem is security related, he would notify the security officer within the company.
- **Data/device preservation:** The goal of containment is to prevent the security incident from becoming a bigger problem, but you are also trying to preserve the state of the system. For example, if the system was hit with a virus, you would disconnect the system from the network to prevent the system from infecting the rest of the network. But if you noticed that the system was hacked into, you are disconnecting the system from the network to prevent the hacker from having continued access to the system. Disconnecting the system can prevent the hacker from destroying logs on the system along with other important data on the device.

## Documentation

When responding to problems or security incidents, you can typically solve a lot of recurring problems by looking to problem-solving documentation systems. Most large companies log all problems including security incidents so that when a problem arises, the administrator troubleshooting the problem can search the documentation system for related problems. If a match is found, the documentation can give the responder a number of steps to perform to respond to the incident.

If the company invests in a documentation system to help solve problems, it is important to train all administrators on how to record problems and solutions into the system. You also need to ensure that the administrators are updating the documentation as new problems arise or different solutions are found to existing problems. The documentation system is useless without the documentation!

## Chain of custody

When responding to incidents, it is important to collect evidence of the incident. The evidence could be an employee’s mobile device such as a phone or laptop, or it could be log files on a web server. When you collect the evidence, you must “bag and tag” the evidence and store it in a secure location at all times.

It is critical that you track the evidence location at all times so that you validate the integrity of the evidence. When collecting the evidence, have forms that are filled out describing the evidence and label the bag with an evidence ID number.

The most critical part of collecting evidence is to have a chain of custody document that lists where the evidence was at all times. If someone takes the evidence out of the secure location to review it, he must fill out the chain of custody to indicate when he took the evidence, when it was returned, and where it was at all times.

# 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. Here some key points to remember when preparing for the exam:

- *Authentication* is the process of proving an identity to the network, but *authorization* is the process of determining whether accessing a resource is allowed after authentication takes place.
- Hackers take many different approaches to compromise a system. Protect your environment from both network-based and software-based attacks, and make sure 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 might 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 as well as creating redundant disk solutions.

Fundamentals of Security

# 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 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

*6* **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

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

**A** ❍ Full backup
**B** ❍ Incremental backup
**C** ❍ Differential backup
**D** ❍ Copy

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

**A** ❍ DoS
**B** ❍ IPSec
**C** ❍ Smart card
**D** ❍ SSL

*9* **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.

*10* **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

# 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 occurs 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 the system's processing power or bandwidth so that it cannot 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 **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."*

6 **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."*

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

8 **D.** Secure Socket Layer (SSL) is used to encrypt Web traffic. You can identify whether you are on a secure Web site by looking for the lock icon at the bottom of the screen. *Peruse "Methods of Securing Transmissions."*

9 **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."*

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