This appendix contains the tables and lists that are part of the Exam Preparation Tasks in each chapter. The following tables and lists cover key topics but are incomplete. Fill them in and check your answers against the complete tables and lists in Appendix B, "Memory Tables Answer Key," on the DVD. The complete tables and lists also appear in the book's chapters.

APPENDIX A

Memory Tables

Chapter 2

Table 2-1 Summary of Malware Threats

Malware Threat	Definition	Example
Virus		
	Similar to viruses except that it self-replicates whereas a virus does not.	Nimda Propagated through network shares and mass e-mailing
	Appears to perform desired functions but are actually performing malicious functions behind the scenes.	
Spyware		Internet Optimizer (aka DyFuCA)
	Software designed to gain administrator-level control over a computer system without being detected.	
Spam		Phishing identity theft e-mails Lottery scam e-mails

Table 2-2 Summary of Malware Prevention Techniques

Malware Threat	Prevention Techniques
Virus	
Worm	
Trojan horse	
Spyware	
Rootkit	
Spam	

Chapter 3

Patch Management

Fill-in the second and fourth phases of patch management, as well as descriptions of each.

- **Planning—**Before actually doing anything, a plan should be set into motion. The first thing that needs to be decided is whether the patch is necessary and if it will be compatible with other systems. Microsoft Baseline Security Analyzer (MBSA) is one example of a program that can identify security misconfigurations on the computers in your network, letting you know if patching is needed. If the patch is deemed necessary, the plan should consist of a way to test the patch in a "clean" network on clean systems, how and when the patch will be implemented, and how the patch will be checked after it is installed.
- _____
  _____
  _____
  _____
  _____
- **Implementing—**If the test is successful, the patch should be deployed to all the necessary systems. In many cases, this will be done in the evening or over the weekend for larger updates. Patches can be deployed automatically using software such as Microsoft's Systems Management Server (SMS).
- _____
  _____
  _____
  _____
  _____

Keeping a Well-Maintained Computer

Fill in the fourth and sixth steps for keeping a well-maintained computer, as well as descriptions of each.

Step 1. **Use a surge protector or UPS—**Make sure the computer and other equipment connect to a surge protector, or better yet a UPS if you are concerned about power loss.

Step 2. **Update the BIOS—**Flashing the BIOS isn't always necessary; check the manufacturer's website for your motherboard to see if an update is needed.

Step 3. **Update Windows—**This includes the latest SPs and any Windows updates beyond that and setting Windows to alert if there are any new updates.

Step 4. _____

_____

_____

_____

_____

Step 5. **Update the firewall—**Be sure to have some kind of firewall installed and enabled; then update it. If it is the Windows Firewall, updates should happen automatically through Windows Update. However, if you have a SOHO router with a built-in firewall, or other firewall device, you need to update the device's ROM by downloading the latest image from the manufacturer's website.

Step 6. _____

_____

_____

_____

_____

Step 7. **(Optional) Create an image of the system**—After all your configurations and hardening of the OS are complete, you might consider creating an image of the system. Imaging the system is like taking a snapshot of the entire system partition. That information is saved as one large file or a set of compressed files that can be saved anywhere. It's kind of like system restore but at another level. The beauty of this is that you can reinstall the entire image if your system fails or is compromised, quickly and efficiently, with very little configuration necessary[md]only the latest security and AV updates since the image was created need to be applied. Of course, most imaging software has a price tag involved, but it can be well worth it if you are concerned about the time it would take to get your system back up and running in the event of a failure. This is the basis for standardized images in many organizations. By applying mandated security configurations, updates, and so on, and then taking an image of the system, you can create a snapshot in time that you can easily revert to if necessary, while being confident that a certain level of security is already embedded into the image.

Chapter 4

Table 4-1 Common Applications and Safeguards

Application Name	Safeguards
Outlook	_____
	_____
	Keep Office up to date with Windows Update. (This also applies to all Office suite applications.)
	_____
	Read messages in plain text instead of HTML.
	_____
	Use a version that enables Object model guard functionality, or download it for older versions.
	_____
	Consider encrypting the authentication scheme, and possibly other traffic, including message traffic between Outlook clients and Exchange servers. Secure Password Authentication (SPA) can be used to secure the login and S/MIME, and PGP can be used to secure actual e-mail transmissions.
Word	_____
	_____
	Use read-only or comments only (tracking changes) settings.
	_____
Excel	Use password protection on worksheets.
	_____
	Consider Excel encryption.

Table 4-2 Summary of Programming Vulnerabilities and Attacks

Vulnerability	Description
	Placed by programmers, knowingly or inadvertently, to bypass normal authentication, and other security mechanisms in place
	When a process stores data outside the memory that the developer intended
	Exploits the trust a user's browser has in a website through code injection, often in web forms
	Exploits the trust that a website has in a user's browser, which becomes compromised and transmits unauthorized commands to the website
	User input in database web forms is not filtered correctly and is executed improperly
	A method of accessing unauthorized parent (or worse, root) directories

Chapter 5

Table 5-1 Private IP Ranges (as Assigned by the IANA)

IP Class	Assigned Range
Class A	
Class B	
Class C	

Table 5-2 Types of IPv6 Addresses

IPv6 Type	Address Range	Purpose
Unicast	Global Unicast starts at 2000	
	Structured like unicast addresses	Address assigned to a group of interfaces on multiple nodes. Packets are delivered to the "first" interface only.
Multicast	FF00::/8	

Table 5-4 Port Ranges

Port Range	Category Type	Description
	Well-Known Ports	This range defines commonly used protocols, for example HTTP uses port 80. They are designated by the IANA (Internet Assigned Numbers Authority), which is operated by the ICANN (Internet Corporation for Assigned Names and Numbers).
1024–49,151	Registered Ports	These must be registered with the IANA. For example, Microsoft registered 3,389 for use with the Remote Desktop Protocol (RDP), aka Microsoft Terminal Server.
49,152–65,535		These ports can be used by applications but cannot be registered by vendors.

Table 5-5 Ports and Their Associated Protocols

Port Number	Associated Protocol (or Keyword)	Full Name	Usage
	Echo	Echo	Testing round trip times between hosts.
19	CHARGEN	Character Generator	Testing and debugging.
21		File Transfer Protocol	Transfers files from host to host.
	SSH		Remotely administers network devices and Unix/Linux systems. Also used by Secure copy (SCP) and Secure FTP (SFTP).
23	Telnet	TErminaL NETwork	Remotely administers network devices (deprecated).
25	SMTP	Simple Mail Transfer Protocol	Sends email.
	TACACS	Terminal Access Controller Access-Control System	Remote authentication.

continues

Table 5-5 Continued

Port Number	Associated Protocol (or Keyword)	Full Name	Usage
53			Resolves IP addresses to host names.
69	TFTP	Trivial File Transfer Protocol	Basic version of FTP.
80	HTTP	Hypertext Transfer Protocol	Transmits web page data.
	Kerberos	Kerberos	Network authentication, uses tickets.
110	POP3		Receives email.
119	NNTP	Network News Transfer Protocol	Transports Usenet articles.
135	RPC/epmap/ dcom-scm	Microsoft End Point Mapper/ DCE Endpoint Resolution	Used to locate DCOM ports. Also known as RPC (Remote Procedure Call).
137-139	NetBIOS	NetBIOS Name, Datagram, and Session Services, respectively	Name querying, sending data, NetBIOS connections.
143	IMAP		Retrieval of email with advantages over POP3.
161		Simple Network Management Protocol	Remotely monitor network devices.
		Lightweight Directory Access Protocol	Maintains directories of users and other objects.
443	HTTPS	Hypertext Transfer Protocol Secure (uses TLS or SSL)	Secure transfer of hypertext through web pages. Used by FTPS.
445	SMB		Provides shared access to files and other resources.
636	LDAP over TLS/SSL	Lightweight Directory Access Protocol (over TLS/SSL)	Secure version of LDAP.
1433	Ms-sql-s	Microsoft SQL Server	Opens queries to SQL server.
	L2TP		VPN protocol with no inherent security. Often used with IPsec.
1723	PPTP	Point-to-Point Tunneling Protocol	VPN protocol with built-in security.
3389	RDP		Remotely views and controls other systems.

Chapter 6

Table 6-1 Summary of NIDS Versus NIPS

Type of System	Summary	Disadvantage/Advantage	Example
NIDS		Pro: Only a limited amount of NIDS are necessary on a network.	Snort Bro-IDS
NIPS		Pro: Detects and mitigates malicious activity.	Dragon IPS McAfee IntruShield
		Con: Uses more resources.	

Chapter 7

Table 7-1 Weak, Strong, and Stronger Passwords

Password	Strength of Password
Prowse	Weak
DavidProwse	
1ocrian7	
This1sV#ryS3cure	

Privilege Escalation

Describe the following terms:

- **Vertical privilege escalation**

- **Horizontal privilege escalation**

  _____

  _____

  _____

  This can be done through hacking or by a person walking over to other people's computers and simply reading their e-mail! Always have your users lock their computer (or log off) when they are not physically at their desk!

Table 7-2 Wireless Protocols

Wireless Protocol	Description	Encryption Level (Key Size)
WEP	Wired Equivalent Privacy (Deprecated)	
WPA		128-bit
WPA2		
TKIP	Temporal Key Integrity Protocol (Deprecated) Encryption protocol used with WEP and WPA	128-bit
	Counter Mode with Cipher Block Chaining Message Authentication Code Protocol Encryption protocol used with WPA2 Addresses the vulnerabilities of TKIP Meets requirements of IEEE 802.11i	
AES	_____ Encryption protocol used with WPA/WPA2 Strongest encryption method in this table	

Chapter 8

Table 8-1 VPN Tunneling Protocols

Tunneling Protocol	Description	Port Used
Point-to-Point Tunneling Protocol (PPTP)	This is the more commonly used tunneling protocol (although that is quickly changing) but the less secure solution of the two listed here. PPTP generally includes security mechanisms and no additional software or protocols need to be loaded. PPTP works within the Point-to-Point Protocol (PPP) that is also used for dial-up connections, as we mentioned earlier.	

Tunneling Protocol	Description	Port Used
Layer 2 Tunneling Protocol (L2TP)	This is quickly gaining popularity due to the inclusion of IPSec as its security protocol. Although this is a separate protocol and L2TP doesn't have any inherent security, L2TP will be considered the more secure solution because IPSec is required in most L2TP implementations.	

Table 8-2 Summary of Authentication Technologies

Authentication Type	Description
	An IEEE standard that defines port-based Network Access Control (PNAC). 802.1X is a Data Link Layer authentication technology used to connect devices to a LAN or WLAN.
	An Application Layer protocol used for accessing and modifying directory services data. It is part of the TCP/IP suite. Originally used in WAN connections, it has morphed into a protocol commonly used by services such as Microsoft Active Directory.
	An authentication protocol designed at MIT that enables computers to prove their identity to each other in a secure manner. It is used most often in a client-server environment; the client and the server both verify each other's identity.
	A service that enables dial-up and various types of VPN connections from remote clients.
	An authentication scheme used by the Point-to-Point Protocol (PPP) that is the standard for dial-up connections. It utilizes a challenge-response mechanism with one-way encryption.
	Used to provide centralized administration of dial-up, VPN, and wireless authentication. It can be used with EAP and 802.1X.
	Another remote authentication protocol, similar to RADIUS, and used more often in UNIX networks though it is deprecated.
	Remote authentication developed by Cisco, similar to RADIUS but separates authentication and authorization into two separate processes.

Chapter 9

Mandatory Access Control

Describe the following terms:

- **Rule-based access control**

  _____
  _____
  _____
  _____

- **Lattice-based access control**

  _____
  _____
  _____
  _____

Table 9-1 Summary of Access Control Models

Tunneling Protocol	Key Points
DAC	Permissions are determined by the owner.
_____	Permissions are determined by the system. Can be rule-based or lattice-based. _____ _____
RBAC	Based on roles, or sets of permissions involved in an operation.

Here are a couple more tips when it comes to user accounts, passwords, and logons. Fill in the title for each description.

- _____— It's nice that Windows has incorporated a separate administrator account: The problem is that by default the account has no password. To configure this account, navigate to **Computer Management > System Tools > Local Users and Groups > Users** and locate the **Administrator** account. In a domain this would be in **ADUC > Domain name > Users**. By right-clicking the account, you see a drop-down menu in which you can rename it and/or give it a password. (Just remember the new username and password!) Now it's great to have this additional administrator account on the shelf just in case the primary account fails; however, some OSs such as Vista disable the account by default. To enable it, right-click the account and select **Properties**. In the General tab, deselect the

Account Is Disabled check box. Alternatively, open the command line and type **net user administrator /active:yes**. The way that the administrator account behaves by default will depend on the version of Windows. The Linux/UNIX counterpart is the root account. The same types of measures should be employed when dealing with this account.

- _____— This can be done by right-clicking the account in question, selecting **Properties** and then selecting the checkbox named **Account Is Disabled**. It is also possible to delete accounts (aside from built-in accounts such as the Guest account): however, companies usually opt to have them disabled instead so that the company can retain information linking to the account. So if an employee is terminated, the system administrator should generally implement the policy of account disablement. By disabling the account, the employee in question will no longer be able to log in to the network, but the system administrator will still have access to the history of that account.
- _____— Pressing Ctrl+Alt+Del before the logon adds a layer of security to the logon process. This can be added as a policy on individual Windows computers. It is implemented by default with computers that are members of a domain.
- _____— Policies governing user accounts, passwords, and so on can help you to enforce your rules, as discussed in the next section. Large organizations with a lot of users will usually implement a self-service password management system. This means that users reset their own passwords after a given amount of time (set in a group policy); the administrator does not create passwords for users.

Chapter 10

Table 10-2 Summary of Risk Assessment Types

Risk Assessment Type	Description	Key Points
Qualitative risk assessment	Assigns numeric values to the probability of a risk, and the impact it can have on the system or network.	_____ _____ _____
_____ _____	Measures risk by using exact monetary values. It attempts to give an expected yearly loss in dollars for any given risk.	_____ _____ _____

Table 10-3 Summary of Chapter 10 Security Tools

Security Tool	Description
LAN Surveyor	
Network Magic	Network mapping tool
	Network diagramming tool
Nessus	
Nmap	Port scanner
Wireshark	
Fluke	Handheld protocol analyzer/network sniffer
	Password cracking tool
John the Ripper	

Chapter 11

Table 11-1 Summary of Monitoring Methodologies

Monitoring Methodology	Description
	Network traffic is analyzed for predetermined attack patterns. These attack patterns are known as signatures.
Anomaly-Based Monitoring	_____ _____ _____ _____
	Looks at the previous behavior of applications, executables, and/or the operating system and compares that to current activity on the system. If an application later behaves improperly, the monitoring system will attempt to stop the behavior.

Network adapters can work in one of two different modes: promiscuous and non-promiscuous. Define each.

- **Promiscuous mode**

  _____
  _____
  _____

- **Non-promiscuous mode**

  _____
  _____
  _____

Chapter 12

Table 12-3 Summary of Symmetric Algorithms

Algorithm Acronym	Full Name	Maximum/Typical Key Size
DES	_____	56-bit
	Triple DES	168-bit
AES	_____	_____
RC4	Rivest Cipher version 4	_____ typical
RC5	Rivest Cipher version 5	_____ typical
RC6	Rivest Cipher version 6	_____ typical

Chapter 14

Table 14.1 Continued

RAID Level	Description	Fault Tolerant?	Minimum Number of Disks
_____	Striping Data is striped across multiple disks to increase performance.	No	Two
_____	_____ Data is copied to two identical disks. If one disk fails, the other continues to operate. See Figure 14-1 for an illustration. This RAID version allows for the least amount of downtime because there is a complete copy of the data ready to at a moment's notice. When each disk is connected to a separate controller, this is known as disk duplexing.	Yes	_____
RAID 5	_____ Data is striped across multiple disks; fault-tolerant parity data is also written to each disk. If one disk fails, the array can reconstruct the data from the parity information. See Figure 14-2 for an illustration.	Yes	Three
_____	Striping with Double Parity Data is striped across multiple disks as it is in RAID 5, but there are two stripes of parity information. This usually requires another disk in the array. This system can operate even with two failed drives and is more adequate for time-critical systems.	_____	Four
_____	Combines the advantages of RAID 0 and RAID 1. Requires a minimum of four disks. This system contains two RAID 0 striped sets. Those two sets are mirrored.	Yes	_____

Table 14.1 Continued

RAID Level	Description	Fault Tolerant?	Minimum Number of Disks
RAID 1+0	Combines the advantages of RAID 1 and RAID 0. Requires a minimum of two disks but will usually have four or more. This system contains at least two mirrored disks that are then striped.	Yes	Two (usually four)

Redundant Sites

Describe the following types of sites:

- **Hot site**

_____
_____
_____
_____
_____
_____
_____
_____

- **Warm site**

_____
_____
_____
_____
_____
_____
_____

- **Cold site**

_____
_____
_____
_____
_____
_____

Data Backup

Describe the following types of backups:

- **Full backup**

- **Incremental backup**

- **Differential backup**

Other Backup Schemes

Describe the following backup schemes:

- **10 tape rotation**

- **Grandfather-father-son**

- **Towers of Hanoi**

Chapter 15

Table 15-1 Summary of Social Engineering Types

Type	Description
_____	When a person invents a scenario, or pretext, in the hope of persuading a victim to divulge information.
Diversion theft	When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location.
Phishing	
Hoax	The attempt at deceiving people into believing something that is false.
_____	When a person uses direct observation to find out a target's password, PIN, or other such authentication information.
Eavesdropping	When a person uses direct observation to "listen" in to a conversation. This could be a person hiding around the corner or a person tapping into a phone conversation.
_____	When a person literally scavenges for private information in garbage and recyclable containers.
Baiting	
_____	When an unauthorized person tags along with an authorized person to gain entry to a restricted area.

Table 15-4 Acts Passed Concerning the Disclosure of Data and PII

Act	Acronym	Description
	n/a	Establishes a code of fair information practice. Governs the collection, use, and dissemination of personally identifiable information about persons' records maintained by federal agencies.
		Governs the disclosure of financial and accounting information. Enacted in 2002.
		Governs the disclosure and protection of health information. Enacted in 1996.
		Enables commercial banks, investment banks, securities firms, and insurance companies to consolidate. Protects against pretexting. Individuals need proper authority to gain access to nonpublic information such as Social Security numbers.
		Requires California businesses that store computerized personal information to immediately disclose breaches of security. Enacted in 2003.

Table 15-5 Summary of Policy Types

Type	Description
	Policy that defines the rules that restrict how a computer, network, or other system may be used.
Change management	
	When more than one person is required to complete a task
Job rotation	When a particular task is rotated among a group of employees
Mandatory vacations	
Due diligence	Ensuring that IT infrastructure risks are known and managed
	The mitigation action that an organization takes to defend against the risks that have been uncovered during due diligence
	The principle that an organization must respect and safeguard personnel's rights