Appendix A

Answers to the Review Questions

Chapter 1

1. **B, D, and F.** Confidentiality, integrity, and availability (known as CIA, the CIA triad, and the security triangle) are the three main goals when it comes to information security. Another goal within information security is accountability.
2. **A.** To protect against malicious attacks, think like a hacker. Then, protect and secure like a network security administrator.
3. **B.** You should use non-repudiation to prevent Tom from denying that he sent the e-mails.
4. **C.** Availability is what the *A* in CIA stands for, as in "the availability of data." Together the acronym stands for confidentiality, integrity, and availability. Although accountability is important and is often included as a fourth component of the CIA triad, it is not the best answer. Assessment and auditing are both important concepts when checking for vulnerabilities and reviewing and logging, but they are not considered to be part of the CIA triad.
5. **C.** For removable storage, the confidentiality of data is the greatest risk because removable storage can easily be removed from the building and shared with others. Although the other factors of the CIA triad are important, any theft of removable storage can destroy the confidentiality of data, and that makes it the greatest risk.
6. **D.** The *I* in CIA stands for integrity. The acronym CIA stands for confidentiality, integrity, and availability. Accountability is also a core principle of information security.
7. **C.** An ID card is an example of a physical security control. Passwords and encryption are examples of technical controls. A disaster recovery plan (DRP) is an example of an administrative control.
8. **B.** The recipient should be concerned about the integrity of the message. If the e-mail client application cannot verify the digital signature of the sender of the e-mail, then there is a chance that the e-mail either was intercepted or is coming from a separate dangerous source. Remember, integrity means the reliability of the data, and whether or not it has been modified or compromised by a third party before arriving at its final destination.
9. **C.** There is a concern about data confidentiality with cloud computing because multiple customers are sharing physical hard drive space. A good portion of customers run their cloud-based systems in virtual machines. Some virtual machines could run on the very same hard drive (or very same array of hard drives). If one of the customers had the notion, he could attempt to break through the barriers between virtual machines, which if not secured properly, would not be very difficult to do.
10. **B.** A script kiddie uses code and probably doesn't understand how it works and what the repercussions will be. Other actors such as hackers, hacktivists, insiders, and so on will usually have a higher level of sophistication when it comes to technology. An advanced persistent threat (APT) is a group of technical processes or the entity that implements those processes. An APT is just that—advanced—and is on the other side of the spectrum from the script kiddie.
11. **D.** A system can never truly be completely secure. The scales are always tipping back and forth; a hacker develops a way to break into a system, then an administrator finds a way to block that attack, and then the hacker looks for an alternative method. It goes on and on; be ready to wage the eternal battle!

Chapter 2

1. **A.** A botnet is a group of compromised computers, usually working together, with malware that was installed by a worm or a Trojan horse. An individual computer within a botnet is referred to as a zombie (among other things). A virus is code that can infect a computer's files. A rootkit is a type of software designed to gain administrator-level access to a system.
2. **C.** Zombies (also known as zombie computers) are systems that have been compromised without the knowledge of the owner. A prerequisite is the computer must be connected to the Internet so that the hacker or malicious attack can make its way to the computer and be controlled remotely. Multiple zombies working in concert often form a botnet. See the section "Delivery of Malware" in Chapter 2 for more information.
3. **A.** You should use a recovery environment. Most often, this would be the one built into Windows. Many manufacturers suggest using this, and more specifically Safe Mode. However, it could also be a Linux rescue disc or flash drive. That's not a true dual-boot though. An actual dual-boot is when Windows and Linux are both installed to the hard drive. Command Prompt only is not enough, nor is it necessary for some virus scanning scenarios. Booting into Windows normally is tantamount to doing nothing. Remember to use a recovery environment when scanning for viruses.
4. **D.** Pop-up windows are common to spyware. The rest of the answers are more common symptoms of viruses.
5. **B.** A worm is most likely the reason that the server is being bombarded with information by the clients; perhaps it is perpetuated by a botnet. Because worms self-replicate, the damage can quickly become critical.
6. **D.** A web browser (for example, Internet Explorer) is the only one listed that is not an example of malicious software. Although a browser can be compromised in a variety of ways by malicious software, the application itself is not the malware.
7. **D.** A DDoS, or distributed denial-of-service, attack uses multiple computers to make its attack, usually perpetuated on a server. None of the other answers use multiple computers.
8. **D.** A logic bomb is a malicious attack that executes at a specific time. Viruses normally execute when a user inadvertently runs them. Worms can self-replicate at will. Ransomware is a type of malware that restricts access to files (or entire systems) and demands a ransom be paid.
9. **A.** Active interception normally includes a computer placed between the sender and the receiver to capture information. All other statements concerning active interception are false. If a person overhears a conversation it can be considered eavesdropping. When a person looks through files it could be normal or malicious. When a person hardens an operating system, that person is making it more secure. We discuss these concepts as we progress through the book.
10. **C.** Malware scanners can locate rootkits and other types of malware. These types of scanners are often found in anti-malware software from manufacturers such as McAfee, Symantec, and so on. Adware scanners (often free) can scan for only adware. Always have some kind of anti-malware software running on live client computers!
11. **A.** Worms self-replicate and do not require a user to execute a program to distribute the software across networks. All the other answers do require user intervention. Stealth refers to a type of virus.
12. **B.** Closing open relays, whitelisting, and blacklisting are all mitigation techniques that address spam. Spam e-mail is a serious problem for all companies and must be filtered as much as possible.
13. **B.** E-mail is the number one reason why network-based viruses spread. All a person needs to do is double-click the attachment within the e-mail, and the virus will do its thing, which is

most likely to spread through the user's address book. Removable media such as optical discs and USB flash drives can spread viruses but are not nearly as common as e-mail. A virus can also spread if it was incorporated into a link within an instant message, or as an attachment to the IM. This is definitely something to protect against, but not quite as common as e-mail-based viruses, especially in larger organizations' networks.

14. **A.** The primary difference between a Trojan horse and a worm is that worms will self-replicate without any user intervention; Trojan horses do not self-replicate.
15. **D.** An armored virus attempts to make disassembly difficult for an antivirus software program. It thwarts attempts at code examination. Stealth viruses attempt to avoid detection by antivirus software altogether. Polymorphic viruses change every time they run. Worms are not viruses.
16. **C.** A Trojan, or a Trojan horse, appears to be legitimate and looks like it'll perform desirable functions, but in reality is designed to enable unauthorized access to the user's computer.
17. **A and C.** Because a virus can affect many users, technical support resources can be consumed by an increase in user phone calls. This can be detrimental to the company because all companies have a limited number of technical support personnel. Another detrimental effect is that unwitting users may be tricked into changing some of their computer system configurations. The key term in the question is "virus hoax." The technical support team might also be inundated by support e-mails from users, but not to the point where the e-mail server capacity is consumed. If the e-mail server is consumed by message traffic, that would be a detrimental effect caused by the person who sent the virus and by the virus itself but not necessarily by the hoax. Although users may be at risk for identity theft, it is not one of the most detrimental effects of the virus hoax.
18. **D.** A Trojan was probably installed (unknown to the user) as part of the keygen package. Illegal downloads often contain malware of this nature. At this point, the computer is compromised. Not only is it infected, but malicious individuals might be able to remotely access it.
19. **C.** The computer is probably now part of a botnet. The reason the system is running slowly is probably due to the fact that there are hundreds of outbound connections to various websites. This is a solid sign of a computer that has become part of a botnet. Spyware, viruses, and rootkits might make the computer run slowly, but they will not create hundreds of outbound connections.
20. **A.** Of the answers listed, the download most likely contains spyware. It could contain other types of malware as well, such as viruses, Trojans, worms, and so on. The rest of the answers are types of network attacks and methods of accessing the computer to drop a malware payload. A DDoS is a distributed denial-of-service attack, which uses many computers to attack a single target. Smurf is an example of a DDoS. We'll talk more about these in Chapter 7. Backdoors are vulnerabilities in code that can allow a hacker (or even the programmer) administrative access to an operating system. Logic bombs are ways of delivering malware; they are based on timing.
21. **D.** The chain messages are e-mails (similar to the archaic chain *letter*) that are being spammed on the network. Therefore, anti-spam security controls need to be implemented. This would be a type of preventive control. Antivirus programs find and quarantine viruses, worms, and Trojans, but unless they are part of an AV suite of software, they will not check e-mail. Anti-spyware tools will attempt to prevent spyware from being installed on the computer. Host-based firewalls block attacks from coming through specific ports, but will not catch spam messages. However, a HIDS (host-based intrusion detection system) could possibly detect spam, and a HIPS (host-based intrusion prevention system) might even prevent or quarantine it. We'll discuss host-based firewalls, HIDS, and HIPS more in Chapter 3.

22. **B.** Most likely, a rootkit was installed. These can evade many routine scans, so there is no fault here. It's just that more in-depth analysis was required to find the rootkit. The hidden processes are the main indicator of the rootkit. Spam is simply harassment by e-mail (and other messaging systems), to put it nicely. Backdoors are programmed ways to bypass security of an operating system. A logic bomb is code that defines when a particular type of malware will execute. Ransomware is when a computer is operationally held hostage; files are not retrievable by the user (because they have been encrypted) until a ransom is paid. It's important to run in-depth scans periodically. They can be time consuming, but they can uncover many threats and vulnerabilities that would otherwise go unnoticed. We'll discuss these types of scans more in Chapters 12 and 13.

Chapter 3

1. **A and D.** Host-based intrusion detection systems (HIDSs) run within the operating system of a computer. Because of this, they can slow a computer's performance. Most HIDS do not detect network attacks well (if at all). However, a HIDS can detect operating system attacks and will usually have a high level of detection for those attacks.
2. **A and D.** Configuring a supervisor password in the BIOS disallows any other user to enter the BIOS and make changes. Setting the hard drive first in the BIOS boot order disables any other devices from being booted off, including floppy drives, optical drives, and USB flash drives. BIOS shadowing doesn't have anything to do with computer security, and although flashing the BIOS may include some security updates, it's not the best answer.
3. **B and C.** By disabling all USB devices in the BIOS, a user cannot use his flash drive. Also, the user cannot use the device if you disable the USB root hub within the operating system. RBAC, which stands for role-based access control, defines access to networks by the person's role in the organization (we will cover this more later in the book). MAC filtering is a method of filtering out computers when they attempt to access the network (using the MAC addresses of those computers).
4. **A and C.** Bluesnarfing and bluejacking are the names of a couple of Bluetooth threats. Another attack could be aimed at a Bluetooth device's discovery mode. To date there is no such thing as blue bearding, and a distributed denial-of-service attack uses multiple computers to attack one host.
5. **B.** A password should be set on the phone, and the phone should lock after a set period of time. When the user wants to use the phone again, the user should be prompted for a password. Disabling the data connection altogether would make access to e-mail impossible on the smartphone. Smartphone encryption of data is possible, but it could use a lot of processing power that may make it unfeasible. Whether the smartphone is used only for company use is up to the policies of the company.
6. **B.** When using an IDS, particular types of traffic patterns refer to signature-based IDS.
7. **A.** Device encryption is the best solution listed to protect the confidentiality of data. By encrypting the data, it makes it much more difficult for a malicious person to make use of the data. Screen locks are a good idea but are much easier to get past than encryption. Antivirus software will not stop an attacker from getting to the data once the mobile device has been stolen. Remote sanitization (remote wipe) doesn't keep the data confidential; it removes it altogether! While this could be considered a type of confidentiality, it would only be so if a good backup plan was instituted. Regardless, the best answer with confidentiality in mind is encryption. For example, if the device was simply lost, and was later found, it could be reused (as long as it wasn't tampered with). But if the device was sanitized, it would have to be reloaded and reconfigured before being used again.
8. **B.** A TPM, or trusted platform module, is a chip that resides on the motherboard of the laptop. It generates cryptographic keys that allow the entire disk to be encrypted, as in full

disk encryption (FDE). Hardware security modules (HSMs) and USB encryption require additional hardware. A host-based intrusion detection system requires either additional software or hardware.

9. **A.** If the device has been lost and you need to be 100% sure that data cannot be retrieved from it, then you should remotely sanitize (or remotely "wipe") the device. This removes all data to the point where it cannot be reconstructed by normal means. GPS tracking might find the device, but as time is spent tracking and acquiring the device, the data could be stolen. Encryption is a good idea, but over time encryption can be deciphered. Screen locks can be easily circumvented.
10. **B.** Geotagging is a concern based on a user taking pictures with a mobile device such as a smartphone. This is because the act of geotagging utilizes GPS, which can give away the location of the user. Application whitelisting is when there is an approved list of applications for use by mobile devices. Usually implemented as a policy, if the mobile device attempts to open an app that is not on the list, the process will fail, or the system will ask for proof of administrative identity. BYOD stands for bring your own device, a technological concept where organizations allow employees to bring their personal mobile devices to work and use them for work purposes. MDM stands for mobile device management, a system that enables a security administrator to configure, update, and secure multiple mobile devices from a central location.
11. **A and E.** Remote wipe and encryption are the best methods to protect a stolen device's confidential or sensitive information. GPS can help to locate a device, but it can also be a security vulnerability in general; this will depend on the scenario in which the mobile device is used. Passwords should never be e-mailed and should not be associated with e-mail. Tethering is when a mobile device is connected to another computer (usually via USB) so that the other computer can share Internet access, or other similar sharing functionality in one direction or the other. This is great as far as functionality goes, but more often than not can be a security vulnerability. Screen locks are a decent method of reducing the chance of login by the average person, but they are not much of a deterrent for the persistent attacker.
12. **B and E.** When encrypting a smartphone, the security administrator should encrypt internal memory and any long-term storage such as removable media cards. The admin must remember that data can be stored on both. Public keys are already encrypted; it is part of their inherent nature. Smartphones don't necessarily use an MBR the way Windows computers do, but regardless, if the internal memory has been encrypted, any boot sector should be secured. Images based on steganography, by their very nature, are encrypted through obfuscation. It is different from typical data encryption, but it's a type of cryptography nonetheless.
13. **A.** By implementing individual file encryption (such as EFS) on files that are stored on a disk encrypted with whole disk encryption, the files will remain encrypted (through EFS) even if they are copied to a separate drive that does not use whole disk encryption. However, running two types of encryption will usually *increase* processing overhead, not reduce it. NTFS permissions aren't relevant here; however, if files are copied to an external drive, those files by default lose their NTFS permissions and inherit new permissions from the parent folder on the new drive. We'll discuss NTFS permissions more in Chapter 11. We shouldn't call this *double* encryption—rather, the files are encrypted twice separately. The bit strength is not cumulative in this example, but there are two layers of encryption, which is an example of defense in depth and security layering.
14. **C.** To meet regulations, a properly configured host-based firewall will be required on the computers that will be transacting business by credit card over the Internet. All of the other answers—antivirus updates, NIDS, and HIPS—are good ideas to secure the system (and/or network), but they do not address the core issue of filtering ports, which is the primary purpose of the firewall. Also, a network-based firewall will often not be secure enough to meet regulations, thus the need for the extra layer of protection on the individual computers.

15. **C.** Of the answers listed, the USB mass storage device would be the most likely asset to be considered for data loss prevention (DLP). It's the only device listed in the answers that should have any real organizational data! A proxy server temporarily caches such data as HTTP and FTP. A print server forwards printed documents to the correct printer (again the data is usually held temporarily). An application server contains programs, but usually doesn't store organizational data files. It's the devices and computers that store actual company data files that we are primarily concerned with.

Chapter 4

1. **C.** By using a virtual machine (which is one example of a virtual instance), any ill effects can be compartmentalized to that particular virtual machine, usually without any ill effects to the main operating system on the computer. Patching a computer does not automatically patch virtual machines existing on the computer. Other virtual machines can be compromised, especially if nothing is done about the problem. Finally, virtual machines can definitely be affected by hacking techniques. Be sure to secure them!
2. **A.** Virtualization enables a person to install operating systems (or applications) in an isolated area of the computer's hard drive, separate from the computer's main operating system.
3. **C.** The Network and Sharing Center is where you can disable file sharing in Windows. It can be accessed indirectly from the Control Panel as well. By disabling file sharing, you disallow any (normal) connections to data on the computer. This can be very useful for computers with confidential information, such as an executive's laptop or a developer's computer.
4. **A.** To hide bootmgr, you either need to click the radio button for Don't Show Hidden Files, Folders, or Drives or enable the Hide Protected Operating System Files checkbox.
5. **A and B.** Two ways to harden an operating system include installing the latest updates and installing Windows Defender. However, virtualization is a separate concept altogether; it can be used to create a compartmentalized OS, but needs to be secured and hardened just like any other OS. PHP scripts will generally not be used to harden an operating system. In fact, they can be vulnerabilities to websites and other applications.
6. **B.** NTFS is the most secure file system for use with today's Windows. FAT and FAT32 are older file systems, and DFS is the distributed file system used in more advanced networking.
7. **A.** The `convert` command is used to upgrade FAT and FAT32 volumes to the more secure NTFS without loss of data. HPFS is the High Performance File System developed by IBM and is not used by Windows. ext4 is the fourth extended filesystem used by Linux. NFS is the Network File System, something you would see in a storage area network.
8. **D.** NTFS and FAT32 support the same number of file formats, so this is not an advantage of NTFS. However, NTFS supports file encryption, larger file sizes, and larger volumes, making it more advantageous in general in comparison to FAT32, and is capable of higher levels of security, most especially down to the file level.
9. **D.** The biggest risk of running a virtual computer is that it will go offline immediately if the server that it is housed on fails. All other virtual computers on that particular server will also go offline immediately.
10. **D.** The beauty of a virtualized browser is that regardless of whether a virus or other malware damages it, the underlying operating system will remain unharmed. The virtual browser can be deleted and a new one can be created; or if the old virtual browser was backed up before the malware attack, it can be restored. This concept applies to entire virtual operating systems as well, if configured properly.
11. **D.** The System State needs to be backed up on a domain controller to recover the Active Directory database in the future. The System State includes user data and system files but

does not include the entire operating system. If a server fails, the operating system would have to be reinstalled, and then the System State would need to be restored. Consider backing up the system state in the command-line—see the following TechNet link for more: https://technet.microsoft.com/en-us/library/cc753201(v=ws.11).aspx.

12. **C.** A patch can fix a single security issue on a computer. A service pack addresses many issues and rewrites many files on a computer; it may be overkill to use a service pack when only a patch is necessary. Also, only older Windows operating systems (for example, Windows 7 and Windows Server 2008 R2 and previous) use service packs. You might obtain the patch from a support website. A baseline can measure a server or a network and obtain averages of usage.

13. **C.** Often, operating system manufacturers such as Microsoft refer to the attack surface as all the services that run on the operating system. By conducting an analysis of which services are necessary and which are unnecessary, an administrator can find out which ones need to be disabled, thereby reducing the attack surface. Updates, service packs, antivirus software, and network intrusion detection systems (NIDSs) are good tools to use to secure an individual computer and the network but do not help to reduce the size of the attack surface of the operating system.

14. **A.** Virtualization of computer servers enables a network administrator to isolate the various network services and roles that a server may play. Analyzing network traffic would have to do more with assessing risk and vulnerability and monitoring and auditing. Adding network services at lower costs deals more with budgeting than with virtualization, although, virtualization can be less expensive. Centralizing patch management has to do with hardening the operating systems on the network scale.

15. **C.** Patch management is an example of verifying any new changes in software on a test system (or live systems for that matter). Verifying the changes (testing) is the second step of the standard patch management strategy. Application hardening might include updating systems, patching them, and so on, but to be accurate, this question is looking for that particular second step of patch management. Virtualization is the creating of logical OS images within a working operating system. HIDS stands for host-based intrusion detection system, which attempts to detect malicious activity on a computer.

16. **B and D.** Updating the host-based intrusion prevention system is important. Without the latest signatures, the HIPS will not be at its best when it comes to protecting against malware. Also, disabling unused services will reduce the attack surface of the OS, which in turn makes it more difficult for attacks to access the system and run malicious code. Disabling the data loss prevention (DLP) device would not aid the situation, and it would probably cause data leakage from the computer. Installing a perimeter firewall won't block malicious software from entering the individual computer. A personal firewall would better reduce the attack surface of the computer, but it is still not meant as an anti-malware tool. Updating the NIDS signatures will help the entire network, but might not help the individual computer. In this question, we want to focus in on the individual computer, not the network. In fact, given the scenario of the question, you do not even know if a network exists.

17. **A.** The best way to establish host-based security for your organization's workstations is to implement GPOs (Group Policy objects). When done properly from a server, this can harden the operating systems in your network, and you can do it from a central location without having to configure each computer locally. It is the only answer that deals with the client operating systems. The other answers deal with database and web servers, and firewalls that protect the entire network.

18. **B.** Of the answers listed, the only one that will not show the version number is `wf.msc`. That brings up the Windows Firewall with Advanced Security. All of the other answers will display the version number in Windows.

19. **A.** If you migrate some of these low-resource servers to a virtual environment (a very smart thing to do), you could end up spending more on licensing, but less on hardware, due to the very nature of virtualization. In fact, the goal is to have the gains of hardware savings outweigh the losses of licensing. Load balancing and clustering deals with an OS utilizing the hardware of multiple servers. This will not be the case when you go virtual, nor would it have been the case anyway, because clustering and load balancing is used in environments where the server is very resource-intensive. Baselining, unfortunately, will remain the same; you should analyze all of your servers regularly, whether they are physical or virtual. These particular servers should not encounter latency or lowered throughput because they are low-resource servers in the first place. If, however, you considered placing into a virtual environment a Windows Server that supports 5,000 users, you should definitely expect latency.

Chapter 5

1. **D.** Alt+F4 is the key combination that is used to close an active window. Sometimes it is okay to click the X, but malware creators are getting smarter all the time; the X could be a ruse.
2. **B.** SPA (Secure Password Authentication) is a Microsoft protocol used to authenticate e-mail clients. S/MIME and PGP can be used to secure the actual e-mail transmissions.
3. **A and C.** By increasing the Internet zone security level to High, you employ the maximum safeguards for that zone. ActiveX controls can be used for malicious purposes; disabling them makes it so that they do not show up in the browser. Disabling a pop-up blocker and adding malicious sites to the Trusted Sites zone would make a Microsoft-based web browser (such as Internet Explorer) less secure.
4. **A.** Heaps and stacks are data structures that can be affected by buffer overflows. Value types are stored in a stack, whereas reference types are stored in a heap. An ethical coder will try to keep these running efficiently. An unethical coder will attempt to use a buffer overflow to affect heaps and stacks, which in turn could affect the application in question or the operating system. The buffer overflow might be initiated by certain inputs and can be prevented by bounds checking.
5. **B.** The best answer is cookies, which can be used for authentication and session tracking and can be read as plain text. They can be used by spyware and can track people without their permission. It is also wise to delete temporary Internet files as opposed to temporary files.
6. **C.** To run Java applets, a web browser must have that option enabled. Java increases the usability of web-enabled systems, and Java is a programming language. It does not use digital signatures for authentication.
7. **B.** Backdoors were originally created to ease administration. However, attackers quickly found that they could use these backdoors for a malicious attack.
8. **A.** A tracking cookie will be used, or misused, by spyware in an attempt to access a user's activities. Tracking cookies are also known as browser cookies or HTTP cookies, or simply cookies. Shopping carts take advantage of cookies to keep the shopping cart reliable.
9. **C.** When a web script runs in its own environment for the express purpose of not interfering with other processes, it is known as running in a sandbox. Often, the sandbox will be used to create sample scripts before they are actually implemented. Quarantining is a method used to isolate viruses. A honey-net is a collection of servers used to attract attackers and isolate them in an area where they can do no damage. VPN is short for virtual private network, which enables the connection of two hosts from remote networks.
10. **C.** In general, the user should click the padlock in the browser; this will show the certificate information. Often, the address bar will have different colors as the background; for example, green usually means that the certificate is valid, whereas red or pink indicates a problem. Or, you might have to click the name of the website listed in the address bar just before where it says HTTPS to find out the validity of the certificate. Contacting the webmaster and calling

the ISP are time-consuming, not easily done, and not something that an end user should do. Although HTTPS:// can tell a person that the browser is now using Hypertext Transfer Protocol Secure, it does not necessarily determine whether the certificate is valid.

11. **C.** Input validation is the best practice to use when coding applications. This is important when creating web applications or web pages that require information to be inputted by the user.
12. **B.** A gray-box test is when you are given limited information about the system you are testing. Black-box testers are not given logins, source code, or anything else, though they may know the functionality of the system. White-box testers are given logins, source code, documentation, and more. SDLC stands for software development life cycle, of which these types of tests are just a part.
13. **C.** In this case a command was entered, and the attacker was attempting to gain access to the password file within the /etc directory. If the attacker tried to inject code, he would not use commands, but rather PHP, ASP, or another language. SQL injections are usually run on databases, not web servers' HTML forms. Buffer overflows have to do with memory and how applications utilize it.
14. **D.** A buffer overflow can be initiated when a string variable is not programmed correctly—for example, if the variable allows for more than the standard amount of bytes. Directory traversal is when an attacker uses commands and code to access unauthorized parent directories. Command injection is when commands and command syntax are entered into an application or OS. XSS or cross-site scripting is when code is injected into a website form to obtain information and unauthorized access. Zero day attacks are ones that are not known to hardware/software manufacturers when they are launched.
15. **A.** Input validation is the best way to prevent SQL injection attacks on web servers and database servers (or combinations of the two). Host-based firewalls aid in preventing network attacks but not necessarily coded attacks of this type. HTTPS pages initiate a secure transfer of data, but they don't necessarily lock out attackers who plan on using SQL injection. Updating the web server is a good idea, but will have little if any effect on the forms that are written by the web programmer.
16. **B.** Cross-site scripting (XSS) can be initiated on web forms or through e-mail. It often uses JavaScript to accomplish its means. SQL injection is when code (SQL based) is inserted into forms or databases. Cross-site request forgery (XSRF) is when a user's browser sends unauthorized commands to a website, without the user's consent. Directory traversal is when an attacker attempts to gain access to higher directories in an OS. A null pointer dereference is a memory dereference that can result in a memory fault error.
17. **C.** Of the listed answers, secure code review should happen first in the SDLC. It should be followed by fuzzing and penetration testing, in that order. Patch management is a recurring theme until the software meets the end of its life cycle.
18. **B.** The windows that are being displayed are most likely pop-ups. Standard pop-up blockers will prevent most of these. Antivirus software of itself does not have pop-up blocking technology but might be combined in a suite of anti-malware software that does have pop-up blocking capability. Screensavers won't affect the users' web sessions. Host-based firewalls are a good idea and will prevent attacks, but since a firewall will allow the connections that users make to websites, it cannot stop pop-ups.
19. **D.** Buffer overflows can be initiated by sending random data to other services on a computer. While JavaScript is commonly used in XSS attacks, it can also be used to create a buffer overflow. DoS stands for denial-of-service, which is when a computer sends many packets to a server or other important system in the hope of making that system fail. SQL and LDAP injection do not use JavaScript.

20. **A.** Input validation is extremely important when it comes to secure programming. To prevent SQL injection attacks, be sure that the developers have thoroughly tested the web page by validating user input. An IDS can help to detect network attacks, but is not going to help prevent SQL injection. Eliminating XSS vulnerabilities might just happen to help with all types of code injection, but you can't be sure. You should validate inputs specifically for each attack. A firewall may stop some network-based attacks, but not coded attacks.
21. **B.** Fuzzing (or fuzz testing) is when a person, or more commonly an automated system, enters random data into a form or application in an effort to test it. XSRF (cross-site request forgery, also abbreviated as CSRF) is an exploit of a website where unauthorized commands are issued from a trusted user. Hardening is the act of securing an operating system or application. Input validation is when forms and other web pages are checked to make sure that they will filter inputted data properly, and is used in conjunction with fuzzing.
22. **D.** You should employ application hardening. This means updating the application, configuring strong passwords, applying policies if necessary, and in general, configuring the settings of the application securely. Network penetration testing is when a group of tools is used to see if a host has open ports or other vulnerabilities. Input validation is when the code of a form is checked to make sure it filters user input correctly. Application whitelisting is when only specific applications are allowed to be run, usually enforced by computer policy.
23. **A.** Anti-spyware can be used to trigger security alerts in case a user's web browser accesses a web page that includes a tracking cookie. Anti-spam software can possibly trigger alerts when an e-mail appears to be spam (or simply move it to a junk folder automatically). Firewalls can be configured to send alerts to security administrators, but usually they concern an IP address that attempted to gain access to the network.
24. **D.** This would be an example of gray-box testing. The IT auditor is not an employee of the company (which is often a requirement for white-box testing) but rather an outside consultant. Being an outside consultant, the IT auditor should not be given confidential details of the system to be tested. However, the auditor was given a real login, so the auditor cannot be employing black-box testing. Penetration testing might be occurring in this scenario as well—this is when an auditor, or other security expert, tests servers' network connections for vulnerabilities. But the scenario only states that the auditor is testing an application.
25. **C.** Configuration management encompasses application patch management and other ways of hardening an OS or application. Policy management is considered separate because it can be used to harden or *soften* a system; plus, it is best done at a server—affecting many systems at once. Fuzzing (or fuzz testing) is the act of providing random data to a computer program, testing it in an automated fashion. Virtualization is the term used to refer to any virtual computing platform.

Chapter 6

1. **A.** A DMZ, or demilitarized zone, can be set up on a SOHO router (in the firewall portion) to create a sort of safe haven for servers. It is neither the LAN nor the Internet, but instead, a location in between the two.
2. **C.** 172.16.0.1 is the only address listed that is private. The private assigned ranges can be seen in Table 6-2. 11.16.0.1 is a public IPv4 address, as is 208.0.0.1. 127.0.0.1 is the IPv4 loopback address.
3. **B.** NAT (network address translation) hides an entire network of IP addresses. SPI, or Stateful Packet Inspection, is the other type of firewall that today's SOHO routers incorporate. Secure Shell (SSH) is a protocol used to log in to remote systems securely over the network. The File Transfer Protocol (FTP) is used to copy files from one system to a remote system.

4. **A.** Static network address translation normally uses a one-to-one mapping when dealing with IP addresses.
5. **A.** A demilitarized zone, or DMZ, can be placed between the LAN and the Internet; this is known as a back-to-back perimeter configuration. This allows external users on the Internet to access services but segments access to the internal network. In some cases, it will be part of a 3-leg firewall scheme. Host-based intrusion detection systems are placed on an individual computer, usually within the LAN. Domain controllers should be protected and are normally on the LAN as well. An extranet can include parts of the Internet and parts of one or more LANs; normally it connects two companies utilizing the power of the Internet.
6. **A.** A switch can reduce network traffic on a particular network segment. It does this by keeping a table of information about computers on that segment. Instead of broadcasting information to all ports of the switch, the switch selectively chooses where the information goes.
7. **A.** Loop protection should be enabled on the switch to prevent the looping that can occur when a person connects both ends of a network cable to the same switch. A DMZ is a demilitarized zone that is used to keep servers in a midway zone between the Internet and the LAN. VLAN segregation (or VLAN separation) is a way of preventing ARP poisoning. Port forwarding refers to logical ports associated with protocols.
8. **D.** IPv6 uses a long string of numbers and letters in the IP address. These addresses are 128-bit in length. IPv4 addresses are shorter (32-bit) and are numeric only. ICMP is the Internet Control Message Protocol, which is used by `ping` and other commands. IPv3 was a test version prior to IPv4 and was similar in IP addressing structure.
9. **C.** Platform as a service (PaaS) is a cloud computing service that offers many software solutions, including easy-to-configure operating systems and on-demand computing. SaaS is software as a service, used to offer solutions such as webmail. IaaS is infrastructure as a service, used for networking and storage. VM stands for virtual machine, which is something that PaaS also offers.
10. **C.** Common Vulnerabilities and Exposures (CVE) can be included in Microsoft Security Bulletins and will be listed for other web server products such as Apache. PHP and CGI are pseudo-programming languages used within HTML for websites. Both can contain harmful scripts if used inappropriately. Transport Layer Security (TLS) is a protocol used by sites secured by HTTPS.
11. **D.** The firewall is the device most likely to have a separate DMZ interface. Switches connect computers on the LAN. VoIP phones are used by individuals to make and answer phone calls on a Voice over IP connection. A proxy server acts as a go-between for the clients on the LAN and the web servers that they connect to, and caches web content for faster access.
12. **C and D.** The hosts using the IP addresses 10.36.36.166 and 10.36.36.184 would be able to communicate with each other because they are on the same subnet (known as subnet ID 5). All of the other answer choices' IP addresses are on different subnets, so they would not be able to communicate with each other (or with the IP addresses of the correct answers) by default. Table 1 provides the complete list of subnets and their ranges for this particular subnetted network. It is noteworthy that the answer 10.36.36.224 is not even usable because it is the first IP of one of the subnets. Remember that the general rule is: you can't use the first and last IP within each subnet. That is because they are reserved for the subnet ID and the broadcast addresses, respectively.

Table 1 List of Subnets for 10.36.36.0/27 (255.255.255.224 Subnet Mask)

Subnet ID	Mathematical IP Range	Usable IP Range
ID 0	10.36.36.0–10.36.36.31	10.36.36.1–10.36.36.30
ID 1	10.36.36.32–10.36.36.63	10.36.36.33–10.36.36.62
ID 2	10.36.36.64–10.36.36.95	10.36.36.65–10.36.36.94
ID 3	10.36.36.96–10.36.36.127	10.36.36.97–10.36.36.126
ID 4	10.36.36.128–10.36.36.159	10.36.36.129–10.36.36.158
ID 5	10.36.36.160–10.36.36.191	10.36.36.161–10.36.36.190
ID 6	10.36.36.192–10.36.36.223	10.36.36.193–10.36.36.222
ID 7	10.36.36.224–10.36.36.255	10.36.36.225–10.36.36.254

13. **A.** The virtual switch is the best option. This virtual device will connect the virtual servers together without being routable to the firewall (by default). Removing the virtual network from the routing table is another possibility; but if you have not created a virtual switch yet, it should not be necessary. A physical standalone switch won't be able to connect the virtual servers together; a virtual switch (or individual virtual connections) is required. Creating a VLAN would also require a physical switch. In that scenario, you can have multiple virtual LANs each containing physical computers (not virtual computers), and each working off of the same physical switch. That answer would keep the VLAN from being routable to the firewall, but not virtual servers.

14. **B.** The IT director is most likely proposing that you use infrastructure as a service (IaaS). A cloud-based service, IaaS is often used to house servers (within virtual machines) that store developed applications. It differs from PaaS in that it is the servers, and already developed applications, that are being moved from the server room to the cloud. However, PaaS might also be required if the applications require further development. The most basic cloud-based service, software as a service (SaaS), is when users work with applications (often web-based) that are provided from the cloud. A community cloud is when multiple organizations share certain aspects of a public cloud.

15. **C.** The demilitarized zone (DMZ) is the best option in this scenario. By creating a DMZ, and placing the front-end servers within it (on a separate branch of the firewall), you create a type of compartmentalization between the LAN (important internal resources) and the front-end servers. A VLAN is used to separate a LAN into multiple virtual units. Virtualization is a general term that usually refers to the virtualizing of operating systems. Cloud computing is another possible option in this scenario, because you could take the front-end servers and move them to the cloud. However, a certain level of control is lost when this is done, whereas with a DMZ, the security analyst still retains complete control.

16. **D.** The best option is to create two VLANs on the switch (one for the VoIP phones, and one for the PCs) and make sure that the switch is connected to the router. Configure access control lists (ACLs) as necessary on the router to allow or disallow connectivity and traffic between the two VLANs. Installing a firewall and configuring ACLs on that firewall is a possibility, but you would also have to use two separate dedicated switches if VLANs are not employed. This is a valid option, but requires additional equipment, whereas creating the two VLANs requires no additional equipment (as long as the switch has VLAN functionality). While subnetting is a possible option, it is more elaborate than required. The VLAN (in this case port-based) works very well in this scenario and is the best option.

17. **C.** The address in the response is a truncated IPv6 address. You can tell it is an IPv6 address because of the hexadecimal numbering, the separation with colons, and the groups of four digits. You can tell it is truncated because of the single zero and the double colon.

A MAC address is also hexadecimal and can use colons to separate the groups of numbers (though hyphens often are used), but the numbers are grouped in twos. An example is 00-1C-C0-A1-54-15. The loopback address is a testing address for the local computer. In IPv6 it is simply ::1, whereas in IPv4 it is 127.0.0.1. Finally, IPv4 addresses in general are 32-bit dotted-decimal numbers such as 192.168.1.100.

18. **A.** The only one of the listed answers that you can infer from the log is that the router implements network address translation (NAT). You can tell this from the first line of the log, which shows the inside of the router using the 192.168.1.1 IP address and the outside using 10.254.254.1. NAT is occurring between the two at the router. This allows the IP 192.168.1.105 to communicate with 10.254.254.10 ultimately. However, the rest of the logs only show the first step of that communication between 10.254.254.10 and the router at 10.254.254.1.

    What's really happening here? The router is showing that port 3030 is being used on 10.254.254.1. That is the port used by an online game known as netPanzer as well as a mass-e-mailing backdoor worm. The client (10.254.254.10) is using port 80 to make a web-based connection to the game. You can see the three-way TCP handshake occurring with the SYN, SYN/ACK, and ACK packets. Ultimately, 10.254.254.10 is communicating with 192.168.1.105, but we only see the first stage of that communication to the router. As a security analyst you would most likely want to shut down the use of port 3030, so that employees can be more productive and you have less overall chance of a network breach.

    As far as the incorrect answers, the router definitely is not filtering out port 80, as traffic is successfully being sent on that port. 192.168.1.105 is not a web server; it is most likely used for other purposes. Finally, even though port 80 is used by the client computer, there is likely no web server in this scenario.

19. **B.** Quality of Service (QoS) should be configured on the router to prioritize traffic, promoting IP telephony traffic to be more available. You'll get some detractors of QoS, especially for the SOHO side of networks, but if used on the right device and configured properly, it can make a difference. This might sound like more of a networking question, but it ties in directly to the CIA triad of security. Data confidentiality and integrity are important, but just as important is availability—the ability for users to access data when required. NAT is network address translation, which interprets internal and external IP networks to each other. NAC is network access control—for example, 802.1X. Subnetting is when a network is divided into multiple logical areas through IP addressing/planning and subnet mask configuring.

20. **A.** You would most likely use a virtual LAN (VLAN). This allows you to segment internal traffic within layer 2 of the OSI model, by using either a protocol-based scheme or a port-based scheme. The DMZ is used to create a safe haven for servers that are accessed by outside traffic. NAT is network address translation, which is a layer 3 option used on routers. Because we are dealing with a layer 2 scenario, routing in general is not necessary.

Chapter 7

1. **D.** TFTP (Trivial File Transfer Protocol) is a simpler version of FTP that uses a small amount of memory. It is generally considered to be a nonessential protocol. The Domain Name System service (or DNS service) is required for Internet access and on Microsoft domains. The Address Resolution Protocol (ARP) is necessary in Ethernet networks that use TCP/IP. TCP stands for Transmission Control Protocol, an essential part of most network communications.

2. **B.** DNS servers are the only types of servers listed that do zone transfers. The purpose of accessing the zone file is to find out what hosts are on the network.

3. **D.** By checking a DNS server's records regularly, a security admin can monitor and protect it. Blocking port 53 on a firewall might protect it (it also might make it inaccessible depending on the network configuration) but won't enable you to monitor it. Pinging the server can simply tell you whether the server is alive. Purging pointer records (PTR) cannot help to secure or monitor the server.
4. **A.** The Lightweight Directory Access Protocol (LDAP) uses port TCP 389. Note: If you are working with secure LDAP, then you will be using port 636. Port 80 is used by HTTP. Port 443 is used by HTTPS. Port 143 is used by IMAP.
5. **A and C.** POP3 uses port 110; IMAP uses port 143; 3389 is used by the Remote Desktop Protocol; and 389 is used by LDAP.
6. **A.** The Domain Name System (DNS) uses port 53. Port 80 is used by HTTP; port 110 is used by POP3; and port 88 is used by Kerberos.
7. **C.** For clients to connect to the server via SSL, the server must have inbound port 443 open. The outbound ports on the server are of little consequence for this concept, and inbound port 80 is used by HTTP.
8. **C.** Session hijacking (or TCP/IP hijacking) is when an unwanted mediator takes control of the session between a client and a server (for example, an FTP or HTTP session).
9. **D.** Spoofing is when a malicious user makes data or e-mail appear to be coming from somewhere else.
10. **A.** Kiting is the practice of monopolizing domain names without paying for them. Newly registered domain names can be canceled with a full refund during an initial five-day window known as an AGP, or add grace period. Domain hijacking is another type of hijacking attack where the attacker changes the registration of a domain name without the permission of the original owner/registrant.
11. **C.** The Address Resolution Protocol, or ARP, resolves IP addresses to MAC addresses. DNS resolves from IP addresses to hostnames, and vice versa. RARP is Reverse ARP; it resolves MAC addresses to IP addresses.
12. **A.** The SMTP relay is when one server forwards e-mail to other e-mail servers. Buffer overflows are attacks that can be perpetuated on web pages. POP3 is another type of e-mail protocol, and cookies are small text files stored on the client computer that remember information about that computer's session with a website.
13. **A.** DNS poisoning can occur at a DNS server and can affect all clients on the network. It can also occur at an individual computer. Another possibility is that spyware has compromised the browser. A denial-of-service is a single attack that attempts to stop a server from functioning. A buffer overflow is an attack that, for example, could be perpetuated on a web page. ARP poisoning is the poisoning of an ARP table, creating confusion when it comes to IP address-to-MAC address resolutions.
14. **B.** A synchronize (SYN) attack misuses the TCP three-way handshake process. The idea behind this is to overload servers and deny access to users. A man-in-the-middle (MITM) attack is when an attacker is situated between the legitimate sender and receiver and captures and (potentially) modifies packets in transit. Though not a common term, an example of a WPA attack would be the cracking of an access point's password. A replay attack is when data is maliciously repeated or delayed.
15. **C.** Port 3389 must be open on the inbound side of the user's computer to enable a remote tech to log in remotely and take control of that computer. Port 21 is the port used by FTP, and 389 is used by LDAP. 8080 is another port used by web browsers that takes the place of port 80.
16. **B.** When multiple computers attack a single server, it is known as a distributed denial-of-service attack, or DDoS. Privilege escalation is when a person who is not normally

authorized to a server manages to get administrative permissions to resources. If a computer is placed between a sender and receiver, it is known as a man-in-the-middle attack. Overhearing parts of a conversation is known as eavesdropping.

17. **B and C.** DNS poisoning and a DNS server's modified hosts files are possible causes for why a person would be redirected to a spoofed website. DoS, or denial-of-service, is when a computer attempts to attack a server to stop it from functioning. Domain name kiting is when a person renews and cancels domains within five-day periods.
18. **C.** User Datagram Protocol (UDP) attacks, or UDP flood attacks, are DoS attacks that use a computer to send a large number of UDP packets to a remote host. The remote host will reply to each of these with an ICMP Destination Unreachable packet, which ultimately makes it inaccessible to clients. The man-in-the-middle (MITM) attack is when an attacker secretly relays and possibly alters information between two parties. TCP/IP hijacking is an attack that spoofs a server into thinking it is talking with a valid client when in reality it is not. An ICMP flood (or ping flood) is a basic DoS where many ICMP packets are sent out without waiting for replies.
19. **C.** A Fraggle attack is a type of DoS attack that sends large amounts of UDP echoes to ports 7 and 19. This is similar to the Smurf attack. Teardrop DoS attacks send many IP fragments with oversized payloads to a target. IP spoofing is when an attacker sends IP packets with a forged source IP address. The replay attack is when valid data transmissions are maliciously repeated or delayed.
20. **B.** Port 49 is used by TACACS+. Port 53 is used by DNS, port 161 is used by SNMP, and port 22 is used by SSH.
21. **C.** Port 88 is used by Kerberos by default. Port 21 is used by FTP, port 80 is used by HTTP, and port 443 is used by HTTPS (TLS/SSL).
22. **A.** SNMP (Simple Network Management Protocol) is the best protocol to use to monitor network devices. Telnet is a deprecated protocol that is used to remotely administer network devices. FTPS provides for the secure transmission of files from one computer to another. IPsec is used to secure VPN connections and other IP connections.
23. **B.** SSH (Secure Shell) is used to remotely administer Unix/Linux systems and network devices. SCP (Secure Copy) is a way of transferring files securely between two hosts—it utilizes SSH. SNMP is used to remotely monitor network equipment. SFTP is used to securely transfer files from host to host—it also uses SSH.
24. **B.** A denial-of-service (DoS) attack probably occurred. The attacker most likely used code to cause an infinite loop or repeating search, which caused the server to crash. It couldn't have been a DDoS (distributed denial-of-service) because only one attacker was involved. MAC spoofing is when an attacker disguises the MAC address of his network adapter with another number. MITM stands for the man-in-the-middle attack, which wasn't necessary since the attacker had direct access to the search fields on the web server. A DNS amplification attack is when an attacker spoofs DNS requests to flood a target website.
25. **A.** SCP (Secure Copy) uses SSH, which runs on port 22 by default. Port 23 is Telnet, port 25 is SMTP, and port 443 is HTTPS (SSL/TLS).
26. **B.** The MAC address is the best way because it is unique and is the hardest to modify or spoof. IP addresses are often dynamically assigned on networks and are easily modified. Computer names (which are effectively NetBIOS names) can easily be changed as well.
27. **A.** FTPS (FTP Secure) uses encryption in the form of SSL or TLS to secure file transfers. The other three options are basically variations on FTP; they do not use encryption, making them less secure.
28. **C.** FTPS (FTP Secure) is the most secure protocol (listed) for transferring files. It uses SSL or TLS to secure FTP transmissions utilizing ports 989 and 990. FTP by itself is inherently

insecure and uses port 21 by default. The truly distracting answer here, SSH, allows a person to remotely access another computer securely, but it's the Secure FTP (SFTP) protocol that works on top of SSH that is considered a secure way of transferring files. Telnet is outdated and insecure. Because of this it is not found on most of today's operating systems, but if it is, it should be removed, or at least stopped and disabled.

29. **B and D.** The Secure FTP (SFTP) and Secure Copy (SCP) protocols provide for the secure transfer of files. The Simple Network Management Protocol (SNMP) is used to monitor various parts of the network. Trivial FTP (TFTP) is not secure by default. The Internet Control Message Protocol (ICMP) is the protocol initiated by ping to invoke responses from other computers.
30. **D and F.** To implement SSL encrypted e-mail communications you would use port 465 for SMTP (or perhaps 587) and port 995 for POP3. Other ports can be assigned by the admin, but they would have to be configured properly at the server side and the client side, and must not conflict with any other well-known ports or other ports currently in use within the organization's network. Port 25 is the default port for regular SMTP. Port 110 is the default for POP3. Port 143 is the default for IMAP. Port 993 is used by IMAP encrypted with SSL/TLS.

Chapter 8

1. **C.** A protocol analyzer has the capability to "drill" down through a packet and show the contents of that packet as they correspond to the OSI model. A TDR is a time-domain reflectometer, a tool used to locate faults in cabling. (I threw that one in for fun. It is a Network+ level concept, so you security people should know it!) A port scanner identifies open network ports on a computer or device; we'll discuss that more in Chapters 12 and 13. A loopback adapter is a device that can test a switch port or network adapter (depending on how it is used).
2. **A.** By creating a honeypot, the administrator can monitor attacks without sustaining damage to a server or other computer. Don't confuse this with a honeynet (answer B), which is meant to attract and trap malicious attackers in an entirely false network. Answer C is not something that an administrator would normally do, and answer D is defining a man trap.
3. **B.** If there was an intrusion, James should check the firewall logs first. DNS logs in the Event Viewer and the performance logs will most likely not show intrusions to the company network. The best place to look first is the firewall logs.
4. **B.** Install a firewall to protect the network. Protocol analyzers do not help to protect a network but are valuable as vulnerability assessment and monitoring tools. Although a DMZ and a proxy server could possibly help to protect a portion of the network to a certain extent, the best answer is firewall.
5. **A.** A firewall contains one or more access control lists (ACLs) defining who is enabled to access the network. The firewall can also show attempts at access and whether they succeeded or failed. A smartphone might list who called or e-mailed, but as of the writing of this book does not use ACLs. Performance Monitor analyzes the performance of a computer, and an IP proxy deals with network address translation, hiding many private IP addresses behind one public address. Although the function of an IP proxy is often built into a firewall, the best answer would be firewall.
6. **C.** Software-based firewalls, such as Windows Firewall, are normally running on the client computers. Although a software-based firewall could also be run on a server, it is not as common. Also, a SOHO router might have a built-in firewall, but not all routers have firewalls.
7. **B.** Proxy servers should normally be between the private network and the public network. This way they can act as a go-between for all the computers located on the private network. This applies especially to IP proxy servers but might also include HTTP proxy servers.

8. **B.** SMTP servers should not be installed on a company firewall. This is not the intention of a firewall device. The SMTP server should most likely be installed within a DMZ.
9. **D.** To monitor the implementation of NIDS on the network, you should configure the network adapter to work in promiscuous mode; this forces the network adapter to pass all the traffic it receives to the processor, not just the frames that were addressed to that particular network adapter. The other three answers have to do with duplexing—whether the network adapter can send and receive simultaneously.
10. **C.** An IP proxy displays a single public IP address to the Internet while hiding a group of internal private IP addresses. It sends data back and forth between the IP addresses by using network address translation (NAT). This functionality is usually built into SOHO routers and is one of the main functions of those routers. HTTP proxies store commonly accessed Internet information. Protocol analyzers enable the capture and viewing of network data. SMTP proxies act as a go-between for e-mail. PAC stands for proxy auto-config, a file built into web browsers that allows the browser to automatically connect to a proxy server.
11. **C.** An Internet content filter, usually implemented as content-control software, can block objectionable material before it ever gets to the user. This is common in schools, government agencies, and many companies.
12. **C.** A honeynet is a collection of servers set up to attract attackers. A honeypot is usually one computer or one server that has the same purpose. A DMZ is the demilitarized zone that is in between the LAN and the Internet. A VLAN is a virtual LAN.
13. **C.** A NIPS, or network intrusion prevention system, detects and discards malicious packets. A NIDS only detects them and alerts the administrator. A proxy server acts as a go-between for clients sending data to systems on the Internet. PAT is port-based address translation.
14. **A, B, and D.** Internet filtering appliances will analyze content, certificates, and URLs. However, certificate revocation lists will most likely not be analyzed. Remember that CRLs are published only periodically.
15. **C.** A NIDS, or network intrusion detection system, will detect suspicious behavior but most likely will not react to it. To prevent it and react to it, you would want a NIPS. Firewalls block certain types of traffic but by default do not check for suspicious behavior. HIDS is the host-based version of an IDS; it checks only the local computer, not the network. A UTM is an all-inclusive security product that will probably include an IDS or IPS—but you don't know which, so you can't assume that a UTM will function in the same manner as a NIDS.
16. **A.** Access control lists can stop specific network traffic (such as FTP transfers) even if the appropriate ports are open. A NIDS will detect traffic and report on it but not prevent it. Antivirus definitions have no bearing on this scenario. If the programmer was able to connect to the FTP server, the password should not be an issue. FTP permissions might be an issue, but since you are working in the firewall, you should check the ACL first; then later you can check on the FTP permissions, passwords, and so on.
17. **D.** Implicit deny (block all) is often the last rule in a firewall; it is added automatically by the firewall, not by the user. Any rules that allow traffic will be before the implicit deny/block all on the list. Time of day restrictions will probably be stored elsewhere but otherwise would be before the implicit deny as well.
18. **B.** An IPS (intrusion prevention system) is a system that prevents or stops attacks in progress. A system that only identifies attacks would be an IDS. A system designed to attract and trap attackers would be a honeypot. A system that logs attacks would also be an IDS or one of several other devices or servers.
19. **A.** A device that is actively monitoring data streams for malicious code is inspecting the content. URL filtering is the inspection of the URL only (for example, https://www.comptia.org). Load balancing is the act of dividing up workload between multiple computers; we'll discuss that more in Chapter 16, "Redundancy and Disaster Recovery." NAT is network address translation, which is often accomplished by a firewall or IP proxy.

20. **C.** Firewall rules (ACLs) are generated to allow or deny traffic. They can be based on ports, protocols, IP addresses, or which way the data is headed. Port security deals more with switches and the restriction of MAC addresses that are allowed to access particular physical ports. Content inspection is the filtering of web content, checking for inappropriate or malicious material. A honeynet is a group of computers or other systems designed to attract and trap an attacker.
21. **B, E, and F.** The security administrator should implement a proxy server, a firewall, and/or a URL filter. These can all act as tools to reduce or limit the amount of traffic based on a specific country. AV software checks for, and quarantines, malware. Spam filters will reduce the amount of spam that an e-mail address or entire e-mail server receives. A load balancer spreads out the network load to various switches, routers, and servers. A NIDS is used to detect anomalies in network traffic.
22. **A.** A honeynet has been employed. This is a group of computers on the Internet, or on a DMZ (and sometimes on the LAN), that is used to trap attackers and analyze their attack methods, whether they are network attacks or malware attempts. A protocol analyzer captures packets on a specific computer in order to analyze them but doesn't capture logs per se. A firewall is used to block network attacks but not malware. A proxy is used to cache websites and act as a filter for clients.
23. **C.** A content filter is an application layer (layer 7) device that is used to prevent undesired HTML tags, URLs, certificates, and so on, from passing through to the client computers. A router is used to connect IP networks. A firewall blocks network attacks. A NIDS is used to detect anomalous traffic.
24. **B.** You should implement a proxy server. This can limit access to specific websites, and monitor who goes to which websites. Also, it can often filter various HTML and website content. A NIDS is used to report potentially unwanted data traffic that is found on the network. Blocking all traffic on port 80 is something you would accomplish at a firewall, but that would stop all users from accessing any websites that use inbound port 80 (the great majority of them!). A honeypot is a group of computers used to lure attackers in and trap them for later analysis.
25. **B.** The firewall rule listed that only denies DNS zone transfers is `deny TCP any any port 53`. As mentioned in Chapter 7, "Networking Protocols and Threats," DNS uses port 53, and DNS zone transfers specifically use TCP. This rule will apply to any computer's IP address initiating zone transfers on the inbound and outbound sides. If you configured the rule for UDP, other desired DNS functionality would be lost. Denying IP in general would have additional unwanted results. When creating a firewall rule (or ACL), you need to be very specific so that you do not filter out desired traffic.

Chapter 9

1. **C.** Wi-Fi Protected Access 2 (WPA2) is the most secure protocol listed for connecting to wireless networks. It is more secure than WPA and WEP. Wired Equivalent Privacy (WEP) is actually a deprecated protocol that should be avoided. The WEP algorithm is considered deficient for encrypting wireless networks. TKIP is also deprecated and is replaceable with CCMP.
2. **C.** Fiber-optic is the most secure because it cannot be tapped like the other three copper-based cables; it does not emit EMI. Although shielded twisted-pair (STP) offers a level of security due to its shielding, it does not offer a level of security like that of fiber-optic and is not the best answer.
3. **D.** MAC filtering disallows connections from any wireless clients unless the wireless client's MAC address is on the MAC filtering list.
4. **B.** The SSID is used to identify the wireless network. It does not secure the WAP; one of the ways to secure a WAP is by disabling the SSID. The SSID does not encrypt data or enforce MAC filtering.

5. **A.** Some types of coaxial cables suffer from the emanation of data from the core of the cable, which can be accessed. Crosstalk occurs on twisted-pair cable. Chromatic dispersion occurs on fiber-optic cable. Jamming occurs when an attacker floods a specific EM spectrum in an attempt to block legitimate transmissions from passing through that medium.
6. **A.** Of the listed answers, crosstalk is the most common problem associated with UTP cable. Older versions of UTP cable (for example, Category 3 or 5) are more susceptible to crosstalk than newer versions such as Cat 5e or Cat 6. Although data emanation can be a problem with UTP cable, it is more common with coaxial cable, as is vampire tapping. Chromatic dispersion is a problem with fiber-optic cable.
7. **D.** The best two security precautions are authentication and WPA. Although WPA2 is more secure than WPA, the term "Identification" is not correct. WEP is a deprecated wireless encryption protocol and should be avoided.
8. **B.** Fiber-optic cable is the only one listed that might suffer from chromatic dispersion, because it is the only cable based on light. All the other answers are based on electricity.
9. **C.** Fiber-optic cable is the least susceptible to a tap because it operates on the principle of light as opposed to electricity. All the other answers suffer from data emanation because they are all copper-based. Wiretaps are easily obtainable for copper-based connections such the ones that use twisted-pair cables.
10. **B.** By removing the SSID (security set identifier), the WAP will be more secure, and it will be tougher for war-drivers to access that network. Of course, no new clients can connect to the WAP (unless they do so manually). MAC filtering, WPA, and firewalls are all components that increase the security of a WAP.
11. **A.** By shielding the network switch, we hope to deflect any interference from the air-conditioning system. Another option would be to move the network switch to another location.
12. **B.** Shielded twisted-pair is the most secure type of cabling listed. It adds an aluminum sheath around the wires that can help mitigate data emanation. By far, fiber-optic would be the most secure type of cabling because it does not suffer from data emanation because the medium is glass instead of copper.
13. **A.** WEP 64-bit is the least secure type of wireless encryption listed in the possible answers. The answers are listed in order from least secure to most secure.
14. **B.** Bluesnarfing is the unauthorized access of information from a Bluetooth device—for example, calendar information, phonebook contacts, and so on. Bluejacking is the sending of unsolicited messages to Bluetooth-enabled devices. Deep Blue is not a valid answer to this question as it was a chess-playing computer developed by IBM. And if you answered the Blues Brothers, you should re-read this entire chapter, and then watch the movie if you have some free time.
15. **A.** Privilege escalation is the act of exploiting a bug or flaw in software to gain access to resources that normally would be protected. Chain of custody is the chronological paper trail used as evidence. A default account is an account such as admin set up by the manufacturer on a device; it usually has a blank or simple password. A backdoor is used in computer programs to bypass normal authentication and other security mechanisms that might be in place.
16. **B.** AP isolation mode segments all wireless users so they can't communicate with each other. They can still communicate with the AP and access the Internet (or other network that the AP connects to). It does not hide the SSID.
17. **C.** An evil twin is a rogue access point that has the same SSID as another access point on the network. War-driving is when a person attempts to access a wireless network, usually while driving in a vehicle. Bluesnarfing is the unauthorized access of information through a Bluetooth connection. An IV attack is one that attempts to break the encryption of wireless protocols.

18. **A.** A rogue AP is an unauthorized wireless router (or WAP) that allows access to a secure network. An evil twin is a type of rogue AP, but it also uses the same SSID as the legitimate network. War-driving is the act of trying to access a wireless network. AP isolation blocks each wireless user from communicating with each other.
19. **D.** To limit the wireless signal, decrease the power levels! This can easily be done in most WAP control panels. Putting the antenna on the exterior of the building would make it easier for war-drivers to access the network, and more difficult for actual users. Disabling the SSID has no effect on the signal level. Nor does MAC filtering, though both of those methods can increase the security of your wireless network.
20. **B.** You should implement EMI shielding. This will help to eliminate EMI and data emanation from the Cat 6 wiring (which by default is UTP and therefore not shielded). Multimode fiber would solve the problem, but only if you tore out all of the twisted-pair cabling and replaced it. Questions of this nature don't expect you to take those kinds of measures or accept those types of expenses. Instead, you should focus on securing the cabling that is already in place. CCTV is a detective control that allows you to monitor what transpires in your building via video. Passive scanning is a technique used to check the vulnerabilities of a computer.
21. **C.** A main distribution frame (MDF) room is where wiring and circuits merge and connect out to external ISPs, and other network providers. Both MDF and intermediate distribution frame (IDF) types of rooms are vulnerable attack points. An attacker can exploit MDF and IDF vulnerabilities from within or from without. Satellite communications (SATCOM) is sometimes used for long distance communications, and sometimes for communicating between buildings in a campus. SATCOM devices can be at risk if their firmware is not updated. Exploits could include the installation of malicious firmware and the execution of arbitrary code. Near field communication (NFC) is a data transmission protocol often used with Bluetooth devices, but it is not necessarily secure. Data can be blocked/destroyed by use of a jammer, and users are also at risk of replay attacks. A group of standards known as TEMPEST refers to the investigations of conducted emissions from electrical and mechanical devices, which could be compromising to an organization.

Chapter 10

1. **C.** Authentication is the verification of a person's identity. Authorization to specific resources cannot be accomplished without previous authentication of the user.
2. **C.** Fingerprints are an example of something a person is. The process of measuring that characteristic is known as biometrics.
3. **A and B.** Video cameras enable a person to view and visually identify users as they enter and traverse a building. Key card access systems can be configured to identify a person as well, as long as the right person is carrying the key card!
4. **C and D.** Kerberos and smart card setups are common single sign-on configurations.
5. **C.** Two-factor authentication (or dual-factor) means that two pieces of identity are needed prior to authentication. A thumbprint and key card would fall into this category. L2TP and IPsec are protocols used to connect through a VPN, which by default require only a username and password. Username and password is considered one-factor authentication. There is no client and server authentication model.
6. **C.** A physical access log's main purpose is to show who entered the facility and when. Different access control and authentication models will be used to permit or prevent employee access.
7. **D.** Common criteria when authenticating users include something you do, something you are, something you know, something you have, and some*where* you are. A person's likes and

dislikes are not common criteria; although, they may be asked as secondary questions when logging in to a system.

8. **A and C.** Two of the authentication mechanisms that require something you physically possess include smart cards and USB flash drives. Key fobs and cardkeys would also be part of this category. Certificates are granted from a server and are stored on a computer as software. The username/password mechanism is a common authentication scheme, but it is something that you type and not something that you physically possess.
9. **C.** Before a user can gain access to domain resources, the final step is to be authorized to those resources. Previously the user should have provided identification to be authenticated.
10. **C.** Multifactor authentication means that the user must provide two different types of identification. The thumbprint is an example of biometrics. Username and password are examples of a domain logon. Single sign-on would only be one type of authentication that enables the user access to multiple resources.
11. **C.** SSO (single sign-on) enables users to access multiple servers and multiple resources while entering their credentials only once. The type of authentication can vary but will generally be a username and password. Smart cards and biometrics is an example of two-factor authentication. VPN is short for virtual private network.
12. **C.** MS-CHAPv2 *is* capable of mutual authentication of the client and server. However, MS-CHAPv1 is not. That's why it is important to use MS-CHAPv2. Mutual authentication *is* accomplished with Kerberos. All the other statements are true.
13. **A and D.** Motion detectors often use infrared technology; heat would set them off. They also use ultrasonic technology; sounds in higher spectrums that humans cannot hear would set these detectors off.
14. **D.** Unlike RADIUS, TACACS+ (Terminal Access Controller Access-Control System Plus) encrypts client-server negotiation dialogues. Both protocols are remote authentication protocols.
15. **C.** Port 636 is the port used to secure LDAP (called LDAPS). Port 389 is the standard LDAP port number. Port 443 is used by HTTPS (SSL/TLS), and port 3389 is used by RDP.
16. **A.** If a biometric system identifies a legitimate user as unauthorized, and denies that user access, it is known as a false rejection. False acceptance on the other hand is when a biometric system authorizes an illegitimate user. FAR is the false acceptance rate—the lower the better. CER stands for crossover error rate, which is the comparison of the FAR and the FRR. False exceptions have to do with software that has failed and needs to be debugged.
17. **C.** The only answer that is not a logical method of access control is biometrics. Biometrics deals with the physical attributes of a person and is the most tangible of the answers. All the rest deal with software, so they are logical methods.
18. **D.** 802.1X permits or denies access to resources through the use of ports. It implements Port-based Network Access Control (PNAC). This is part of the 802.1 group of IEEE protocols. 802.1X should not be confused with 802.11x, which is an informal term used to denote any of the 802.11 standards including 802.11b, 802.11g, 802.11n, and 802.11ac. A hub connects computers by way of physical ports but does not permit or deny access to any particular resources; it is a simple physical connector of computers.
19. **C and D.** A mantrap is a device made to capture a person. It is usually an area with two doorways, the first of which leads to the outside and locks when the person enters, the second of which leads to the secure area and is locked until the person is granted access. Biometrics can help in the granting of this access by authenticating the user in a secure way, such as thumbprint, retina scan, and so on. Software-based token systems and access control lists are both logical and do not play into physical security.

20. **D.** CHAP, the Challenge Handshake Authentication Protocol, authenticates a user or a network host to entities like Internet access providers. CHAP periodically verifies the identity of the client by using a three-way handshake; the verification is based on a shared secret. After a link has been established, the authenticator sends a challenge message to the peer; this does not happen in the other three authentication methods listed.
21. **C.** The Internet is used to connect hosts to each other in virtual private networks. A particular computer will probably also use a VPN adapter and/or a network adapter. Modems generally are used in dial-up connections and are not used in VPNs.
22. **C.** Before users can be given access to the network, the network needs to identify them and authenticate them. Later, users may be authorized to use particular resources on the network. Part of the authentication scheme may include a username and password. This would be known as an access control method.
23. **A and D.** Kerberos uses a ticket distribution service and an authentication service. This is provided by the Key Distribution Center. A Faraday cage is used to block data emanations. Port 389 is used by LDAP. One of the more common ports that Kerberos uses is port 88.
24. **C.** Kerberos uses a KDC (key distribution center) to centralize the distribution of certificate keys and keep a list of revoked keys.
25. **D.** Unlike RADIUS, TACACS+ separates authentication, authorization, and auditing capabilities. The other three answers are incorrect and are not differences between RADIUS and TACACS+.
26. **A.** You can achieve port security by applying a security control (such as 802.1X), which ties specific physical ports to end-device MAC addresses and prevents additional devices from being connected to the network. Note that port security solutions such as 802.1X are data link layer technologies (layer 2) so they deal with MAC addresses, not IP addresses. You wouldn't want to exclude all devices from being connected to the network as this would cause a severe problem with connectivity.
27. **D.** RADIUS is a common back-end authenticator for 802.1X. When setting up a wireless access point, the two security mode options are usually PSK (pre-shared key), which is stored on the WAP, and Enterprise, which usually refers authentication to an external RADIUS server. Kerberos deals with authentication to Microsoft domains. CAC cards are smart cards that are used for ID and authentication to systems.
28. **C and E.** If a person doesn't have the proper proximity card, that person will be prevented from entering a server room or other protected room. Security guards can also prevent people from accessing unauthorized areas. However, bollards (short vertical posts) probably wouldn't stop a person, besides they aren't normally installed in front of a server room entrance. A barricade might stop a person, but again, would be out of place! CCTV video surveillance is a detective control, but not a preventive control. 802.1X deals with authentication, not with physical security.
29. **B.** Kerberos is the most secure method of authentication listed. It has a more complicated system of authentication than TACACS (which is outdated) and RADIUS (which is used in different scenarios than Kerberos). LDAP deals with directories (for example, the ones on a Microsoft domain controller), which Kerberos first needs to give access to.
30. **C.** TACACS+ is the only answer listed that uses separate processes for authentication, authorization, and auditing. That is one of the main differences between it and RADIUS. TACACS is deprecated and is not often seen in the field. LDAP deals with managing directories of information.
31. **A.** Fingerprint technology is part of the realm of biometrics. Single sign-on means that you can use one type of authentication to get access to more than one system. While that could be going on in this scenario, it is not explicit, so biometrics is the more accurate answer.

Multifactor means that more than one type of authentication is needed; for example, a fingerprint and a PIN. Let's say that users were expected to type a PIN into a keypad to gain access to the data center. You might find over time that some persons who enter don't match the owner of the PIN. That uncertainty can be avoided by incorporating biometrics. Tokens are used to gain access to systems and networks, and might include rolling one-time passwords, but do not incorporate a person's physical characteristics such as a fingerprint.

32. **C.** RADIUS is the authentication system that uses UDP as the transport mechanism. The others all use TCP. Remember, RADIUS uses ports 1812 and 1813 (or 1645 and 1646), LDAP uses 389 (or 636 for secure LDAP), Kerberos uses port 88, and TACACS+ uses port 49.
33. **D.** A badge encoded with a private encryption key would be an example of a smart card. Tokens are software-based and could be used with a USB flash drive or could be stored on a mobile device. An example of biometrics is a thumbprint scan or retina scan. Kerberos is an authentication technology used by operating systems such as Windows (often in domain scenarios).
34. **B.** If the organization runs Active Directory, that means it has a Windows Server that is acting as a domain controller. These use the Kerberos authentication system by default. TACACS+ is an example of a remote authentication system, but is owned by Cisco, and is not a part of Active Directory. LDAP is the protocol in Windows that controls Active Directory objects, and works in conjunction with Kerberos, but is not the actual authentication method used. 802.1X is an authentication method used by network adapters on the data link layer.
35. **D.** TACACS+ is an authentication, accounting, and authorization service. It uses TCP as its transport mechanism. Kerberos authenticates only, and can use TCP and UDP. RADIUS performs authentication and accounting but uses UDP as the transport mechanism. A captive portal redirects people in an effort to authenticate them. It will often do this within a web browser, and might use TCP (HTTPS), but does not perform accounting services.

Chapter 11

1. **C.** The answer This1sV#ryS3cure incorporates case-sensitive letters, numbers, and special characters and is 16 characters long. The other answers do not have the complexity of This1sV#ryS3cure.
2. **A.** User Account Control (UAC) adds a layer of security to Windows that protects against malware and user error and conserves resources. It enforces a type of separation of duties.
3. **C.** Ctrl+Alt+Del is the key combination used to help secure the logon process. It can be added by configuring the Local Security policy.
4. **A.** By far the username and password combination is the most common authentication model. Although biometrics, key cards, and tokens are also used, the username/password is still the most common.
5. **A.** Rule-based access control uses rules to govern whether an object can be accessed. It is a type of mandatory access control (MAC).
6. **A.** Labels are required in the mandatory access control (MAC) model.
7. **D.** In the MAC (mandatory access control) model, users cannot share resources dynamically. MAC is not a dynamic model; it is a static model. Owners cannot establish access privileges to a resource; this would be done by the administrator. MAC is indeed very restrictive, as restrictive as the administrator wants it to be.
8. **B.** In the discretionary access control (DAC) model, permissions to files are identified by access control lists (ACLs). Role membership is used in RBAC. The mandatory access control model predefines permissions. Either way, it is not identified automatically.

9. **B.** Access control lists (ACLs) are used in the discretionary access control model. This is different from role-based, rule-based, and MAC (mandatory access control) models.

10. **A.** The first thing administrators should do when they notice that the company has a high attrition rate (high turnover of employees) is to conduct a thorough review of user permissions, rights, and access control lists. A review of group policies might also be necessary but is not as imperative. Performance logs and the Application log will probably not pertain to the fact that the company has a lot of employees being hired and leaving the company.

11. **D.** It would be difficult for administrators to deal with thousands of users' passwords; therefore, the best management system for a company with 1000 users would be self-service password resetting.

12. **A.** In the discretionary access control (DAC) model, the owner of the resource is in charge of setting permissions. In a mandatory access control model, the administrator is in charge.

13. **C.** By using a template, you can add many users to a group at once simply by applying the template to the users. Propagation and inheritance deal with how permissions are exchanged between parent folders and subfolders. Access control lists show who was allowed access to a particular resource.

14. **D.** The mandatory access control model uses predefined access privileges to define which users have permission to resources.

15. **D.** To have a secure password scheme, passwords should be changed by the user. They should not be generated by the administrator. If an administrator were to generate the password for the user, it would have to be submitted in written (and unencrypted) form in some way to the user. This creates a security issue, especially if the user does not memorize the password and instead leaves a written version of it lying around. All the other answers would increase the level of password security.

16. **D.** The mandatory access control (MAC) model uses object and subject labels. DAC (discretionary access control), RBAC (role-based access control), and ABAC (attribute-based access control) do not. Rule-based access control is a portion of MAC, and although it might use labels, MAC is the best answer.

17. **C.** Previous logon notification can identify whether unauthorized access has occurred. Two-factor authentication means that person will supply two forms of identification before being authenticated to a network or system. Session termination is a mechanism that can be implemented to end an unauthorized access. Session lock mechanisms can be employed to lock a particular user or IP address out of the system.

18. **A.** Access control lists can be used to control the traffic that is allowed in or out of a network. They are usually included as part of a firewall, and they are the better answer because they specifically will control the traffic. Address Resolution Protocol (ARP) resolves IP addresses to MAC addresses. In the discretionary access control model, the owner controls permissions of resources.

19. **C.** When a company cross-trains people, it is known as job rotation. Separation of duties is in a way the opposite; this is when multiple people are needed to complete a single task. Chain of custody has to do with the legal paper trail of a particular occurrence. Least privilege is a mitigation technique to defend against privilege escalation attacks.

20. **D.** If a resource is not given specific access, it will be implicitly denied by default. Access control lists are used to permit or deny access from one network to another and are often implemented on a firewall.

21. **A.** Role-based access control is when different groups or roles are assigned different levels of permissions; rights and permissions are based on job function. (Note: Attribute-based access control [ABAC] is similar to RBAC, but uses Boolean logic such as IF-THEN statements.) In the mandatory access control model, an administrator centrally controls permissions. In the discretionary access control model, the owner of the user sets permissions. In the rule-based access control model, rules are defined by the administrator and are stored in an ACL.
22. **D.** By implementing password complexity requirements, users will be forced to select and enter complex passwords—for example, eight characters or more, uppercase characters, special characters, and more. Disabling the SSID deals with wireless networks, time-of-day restrictions are applied only after persons log in with their username and password, and changing default passwords should be part of a password policy.
23. **D.** If a network has a large number of users, the administrator should set up a system, and policies to enforce the system, that will allow for users to reset their own passwords. The passwords should be stored centrally, not locally. Also, it would be best if single sign-on were implemented and not a multiple access method.
24. **D.** By implementing CAPTCHA, another level of security is added that users have to complete before they can register to and/or post to a bulletin board. Although banning a user or the user's IP address can help to eliminate that particular person from spamming the site, the best way is to add another level of security, such as CAPTCHA. This applies to all persons who attempt to attack the bulletin board.
25. **A.** Password length is the policy that deals with how many characters are in a password. Password expiration and minimum (and maximum) password age define how long a password will be valid. Password complexity defines whether the password should have uppercase letters, numbers, and special characters.
26. **C.** The password expiration policy should be configured. For example, in Windows, the maximum password age policy should be set to 30 days. Password length deals with how many characters are in the password. Password recovery defines how (and if) a user can get back his password or create a new one. Account lockout policies dictate how many times the user has to type a password incorrectly to be locked out of the system, and for how long the user will remain locked out.
27. **C.** Conduct user permission reviews to ensure that long-term users are getting the proper permissions to data. Privilege creep is when, over time, additional permissions are given to a particular user because that user needs to access certain files on a temporary basis. Mandatory vacations are enforced on many personnel to ensure that there is no kind of fraud or other illegitimate activity going on. Job rotation is implemented so that multiple people can perform the same job, in the case that one person is not available. Separation of duties is when a group of users will each perform an individual task, which collectively forms the entire job.
28. **B.** When you are dealing with access controls based on the classification of data and need-to-know information, you are most likely working with a mandatory access control (MAC) system. Least privilege means the lowest amount of permissions possible. This differs from need-to-know in that a user configured as need-to-know might need to have access to a lot of data, and actually require a good deal of permissions. Role-based access control (RBAC), like MAC, is controlled by the system, but it works with sets of permissions based on user roles. Implicit deny means that unless otherwise configured, all access to data is denied.
29. **D.** Firewalls are most often considered to be based off of the rule-based access control model. This is because you indeed create rules (ACLs) that govern how data is transmitted through the firewall.

30. **C.** The attacker most likely exploited the account lockout policy, a security control originally implemented by the organization. The script modified the policy and caused all of the users to be locked out when they attempted to log in. Password complexity is the level of intricacy of a password; it usually entails using uppercase letters, numerals, and special characters, and is defined by a policy, just as the account lockout threshold is. DoS stands for denial-of-service, an attack that floods a network device (or server) with so much data that the device cannot perform its duties. Password length is the number of characters in a password, also definable by policy.

Chapter 12

1. **D.** A password cracker can check for weak passwords on the network. Antivirus software can scan for viruses on a computer. Performance Monitor enables you to create baselines to check the performance of a computer. Wireshark is a protocol analyzer.
2. **A.** OVAL (Open Vulnerability and Assessment Language) uses XML as a framework for the language. It is a community standard dealing with the standardization of information transfer. 3DES is an encryption algorithm. WPA is a wireless encryption standard, and the deprecated PAP is the Password Authentication Protocol, used for identifying users to a server.
3. **B.** Passive security analysis or passive security testing would be one that possibly does not include a hands-on test. It is less tangible and often includes the use of documentation only. To better protect a system or network, a person should also use active security analysis.
4. **C.** The best way to find all the security holes that exist on a network is to perform a vulnerability assessment. This may include utilizing a port scanner and using a network sniffer and perhaps using some sort of IDS.
5. **D.** If you find ports open that you don't expect, be sure to examine the services and/or processes that use those ports. You may have to close some or all those ports. When you finish with your examination, and after you have taken action, run the port scan again to verify that those ports are closed.
6. **C.** Nessus is a vulnerability assessment tool. Aircrack-ng is used to crack wireless encryption codes. John the Ripper and Cain & Abel are password-cracking programs.
7. **A.** A network mapper is the best tool to use to determine the topology of the network and to find out what devices and computers reside on that network. One example of this is the Network Topology Mapper.
8. **B.** A network scanner is a port scanner used to find open ports on multiple computers on the network. A protocol analyzer is used to delve into packets. A firewall protects a network, and a performance monitor is used to create baselines for and monitor a computer.
9. **A.** Port scanning can be used in a malicious way to find out all the openings to a computer's operating system; this is known as the "fingerprint" of the operating system. Port scanning cannot find out the topology of the network, computer names, usernames, or passwords.
10. **D.** A protocol analyzer can delve into the packets sent across the network and determine whether those packets contain clear-text passwords. Rainbow tables and John the Ripper deal with cracking passwords that were previously encrypted; they aren't necessary if the passwords were sent via clear text. Port scanners scan computers for any open ports.
11. **C.** Residual risk is the risk left over after a security plan and a disaster recovery plan have been implemented. There is always risk, because a company cannot possibly foresee every future event, nor can it secure against every single threat. Senior management as a collective whole is ultimately responsible for deciding how much residual risk there will be in a company's network. No one person should be in charge of this, but it should be decided on as a group. If the group decides that residual risk is too high, the group might decide to get

insurance in addition to its security plan. The security administrator is in charge of finding and removing risks to the network and systems and should mitigate risks if possible. The disaster recovery plan (DRP) coordinator usually assesses risks and documents them, along with creating strategies to defend against any disastrous problems that might occur from that risk, but that person does not decide on the amount of acceptable residual risk to a company.

12. **B.** When dealing with dollars, risk assessments should be based upon a quantitative measurement of risk, impact, and asset value.
13. **C.** The main objective of risk management is to reduce risk to a level that the organization or company will accept. Mitigation is the act of reducing threats in general.
14. **D.** The best answer for why a security administrator would use a vulnerability scanner is to find open ports on a particular computer. Although a vulnerability scanner can do more than scan for open ports, it is the best answer listed.
15. **B.** A password cracker is considered to be a program that does comparative analysis. It systematically guesses the password and compares all previous guesses before making new ones until it cracks the password.
16. **A and B.** Nonessential services are often not configured and secured by the network administrator; this goes hand-in-hand with the fact that they are not monitored as often as essential services. It is imperative that network administrators scan for nonessential services and close any corresponding ports. Even though services may be nonessential, that doesn't necessarily mean that they are not used. An IDS, if installed properly, should monitor everything on a given system.
17. **A.** A ping scanner uses the Internet Control Message Protocol (ICMP) to conduct its scans. Ping uses ICMP as its underlying protocol and IP and ARP. Image scanners are found in printers and as standalone items that scan images, photos, and text into a computer. Barcode scanners are used to scan barcodes, for example, at the supermarket.
18. **D.** `Netstat` shows sessions including the local computer and remote computer. It shows these connections by computer name (or IP) and port name (or number).
19. **A.** Asset value is assigned when performing quantitative risk analysis. Surveys, focus groups, and best practices might help with qualitative risk analysis but do not offer concrete data that a quantitative risk analysis requires. Money is the key ingredient here when it comes to quantitative risk analysis.
20. **B.** When you are given limited information of a system or network, it is known as gray-box testing. White-box testing is when you are given in-depth or complete information about the system. Black-box testing is when you know very little (or nothing) about the system to be tested. Penetration tests are active and are meant to test for a single threat and exploit it. Passive vulnerability scans are different tests altogether and test for as many threats as they can find, without exploiting one of them.
21. **C.** The least privilege concept is executed as a technical control. A process that is severely limited in its functionality and a user who has very limited rights are some of the things that must be initiated technically. A disaster recovery plan and baseline configuration development would be operational controls. The categorization of system security would be a management control.
22. **D.** CCTV (closed-circuit television) is an example of a detective security control. It can detect who is entering a building and when it happened. Bollards (vertical posts often found in parking lots or in front of doorways) and firewalls are preventive controls, while tape backup is a corrective control.
23. **A.** When performing a qualitative risk analysis, a person often uses his own judgment. Asset value, threat frequency, and SLE (single loss expectancy) are all components of a quantitative risk analysis.

24. **D.** When conducting vulnerability assessments, you should organize the collected data by vulnerability and exploit severity as well as the asset value of the possibly affected equipment/systems. Documenting your scan results for a change control board may come later depending on some decision-making by the corporation. You should have already used a network sniffer to find vulnerabilities and possible exploits. Updating the systems will most likely happen at some point, but for the time being, it should be a recommendation within your vulnerability assessment. Management will decide how and if that will occur.

25. **A.** If a new solution poses the potential for new vulnerabilities to your network, you should run an in-depth risk assessment of the new product. In this case, you are not yet doing any coding, so a code assessment is not necessary, but should be implemented as part of a secure code review in the case that you make any programming changes to the database server. You have already run a vulnerability assessment when you did the vulnerability scans. You found that the solution is not a threat but could pose other threats. The risk assessment defines what kind of issues your organization could face due to the threats and vulnerabilities.

26. **B.** Penetration testing is an active test that seeks to exploit one vulnerability. It can indeed cause system instability, so it should be run only during controlled conditions and with express consent of the system owner. Vulnerability scanners are usually passive and should not cause network flooding. Zero-day attacks are based on vulnerabilities that are unknown to the system designer. In a white-box testing environment, zero-day vulnerabilities may become uncovered (at which point they are not quite zero-day anymore), but the fact remains that penetration testing can cause system instability.

27. **D.** An operating system lock (or screen saver lock) is an example of a technical control; it is also considered more technically to be a preventive control. An example of a detective control would be CCTV. An example of an operational control would be security awareness training. An example of a management security control would be the software development life cycle (SDLC).

28. **A.** The brute-force method can be used to recover a user's password from a protected file or otherwise protected area of an operating system. Tools such as these are used by security administrators to recover passwords, but are also used by attackers to crack password codes in order to obtain unauthorized access. Packet sniffing can be used to find passwords that have been sent over the network in clear text (which happens more often than you might suspect), but cannot crack the password stored in a protected file. Social engineering is when con artists attempt to find out information (such as a password) from unsuspecting users. But in the scenario of the question, the user has forgotten the password (thus the need for recovery), so social engineering would be pointless. The cognitive password is an authentication type where, in addition to the password, the user must answer a question of some sort; used collectively, the authentication system grants access if the answer and the password are correct. This is an excellent method to use in the case an attacker does crack a password, because that second level of authentication (based on the user's knowledge) is necessary. And that is when social engineering could perform wonders, attempting to elicit that information from the user. But again, for this question, brute-force is the answer, because the security administrator is simply trying to recover the password for the user.

29. **D.** If an attacker or white hat is performing passive reconnaissance, that person is attempting to gain information about a target system without engaging the system. For example, a basic port scan of a system, without any further action can be considered passive reconnaissance. However, if the attacker or white hat then uses that information to exploit vulnerabilities associated with those ports, then it is known as active reconnaissance. Banner grabbing is a technique used to find out information about web servers, FTP servers, and mail servers. For example, it might be used by a network administrator to take inventory of systems and services running on servers. Or, it could be used by an attacker to grab information such as HTTP headers, which can tell the attacker what type of server is running, its version

number, and so on. Annualized loss expectancy (ALE) is the total loss in dollars per year due to a specific incident. It is computed with the following calculation: SLE × ARO = ALE.

Chapter 13

1. **B.** Audit trails are records showing the tracked actions of users. Performance Monitor is a tool in Windows that enables you to track the performance of objects such as CPU, RAM, network adapter, physical disk, and so on. Permissions grant or deny access to resources. To see whether permissions were granted, auditing must be enabled. The System log and other logs record events that happened in other areas of the system—for example, events concerning the operating system, drivers, applications, and so on.
2. **D.** Performance Monitor can be configured in such a way that alerts can be set for any of the objects (processor, RAM, paging file) in a computer. For example, if the processor were to go beyond 90% usage for more than 1 minute, an alert would be created and could be sent automatically to an administrator. A TDR is a time-domain reflectometer, an electronic instrument used to test cables for faults. A password cracker is a software program used to recover or crack passwords; an example would be Cain & Abel. The Event Viewer is a built-in application in Windows that enables a user to view events on the computer such as warnings, errors, and other information events. It does not measure the objects in a server in the way that Performance Monitor does.
3. **A.** SNMP (Simple Network Management Protocol) is used when a person installs agents on client computers to monitor those systems from a single remote location. SMTP is used by e-mail clients and servers. SMP is symmetric multiprocessing, which is not covered in the Security+ exam objectives. Performance Monitor enables a person to monitor a computer and create performance baselines.
4. **A, C, and D.** To audit events on a computer, an administrator would need to enable auditing within the computer's policy, then turn on auditing for an individual object (folder, file, and so on), and then view the events within the Security log of the Event Viewer. The size of the log file won't matter in this case—aside from events being overwritten. However, the person should still be able to see some events if all the other criteria have been met because 10 MB is big enough for many events to be written to it.
5. **D.** A protocol analyzer captures data including things such as GET requests that were initiated from an FTP client. Vulnerability scanners and port scanners look for open ports and other vulnerabilities of a host. Performance Monitor is a Windows program that reports on the performance of the computer system and any of its parts.
6. **B.** When using an IDS, particular types of traffic patterns refer to signature-based IDS. Anomaly-based and behavior-based systems use different methodologies. Inline IDS means that the device exists on the network (often between a firewall and the Internet) and directly receives packets and forwards those packets to the intended destination.
7. **C.** After auditing is turned on and specific resources are configured for auditing, you need to check the Event Viewer's Security log for the entries. These could be successful logons or misfired attempts at deleting files; there are literally hundreds of options. The Application log contains errors, warnings, and informational entries about applications. The System log deals with drivers, system files, and so on. A System Maintenance log can be used to record routine maintenance procedures.
8. **A.** Performance monitoring software can be used to create a baseline and monitor for any changes to that baseline. An example of this would be the Performance console window within Windows Server. (It is commonly referred to as Performance Monitor.) Antivirus and anti-spyware applications usually go hand-in-hand and are not used to monitor server baselines. Vulnerability assessing software such as Nessus or Nmap is used to see whether open ports and other vulnerabilities are on a server.

9. **B.** SNMP (Simple Network Management Protocol) enables you to gather information from a remote printer. HTTP is the Hypertext Transfer Protocol that deals with the transfer of web pages. A CA is a certificate authority, and SMTP is the Simple Mail Transfer Protocol.

10. **A.** A protocol analyzer can look inside the packets that make up a TCP/IP handshake. Information that can be viewed includes SYN, which is synchronize sequence numbers, and ACK, which is acknowledgment field significant. Port scanners and Performance Monitor do not have the capability to view flags set in a TCP/IP handshake, nor can they look inside packets in general.

11. **C.** Signature-based IDS is the most basic form of intrusion detection system, or IDS. This monitors packets on the network and compares them against a database of signatures. Anomaly-based, behavioral-based, and statistical-based are all more complex forms of IDS. Anomaly-based and statistical-based are often considered to be the same type of monitoring methodology.

12. **D.** A configuration baseline deals with the standard load of a server. By measuring the traffic that passes through the server's network adapter, you can create a configuration baseline over time.

13. **B and C.** It is important to calculate how much disk space you will require for the logs of your database server and verify that you have that much disk space available on the hard drive. It is also important to plan what information will be needed in the case that you need to reconstruct events later. Group Policy information and virtual memory are not important for this particular task.

14. **C.** It is important to copy the logs to a secondary server in case something happens to the primary log server; this way you have another copy of any possible security breaches. Logging all failed and successful login attempts might not be wise, because it will create many entries. The rest of the answers are not necessarily good ideas when working with log files.

15. **B.** Security administrators should frequently view the logs of a DNS server to monitor any unauthorized zone transfers. Aliases are DNS names that redirect to a hostname or FQDN. Simply viewing the logs of a DNS server will not defend against denial-of-service attacks. Domain name kiting is the process of floating a domain name for up to five days without paying for the domain name.

16. **B.** The information listed is an example of a port scan. The source IP address perpetuating the port scan should be banned or blocked on the firewall. The fact that the source computer is using port 53 is of no consequence during the port scan and does not imply DNS spoofing. It is not a denial-of-service attack; note that the destination IP address ends in 80, but the number 80 is part of the IP address and is not the port.

17. **B and C.** The log files should be retained in some manner either on this computer or on another computer. By hashing the log files, the integrity of the files can be checked even after they are moved. Cyclic redundancy checks, or CRCs, have to deal with the transmission of Ethernet frames over the network. Temporary files are normally not necessary when dealing with log files.

18. **A.** A protocol analyzer should be used to diagnose which network adapter on the LAN is causing the broadcast storm. It is also useful for detecting flooding attacks and fragmented packets. A firewall cannot diagnose attacks perpetuated on a network. A port scanner is used to find open ports on one or more computers. A network intrusion detection system (NIDS) is implemented to locate and possibly quarantine some types of attacks but will not be effective when it comes to broadcast storms. A port mirror copies all packets from one or more ports to the monitoring port. It is preferred if you are doing a diagnosis of a broadcast storm, but it is not *required*, and may not even be possible in some cases.

19. **C.** If an audit recording fails, there should be sufficient safeguards employed that can automatically send an alert to the administrator, among other things. Audit records should not be overwritten and in general should not be stopped.

20. **D.** The Security log file should show attempts at unauthorized access to a Windows computer. The Application log file deals with events concerning applications within the operating system and some third-party applications. The System log file deals with drivers, system files, and so on. A DNS log will log information concerning the domain name system.

21. **B.** The System log will show when a computer was shut down (and turned on, for that matter, or restarted). The Security log shows any audited information on a computer system. The Application log deals with OS apps and third-party apps. The DNS log shows events that have transpired on a DNS server.

22. **A and C.** Behavior-based monitoring and anomaly-based monitoring require creating a baseline. Many host-based IDS systems will monitor parts of the dynamic behavior and the state of the computer system. An anomaly-based IDS will classify activities as either normal or anomalous; this will be based on rules instead of signatures. Both behavior-based and anomaly-based monitoring require a baseline to make a comparative analysis. Signature-based monitoring systems do not require this baseline because they are looking for specific patterns or signatures and are comparing them to a database of signatures. Performance Monitor can be used to create a baseline on Windows computers, but it does not necessarily require a baseline.

23. **A.** A performance baseline and audit trails are not necessarily needed. Security logs are usually not performance-oriented. For example, you might get this list from a Windows Server's Security log in the Event Viewer. Auditing this much information could be unfeasible for one person. However, it is important to implement time stamping of the logs and store log details. Before implementing the logging server, Jason should check whether he has enough storage and backup space to meet his requirements.

24. **B.** The initial baseline configuration is most likely affected. Because the application has just been installed, there is only an initial baseline, but no other baselines to yet compare with. Since it is a testing environment, and the developer has just installed the application, security is not a priority. The developer probably wants to see what makes the application tick, and possibly reverse engineer it, but is not yet at the stage of application design, and probably won't be until a new application or modification of the current application is designed.

25. **D.** If the web server is showing a drop in processor and hard disk speed, it might have been compromised. Further analysis and comparison to a pre-existing baseline would be necessary. All the other answers are common for a web server.

26. **A.** A computer security audit is an example of a detective security control. If a security administrator found that a firewall was letting unauthorized ICMP echoes into the network, the administrator might close the port on the firewall—a corrective control, and for the future, a preventive control. The term *protective control* is not generally used in security circles as it is a somewhat ambiguous term.

27. **A.** Most likely, the anomaly-based IDS needs to be reconfigured. It is alerting you to legitimate traffic, which amounts to false positives. These are not actually anomalies. If the traffic being analyzed has no specific signature (or known signature), then a signature-based IDS or IPS will not be able to identify it as legitimate or illegitimate. A UTM is a unified threat management device. This device may or may not have an IDS or IPS, and even then, it may or may not be capable of anomaly-based analysis, so it is not as likely an answer as the anomaly-based IDS. SIEM stands for security information and event management, and comes in the form of a software product or service or an appliance; it deals with real-time monitoring.

28. **C.** SNMPv3 should be used because it provides a higher level of security (encryption of packets, message integrity, and authentication), allowing you to gather information without fear of the data being compromised. SNMPv1 and v2 do not have the elaborate security of SNMPv3. ICMP is the Internet Control Message Protocol used with the ping utility, among other things. It has little to do with monitoring. SSH is Secure Shell, which is a more secure way of remotely controlling systems; it acts as a secure alternative to Telnet.

29. **C.** Continuous monitoring will help an already secure organization to assess security vulnerabilities and weaknesses in real time. Baselining and ACLs are things that have happened, or were configured in the past. Video surveillance is surely in real time, but it is doubtful as to whether it can *assess* security vulnerabilities in real time, even if someone is watching the video stream as it happens.

30. **C.** You are observing a Remote Desktop Protocol (RDP) acknowledgement packet. You can tell because the source IP address (192.168.1.5) is using port 3389, the default port for RDP, and is sending the ACK to 10.254.254.57 (which was connecting on the secondary HTTP port 8080). So the client is using an HTTP port, but that is inconsequential because the packet is being generated by the source (SRC) IP. HTTPS (port 443) is not involved in this packet capture. Neither is SFTP, as it rides on SSH using port 22.

Chapter 14

1. **A.** BitLocker uses symmetric encryption technology based on AES. Hashing is the process of summarizing a file for integrity purposes. WPA2 is a wireless encryption protocol.

2. **D.** A hash provides integrity checks; for example, MD5 hash algorithms. Public and private keys are the element of a cipher that allows for output of encrypted information. WEP (Wired Equivalent Privacy) is a deprecated wireless encryption protocol.

3. **A.** Steganography is the act of writing hidden messages so that only the intended recipients know of the existence of the message. This is a form of security through obscurity. Steganographers are not as concerned with data integrity or encryption because the average person shouldn't even know that a message exists. Although steganography can be accomplished by using compromised wireless networks, it is not used to gain wireless access.

4. **A.** Symmetric encryption is the best option for sending large amounts of data. It is superior to asymmetric encryption. PKI is considered an asymmetric encryption type, and hashing algorithms don't play into sending large amounts of data.

5. **A.** The easiest way for an attacker to get at encrypted data is if that encrypted data has a weak encryption key. The algorithm isn't of much use to an attacker unless it has been broken, which is a far more difficult process than trying to crack an individual key. Captured traffic, if encrypted, still needs to be decrypted, and a weak key will aid in this process. The block cipher is a type of algorithm.

6. **C.** Symmetric key encryption uses a secret key. The term *symmetric key* is also referred to as the following: private key, single key, and shared key (and sometimes as session key). PKI and public keys at their core are asymmetrical.

7. **A.** A private key should be used by users when logging in to the network with their smart card. The key should certainly not be public. A key actually determines the function of a cipher. Shared key is another term for symmetric key encryption but does not imply privacy.

8. **D.** In cryptography, the one-way function is one option of an algorithm that cannot be reversed, or is difficult to reverse, in an attempt to decode data. An example of this would be a hash such as SHA-2, which creates only a small hashing number from a portion of the file or message. There are ways to crack asymmetric and symmetric encryptions, which enable complete decryption (decoding) of the file.

9. **D.** The Diffie-Hellman algorithm relies on key exchange before data can be sent. Usernames and passwords are considered a type of authentication. VPN tunneling is done to connect a remote client to a network. Biometrics is the science of identifying people by one of their physical attributes.
10. **A.** Steganography replaces the least significant bit of each byte. It would be impossible to replace a byte of each bit, because a byte is larger than a bit; a byte is eight bits.
11. **D.** If a hashing algorithm generates the same hash for two different messages within two different downloads, a collision has occurred and the implementation of the hashing algorithm should be investigated.
12. **D.** The purpose of the MD5 hash is to verify the integrity of a download. SHA is another example of a hash that will verify the integrity of downloads. LANMAN hashes are older, deprecated hashes used by Microsoft LAN Manager for passwords. Encrypted AES and SSL connections are great for encrypting the data transfer but do not verify integrity.
13. **B.** The RSA encryption algorithm uses two prime numbers. If used properly they will be large prime numbers that are difficult or impossible to factor. SHA-1 is an example of a Secure Hash Algorithm—albeit a deprecated one. WPA is the Wi-Fi Protected Access protocol, and RSA is an example of an asymmetric method of encryption.
14. **B.** ECC (elliptic curve cryptography) is an example of public key cryptography that uses an asymmetric key algorithm. All the other answers are symmetric key algorithms.
15. **C.** AES-256 enables a quick and secure encrypted connection for use with a USB flash drive. It might even be used with a whole disk encryption technology, such as BitLocker. SHA-2 and MD5 are examples of hashes. 3DES is an example of an encryption algorithm but would not be effective for sending encrypted information in a highly secure manner and quickly to a USB flash drive.
16. **D.** Pretty Good Privacy (PGP) encryption uses a symmetric key scheme for the session key data, and asymmetric RSA for the *sending* of the session key, plus a combination of hashing and data compression. Key distribution systems are part of an entire encryption scheme, which typically includes a technology such as Kerberos (key distribution center) or quantum cryptography.
17. **B.** RC5 (Rivest Cipher version 5) can encrypt and decrypt data. SHA-256 is a type of SHA-2. It and MD5 are used as hashing algorithms, and NTLM (NT LAN Manager) is used by Microsoft as an authentication protocol and a password hash.
18. **D.** Ciphers can be reverse engineered but hashes cannot when attempting to re-create a data file. Hashing is not the same as encryption; hashing is the digital fingerprint, so to speak, of a group of data. Hashes are not reversible.
19. **A.** AES (Advanced Encryption Standard) is fast and secure, more so than 3DES. SHA-512 (a type of SHA-2) and MD5 are hashing algorithms. Not listed is RSA, which is commonly implemented to secure credit card transactions.
20. **A.** A hash is collision resistant if it is difficult to guess two inputs that hash to the same output.
21. **A.** DES (Data Encryption Standard) was developed in the 1970s; its 56-bit key has been superseded by 3DES (max 168-bit key) and AES (max 256-bit key). DES is now considered to be insecure for many applications. RSA is definitely stronger than DES even when you compare its asymmetric strength to a relative symmetric strength. SHA is a hashing algorithm.
22. **A and D.** Smart cards and USB flash drives can be used as devices that carry a token and store keys; this means that they can be used for authentication to systems, often in a multifactor authentication scenario. Network adapters and PCI Express cards are internal to a PC and would not make for good key storage devices.

23. **A.** A birthday attack exploits the mathematics behind the birthday problem in probability theory. It deals with two different messages using the same hash function, generating the same message digest. Bluesnarfing deals with Bluetooth devices. The man-in-the-middle attack is when a person or computer intercepts information between a sender and the receiver. A logic bomb is a malicious attack set to go off at a particular time; often it is stored on a zombie computer.
24. **A.** Public keys can be used to decrypt the hash of a digital signature. Session keys are used to encrypt web browser traffic. Private keys are used to digitally sign a message and decrypt wireless messages.
25. **A.** A one-time pad is a stream cipher that encrypts plaintext with a secret random key that is the same length as the plaintext. Encryption is accomplished by combining the keystream with the plaintext message using the bitwise XOR operator to produce the ciphertext. Obfuscation means to make something obscure and unclear. PBKDF2 is an example of key-stretching software. Elliptic Curve Diffie-Hellman, or ECDH, uses elliptic curve public/private key pairs to establish the secret key.
26. **D.** RC4 has several vulnerabilities when used incorrectly by protocols such as WEP. WEP does not use AES, RSA, or RC6, all of which are secure protocols if used correctly.
27. **A.** Symmetric key systems use the same key on each end during transport of data. Asymmetric key systems (such as public key cryptography systems) use different keys.
28. **A and D.** Many systems have a recovery agent that is designed just for this purpose. If the account that encrypted the file is deleted, it cannot be recreated (without different IDs and therefore no access to the file), and the recovery agent will have to be used. If there is no recovery agent (which in some cases needs to be configured manually), then the file will be unrecoverable. This file was encrypted with a private key and needs to be decrypted with a private key—PKI is a system that uses asymmetric key pairs (private and public). The root user account does not have the ability to recover files that were encrypted by other users.
29. **C.** RSA can both encrypt and authenticate messages. Diffie-Hellman encrypts only. BitLocker is a type of whole disk encryption (WDE), which deals with encrypting entire hard drives but is not used to send and receive messages. SHA-384 is a cryptographic hash function used to preserve the integrity of files.
30. **A.** RC4 is a symmetric encryption algorithm that uses a stream cipher. It is the only listed answer that is not a valid cryptographic hash function.
31. **B.** Jason chose a block cipher; for example, the 128-bit version of AES. Don't let the phrase "network stream" fool you; stream ciphers will encrypt each bit in the stream. Hashing algorithms are not used to encrypt network streams of data. RC4 is a stream cipher.
32. **B.** The ECC (elliptic curve cryptography) method allows for lesser key lengths but at the same level of strength as other asymmetric methods. This reduces the computational power needed. RSA and Diffie-Hellman require more computational power due to the increased key length. DHE especially uses more CPU power because of the ephemeral aspect. (ECDHE would be the solution in that respect.) Twofish is a symmetric algorithm.

Chapter 15

1. **D.** In X.509, the owner does not use a symmetric key. All the other answers apply to X.509.
2. **B and C.** A digital certificate includes the certificate authority's (CA) digital signature and the user's public key. A user's private key should be kept private and should not be within the digital certificate. The IP address of the CA should have been known to the user's computer before obtaining the certificate.
3. **D.** When creating key pairs, PKI has two methods: centralized and decentralized. Centralized is when keys are generated at a central server and are transmitted to hosts.

Decentralized is when keys are generated and stored on a local computer system for use by that system.

4. **A.** IPsec is usually used with L2TP. SSH is a more secure way of connecting to remote computers. PHP is a type of language commonly used on the web. SHA is a type of hashing algorithm.
5. **B.** Certificate revocation lists (CRLs) are digitally signed by the certificate authority for security purposes. If a certificate is compromised, it will be revoked and placed on the CRL. CRLs are later generated and published periodically.
6. **A.** The public key infrastructure, or PKI, is based on the asymmetric encryption concept. Symmetric, elliptical curve, and quantum cryptography are all different encryption schemes that PKI is not associated with.
7. **A.** You should implement a CRL (certificate revocation list) so that stolen certificates, or otherwise revoked or held certificates, cannot be used.
8. **B and D.** When dealing with certificate authentication, asymmetric systems use one-to-one mappings and many-to-one mappings.
9. **A.** SSH, or Secure Shell, enables two computers to send data via a secure channel. SMTP is the Simple Mail Transfer Protocol, which deals with e-mail. SNMP is the Simple Network Management Protocol, which enables the monitoring of remote systems. P2P is an abbreviation of peer-to-peer network.
10. **B.** Port 443 is used by HTTPS, which implements TLS/SSL for security. SFTP is the Secure File Transfer Protocol. There are no protocols named SSHTP and SSLP.
11. **A.** In VPNs (virtual private networks), Layer Two Tunneling Protocol (L2TP) creates an unencrypted tunnel between two IP addresses. It is usually used with IPsec to encrypt the data transfer. PPTP is the Point-to-Point Tunneling Protocol, which includes encryption.
12. **A.** A private key should be used to encrypt the signature of an e-mail in an asymmetric system such as PKI. Public keys and shared keys should never be used to encrypt this type of information. A hash is not used to encrypt in this fashion; it is used to verify the integrity of the message.
13. **B and C.** In an SSL session, a session key and a public key are used. A recovery key is not necessary unless data has been lost. A key card would be used as a physical device to gain access to a building or server room.
14. **B.** IPsec is a dual-mode, end-to-end security scheme that operates at layer 3, the network layer of the OSI model, also known as the Internet layer within the Internet Protocol suite. It is often used with L2TP for VPN tunneling, among other protocols.
15. **C.** The session layer provides encryption. SSL, or Secure Sockets Layer, and its successor, Transport Layer Security (TLS), encrypt segments of network connections that start at the transport layer. The actual encryption is done at the session layer, and the protocol is known as an application layer protocol.
16. **C.** S/MIME (Secure/Multipurpose Internet Mail Extensions) enables users to send both encrypted and digitally signed e-mail messages, enabling a higher level of e-mail security. It does not make the delivery of e-mail any faster, nor does it have anything to do with return receipts. Return receipts are usually controlled by the SMTP server. Anonymous e-mail messages would be considered spam, completely insecure, and something that a security administrator wants to reduce, and certainly does not want users to implement.
17. **C.** Key revocation is the proper way to approach the problem of a compromised PKI key. The revoked key will then be listed in the CRL (certificate revocation list).
18. **B.** The only statement that is true is that the authentication information is a keyed hash that is based on all the bytes in the packet. A hash will not remain the same if the bytes change on

transfer; a new hash will be created for the authentication header (AH). The authentication header can be used in combination with the Encapsulating Security Payload (ESP).

19. **C.** PPP, or Point-to-Point Protocol, does not provide security and is not used to create VPN connections. You will see PPP used in dial-up connections, and it is an underlying protocol used by L2TP, PPTP, and IPsec, which are all used in VPN connections.

20. **A and C.** IPsec contains (or uses) a key exchange (either Internet Key Exchange or Kerberized Internet Negotiation of Keys) and an authentication header (in addition to many other components). TKIP and AES are other encryption protocols.

21. **A.** A compromised certificate should be published to the CRL (certificate revocation list). The CA is the certificate authority that houses the CRL. PKI stands for public key infrastructure—the entire system that CRLs and CAs are just components of. AES is an encryption protocol.

22. **B.** PKI uses public keys to authenticate users. If you are looking for a cryptographic process that allows for decreased latency, then symmetrical keys (private) would be the way to go. So, the PKI system uses public keys to authenticate the users, and the database uses private keys to encrypt the data.

23. **C.** HTTPS will govern the entire session when a person attempts to connect to a website securely (for example, HTTPS://www.*yourbanknamehere*.com). It initiates a key exchange using SSL or TLS, riding on asymmetric encryption such as RSA or ECC. Then, it performs the rest of the session data transfer using symmetric encryption such as AES. SFTP is Secure FTP, based on SSH. TFTP is Trivial FTP, which has little security.

24. **B.** Key escrow is implemented to secure a copy of the user's private key (not the public key) in case it is lost. It has nothing to do with the CRL.

25. **A.** The browser must present the public key, which is matched against the CA's private key. Symmetric and secret keys are other names for private keys.

Chapter 16

1. **B.** RAID 1 is known as mirroring. If one drive fails, the other will still function and there will be no downtime and no degraded performance. All the rest of the answers are striping-based and therefore have either downtime or degraded performance associated with them. RAID 5 is the second best option because in many scenarios it will have zero downtime and little degraded performance. RAID 0 will not recover from a failure; it is not fault tolerant.

2. **D.** A hot site can facilitate a full recovery of communications software and equipment within minutes. Warm and cold sites cannot facilitate a full recovery but may have some of the options necessary to continue business. Reestablishing a mirror will not necessarily implement a full recovery of data communications or equipment.

3. **B.** A UPS (uninterruptible power supply) ensures that a computer will keep running even if a power outage occurs. The number of minutes the computer can continue in this fashion depends on the type of UPS and battery it contains. A backup generator can also be used, but it does not guarantee 100% uptime, because there might be a delay between when the power outage occurs and when the generator comes online. RAID 1 has to do with the fault tolerance of data. Redundant NICs (network interface cards, also known as network adapters) are used on servers in the case that one of them fails. Hot sites are completely different places that a company can inhabit. Although the hot site can be ready in minutes, and although it may have a mirror of the server in question, it does not ensure that the original server will not shut down during a power outage.

4. **C.** The grandfather-father-son (GFS) backup scheme generally uses daily backups (the son), weekly backups (the father), and monthly backups (the grandfather). The Towers of Hanoi is a more complex strategy based on a puzzle. Incremental backups are simply one-time back-

ups that back up all data that has changed since the last incremental backup. These might be used as the son in a GFS scheme. Differential backups back up everything since the last full backup. A snapshot is a backup type, not a method; it is primarily designed to image systems.

5. **D.** A UPS (uninterruptible power supply) protects computer equipment against surges, spikes, sags, brownouts, and blackouts. Power strips, unlike surge protectors, do not protect against surges.
6. **B.** Patching a system is part of the normal maintenance of a computer. In the case of a disaster to a particular computer, the computer's OS and latest service pack would have to be reinstalled. The same would be true in the case of a disaster to a larger area, like the building. Hot sites, backing up computers, and tape backup are all components of a disaster recovery plan.
7. **A and B.** When evaluating assets to a company, it is important to know the replacement cost of those assets and the value of the assets to the company. If the assets were lost or stolen, the salvage value is not important, and although you may want to know where the assets were purchased from, it is not one of the best answers.
8. **B.** You need two tapes to restore the database server—the full backup tape made on Friday and the differential backup tape made on the following Wednesday. Only the last differential tape is needed. When restoring the database server, the technician must remember to start with the full backup tape.
9. **B.** Backup tapes should be kept away from power sources, including power lines, CRT monitors, speakers, and so on. And the admin should keep backup tapes away from sources that might emit EMI. LCD screens, servers, and fiber-optic cables have low EMI emissions.
10. **B.** The line conditioner is constantly serving critical equipment with clean power. It should be first and should always be on. The UPS battery should kick in only if there is a power outage. Finally, the generator should kick in only when the UPS battery is about to run out of power. Often, the line conditioner and UPS battery will be the same device. However, the line conditioner function will always be used, but the battery comes into play only when there is a power outage, or brownout.
11. **D.** The best way to test the integrity of backed up data is to restore part of that backup. Conducting another backup will tell you if the backup procedure is working properly, and if isn't, after testing the integrity of the backup and after the restore, a person might need to use software to recover deleted files. It's always important to review written procedures and amend them if need be.
12. **B.** Load balancing is a method used when you have redundant servers. In this case, the six web servers will serve data equally to users. The UPS is an uninterruptible power supply, and RAID is the redundant array of inexpensive disks. A warm site is a secondary site that a company can use if a disaster occurs; a warm site can be up and running within a few hours or a day.
13. **C.** A secondary ISP enables the network to remain operational and still gain Internet access even if the fiber-optic connection (or whatever connection) fails. This generally means that there will be a second ISP and a secondary physical connection to the Internet. Redundant network adapters are used on servers so that the server can have a higher percentage of uptime. RAID 5 is used for redundancy of data and spreads the data over three or more disks. A UPS is used in the case of a power outage.
14. **A.** In the case that a building's primary site is lost, data should be backed up to tape stored at a sister site in another city. Storing information across the street might not be good enough, especially if the area has to be evacuated. Company information should never be stored at an employee's home. And of course if the data were stored in the primary building's basement and there were a complete disaster at the primary site, that data would also be lost.

15. **A.** An incremental backup backs up only the files that have changed since the last incremental or full backup. Generally it is used as a daily backup. Differential backups are meant to be used to back up files that have changed since the last full backup. A full backup backs up all files in a particular folder or drive, depending on what has been selected; this is regardless of any previous differential or incremental backups. Copies of data can be made, but they will not affect backup rotations that include incremental, differential, and full backups. Technically, this question could be answered "Incremental" or "Differential," but "Incremental" is the accepted (and therefore best) answer. The CompTIA objectives expect a person to understand that an incremental backup will back up anything that was created/changed since the last incremental backup, or the last full backup if that was the last one completed.
16. **B.** The greatest risk involved in this scenario is that the single web server is a single point of failure regardless that it is connected to three other distribution servers. If the web server goes down or is compromised, no one can access the company's website. A Fraggle is a type of denial-of-service attack. Although denial-of-service attacks are a risk to web servers, they are not the greatest risk in this particular scenario. A company should implement as much redundancy as possible.
17. **A.** An RPO (recovery point objective) defines acceptable data loss. A warm site is a secondary site that will have computers and phones ready for users, but data and services need to be configured and loaded before work can commence. MTBF is the mean time between failure, which defines the average number of failures per million hours, and is usually a number derived from multiple customers of a product. MTTR is the mean time to repair. Both of these are more similar to RTO as opposed to RPO.
18. **C.** Load balancing uses multiple computers to share work, for example, in a load-balancing cluster configuration. RAID uses multiple hard drives to increase speed or create fault tolerance. VPN concentrators allow for remote access of multiple employees over the Internet. Switching (in its simplest form) is the moving of data across the LAN.
19. **A.** RAID should be employed; specifically a fault-tolerant version of RAID (1, 5, 6, and so on). This will ensure that data will still be accessible if one drive fails. Load balancing uses multiple computers to share the load of processing data—often in the form of CPU and RAM collectives—but it does not ensure that data will be accessible in the case of a failure. A cold site is not fault tolerant because it takes at least a day or two to get it up and running. Towers of Hanoi is a tape backup schedule, and as such is not fault tolerant either.
20. **D.** Load balancing is the best option for application availability and expansion. You can cluster multiple servers together to make a more powerful supercomputer of sorts—one that can handle more and more simultaneous access requests. RAID 6 is meant more for data files, not applications. It may or may not be expandable depending on the system used. Multi-CPU motherboards are used in servers and power workstations, but are internal to one system. The CPUs are indeed used together, but will not help with expandability, unless used in a load-balancing scenario.

Chapter 17

1. **B.** The Faraday cage will reduce data emanations. The cage is essentially an enclosure (of which there are various types) of conducting material that can block external electric fields and stop internal electric fields from leaving the cage, thus reducing or eliminating data emanations from such devices as cell phones.
2. **C.** When you think Class C, think copper. Extinguishers rated as Class C can suppress electrical fires, which are the most likely kind in a server room.
3. **A and C.** Signals cannot emanate outside a Faraday cage. Therefore, smartphones and tablets (by default) will not work inside the Faraday cage. Generally, a Faraday cage is

"constructed" for a server room, data center, or other similar location. Servers and switches are common in these places and are normally wired to the network, so they should be able to communicate with the outside world.

4. **B.** Dumpster diving is when a person goes through a company's trash to find sensitive information about an individual or a company. Browsing is not an attack but something you do when connected to the Internet. Phishing is known as acquiring sensitive information through the use of electronic communication. Nowadays, hacking is a general term used to describe many different types of attacks.
5. **A, B, and D.** User education and awareness can help defend against social engineering attacks, phishing, and dumpster diving. Rainbow tables are lookup tables used when recovering passwords.
6. **A.** Social engineering is the practice of obtaining confidential information by manipulating people. Using someone else's network is just theft. Hacking into a router is just that, hacking. And a virus is a self-spreading program that may or may not cause damage to files and applications.
7. **D.** User awareness is extremely important when attempting to defend against social engineering attacks. Vulnerability testing and auditing are definitely important as part of a complete security plan but will not necessarily help defend against social engineering and definitely will not help as much as user awareness training. People should not share passwords.
8. **A and E.** Public buildings with shared office space and organizations with IT employees who have little training are environments in which social engineering attacks are common and would be most successful. Social engineering will be less successful in secret buildings, buildings with a decent level of security such as military facilities, and organizations with dedicated and well-trained IT staff.
9. **A.** Eavesdropping is when people listen to a conversation that they are not part of. A security administrator should keep in mind that someone could always be listening, and thus should always try to protect against this.
10. **C.** CO_2 is the best answer that will prevent damage to computers because CO_2 is air-based, not water-based. CO_2 displaces oxygen. Fire needs oxygen; without it the fire will go out. All the other options have substances that can damage computers. However, because CO_2 can possibly cause ESD damage, the best solution in a server room would be Halotron or FE-36.
11. **C.** Any person pretending to be a data communications repair person would be attempting a social engineering attack.
12. **C.** Turnstiles, double entry doors, and security guards are all examples of preventative measures that attempt to defeat piggybacking. Dumpster diving is when a person looks through a coworker's trash or a building's trash to retrieve information. Impersonation is when a person attempts to represent another person, possibly with the other person's identification. Eavesdropping is when a person overhears another person's conversation.
13. **A and C.** The most common techniques that attackers use to socially engineer people include flattery, dumpster diving, bribery, and forgery. Although assuming a position of authority is an example of social engineering, it is not one of the most common. A WHOIS search is not necessarily malicious; it can be accomplished by anyone and can be done for legitimate reasons. This type of search can tell a person who runs a particular website or who owns a domain name.
14. **A.** Mantraps are the best solution listed—they are the closest to foolproof of the listed answers. Mantraps (if installed properly) are strong enough to keep a human inside until he completes the authentication process or is escorted off the premises. This is a type of preventive security control meant to stop tailgating and piggybacking. Video surveillance will not

prevent an unauthorized person from entering your data center; rather, it is a detective security control. Security guards are a good idea, but if they work only at night, then they can't prevent unauthorized access at all times. 802.1X is an excellent authentication method, but it is logically implemented as software and devices; it is not a physical security control.

15. **D.** Spear phishing is a targeted attack, unlike regular phishing, which usually works by contacting large groups of people. Pharming is when a website's traffic is redirected to another, illegitimate, website. Vishing is the phone/VoIP version of phishing.
16. **B.** Password masking is when the characters a user types into a password field are replaced, usually by asterisks. This is done to prevent shoulder surfing. Tailgating is when an unauthorized person follows an authorized person into a secure area, without the second person's consent. Impersonation is when a person masquerades as another, authorized user. A hoax is an attempt at deceiving people into believing something that is false.
17. **C.** Whaling is a type of spear phishing that targets senior executives such as CFOs. Regular old phishing does not target anyone, but instead tries to contact as many people as possible until an unsuspecting victim can be found. Vishing is the telephone-based version of phishing. Spear phishing does target individuals but not senior executives.
18. **A.** Humidity (if increased) can reduce the chance of static discharges. Temperature does not have an effect on computer systems (within reason). EMI and RFI are types of interference that in some cases could possibly increase the chance of static discharge.
19. **D.** The watering hole attack is a strategy that targets users based on the common websites that they frequent. A pre-action sprinkler system is similar to a dry pipe system, but there are requirements for it to be set off such as heat or smoke. Implementing hot and cold aisles in server rooms is a way to improve air circulation. Supervisory control and data acquisition (SCADA) systems combine hardware monitoring devices (pressure gauges, electrodes, remote terminal units that connect to sensors) with software that is run on an admin's (or building management employee's) workstation, allowing the admin to monitor the HVAC system in real time.
20. **A and D.** The privacy screens are being implemented to prevent shoulder surfing. The secure shredding system is being implemented to mitigate dumpster diving. Impersonation is when an unauthorized person masquerades as a legitimate, authorized person. Phishing is when an attacker attempts to fraudulently obtain information through e-mail scams. Tailgating is when a person (without proper credentials) attempts to gain access to an unauthorized area by following someone else in.

Chapter 18

1. **B.** Purging (or sanitizing) removes all the data from a hard drive so that it cannot be reconstructed by any known technique. If a hard drive were destroyed, it wouldn't be of much value at a company computer sale. Clearing is the removal of data with a certain amount of assurance that it cannot be reconstructed; this method is usually used when recycling the drive within the organization. Formatting is not nearly enough to actually remove data because it leaves data residue, which can be used to reconstruct data.
2. **A.** SOX, or Sarbanes-Oxley, governs the disclosure of financial and accounting data. HIPAA governs the disclosure and protection of health information. GLB, or the Gramm-Leach-Bliley Act of 1999, enables commercial banks, investment banks, securities firms, and insurance companies to consolidate. Top secret is a classification given to confidential data.
3. **B.** A chain of custody is the chronological documentation or paper trail of evidence. A disaster recovery plan details how a company will recover from a disaster with such methods as backup data and sites. A key distribution center is used with the Kerberos protocol. Auditing is the verification of logs and other information to find out who did what action and when and where.

4. **D.** The Gramm-Leach-Bliley Act protects private information such as Social Security numbers. HIPAA deals with health information privacy. SOX, or the Sarbanes-Oxley Act of 2002, applies to publicly held companies and accounting firms and protects shareholders in the case of fraudulent practices.
5. **D.** Non-repudiation, although an important part of security, is not part of the incident response process. Eradication, containment, and recovery are all parts of the incident response process.
6. **C.** The code of ethics describes how a company wants its employees to behave. A chain of custody is a legal and chronological paper trail. Separation of duties means that more than one person is required to complete a job. Acceptable use policy is a set of rules that restricts how a network or a computer system may be used.
7. **A.** Before analyzing any acquired data, you need to make sure that the data has not been tampered with, so you should verify the integrity of the acquired data before analysis.
8. **A.** Most organizations' incident response procedures will specify that containment of the malware incident should be first. Next would be the removal, then recovery of any damaged systems, and finally monitoring that should actually be going on at all times.
9. **A.** Acceptable use (or usage) policies set forth the principles for using IT equipment such as computers, servers, and network devices. Employees are commonly asked to sign such a document that is a binding agreement that they will try their best to adhere to the policy.
10. **D.** He should follow the change management process as dictated by your company's policies and procedures. This might include filing forms in paper format and electronically, and notifying certain departments of the proposed changes before they are made.
11. **A.** An SLA, or service-level agreement, is the agreement between the Internet service provider and you, defining how much traffic you are allowed and what type of performance you can expect. A VPN is a virtual private network. A DRP is a disaster recovery plan. And WPA is Wi-Fi Protected Access.
12. **C.** Human resources personnel should be trained in guidelines and enforcement. A company's standard operating procedures will usually have more information about this. However, a security administrator might need to train these employees in some areas of guidelines and enforcement.
13. **D.** In classified environments, especially when accessing top secret information, a person can get access to only what he needs to know.
14. **D.** A code of ethics is documentation that describes the minimum expected behavior of employees of a company or organization. Need to know deals with the categorizing of data and how much an individual can access. Acceptable usage defines how a user or group of users may use a server or other IT equipment. Separation of duties refers to a task that requires multiple people to complete.
15. **C.** When an employee has been terminated, the employee's account should be disabled, and the employee's data should be stored for a certain amount of time, which should be dictated by the company's policies and procedures. There is no need to speak to the employee's supervisor. It is important not to delete the user account because the company may need information relating to that account later on. Changing the user's password is not enough; the account should be disabled.
16. **C.** By creating a policy that disallows personal music devices, you reduce the possibility of data leakage. This is because many personal music devices can store data files, not just music files. This could be a difficult policy to enforce since smartphones can play music and store data. That's when you need to configure your systems so that those devices cannot connect to the organization's network. DLP devices would also help to prevent data leakage.

Network shares are part of the soul of a network; without them, there would be chaos as far as stored data. If network shares are configured properly, there shouldn't be much of a risk of data leakage. Password protecting files is something that would be hard to enforce, and the encryption used could very easily be subpar and easily cracked. Hardware security modules (HSMs) are inherently encrypted; that is their purpose. To allow an HSM would be a good thing, but there are no unencrypted HSMs.

17. **B and D.** PII (personally identifiable information) must be handled and distributed carefully to prevent ID theft and fraud. In a BYOD environment, personal electronic devices should also be protected and secured and require special policies as well because the devices are being used for personal *and* business purposes. Phishing is the attempt at obtaining information fraudulently. SOX (Sarbanes-Oxley) is an act that details the disclosure of banking information.

18. **B.** Job rotation is when people switch jobs, usually within the same department. This is done to decrease the risk of fraud. It is closely linked with separation of duties, which is when multiple people work together to complete a task; each person is given only a piece of the task to accomplish. Least privilege is when a process (or a person) is given only the bare minimum needed to complete its function. Mandatory vacations are when an employee is forced to take X number of consecutive days of vacation away from the office.

19. **D.** The most important activity when implementing a GRC system in this scenario is continuous security monitoring. It will provide for a secure posture while overseeing the work of the third-party vendor. Baselining is important as well as part of vulnerability management, but the answer "baseline configuration" refers more to the building of a baseline, and not the constant monitoring of that baseline. An SLA is a service-level agreement, which, once agreed to, isn't something you normally *monitor* so to speak. It is a contract of sorts. Security alerting and trending is a part of continuous security monitoring.

20. **C.** Of the listed answers, a hard drive would be considered the least volatile when performing incident response procedures. The order of volatility defines any type of registers as the most volatile, and cache and RAM as slightly less volatile. On the other hand, backup tapes are less volatile than hard drives, and optical discs are less volatile as well. Those last two options make for good options if forensics data needs to be stored over the long term.

21. **A.** The best practice in this scenario is to document. In fact, you should always document. Document everything to be on the safe side. Work around the problem as best you can. Never try to hide anything. It could be costly to the investigation, and your livelihood. You shouldn't have to assess another area of the disc, because you have made a copy (or more than one) and should be able to still access that portion of the disc where the mistake occurred. You should always verify the tools and software used, but this is more of a standard procedure and less of a *best practice*; besides, it doesn't necessarily have to do with the mistake.