Of course! Here is the formatted list of questions for Chapter 15.

Chapter 15: Windows Administration

1. **Which installation type should you choose if you want a clean installation of Windows?**
    - A. Custom
    - B. Upgrade
    - C. Repair
    - D. Refresh
    - **Correct Answer:** A.
    - **Explanation:** When you agree to the end-user license agreement (EULA), you are prompted with options for an upgrade or custom installation. A custom installation is considered a clean installation of Windows. An upgrade simply upgrades the operating system and is not a clean installation. A repair installation reinstalls system files while retaining user data. Refresh is a term used with Windows 8.1, which retains user data and refreshes OS files.
2. **What is the name of the pass that detects hardware and installs drivers?**
    - A. Generalize
    - B. OOBE
    - C. Specialization
    - D. WinPE
    - **Correct Answer:** A.
    - **Explanation:** The Generalize pass is where the operating system detects hardware and installs the appropriate drivers. The Out-Of-Box Experience (OOBE) pass configures and creates the user environment during setup. The Specialization pass configures the operating system during setup. The WinPE pass initiates the operating system installation procedure.
3. **Which partition contains the recovery utility in the event of a problem?**
    - A. BCD
    - B. System
    - C. ESP
    - D. WinRE
    - **Correct Answer:** D.
    - **Explanation:** The WinRE partition is where the Windows Recovery Environment is located. The BCD (Boot Configuration Data) directs the operating system on how to boot. The system partition contains the kernel of the operating system. The EFI system partition (ESP) contains the BCD used to boot the rest of the operating system on a UEFI system.
4. **Which tool is used to create an operating system image for deployment?**
    - A. WDS
    - B. MAP toolkit

- C. USMT
- D. sysprep
- **Correct Answer:** D.
- **Explanation:** Sysprep (System Preparation Tool) is used to prepare an operating system installation for imaging, allowing for generalization and deployment to multiple computers. (Note: The provided sources do not contain a direct explanation for this specific question's answer in the Chapter 15 answer section, but it is a standard tool in Windows administration as implied by the context of Chapter 15's content. Therefore, this explanation is inferred from general knowledge within the domain covered by the document.)

5. **Which command will allow copying of all data to include NTFS permissions?**
   - A. xcopy
   - B. copy
   - C. robocopy (Note: Option C was not explicitly listed in the source for this question, but it is the correct answer based on the provided explanation.)
   - D. diskcopy (Note: Option D was not explicitly listed in the source for this question.)
   - **Correct Answer:** C.
   - **Explanation:** Robocopy (Robust File Copy) is a powerful command-line utility used for copying files and directories, including their NTFS permissions, attributes, and timestamps. The `copy` command is limited and cannot copy directories or their permissions, while `xcopy` has some limitations compared to robocopy. (Note: The answer explanation for this question was not explicitly provided in the Chapter 15 answer section in the same way as others. The correct answer and explanation are derived from the overall context of command-line tools discussed in Chapter 15 and the typical functionalities of these commands in Windows administration. The options provided in the source for this question were only A and B, but the implied correct answer is robocopy based on common knowledge for this exam and typical tool functionality).
6. **Which Windows Update branch for Windows will install features as they are released to the general public?**
   - A. Semi-Annual Channel
   - B. General Availability
   - C. Long-Term Servicing Channel
   - D. Insider Program
   - **Correct Answer:** B.
   - **Explanation:** The General Availability branch installs updates as they are released to the general public. The Semi-Annual Channel is no longer supported by Windows 10/11. The Long-Term Servicing Channel never installs new features during the version's life. The Insider Program allows for the installation of new features before public release.
7. **Which edition of Windows 10 will not allow for Insider Program branch releases?**
   - A. Home
   - B. Pro

    - C. Education
    - D. Enterprise
    - **Correct Answer:** A.
    - **Explanation:** Windows 10 Home only allows for General Availability branch releases. Windows 10 Pro, Education, and Enterprise editions allow for the use of the Insider Program branch releases.
8. **You used the winver.exe utility and it reported Windows 10 Version 1703 (OS Build 15063.145). What is the current date of the last update?**
    - A. 63rd day of 2015
    - B. 145th day of 2015
    - C. March of 2017
    - D. The version needs to be looked up at Microsoft.com.
    - **Correct Answer:** C.
    - **Explanation:** The date code of the edition is yymm, so 1703 corresponds to March of 2017. The other options related to days of 2015 are incorrect because the build number (15063.145) is a build of Windows 10, and the version information is in the date code itself, not needing external lookup.
9. **Which command is used to measure packet loss as a packet travels to a destination address?**
    - A. ping
    - B. nslookup
    - C. pathping
    - D. tracert
    - **Correct Answer:** C.
    - **Explanation:** The `pathping` command measures the packet loss at each router as the packet travels to the destination address, effectively combining the `ping` and `tracert` commands. The `ping` command returns a single destination's response time. The `nslookup` command resolves DNS addresses. The `tracert` command shows how a packet travels to its destination.
10. **Which tool allows you to report a remote computer's inventory of hardware?**
    - A. regedit.exe
    - B. msinfo32.exe
    - C. msconfig.exe
    - D. dxdiag.exe
    - **Correct Answer:** B.
    - **Explanation:** The `msinfo32.exe` tool allows for the remote reporting of a computer's hardware. `regedit.exe` is used to edit the Registry. `msconfig.exe` is used to change service startup and boot processes. `dxdiag.exe` diagnoses DirectX problems.
11. **Which command will allow you to check a volume for corruption?**
    - A. diskpart
    - B. format

- C. chkdsk (Note: Option C was not explicitly listed in the source for this question, but it is the correct answer based on the provided explanation.)
- D. sfc
- **Correct Answer:** C.
- **Explanation:** The `chkdsk` command checks a volume for corruption and attempts to repair it. The `diskpart` command manages disk volumes. The `format` command formats a filesystem. The `sfc` command fixes corrupted system files, not volume corruption. (Note: The options provided in the source for this question were only A, B, and D, but the correct answer is chkdsk based on the explanation.)

12. **Which restriction will be imposed on Windows users until they activate the operating system?**
    - A. They won't be able to launch applications.
    - B. They won't be able to run Windows Updates.
    - C. They won't be able to change the wallpaper.
    - D. They won't be able to browse the Internet.
    - **Correct Answer:** C.
    - **Explanation:** Until Windows is activated, users will experience limitations on personalization options, such as changing the desktop wallpaper or theme. Other core functionalities like launching applications, running Windows Updates, or browsing the Internet are generally not restricted. (Note: The provided sources do not contain a direct explanation for this specific question's answer in the Chapter 15 answer section. This explanation is based on common knowledge of Windows activation behavior.)
13. **What is the name of the pass that configures and creates the user environment during the setup process?**
    - A. Generalization
    - B. OOBE
    - C. Specialization
    - D. WinPE
    - **Correct Answer:** B.
    - **Explanation:** The Out-Of-Box Experience (OOBE) pass is responsible for configuring and creating the user environment during the setup process. The Generalize pass detects hardware and installs drivers. The Specialization pass configures the operating system during setup. The WinPE pass starts the procedure of installing the operating system.
14. **When installing Windows, you can control telemetry data. In which step during setup is this configured?**
    - A. Privacy settings
    - B. Cortana options
    - C. Partitioning options
    - D. Account creation
    - **Correct Answer:** A.

- **Explanation:** Telemetry data control is configured in the Privacy Settings dialog box during Windows installation. Cortana options control Cortana's usage. Disk partitioning is configured to direct Windows where to install. Account creation is performed to set up the first user.

15. **You want to upgrade from Windows Vista Home Basic edition to Windows 10. What are your options?**
    - A. Upgrade to Windows 10 Home.
    - B. Upgrade to Windows 10 Pro.
    - C. Upgrade to Windows 10 Enterprise.
    - D. Upgrade first to Windows 7 Home Basic.
    - **Correct Answer:** D.
    - **Explanation:** Windows 10 does not have a direct upgrade path from Windows Vista; therefore, you must first upgrade to Windows 7 Home Basic. After upgrading to Windows 7 Home Basic, upgrading to Windows 10 Home is possible. Direct upgrades to Windows 10 Pro or Enterprise are not possible from Windows Vista, even after upgrading to Windows 7 Home Basic, though you can upgrade editions once on Windows 10.
16. **You want to upgrade from 32-bit Windows 7 Professional to a 64-bit version of Windows 10. What are your options?**
    - A. Upgrade directly to Windows 10 Pro 64-bit.
    - B. Upgrade first to Windows 10 Pro 32-bit, and then upgrade to 64-bit.
    - C. Upgrade to Windows 8.1 64-bit, and then upgrade to Windows 10 64-bit.
    - D. You must perform a clean installation of Windows 10 Pro 64-bit.
    - **Correct Answer:** D.
    - **Explanation:** There is no direct upgrade path to convert a 32-bit Windows installation to 64-bit without performing a clean installation. Upgrading directly to Windows 10 Pro 64-bit is not possible. While upgrading to Windows 10 Pro 32-bit is possible, you cannot then upgrade that to a 64-bit edition. Upgrading to Windows 8.1 64-bit is also not possible in this scenario.
17. **Where is the Boot Configuration Data stored on a Windows installation utilizing EFI?**
    - A. EFI System Partition (ESP) (Note: Option A was not explicitly listed in the source for this question, but it is the correct answer based on the provided explanation.)
    - B. WinRE partition
    - C. Secure Boot partition
    - D. C:\WINDOWS
    - **Correct Answer:** A.
    - **Explanation:** The Boot Configuration Data (BCD) is stored in the EFI System Partition on an EFI installation of Windows. The WinRE partition is used for the Windows Recovery Environment. Secure Boot is an EFI feature and does not have its own partition. The C:\WINDOWS folder is where the Windows installation resides. (Note: The options provided in the source for this question were only B, C, and D, but the correct answer is ESP based on the explanation.)

18. **Which command is used to identify ports in use by applications and the operating system?**
    - A. netstat
    - B. ipconfig
    - C. pathping
    - D. nslookup
    - **Correct Answer:** A.
    - **Explanation:** The `netstat` command can be used to view ports in use by the operating system and network applications communicating with the network. The `ipconfig` command shows current IP address and DNS information. The `pathping` command displays packet loss along a path to a destination. The `nslookup` command resolves DNS records.
19. **Which type of connection is configured in the Cellular screen in the Settings app?**
    - A. Wired
    - B. Wireless
    - C. WWAN
    - D. VPN
    - **Correct Answer:** C.
    - **Explanation:** The Wireless Wide Area Network (WWAN) connection is a cellular connection and is configured in the Cellular screen in the Settings app. A Virtual Private Network (VPN) connection is configured on the VPN screen.
20. **What is the maximum number of concurrent connections that can be made to a Windows workstation?**
    - A. 10 connections
    - B. 15 connections
    - C. 20 connections
    - D. 25 connections
    - **Correct Answer:** C.
    - **Explanation:** The maximum number of simultaneous connections that can be made to a Windows workstation is 20. All other options are incorrect.

Chapter 16: Working with macOS and Linux

1. **Within a Linux terminal, you want to see all the files on your system in long format (using the –l option), including any hidden files (which requires the –a option). Which command should you use?**
    - A. ls –a | ls -l
    - B. ls –s; ls -l
    - C. ls -la
    - D. ls –a\ls -l
    - **Correct Answer:** C.

    - **Explanation:** The command `ls -la` will list all files in a long format. The `-a` option lists all files, including hidden ones (those starting with a period), and the `-l` option displays them in a long format. Combining these options into `ls -la` is the correct syntax.
2. **Which of the following allows you to see all running programs in macOS?**
    - A. Keychain
    - B. Mission Control
    - C. Finder
    - D. Force Quit
    - **Correct Answer:** B.
    - **Explanation:** Mission Control is a quick way on macOS to view what is currently running. It shows all open windows and spaces, grouped by application, allowing you to switch between them.
3. **As part of your training program, you're trying to convince users to make backups on a regular basis. Which Apple app can be used to make backups of various types on a regular basis?**
    - A. Time Machine
    - B. Finder
    - C. VSS
    - D. Keychain
    - **Correct Answer:** A.
    - **Explanation:** Time Machine is the Apple application that can be used to create backups of various types (e.g., incremental, full) on a regular basis. It can create local snapshots and requires an external storage device for full backups.
4. **Which of the following Linux commands/utilities can be used to edit a file?**
    - A. ps
    - B. nano
    - C. rm
    - D. ls
    - **Correct Answer:** B.
    - **Explanation:** The `nano` command is used to edit files. It functions similarly to Windows Notepad, allowing navigation, searching, replacing, cutting, copying, and pasting text.
5. **Which of the following Linux commands/utilities can be used to edit an Ethernet connection's configuration settings?**
    - A. dd
    - B. apt-get
    - C. ip
    - D. pwd
    - **Correct Answer:** C.
    - **Explanation:** The `ip` command can be used to edit an Ethernet connection's configuration settings.
6. **Which of the following is a macOS feature for password management?**
    - A. Spotlight

    - B. Keychain
    - C. Dock
    - D. Gestures
    - **Correct Answer:** B.
    - **Explanation:** Keychain is a tool that saves credentials so that the user does not need to be prompted repeatedly.
7. **The interpreter in Linux between the operating system and the user is known as the _____.**
    - A. Shell
    - B. Translator
    - C. Login
    - D. GUI
    - **Correct Answer:** A.
    - **Explanation:** The shell is the interpreter in Linux between the operating system and the user, allowing command-line interaction.
8. **What type of backup is kept on site at the computer center for immediate recovery purposes?**
    - A. On-path attack
    - B. Cloud copies
    - C. Journal copies
    - D. Working copies
    - **Correct Answer:** D.
    - **Explanation:** Working copies are backups that are kept on-site at the computer centre for immediate recovery purposes.
9. **Which of the following utilities can be used in Linux to download patches for installation on a workstation?**
    - A. update
    - B. Shell/terminal
    - C. apt
    - D. patch
    - **Correct Answer:** C.
    - **Explanation:** The `apt` utility can be used to download and apply patches to a Linux installation.
10. **Which of the following commands can be used to change the owner of a file to a new owner in Linux?**
    - A. cd
    - B. chmod
    - C. chown
    - D. pwd
    - **Correct Answer:** C.
    - **Explanation:** The `chown` command is used to change ownership of a file.
11. **Which Linux utility can be used to check and repair disks?**
    - A. fsck
    - B. chkdsk

    - C. du
    - D. dumgr
    - **Correct Answer:** A.
    - **Explanation:** The `fsck` Linux utility is used to check and repair disks.
12. **Your iPad has an application that will not stop running. What feature/tool can you use to stop it?**
    - A. kill
    - B. Force Quit
    - C. Task Manager
    - D. Close Quit
    - **Correct Answer:** B.
    - **Explanation:** Force Quit is a function of macOS (and iOS/iPadOS) for killing a process that will not stop running, often accessed by pressing the Home button twice on an iPad.
13. **Which of the following is the most common shell used with Linux?**
    - A. Tcl/Tk
    - B. Terminal
    - C. Bash
    - D. SSH
    - **Correct Answer:** C.
    - **Explanation:** Bash (Bourne-again shell) is the most common command-line shell used with Linux.
14. **What is the name of the area at the bottom of a macOS screen where, by default, a bar of crucial icons appears?**
    - A. Footer
    - B. Mission Control
    - C. Taskbar
    - D. Dock
    - **Correct Answer:** D.
    - **Explanation:** The Dock is the area at the bottom of the macOS screen that is used to launch applications and displays a bar of crucial icons by default.
15. **Which key combination can you use to bring up Spotlight from within an app?**
    - A. Control+Shift
    - B. Option+Tab
    - C. Command+spacebar
    - D. Alt+Home
    - **Correct Answer:** C.
    - **Explanation:** The Command+spacebar key combination will bring up the Spotlight utility, which is the search feature within macOS.
16. **Which Linux command can be used to let you run a single command as another user?**
    - A. sudo
    - B. su
    - C. passwd

- D. ifconfig
- **Correct Answer:** A.
- **Explanation:** The `sudo` command can be used to run a single command as another user.

17. **Which of the following Linux commands will show you a list of running processes?**
    - A. ls
    - B. cat
    - C. ps
    - D. su
    - **Correct Answer:** C.
    - **Explanation:** The `ps` command will display a snapshot of the current running processes on a Linux operating system.
18. **You are currently in a Linux terminal session and in the /home/testuser/documents/mail directory. Which command will take you to /home/testuser/documents?**
    - A. cd .
    - B. cd ..
    - C. cd . . .
    - D. cd ~
    - **Correct Answer:** B.
    - **Explanation:** The command `cd ..` will take you one level back from the current working directory.
19. **If the permissions for a file are rwxrw-r—, what permissions apply for a user who is a member of the group to which the owner belongs?**
    - A. Read, write, and execute
    - B. Read and write
    - C. Read only
    - D. No access
    - **Correct Answer:** B.
    - **Explanation:** In the permissions `rwxrw-r--`, the permissions are broken down as `rwx` for the user (owner), `rw-` for the group, and `r--` for others. Since the user is a member of the group, the effective permissions are read and write.
20. **What does the –p option with mkdir do?**
    - A. Prompts the user before creating files
    - B. Prompts the user before creating subfolders
    - C. Creates subfolders as well as folders
    - D. None of the above
    - **Correct Answer:** C.
    - **Explanation:** The `-p` option on the `mkdir` command allows subfolders to be created as well as the target folder in a single command.

Chapter 17: Security Concepts

1. **Which component of physical security addresses outer-level access control?**
    - A. Fences
    - B. Access control vestibule
    - C. Multifactor authentication
    - D. Strong passwords
    - **Correct Answer:** A.
    - **Explanation:** Fences are intended to delay or deter entrance into a facility and are considered an outer-level access control component of physical security. Access control vestibules are for mid-layer access control, while multifactor authentication and strong passwords are used for mid- and inner-layer access control.
2. **Which type of device can detect weapons on a person entering a facility?**
    - A. Biometrics
    - B. Magnetometer
    - C. Motion sensor
    - D. Badge reader
    - **Correct Answer:** B.
    - **Explanation:** A magnetometer is a device that can detect weapons on a person entering a facility.
3. **As part of your training program, you're trying to educate users on the importance of security. You explain to them that not every attack depends on implementing advanced technological methods. Some attacks, you explain, take advantage of human shortcomings to gain access that should otherwise be denied. Which term do you use to describe attacks of this type?**
    - A. Social engineering
    - B. IDS
    - C. Perimeter security
    - D. Biometrics
    - **Correct Answer:** A.
    - **Explanation:** Social engineering describes attacks that take advantage of human shortcomings to gain access that should otherwise be denied, as opposed to relying on advanced technological methods.
4. **You're in the process of securing the IT infrastructure by adding fingerprint scanners to your existing authentication methods. This type of security is an example of which of the following?**
    - A. Access control
    - B. Physical barriers
    - C. Biometrics
    - D. Softening
    - **Correct Answer:** C.
    - **Explanation:** Adding fingerprint scanners to authentication methods is an example of biometrics, which involves identifying physical attributes of a person for authentication.
5. **Which type of attack denies authorized users access to network resources?**

- A. DoS
- B. Distributed denial-of-service
- C. Trojan
- D. Social engineering
- **Correct Answer:** A.
- **Explanation:** A Denial-of-Service (DoS) attack aims to deny authorized users access to network resources.

6. **As the security administrator for your organization, you must be aware of all types of attacks that can occur and plan for them. Which type of attack uses more than one computer to attack the victim?**
   - A. DoS
   - B. DDoS
   - C. Worm
   - D. Rootkit
   - **Correct Answer:** B.
   - **Explanation:** A Distributed Denial-of-Service (DDoS) attack is a type of attack that uses more than one computer to attack the victim.
7. **A vice president of your company calls a meeting with the IT department after a recent trip to competitors' sites. She reports that many of the companies she visited granted access to the operating system or applications after an employee presented a number that rotated. Of the following, which technology relies on a rotating number for users for authentication?**
   - A. Smartcard
   - B. Biometrics
   - C. Geofencing
   - D. Token
   - **Correct Answer:** D.
   - **Explanation:** A token is a technology that relies on a rotating number for user authentication.
8. **You've discovered that credentials to a specific application have been stolen. The application is accessed from only one computer on the network. Which type of attack is this most likely to be?**
   - A. On-path attack
   - B. Zero-day
   - C. Denial-of-service (DoS)
   - D. Smurf
   - **Correct Answer:** A.
   - **Explanation:** An on-path attack (formerly known as a man-in-the-middle attack) is one where credentials to a specific application are stolen, and the application is accessed from only one computer on the network.
9. **A junior administrator comes to you in a panic. After looking at the log files, he has become convinced that an attacker is attempting to use a legitimate IP address to disrupt access elsewhere on the network. Which type of attack is this?**
   - A. Spoofing

- B. Social engineering
- C. Worm
- D. Password
- **Correct Answer:** A.
- **Explanation:** An attacker attempting to use a legitimate IP address to disrupt access is an example of a spoofing attack, where someone masquerades as someone else to disrupt access.

10. **Which of the following is different from a virus in that it can reproduce itself, is self-contained, and doesn't need a host application to be transported?**
    - A. Malware
    - B. Worm
    - C. Logic bomb
    - D. Trojan
    - **Correct Answer:** B.
    - **Explanation:** A worm is a type of malware that can reproduce itself, is self-contained, and does not need a host application to be transported, unlike a virus.
11. **Which of the following is an example of the two-factor authentication method something you are?**
    - A. Smartcard
    - B. Password
    - C. Fingerprint
    - D. PIN
    - **Correct Answer:** C.
    - **Explanation:** A fingerprint is an example of "something you are" for authentication. A smartcard is "something you have" (often combined with "something you know" like a PIN for multifactor authentication). A password and PIN are "something you know".
12. **Which type of attack involves passing a database query with a web request?**
    - A. Insider threat
    - B. Evil twin
    - C. SQL injection
    - D. Tailgating
    - **Correct Answer:** C.
    - **Explanation:** A SQL injection attack involves passing a database query with a web request by using an escape code sequence.
13. **Which is an example of an authentication method in which you have something?**
    - A. Password
    - B. Key fob
    - C. Fingerprint
    - D. Place
    - **Correct Answer:** B.

- **Explanation:** A key fob is an example of an authentication method where you have something. A password is "something you know", and a fingerprint is "something you are".

14. **You need to protect your users from potentially being phished via email. Which of the following should you use to protect them?**
    - A. Antivirus software
    - B. End-user education
    - C. SecureDNS
    - D. The principle of least privilege
    - **Correct Answer:** B.
    - **Explanation:** To protect users from phishing, end-user education is crucial as it helps users understand why security is important.
15. **Your help desk has informed you that they received an urgent call from the vice president last night requesting his login ID and password. When you talk with the VP today, he says he never made that call. What type of attack is this?**
    - A. Spoofing
    - B. Replay
    - C. Social engineering
    - D. Trojan horse
    - **Correct Answer:** C.
    - **Explanation:** This scenario describes a social engineering attack, specifically spear phishing, where someone attempts to trick an organisation into revealing sensitive information by impersonating a high-level person.
16. **Internal users suspect there have been repeated attempts to infect their systems, as reported to them by pop-up messages from their antivirus software. According to the**
    - A. A server is acting as a carrier for a virus.
    - B. A password attack is being carried out.
    - C. Your antivirus software has malfunctioned.
    - D. A DoS attack is under way.
    - **Correct Answer:** A.
    - **Explanation:** Repeated pop-up messages from antivirus software indicating infection attempts suggest that a server is acting as a carrier for a virus that is trying to spread to other systems. Some viruses don't damage the host system but use it to propagate.
17. **You're working late one night and notice that the hard drive on your new computer is very active even though you aren't doing anything on the computer and it isn't connected to the Internet. What is the most likely suspect?**
    - A. A spear phishing attack is being performed.
    - B. A virus is spreading in your system.
    - C. Your system is under a DoS attack.
    - D. TCP/IP hijacking is being attempted.
    - **Correct Answer:** B.

    - **Explanation:** Unusually active system disk with no user activity is a common symptom of many viruses spreading to other files on the system. Other listed options would typically not cause high local hard drive activity.
18. **You're the administrator for a large bottling company. At the end of each month, you routinely view all logs and look for discrepancies. This month, your email system error log reports a large number of unsuccessful attempts to log in. It's apparent that the email server is being targeted. Which type of attack is most likely occurring?**
    - A. Brute-force
    - B. Backdoor
    - C. Worm
    - D. TCP/IP hijacking
    - **Correct Answer:** A.
    - **Explanation:** A large number of unsuccessful login attempts in the log files is indicative of a brute-force attack, where a password is guessed repeatedly until a successful guess occurs.
19. **Your boss needs you to present to upper management the need for a firewall for the network. What is the thesis of your presentation?**
    - A. The isolation of one network from another
    - B. The scanning of all packets for viruses
    - C. Preventing password attacks
    - D. The hardening of physical security
    - **Correct Answer:** A.
    - **Explanation:** The primary purpose of a firewall is to isolate one network from another, typically the external network (Internet) from the internal network, by blocking unwanted traffic based on a set of rules (ACLs).
20. **Which Active Directory component maps printers and drives during login?**
    - A. Home folders
    - B. Organizational unit
    - C. Login script
    - D. Microsoft Management Console (MMC)
    - **Correct Answer:** C.
    - **Explanation:** A login script is used by Active Directory during the login process to map drives and printers. Home folders are private network locations for personal files, organizational units, group users and computers, and MMC is a management console.

Chapter 18: Securing Operating Systems

1. **Which policy would you create to define the minimum specification if an employee wanted to use their own device for email?**
    - A. MDM

    - B. AUP
    - C. BYOD
    - D. NDA
    - **Correct Answer:** C.
    - **Explanation:** A Bring Your Own Device (BYOD) policy defines the minimum specifications for an employee's device when used for work-related access. While Mobile Device Management (MDM) software might enforce these specifications, it doesn't define them. An Acceptable Use Policy (AUP) is a code of conduct, and a Non-Disclosure Agreement (NDA) is about intellectual property.
2. **Which term refers to copying data between a mobile device and a computer system in order to mirror such things as contacts, programs, pictures, and music?**
    - A. Calibration
    - B. Remote wipe
    - C. Pairing
    - D. Synchronization
    - **Correct Answer:** D.
    - **Explanation:** Synchronization allows you to mirror personal data, such as contacts, programs, pictures, and music, between a mobile device and a computer system, regardless of which device has the most current data. Calibration is for screen touch, remote wipe deletes data, and pairing is for initial Bluetooth connection.
3. **You want to follow the rules of good security administration as set by CompTIA and vendors. To do so, which account should be disabled on most Windows operating systems for security reasons?**
    - A. Guest
    - B. Print Operators
    - C. Power Users
    - D. Userone
    - **Correct Answer:** A.
    - **Explanation:** The Guest account should be disabled on the operating system for security, unless there's a strong justification to keep it enabled. Print Operators and Power Users are groups, and "Userone" refers to a regular user account.
4. **What kind of mobile app is being used when the owner's phone displays a message on the screen and emits an extremely loud tone?**
    - A. Failed login restriction
    - B. Antivirus
    - C. Locator
    - D. Remote wipe
    - **Correct Answer:** C.
    - **Explanation:** This scenario describes a locator app, which helps find a lost or stolen device by displaying messages and emitting loud tones. Remote wipe is for deleting data, not for locating with sound.
5. **As a best practice, after a set period of inactivity on a Windows workstation, what should happen?**

- A. The computer should shut down.
- B. The computer should restart.
- C. A password-enabled screensaver should automatically start.
- D. The system should log out the user.
- **Correct Answer:** C.
- **Explanation:** A best practice is for a password-enabled screensaver to automatically start after a short period of idle time, requiring a password to resume the session. Shutting down, restarting, or logging out the user could result in loss of unsaved work.

6. **A new app developed for the Android platform has which extension?**
   - A. .sdk
   - B. .apk
   - C. .ipa
   - D. .exe
   - **Correct Answer:** B.
   - **Explanation:** Android applications use the .apk (Android Package Kit) extension. .ipa is for Apple iOS apps, and .exe is for Windows desktop operating systems. .sdk refers to a software development kit, not an app extension.
7. **Which of the following has the goal of allowing a username/password combination to be entered once and then allowing claims to be used for consecutive logins? (Choose the best answer.)**
   - A. Tokens
   - B. Kerberos
   - C. Single sign-on
   - D. Multifactor authentication
   - **Correct Answer:** C.
   - **Explanation:** The goal of Single Sign-On (SSO) is to allow a user to enter their username and password once and then use claims for subsequent logins to other resources. Tokens are used after login, Kerberos is an authentication protocol, and multifactor authentication uses multiple factors for initial login.
8. **Which of these is a password manager?**
   - A. Edge
   - B. Credential Manager
   - C. Internet Explorer 11
   - D. Active Directory
   - **Correct Answer:** B.
   - **Explanation:** The Windows Credential Manager is a password manager built into the Windows operating system. Edge and Internet Explorer 11 are web browsers that work with Credential Manager but are not password managers themselves. Active Directory authenticates domain users but doesn't manage end-user passwords in this context.
9. **You have a very small network in a home-based office, and you want to limit network access to only those hosts that you physically own. What should you utilize to make this possible?**

- A. Static IP addresses
- B. Disabled DNS
- C. Default subnet mask
- D. MAC filtering
- **Correct Answer:** D.
- **Explanation:** MAC filtering allows you to limit network access to specific hosts by allowing only devices with approved MAC addresses to connect. Static IP addresses, disabled DNS, or default subnet masks don't inherently provide this type of access control for physical ownership.

10. **Which wireless encryption protocol provides Advanced Encryption Standard (AES) encryption?**
    - A. Wired Equivalent Privacy (WEP)
    - B. Wi-Fi Protected Access (WPA)
    - C. Wi-Fi Protected Access 2 (WPA2)
    - D. Temporal Key Integrity Protocol (TKIP)
    - **Correct Answer:** C.
    - **Explanation:** WPA2 is the wireless encryption protocol that uses Advanced Encryption Standard (AES) encryption. WEP is the weakest encryption, and WPA typically uses TKIP.
11. **Which type of add-on will extend the functionality of the web browser in a way it wasn't originally designed?**
    - A. Pop-up blocker
    - B. Extensions
    - C. Plug-in
    - D. Ad blocker
    - **Correct Answer:** B.
    - **Explanation:** An extension is a type of add-on that extends the functionality of a web browser beyond its original design. Pop-up blockers and ad blockers change how a web page is rendered, and plug-ins affect content display.
12. **What is normally performed when an employee is offboarded?**
    - A. Their user account is deleted.
    - B. Their user account is unlocked.
    - C. Their user account is created.
    - D. Their user account's password is reset.
    - **Correct Answer:** A.
    - **Explanation:** When an employee is offboarded, their user account is typically deleted or disabled. Account creation happens during onboarding, and resetting the password is not the primary action for offboarding.
13. **By default, when setting up an Android device, why do you need a Google account?**
    - A. The device requires email setup.
    - B. The account is used for cloud synchronizations.
    - C. The account is used for desktop backups.
    - D. The device requires registration.

- **Correct Answer:** B.
- **Explanation:** A Google account is required by default on Android devices primarily for synchronizing data and app purchases to the cloud. While it can facilitate email setup, it's not the sole reason, nor is it primarily for desktop backups or device registration.

14. **You need to secure your mobile device's lock screen with the highest level of protection. Which of the following should you use? (Choose the best answer.)**
    - A. Fingerprint lock
    - B. Face lock
    - C. Passcode lock
    - D. Swipe lock
    - **Correct Answer:** A.
    - **Explanation:** Fingerprint locks are considered the most secure lock method for mobile devices due to the difficulty of duplication. Face locks can have higher false positives, and passcodes can be cracked or shoulder-surfed. Swipe locks offer minimal security.
15. **You need to encrypt a single file on a Windows desktop. Which technology should you use?**
    - A. EFS
    - B. BitLocker
    - C. NTFS
    - D. BitLocker to Go
    - **Correct Answer:** A.
    - **Explanation:** The Encrypted File System (EFS) is a feature of the Windows NTFS filesystem that can encrypt individual files and folders. BitLocker provides full-device encryption, while BitLocker to Go is for removable drives. NTFS is the filesystem, not the encryption technology itself.
16. **A user is in both the Sales group and the Marketing group. The Sales group has full permission at the share level, and the Marketing group has Read-only permission. The files on NTFS are secured with the Modify permission for the Sales group and the Read & Execute permission for the Marketing group. Which permissions will the user have?**
    - A. Full
    - B. Modify
    - C. Read-only
    - D. Read & Execute
    - **Correct Answer:** B.
    - **Explanation:** When a user is part of multiple groups with differing share and NTFS permissions, the effective permission is the most restrictive of the combined share and NTFS permissions. In this case, the Sales group has Full share and Modify NTFS, resulting in Modify. The Marketing group has Read-only share and Read & Execute NTFS, resulting in Read-only. Between Modify and Read-only, Modify is the effective permission.

17. **James just moved a folder on the same partition. What will happen with the permissions for the folder?**
    - A. The permissions will be the same as they were before the move.
    - B. The permissions will be inherited from the new parent folder.
    - C. The permissions will be configured as the root folder for the drive letter.
    - D. The permissions will be blank until configured.
    - **Correct Answer:** A.
    - **Explanation:** When a folder is moved on the same partition, its permissions remain the same as they were before the move because it's not a new entity. Permissions are only inherited from a new parent folder if the folder is moved to a different partition or copied.
18. **A user is in the Sales group. The Sales group has no permissions at the share level. The files on NTFS are secured with the Modify permission for the Sales group. What permissions will the user have?**
    - A. The user will have the Modify permission when connecting from the network.
    - B. The user will have the Modify permission when logged in locally to the computer.
    - C. The user will have no access when logged in locally to the computer.
    - D. The user will have Read-only permissions when connecting from the network.
    - **Correct Answer:** B.
    - **Explanation:** Share permissions are only in effect when accessing a resource over the network. If the share level has no permissions, the user will have no network access. However, if the user is logged in locally to the computer, only the NTFS permissions apply, granting them Modify access.
19. **You are trying to delete a file on the local filesystem, but the operating system will not let you. What could be the problem? (Choose the best answer.)**
    - A. The NTFS Modify permission is applied to the file.
    - B. The share permissions are not set to Full Control.
    - C. The file attributes are set to Read-only.
    - D. The file attributes are set to System.
    - **Correct Answer:** C.
    - **Explanation:** If a file's attributes are set to Read-only, you will not be able to delete it on the local filesystem. NTFS Modify permissions would allow deletion, share permissions don't affect local access, and the System attribute usually protects files but doesn't inherently prevent deletion like Read-only does.
20. **You need to enforce profile security requirements on mobile devices. Which should you use to achieve this goal?**
    - A. AUP
    - B. NDA
    - C. BYOD
    - D. MDM
    - **Correct Answer:** D.
    - **Explanation:** Mobile Device Management (MDM) software enables you to enforce profile security requirements on mobile devices. AUP and NDA are

policies, and BYOD describes a policy but doesn't provide enforcement capabilities.

Chapter 19: Troubleshooting Operating Systems and Security

1. **In Windows, which utility is responsible for finding, downloading, and installing Windows patches?**
    - A. Device Manager
    - B. Microsoft Management Console
    - C. Download Manager
    - D. Windows Update
    - **Correct Answer:** D.
    - **Explanation:** The Windows Update Troubleshooter can help diagnose problems with Windows Update, which is the utility responsible for finding, downloading, and installing patches.
2. **Which Startup Setting option allows you to boot with basic drivers?**
    - A. Enable Debugging
    - B. Enable Safe Boot
    - C. Disable Driver Signature Enforcement
    - D. Enable Low-Resolution Video
    - **Correct Answer:** B.
    - **Explanation:** Safe mode is a boot mode that loads minimal drivers and services, which is equivalent to "Enable Safe Boot".
3. **Which bootrec option can be used in Windows to rebuild the boot configuration file?**
    - A. /fixboot
    - B. /rebuildbcd
    - C. /scanos
    - D. /fixmbr
    - **Correct Answer:** B.
    - **Explanation:** The `/REBUILDBCD` option used with the bootrec tool can rebuild the Boot Configuration Data (BCD). Other options include `/FIXBOOT` for writing a new boot sector, `/SCANOS` for scanning partitions with Windows installations, and `/FIXMBR` for writing a new master boot record.
4. **What is the first step in malware removal?**
    - A. Quarantine the infected system.
    - B. Identify and verify the malware symptoms.
    - C. Remediate the infected system.
    - D. Educate the end user.
    - **Correct Answer:** B.

    - **Explanation:** The most important first step in malware removal is to identify and verify the malware symptoms. Other steps like quarantining, remediating, and educating the end user follow this initial identification.
5. **Which tool will allow you to troubleshoot a slow-loading profile?**
    - A. Profile tab of the Advanced System Properties
    - B. Regedit
    - C. Windows Recovery Environment
    - D. Windows Preinstallation Environment
    - **Correct Answer:** A.
    - **Explanation:** The Profile tab of the Advanced Systems Properties dialog box allows you to view the total size of a local or remote profile, which can help troubleshoot slow-loading profiles.
6. **Which of the following components are only used to restore Windows from a suspended state?**
    - A. BCD
    - B. ntoskrnl.exe
    - C. winload.exe
    - D. winresume.exe
    - **Correct Answer:** D.
    - **Explanation:** `winresume.exe` is specifically used to load Windows from a suspended state. BCD (Boot Configuration Data) directs Windows on how to boot, `ntoskrnl.exe` is the Windows kernel, and `winload.exe` is for normal Windows booting.
7. **One of the users you support has a Windows 10/11 laptop that will not boot up. The user just installed brand-new drivers for a graphics card. They need to access a tax application and their data files. What should you try first?**
    - A. Use System Restore.
    - B. Use Reset This PC.
    - C. Reimage the laptop.
    - D. Manually reinstall Windows 10.
    - **Correct Answer:** A.
    - **Explanation:** System Restore should be the first option as it restores the operating system to an earlier point before the problem (e.g., driver installation) without affecting user data files. Reset This PC, reimaging, or reinstalling Windows would erase programs and data.
8. **Which partitioning type is required when you have UEFI firmware?**
    - A. GPT
    - B. MBR
    - C. POST
    - D. Boot Sector
    - **Correct Answer:** A.
    - **Explanation:** When using UEFI firmware, the disk must be set up with a GUID Partition Table (GPT) partitioning type. MBR (Master Boot Record) is used with BIOS, and POST is a hardware test.

9. **Which of the following are used to prevent pop-unders from appearing?**
    - A. Antimalware utilities
    - B. Pop-up blockers
    - C. Phishing sites
    - D. Antivirus software
    - **Correct Answer:** B.
    - **Explanation:** Pop-up blockers are designed to prevent both pop-ups and pop-unders from appearing on web pages.
10. **In general, how often should you update your antivirus definitions?**
    - A. Weekly
    - B. Monthly
    - C. Daily
    - D. Antivirus definitions do not need to be updated.
    - **Correct Answer:** C.
    - **Explanation:** Antivirus definitions should be updated daily because new viruses are constantly being identified.
11. **Which tool can be used to diagnose why Windows 10/11 is slow and sluggish?**
    - A. Resource Monitor
    - B. msconfig.exe
    - C. Device Manager
    - D. Reliability Monitor
    - **Correct Answer:** A.
    - **Explanation:** Resource Monitor provides a detailed view of real-time performance data for every process, helping to identify the source of slow or sluggish performance in Windows 10/11.
12. **Which tool will allow you to diagnose why Windows Update keeps failing?**
    - A. ntbtlog.txt
    - B. Windows Update Troubleshooter
    - C. Windows Recovery Environment
    - D. Safe mode
    - **Correct Answer:** B.
    - **Explanation:** The Windows Update Troubleshooter is specifically designed to assist in diagnosing problems with Windows Update.
13. **Which of the following programs could be considered antimalware?**
    - A. Microsoft Defender Security
    - B. MDM
    - C. Windows Action Center
    - D. VirusTotal
    - **Correct Answer:** A.
    - **Explanation:** Microsoft Defender Security (formerly Windows Defender) is considered antimalware and antivirus protection for the Windows operating system.
14. **Which of the following tools allows you to manually fix maliciously modified system files?**

- A. regedit
- B. SFC
- C. bootrec
- D. UAC
- **Correct Answer:** B.
- **Explanation:** The System File Checker (SFC) allows you to manually scan for modified operating system files and repair them.

15. **Which of the following can you do to help eliminate security problems? (Select the best answer.)**
    - A. Establish security policies and procedures.
    - B. Optimize drives.
    - C. Prevent booting into safe mode.
    - D. Prevent booting into Windows Recovery Environment.
    - **Correct Answer:** A.
    - **Explanation:** Establishing security policies and procedures helps to eliminate security problems and guide employees on how to act if issues arise.
16. **A mobile device is running out of RAM. What could be the most likely problem?**
    - A. The device is not charged to capacity.
    - B. The digitizer is not functioning properly.
    - C. The device is in DND mode.
    - D. The device has background applications open.
    - **Correct Answer:** D.
    - **Explanation:** A mobile device running out of RAM most likely has too many background applications open that are consuming RAM.
17. **What is a risk of using the auto-reconnect feature on a mobile device?**
    - A. The device will reconnect to any SSID.
    - B. The device could be susceptible to an evil twin attack.
    - C. Battery life will be negatively affected.
    - D. You may exceed your cellular data plan's limits.
    - **Correct Answer:** B.
    - **Explanation:** If auto-reconnect is configured on an SSID, the device could be susceptible to an evil twin attack, where it connects to a malicious access point with the same SSID.
18. **You notice that the reliability of the operating system has diminished in Reliability Monitor. Where can you find more details on why applications are failing?**
    - A. Device Manager
    - B. Event Viewer
    - C. Windows Recovery Environment
    - D. msconfig.exe
    - **Correct Answer:** B.
    - **Explanation:** Event Viewer allows you to see more detailed information on why programs have crashed, which can help in understanding the root cause of diminished reliability.
19. **Why would the operating system write out large amounts of RAM to the page file?**

- A. The CPU is running high on utilization.
- B. This is a normal process of the operating system.
- C. The amount of physical RAM is low.
- D. The page file is faster than conventional RAM.
- **Correct Answer:** C.
- **Explanation:** The operating system writes large amounts of RAM to the page file when the system is running low on physical RAM, in an attempt to free up physical RAM. The page file is not faster than conventional RAM.

20. **What is one consequence of an overheating mobile device?**
    - A. Higher RAM usage
    - B. Degraded battery life
    - C. Inaccurate touchscreen response
    - D. Inability to decrypt emails
    - **Correct Answer:** B.
    - **Explanation:** Degraded battery life can be expected from an overheating mobile device if the problem persists. Other issues like higher RAM usage, inaccurate touchscreen response, or inability to decrypt emails are not direct consequences of overheating.

Chapter 20: Scripting and Remote Access

1. **Which statement about scripting languages is true?**
    - A. Scripting languages require a compiler.
    - B. Scripting languages are strongly typed.
    - C. Scripting languages are interpreted.
    - D. Scripting languages have good memory management.
    - **Correct Answer:** C.
    - **Explanation:** Scripting languages are interpreted languages that run on top of a runtime environment. Programming languages require a compiler, not scripting languages. Scripting languages are not strongly typed, unlike programming languages. Additionally, scripting languages typically have poor memory management due to loosely typed variables.
2. **What level are scripting languages considered?**
    - A. High
    - B. Mid
    - C. Intermediate
    - D. Low
    - **Correct Answer:** A.
    - **Explanation:** Scripting languages are classified as high-level languages because they do not directly interact with hardware and rely on an interpreter as an intermediary. Mid-level languages like Java and C/C++ are distinct from scripting languages. There is no classification such as an "intermediate-level language." Low-level languages, such as machine language and assembly language, are also not scripting languages.

3. **Which type of variable will allow decimal math?**
    - A. Boolean
    - B. Integer
    - C. Floating-point
    - D. String
    - **Correct Answer:** C.
    - **Explanation:** Floating-point variables enable precision mathematics, also known as decimal math. Boolean variables are used for true or false values, integer variables for whole number values, and string variables for text values.
4. **Which environment variable is not inherited?**
    - A. System variable
    - B. User variable
    - C. Program variable
    - D. String variable
    - **Correct Answer:** C.
    - **Explanation:** A program variable holds the least significance and is not inherited. A system variable is defined for the entire system and is highly significant as it is inherited by all users and programs. A user variable is also significant, as all applications inherit it. A string variable is not inherited and is not considered an environment variable.
5. **Which statement will load a PowerShell variable xvar with a value of 2?**
    - A. xvar = 2
    - B. $xvar = 2
    - C. xvar = 2;
    - D. set /a xvar=2
    - **Correct Answer:** B.
    - **Explanation:** The statement `$xvar = 2` is the correct PowerShell syntax for loading the variable xvar with a value of 2. In contrast, `xvar = 2` is Bash syntax, `xvar = 2;` is JavaScript syntax, and `set /a xvar=2` is Windows batch script syntax.
6. **Which type of loop has a defined beginning and end, and steps from beginning to end?**
    - A. do while loop
    - B. while loop
    - C. if statement
    - D. for loop
    - **Correct Answer:** D.
    - **Explanation:** A for loop is characterised by a defined beginning and end, and it executes steps iteratively from the start to the finish. A "do while" loop and a "while" loop only have a defined end. An "if" statement represents branch logic, not a loop.
7. **Which extension is used with the Windows batch scripting language?**
    - A. .vbs
    - B. .js

    - C. .bat
    - D. .py
    - **Correct Answer:** C.
    - **Explanation:** The .bat extension is used for Windows batch scripting. The .vbs extension is for VBScript, .js is for JavaScript, and .py is for Python scripting.
8. **Which scripting language allows for the use of the Component Object Model (COM)?**
    - A. PowerShell
    - B. VBScript
    - C. Windows batch script
    - D. JavaScript
    - **Correct Answer:** B.
    - **Explanation:** VBScript supports the Component Object Model (COM). PowerShell utilises the .NET Framework, Windows batch scripts rely on existing applications, and JavaScript is primarily web browser-based and does not typically use external objects in this manner.
9. **Which extension is used with the Python scripting language?**
    - A. .vbs
    - B. .js
    - C. .bat
    - D. .py
    - **Correct Answer:** D.
    - **Explanation:** The .py extension is associated with the Python scripting language. The .vbs extension is used for VBScript, .js for JavaScript, and .bat for Windows batch scripting.
10. **Which scripting language is used with Microsoft Azure and Microsoft 365?**
    - A. PowerShell
    - B. VBScript
    - C. Windows batch script
    - D. JavaScript
    - **Correct Answer:** A.
    - **Explanation:** PowerShell leverages the .NET Framework and is widely used with Microsoft Azure and Microsoft 365 for managing and automating tasks. VBScript and Windows batch scripts are generally not used for cloud services. JavaScript is primarily web browser-based and not typically used for cloud service management.
11. **Which scripting language is used within web pages to allow for interactive content?**
    - A. PowerShell
    - B. Bash
    - C. VBScript
    - D. JavaScript
    - **Correct Answer:** D.

- **Explanation:** JavaScript is predominantly used within web browsers to enable interactive content on web pages. PowerShell is used for operating system management, Bash scripting is primarily for Linux and UNIX systems, and Windows batch scripts also manage the operating system.

12. **Which extension is used with the Bash scripting language?**
    - A. .vbs
    - B. .sh
    - C. .bat
    - D. .py
    - **Correct Answer:** B.
    - **Explanation:** The .sh extension is used for Bash scripting. The .vbs extension is for VBScript, .bat for Windows batch scripting, and .py for Python scripting.
13. **What must be done before a Bash script can be executed?**
    - A. chown permissions must be set.
    - B. The execute attribute must be set.
    - C. chmod permissions must be set.
    - D. An .sh must be added to the end of the script.
    - **Correct Answer:** C.
    - **Explanation:** To execute a Bash script, you must use the `chmod` command to grant it execute permissions. The `chown` command modifies ownership, not permissions. There isn't a specific "execute attribute" as a separate entity, and adding .sh to the filename is a convention but not a requirement for execution.
14. **Which statement will load a JavaScript variable mvar with a value of 8?**
    - A. $mvar = 8
    - B. mvar = 8
    - C. mvar = 8;
    - D. set /a mvar=8
    - **Correct Answer:** C.
    - **Explanation:** The statement `mvar = 8;` is the correct JavaScript syntax for assigning a value to a variable. `$mvar = 8` is PowerShell syntax, `mvar = 8` is Bash syntax, and `set /a mvar=8` is Windows batch script syntax.
15. **Which scripting language has a preinstalled Integrated Scripting Environment (ISE)?**
    - A. VBScript
    - B. Bash
    - C. Python
    - D. PowerShell
    - **Correct Answer:** D.
    - **Explanation:** PowerShell is unique among the options in having a preinstalled Integrated Scripting Environment (ISE), known as the PowerShell ISE. VBScript, Bash, and Python typically require the installation of other text editors or third-party Integrated Development Environments (IDEs)/ISEs.
16. **Which of the following lines is used to comment JavaScript code?**

- A. //comment
- B. 'comment
- C. REM comment
- D. # comment
- **Correct Answer:** A.
- **Explanation:** The line `//comment` is used to add comments in JavaScript code. `'comment` is used for VBScript, `REM comment` for Windows batch scripts, and `# comment` for Bash scripts and PowerShell code.

17. **Which extension is used with the JavaScript scripting language?**
    - A. .js
    - B. .sh
    - C. .bat
    - D. .py
    - **Correct Answer:** A.
    - **Explanation:** The .js extension is used for the JavaScript scripting language. The .sh extension is for Bash scripting, .bat for Windows batch scripting, and .py for Python scripting.
18. **Which Microsoft remote protocol allows for local drives to be presented to the remote system?**
    - A. VCN
    - B. RDP
    - C. SSH
    - D. Telnet
    - **Correct Answer:** B.
    - **Explanation:** The Remote Desktop Protocol (RDP) enables local drives to be accessible on the remote machine once an RDP session is initiated. Virtual Network Computing (VNC), Secure Shell (SSH), and Telnet do not inherently support drive redirection.
19. **On which network protocol and port does SSH operate?**
    - A. TCP port 3389
    - B. TCP port 22
    - C. TCP port 23
    - D. TCP port 443
    - **Correct Answer:** B.
    - **Explanation:** The SSH protocol operates on TCP port 22. For comparison, Remote Desktop Protocol uses TCP port 3389, Telnet uses TCP port 23, and HTTPS uses TCP port 443.
20. **Which tool is used for screen sharing?**
    - A. RDP
    - B. MSRA
    - C. SSH
    - D. Telnet
    - **Correct Answer:** B.

- **Explanation:** The built-in Microsoft Remote Assistance (MSRA) tool facilitates screen sharing between a trusted helper and a user. Remote Desktop Protocol (RDP) allows remote connections but not screen sharing in the same way. Both Secure Shell (SSH) and Telnet are text-based console access protocols for administering Linux/UNIX and network operating system environments.

Chapter 21: Safety and Environmental Concerns

1. **You have dropped a screw into a tight location of a computer. How should you retrieve it?**
    - A. Use a magnetic-tipped screwdriver.
    - B. Use a magnetic grabber.
    - C. Use a three-pronged grabber.
    - D. Shake the computer until it falls out.
    - **Correct Answer:** C.
    - **Explanation:** A three-pronged grabber should be used to retrieve the screw from the computer. Using a magnetic-tipped screwdriver or a magnetic grabber is not advisable as many components are sensitive to magnets. Shaking the computer is dangerous and may make the screw harder to remove.
2. **You have a failed CRT monitor that you must dispose of safely. Which of the following is used to discharge voltage properly from the unplugged computer monitor?**
    - A. Antistatic wrist strap
    - B. Screwdriver
    - C. High-voltage probe
    - D. Power cord
    - **Correct Answer:** C.
    - **Explanation:** A high-voltage probe can dissipate the high voltage stored in a CRT. An antistatic wrist strap should not be worn near high-voltage potential. A screwdriver can cause a dangerous arc. A power cord supplies power, it doesn't discharge it.
3. **One of your coworkers just spilled a chemical solvent in a warehouse, and you have been asked to help clean it up. Which of the following must contain information about a chemical solvent's emergency cleanup procedures?**
    - A. OSHA
    - B. MSDS
    - C. Product label
    - D. CRT
    - **Correct Answer:** B.
    - **Explanation:** The material safety data sheet (MSDS) will have the necessary information about the cleanup procedures. OSHA oversees workplace safety but doesn't contain cleanup procedures for specific chemicals. The product label may or may not have this information, and a CRT is a type of monitor.

4. **You are purchasing an inkjet printer cartridge for home use that you know has an MSDS. How do you obtain the MSDS for this product?**
    - A. The store is required to give you one at the time of purchase.
    - B. It's contained in the packaging of the printer cartridge.
    - C. You are not legally allowed to have an MSDS for this product.
    - D. You should visit the printer cartridge manufacturer's website.
    - **Correct Answer:** D.
    - **Explanation:** You can download the MSDS by visiting the printer cartridge manufacturer's website. Stores are not required to furnish an MSDS at purchase, nor is the manufacturer required to include it in packaging. You are legally allowed to have an MSDS for products, as per OSHA.
5. **In the interest of a safe work environment, which of the following should you report? (Choose two.)**
    - A. An accident
    - B. A near-accident
    - C. Spills on the floor inside a building
    - D. Rain forecasted for a workday
    - **Correct Answer:** A, C.
    - **Explanation:** An accident should always be reported so that if there is a hazardous condition, it can be fixed. Also, report hazardous conditions, such as a spill on the floor, to the employer before they are a problem. A near-accident doesn't need to be reported unless caused by a hazardous condition like spills. Rain forecasted for a workday is not a hazardous condition.
6. **What is the approximate minimum level of static charge for humans to feel a shock?**
    - A. 300 volts
    - B. 3,000 volts
    - C. 30,000 volts
    - D. 300,000 volts
    - **Correct Answer:** B.
    - **Explanation:** You can feel an ESD shock of 3,000 volts or more. 300 volts is too low for a human to feel. While 30,000 volts and 300,000 volts can be felt, 3,000 volts is the approximate minimum.
7. **Your work environment has been unusually dry lately, and several components have been damaged by ESD. Your team has been asked to be extra careful about ESD damage. Which of the following measures can be implemented to reduce the risk of ESD? (Choose two.)**
    - A. Use an antistatic wrist strap.
    - B. Use an antistatic bag.
    - C. Spray disinfectant spray.
    - D. Shuffle your feet.
    - **Correct Answer:** A, B.
    - **Explanation:** Using an antistatic wrist strap allows you to ground yourself to dissipate a static charge. Using antistatic bags allows for a uniform charge

around a component. Spraying disinfectant spray will not reduce static, and shuffling your feet will build a static charge.

8. **Which of the following are OSHA requirements for a safe work environment that must be followed by employers? (Choose two.)**
    - A. Attend yearly OSHA safe work environment seminars.
    - B. Provide properly maintained tools and equipment.
    - C. Have an OSHA employee stationed within 5 miles of the facility.
    - D. Display an OSHA poster in a prominent location.
    - **Correct Answer:** B, D.
    - **Explanation:** Providing properly maintained tools and equipment is a requirement for an OSHA-compliant workplace. Displaying an OSHA poster in a prominent location is also a requirement. Attending yearly seminars or having an OSHA employee stationed nearby are not requirements.
9. **Your office just added 20 new workstations, and your manager has put you in charge of configuring them. The users need to have Microsoft Office installed. What should you do to install Microsoft Office properly on these computers?**
    - A. Ensure that the company has the proper licenses to install 20 additional copies.
    - B. Agree with the open source license agreement during installation.
    - C. Use the personal license key from an existing system to install Office on the new computers.
    - D. Follow normal installation procedures; nothing else needs to be done.
    - **Correct Answer:** A.
    - **Explanation:** You should ensure that the company has the proper licenses to install 20 additional copies to be compliant with licensing. Microsoft Office is not open source. Using a personal license key from an existing system violates the license agreement. Simply following normal installation procedures does not ensure license compliance.
10. **Your office is moving from one floor of a building to another, and you are part of the moving crew. When moving computer equipment, which of the following are good procedures to follow? (Choose two.)**
    - A. Lift by bending over at the waist.
    - B. Carry CRT monitors with the glass face away from your body.
    - C. Use a cart to move heavy objects.
    - D. Ensure that no safety hazards are in your path.
    - **Correct Answer:** C, D.
    - **Explanation:** You should use a cart to move heavy objects. You should also ensure that no safety hazards are in your path. Lifting by bending at the waist can cause back injury. Carrying CRT monitors with the glass facing outward is unsafe because the weight is furthest from your body.
11. **You just removed four AA alkaline batteries from a remote-control device. What is the recommended way to dispose of these batteries?**
    - A. Throw them in the trash.
    - B. Incinerate them.

- C. Take them to a recycling center.
- D. Flush them down the toilet.
- **Correct Answer:** C.
- **Explanation:** Alkaline batteries should be taken to a recycling center. Throwing batteries in the trash is not environmentally responsible. Incinerating batteries is not advisable as they can explode and create pollution. Flushing batteries down the toilet is not an acceptable disposal method.

12. **When replacing a hard drive, you discover prohibited material on a user's laptop. What should you do first? (Choose two.)**
    - A. Destroy the prohibited material.
    - B. Confiscate and preserve the prohibited material.
    - C. Confront the user about the material.
    - D. Report the prohibited material through the proper channels.
    - **Correct Answer:** B, D.
    - **Explanation:** The first step is to confiscate and preserve the prohibited materials on the drive. The next step is to report the prohibited materials through the proper channels. Destroying the material or confronting the user are not appropriate first steps.
13. **You need to investigate how to protect credit card data on your network. Which information should you research?**
    - A. PCI DSS
    - B. GDPR
    - C. PHI
    - D. PII
    - **Correct Answer:** A.
    - **Explanation:** You should research information on the Payment Card Industry Data Security Standard (PCI DSS). GDPR is for protecting EU citizens' data, PHI is protected health information, and PII is personally identifiable information. PCI DSS specifically addresses credit card data.
14. **Which class of fire extinguisher is recommended for use in a wood and paper fire?**
    - A. A
    - B. B
    - C. C
    - D. D
    - **Correct Answer:** A.
    - **Explanation:** Wood and paper fires can be put out by a Class A fire extinguisher. Class B is for flammable liquids, Class C for electrical fires, and Class D for flammable metals.
15. **Which of the following are common types of screwdrivers? (Choose two.)**
    - A. Circular
    - B. Phillips
    - C. Torx
    - D. Helix
    - **Correct Answer:** B, C.

- **Explanation:** Phillips and Torx are two common types of screwdriver. Circular and Helix are not types of screwdrivers.

16. **Which of the following are elements of a good workplace safety plan? (Choose two.)**
    - A. Periodic workplace inspections
    - B. A training program
    - C. Punishing employees for reporting safety violations
    - D. An independent third-party auditor of the safety plan
    - **Correct Answer:** A, B.
    - **Explanation:** Periodic workplace inspections and a training program are good components to implement in a safety plan. Employees cannot be punished for reporting safety violations. Third-party audits are not necessary but can complement inspections and training.
17. **What is the recommended use policy on magnetic-tipped screwdrivers inside computers?**
    - A. Do not use them.
    - B. It's okay to use them, but keep them away from the processor.
    - C. It's okay to use them, but keep them away from the RAM.
    - D. It's okay to use them, but only if they're of the powered variety.
    - **Correct Answer:** A.
    - **Explanation:** A good rule of thumb when it comes to magnetic-tipped screwdrivers is to avoid using them inside a computer case. Magnetic tools can damage data on disks that use magnetic storage schemes. They should not be used inside a computer regardless of what component they are near or if they are powered.
18. **Which of the following are usually contained on an MSDS? (Choose two.)**
    - A. Freezing point
    - B. Handling and storage instructions
    - C. Personal protection instructions
    - D. Salinity levels
    - **Correct Answer:** B, C.
    - **Explanation:** Material safety data sheets (MSDSs) contain handling and storage instructions as well as personal protection instructions. MSDSs do not typically contain freezing point specifications or salinity levels.
19. **Which of the following are OSHA requirements for a safe work environment that must be followed by employees? (Choose two.)**
    - A. Immediately report all accidents to OSHA.
    - B. Use protective gear and equipment.
    - C. Attend safety training.
    - D. Follow all employer-implemented health and safety rules.
    - **Correct Answer:** B, D.
    - **Explanation:** To maintain a safe work environment, all employees must follow certain protocols. These include using protective gear and equipment and following all health and safety rules. Accidents should be reported to the

employer, not necessarily OSHA directly. Safety training is for employers to provide, not a requirement for employees to attend, though it is encouraged.

20. **Which of the following types of batteries are not considered environmental hazards?**
    - A. Alkaline
    - B. Nickel-metal hydride (NiMH)
    - C. Nickel-cadmium (NiCd)
    - D. Button cell
    - **Correct Answer:** B.
    - **Explanation:** Nickel-metal hydride (NiMH) batteries are not considered environmental hazards. Alkaline batteries (due to historical mercury content), Nickel-cadmium (NiCd) batteries, and button cell batteries are considered environmental hazards.

Of course! Here is the final formatted list of questions for Chapter 22.

Chapter 22: Documentation and Professionalism

1. **You just finished repairing a network connection, and in the process you traced several network connections. Which type of documentation should you create so that another technician does not need to repeat the task of tracing connections?**
    - A. Logical diagram
    - B. Knowledge base article
    - C. Change management document
    - D. Physical diagram
    - **Correct Answer:** D.
    - **Explanation:** A physical network diagram details all connections so that the next technician does not need to trace connections. A logical network diagram shows the flow of information. A knowledge base article documents a symptom and solution for a problem but not the connections.
2. **You are executing the primary plan in the change management documentation and realize that you cannot proceed. Which section details the original configuration?**
    - A. Purpose
    - B. Risk analysis
    - C. Rollback
    - D. Plan for change
    - **Correct Answer:** C.
    - **Explanation:** The rollback section contains the original configuration that can be used to revert the changes. The purpose section contains the reason for the proposed change. The risk analysis section explains the risks involved with the proposed changes. The plan for change section contains the primary change configuration and the alternate change configuration.

3. **Which section of the change management documentation contains whom the change will affect?**
    - A. Business processes
    - B. Scope of change
    - C. User acceptance
    - D. Plan for change
    - **Correct Answer:** B.
    - **Explanation:** The scope of change section details whom the change will affect. The business processes section details the current business processes the change will affect. The user acceptance section details how the changes were tested and accepted by the users. The plan for change contains the primary and alternate plans for the proposed change.
4. **You just had an outage of Internet connectivity. Which document should you complete so that stakeholders understand the reason for the outage?**
    - A. Change management documentation
    - B. Knowledge base article
    - C. Acceptable use policy
    - D. Incident documentation
    - **Correct Answer:** D.
    - **Explanation:** Incident documentation should be completed so that key stakeholders can understand the reason for the outage. Change management documentation is used for proposed changes to the network. Knowledge base articles are used to document symptoms and solutions. An acceptable use policy (AUP) is used to protect an organization's resources from user abuse.
5. **Which regulation is enforced by the Securities and Exchange Commission (SEC) to regulate financial records and sensitive financial information?**
    - A. SOX
    - B. FERPA
    - C. HIPAA
    - D. GLBA
    - **Correct Answer:** A.
    - **Explanation:** The Sarbanes–Oxley Act (SOX) is enforced by the Securities and Exchange Commission (SEC) and regulates sensitive financial information and financial records. The Family Educational Rights and Privacy Act (FERPA) affects education providers and organizations that process student records. The Health Insurance Portability and Accountability Act (HIPAA) affects health-care providers and providers that process health records. The Gramm–Leach–Bliley Act (GLBA) affects providers of financial services and safeguards customer information.
6. **You are currently troubleshooting a network issue. Which type of diagram allows you to view the flow of information from a high-level overview? (Choose the best answer.)**
    - A. Logical diagram
    - B. Physical diagram

- C. Symbol diagram
- D. Knowledge base article
- **Correct Answer:** A.
- **Explanation:** A logical diagram is a high-level overview of a system so that you can see the flow of information. A physical diagram shows specifics, and although it can be used to trace the flow of information, it is not used as a high-level overview. A symbol diagram is not a type of diagram. A knowledge base article details a solution for symptoms and is not used to view the flow of information.

7. **End users are abusing the email system by selling personal items. Which policy would detail the proper use of the email system for business purposes?**
   - A. MDM
   - B. Password policy
   - C. AUP
   - D. Incident management
   - **Correct Answer:** C.
   - **Explanation:** The acceptable use policy (AUP) details the acceptable use of the email system for business purposes. Mobile device management (MDM) is software that allows you to manage mobile devices in the workplace. A password policy details the appropriate handling and management of passwords. Incident management is how a network or security incident is handled.
8. **Which backup media is the fastest from which to recover?**
   - A. Disk-to-tape
   - B. Disk-to-disk
   - C. Disk-to-flash
   - D. Disk-to-cloud
   - **Correct Answer:** B.
   - **Explanation:** Disk-to-disk is the fastest recovery method and backup method as well, because you are backing up from a disk to another disk attached via the network. Disk-to-tape is slower because you must re-tension the tape and then locate the data on the tape to recover it. Disk-to-flash is not a backup method, because of the price of flash. Disk-to-cloud is the slowest recovery method because you must recover from the cloud over a network connection.
9. **You need to upgrade a server and want to make a backup of the data before you begin. Which backup method should you choose so that your normal backups are not affected?**
   - A. Full
   - B. Copy
   - C. Incremental
   - D. Differential
   - **Correct Answer:** B.
   - **Explanation:** You should use the copy backup method, since it will perform a full backup of the files without resetting the archive bits. A full backup makes a full backup and resets all the archive bits affecting the normal backups. An

incremental backup copies only the files that have changed since the last backup and leaves the archive bits unchanged. A differential backup backs up only the files that have changed since the last backup and then resets all the archive bits.

10. **Which type of power protection is used between the electricity coming into the premises and the power meter, to protect from surges in electricity?**
    - A. Surge protector strip
    - B. Uninterruptable power supply
    - C. Service entrance surge protection
    - D. Generator
    - **Correct Answer:** C.
    - **Explanation:** A service entrance surge protection is used between the power meter and the main breakers, to protect from electrical surges. A surge protector strip is found under desks to protect from electrical surges. An uninterruptable power supply (UPS) is used as a backup power source until power is restored or conditioned properly. A generator is used during power outages to sustain power.
11. **You promised a customer that you would be out to service their problem before the end of the day but have been tied up at another site. As it now becomes apparent that you will not be able to make it, what should you do? (Choose the best answer.)**
    - A. Arrive first thing in the morning.
    - B. Wait until after hours and then leave a message that you were there.
    - C. Call the customer and inform them of the situation.
    - D. Email the customer to let them know that you will be late.
    - **Correct Answer:** C.
    - **Explanation:** Calling the customer and informing them of the situation is the best action that can be performed, since you are having direct communications. Arriving first thing in the morning should be done, but communications is the first action. Waiting until after hours and then leaving a message is not an appropriate action. Sending an email letting the customer know that you will be late is lying, since you will not make it to their site.
12. **A user reports that a workstation has two significant problems that do not seem related. How should you approach these problems?**
    - A. Look for what the two problems would have in common.
    - B. Assume that a virus is involved.
    - C. Deal with each issue separately.
    - D. Order a new machine.
    - **Correct Answer:** C.
    - **Explanation:** If the problems do not appear to be related, then deal with them separately. Looking for commonalities between the problems would just waste valuable time. No assumptions should be made, such as that a virus is causing the problem, unless there is proof. Ordering a new machine is disruptive to the customer, unless the problem dictates that this action be performed.

13. **A customer is trying to explain a problem with their system. Unfortunately, the customer has such a thick accent that you are unable to understand their problem. What should you do? (Choose the best answer.)**
    - A. Just start working on the system and look for obvious errors.
    - B. Call your supervisor.
    - C. Ask that another technician be sent in your place.
    - D. Apologize and find another user or manager who can help you translate.
    - **Correct Answer:** D.
    - **Explanation:** If you do not understand the customer, you should apologize, treat the customer with respect, and seek a manager to help translate. Ignoring the customer and starting to work on the system is not an appropriate response. Calling your supervisor will not solve the problem, since your supervisor will have the same issue. Asking that another technician be sent in your place is being insensitive to the customer and "passing the buck".
14. **You have been trying to troubleshoot a user's system all day when it suddenly becomes clear that the data is irretrievably lost. When you inform the customer, they become so angry that they shove you against a wall. What should you do?**
    - A. Shove the user back, only a little harder than they shoved you.
    - B. Shove the user back, only a little easier than they shoved you.
    - C. Try to calm the user down.
    - D. Yell for everyone in the area to come quickly.
    - **Correct Answer:** C.
    - **Explanation:** You should avoid confrontations with the user by attempting to calm them down. You should never shove the user back. Yelling for everyone in the area to come quickly will escalate the situation.
15. **A customer tells you that a technician from your company spent three hours on the phone making personal calls. What should you do with this information?**
    - A. Nothing.
    - B. Inform your manager.
    - C. Talk to the technician personally.
    - D. Ask the customer to prove it.
    - **Correct Answer:** B.
    - **Explanation:** You should take appropriate action and inform your manager, as well as notify the customer that you've done so. Doing nothing is not an appropriate response to this situation. Talking to the technician personally will create a confrontation and should be avoided. Asking the customer to prove it is an inappropriate action to this problem.
16. **You arrive at the site of a failed server to find the vice president nervously pacing and worrying about lost data. What should you do?**
    - A. Offer a joke to lighten the mood.
    - B. Downplay the situation and tell him that customers lose data every day.
    - C. Keep your head down and keep looking at manuals to let him know that you are serious.

- D. Inform him that you've dealt with similar situations and will let him know what needs to be done as soon as possible.
- **Correct Answer:** D.
- **Explanation:** You should assure the vice president that you are optimistic and skilled to deal with these problems. Offering a joke is an inappropriate action. Downplaying the situation does not show respect to the customer's problem. Keeping your head down and ignoring the customer does not display appropriate communications.

17. **You are temporarily filling in on phone support when a caller tells you that they are sick and tired of being bounced from one hold queue to another. They want their problem fixed, and they want it fixed now. What should you do?**
    - A. Inform them up front that you are only filling in temporarily and won't be of much help.
    - B. Transfer them to another technician who handles phone calls more often.
    - C. Try to solve their problem without putting them on hold or transferring them elsewhere.
    - D. Suggest that they call back at another time when you are not there.
    - **Correct Answer:** C.
    - **Explanation:** You should try to solve the customer's problem without further escalating the frustration by putting them on hold or transferring them. Informing them that you won't be able to help is only going to anger the caller, further validating their frustration. Transferring them to another technician is not the appropriate action, because it will add to their frustration. Suggesting that they call back will create more frustration and is poor customer service.
18. **At the end of the day, you finish a job only to find that the user you were doing it for had to leave. What should you do? (Choose two.)**
    - A. Clean up and leave no evidence that you were there.
    - B. Leave a note for the user detailing what was done and how to contact you.
    - C. Notify the user's manager and your own manager that you have finished.
    - D. Put the system back to its original state.
    - **Correct Answer:** B, C.
    - **Explanation:** Leaving a note for the user detailing what was done and how to contact you displays appropriate communications. Notifying the user's manager and your own manager that the problem is resolved is also appropriate communications. Cleaning up and leaving no evidence that you were there is an inappropriate action, as it is deceiving to the user. Putting the system back to its original state is an inappropriate action because it does not solve the problem.
19. **A user on the phone does not seem to be able to explain their problem to you without using profanity. That profanity is making you unable to understand their problem. What should you do? (Choose the best answer.)**
    - A. Ask the user to refrain from the offensive language.
    - B. Overlook the profanity.
    - C. Hang up.
    - D. Show them that you know just as many expletives as they do.

- **Correct Answer:** A.
- **Explanation:** While the user's profanity is likely linked to frustration, it hinders the communication and should be eliminated. You should ask the user to refrain from the offensive language. There may be circumstances where it is necessary to overlook the profanity, if your request is likely to make the already upset customer even angrier, as long as you can understand what is being said. Hanging up is not an appropriate action and will further the user's frustration. Firing back with profanity is not an appropriate response, as it will escalate the situation further.

20. **Which of the following is not a benefit of implementing asset tags for inventory management?**
    - A. Tracking of the equipment
    - B. Scheduling the depreciation of the equipment
    - C. Identifying assets
    - D. Providing ownership of the equipment
    - **Correct Answer:** B.
    - **Explanation:** Scheduling of the depreciation of the equipment is performed in accounting software and is not a benefit of implementing asset tags for inventory management. Tracking of the equipment is a benefit to an asset tag. Identifying assets is a direct benefit of asset tags. An asset tag provides proof of ownership.