Answers to Additional Exercises

Chapter 1

▸ Answers will vary. One possible drawing will look similar to Figure 1.2 as a triangle with three sides of confidentiality, integrity, and availability.

▸ Answers will vary. You can use the steps in the “Reducing the Attack Surface” section of this chapter. After opening the file, search for “SMTPSVC”.

▸ Answers will vary. You can use the steps in the “Reducing the Attack Surface” section of this chapter. After opening the file, search for “Logon” in the Microsoft.OS.Audit section. If it lists Success="True", then successful logon events are logged. If it lists Failure="True", then unsuccessful logon events are logged.

▸ Answers will vary. On Windows 2008, you can choose Start ➢ Administrative Tools ➢ Windows Firewall With Advanced Security. This will indicate either Windows Firewall Is On or Windows Firewall Is Off.

Chapter 2

▸ You can read about the tool and download it here: www.microsoft.com/security/malwareremove. After downloading it, double-click it to run it. After the intro screen, you’ll be prompted to choose a scan. Pick Quick Scan, and click Next.

▸ Answers will vary. The MessageLabs site (hosted by Symantec) includes an Intelligence Reports page with reports on current threats, available here: www.messagelabs.com/resources/mlireports

▸ Answers will vary. You can view the SIR page here: www.microsoft.com/security/sir

▸ You can locate the rogue security software section within the SIR Malware category here: www.microsoft.com/security/sir/guide/default.aspx#section_4_4
Appendix C • Answers to Additional Exercises

Chapter 3

► The site shows the following results:
  ► password is weak.
  ► Password is weak.
  ► Password1 is weak.
  ► Pa$$w0rd1 is medium.
  ► Pa$$w0rdPa$$w0rd is strong.

► Follow one of the procedures in the “Creating Strong Passwords” section.
► Follow the steps listed in the “Creating a Password-Reset Disk” section.
► Click Start, and right-click any application on the Start menu. Most applications include
  the Run As Administrator command. If you have Administrator credentials, you can enter
  them and run the application as an administrator.

Chapter 4

► Use Windows Explorer to create the folder. Check the permissions by right-clicking the
  folder, selecting Properties, and selecting the Security tab. Inherited permissions are as
  follows: Administrators and System have Full Control; Users have Read, Read & Execute,
  and List Folder Contents; and Creator Owner has Special Permissions (which equate to
  Full Control in this case). If the default permissions on the root of the drive have been
  modified, your results may be different.

► The default permissions are Read for the Everyone group.

► The Delegation of Control Wizard is the tool used to assign permissions in Active Directory
  Users and Computers. It’s accessed by right-clicking over an OU and selecting Delegate
  Control.

► Answers may vary. By default, the user’s account and the Administrators group will have
  Full Control.

Chapter 5

► Use Windows Explorer to create the folder, and then enable auditing on the folder using
  the steps in the “Enabling Object Access Auditing” section. Enable auditing in the Local
  Security Policy for Object Access auditing using the steps in the “Enabling Auditing”
  section.
Launch the Event Viewer, and view the Security log.

Follow the steps in the “Viewing Audit Information” section. When entering the event ID numbers, enter 4000-5000.

Enable auditing in the Local Security Policy for successful system events. Launch the Event Viewer, and look for event ID 1102 in the Security log.

Chapter 6

Use the procedure outlined in the “Modifying User Account Control” section.

Use the procedure outlined in the “Updating Systems with Automatic Updates” section.

Use the procedure outlined in the “Encrypting Offline Folders” section.

Launch the Local Security Policy, and browse to the node shown in Figure 6.10. This node is empty if software restriction policies aren’t defined locally.

Chapter 7

A search on Bing for “ping of death” shows multiple pages describing this vulnerability. It uses malformed packets that can cause problems when a system tries to handle it. This is one of the common attacks that Microsoft’s Forefront Threat Management Gateway can detect, as described here: http://technet.microsoft.com/en-us/library/cc984458.aspx.

These are well-known ports for NetBIOS. You can identify the well-known ports and their matching protocols here: www.iana.org/assignments/port-numbers.

Answers may vary, but they should resemble either Figure 7.4 or 7.5.

A search on Bing for “dnssec root dns” shows multiple pages. http://www.root-dnssec.org/ provides a high-level timeline and shows that it was deployed to all DNS root servers in 2010 (as deliberately unvalidatable root zone DURZ).

Chapter 8

The WEP security algorithm is the least secure. The WPA protocol is more secure than WEP. WPA2 is more secure than both.

Answers will vary. Many people are running WEP without understanding all of its vulnerabilities.
Answers will vary. If the system supports WPA2, use WPA2. You’ll need to configure each device to match the security protocol used on the WAP or wireless router.

Answers will vary. By default, MAC filtering is disabled on most, if not all, wireless routers and wireless access points.

Chapter 9

Answers will vary. They could include fences, lighting, cameras, guards, cipher locks, card readers, motion detectors, and more.

Answers will vary. If you have physical access to the networking closet or server room, you can inspect it. If not, you may need to ask IT personnel if hubs are used. Many organizations don’t use hubs for security, but some organizations still use them due to the low cost.

You can use the steps in the “Using Group Policy to Enhance Computer Security” section. Use the Allow Log On Locally setting.

Answers will vary. Many of today’s phones can be password-protected.

Chapter 10

Symmetric encryption uses a single key for encryption and decryption. Asymmetric encryption uses two keys (a public key and a private key) for encryption and decryption.

Answers will vary. The capability is often available for users within organizations but not available by default for home users. In Outlook 2010, you can use the following steps:

1. Create a new email. Enter a To address.
2. Select the Options tab, and click More Options.
3. Click the Security Settings button.
4. Click the Change Settings button.
5. Click Choose next to the Signing Certificate. If a certificate is available that is associated with your email address, you can select it and digitally sign emails.

You can use the steps in the “Understanding EFS” section to encrypt the folder. The file will be green, indicating that it’s encrypted.

You can use the steps in the “Using BitLocker To Go” section of the chapter.
Chapter 11

- You can use the steps in the “Viewing Certificate Properties” section to view the Trusted Root Certification Authority store. Any Microsoft system will have root certificates from Microsoft unless they were removed.

- You can use the steps in the “Viewing Certificate Properties” section to view the Trusted Root Certification Authority store. Almost all systems have root certificates from VeriSign.

- There will be an error with the certificate similar to that shown in Figure 11.5.

Chapter 12

- You can use the steps in the “Selecting Cookies Settings” section of this chapter.

- You can use the steps in the “Deleting Browser History” section of this chapter to delete temporary data and then use the steps in the “Selecting Cookies Settings” section to see that the cookies have been deleted.

- You can use the steps in the “Using InPrivate Filtering and InPrivate Browsing” section. You’ll see that the browsing experience isn’t really any different even though user data isn’t retained on the system.

- You can use the procedure described in the “Comparing Security Zones” section. By default, ActiveX controls are blocked for the restricted sites zone.