Chapter 19

REVIEWING THE BASICS

1. What encryption protocol does Windows XP use when sending an account name and password to a domain controller for validation?

Kerberos

2. Which policy in Group Policy must be enabled before you can monitor failed attempts at logging onto a Windows 2000/XP system?

Audit policy

3. Define and explain the differences between viruses, worms, logic bombs, and Trojans.

A virus is a program that can replicate by attaching itself to another program. A worm can spread copies of itself throughout a network without a host program. A Trojan horse, like a worm, does not need a host program to work; it substitutes itself for, and pretends to be, a legitimate program. A logic bomb is dormant code added to software and triggered by a predetermined event.

4. Where can viruses hide?

Viruses can hide in the boot sector, in a file, in a macro within a file, or in a combination of the boot sector and a file (for a multipartite virus).

5. What is the best way to protect a computer or network against worms?

Use a firewall.

6. What is the best way to determine if an e-mail message warning about a virus is a hoax?

Check Web sites on the Internet that track virus hoaxes.

7. Are boot sector viruses limited to hard drives? Explain.

No. On a floppy disk, a boot sector virus hides in the boot program of the boot sector.

8. Which feature must you disable in the Folders Options applet of Control Panel before you can control which user group or user has access to a shared file or folder?

Simple file sharing

9. What is the most likely way that a virus will get access to your computer?

From an e-mail message

10. List three products to remove malicious software that can deal with adware and spyware.

Ad-Aware, Spybot Search and Destroy, Windows Defender

11. Why is it best to run AV software in Safe Mode?

Because malware is less likely to be running in the background to prevent AV software from detecting it

12. Which Windows tool do you use to view a recorded log of network activity?

Event Viewer

13. What registry key keeps information about services that run when a computer is booted into Safe Mode?

HKLM\System\CurrentControlSet\Control\SafeBoot

14. What does AV software look for to determine that a program or a process is a virus?

A virus signature

15. What Windows tool can you use to solve a problem of an error message displayed at startup just after your AV software has removed malware?

Msconfig

16. What folder is used by Windows to hold System Restore restore points?

\System Volume Information

17. How can you delete all restore points and clean up the restore points data storage area?

Turn off System Restore and reboot the system.

18. What two methods does anti-rootkit software use to detect a rootkit?

- The software looks for running processes that do not match up with the underlying program filename.
- The software compares files, registry entries, and processes provided by the OS to the lists it generates from the raw data. If the two lists differ, a rootkit is suspected.

19. Name two anti-rootkit products.

Rootkit Revealer by Sysinternals (*www.sysinternals.com*)

BackLight by F-Secure (*www.f-secure.com*)

20. What is the major disadvantage of using an AV software installation CD to install the AV software to rid a system of viruses?

The software on the CD will not contain the latest virus signatures and other software *updates*; therefore, the AV software will not catch new viruses. For best results, after the AV software is installed, you must download the latest updates to the software.

21. Why does having Windows display known file extensions help prevent a system from being infected with malware?

It helps prevent a system from being infected because users are less likely to be deceived that a file is actually a program or script, rather than a graphics file, some other innocent file type, or URL.

22. How does a rootkit running in user mode normally hide?

By intercepting API calls

23. What is the difference between spyware and adware?

Spyware looks for information about you to pass to a Web site. Adware is displaying annoying ads on your PC. One is stealing information; the other is giving information.

24. For what is the Windows Scripting Host utility used, and what is the command line to execute it?

The Windows Scripting Host utility uses Windows commands to execute scripts that programmers have written using a scripting language such as VBScript or Jscript. To run the script, type wscript.exe filename in the Run dialog box.

25. Why is using an ActiveX control considered a security risk?

It is considered a security risk because it allows a Web page to execute code (which may be malicious) on a user's computer.

26. What must you do before you can use the Windows Backup utility on a Windows XP Home Edition PC?

Install the utility from the Windows XP setup CD.

27. Name one browser other than Internet Explorer by Microsoft.

Firefox by Mozilla

28. Name two e-mail clients other than Outlook or Outlook Express by Microsoft.

Eudora by Qualcomm and Thunderbird by Mozilla

29. What are five file extensions that might be used for scripts?

.js, .jse, .vbe, .vbs, and .wsf

30. Why might someone see better security when using a browser other than Internet Explorer?

It is because authors of malware attack IE more than other products, IE allows Web pages to run ActiveX code, and IE is closely integrated with—and may provide access to—core components of the Windows operating system.

THINKING CRITICALLY

1. A virus has attacked your hard drive and now when you start up Windows, instead of seeing a Windows desktop, the system freezes and you see a "blue screen of death" (an error message on a blue background). You have extremely important document files on the drive that you cannot afford to lose. What do you do first?

a. Try a data recovery service even though it is very expensive.

b. Remove the hard drive from the computer case and install it in another computer.

c. Try GetDataBack by Runtime Software (*www.runtime.org*) to recover the data.

d. Use Windows utilities to attempt to fix the Windows boot problem.

e. Run antivirus software to remove the virus.

Because recovering the data is certainly the top priority, you do not want to do anything to risk doing further damage to this data. The choice that is least likely to affect the data is to remove the hard drive from this computer case and install it in another computer. Then boot into Windows and try copying the data from the bad hard drive to the good drive.

2. Just after you reboot after running AV software, an error message is displayed that contains a reference to a strange DLL file that is missing. What do you do first?

a. Run the AV software again.

b. Run Msconfig and look for startup entries that are launching the DLL.

c. Run Regedit and look for keys that refer to the DLL.

d. Search the Internet for information about the DLL.

Either run Msconfig and look for startup entries that are launching the DLL or search the Internet for information about the DLL. Both are good choices.

3. Suppose a user has encrypted important data files and now is no longer working for your company. How do you decrypt these files so they can be read?

Log on as an administrator and decrypt the files, either by changing the properties of the folder the files are in or by using the Cipher command.