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.
## Memory Tables

### Chapter 2

**Table 2-1** Summary of Malware Threats

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

<table>
<thead>
<tr>
<th>Application Name</th>
<th>Safeguards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Outlook</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Keep Office up to date with Windows Update. (This also applies to all Office suite applications.)</td>
</tr>
<tr>
<td></td>
<td>Read messages in plain text instead of HTML.</td>
</tr>
<tr>
<td></td>
<td>Use a version that enables Object model guard functionality, or download it for older versions.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>Word</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use read-only or comments only (tracking changes) settings.</td>
</tr>
<tr>
<td>Excel</td>
<td>Use password protection on worksheets.</td>
</tr>
<tr>
<td></td>
<td>Consider Excel encryption.</td>
</tr>
</tbody>
</table>
Table 4-2  Summary of Programming Vulnerabilities and Attacks

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

Chapter 5

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

<table>
<thead>
<tr>
<th>IP Class</th>
<th>Assigned Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class A</td>
<td></td>
</tr>
<tr>
<td>Class B</td>
<td></td>
</tr>
<tr>
<td>Class C</td>
<td></td>
</tr>
</tbody>
</table>

Table 5-2  Types of IPv6 Addresses

<table>
<thead>
<tr>
<th>IPv6 Type</th>
<th>Address Range</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unicast</td>
<td>Global Unicast starts at 2000</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Structured like unicast addresses</td>
<td>Address assigned to a group of interfaces on multiple nodes. Packets are delivered to the “first” interface only.</td>
</tr>
<tr>
<td>Multicast</td>
<td>FF00::/8</td>
<td></td>
</tr>
</tbody>
</table>
### Table 5-4  Port Ranges

<table>
<thead>
<tr>
<th>Port Range</th>
<th>Category Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Well-Known Ports</td>
<td>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).</td>
</tr>
<tr>
<td>1024–49,151</td>
<td>Registered Ports</td>
<td>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.</td>
</tr>
<tr>
<td>49,152–65,535</td>
<td></td>
<td>These ports can be used by applications but cannot be registered by vendors.</td>
</tr>
</tbody>
</table>

### Table 5-5  Ports and Their Associated Protocols

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

*continues*
<table>
<thead>
<tr>
<th>Port Number</th>
<th>Associated Protocol (or Keyword)</th>
<th>Full Name</th>
<th>Usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>53</td>
<td>Resolves IP addresses to host names.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>69</td>
<td>TFTP</td>
<td>Trivial File Transfer Protocol</td>
<td>Basic version of FTP.</td>
</tr>
<tr>
<td>80</td>
<td>HTTP</td>
<td>Hypertext Transfer Protocol</td>
<td>Transmits web page data.</td>
</tr>
<tr>
<td></td>
<td>Kerberos</td>
<td>Kerberos</td>
<td>Network authentication, uses tickets.</td>
</tr>
<tr>
<td>110</td>
<td>POP3</td>
<td>Receives email.</td>
<td></td>
</tr>
<tr>
<td>119</td>
<td>NNTP</td>
<td>Network News Transfer Protocol</td>
<td>Transports Usenet articles.</td>
</tr>
<tr>
<td>135</td>
<td>RPC/epmap/dcom-scm</td>
<td>Microsoft End Point Mapper/ DCE Endpoint Resolution</td>
<td>Used to locate DCOM ports. Also known as RPC (Remote Procedure Call).</td>
</tr>
<tr>
<td>137-139</td>
<td>NetBIOS</td>
<td>NetBIOS Name, Datagram, and Session Services, respectively</td>
<td>Name querying, sending data, NetBIOS connections.</td>
</tr>
<tr>
<td>143</td>
<td>IMAP</td>
<td>Retrieval of email with advantages over POP3.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lightweight Directory Access Protocol</td>
<td>Maintains directories of users and other objects.</td>
<td></td>
</tr>
<tr>
<td>443</td>
<td>HTTPS</td>
<td>Hypertext Transfer Protocol Secure (uses TLS or SSL)</td>
<td>Secure transfer of hypertext through web pages. Used by FTPS.</td>
</tr>
<tr>
<td>445</td>
<td>SMB</td>
<td>Provides shared access to files and other resources.</td>
<td></td>
</tr>
<tr>
<td>1433</td>
<td>Ms-sql-s</td>
<td>Microsoft SQL Server</td>
<td>Opens queries to SQL server.</td>
</tr>
<tr>
<td></td>
<td>L2TP</td>
<td>VPN protocol with no inherent security. Often used with IPsec.</td>
<td></td>
</tr>
<tr>
<td>1723</td>
<td>PPTP</td>
<td>Point-to-Point Tunneling Protocol</td>
<td>VPN protocol with built-in security.</td>
</tr>
<tr>
<td>3389</td>
<td>RDP</td>
<td>Remotely views and controls other systems.</td>
<td></td>
</tr>
</tbody>
</table>
Chapter 6

Table 6-1  Summary of NIDS Versus NIPS

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

Chapter 7

Table 7-1  Weak, Strong, and Stronger Passwords

<table>
<thead>
<tr>
<th>Password</th>
<th>Strength of Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prowse</td>
<td>Weak</td>
</tr>
<tr>
<td>DavidProwse</td>
<td></td>
</tr>
<tr>
<td>locrian7</td>
<td></td>
</tr>
<tr>
<td>This1sV#ryS3cure</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Wireless Protocol</th>
<th>Encryption Level (Key Size)</th>
</tr>
</thead>
<tbody>
<tr>
<td>WEP (Depreciated)</td>
<td>Wired Equivalent Privacy</td>
</tr>
<tr>
<td>WPA</td>
<td>128-bit Encryption protocol used with WEP and WPA</td>
</tr>
<tr>
<td>TKIP (Depreciated)</td>
<td>Temporal Key Integrity Protocol Encryption protocol used with WEP and WPA</td>
</tr>
<tr>
<td></td>
<td>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</td>
</tr>
<tr>
<td>AES</td>
<td>Encryption protocol used with WPA/WPA2 Strongest encryption method in this table</td>
</tr>
</tbody>
</table>

Table 8-1 VPN Tunneling Protocols

<table>
<thead>
<tr>
<th>Tunneling Protocol</th>
<th>Description</th>
<th>Port Used</th>
</tr>
</thead>
<tbody>
<tr>
<td>Point-to-Point Tunneling Protocol (PPTP)</td>
<td>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.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 8-2  Summary of Authentication Technologies

<table>
<thead>
<tr>
<th>Authentication Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>802.1X</td>
<td>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.</td>
</tr>
<tr>
<td>LDAP</td>
<td>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.</td>
</tr>
<tr>
<td>Kerberos</td>
<td>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.</td>
</tr>
<tr>
<td>PPTP</td>
<td>A service that enables dial-up and various types of VPN connections from remote clients.</td>
</tr>
<tr>
<td>PAP</td>
<td>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.</td>
</tr>
<tr>
<td>Radius</td>
<td>Used to provide centralized administration of dial-up, VPN, and wireless authentication. It can be used with EAP and 802.1X.</td>
</tr>
<tr>
<td>CHAP</td>
<td>Another remote authentication protocol, similar to RADIUS, and used more often in UNIX networks though it is deprecated.</td>
</tr>
<tr>
<td>Cisco Radius</td>
<td>Remote authentication developed by Cisco, similar to RADIUS but separates authentication and authorization into two separate processes.</td>
</tr>
</tbody>
</table>

### Tunneling Protocol

<table>
<thead>
<tr>
<th>Tunneling Protocol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Layer 2 Tunneling Protocol (L2TP)</td>
<td>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.</td>
</tr>
</tbody>
</table>
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

<table>
<thead>
<tr>
<th>Tunneling Protocol</th>
<th>Key Points</th>
</tr>
</thead>
<tbody>
<tr>
<td>DAC</td>
<td>Permissions are determined by the owner.</td>
</tr>
<tr>
<td></td>
<td>Permissions are determined by the system.</td>
</tr>
<tr>
<td></td>
<td>Can be rule-based or lattice-based.</td>
</tr>
<tr>
<td>RBAC</td>
<td>Based on roles, or sets of permissions involved in an operation.</td>
</tr>
</tbody>
</table>

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 \texttt{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.

\section*{Chapter 10}

\begin{table}[ht]
\centering
\caption{Summary of Risk Assessment Types}
\begin{tabular}{|l|p{3in}|p{3in}|}
\hline
Risk Assessment Type & Description & Key Points \\
\hline
Qualitative risk assessment & Assigns numeric values to the probability of a risk, and the impact it can have on the system or network. & \\
\hline
& Measures risk by using exact monetary values. It attempts to give an expected yearly loss in dollars for any given risk. & \\
\hline
\end{tabular}
\end{table}
Table 10-3  Summary of Chapter 10 Security Tools

<table>
<thead>
<tr>
<th>Security Tool</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LAN Surveyor</td>
<td></td>
</tr>
<tr>
<td>Network Magic</td>
<td>Network mapping tool</td>
</tr>
<tr>
<td></td>
<td>Network diagramming tool</td>
</tr>
<tr>
<td>Nessus</td>
<td></td>
</tr>
<tr>
<td>Nmap</td>
<td>Port scanner</td>
</tr>
<tr>
<td>Wireshark</td>
<td></td>
</tr>
<tr>
<td>Fluke</td>
<td>Handheld protocol analyzer/network sniffer</td>
</tr>
<tr>
<td></td>
<td>Password cracking tool</td>
</tr>
<tr>
<td>John the Ripper</td>
<td></td>
</tr>
</tbody>
</table>

Chapter 11

Table 11-1  Summary of Monitoring Methodologies

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

<table>
<thead>
<tr>
<th>Algorithm Acronym</th>
<th>Full Name</th>
<th>Maximum/Typical Key Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>DES</td>
<td>❌</td>
<td>56-bit</td>
</tr>
<tr>
<td></td>
<td>Triple DES</td>
<td>168-bit</td>
</tr>
<tr>
<td>AES</td>
<td>❌</td>
<td></td>
</tr>
<tr>
<td>RC4</td>
<td>Rivest Cipher version 4</td>
<td>❌ typical</td>
</tr>
<tr>
<td>RC5</td>
<td>Rivest Cipher version 5</td>
<td>❌ typical</td>
</tr>
<tr>
<td>RC6</td>
<td>Rivest Cipher version 6</td>
<td>❌ typical</td>
</tr>
</tbody>
</table>
## Table 14.1

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>Description</th>
<th>Fault Tolerant?</th>
<th>Minimum Number of Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>__________</td>
<td>___________</td>
<td>_______________</td>
<td>_______________</td>
</tr>
<tr>
<td>__________</td>
<td>___________</td>
<td>_______________</td>
<td>_______________</td>
</tr>
</tbody>
</table>

### Table 14.1 Continued

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>Description</th>
<th>Fault Tolerant?</th>
<th>Minimum Number of Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>__________</td>
<td>___________</td>
<td>_______________</td>
<td>_______________</td>
</tr>
</tbody>
</table>

| RAID 5 | ___________ | Yes | Three |
|--------|_____________|-----|-------|

<table>
<thead>
<tr>
<th>__________</th>
<th>Striping with Double Parity</th>
<th>___________</th>
<th>Four</th>
</tr>
</thead>
</table>

| __________ | 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. | ___________ | 
|------------|-----------------------------------------------------------------|--------------|------|

Data is striped across multiple disks to increase performance.

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.

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.

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.
Table 14.1  Continued

<table>
<thead>
<tr>
<th>RAID Level</th>
<th>Description</th>
<th>Fault Tolerant?</th>
<th>Minimum Number of Disks</th>
</tr>
</thead>
<tbody>
<tr>
<td>RAID 1+0</td>
<td>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.</td>
<td>Yes</td>
<td>Two (usually four)</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>When a person invents a scenario, or pretext, in the hope of persuading a victim to divulge information.</td>
</tr>
<tr>
<td>Diversion theft</td>
<td>When a thief attempts to take responsibility for a shipment by diverting the delivery to a nearby location.</td>
</tr>
<tr>
<td>Phishing</td>
<td></td>
</tr>
<tr>
<td>Hoax</td>
<td>The attempt at deceiving people into believing something that is false.</td>
</tr>
<tr>
<td></td>
<td>When a person uses direct observation to find out a target’s password, PIN, or other such authentication information.</td>
</tr>
<tr>
<td>Eavesdropping</td>
<td>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.</td>
</tr>
<tr>
<td></td>
<td>When a person literally scavenges for private information in garbage and recyclable containers.</td>
</tr>
<tr>
<td>Baiting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>When an unauthorized person tags along with an authorized person to gain entry to a restricted area.</td>
</tr>
</tbody>
</table>
Table 15-4  Acts Passed Concerning the Disclosure of Data and PII

<table>
<thead>
<tr>
<th>Act</th>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>n/a</td>
<td></td>
<td>Establishes a code of fair information practice.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Governs the disclosure and protection of health information. Enacted in 1996.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enables commercial banks, investment banks, securities firms, and insurance companies to consolidate.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Protects against pretexting. Individuals need proper authority to gain access to nonpublic information such as Social Security numbers.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Requires California businesses that store computerized personal information to immediately disclose breaches of security.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Enacted in 2003.</td>
</tr>
</tbody>
</table>

Table 15-5  Summary of Policy Types

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