CompTIA 220-1102

Exam Code: 220-1102

Title : CompTIA A+ (Core 2)

QUESTION 1
What type of structure is "For Next" in scripting?

A. Loop
B. Branch
C. Constant
D. Variable

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.8: A loop deviates from the initial program path to some sort oflogic condition. In a loop, the computer repeats the task until a condition is met. Often implemented with For, For Next, While, or Do While statements. For example, a short script like (For i=I to 100, print I, next) would print the numbers from I to I 00 to the screen. A constant is a specific identifier that contains a value that cannot be changed within the program. For example, the value to convert a number from F to Cis always 5/9 because the formula is C = (F -32) * 5/9. A branch is used to control the flow within a computer program or script, usually based on some logic condition. Often, these are implemented with IF THEN ELSE statements. A variable is a placeholder in a script containing a number, character, or string of characters. Variables in scripts do not have to be declared (unlike in programming Languages) but can be assigned a value. Then, the variable name is referenced throughout the script instead of the value itself.

QUESTION 2
While investigating a data breach, you discover that the account credentials used belonged to an employee who was fired several months ago for misusing company IT systems. The IT department never deactivated the employee's account upon their termination. Which of the following categories would this breach be classified as?

A. Advanced persistent threat
B. Insider Threat
C. Known threat
D. Zero-day

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: An insider threat is any cwTent or former employee, contTactor, or business partner who has or had authorized access to an organization's network, system, or data and intentionally exceeded or misused that access in a manner that negatively affected the confidentiality, integrity, or availability of the organization's information or information systems. Based on the details provided in the question, jt appears the employee's legitimate credentials were used to conduct the breach. This would be classified as an insider threat. A zero-day is a vulnerability in software unpatched by the developer or an attack that exploits such a vulnerability. A known threat is a threat that can be identified using a basic signature or pattern matching. An advanced persistent threat (APT) is an attacker with the ability to obtain, maintain, and diversify access to network systems using exploits and mal ware.

QUESTION 3
You are configuring a SOHO network for a small coffee shop. They have found that certain customers will buy a single coffee cup and then sit at the coffee shop aU day to use the WiFi. The owner has asked you to block this customer's laptop from connecting by placing it on a blocklist. Which of the following configurations would you use to blockJist this customer's device based on its unique hardware identifier?

A. Enforce a WPA2 password

B. Port filtering
C. MAC fi ltering
D. Poti forwarding

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: MAC filtering is the application of an access control list to a switch or access point so that only clients with approved MAC addresses connect. Port forwarding allows a router to take requests from the Internet for a particular application and send them to a designated host on the LAN. An allow list is a form ofprotection where only the items identified specifically on the list are allowed, whereas all others are denied. For example, if you create an access control list that relies on an allow list, it would block evety IP address that is not found in the allow I ist. A blockJist contains every address or port that is blocked fi·om accessing the network.

QUESTION 4
A penetration tester sends an email out to 100,000 random email addresses. In the email the attacker sent, it claims that "Your Bank of America account is locked out. Please click here to reset your password." Which of the following attack types is being used?

A. Vishing
B. Phishing
C. Spear phishing
D. Whaling

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: Phishing is an emai l-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to induce targeted individl!lals to reveal confidential information. Spear phishing attacks focus on a targeted set of people, not just an indiscriminate large group of random people. Whaling is an email-based or web-based form of phishing that targets senior executives or wealthy individuals. Vishing is a social-engineering attack where the attacker extracts information while speaking over the phone or leveraging IP-based voice messaging services (VoiP).

QUESTION 5
Which of the following macOS features is used to backup and restore files to an external hard disk?

A. Time Machine
B. Boot Camp
C. Snapshot
D. Remote disc

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.10: Time Machine is the built-in backup feature of the macOS operating system. The Time Machine utility enables data to be backed up to an external drive. By default, Time Machine keeps hourly backups for the past 24 hours, daily backups for a month, and weekly backups for all previous months. When the drive used to store
backups becomes full, Time Machine removes older backups to free up space. Time Machine automatically backs up all of the system's files, including apps, music, photos, email, documents, and system fi les. Once a user has a valid backup in Time Machine, they can restore files from the backup if the original files are ever

corrupted or deleted on their Mac or if the hard disk (or SSD) is erased or replaced. Remote disc is a feature in macOS that enables a user to access a CD/DVD on another Mac or Windows computer. This was created because Apple's Mac compll!ters have not been sold with an internal optical drive since 20 16. Boot Camp is "Best Material, Great Results". ~W.:f&_r:t;~i.t:tC:!~Qm,~.Q.I!l. 4

used to allow dual booting on a Macintosh computer. It allows the user to boot into either macOS (OS X) or Windows as the computer is rebooted. Boot Camp is only supp01ied on Intel-based macOS systems, though. A snapshot is used to backup virtual machines by creating a state of the disk at a particular point in time. Snapshots allow a technician to roll back any changes made to a VM during a session if needed.

QUESTION 6
A company has had several virus infections over the past few months. The root cause was determined to be known vulnerabilities in the software applications in use by the company. What should an administrator implement to prevent future outbreaks?

A. Incident response team
B. Patch management
C. Acceptable use policies
D. Host-based intrusion detection systems

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.11: Since the viruses exploited known vulnerabilities, there should be patches available from the manufacturer/vendor. Patch management is the process of di stributing and applying updates to the software to prevent vulnerabilities from being exploited by an attacker or mal ware. Proper patch management is a technical control that would prevent future outbreaks. An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network or the Internet. While some items in the AUP might help prevent a malware infection (such as not al.lowing users to download and run programs from the internet), it is considered an administrative control, and choosing a technical control like patch management would better protect the network. An incident response team or emergency response team is a group of people who prepare for and respond to any emergency incident, such as a natural disaster or an interruption of business operations. An incident response team wi IL respond to the virus infections, but they would not prevent them from occurring. Host-based intrusion detection systems (RIDS) help organizations to identify threats inside the network perimeter by monitoring host devices for malicious activity that, if left undetected, could lead to serious breaches. A HIDS may detect the effects of a virus infection, such as a client becoming a zombie in a botnet, but it will not prevent these outbreaks from occurring.

QUESTION 7
Which Linux command is used to print the full contents of a file to the screen at once?

A. grep
B. cat
C. dig
D. ls

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.11: The cat (short for "concatenate") command is one of the most frequently used commands in Linux/ Unix. The cat command allows the creation of single or multiple fi les, view file contents, concatenate files, and redirect output in the termina l to a file. The grep is a command-line utility for searching plain-text data sets for lines that match a regular expression. The grep command works on Unix, Linux, and macOS operating systems. Grep is an acronym that stands for Global Regular Expression Print. The dig command is used to

query the domain name system (DNS) to obtain information about host addresses, mail exchanges, nameservers, and related information. The ls command lists the files or directories in the current path of a Unix, Linux, or Mac operating system. When invoked without any arguments, ls lists the fi les in the cun-ent working directory.

QUESTION 8
Which of the following data types would be used to store the user's middle initial?

A. Boolean
B. String
C. Character
D. Integers

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.8: A character stores a single character, such as J, D, or Z. A character data type usually consumes one byte (8 bits) of storage. A string stores a group of characters, such as Hello, PYTHON, or JasonDion. A string data type usually consumes as much storage as necessary. Each character in the string usually requires 1 byte of storage. A boolean stores a value of TRUE (1) or FALSE (0). It usually consumes only 1 bit of storage (a zero or a one). An integer stores a whole number, such as 21, 143, or 1024. An integer data type usually consumes 8 bytes of storage.

QUESTION 9
Which of the following types of attacks are usually used as part of an on-path attack?

A. Brute force
B. Spoofing
C. DDOS
D. Tailgating

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: Spoofing is often used to inject the attacker into the conversation path between the two parties. Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. An on-path attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. The attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection. The attacker will intercept all relevant messages passing between the two victims and inject new ones. A Distributed Denial of Service (DOoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic fi·om multiple sources. Tailgating is a social engineering technique to gain access to a building by following someone unaware of their presence. A brute-force attack consists of an attacker submitting many passwords or pass phrases with the hope of eventually guessing correctly.

QUESTION 10
A salesperson uses their smartphone as a hotspot while traveling. The first week of their trip, their smartphone could download files at 24 Mbps and stream online videos without any problems. Unfortunately, this week their smartphone is only operating at 256 Kbps when they attempt to download a file. Additionally, they are having diifficulty watching online videos due to excessive buffering. Which of the following is MOST likely the problem?

A. The smartphone's hotspot is defedive

B. The smartphone is overheating
C. The smartphone is not connected to WiFi
D. E. The smartphone's data connection is being throttled

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3 .4: Throttling occurs when an internet service provider purposely slows down a user's data transmission. If a device is getting lower speeds without any corresponding device issues, it is likely a result of throttling by the service provider. Most smartphone plans come with a limited amount of fullspeed bandwidth, after which the connection is throttled to a slower speed until the next month's plan begins.

QUESTION 11
You are partitioning a 1 TB hard drive on a new workstation. The hard disk has been partitioned into four different partitions with I 00 GB, 150 GB, 250 GB, and 500 GB. How many different file system types could you support on this 1 TB hard drive?

A. 4
B. 3
C. 2
D. 1

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.9: Partitioning is the act of dividing a physical disk into logically separate storage areas, ofiten referred to as drives. Each partition can be formatted with any fi le system type. Since there are 4 distinct partitions on this single hard drive, it can support up to 4 different file systems.

QUESTION 12
You have been asked to install a new hard drive in a Windows 10 system. You have already installed the hard drive and booted the system up. Which tool should you use to create the new partitions on the hard drive?

A. Disk Management
B. DxDiag
C. Disk Defragmenter
D. Dd

Correct Answer: A
Explanation

Explanation/Reference:
OBJ- 1.3: The disk management tool is used to display the drive status, mount the drive, initialize the drive, and create/split/extend/shrink drive partitions. The DxDiag (DirectX Diagnostic) utility is used to collect info about devices to help troubleshoot problems with DirectX sound and video. It is a diagnostics tool used to test DirectX functionality and troubleshoot video-related or sound-related hardware problems. DirectX Diagnostic can save text files with the scan results. The disk defragmenter utility is used to rearrange fragmented data so that disks and drives can operate more efficiently. Disk defragmenter runs on a schedule, but can also analyze and defragment di sks and drives manually. The dd command is a Linux utility that is used to copy and convert raw data from one source to another such as a hard disk to an image file.

QUESTION 13
Dion Training uses DHCP to assign private Class C IP addresses to its Windows 10 workstations.
Which of the following IP addresses is a Class C address?

A. 192.168.3.5
B. 172.18.21.25
C. 10.1.2.3
D. 169.254.1.52

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.6: Private IP addresses are any addresses in a specified range that are not allowed to be routed over the Internet. This allows companies to use these private IP addresses in their local area networks without having to purchase them from an internet registry. The class A private IP address range contains the addresses from [0.0.0.0 to 10.255.255.255.255. The class B private IP address range contains the addresses from 172.16.0.0 to 172.31.255.255. The class C private IP address range contains the addresses from 192.168.0.0 to 192.168.255.255. The APIPA/link-local autoconfiguration range is from 169.254.0.0 to 169.254.255.255.

QUESTION 14
You are troubleshooting a user's computer. As part of your efforts, you want to install a new login with administrative privileges. Which of the following utilities should you use?

A. System Information
B. System Configuration
C. Group Policy
D. Local Users and Groups

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.1: Local users and groups (lusnngr.msc) is a utility used to assign rights and roles to different users and groups on a local computer. Group policy editor (gpedit.msc) is a utility used to define and control how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, a group policy is applied to users or computers based on their membership in sites, domains, or organizational units. System configuration (msconfig.exe) is a system utility to troubleshoot the Microsoft Windows startup processes. MSConfig is used to disable or re-enable software, device drivers, and Windows services that run at startup, or to change boot parameters. System infotmation (msinfo32.exe) is a utility that gathers information about your computer and displays a comprehensive list of hardware, system components, and the software environment that can be used to diagnose computer issues.

QUESTION 15
Christina recently purchased a new Android smartphone and is going on a trip. At the airport, she found a public wireless network called "FreeAirportWiFi" and connects to it. She noticed a question mark (?) icon showing in the toolbar next to the Wi-Fi icon. Christina attempts to open a webpage but gets an error of "The page cannot be displayed." She begins to troubleshoot the device by verifying that the airplane mode is disabled, Bluetooth is enabled, and tethering is enabled. Next, Christina attempts to make a phone call, which works without any issues. Which of the following is MOST likely the issue with Christina's smartphone?

A. The smartphone's SIM card is deactivated
B. The smartphone is connected to the FreeAirportWifi but is not authenticated yet
C. The smartphone does not have a valid data plan enabled
D. The smartphone can only support 3G data networks

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.5: When an Android smartphone is connected to the Wi-Fi but shows a question mark(?) next to the Wi-Fi's radio icon, this indicates that there is a lack of internet connectivity on the current wireless network. It appears that Christina's smartphone is fully connected to the FreeAirportWiFi, but she has not completed the authentication. These types of public wireless networks often have a captive portal or redirect page with the Acceptable Use Policy that must he accepted before giving the smartphone full connectivity to the internet. Once the acceptance is made to the captive portal, the smartphone is logically connected to the internet, and the question mark will be removed.

QUESTION 16
A hospital's file server has become infected with malware. The files on the server all appear to be encrypted and cannot be opened. The network administrator receives an email firom the attacker asking for 20 bitcoin in exchange for the decryption key. Which type of malware· MOST likely infected these computers?

A. Ransomware
B. Spyware
C. Keylogger
D. Rootkit

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.3: Ransomware is a type ofmalware designed to deny access to a computer system or data until a ransom is paid. Ransom ware typically spreads through phishing emails or by unknowingly visiting an infected website. Once infected, a system or its files are encrypted, and then the decryption key is withheld from the victim unless payment is received. Spyware is a program that monitors user activity and sends the information to someone else. It may be installed with or without the user's knowledge. It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms, or external users. A key logger actively attempts to steal confidential information by capturing the data when entered into the computer by the user. This is done by recording keystrokes entered into a web browser or other application. A software key logger can be run in the background on a victim's computer. A hardware keylogger may be placed between the USB port and the wired keyboard. A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. A rootkit is generally a collection of tools that enabled administrator-level access to a computer or network. They can often disguise themselves from detection by the operating system and anti-malware solutions. If a rootkit is suspected on a machine, it is best to reformat and reimage the system.

QUESTION 17
Dion Training is concerned with the possibility of employees accessing another user's workstation in secured areas without their permission. Which of the following would BEST be able to prevent this from happening?

A. Require biometric identification for user logins
B. Enforce a policy that requires passwords to be changed every 30 days
C. Require a username and a password for user logins
D. Install security cameras in secuTe areas to monitor log ins

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.1: The BEST choice is to implement biometric identification for user logins, such as a fingerprint reader or a retina scanner. This would ensure that even if an employee could discover another employee's usemame and password, they would be prevented from logging into the workstation without the employee's finger or eye to scan. Enforcing short password retention can limit the possible damage when a password is disclosed, but it won't prevent a login during the valid period. Security cameras may act as a deterrent or detective control, but

they cannot prevent an employee from logging into the workstation as another employee. Security cameras could be used to determine who logged in after the fact, though.

QUESTION 18
Which of the following backup rotation schemes requires at least one monthly full backup to be stored safely off-site?

A. Tower of Hanoi
B. Grandfather-father-son
C. FIFO Backup
D. 3-2-1 backup

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.3: The 3-2-1 backup rule states that an organization should create (3) one primary backup and two copies of the data, (2) save the backups to two different types of media, and (1) keep at least one backup copy off-site. The grandfather-father-son (GFS) backup rotation scheme is widely used to combine full and incremental backups to reduce backup time and enhance storage security. The grandfather is a ful ~ backup that is stored off-site once per month. The father is a weekly full backup that is conducted. The son is an incremental or differential backup conducted each day. For example, each Monday a full backup can be conducted whiclh becomes the father. Then, each day of the week a son is created by performing an incremental or differential backup. Once per month, a full backup is conducted to become the grandfather. The Tower of Hanoi is a backup rotation scheme that rotates backup media sets throughout the backup process to minimize wear and failure of tape backup media. For example, when using this method with four backup tapes labeled A, 8 , C, and D, a total of 16 days of backups can be maintained with just 4 tapes. Tape A is used every odd-numbered day for 16 days. Tape 8 is used on days 2, 6, 10, and 14. Tape C is used on days 4 and 12. TapeD is used on days 8 and 16. This allows Tape A to be overwritten evety other day, while Tapes B is overwr itten every four days and Tapes C and D are overwritten every 8 days. The First In First Out (FIFO) backup scheme uses a set number of tapes and overwrites the oldest tape with the newest information. For example, if there are 7 tapes in use, every evening a new backup is conducted over the previous week's daily backup. To have a longer amount of days of backups, a technician simply needs to increase the number of tapes from 7 to 14 or 21 .

QUESTION 19
A customer is complaining that her laptop is too slow. You have thoroughly checked the device but cannot find anything wrong with it. Which of the foUowing is the best thing to say NEXT?

A. "Excuse me for a moment; my phone is buzzing."
B. "Can you tell me more about the problem? What do you mean by 'it is acting slow'?"
C. "I found nothing wrong with this laptop that would make it slow."
D. "I don't understand what you are complaining about; this laptop seems plenty fast to me."

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4. 7: When dealing with a difficult customer or situation, you should follow five key principles: (I) Do not argue with customers and/or become defensive; (2) Avoid dismissing customer problems; (3) Avoid being judgmental; (4) Clarify customer statements (ask open-ended questions to narrow the problem's scope, restate the issue, or question to verify understanding); and (5) Do not disclose experiences via social media outlets. The only option that follows these principles is asking the customer a more clarifying, openended question. The other three options all violate these principles.

QUESTION 20
A cybersecurity analyst from BigCorp contacts your company to notify them that several of your computers

were seen attempting to create a denial of service condition against their servers. They believe your company has become infected with mal ware, and those machines were part of a larger botnet. Which of the following BEST describes your company's infected computers?

A. Zero-day
B. Zombie
C. Monsters
D. Bugs

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: A zombie is a computer connected to the internet that has been compromised by a hacker, computer virus, or trojan horse program and can be used to perform malicious tasks of one sort or another und!er remote direction. Botnets of zombie computers are often used to spread email spam and launch denial-of-service attacks (DoS attacks). A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited, and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability, hence the term zero-day. A software bug is an error, flaw, or fault in an application. This error causes the application to produce an unintended or unexpected result, such as crashing or producing invalid results.

QUESTION 21
You are troubleshooting a user's workstation that is operating extremely slowly. You open the Task Manager and see that only Microsoft Word is currently running, but the CPU and network utilization is consistently running between 95-100%.
Which of the following is MOST likely causing this issue?

A. The computer is the victim of a DoS attack
B. The network's firewall is blocking outbound traffic
C. The computer has become a zombie
D. The application is not compatible with this OS

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.2: The workstation has most likely become a zombie. A zombie is any workstation running unauthorized software that directs the device to participate in a DDoS attack as part of a larger botnet. A botnet is a network of computers that have been compromised by a Trojan, rootkit, or worm mal ware. This workstation would then attempt to flood the victim's computer with requests over the network. These requests would require CPU and network resources to make, causing the utilization to rise to 95-100% resource utilizabon. Since Microsoft Word can run macros, it is possible it has become infected and is now part of a larger botnet.

QUESTION 22
Which of the following types of wireless encryption uses a 40-bit encryption key with an RC4 encryption cipher?

A. WPA2
B. WEP
C. Open
D. WPA

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.2: The Wired Equivalent Privacy (WEP) encryption system is based on the RC4 encryption cipher. WEP uses a 40-bit enctyption key and a 24-bit initialization vector by default, creating a 64-bit key. Newer versions of WEP support a 128-bit key size. A larger encryption key creates stronger encryption and is more difficult to attack. WEP is considered weak by today's standards and should be replaced by WPA2 or strong encryption schemes. Wi-Fi protected access (WPA) is an improved encryption scheme for protecting Wi-Fi communications designed to replace WEP. WPA uses the RC4 cipher and a temporal key integrity protocol (TKIP) to overcome the vulnerabilities in the older WEP protection scheme. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.1 1 i security standard. WP A2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WP A2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption. An open network does not use an encryption key or preshared key to protect the network.

QUESTION 23
An Android user recently cracked their screen and had it replaced. If they are in a dark room, the phone works fine. If the user enters a room with normal lights on, then the phone's display is dim and hard to read. What is MOST likely the problem?

A. Auto-brightness is enabled
B. Faulty ambient light sensor
C. Low battery
D. Defective display

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: The ambient light sensor appears to be broken or malfunctioning. The ambient light sensor may be too sensitive as it is taking in more light than usual. This can occur if the sensor is faulty or if the screen was replaced ly, and the technician forgot to install the black gasket around the ambient light sensor. The auto-brightness setting being enabled would increase the brightness in a lit room and decrease the brightness in a dark room. If the device has a low battery, it may dim the display to save battery life but it would still be readable. If the display was defective, it would be difficult to read in all light conditions and not just in the bright room.

QUESTION 24
A user contacts the service desk, stating their account is locked out, and they are unable to login to their local workstation. Which of the following log files should you review to determine the source of the lockout on the local workstation·?

A. Security log
B. System log
C. Setup
D. Application log

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3. 1: The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems. The security log contains information regarding audit data and security on a system. For example, the security log contains a list of every successful and failed login attempt. The fi le (security.evtx) is stored in the %System Root%\System32\ Winevt\Logs\ folder and can be opened using the Event Viewer. The application log contains information regarding application errors. The file (application.evtx) is stored in the %System Root% \System32\ Winevt\Logs\ folder and can be opened using the Event Viewer. The setup log contains a record of

the events generated during the Windows installation or upgrade process. The file (setup.evtx) is stored in the %System Root%\System32\ Winevt\Logs\ fo lder and can be opened using the Event Viewer. The system log contains information about service load failures, hardware conflicts, driver load failures, and more. The file (system.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer.

QUESTION 25
A network administrator needs to allow employees to upload files to a remote server securely. What port must be allowed through the firewall?

A. 21
B. 161
C. 22
D. 25

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.9: To securely upload a file, the employees could use SFTP (Secure FTP) or SCP (Secure Copy). Both SFTP and SCP operate over port 22, therefore port 22 must be opened by the firewall so that the employees can reach the file servers. Port 21 is used by the File Transfer Protocol, but it is not a secure method of sending files. There is a more secure version of FTP known as FTPS, but that uses port 990. Port 25 is reserved for the simple mail transfer protocol (SMTP), which is an internet standard communication protocol for electronic mail transmission. Port 161 is reserved for simple network management protocol (SNMP), which is a networking protocol used for the management and monitoring of network-connected devices in Intemet Protocol networks.

QUESTION 26
Which of the following policies or plans would describe the access requirements for connecting a user's laptop to the corporate network?

A. Password policy
B. Onboarding policy
C. Bring your own device policy
D. Remote access policy

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.7: A bring your own device (BYOD) policy allows, and sometimes encourages, employees to access enterprise networks and systems using personal mobile devices such as smartphones, tablets, and laptops. A remote access policy is a document that outlines and defines acceptable methods of remotely connecting to the internal network. A password policy is a set of rules created to improve computer security by motivating users to create dependable,. secure passwords and then store and utilize them properly. This document promotes strong passwords by specifying a minimum password length, complexity requirements, requiring periodic password changes, and placing limits on the reuse of passwords. An onboarding policy is a documented policy that describes all the requirements for integrating a new employee into the company and its cultures, as well as getting that new hire all the tools and information they need to begin their job successfully.

QUESTION 27
Which of the following should be implemented to allow wireless network access for clients in the lobby using a shared password as the key?

A. WPA2

B. Firewall
C. IPsec
D. Geofencing

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.2: Wi-Fi Protected Access 2 Pre-Shared Key or WPA2-PSK is a system of encryption used to authenticate users on wireless local area networks using a shared password as the key. WPA2-PSK [AES] is the recommended secure method of making sure no one can listen to your wireless data while it is being transmitted back and forth between your router and other devices on your network. A Firewall is a network secmity device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies,
not a shared password. Internet Protocol Security (IPsec) is a secure network protocol suite that authenticates and encrypts the packets of data to provide secure encrypted communication between two computers over an Internet Protocol network and is used in virtual private networks. A geofence is a virtual perimeter for a real-world geographic area. Geofencing does not use shared passwords to secure your next, it uses GPS coordinates or other location-based data.

QUESTION 28
Which RAID solution will provide the BEST speed and redundancy for a backup and disaster recovery server?

A. RAID 10
B. RAID 0
C. RAID 5
D. RAID l

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.3: RAID 10 provides the system with both speed and efficiency. With RAID 10, the system has a minor of striped disks for full redundancy and double fault tolerance. RAID 10 configuration (also known as RAID 1 +0) requires a mjnimum of four disks and mirrors data across a striped disk pair. This is not only the best option presented in this question but also the most expensive option. A RAID 0 provides disk striping (speed/ performance) but not mirroring with a minimum of two disks. A RAID 1 provides mirroring (redundancy) but not disk striping with a minimum of two disks. A RAID 5 provides block-level striping with distributed parity to provide redundancy using a minimum of three disks.

QUESTION 29
You are troubleshooting an issue with multiple workstations that are having network connectivity issues. The network also bas two servers connected to the network, but they do not have any connectivity issues. You look at the network configuration of the two servers and notice they are using static IP addresses. Based on what you know so far, what is most likely the cause of the workstation's network connectivity issue?

A. The workstations are most likely configured to use dynamically assigned IP addresses and DHCP is not working properly
B. The internet connection for the network is down
C. The wireless network adapter for each workstation was accidentally disabled
D. The network's router is currently down

Correct Answer: A
Explanation

Explanation/Reference:

OBJ-1.6: Based on the symptoms provided, it appears that the servers are using static IP addresses, and the workstations are using dynamically assigned ones. If the DHCP is not functioning properly for the network, any workstations that rely on a dynamically assigned IP address will have connectivity problems. This issue would not affect statica lly assigned machines such as the servers. To fix this issue, the DHCP services need to be restored and be available to accept connections from the clients on the network who require dynamic TP assignments.

QUESTION 30
Which of the following file types are commonly used by network administrators to perform repetitive tasks using a Microsoft proprietary programming language?

A. py
B. vbs
C. js
D. sh

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.8: VBScript is a scripting language based on Microsoft's Visual Basic programming language. Network administrators often use VBScript to perform repetitive administrative tasks. With VBScript, you can run your scripts from either the command-line or the Windows graphical interface. Scripts that you write must be run within a host environment. Windows 10 provides Internet Explorer, liS, and Windows Script Host (WSH) for this purpose. A shell script is a fi le that contains a list of commands to be read and executed by the shell in Limnx and macOS. A .sh file is used for a shell script and its first line always begins with #!/bin/bash that designates the interpreter. This line instructs the operating system to execute the script. Shell scripts al low you to perfonn variot1s functions. These functions include automation of commands and tasks of system administration and troubleshooting, creating simple applications, and manipulating text or files. Python is a general-purpose programming language that can develop many different kinds of applications. It is designed to be easy to read, and the programs use fewer Lines of code compared to other programming languages. The code runs in an interpreter. Python is preinstalled on many Linux distributions and can be installed on Windows. Python scripts are saved using the .py extension. JavaScript is a scripting language that is designed to create interactive web-based content and web apps. The scripts are executed automatically by placing the script in the HTML code for a web page so that when the HTML code for the page loads, the script is run.
JavaScript is stored in a .js file or as part of an HTML file.

QUESTION 31
Mark's laptop is running Windows 10 and appears to become slower and slower over time with use. You decide to check the current CPU utilization and observe that it remains in the 95°/o to 1 00°/o range fairly consistently. You close three of Mark's open applications and recheck the CPU utilization. You notice the utilization dropped to the 30°/o to 35°/o range. A week later, Mark calls you again and says the computer is extremely slow. Which of the following tools can you use to check the CPU utilization and manage any high-resource :processes?

A. Msconfig
B. RDS
C. PerfMon
D. Task Manager

Correct Answer: D
Explanation

Explanation/Reference:
OBJ- 1.3: The task manager is an advanced Windows tool that has 7 tabs that are used to monitor the Processes, Performance, App History, Startup, Users, Details, and Services on a computer. The Processes tab in the task manager is helpful to quickly see how system resources are utilized, help troubleshoot

applications, or find out why the computer is performing slowly. Remote desktop services (RDS) is used to connect to a remote desktop session host servers or other remote computers, edit an existing remote desktop connection (.rdp) configuration file, and migrate legacy connection files that were created with the client connection manager to the newer .rdp connection fi le type. MSConfig is a system utility to troubleshoot the Microsoft Windows startup processes MSConfig is used to disable or re-enable software, device drivers, and Windows services that run at startup, or to change boot parameters. PerfM.on is a performance monitoring and system monitoring uti lity in Windows that is used to monitor the activities on CPU and memory activity on a computer. Performance monitor is used for viewing performance data either in realtime or from a log file. The performance monitor can only monitor the resource utilization, but it cannot manage or terminate those processes.

QUESTION 32
Dion Training wants to provide governance for how employees can utilize the corporate network, email, and laptops while working for the company. Within which of the following should this be documented?

A. Asset management policy
B. Acceptable use policy
C. Password polic
D. Knowledge base

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.1: An acceptable use policy (A UP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network or the internet. For example, an AUP may state that they must not attempt to break any computer network security, hack other users, or visit pornographic websites from their work computer. An asset management policy describes the process of identifying each asset and recording its location, attributes, and value in a database. A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. It contains items like password complexity, password age, and password history requirements. A Knowledge Base (KB) is a reference document that is used to assist a technician when they are installing, configuring, and troubleshooting hardware and software. A knowledge base article might be created by a vendor to support their products, too. A company might create an internal KB, populated with guidelines, procedures, information, and frequently asked questions from their service tickets.

QUESTION 33
A computer was recently infected with a piece of mal ware. Without any user intervention, the malware is now spreading throughout the corporate network and infecting other computers that it finds. Which type of malware MOST likely infected these computers?

A. Trojan
B. Ransomware
C. Virus
D. Worm

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.3: A worm is a standalone malware computer program that replicates itself to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. A worm can spread on its own, whereas a virus needs a host program or user interaction to propagate itself. A virus is malicious software designed to infect computer files or disks when it is activated. A virus may be programmed to carry out other malicious actions, such as deleting files or chan ging system settings. A trojan is a type of mal ware that looks legitimate but can take control of your computer. A

Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. The most common form of a trojan is a Remote Access Trojan (RAT), which allows an attacker to control a workstation or steal infonnation remotely. To operate, a trojan will create numerous processes that run in the background of the system. Ransom ware is a type of mal ware designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Once infected, a system or its fi les are encrypted, and then the decryption key is withheld from the victim unless payment is received.

QUESTION 34
Which of the following should you use to remove any usernames and passwords that you no longer wish to store in Windows 10?

A. Device manager
B. Keychain
C. Credential manager
D. Internet options

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.4: Credential Manager lets you view and delete your saved credentials for signing in to websites, connected applications, and networks. To open Credential Manager, type credential manager in the search box on the taskbar and select the Credential Manager Control panel. You can remove any credentials that you no longer want to store. Removing a credential may also resolve an authentication or service problem. You can view the plaintext of a web credential but not of a Windows credential. The Internet Options section of the Control Panel allows a technician to manage the Internet settings for their computers, including the security settings, access settings, and add-on control settings. Using Internet Options, a technician can set the homepage of the browser, set up the proxy server connection details, and change the trust and security settings used by the system. The Device Manager is used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it. Keychain is a macOS app for managing passwords cached by the OS and supported browser/web applications.

QUESTION 35
A web server has a planned firmware upgrade for Saturday evening. During the upgrade, the power to the building is lost, and the firmware upgrade fails. Which of the following plans should be implemented to revert to the most recent working version of the firmware on the webserver?

A. Backup plan
B. Alternative plan
C. Rollback plan
D. Contingency plan

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.2: A backout plan or rollback plan is an IT governance integration approach that specifies the processes required to restore a system to its original or earlier state in the event of failed or aborted implementation. Every change should be accompanied by a rollback plan so that the change can be reversed if it has harmful or unforeseen consequences. A backup plan is a documented business process that identifies how data will be available for recovery by quickly copying critical data from a backup system to the production environment. A contingency plan is a p lan devised for an outcome other than the usual (expected) plan. It is often used for risk management for an exceptional risk that, though unlikely, would have catastrophic consequences. For example, Dion Trai.ning is located in a hun·icane-prone area, so we have a contingency plan for how we wi ll continue operations during a hurricane by shifting our operations to another data center. An a lternative plan is

another word for a contingency plan.

QUESTION 36
Which of the following types of backups generates the recovered files from a complete copy of a file created at some point in time and one or more partial backups created at later times to merge them into the recovered data?

A. Differential
B. Synthetic
C. Full
D. Incremental

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.3: Synthetic backup is the process of generating a file from a complete copy of a file created at some past time and one or more incremental copies created at later times. The expression synthetic in this context refers to the fact that the assembled file is not a direct copy of any single current or previously created file. Instead, a synthet ic file is merged or synthesized by a specialized application program from the original fi le and one or more modifications to it. A full backup creates a copy of all the selected data regardless of when it was previously backed up. It takes the most time to complete a backup but is the fastest when conducting a restoral of all the data on a hard drive. A differential backup only creates a copy of the selected data that has been modified since the last full backup. It is a good compromise in speed between a full backup (which takes the longest to backup and the least to restore) and an incremental backup (which takes the least to backup and the longest to restore). An incremental backup only creates a copy of new files and files modified since the last full, incremental, or differential backup. Therefore, it takes the least amount of time to complete a backup. Unfortunately, it also takes the most time to restore since you have to first restore the full backup, then any differential and incremental backups until all your data is restored.

QUESTION 37
Which of the following types of attacks occurs when an attacker specifically targets the CEO, CFO, CIO, and other board members during their attack?

A. Vishing
B. Whaling
C. Phishing
D. Spear phishing

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: Whaling is an email-based or web-based form of phishing that targets senior executives or wealthy individua ls. Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to induce targeted indiv iduals to reveal confidential information. A spear phishing attack is focused on a targeted set of people, not just an indiscriminate large group of random people. Phishing is an ema il-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Vishing is a social-engineering attack where the attacker extracts information while speaking over the phone or leveraging IP-based voice messaging services (VoiP).

QUESTION 38
Jason has an old 2017 Dell Laptop that he uses to connect to his office network while traveling. The computer is slow and is running Windows 7. The laptop's screen was recently cracked and needs replacement. Jason brings the laptop to the computer store you work at and asks for your assistance.
Which of the following do you recommend?

A. Replace the display and contact the manufacturer for reimbursement
B. Purchase a new laptop as the cost to repair might be more than a new laptop
C. Sell him an external15" tablet/monitor to connect to the laptop as a workaround
D. Replace the display and charge him for the parts/installation

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4. 7: In this scenario, you should recommend that he purchase a new laptop. Since the laptop is 5-7 years old, it is unlikely to be worth the cost of repair since he could buy a new laptop for $200 to $500. This new laptop would be faster, more secure, and last longer than repairing this old laptop. As a technician, yoll! should weigh the benefits and drawbacks of a particular repair and provide a good recommendation to yotllr customer.

QUESTION 39
Peter is attempting to print to his office printer, but nothing comes out. Yesterday, his printer was working just fine. Peter does not notice any errors on the ta·skbar's printer icon. Which of the following actions should Peter try FffiST to solve this issue?

A. Check that the printer is not offline
B. Cancel all documents and print them again
C. Check the status of the print server queue
D. Check to ensure the printer selected is the default printer

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.1: When this issue occurs, it is often because the system properly sent the print job to the print queue, but the print que ue has become stuck. If no error is shown in the taskbar's printer icon, the user should open the print queue to determine if the print job has become stuck. If it is, then the print queue can be emptied or reset.

QUESTION 40
Which of the following MacOS features is used to manage passwords cached by the OS and is the equivalent of the Credential Manager in Windows?

A. Spotlight
B. Keychain
C. Apple ID
D. Mission Control

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.10: Keychain is a macOS app for managing passwords cached by the OS and supported browser/web applications. This feature is also available as iCloud Keychain that uses the same passwords securely available across all macOS and iOS devices. The Keychain makes password management much easier, but occasionally problems can happen. If there are any problems, they will be identified by the Keychain Access app in the Utilities folder. Mission Control is an application for facilitating multiple desktops in the macOS environment. Spotlight is the file system search feature in the macOS environment. An Apple ID is a user account on an Apple device based on the sign-in email address that is used to sign in to the App Store, access iCioud, and other Apple features and functions.

QUESTION 41
During the reconnaissance phase of a penetration test, you have determined that your client's employees all use Android smartphones that connect back to the corporate network over a secure VPN connection. Which of the following methods would MOST likely be the best method for exploiting these?

A. Use social engineering to trick a user into opening a malicious APK
B. Use a tool like ICSSPLOIT to target specific vulnerabilities
C. Use web-based exploits against the devices web interfaces
D. Identify ajailbroken device for easy exploitation

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.5: When targeting mobile devices, you must first determine if the company uses iPhones or Android-based devices. If they are using Android-based devices, you can use social engineering to trick a user into installing a malicious APK. As a penetration tester, you can create a malicious APK using msfvenom in the Metasploit framework. The user can install it directly from your website instead of the Google Play store.

QUESTION 42
You are troubleshooting a user's laptop that is unable to print a document. You have verified the printer is working and properly connected to the workstation by USB. Which log in Windows 10 would you review to determine if the print spooler service is causing this issue?

A. System log
B. Security log
C. Setu
D. Application log

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems. The system log contains information about service load failures, hardware conflicts, driver load failures, and more. The file (system.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The security log contains information regarding audit data and security on a system. For example,
the security log contains a list of evety successful and failed login attempt. The file (security.evtx) is stored in the %System Root%\System32\Winevt\Logs\ fo lder and can be opened using the Event Viewer. The application log contains infonnation regarding application etTors. The fi le (application.evtx) is stored in the % System Root%\System32\ Winevt\Logs\ folder and can be opened using the Event Viewer. The setup log contains a record of the events generated during the Windows installation or upgrade process. The file (setup.evtx) is stored in the %System Root%\System32\Winevt\Logs\ fo lder and can be opened using the Event Viewer.

QUESTION 43
Several users have contacted the help desk to report that they received an emaiJ from a well-known bank stating that their accounts have been compromised and they need to "click here" to reset their banking password. Some of these users are not even customers of this particular bank, though.
Which of the following best describes this type of attack?

A. Whaling
B. Phishing
C. Spear phishing

D. Brute force

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to tly to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people. The email in this scenario appears to be untargeted since it was sent to both customers and non-customers of this particular bank so it is best classified as phishing. Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to induce targeted individuals to reveal confidential information. Whaling is an emailbased or web-based form ofphishing that targets senior executives or wealthy individuals. A brute-force attack consists of an attacker submitting many passwords or pass phrases with the hope of eventually guessing correctly.

QUESTION 44
Which of the following should be used to uniquely identify every piece of hardware installed on the corporate network, including servers, desktops, laptops, printers, and monitors?·

A. Location
B. TP address
C. Asset ID
D. MAC address

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4. I: The asset TD should be used to uniquely identify each piece of hardware tracked in an asset management database. An asset management database can be configured to store as much or as little information as is deemed necessary. Typical data would be type, model, serial number, asset ID, location, user (s), value, and service information. Tangib le assets can be identified using an identification number, barcode label, or Radio Frequency ID (RFID) tag attached to the device. An RFID tag is a chip programmed with asset data. When in range of a scanner, the chip powers up and signals the scanner. The scanner alerts management software to update the device's location. As well as asset tracking, this allows the management software to track the device's location, making theft more difficult. An IP address is a logical identifier, but it is frequently changed when using
a network with DHCP and cannot be used to reliably identify a piece of hardware. The location of a device is not a unique way of identify ing an asset s ince many pieces of hardware may be located in the space location. Addi tionally, virtual machines cannot easily be tracked using their physical location. This MAC address is used to identify every devioe on the local area network uniquely if an Asset ID is not available, but would not be useful when trying to identify monitors since they do not use a MAC address.

QUESTION 45
A user's computer is experiencing repeated BSODs and calls the service desk. The call is routed to Tier 2 support, and the Tier 2 technician is scheduled for a break in about 2 minutes when the call comes in. Which of the following actions should the technician do?

A. Troubleshoot the issue for the user regardless of how long it takes
B. Answer the phone, put the user on hold, and help them after their scheduled break
C. Ask another Tier 2 technician to answer the call since it will take too long to solve
D. Answer the phone and politely ask the user to call back later

Correct Answer: C
Explanation

Explanation/Reference:

OBJ-4.7: Since the Tier 2 technician already knows that this will take some time to resolve, it would be best to ask another technician to help the user since they are scheduled for their break. It would be improper to either ask the user to call back later or put them on a long hold. While the technician may opt to troubleshoot the user's issue right now, depending on the organization's break structure, that may not be possible. Often in large organizations, break times are scheduled, and if the technician postpones their break, it could have a cascading effect across numerous other technicians' schedules. Therefore, the best choice is to have another technician take the call to avoid causing issues for the customer and the rest of the technicians' break schedules.

QUESTION 46
Your company recently downloaded and installed the latest audio card driver for all of its workstations. Now, several users have had their usernames and passwords for several websites compromised. You believe the two issues are related. If they are, which of the following was MOST likely contained in the audio card driver file that was installed?

A. Keylogger
B. Ransomware
C. Viru
D. Worm

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.2: Based on the events' descript ion, it is like ly that the video card driver contained a keylogger. Key loggers actively attempt to steal confidential information by capturing a credit card number by recording keystrokes entered into a website. This question is based on a real event that occurred in 2017. HP released new audio card drivers for their Conexant audio chips, and it contained a key logger as pati of the driver. Flaws in Conexant's MicTray64.exe application created the keylogger. It's designed to monitor keystrokes and respond to user input, probably to respond to commands to mute or unmute the microphone or begin capturing information within an application. Unfortunately, it also writes out all keystroke data into a publicly accessible fi le located at C:\Users\Public\MicTray.log. If this log file does not exist, the keystrokes are passed to the OutputDebugString API, allowing any process to capture this information without being identified as a malicious program.

QUESTION 47
Which of the following Control Panel sections would a technician use to configure a Windows 10 computer to use Narrator mode to read aloud the List of files that appear on the screen to the user?

A. Ease of Access
B. Soun
C. Indexing Options
D. File Explorer Options

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.4: The Ease of Access section of the Control Panel brings together the functionality for the accessibility features in Windows, including visual, tactile input, and speech recognition settings to assist those with disabilities. For example, the Ease of Access section can be used to tum on the Narrator function which will read any text on tlhe screen aloud to a user who is visually impaired. The File Explorer Options section of the Control Panel allows technicians to customize the display of files and folders. For example, the File Explorer Options can enable or disable the ability to show hidden files, hide file extensions, and more. The Indexing Options is used to configure the method used by Windows when searching for content within the storage devices. When indexing is properly configured, the system will catalog the information on the computer using the words within the files and their metadata to more easily find the content when requested by a user. The

Sound section of the Control Panel allows technicians to configure settings for the playback, recording, and sound effects on the computer.

QUESTION 48
Which of the following backup rotation schemes uses a t hree-tiered approach to ensure at least one monthly full backup is conducted?

A. FIFO Backup
B. Tower of Hanoi
C. 3-2-1 backup
D. Grandfather-father-son

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.3: The grandfather-father-son (GFS) backup rotation scheme is widely used to combine full and incremental backups to reduce backup time and enhance storage security. The grandfather is a fuH backup that is stored off-site once per month. The father is a weekly full backup that is conducted. The son is an incremental or differential backup conducted each day. For example, each Monday a full backup can be conducted which becomes the father. Then, each day of the week a son is created by performing an incremental or differential backup. Once per month, a full backup is conducted to become the grandfather. The 3-2-1 backup rule states that an organization should create (3) one primary backup and two copies of the data, (2) save the backups to two different types of media, and (1) keep at least one backup copy off-site. The Tower of Hanoi is a backup rotation scheme that rotates backup media sets throughout the backup process to minimize wear and failure of tape backup media. For example, when using this method with four backup tapes labeled A, B, C, and D, a total of 16 days of backups can be maintained with just 4 tapes. Tape A is used every odd-numbered day for 16 days. Tape B is used on days 2, 6, 10, and 14. Tape Cis used on days 4 and 12. TapeD is used. on days 8 and 16. This a llows Tape A to be overwritten every other day, while Tapes B is overwritten every four days and Tapes C and Dare overwritten every 8 days. The First In First Out (FIFO) backup scheme uses a set number of tapes and
overwrites the oldest tape with the newest infotmation. For example, if there are 7 tapes in use, every evening a new backup is conducted over the previous week's daily backup. To have a longer amount of days of backups, a technician simply needs to increase the number of tapes from 7 to 14 or 21.

QUESTION 49
What permissions would be represented by the octal 517?

A. rwx--xr-x
B. r-xrwx--x
C. r-x--xrwx
D. --xr-xrwx

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.6: R-X is 5, --X is 1, and RWX is 7. In Linux, you can convert letter permissions to octal by giving 4 for each R, 2 for each W, and 1 for each X. R is for read-only, W is for write, and X is for execU!te. The permissions strings are written to represent the owner's permissions, the group's permissions, and the other user's permissions.

QUESTION 50
Elizabeth was replacing a client's security device that protects their screened subnet. The client has an application that allows external users to access the application remotely. After replacing the devices, the external users cannot connect remotely to the application anymore. Which of the following devices was MOST likely misconfigured and is now causing a problem?

A. DNS
B. Content fi lter
C. Firewall
D. DHCP

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: A firewall is an integral part of creating a screened subnet. If configured correctly, it can regulate exactly what traffic and users are allowed to access the server. This is different from a content fi lter because a content filter denies traffic to a user based on content, but not access to a server. If the firewall ruleset was not configured to allow external users to access the application remotely, the default condition is to "deny by default". Content filtering is the use of a program to screen and/or exclude access to web pages or emails deemed objectionable. The Dynamic Host Configuration Protocol (DHCP) uses port 67 and is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client-server architecture. The Domain Name System (DNS) uses port 53 and is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

QUESTION 51
Which command-line tool is used on a Windows system to move upward in a directory within the system's directory structure?

A. cd.
B. cd ..
C. ls
D. dir

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.2: The cd command is used to change the directory. !fused with the "cd .. "option, it will move up one directory in the file system's directory structure. I fused with the "cd ."option, it will remain in the current directory. The cd command can be used to move directly to another directory or path if entered as "cd (some other directory or path)" into the command line. The dir command is used to list a directory's files and subdirectories. The ls command is used on a Linux system to list a directory's files and subdirectories. The ls command only works on a Windows system when you are using PowerShe ll, not the command line.

QUESTION 52
A home user brought their Windows 10 laptop to the electnmics store where you work because they suspect it has a malware infection. You are in the process of remediating the infected system. Which of the following actions should you be performing?

A. Disable the laptop's wired and wireless network cards
B. Remove, quarantine, or erase the infected files
C. Enable System Restore and perform a backup
D. Review the type, symptoms, purpose, and removal of the mal ware

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.3: Based on the question, you are now in step four of the malware removal process: Remediate the

infected system. If a file is infected with a virus, you can (hopefully) use antivirus software to try to remove the infection (cleaning), quarantine the file (the antivirus software blocks any attempt to open it), or erase the file. You might also choose to ignore a reported threat if it is a false positive. You could also configure the action that software should attempt when it discovers mal ware as part of a scan. Reviewing the information conceming the mal ware is step one of the process. Disabling the laptop's network cards is step two of the process. Enabling system restore is step six of the process.

QUESTION 53
Another technician teUs you that they are PXE booting a computer. What is the technician MOST likely doing with the computer?

A. Installing an image to the computer over the network
B. Using a multi boot configuration
C. An in-place upgrade of the OS
D. Conducting a system repai

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .9: The Preboot eXecution Environment (PXE) specification describes a standardized client-server environment that boots a software assembly, retrieved from a network, on PXE-enabled clients. It allows a workstation to boot from a server on a network before booting the local hard drive's operating system. It is usually used to install an image on the computer over the network. An in-place upgrade is a means of installing an operating system on top of an existing version of the operating system. Applications, user settings, and data files are retained when conducting an in-place upgrade. A repair is used to check and replace any modified system files within the operating system. A multi-boot configuration allows multiple operating systems to be set up on the same computer and the us.er can choose which to boot up when starting up the computer.

QUESTION 54
Which edition of Windows 10 does not have the group policy editor enabled?

A. Home
B. Pro
C. Enterprise
D. Pro for Workstations

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.1: The Group Policy Editor gpedit.msc is only available in Professional and Enterprise editions of the Windows 11 operating systems. A Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, Group Policy is applied to users or computers based on their membership in sites, domains, or organizational units.

QUESTION 55
Dion Training just released a new corporate policy that dictates all access to network resour·ces will be controlled based on the user's job functions and tasks within the organization. For example, only people working in Human Resources can access employee records, and only the people working in finance can access customer payment histories. Which of the following security concepts is BEST described by this new policy?

A. Least privilege
B. Zero trust

C. C. Acceptable use policy
D. D. Defense in depth

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.1: Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. Privilege itself refers to the authorization to bypass certain security restraints. Zero-trust is a security framework that requires all users, whether in or outside the organization's network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data. Defense in Depth is an approach to cybersecurity in which a series of defensive mechanisms are layered to protect valuable data and information. An acceptable use policy (AUP) is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict how the network, website, or system may be used and sets guidelines as to how it should be used.

QUESTION 56
An administrator arrives at work and is told that network users are unable to access the shared drive on a Windows server. The administrator logs into the server and sees that some Windows Updates were automatically installed last night successfully, but now the network connection shows '"limited" with no availability. What rollback action should the technician perform?

A. AntiviTus updates
B. Server's IP address
C. Server's NIC drivers
D. Web browser

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3 .I : When automat ically receiving updates through the Windows Update service, your server can receive driver updates for its network interface card (NIC), graphics cards, and other peripherals. This can accidentally install an incompatible driver that causes network connectivity issues to occur. A best practice is to always set driver updates to "manual" so that you can download and test them in a lab before upgrading your production servers. If your drivers were updated and this is causing the connectivity issue, you can perform a driver rollback to the last known working version of the drivers. An IP address is bound to a network interface card us ing DHCP and there is no such thing as a "rollback" for a server's IP address. The error of "limited" connectivity is associated with the network interface card and the network connection, not the antivirus or the web browser.

QUESTION 57
You have just updated the graphics card's driver to the latest version. After installation, the Windows workstation crashes and reports an error code. You attempt to reboot the workstation, but it fails again. You decide to reboot the workstation into Safe Mode. \Vhat should you do NEXT?

A. Perform an antivirus scan
B. Perform a Windows Update
C. Disable the graphics driver
D. Rollback the graphics driver

Correct Answer: D
Explanation

Explanation/Reference:

OBJ-3.1 : Since the issue began once you installed the latest graphics driver, you should roll back the driver to the last stable version. This should resolve the issue and then allow you to reboot the system back to the normal Windows desktop. Every change should be accompanied by a rollback (or backout) plan so that the change can be reversed if it has harmful or unforeseen consequences. If you are experiencing problems with a device and you have recently updated the driver, Windows also provides a Roll Back Driver feature. A new driver may not work properly because it has not been fully tested or it may not work on your particular system. Driver rollback can recover a system speedily and easily where this has occutTed. You can use Device Manager to revert to the previous driver. Right-click the device and select Properties. Click the Driver tab then click the Roll Back Driver button.

QUESTION 58
You are working as a file server administrator. You are backing up the files on the server when you observe numerous inappropriate photos and videos stored on the corporate share drive by the user jsmith. These files are clearly in violation of the company's AUP. What should you do FIRST?

A. Copy the fi les to an external hard drive
B. Contact the user and ask them to remove the files
C. Delete the files immediately
D. Notify your immediate supervisor

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.7: Since this is a violation of the company's AUP, you should notify your supervisor immediately. Your supervisor wil l then direct you with the correct actions to take according to your company's policies. Then can they provide you with the correct actions to take next based on the organization's policies and guidelines. An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network or the Internet. While some items in the AUP might help prevent a malware infection (such as not allowing users to download and run programs from the internet), it is considered an administrative control, and choosing a technical control like patch management would better protect the network.

QUESTION 59
You have submitted an RFC to install a security patch on all of your company's Windows 2019 servers during the weekly maintenance window. Which of the foiJowing change request documents would describe why the change will be instaiJed during this maintenance window?

A. Plan
B. B. Purpose
C. C. Scope
D. D. Risk analysis

Correct Answer: B
Explanation

Explanation/Reference:
OBJ -4.2: The purpose of the change defines why the change or installation will occur. The change request documentation should define the 5 W's (who, what, when, where, why, and how) to define the why behind the change. For example, the purpose might be "to remediate several category one vulnerabilities so that our security is improved." The change's scope defines the area, number, size, or scale of a particular change. The change request documentation should define the exact scope of the change. In th~s example, only some oftlhe Windows 2019 servers will receive the patch. If 50% of them are listed by their asset tracking number will receive the patch, this would clearly define thi s change's scope. The plan of the change defines how the change or installation will occur. The change request documentation should define the 5 W's (who, what, when, where, why, and how), with the plan documentation covering how the change is implemented. For example, the plan might say that the installation will be performed manually or through an automated patching

process. It may also dictate that all servers will receive the update simultaneously or that five servers will receive it first, then another ten, then the remaining twenty. The risk analysis portion of the change request documentation provides the risk levels of carrying out the change, or not performing the requested change at this time. Risk is the likelihood and impact (or consequence) of a given action. It is important to understand the risk involved with a change before deciding to proceed with implementing the change.

QUESTION 60
A customer's Android smartphone is only 6 months old but is becoming excessively slow. When questioned, the customer states it was acting fine until they recently installed a new stock market tracking app. What action should you take to troubleshoot the slow performance on this phone?

A. Perform a hard reboot of the smartphone
B. Uninstall the app, reboot the phone, and reinstall the app
C. Replace the phone with a newer model
D. Factory reset the smartphone and reinstall all the apps

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: The best option in this scenario is to uninstall and reinstall the stock market app. When apps are updated automatically, they can sometimes become faulty or corrupted and slow down performance on the device. With Android phones, much like iPhones, apps can run in the background and may begin to take up excess resources. If the app is removed, the phone is rebooted, and the app is reinstalled, and the issue persists, then the app should be removed, and an alternate app selected to replace it. Remember, in the CompTIA troubleshooting method we should always question the obvious. In the question, the thing that recently changed was the installing of a new app, so it is likely the issue.

QUESTION 61
Which of the following Windows 10 power options will turn off individual devices connected to a laptop to save energy?

A. Hibernate
B. Sleep
C. Fast startup
D. USB selective suspend

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.4: The USB selective suspend feature allows the hub driver to suspend an individual port without affecting the operation of the other ports on the hub. Selective suspension of USB devices is helpful when using a laptop computer as it helps to conserve battery power by powering off USB ports that are not needed at the time. Hibernate mode is used to save the current session to disk before powering off the computer to save battery life when the system is not being used. The computer takes ~onger to start up again from hibernate mode than it does from the sleep or standby mode. Sleep or standby mode is used to save the current session to memory and put the computer into a minimal power state to save battery life when the system is not being used. The computer takes less time to start up again from the sleep or standby mode than it does from the hibernate mode. Fast startup is a mode in between a full shutdown and a hibernation mode. With a fast startup, the computer will log out of the computer close all of its op,en files when being shut down. Before the system powers off, though, a small hibernation file is created to help speed up the bootup process when the computer is powered on again.

QUESTION 62
Which of the following tools in Windows 10 allows a technician to add different utilities, such as disk management, computer management, performance monitor, print management, and others to create a

modular and customized tool kit for the technician to utilize?

A. RDS
B. UAC
C. PerfMon
D. MMC

Correct Answer: D
Explanation

Explanation/Reference:
OBJ- 1.3: The Microsoft management console (MMC) is a utility that uses snap-ins for various Windows tools such as disk management, computer management, performance monitor, print management, and others to perform operations on a local or networked computer. Remote desktop services (RDS) is used to connect to a remote desktop session host servers or other remote computers, edit an existing remote desktop connection (.rdp) configuration file, and migrate legacy connection files that were created with the client connection manager to the newer .rdp connection file type. User account control (UAC) is used to prevent malware from damaging a PC by blocking the automatic installation of unauthorized apps and preventing inadvertent changes to system settings. PerfMon is a performance monitoring and system monitoring utility in Windows that is used to monitor the activities on CPU and memory activity on a computer. Performance monitor is used for viewing perfonnance data either in real-time or from a log file. The performance monitor can only monitor the resource utilization, but it cannot manage or terminate those processes.

QUESTION 63
What is the minimum amount of storage space required to install Windows 10 (x64) on a device?

A. 20GB
B. 64GB
C. 16GB
D. 32 GB

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.7: For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 11 (64-bit) operating system, the minimum requirements are a dual-core l GHz processor, 4 GB of RAM, and at least 64 GB of hard drive space.

QUESTION 64
Your company wants to ensure that users cannot access USB mass storage devices. You have conducted some research online and found that if you modify the HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet \Services\UsbStor key, it will prevent USB storage devices from being used. Which of the following tools should you use to modify this key?

A. MMC
B. MSConfig
C. RegEdit
D. RDS

Correct Answer: C
Explanation

Explanation/Reference:

OBJ-1.3: The registry editor (RegEdit) allows you to view and make changes to system files and programs that you wouldn't be able to access otherwise. The registry is a database made up of hives and keys that control various settings on a Windows system. ly editing the Registry can permanently damage your computer, so it is important to be very careful when modifying the registry using RegEdit. MSConfig is a system utility to troubleshoot the Microsoft Windows startup processes MSConfig is used to disable or reenable software, device drivers, and Windows services that run at startup, or to change boot parameters. Remote desktop services (RDS) is used to connect to a remote desktop session host servers or other remote computers, edit an existing remote desktop connection (.rdp) configuration file, and migrate legacy connection fi les that were created with the client connection manager to the newer .rdp connection file type. The Microsoft management console (MMC) is a utility that uses snap-ins for various Windows tools such as disk management, computer management, performance monitor, print management, and others to perform operations on a local or networked computer.

QUESTION 65
Which of the tools should a technician NOT use with a solid-state device on a workstation?

A. Device manager
B. Disk defragmenter
C. Perfonnance monitor
D. Disk c leanup

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.3: The disk defragmenter utility is used to rearrange fragmented data so that disks and drives can operate more efficiently. Disk defragmenter runs on a schedule, but can also analyze and defragment disks and drives manually. Disk defragmentation should not be run on a solid-state device. Solid-state devices have a limited number of rewrites available before the drive will fail and using a defragmentation tool will use those rewrites without any benefit in performance. Solid-state devices have a O.lms seek time, so there is no need to defragment a solid-state device. The disk cleanup utility is used to free up disk space on the hard drive or solid-state drive by searching and analyzing the storage device for fi les that are no longer needed and removing them. PerfMon is a performance monitoring and system monitoring utility in Windows that is used to monitor the activities on CPU and memory activity on a computer. Performance monitor is used for viewing performance data either in real-time or from a log file. The perfmmance monitor can only monitor the resource utilization, but it cannot manage or terminate those processes. Device manager (devmgmt.msc) is a utility used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it.

QUESTION 66
You are a member of a project team contracted to install twenty new wireless access points (W APs) for a college campus. Your team has already determined the locations for the new W APs and notated them in the physical and logical network diagrams. Your team is still finalizing the change request documents for the installation. The project cannot move forward with the installation until the change request is finalized and approved. Which of the following is the MOST important thing to add to the scope of work and change request before its approval?

A. Plan for change
B. End-user acceptance
C. Risk analysis
D. E. Rollback plan

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.2: This is a difficult question because all of these items should be included in a Request for Change

(RFC), but the most important is a proper backout plan. A rollback plan is an IT governance integration approach that specifies the processes required to restore a system to its original or earlier state in tlhe event of failed or aborted implementation. Every change should be accompanied by a rollback plan so that the change can be reversed if it has harmful or unfores·een conseque nces. Changes should also be scheduled sensitively if they are likely to cause system downtime or other negative impacts on the workflow of the business units that depend on the IT system being modified. Most organizations have a scheduled maintenance window period for authorized downtime. By following this guidance, the team can back out and restore service on the legacy/previous system if something goes wrong with the installation. End-user acceptance is the process of verifying a change was successfully implemented and turned over to the enduser for future operation. A plan for change is the documented method for installing or modifying the asset as documented in the change request. While this is important, the most important thing is still a backout p lan since many changes are routine changes that do not require a detailed plan of change. A risk analysis determines the severity level of a cha11ge and is used to help the change approval board (CAB) make an informed approval decision.

QUESTION 67
Which version of Windows 10 does NOT support joining a domain or using Group Policy management?

A. A.Home
B. Pro
C. Enterprise
D. Education

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.1: Windows 10 supports domains and Group Policy management in every version except the Home edition. If you are using the Pro, Education, and Enterprise edition, you can join a domain and use Group Policy management. Group Policy (GP) is a Windows management feature that allows you to control multiple users' and computers' configurations within an Active Directory environment. This feature helps network admins in large Windows environments to save time by not having to go through every computer to set a new configuration.

QUESTION 68
Jonathan's father is visually impaired and is having difficulty seeing some of the items on his Windows 10 laptop. Which of the following Control Panel sections would a technician use to configure the Magnifier feature so that his father can zoom in on the different parts of the screen and see them easier?

A. File Explorer Options
B. Indexing Options
C. Ease of Access
D. Sound

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.4: The Ease of Access section of the Control Panel brings together the functionality for the accessibility features in Windows1 including visual, tactile input, and speech recognition settings to assist those with disabilities. For example, the Ease of Access section can be used to tum on the Magnifier that can zoom in anywhere on the screen to make everything in the area larger and easier for a visually impaired user to see. The File Explorer Options section of the Control Panel allows technicians to customize the display of files and folders. For example, the File Explorer Options can enable or disable the ability to show hidden files, hide file extensions, and more. The Indexing Options is used to configure the method used by Windows when searching for content within the storage devices. When indexing is properly configured, the system will catalog the information on the computer using the words within the files and their metadata to more easily fmd the

content when requested by a user. The Sound section of the Control Panel allows technicians to configure settings for the playback, recording, and sound effects on the computer.

QUESTION 69
You have submitted an RFC to install a security patch on some of your company's Windows 2019 servers during the weekly maintenance window. Which of the following change request documents would describe which servers will receive the patch during this maintenance window?

A. Risk analysis
B. Purpose
C. Scope
D. Plan

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.2: The change's scope defines the area, number, size, or scale of a particular change. The change request documentation should define the exact scope of the change. In this example, only some of the Windows 2019 servers will receive the patch. If 50% of them are listed by their asset tracking number will receive the patch, this would clearly define this change's scope. The plan of the change defines how the change or instaUation will occur. The change request documentation should define the 5 W's (who, what, when, where, why, and how), with the plan documentation covering how the change is implemented. For example, the plan might say that the installation will be performed manually or through an automated patching process. It may also dictate that all servers will receive the update simultaneously or that five servers will receive it first, then another ten, then the remaining twenty. The ri sk analysis portion of the change request documentation provides the risk levels of carrying out the change, or not performing the requested change at this time. Risk is the likelihood and impact (or consequence) of a given action. It is important to understand the risk involved with a change before deciding to proceed with implementing the change. The purpose of the change defines why the change or installation will occur. The change request documentation should define the 5 W's (who, what, when, where, why, and how) to define the why behind the change. For example, the purpose might be "to remediate several category one vulnerabilities so that our security is improved."

QUESTION 70
Windows file servers commonly hold sensitive files, databas.es, passwords, and more. What common vulnerability is usually used against a Windows file server to expose sensitive flies, databases, and passwords?

A. Cross-·site scripting
B. SQL injection
C. CRLF injection
D. Missing patches

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.4: Missing patches are the most common vulnerability found on both Windows and Linux systems. When a security patch is released, attackers begin to reverse engineer the security patch to exploit the vulnerability. If your servers are not patched against the vulnerability, they can become victims of the exploit, and the server's data can become compromised. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. Cross-site scripting focuses on exploiting a user's workstation, not a server. CRLF injection is a software application coding vulnerability that occurs when an attacker injects a CRLF character sequence where it is not expected. SQL injection is the placement of malicious code in SQL statements via web page input. SQL is commonly used against databases, but they are not useful when attacking file servers.

QUESTION 71
Which of the following file system formatting types should be used with older recordable optical discs?

A. FAT32
B. NTFS
C. CDFS
D. UDF

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.8: The CD File System (CDFS or ISO 9660) is a legacy file system used for CD optical disc media (CD-ROM and CD-R). CDFS supports two main data writing modes: mode 1 has better en-or cmTection, whereas mode 2 allows more data to be written to the disc. Joliet is an extension to CDFS that enables long filename support and Unicode characters in file names. The universal disk format (UDF or ISO 13346) is an updated file system for optical media supporting multisession writing. It is the standard used by Windows, referred to as the Live File System, for CD and DVD recordable and rewritable discs. There are several different versions ofUDF, with 2.01 being the default in Windows. Blu-ray reading and writing requires version 2.5 and third-party software. The NT file system (NTFS) is a Windows file system that supports a 64-bit address space and can provide extra features such as file-by-file compression and RAID support as well as advanced file attribute management tools, encryption, and disk quotas. NTFS can support a maximum volume size ofup to 8 PB. The file allocation table 32-bit (FAT32) is the 32-bit file system supported by Windows, macOS, and Linux computers. FA T32 can support maximum volume sizes of up to 2 TB and maximum file sizes ofup to 4GB.

QUESTION 72
You are trying to copy a 4.7 GB file from your Windows laptop to an external hard drive using USB 3. The external hard drive lis formatted with FAT32. Every time you attempt this copy, you receive an error. What is MOST likely the issue?

A. The external hard drive must be formatted as APFS to support this transfer
B. Files over 4GB cannot be stored on a FAT32 formatted drive
C. The laptop must be reformatted as FA T32 to support this transfer
D. USB 3 is too slow to transfer a fiJe this large

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.8: Since this file is 4. 7GB in size, it cannot be stored as a single file on the FAT32 hard drive. The file allocation table 32-bit (F AT32) is the 32-bit file system supported by Windows, macOS, and Linux computers. FAT32 can support maximum volume sizes ofup to 2 TB and maximum fi le sizes ofup to 4 GB. The Apple file system (APFS) is the default file system for Mac computers using macOS 10.13 or later and features strong encryption, space sharing, snapshots, fast directory sizing, and improved file system fundamenta ls.

QUESTION 73
Jason is working in Microsoft Word, but the application appears to have become frozen and unresponsive. Which of the foUowing features in the Task Manager shouJd he use to terminate the unresponsive program?

A. Services
B. Processes
C. Performance
D. Startup

Correct Answer:
Explanation

Explanation/Reference:
OBJ-1.3: The task manager is an advanced Windows tool that has 7 tabs that are used to monitor the Processes, Performance, App History, Startup, Users, Details, and Services on a computer. The Processes tab in the task manager is helpful to quickly see how system resources are utilized, help troubleshoot applications, or find out why the computer is perfonning slowly . The task manager can identify and stop processes that use excessive
system resources and keep the computer operating at higher speeds. By clicking the Startup tab, the technician can see every program configured to start up when Windows is booted up. This can be used to disable unwanted programs from launching during the boot-up process. By clicking the Processes tab, the technician can manage and terminate running apps and services. By clicking the Servkes tab, the technician can list all of the services installed on the computer, display their status, and start/stop/restart those services.

QUESTION 74
Sagar is planning to patch a production system to correct a detected vulnerability during his most recent network vulnerability scan. What process should he follow to minimize the risk of a system failure while patching this vulnerability?

A. Wait 60 days to deploy the patch to ensure there are no associated bugs reported with it
B. Deploy the patch in a sandbox environment to test it before patching the production system
C. Contact the vendor to determine a safe time frame for deploying the patch into the production environment
D. Deploy the patch immediately on the production system to remediate the vulnerability

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.2: While patching a system is necessary to remediate a vulnerability, you should always test the patch before implementation. It is cons idered a best practice to create a staging or sandbox environment to test the patches' installation before installing them into the production environment. This reduces the risks of the patch breaking something in the production system. Unless you are dealing with a very critical vulnerabi lity and the risk of not patching is worse than the risk of patching the production system directly, yoU! should not immediately patch the production systems without testing the patch first. You should not wait 60 days to deploy the patch. Waiting this long provides attackers an opportunity to reverse engineer the patch and create a working exploit against the vulnerability. Finally, asking the vendor for a safe time frame is not helpful since the vendor does not know the specifics of your environment or your business operations.

QUESTION 75
You recently read a news article about a new crypto-malware worm that is causing issues for corporate networks. Today, you noticed that four of your company's workstations had their files encrypted. You are worried about the rest of the network's workstations. What should you do FIRST?

A. Format the affected workstation's hard drives and reinstall Windows
B. Update the antimalware scanner's signatures on all workstations
C. Perform a full disk antimalware scan on the affected workstations
D. Immediately quarantine the affected workstations

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.3: Based on the scenario, these four workstations have likely been infected with the crypto-malware worm. You should immediately isolate and quarantine the workstations to prevent the infection from spreading across the network. Then, you could begin the remediation process on those workstations. The seven steps of the mal ware removal procedures are (1) Investigate and verify mal ware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, preinstallation

environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 76
Which of the following must be enabled to allow a video game console or VoiP handset to configure your firewall automatically by opening the IP addresses and ports needed for the device to function?

A. DHCP
B. MDM
C. UPnP
D. NAT

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: Universal plug-ancll-play (UPnP) is a protocol framework allowing network devices to autoconfigure services, such as allowing a games console to request appropriate settings from a firewall. UPnP is associated with several security vulnerabilities and is best disabled if not required. You should ensure that the router does not accept UPnP configuration requests from the external (internet) interface. If using UPnP, keep up-to-date with any security advisories or firmware updates from tfue router manufacturer. A mobile device management (MDM) software suite is used to manage smartphones and tablets within an enterprise. The dynamic host control protocol (DHCP) is a protocol used to allocate IJP addresses to a host when it joins a network. DHCP utilizes UDP
ports 67 and 68. Network address translation (NAT) is a network service provided by the router or proxy server to map private local addresses to one or more publicly accessible IP addresses. NAT can use static mappings but is commonly implemented as network port address translation (PAT) or NAT overloading, where a few public IP addresses are mapped to multiple LAN hosts using p011 allocations.

QUESTION 77
Which of the following authentication protocols was developed by Cisco to provide authentication, authorization, and accounting services?

A. CHAP
B. Kerberos
C. TACACS+
D. RADIUS

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.2: TACACS+ is an extension to TACACS (Tetminal Access Controller Access Control System) and was developed as a proprietary protocol by Cisco. The Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that operates on pOI11812 and provides centralized Authentication, Authorization, and Accounting management for users who connect and use a network service, but Cisco did not develop it. Kerberos is a network authentication protocol designed to provide strong mutual authentication for client/server applications using secret-key cryptography developed by MIT. ChallengeHandshake Authentication Protocol (CHAP) is used to authenticate a user or network host to an authenticating entity. CHAP is an authentication protocol but does not provide authorization or accounting services.

QUESTION 78
Which of the following would leave a user's programs running on their Windows l 0 laptop while preventing other users from accessing them without entering the correct password?

A. Hibernate

B. Shutdown
C. Lock
D. Sleep

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.4: If you need to leave your computer for a moment, you can use the lock option. This will allow any currently running programs and files to remain open while simultaneously preventing other users from accessing or using the computer while you are away. There are no power savings when you are in this mode, though. Hibernate mode is used to save the current session to disk before powering off the computer to save battery life when the system is not being used. The computer takes longer to start up again from hibernate mode than it does from the s leep or standby mode. Sleep or standby mode is used to save the current session to memory and put the computer into a minimal power state to save battery life when the system is not being used. The computer takes less time to start l!.lp again from the sleep or standby mode than it does from the hibernate mode. Shutdown mode completely powers off the computer and does not save the current user session to disk. Instead, the shutdown will close all open files and log out the user during the shutdown process.

QUESTION 79
You are configuring a SOHO network and only allowing specific IP addresses to access the network while blocking any IP addresses that are not on the list. Which of the following should be implemented?

A. MAC filtering
B. Blocklist
C. Port forwarding
D. Allow list

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.9: An allow list is a form of protection where only the items identified specifically on the list are allowed, whereas all others are denied. For example, if you create an access control list that relies on an allow list, it would block every IP address that is not found in the allow list. A blocklist contains every address or port that is blocked from accessing the network. MAC filtering is the application of an access control list to a switch or access point so that only clients with approved MAC addresses connect. Port forwarding allows a router to take requests from the Internet for a particular application and send them to a designated host on the LAN.

QUESTION 80
A user is having an issue wlith a specific application on their Android devices. The user works for DionTraining, and every employee has the exact same model of smartphone issued by the company. Whenever the user attempts to launch the application, the app fails and generates an error message. Which of the following should the technician attempt FIRST to solve this issue?

A. Update the operating system of the two smartphones
B. Reinstall the malfunctioning application
C. Rollback the application to the previous version
D. Clear the local application cache

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.4: To solve an issue with a mobile application, you should normally attempt the following steps. First,

clear the application cache since this locally stored information can become glitchy and cause an app to crash. If you !have two of the same smartphones having the same issue, it is unlikely to be the application cache causing the issue. In this case, the technician would then attempt to update the OS of the smartphones. Updating the operating system can minimize compatibility issues and fix crashing applications. Third, you can try reinstalling the application if the other two options don't work.

QUESTION 81
The server administrators have asked you to open the default port on the firewaU for a new DNS server. Which of the following ports should you set to ALLOW in the ACL?

A. 67
B. 3389
C. 53
D. 110

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: Port 53 is used for DNS. The Domain Name System (DNS) is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. Port 67 is used for DHCP. The Dynamic Host Configuration Protocol (DHCP) is a network management protocol used on Internet Protocol (IP) networks for automatically assigning IP addresses and other communication parameters to devices connected to the network using a client-server architecture. Port 110 is used for POP3. Post Office Protocol version 3 (POP3) is an application-layer Internet standard protocol used by e-mail clients to retrieve e-mail from a mail server. Port 3389 is used for RDP. Remote Desktop Protocol (RDP) is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.

QUESTION 82
A macOS user is browsing the internet in Google Chrome when they see a notification that says, "Windows Enterprise Defender: Your computer is infected with a virus, please click here to remove it!" What type of threat is this user experiencing?

A. Phanning
B. Worm
C. Rogue anti-virus
D. Phishing

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.2: Rogue anti-virus is a form of malicious software and internet fraud that misleads users into believing there is a virus on their computer and to pay money for a fake malware removal tool (that actually introduces mal ware to the computer). It is a form of scareware that manipulates users through fear and a form of ransom ware. Since the alert is being displayed on a macOS system but appears to be meant for a Windows system, it is obviously a scam or fake alert and most likely a rogue anti-virus attempting to infect the system. Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people. A worm is a standalone mal ware computer program that replicates itself to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. A worm can spread on its own, whereas a virus needs a host program or user interaction to propagate itself. Pharming is a type of social engineering attack that redirects a request for a website, typicaHy an e-commerce site, to a similar-looking, but fake, website. The attacker uses DNS spoofing to redirect the user to the fake site.

QUESTION 83
Which command-line tool is used on a Windows system to erase all the data on a hard disk and ensure it is ready to accept new \Vindows files?

A. diskpart list disk
B. sfc /now
C. chkdsk lf
D. format /fs:NTFS

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.2: The format command creates a new root directory and fi le system for the disk. It can check for bad areas on the disk, and it can delete all data on the disk. To use a new disk, you must first use the format command to format the disk. The chkdsk command is used to check the fi le system and file system metadata of a volume for logical and physical errors. I fused without parameters, chkdsk displays only the status of the volume and does not fix any errors. If used with the If, /r, /x, or /b parameters, it fixes errors on the volume. The diskpart command is a command-line disk-partitioning utility available for Windows that is used to view, create, delete, and modify a computer's disk partitions. The system file checker (SFC) command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from the command line.

QUESTION 84
A user cannot change their iPad display from landscape to portrait when they are on the home screen. Which of the following is MOST likely the reason for this issue?

A. NFC is disabled
B. Autorotate is disabled
C. Developer mode is enabled
D. Smartphone has overheated

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.4: If the iiPad will not change from landscape to pm1rait mode, it is likely that the autorotate feature has been disabled by the user accidentally. To enable autorotation, the user needs to swipe down from the top right comer of the screen to open their Control Center. Then, they need to tap the lock and arrow icon to tum off the rotation lock to enable autorotation.

QUESTION 85
Which version of Windows supports Virtual Desktops?

A. Windows 8
B. Windows 7
C. Windows 10
D. Windows 8.1

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.1: Windows 10 added support for Virtual Desktops like those long seen on Linux and Mac OS X. These allow users without multi-monitor setups to create multiple virtual desktops that are handy for splitting usage between work and leisure work into projects, or whatever you require. Older versions of Windows, such as Windows 7, Windows 8, and Windows 8.1 do not support Virtual Desktops and are currently considered end-

of-life operating systems.

QUESTION 86
A coworker is creating a file containing a script. You look o·ver their shoulder and see "#!/bin/bash" as the first line in the file. Based on this, what type of file extension should this script use?

A. vbs
B. py
C. bat
D. sh

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.8: A shell script is a file that contains a list of commands to be read and executed by the she ll in Linux and macOS. A .sh fi le is used for a shell script and its first line always begins with # !/bin/bash that designates the interpreter. This line instructs the operating system to execute the script. Shell scripts allow you to perform various functions. These functions include automation of commands and tasks of system administration and troubleshooting, creating simple applications, and manipulating text or files. Python is a general-purpose programming language that can develop many different kinds of applications. It is designed to be easy to read, and the programs use fewer lines of code compared to other programming languages. The code runs in an interpreter. Python is preinstalled on many Linux distributions and can be installed on Windows. Python scripts are saved using the .py extension. VBScript is a scripting language based on Microsoft's Visual Basic programming language. Network administrators often use VBScript to perform repetitive administrative tasks. With VBScript, you can run your scripts from either the commandline or the Windows graphical interface. Scripts that you write must be run within a host environment. Windows 10 provides Internet Explorer, IIS, and Windows Script Host (WSH) for this purpose. Batch scripts run on the Windows operating system and, in their simplest form, contain a lis.t of several commands that are executed in a sequence. A .bat file is used for a batch script. You can run the file by calling its name from the command line or double-clicking the fi le in File Explorer. Generally, batch fi le scripts run from end to end and are limited in branching and user input.

QUESTION 87
An employee at Dion Training complains that their smartphone is broken. They state that it cannot connect to the internet, nor can it make or receive phone calls and text messages. You ask them to start up the music player on his phone, and it opens without any issues. It appears the common issue has to do with the device's network connectivity. Which of the following is MOST likely the problem with this smartphone?

A. The cellular radio in it is broken
B. Airplane mode is enabled on the device
C. The VPN password was entered ly
D. The Bluetooth connection is disabled

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: If the smartphone is functioning properly except for applications that require network connectivity, then the issue is either a misconfiguration (like enabling airplane mode by mistake), a defective cellular radio chip, or a similar issue. The most likely cause is that the employee accidentally enabled the airplane mode on the device that turns off the cellular radio for the smartphone and can cause the network connectivity to be lost. A technician should first verify that airplane mode is disabled and that the cellular radio is enabled. If that doesn't solve the problem, then the teclmician should investigate whether it is a hardware issue (such as a broken cellular radio chip). The Bluetooth connection being disabled would affect paired devices like a headset or wireless speaker, not the ability of the device to connect to the internet. According to the scenario presented, there is no mention of a VPN, so the VPN password being ly answered is not conect.

QUESTION 88
You are renting space in another company's data center. To protect your server from being physically accessed when you are not in the building, what device should you use?

A. USB lock
B. Entry control roste
C. Smart card
D. Server lock

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2. 1: A server lock is a physical locking mechanism installed on a server cabinet to prevent unauthorized from accessing the servers. The server lock could be a cipher lock, biometric lock, or a simple keyed lock depending on the level of security needed. USB lock prevents unauthorized data transfer through USB ports, reducing the risk of
data leakage, data theft, computer viruses, and malware by physically locking and blocking the USB Ports. A smart card, chip card, PIV card, or integrated circuit card is a physical, electronic authorization device used to control access to a resource. It is typically a plastic credit card-sized card with an embedded integrated circuit chip. In high-security environments, employee badges may contain a smart card embedded chip that must be inserted into a smart card reader to log in or access information on the system.
An entry control roster is an administrative control used to log each person who enters or leaves a secure room.

QUESTION 89
A customer has requested you install an external video card into their gaming PC. Which of the following tools should you utilize to protect the video card as you carry it from the storage r oom to your workbench?

A. Air filter mask
B. Latex g loves
C. Web browser
D. Antistatic bag

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.4: An antistatic bag is a packaging material containing anti-ESD shielding or dissipative materials to protect components from ESD damage. Whenever you move a sensitive component from one location to another, you should place it inside an antistatic bag. An electrostatic discharge (ESD) is the release of a charge from metal or plastic surfaces that occurs when a potential difference is fonned between the charged object and an oppositely charged conductive object. This electrical discharge can damage silicon c hips and computer components if they are exposed to it. An air filter mask is a mask manufactured from polyester sheets that cover your nose and mouth to prevent the dust from being breathed in by a technician. Latex gloves are hand coverings to protect the technician when they are working with toner or other chemicals. An ESD strap is placed around your wrist and di ssipates any static electricity from your body to protect sensitive hardware such as processors~ memory, expansion cards, and SSDs during installation.

QUESTION 90
A customer brought in a computer that has been infected with a virus. Since the infection, the computer began redirecting all three of the system's web browsers to a series of malicious websites whenever a valid website is requested. You quarantined the system, disabled the system restore, and then perform the remediation to remove the malware. You have scanned the machine with several anti-virus and anti-malware programs and determined it is now cleaned of all malware. You attempt to test the web browsers ag:ain, but a small number of valid websites are still being redirected to a malicious website. Luckily, the updated anti-virus you installed blocked any new malware from infecting the system. Which of the following actions should you perform NEXT

to fix the redirection issue with the browsers?

A. Verify the hosts.ini file has not been maliciously modified
B. Perform a System Restore to an earlier date before the infection
C. Install a secondary anti-malware solution on the system
D. Reformat the system and reinstaU the OS

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.2: Browser redirection usually occurs if the browser's proxy is modified or the hosts.ini file is modified. If the redirection occurs only for a small number of sites or occurs in all web browsers on a system, it is most likely a maliciously modified hosts.ini file. The hosts.ini file is a local file that allows a user to specify specific domain names to map to particular addresses. It works as an elementary DNS server and can redirect a system's internet connection. For example, if your children are overrusing YouTube, you can change Y ouTube.com to resolve to Y ourSchool.edu for just your child's laptop.

QUESTION 91
You are going to replace a power supply in a desktop computer. Which of the following actions should you take FIRST?

A. Use a grounding probe to discharge the power supply
B. Remove any jewelry you are wearing
C. Dispose of the old power supply
D. Verify proper cable management is being used

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.4: Before working on a computer or server, you should always remove your jewelry. Jewelry such as bracelets and necklaces can often dangle and come into contact with sensitive components or electrical connections that can cause damage to the components or injure you. Therefore, all jewelry should be removed before working on an electrical system or computer to reduce the risk of shock. A grounding probe is not required to discharge the power supply since the technician should never be opening up the case of a power supply. The old power supply should be safely disposed of after it is removed, but it should not be removed until you have removed your jewelry. Proper cable management is important when installing a power supply, but again t his should only occur after removing your jewelry.

QUESTION 92
What umask should be set for a directory to have 700 as its octal permissions?

A. r--r--r--
B. rwx---rwx
C. rwx------
D. Rwxrwxrwx

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.6: RWX is 7 and --- is 0. In Unux, you can convert letter permissions to octal by giving 4 for each R, 2 for each W, and 1 for each X. R is for read-only, W is for write, and X is for execute. The permissions strings are written to represent the owner's permissions, the group's permissions, and the other user's permissions.

QUESTION 93
Which of the following physical security controls would be the most effective in preventing an attacker from driving a vehicle through the glass doors at the front of the organization's headquarters?

A. Bollards
B. Intrusion alarm
C. Access control vestibule
D. Security guards

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.1: Bollards are a physical security control that is designed to prevent a vehicle-ramming attack. Bollards are typically designed as sturdy, short, vertical posts. Some organizations have installed more decorative bollards created out of cement and are large enough to plant flowers ortrees inside. Access control vestibules are designed to prevent individuals from tailgating into the building. Security guards and intrusion alarms could detect this ftram occurring: but not truly prevent them ..

QUESTION 94
Which of the following tools should you utilize to ensure you don't damage a laptop's SSD whille replacing it?

A. Air filter mask
B. Antistati'c bag
C. ESD strap
D. Latex gloves

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.4: The key to answering this question is the word "while" in the sentence. Since you need to protect the SSD "while" you are replacing it, you must ensure you wear an ESD strap. An ESD strap is placed around your wrist and dissipates any static electricity from your body to protect sensitive hardware such as processors, memory, expansion cards, and SSDs during installation. An electrostatic discharge (ESD) is the release of a charge from metal or plastic surfaces that occurs when a potential difference is formed between the charged object and an oppositely charged conductive object. This electrical discharge can damage silicon chips and computer components if they are exposed to it. An antistatic bag is a packaging material containing anti-ESD shielding or dissipative materials to protect components from ESD damage. An antistatic bag is a packaging material containing anti-ESD shielding or dissipative materials to protect components from ESD damage. An air filter mask is a mask manufactured from polyester sheets that cover your nose and mouth to prevent the dust from being: breathed in by a technician. Latex gloves are hand coverings to protect the technician when they are working with toner or other chemicals.

QUESTION 95
You are working on upgrading the memory of a laptop. After removing the old memory chips from the laptop, where should you safely store them until you are ready to reuse them in another laptop?

A. Ziplock bags
B. Manila envelopes
C. Cardboard box
D. Antistatic bag

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.4: To properly handle and store sensitive components, like a memory chip, you should use an ESD strap and place the components in an antistatic bag. An antistatic bag is a bag used for storing electronic components, which are prone to damage caused by electrostatic discharge (ESD). These bags are usually plastic polyethylene terephthalate (PET) and have a distinctive color (silvery for metalized film, p~ink or black for polyethylene).

QUESTION 96
Which type of authentication method is commonly used with physical .access control systems and relies upon RFID devices embedded into a token?

A. Smart cards
B. HOTP
C. TOTP
D. Proximity cards

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.1: A proximity card is a contactless card that usually utilizes RFID to communicate with the reader on a physical access system. These are commonly used to access secured rooms (such as server rooms) or even a building itself (such as at an access control vestibule). Some smart cards contain proximity cards within them, but the best answer to this question is proximity cards since that is the function of the smart card would be the device used to meet this scenario's requirements. An HMAC-based one-time password (HOTP) is a one-time password algorithm based on hash-based message authentication codes. A Time-based one-time password (TOTP) is a computer algorithm that generates a onetime password that uses the current time as a source of uniqueness.

QUESTION 97
You are formatting a 4 TB external hard drive on your MacBook. The drive will be used to share files large video files between your MacBook and your friend's Windows 10 desktop. Which file format should you use?

A. HFS
B. FAT32
C. NTFS
D. exFAT

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.8: The only file system format that would work for this situation is exFAT. A macOS system can format a hard drive as APFS, HFS+, HFS, exFAT, or FAT32. The Windows system would only be able to read exFAT or FAT32. Unfortunately, FAT32 only supports drive sizes up to 32GB, and file sizes up to 4GB. Therefore, exFAT should be used as it supports sizes up to 128 petabytes.

QUESTION 98
Jason is out of town on a business trip and needs to access the share drive on his company's corporate network. Which of the following types of network connections should he use to access the share drive from his hotel room?

A. Wireless
B. Dial-up
C. Wired
D. VPN

Correct Answer: D
Explanation

Explanation/Reference:
Explanat ion
OBJ-1.6: The user must connect remotely through a VPN to access the company's shared drive and shared resources. The VPN connection is established over a wired, wireless, cellular, or dial-up connection, but Jason wi ll not access the corporate resources without first authentication t hrough the VPN. A virtual private network creates a secure tunnel between two endpoints connected via an insecure network such as t he Internet. VPNs use encryption software is used to ensure the privacy of data as messages t ransit through the public network. VPNs also use authentication software to validate the user has permission to connect. Once connected to the VPN, the user will be able to access all of the resources on the local area network as if they were st ill located in their office.

QUESTION 99
An employee's inbox is now filled with unwanted emails after their email password had been compromised last week. You helped them reset their password and regain access to their account. Many of the emails are coming from different email addresses such as @yahoo.com, @gmail.com, and @hotmail.com. Which of the following actions should the user take to help reduce the amount of spam they receive?

A. Create a domain-based email filter
B. Click the unsubscribe button of each email
C. Establish an allow list of trusted senders
D. Mark each email as spam or junk

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.2: At the user level, the software can redirect spam t o a junk folder or similar. Email filtering is any technique used to prevent a user f rom being overwhelmed with spam or junk email. Spam can be blocked from reaching an organization using a mail gateway to fi lter messages. Anti-spam filtering needs to balance blocking illegitimate traffic with permitting legitimate messages. Anti-spam techniques can also use lists of known spam servers by establishing a blacklist. If an allow list is used, only a small number of senders could send emails to t he user. The technician should not create a domain-based email filter since the spammers are using Yahoo, Gmail, and Hotmail accounts to send the spam. If a domain-based email filter i's created, it will block emails from all users on t hose email providers and prevent legitimate emails f rom being received.

QUESTION 100
You recently built a new gaming PC for a customer. The system has an ,octa-core 64-bit processor, 32GB of DDR4 RAM, 1 TB SSD, a PCI x16 video card with 8GB of RAM, and Windows 10 Pro (x86) installed. When you turn on the system, you notice that Windows only recognizes 3.5 GB of RAM. Which component should be upgraded to correct this issue?

A. Set the processor to VT-enabled in the BIOS
B. Replace the 32GB of DDR4 RAM with DDRS
C. Replace the 1 TB SSD with a 4 TB 7200 RPM HOD
D. Replace the OS with Windows 10 Pro {x64) edition

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.1: Even if the processor is 64-bits, the operating system will not recognize over 3.5 GB of RAM unless it is designed to operate at 64-bits. Since the Windows 10 edition installed was for an x86 system, known as a 32-bit system, it will not recognize any RAM over 3.5 GB. If you reinstall a 64-bit version of Windows, t hen it

will immediately recognize the full 32 GB of DDR4 RAM in the system.

QUESTION 101
Which of the following would a technician use when trying to find the exact steps required to install a custom software package within their organization?

A. sow
B. SOP
C. MSDS
D. AUP

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.1: A standard operating procedure (SOP) is an inflexible, step-by-step listing of the actions that must be completed for any given task. The Material Safety Data Sheet (MSDS) is a document that contains information on the potential hazards (health, fire, reactivity, and environmental) and how to work safely with t he chemical product. The MSDS is an essential starting point for the development of a complete health and safety program that includes the direct ions for proper handling and disposal ofthe chemicals. An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network or the internet. For example, an AUP may state that t hey must not attempt to break any computer network security, hack other users, or visit pornographic websites from their work computer. A statement of work (SOW), or a scope of work, is a document that outlines all the work that is to be performed, as well as the agreed-upon deliv,erables and t imelines.

QUESTION 102
You have been asked to replace a computer's hard drive. Which of the following steps should you take FIRST to prevent an electrical hazard while working on the computer?

A. Place the computer and its components on an ESD mat
B. Place the computer on a grounded workbench
C. Disconnect the power before servicing the computer
D. Connect an ESD strap to yourself to prevent shock

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.4: The FIRST thing that you need to do is disconnect the power to the computer. This will eliminate many electrical hazards and prevent you from getting an electrical shock while working on the machine. After it is disconnected, it is a good idea to use an ESD strap, place the computer and its components on an ESD mat, and work on the computer on top of a grounded workbench.

QUESTION 103
A user is complaining about slow data speeds when they are at home in a large apartment building. The user uses Wi-Fi when they get home, and the device works fine on other wireless networks they connect to. Which of the following actions should the user take to increase their data speeds?

A. Turn off Wi-Fi and rely on their cellular data plan
B. Increase the Wi-Fi signal being transmitted by their WAP
C. Enable MAC filtering on their WAP
D. Upgrade to a new smartphone

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: Slow data speeds can be caused by too much interference or a weak signal. Try changing the channel on Wi-Fi routers to less-used channels or boost the signal being transmitted, and the performance should increase. Alternat ively, if the cellular signal is too low, you can install a signal booster or microcell in the home or office. Enabling MAC filtering would block devices attempting to connect to the Wi-Fi. Turning off the Wi-Fi and using their cellular data plan might be a valid workaround, but it does not solve the issue of the Wi-Fi not functioning properly at home. Upgrading t he smartphone would not increase the speed of t heir home Wi-Fi, as their current smartphone already operates at faster speeds on other Wi-Fi networks.

QUESTION 104
A computer has been performing slowly. During your troubleshooting, you notice that the Task Manager shows the processor is utilizing 90-100% of the system resources immediately after completing the boot-up process. Which of the following actions should you take?

A. UninstaU and reinstall the applications
B. Disable any unneeded applications configure to automatically startup
C. Remove a recently added hardware device
D. Verify that disabling 01ne service has not affect ed others

Correct Answer: B
Explanation

Explanation/Reference:
Explanat ion
OBJ-3.1: One way to increase the system's performance is to disable any unneeded applications from starting up when the computer boot s. You can use the System Configuration Utility (msconfig) or Task Manager to prevent unnecessary services and programs from running at startup. If you need to run the services, consider setting them to delayed startup or manual startup to avoid slowing down boot t imes too much. The task manager is an advanced Windows tool that has 7 tabs t hat are used to monitor the Processes, Performance, App History, Startup, Users, Details, and Services on a computer. By clicking t he Startup tab, the technician can see every program configured to start up when Windows is booted up. This can be used to disable unwanted programs from launching during t he boot-up process. By clicking the Services tab, t he technician can list all of the services installed on the computer, display their status, and start/stop/restart those services. System configuration (msconfig.exe) is a system utility to troubleshoot the Microsoft Windows startup processes. MSConfig is used to disable or re-enable software, device drivers, and Windows services that run at startup, or to change boot parameters.

QUESTION 105
A home user brought their Windows 10 laptop to the electronics store where you work because they suspect it has a malware infection. Which of the following actions should you perform FIRST?

A. Run Windows Update
B. Disable System Restore
C. Investigate malware symptoms
D. Enable System Restore

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.3: The first step of the malware removal process is to investigate and verify malware symptoms. This is done by questioning the cusitomer about what they observed and direct observation of the system and its operations. The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and

create a restore point in Windows, and (7) Educate the end user.

QUESTION 106
Your boss has asked you to write a script that will copy all of the f iles from one hard drive to another each evening. This script should mirror the directories from one drive to the other and ensure they are synchronized each evening. Which command-line tool should you use in your script?

A. xcopy
B. cp
C. copy
D. robocopy

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.2: The robocopy tool is used to mirror or synchronize directories and their contents. Robocopy will check the destination directory and remove files no longer in the main tree. It also checks the files in the destination directory against the files to be copied and doesn't waste time copying unchanged files. The xcopy tool, on the other hand, copies all of the files from one directory to another. To meet your boss's requirements to synchronize the two hard drive's contents, you must use robocopy since it wi ll also remove files from the second drive that were removed from the first drive, too. The copy command is used to copy one or more files from one location to another. The copy command cannot copy files that are 0 bytes long or for copying all of a directory's files and subdirectories. The cp command is used in Linux to copy one or more files and directories from one location to another.

QUESTION 107
You have decided that you wanted to install a second operating system on your computer. After installing the OS and rebooting the computer, you see the "Operating System Not Found" error on your display. You verify that the boot.ini file is configured properly, but the error still appears. What is MOST likely causing this error?

A. An unsupported version of Linux is installed
B. The MBR bootloader was installed accidentally
C. Windows Startup services are not properly running
D. An incompatible partition is marked as active

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.1: This issue may occur if one or more of the following conditions are true: (1) the basic input/output system (BIOS) does not detect the hard disk, (2) the hard disk is damaged, (3) sector 0 of the physical hard disk drive has an or malformed master boot record (MBR), (4) an incompatible partition is marked as Active, or (5) a partition that contains the MBR is no longer active. The only option provided in this list is that an incompatible partition is marked as active.

QUESTION 108
Madison is trying to open up her anti-malware solution to run a full system scan because she suspects her computer has become infected. When she attempts to run the tool, an error of "Access denied" is received. What security issue is MOS'J likely occurring?

A. Disappearing files
B. Renamed system files
C. File permission change
D. Rogue anti-virus

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.2: If the user receives an "access denied" error message, it indicates that the file permissions have been changed. If the system files were renamed or the files disappeared, an error of "file not found" would be seen instead. Rogue antivirus is a particularly popular way to disguise a Trojan. In the early versions of this attack, a website would display a pop-up disguised as a normal Windows di'alog box with a fake security alert, warning the user that viruses have been detected. As browsers and security software have moved to block this vector, cold calling vulnerable users claiming to represent Microsoft support has become a popular attack.

QUESTION 109
Which mobile device strategy is most likely to introduce vulnerable devices to a corporate network?

A. COPE
B. MOM
C. BYOD
D. CYOD

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.4: The BYOD (bring your own device) strategy opens a network to many vulnerabilities. People can bring their personal devices to the corporate network, and their devices may contain vulnerabilities that could be allowed to roam free on a corporate network. COPE (company-owned/personally enabled) means that the company provides the users with a smartphone primarily for work use, but basic functions such as voice calls, messaging, and personal applications are allowed, with some controls on usage and f lexibility. With CYOD, the user can choose which device they wish to use from a small selection of devices approved by the company. The company then buys, procures, and secures the device for the user. The MDM is a mobile device management system that gives centralized control over COPE company-owned personally enabled devices.

QUESTION 110
Upon booting up a Windows 10 machine, you see an error message stating, "One or more services failed to start." Which of the following actions should you take?

A. Uninstall and reinstall the service
B. Verify that disabling 01ne service has not affected others
C. Disable application startup
D. Check the configuration of antivirus software

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.1: If you see a message such as "One or more services fai led to start" during the Windows load sequence, check Event Viewer and/or the Services snap-in to identify which service has failed. Troubleshooting services can be complex. Of t he options presented in t his question, only the one for verifying that disabling one service has not affected others would help correct a service t hat fai ls to start. This is because some services depend on other services to run, so if something or someone has disabled one service, it could have inadvertently affected others.

QUESTION 111
Which of the following is the BEST way to regularly prevent different security threats from occurring within your network?

A. Business continuity training
B. Disaster recovery planning
C. Penetration testing
D. User training and awareness

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.3: An enterprise network's end users are the most vulnerable attack vector. Studies have shown that an investment in end-user cybersecurity awareness training has the best return on investment of any risk mitigation strategy. While a penetration test might detect various threats and vulnerabilities in your network, it does not prevent them from occurring. Disaster recovery planning creates a disaster recovery plan, which is a documented, structured approach that describes how an organization can quickly resume work after an unplanned incident. Business cont inuity training will teach employees what to do in the case of a business cont inuity plan execution. A business continuity plan def ines how an organization will continue the delivery of products or services at pre-defined acceptable levels following a disruptive incident. Only end-user awareness training mitigates the biggest network vulnerability we have: our users.

QUESTION 112
A cybersecurity analyst notices that an attacker is trying to crack the WPS pin associated with a wireless printer. The device logs show that the attacker tried 00000000, 00000001, 00000002 and continued to increment by 1 number each time until they found the correct PIN52342. Which of the following type of password cracking was being performed by the attacker?

A. Dictionary
B. Hybrid
C. Brute-fo1rce
D. Rainbow table

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.4: A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. In a traditional brute-force attack, t he passcode or password is incrementally increased by one letter/number each time until t he right passcode/password is found. A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibilities, such as words in a dictionary. A rainbow table is a precomputed list of possible hashes used when trying to speed up the process of password cracking. A hybrid password cracking attack combines the use of a brute-force, attack with a dictionary attack by using words from the dictionary's list as the basis for the brute-force attack. For example, if the diction had the word Jason in it, the hybrid attack might try Jason123, Jason!@#, and J@$On as possible combinations based on the word Jason.

QUESTION 113
Which type of antivirus scan provides the best protection for a typical home user?

A. Daily scheduled scan
B. Weekly scheduled scans
C. On-access scans
D. Safe mode scans

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.5: On-access scans are a type of antivirus scan where the AV software intercepts operating system calls to open files to scan the file before allowing or preventing the file from being opened. On-acces.s scans reduce performance somewhat but are essential to maintaining effective protection against malware. Weekly and daily scans are good to use, but they are not as effective in preventing infe,ctions as an on-access scan. A system administrator normally conducts safe mode scans after malware is found by an on-access scan, daily, or weekly scan.

QUESTION 114
Samuel's computer is taking a very long time to boot up, and he has asked for your help speeding it up. Which TWO of the following actions should you perform to BEST resolve this issue with the least amount of expense?

A. Remove unnecessary applications from startup
B. Terminate processes in the Task Manager
C. Install additional RAMI
D. Perform a Disk Cleanup
E. Defragment the hard drive
F. Replace the hard drive with an SSD

Correct Answer: AE
Explanation

Explanation/Reference:
OBJ-3.1: To speed up the boot process, you can defragment the hard drive, remove unnecessary applications from startup, install additional RAM, and replace the hard drive with an SSD. But, to do it with the least amount of expense, you can only defragment the hard drive or remove unneoessary applications from starting up since these actions do not require any additional components to be purchased.

QUESTION 115
An attacker is using a word list that contains 1 million possible passwords as they attempt to crack your Windows password. What type of password attack is this?

A. Hybrid
B. Brute-fo1rce
C. Rainbow table
D. Dictionary

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.4: A dictionary attack uses a list of common passwords to crack a user's password. These lists do not have just dictionary words, though. For example, the word Dr@gOnBr3@+h (dragon breath) may be one such word but rewritten by substitut ing symbol.s or numbers for various letters. The dictionary file might have words like DRAGON, dragon, Dr@gOn, and many other forms. Most dictionary files contain millions of entries, and the password cracking tries each one until a match is found. A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. A hybrid attack combines a dictionary list with the ability to add brute-force combinations to crack a password that is slightly different than the dictionary list entry. A rainbow table is a tool for speeding up attacks against Windows passwords by precomputing possible hashes. A rainbow table is used to authenticate users by comparing the hash value of the entered password against the one stored in the rainbow table. Using a rainbow table makes password cracking a lot faster and easier for an attacker.

QUESTION 116
You are working as a penetration tester and have discovered a new method of exploiting a vulnerability within the Windows 10 operating system. You conduct some research online and discover that a security patch

against this particular vulnerability doesn't exist yet. Which type of threat would this BEST be categorized as?

A. Zero-day
B. Brute force
C. DDOS
D. Spoofing

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.4: A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited, and attackers release malware before a developer has an opportwnity to creat e a patch to fix the vulnerability, hence the term zero-day. A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. A brute-force attack consists of an attacker systematically trying all possible password and passphrase combinations until the correct one is found. Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source.

QUESTION 117
When using an MBR, which of the following types of partitions can only have up to four partitions?

A. Logical
B. Swap
C. Extended
D. Primary

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.9: Primary partitions are limited to only four primary partitions on a system using MBR. To overcome this limitation, extended partitions can be used. An extended partition is a partition that can be divided into additional logical drives. Unlike a primary partition, you don't need to assign it a drive letter and install a file system. When using MBR, you can support up to 23 logical drives in an extended partition. The swap partition on a Linux system is a portion of the hard disk formatted with a minimal kind of file system and used in s'ituations when the operating system runs out of physical memory and needs more of it. It can only be used by the memory manager and not for the storage of ordinary data files.

QUESTION 118
Dion Training uses DHCP to assign private Class A IP addresses to its Windows 10 workstations. Which of the following IP addresses is a Class A address?

A. 10.5.34.15
B. 169.254.125.154
C. 172.16.13.12
D. 192.168.2.14

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.6: Private IP addresses are any addresses in a specified range that are not allowed to be routed over the Internet. This allows companies to use these private IP addresses in their local area networks without having to purchase them from an internet registry .. The class A private IP address range contains the addresses from 10.0.0.0 to 10.255.255.255. The class B private IP address range contains the addresses

from 172.16.0.0 to 172.31.255.255. The class C private IP address range contains the addresses from 192.168.0.0 to 192.168.255.255. The APIPA/link-local autoconfiguration range is from 169.254.0.0 to 169.254.255.255.

QUESTION 119
A home user brought their Windows 10 laptop to the electronics store where you work. They claim their computer has become infected with malware. You begin troubleshooting the issue by first pressing the power button, and the laptop loads properly without any issues. When you open Microsoft Edge, you notice that multiple pop-ups appear almost immediately. Which of the following actions should you take NEXT?

A. Clear the browser's cookies and history, enable the pop-up blocker, and scan the system for malware
B. Quarantine the machine and report it as infected to your company's cybersecurity department for investigation
C. Reinstall or reimage the operating system
D. Document the pop-ups displayed and take a screenshot

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.2: Malware often targets the web browser. Malware such as adware and spyware is designed with commercial or criminal intent rather than to vandalize the computer system. Common infection symptoms of spyware or adware are popups or additional tool bars, the home page or search provider changing suddenly, searches returning results that are different to other computers, slow performance, and excessive crashing. Viruses and Trojans may spawn pop-ups without the user opening the browser. Since this is a home user's laptop, you should remediate the issue and return the system to them .. Since this is not a system owned by your company, there is no reason to report it to your company's cybersecurity department.

QUESTION 120
You are configuring a Windows 10 Professional workstation to connect to the Dion Training domain. To provide additional security to its users, Dion Training requires that all uses route their internet traffic through a server located at 10.0.0 .15 for inspection before it is sent to the internet. Once inspected, the server will route the traffic to the WAN router whose IP is 10.0.0.1. Which of the following settin.gs should be configured on the workstation to achieve this?

A. Under Network Adapter, configure the proxy server address as 10.0.0.15
B. Under Internet Options, configure the workstation's gateway as 10.0.0 .. 15
C. Under Internet Options, configure the proxy server address as 10.0.0.15
D. Under Network Adapter, configure the workstation's gateway as 10.0.0.15

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.6: A proxy server is a web server t hat acts as a gateway between a client application. To route all of the workstat ion's internet t raffic to the proxy server, a technician should configure the proxy server address under the Connections tab of the Internet Opt ions sect ion of the Cont rol Panel. The Internet Opt ions section of the Control Panel allows a technician ito manage the Internet settings for their computers, including the security settings, access set tings, and add-on cont rol settings. Using Internet Options, a technician can set t he homepage of the browser, set up the proxy server connection details, and change the trust and security settings used by the system.

QUESTION 121
Susan is installing several updates on a Windows computer. Nine of the updates were installed without any issues, but one update produced an error and failed to install. Susan restarts the computer as part of the troubleshooting process, and the computer automatically attempts to install the failed update again. Again, the update fails to inst all. What should Susan do NEXT?

A. Research the error number for the failed update and determine if there is a known ~ssue with this update
B. Download the update from a third-party website like Source Forge and install it
C. Manually download and install the failed update
D. Review the Event Viewer to determine the cause of the failure

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.2: If an automated system update f ails to install, you should research the error number for the failed update to determine if the issue is a known error. Based on the error code, you can then determine the best method to overcome t he issue. For example, a common cause of errors is inadequate space on the hard disk. If a technician needs to determine how to solve this issue best, researching the error code at Microsoft. com can help.

QUESTION 122
You are working on a customer's computer when your cellphone begins to ring. What should you do?

A. Apologize to the customer and send the call to voicemail
B. Answer the phone while continuing to work on the customer's computer
C. Ignore the phone and let it continue ringing until it goes to voicemail
D. Apologize to the customer and answer the phone

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.7: When working on a customer's computer, you should avoid dist ractions. You should not take personal calls, check your text messages,. talk to coworkers, or partake in other personal interruptions. It is important to remain professional. If your phone rings during your troubleshooting effort s, you should send it to voicemail and then apologize to the customer for the interruption.

QUESTION 123
A corporate workstation was recently infected with malware. The malware was able to access t he workstation's credential store and steal all the usernames and passwords from the machine. Then, the malware began to infect other workstations on the network using the usernames and passwords it stole from the first workst ation. The IT Director has directed its IT staff to develop a plan to prevent this issue from occurring again. Which of the following would BEST preve·nt this from reoccurring?

A. Install an anti-virus or anti-malware solution that uses heuristic analysis
B. Install a Unified Threat Management system on the network to monitor for suspicious traffic
C. Install a host-based intrusion detection system on all ofthe c.orporate workstations
D. Monitor all workstations for failed login attempts and forward them to a centralized SYSLOG server

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.3: The only solution that could stop tnis from reoccurring would be to use an anti-virus or anti-malware solution with heuristic analysis. The other options might be able to monitor and detect the issue but not stop it from spreading. Heuristic analysis is a method employed by many computer anti-virus programs designed to detect previously unknown computer viruses and new variants of viruses already in the wild. This is behavior-based detection and prevention, so it should detect the issue and stop it from spreading throughout the network. A host-based intrusion detection system (HIDS) is a device or software application that monitors a system for malicious activity or policy violations. Any malicious activity or violation is typically reported to an

administrator or collected centrally using a security information and event management system. The UTM is also acting as an IDS in this scenario based on the option presented.

QUESTION 124
Which of the following MacOS features allows you to use multiple desktops or spaces on a single system?

A. Finder
B. Dock
C. Mission Control
D. Boot Camp

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.10: Mission Control is an application for facilitating multiple desktops in the macOS environment. This enables the user to set up one or more desktops with different sets of apps, backgrounds, and so on, which is an easy way of managing tasks more effectively. To set up a new desktop, activate Mission Control with the F3 key. Dock is a macOS feature for managing applications from the desktop that is similar to the Windows taskbar. The Finder is the first thing that you see when your Mac finishes starting up. It opens automatically and stays open as you use other apps. It includes the Finder menu bar at the top of the screen and the desktop below that. It uses windows and icons to show you the contents of your Mac, iCioud Drive, and other storage devices. According to Apple, it is called the Finder because it helps you to find and organize your files. Boot Camp is used to allow dual booting on a Macintosh computer. It allows the user to boot into either macOS (OS X) or Windows as the computer is rebooted. Boot Camp is only supported on lntel-based macOS systems, though.

QUESTION 125
Dion Training has configured Windows Defender Firewall on all of its corporate Windows 10 laptops. When connected to a public network, the firewall has been configured to allow only inbound connections that match an existing rule and to only allow outbound connections that do match an existing rule to achieve the highest level of security. What type of security posture has Dion Trainin,g implemented?

A. Implicit allow for inbound, implicit allow for outbound
B. Implicit allow for inbound, explicitly allow for outbound
C. Explicit allow for inbound, implicit allow for outbound
D. Explicit allow for inbound, explicit allow for outbound

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.4: The Windows Defender Firewall is a software-based firewall that is installed by default on Windows workstations. The Windows Defender firewall is used to prevent hackers and malicious software from gaining access to the workstation over the Internet or t he local area network. Explicit allow refers to a security posture where the system will only allow an item to traverse the firewall if the traffic matches an existing rule. Implicit allow refers to a security posture where the system will allow all traffic to trav,erse the firewall unless there is a specif ic rule to prevent it. This type of explicit allow for both inbounder and outbound is known as an allow list posture as opposed to a blacklist or deny list posture.

QUESTION 126
You have just installed a new photo-sharing social media app on your smartphone. When you try to take a photo with the app, you hear the picture-taking sound. Unfortunately, when you check the app and your photo album, you cannot find any new pictures. Which of the following actions should you take to fix this issue?

A. Verify the app has the correct permissions

B. Perform a firmware update
C. Uninstalll and reinstall the app
D. Update all the smartphone's apps

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.4: Each app has to have the proper permissions to u1se the smartphone's various components, such as the microphone, camera, and storage. If the app has the correct permissions for the camera but not the storage, it will not store the phot os being taken. This issue can be quickly corrected by checking the permissions under the app's settings and the smartphone's settings.

QUESTION 127
You have submitted an RFC to install a security patch on all of your company's Windows 2019 servers during the weekly maintenance window. Which of the following change request documents would describe how the installation of the change will be performed during this maintenance window?

A. Plan
B. Scope
C. Risk analysis
D. Purpose

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.2: The plan of the change defines how the change or installation will occur. The change request documentation should define the 5 W's (who, what, when, where, why, and how), with the plan documentation covering how the change is implemented. For example, the plan might say that the installation will be performed manually or through an automated patching process. It may also dictate that all servers will receive the update simultaneously or that five servers will receive it first, then another ten, then the remaining twenty. The risk analysis portion of the change request documentation provides the risk levels of carrying out the change, or not performing the requested change at this time. Risk is the likelihood and impact (or consequence) of a given action. It is important to understand the risk involved with a change before deciding to proceed with implementing the change. The purpose of the change defines why the change or installation will occur. The change request documentation should define the 5 W's (who, what, when, where, why, and how) to define the why behind the change. For example, the purpose might be "to remediate several category one vulnerabilities so that our security is improved." The change's scope defines the area, number, size, or scale of a particular change. The change request documentation should define the exact scope of the change. In this example, only some of the Windows 2019 servers will receive the patch. If 50% of them are listed by their asset tracking number will receive the patch, this would clearly define this change's scope.

QUESTION 128
Which of the following remote access protocols should you use to connect to a Linux server seturely over the internet?

A. RDP
B. SSH
C. FTP
D. Telnet

Correct Answer: B
Explanation

Explanation/Reference:

OBJ-4.9: SSH (Secure Shell) is used to remotely connect to a network's switches and routers to configure them securely. SSH is typically used for logging into a remote machine and executing commands, but it also supports tunneling, forwarding TCP ports, and Xll connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model. Telnet should not be used in a network due to its weak security posture. Tel net transmits all of the data in plain text (without encryption), including usernames, passwords, commands, and data files. For this reason, it should never be used in production networks and has been replaced by SSH in most corporate networks. Remote Desktop Protocol (RDP) is a Microsoft protocol designed to facilitate application data transfer security and encryption between client user devices and a virtual network server. It enables a remote user to add a graphical interface to the desktop of another computer. FTP is used for file transfer only, not remote access.

QUESTION 129
Which file system type is used by default when installing macOS on a modern workstation?

A. NTFS
B. HFS+
C. APFS
D. FAT32

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.8: The Apple file system (APFS) is the default f ile system for Mac computers using macOS 10.13 or later and features strong encryption, space sharing, snapshots, fast directory sizing, and an improved f ile system fundamentals. The extended hierarchical file system (HFS+) is a journaling file system used natively by Apple's macOS systems before APFS was released in 2017. HFS+ can support a maximum volume size of 8 EB .. The NT file system (NTFS) is a Windows file system t hat supports a 64-bit address space and can provide extra feat ures such as file-by-file compression and RAID support as well as advanced file attribute management tools, encryption, and disk quotas. NTFS can support a maximum volume size of up to 8 PB. The file allocation table 32-bit (FAT32) is the 32-bit file system supported by Windows, macOS, and Linux computers. FAT32 can support maximum volume sizes of up to 2 TB and maximum file sizes of up to 4GB.

QUESTION 130
You are working as a service desk analyst. This morning, you have received multiple calls from users reporting that they cannot access websites from their work computers. You decide to troubleshoot the issue by opening up your command prompt on your Windows machine and running a program to determine where the network connectivity outage is occurring. This tool tests the end-to-end connection and reports on each hop found in the connection. Which tool should you use to determine if the issue is on the intranet portion of your corporate network or if it is occurring due to a problem with your ISP?

A. tracert
B. ping
C. nslookup
D. Netstat

Correct Answer: A
Explanation

Explanation/Reference:
Explanat ion
OBJ-1.2: Tracert is a command-line ut ility used to trace an IP packet's path as it moves from its source to its destinat ion. While using ping will tell you if the remote website is reachable or not, it will not tell you where the connection is broken. Tracert performs a series of ICMP echo requests to determine which device in the connection path is not responding appropriately. This will help to identify if the connectivity issue lies within your intranet or is a problem with the ISP's connection. The nslookup tool is used to troubleshoot DNS issues. The netstat tool is used to display network statistics and active connections. The ping tool is used to t est an

end-to-end connection, but it will not provide any data on t he hops found in the connection.

QUESTION 131
A network administrator has set up a firewall and set up only three allow rules so that traffic can be sent over ports 21, 110, and 25. Next, they added a f inal rule of "deny any any" to the end of the ACL to minimize the attack surface and better secure the network. Unfortunately, now the administrator is receiving complaints from users that they cannot access any web pages using their URLs, such as DionTraining.com. Which of the following should the administrator do to correct this issue?

A. Add a rule to the ACL to allow traffic on ports 110 and 389
B. Add a rule to the ACL to allow traffic on ports 80 and 53
C. Add a rule to the ACL to allow traffic on ports 139 and 445
D. Add a rule to the ACL to allow traffic on ports 143 and 22

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.1: The Hypertext Transfer Protocol (HTIP) uses port 80 and is an application layer protocol for distributed, collaborative, hypermedia information systems using unencrypted data transfer. The Domain Name System (DNS) uses port 53 and is a hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network. lfthe outbound port 80 is not open, then users will not be able to connect to a r,emote web server. If the outbound port 53 is not open, then the users will be unable to conduct a DNS name resolution and determine the IP address of the given web server based on its domain name. Port 22 is used for SSH/SCP/SFTP. Port 143 is used for I MAP. Port 139 and 445 are used for SMB. Port 389 is used for LDAP. Port 110 is used for POP3.

QUESTION 132
A user has asked you for a recommendation on which word processing software they should install. There are four different software packages they are considering, and ea,ch uses a different licensing type. The user states they do not want to pay for the software. Which of the following would MOST likely be the best option for them?

A. Open-source
B. Corporate
C. Enterprise
D. Personal

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.6: Open source is software that also makes the program code used to design it available. Generally, open-source software is free to use and distribute, but you may need to pay for ongoing support if you have technical issues. The idea is that other programmers can investigate the program and make it more stable and useful. An open-source license does not forbid commercial use of applications derived from the original, but it is likely to impose the same conditions on further redistributions. A Personal license is an option for private individuals who purchase a license with their own funds and solely for their own use. Personal licenses are not to be purchased, refunded, or in any way financed by companies. A business license is the standard licensing option for organizations and business entities. With Microsoft, a com[Pany can purchase anywhere from 1 to 300 user licenses under the business license program. An enterprise license is like a business licens,e, but for an unlimited number of users and is designed for large corporate and government networks.

QUESTION 133
Your coworker is creating a script to run on a Windows server using PowerShell. Which of the following file formats should the script use?

A. py
B. bat
C. psl
D. sh

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.8: Windows PowerShell enables you to perform management and administrative tasks in Windows 7 and later. It is fully integrated with the operating system and supports both remote execution and scripting. Microsoft provides the Windows PowerShellIntegrated Scripting Environment (ISE) to help create and manage your Windows PowerShell scripts. If you want to save a series of PowerShell commands in a file to rerun them later, you effectively create a PowerShell script by creating a text file with a .psl extension. The file can contain a series of PowerShell commands, with each command appearing on a separate line. Python is a general-purpose programming language that can develop many different kinds of applications. It is designed to be easy to read, and the programs use fewer lines of code compared to other programming languages. The code runs in an interpreter. Python is preinstalled on many Linux distributions and can be installed on Windows. Python scripts are saved using the .py extension. Batch scripts run on the Windows operating system and, in their simplest form, contain a list of several commands that are executed in a sequence. A .bat file is used for a batch script. You can run the file by calling its name from the command line or double-clicking the file in File Explorer. Generally, batch file scripts run from end to end and ar,e limited in branching and user input. A shell script is a file that contains a list of commands to be read and executed by the shell in Linux and macOS. A .sh file is used for a shell script and its first line always begins with #!/bin/bash that designates the interpreter. This line instructs the operating system to execute the script. Shell scripts allow you to perform various functions. These functions include automation of commands and tasks of system administration and troubleshooting, creating simple applications, and manipulating text or files.

QUESTION 134
Which type of installation would require an answer file to install the operating system?

A. Unattended
B. Repair
C. Upgrade
D. Clean

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.9: An unattended installation is a traditional method of deploying a Windows operating system in a large enterprise environment. Unattended installations use an answer file that contains user input to various GUI dialog boxes that would otherwise appear during the installation process. Unattended installation is the most practical way to install Windows when the client computers have different hardware components, and an image file cannot be used. Unattended installations save deployment time and can be used either for clean installs or in-place upgrades. A clean install is a means of installing the operating system to a new computer or completely replacing the operating system on an old computer. All existing user data or settings will be deleted during the setup process when a clean installation is conducted. An in-place upgrade is a means of installing an operating system on top of an existing version of the operating system. Applications, user settings, and data files are re,tained when conducting an in-place upgrade. A repair is used to check and replace any modified system f iles within t he operating system.

QUESTION 135
Sarah is installing Windows 10 {64-bit) in a virtual machine. The installation is continually failing and producing an error. She has configured the virtual machine with a dual-core 950 MHz processor, 4GB of memory, a 64GB hard drive, and a 1280 x 720 screen resolution. Which item in the virtual machine should be increased to fix the i nstallation issue experienced?

A. The amount of RAM is insufficient
B. The screen resolution is insufficient
C. The amount of storage space is insufficient
D. The processor is insufficient

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.7: The processor needs to be increased to at least 1 GHz or more. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space. For t he Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64GB of hard drive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space.

QUESTION 136
Jason is building a new workstation for his son to utilize w hen writing reports for school. The new computer will have an Intel x86 processor, 3GB of memory, and a 256GB SSD. Which of the following editions of Windows 10 would support this workstation at the lowest cost?

A. Pro for Workstations
B. Home
C. Pro
D. Enterprise

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.1: Windows 10 Home costs about $139 and is suited for a home computer or gaming. The Home edit ion is the cheapest edition of Windows and can support up to 128GB of RAM when using an x64 processor. Since t his workstation is only using an x86 processor, though, it is limited to 32-bits for memory addressing which results in a maximum of 4GB of RAM being supported. Windows 10 Pro, Pro for Workstations, and Enterprise will all have t his same memory limitation due to the x86 processor used in the workstation.

QUESTION 137
What is the minimum processor required to install Windows 10 (x86} on a device?

A. 2 GHz single-core processor
B. 1 GHz single-core processor
C. 1 GHz dual-core processor
D. 2 GHz dual-core processor

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.7: For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1GB of RAM, and at least 16GB of hard drive space. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20 GB of hard drive space. For the Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64GB of hard drive space.

QUESTION 138
Which of the following BEST describes how a DHCP reservation works?

A. By leasing a set of reserved IP addresses according to their category
B. By assigning options to the computers on the network by priority
C. By matching a MAC address to an IP address within the DHCP scope
D. By letting the network switches assign IP addresses from a reserved pool

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: When the client requests an IP address by sending a message on the network to the DHCP server, the DHCP server will assign an IP from its DHCP scope to the client and reserve it based on its MAC address. DHCP reservations allow the DHCP server to pre-set an IP address to a specific client based on its MAC address. This ensures that the cl ient will always get the same IP address from the DHCP server when it connects to the network. DHCP reservations are usually used with servers or printers on your internal network and are rarely used with end-user or client devices.

QUESTION 139
Two weeks ago, David's computer was infected with a virus. A technician performed the malware removal process on the machine, removed the infection from the system, update the system's software, and closed the trouble ticket. Now, many of the symptoms have returned on David's computer. Which of the following steps of the malware removal procedure did the technician MOST likely forget to perform as part of the original remediation?

A. Educate the end-user about how to avoid malware in the future
B. Update the anti-virus software and run a full system scan
C. Quarantine the infected system by removing its network connectivity
D. Enable System Restore and create a restore point in Windows

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.3: If a technician neglects to educate the end-user about avoiding malware in the future, they will likely get their computer infected again. For example, educating the user on best practices like being cautious when opening an attachment or clicking a link in an email, instant message, or post on social networks can prevent future infections.

QUESTION 140
Which command-line tool and option on a Windows system is used to force a background refresh of all group policy settings on a system?

A. dism /force
B. gpupdate /force
C. sfc /force
D. gpresult /force

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.2: A Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, Group Policy is applied to users or computers based on their membership in sites, domains, or organizat ional units. The gpupdate command-line tool is used to update the group policy settings on a Windows system. For an administrator to force a background update of all Group Policy settings regardless of

whether they have changed, they need to run "gpupdate /force" from the command line. The gpresult command is used to display the Resultant Set of Policy (RSoP) information for a remote user and computer. Because you can apply overlapping policy settings to any computer or user, the Group Policy feature generates a resulting set of policy settings when the user logs on. The gpresult command displays the resu lting set of policy settings that were enforced on the computer for the specified user when the user logged on. The deployment image servicing and management (DISM) is a command-line tool used to mount and service Windows images before deployment. The dism command with the /RestoreHealth option can run a scan to identify and repair any image or virtual hard drive corruption. The system fi le checker (SFC) command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from the command line.

QUESTION 141
Which command-line tool on a Windows system is used to display the resulting set of policy settings that were enforced on a computer for a specified user when they logged on?

A. dism
B. gpresult
C. sfc
D. Gpupdate

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.2: A Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, Group Policy is applied to users or computers based on their membership in sites, domains, or organizat ional units. The gpresult command is used to display the Resultant Set of Policy (RS.oP) information for a remote user and computer. Because you can apply overlapping policy settings to any computer or user, the Group Policy feature generates a resulting set of policy settings when the user logs on. The gpresult command displays the resulting set of policy settings that were enforced on the computer for the specified user when the user logged on. The gpupdate command-line tool is used to update the group policy settings on a Windows system. For an administrator to force a background update of all Group Policy settings regardless of whether they have changed, they need to run "gpupdate /force" from the command line. The deployment image servicing and management (DISM) is a command-line tool used to mount and service Windows images before deployment. The dism command with the /RestoreHealth option can run a scan to identify and repair any image or virtual hard drive corruption. The system fi le checker (SFC) command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from the command line.

QUESTION 142
Which mitigation provides the best return on investment by mitigating the most vulnerable attack vector in an enterprise network?

A. Update all antivirus definitions on workstations and servers
B. Provide end-user awareness trai1ning for office staff
C. Enable biometrics andl SSO for authentication
D. Remove unneeded services running on the servers

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.3: An enterprise network's end users are the most vulnerable attack vector. Studies have s.hown that an investment in end-user cybersecurity awareness t raining has the best return on investment of any r isk mit igation strategy. While all of the options presented are valid security mitigations, only end-user awareness training mitigates the biggest network vulnerability we have: our users.

QUESTION 143
A programmer is writing a script to calculate the disk space needed to perform a daily backup. The programming wants to document his script so that other programmers can understand what his logic was when he wrote it. Which of the following should he use?

A. Loop
B. Comment
C. Variable
D. Constant

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.8: A comment is written into the code to help a human understand the initial programmer's logic. In Python, for example, you can use the# symbol to comment on a line of code. Anything on the line after the# is ignored by the computer when the· script is being executed. A variable is a placeholder in a script containing a number, character, or string of characters. Variables in scripts do not have to be declared (unlike in programming languages) but can be assigned a value. Then, the variable name is referenced throughout the script instead of the value itself. A loop deviates from the initial program path to some sort of logic condition. In a loop, the computer repeats the task until a condition is met. Often implemented with For or While statements. For example, a short script like (For i=I to 100, print I, next) would print the numbers from 1 to 100 to the screen. A constant is a specific identifier tlhat contains a value that cannot be changed within the program. For example, the value to convert a number from F to Cis always 5/9 because the formula is C = (F -32) * 5/9.

QUESTION 144
Which of the following types of backups only copies data modified since the last full backup?

A. Differential
B. Incremental
C. Synthetic
D. Full

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.3: A differential backup only creates a copy of the selected data that has been modified since the last full backup. It is a good compromise in speed between a full backup (which takes the longest to backup and the least to restore) and an incremental backup (which takes the least to backup and the longest to restore). An incremental backup only creates a copy of new files and files modified since the last full, incremental, or differential backup. Therefore, it takes the least amount of time to complete a backup. Unfortunately, it also takes the most time to restore since you have to first restore the full backup, then any differential and incremental backups until all your data is restored. A full backup creates a copy of all the selected data regardless of when it was previously backed up. It takes the most time to complete a backup but is the fastest when condu,cting a restoral of all the data on a hard drive. Synthetic backup is the process of generating a file from a complete copy of .a file created at some past time and one or more incremental copies created at later times. The expression synthetic in this context refers to the fact that the assembled file is not a direct copy of any single current or previously created file. Instead, a synthetic file is merged or synthesized by a specialized application program from the original file and one or more modifications to it.

QUESTION 145
Your company wants to increase the security of its server room. Which TWO of the following should they install to protect the server room's contents?

A. Cable lock

B. Biometric lock
C. Badge reader
D. Privacy window shades
E. Strong passwords
F. Bollard

Correct Answer: BC
Explanation

Explanation/Reference:
OBJ-2.1: A badge re.ader and biometric lock can be used on a server room door to provide multifactor authent ication. Biometrics are identifying features stored as digital data t hat can be used to authenticate a user. Typical features used include facial pattern, iris, retina, or f ingerprint pattern, and signature recognition. This requires a relevant scanning device, such as a f ingerprint reader, and a database of biometric information for authentication to occur. A badge reader can be used to read a security badge using RFID, a smart card, or a barcode to authenticate a user. Cable locks are used for laptops, not servers or server rooms. A bollard is used in t he parking lot or the front of a building. Strong passwords are used for the servers, not the server room itself. Privacy windows shades could be used, but they are not as strong of a defense as a badge reader and biomet ric keypad on the door to the server room.

QUESTION 146
Dion Training wants to implement a new wireless network in their offices. Which of the following types would support encry[ption for traffic being sent and received over the network while still allowing users to connect to the open network without a password, passphrase, or digital certificate?

A. WPA3
B. WEP
C. WPA2
D. WPA

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.2: One of the features of WPA3 (WIFI6) is enhanced open. Enhanced Open enables encryption for traffic being sent and received over a wireless network when still using open authentication. WEP, WPA, WPA2 do not provide encryption of traffic sent over the network unless the network is protected by a password, passphrase, or digital certificat e.

QUESTION 147
What is the minimum amount of storage space required to install Windows 11 (x64} on a device?

A. 16GB
B. 32GB
C. 20GB
D. 64GB

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.7: For the Windows 11 (64-bit) operat ing system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64 GB of hard drive space. For the Windows 10 (32-bit) operat ing system, the minimum requirements are a 1 GHz processor, 1GB of RAM, and at least 16GB of hard drive space. For the Windows 10 (64-bit) operating system, t he minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space.

QUESTION 148
Your organization has recently suffered a data breach due to a server being exploited. As a part of the remediation efforts, the comparny wants to ensure that the default administrator password on each of the 1250 workstations on the network is changed. What is the easiest way to perform this password change requirement?

A. Revoke the digital certificate
B. Utilize the key escrow process
C. Create a new security group
D. Deploy a new group policy

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.1: A group policy is used to manage Windows systems in a Windows network domain environment utilizing a Group Policy Object (GPO). GPOs can include many settings related to credentials, such as password complexity requirements, password history, password length, and account lockout settings. You can force a reset of the default administrator account password by using a group policy update.

QUESTION 149
Tamera and her husband are driving to the beach for t he weekend. While her husband drives, she is using her iPhone to browse Facebook. Her phone shows only 1 bar of 3G signal in the current location. She can make and receive calls, but Facebook is refusing to load her news feed. Which of the following is MOST likely the problem?

A. The baseband firmware needs to be updated
B. The data speeds are insufficient with only one bar of signal
C. The cellular radio cannot connect to the cellphone towers
D. The smartphone has been infected with a virus

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: To make and receive a call using a smartphone, you need at least one bar of signal. A phone ca ll requires much less signal t han using cellular data. As the signal strength decreases, so does the data speed. Depending on the frequency and type of signal being used, you may see speeds under 100 Kbps with one bar. This is too slow to load a Facebook news feed adequat ely.

QUESTION 150
Jason took home a ,company-issued Windows 10 laptop home to do some work. He successfully connected it to his home's wireless network and verified he could access the internet and browse his favorite websites. Unfortunately, Jason cannot access any of the network's shared files from his home network's media server. Which of the following may be why Jason cannot access the network shares in his home network?

A. The laptop has an IP conflict
B. The laptop must join the network as private
C. The laptop's gateway is not properly configured
D. The laptop's DNS configuration is not properly setup

Correct Answer: B
Explanation

Explanation/Reference:

OBJ-1.6: The Network and Sharing Center in the Control Panel allows a technician to see information and modify the configuration settings of the network adapters in the workstation. The Network and Sharing Center is used to connect to a network using broadband, dial-up, or VPN connection, or add/remove fi le and printer sharing over the network on the workstation. When connecting to a network for the first time, the user must select if it is a public or private network. A public network will hide your computer from other devices on t he network and prevent file and printer sharing. A private network is considered trusted, allows the computer to be discoverable to other devices on the network, and supports the use of f ile and printer sharing.

QUESTION 151
Which type of security measure is used to control access to an area by using a retina scan?

A. Biometric
B. Optical reader
C. Cipher locks
D. Two-factor authentication

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.1: Retina scans are considered a biometric control. Other biometric controls contain fingerprint readers and facial scanners. A cipher lock is a lock that is opened with a programmable keypad that is used to limit and control access to a highly sensitive area. An opt ical reader is a device found within most computer scanners that can capture visual information and translate the image into digital information the computer is capable of understa1nding and displaying. Multi-factor authentication is an electronic authentication method in which a user is granted access t o a websit e or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: knowledge, possession, and inherence.

QUESTION 152
You have just installed a second monitor for a bookkeeper's workstation so they can stretch their spreadsheets across both monitors. This would essentially let them use the two monitors as one combined larger monitor. Which of the following settings should you configure?

A. Extended mode
B. Resolution
C. Refresh rate
D. Color depth

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: The extended mode allows t he Windows output to be stretched across two or more monitors as if they were a single monitor. This can be configured under the Display settings in Windows 10. Refresh rate is t he measure of how fast an image can be updated on a monitor or display. If a monitor has a lower refresh rate, then blurring and ghost ing can occur. Color depth defines how many unique colors can be displayed by the projected image at once. Most monitors have a default or native resolution. When you first connect a monitor to a Windows workstation, this native resolution is detected, and Windows attempts to configure itself automatically. If this creates an imbalance between the two monitors, a technician can adjust the screen's resolution by changing it in the Display settings area of Windows 10.

QUESTION 153
Dion Training is building a new computer for its video editor to use. The new computer will use an octa-core Intel processor, 3 TB of DDR4 memory, and a RAID 0 with two 4 TB SSDs for optimal performance. Which of the following editions of Windows 10 would support all of this computer's memory properly?

A. Home

B. Pro
C. Enterprise
D. Education

Correct Answer: C
Explanation

Explanation/Reference:
Explanat ion
OBJ-1.1: Microsoft Windows 10 Enterprise and Windows 10 Pro for Workstations are designed to run on devices with highperformance configurations, including server-grade Intel Xeon and AMD Opteron processors. Windows 10 Enterprise and Windows 10 Pro for Workstations both support up to four physical CPUs and 6 TB of RAM. Windows 10 Pro and Windows 10 Education both only support two physical CPUs and 2 TB of RAM. Windows 10 Home only supports one physical CPU and up to 128GB of RAM.

QUESTION 154
Jason's company issued him an old 20181aptop with an internal hardware security key that he uses to connect to his office network over a VPN while t raveling. Without this laptop, Jason cannot access his company's internal servers, email, or share drive files. The Windows 10 laptop is extremely slow, and the screen recently cracked and needs to be replaced. When Jason returns to the company's headquarters, the company will provide him with a new laptop due to the broken screen. Until then, he is working out of his hotel room during a 45-day business trip and needs to continue using this laptop. Jason brings the laptop to the computer store you work at and asks for your assistance. Which of the following do you recommend?

A. Replace the display and contact t he manufacturer for reimbursement
B. Sell him an externallS'" tablet/monitor to connect to the laptop as a workaround
C. Replace the display and charge him for the parts/installation
D. Purchase a new laptop as the cost to repair might be more than a new laptop

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.7: In this scenario, you should recommend that he purchase an external15" tablet/monitor to connect to the laptop as a workaround until he can return to the company's headquarters. Since the laptop has an internal hardware key, if he replaces it with a new laptop then it will not connect to the corporate network over the VPN. The laptop is outside of the warranty period, making the recommendation of replacing the display and being reimbursed by the manufacturer . While you could replace the display and charge him for the parts/ installation, this would likely be more expensive than simply buying an external tablet/monitor as a workaround. A laptop replacement display usually costs between $300-500, whereas an external tablet/monitor costs between $100-150. The cheapest and quickest option provided would be to purchase an external monitor to use in his hotel until he gets back to the office.

QUESTION 155
What type of structure is a "Do While" in scripting?

A. Constant
B. Branch
C. Loop
D. Variable

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.8: A loop deviates from the initial program path to some sort of logic condition. In a loop, the computer

repeats the task until a condition is met. Often implemented with For, For Next, While, or Do While statements. For example, a short script like (For i=1 to 100, print I, next) would print the numbers from 1 to 100 to the screen. A branch is used to control the flow within a computer program or script, usually based on some logic condition. Often, these are implemented with IF THEN ELSE statements. A variable is a placeholder in a script containing a number, ,character, or string of characters. Variables in scripts do not have to be declared (unlike in programming languages) but can be assigned a value. Then, the variable name is referenced throughout the script instead of the value itself. A constant is a specific identifier that contains a value that cannot be changed within the program. For example, the value to convert a number from F to Cis always 5/9 because the formula is C = (F -32) * 5/9.

QUESTION 156
You are troubleshooting a comput er that is operating slowly. Which of the following tools should you use to troubleshoot this workstation?

A. DxDiag
B. Device manager
C. Task scheduler
D. Performance monitor

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.1: Windows Performance Monitor can be used to provide real-time charts of system resources or can be used to log information to a file for long-term analysis. By monitoring different resources at different times of the day, you can detect bottlenecks in a system that are causing problems. It may be that a particular application starts freezing for longer and longer periods. Many things could cause this. Perhaps it is that the processor is too slow, which would cause the requests to take longer. If the hard disk is too slow, this would mean that it takes too long for the computer to open and save files. If the application uses a network link, that link could have become faulty or congested. The task scheduler is a tool included with Windows that allows predefined actions to be automat ically executed whenever a certain set of conditions is met. For example, you can schedule a task to run a backup script every night or send you an email whenever a certain system event occurs. Device manager (devmgmt.msc) is a utility used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware t hat is not working so that a technician can repair or replace it. The DirectX diagnostic (dxdiag.exe) utility is used to collect info about devices to help t roubleshoot problems with DirectX sound and video. It is a diagnostics tool used to test DirectX functionality and troubleshoot video-related or sound-related hardware problems. DirectX diagnostic can save text files with the scan results.

QUESTION 157
Which of the following types of encryption is considered the most secure to utilize in a SOHO network?

A. WPS
B. WEP
C. WPA3
D. WPA2

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.2: Wi- Fi protected access version 3 (WPA3) has replaced WPA2 as the most secure wireless encryption method. WPA3 uses the simultaneous authentication of equals (SAE) to increase the security of preshared keys. WPA3 provides the enhanced open mode that encrypts transmissions from a client to the access point when using an open network. WPA3 Enterprise mode supports the use of AES with the Galois/ counter mode protocol (GCMP-256) for the highest levels of encryption. Wi-Fi protected access version 2 {WPA2) replaced the original version of WPA after the completion of the 802.11i security standard. WPA2

features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is sti ll available for home and small office networks. WPA2 uses t he improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption. Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks that can break its encryption. WEP relies on the use of a 24-bit initialization vector to secure its preshared key. The Wi-Fi Protected Setup (WPS) is a mechanism for auto-configuring a WLAN securely for home users. On compatible equipment, users push a button on the access point and connect adapters to associate them securely. WPS is subject to brute force attacks against the PIN used to secure them, making them vulnerable to attack.

QUESTION 158
Which of the following allows a user to save their current session to memory and put a Windows 10 computer into a minimal power state?

A. Shutdown
B. Lock
C. Hibernate
D. Sleep

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.4: Sleep or standby mode is used to save the current session to memory and put the computer into a minimal power state ito save battery life when the system is not being used. The comput er takes less time to start up again from the sleep or standby mode than it does from the hibernate mode. Hibernate mode is used to save the current session to disk before powering off the computer to save battery life when the system is not being used. The computer takes longer to start up again from hibernate mode than it does from the sleep or standby mode. Shutdown mode completely powers off the computer and does not save the current user session to disk. Instead, the shutdown will close all open fi les and log out the user during the shutdown process. A lock will secure the desktop with a password while leaving programs running.

QUESTION 159
You are troubleshooting a computer that is not producing any sounds through its speakers. Which of the following tools should you use to troubleshoot this workstation?

A. Performance monitor
B. Task scheduler
C. Device manager
D. RDS

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.1: Device manager (devmgmt.msc) is a util ity used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it. If there is no audio being played, it could be an issue with the audio card or its drivers. Performance monitor (perfmon.msc) is a performance monitoring and system monitoring utility in Windows that is used to monitor the activities on CPU and memory activity on a computer. The performance monitor is used to view performance data either in rea l-time or from a log file. The performance monitor can only monitor the resource utilization, but it cannot manage or terminate those processes. The t ask scheduler is a tool included with Windows that allows predefined actions to be automatically executed whenever a certain set of conditions is met. For example, you can schedule a task to run a backup script every night or send you an email whenever a certain system event occurs. Remote desktop services (RDS) is used to connect to a remote desktop session host servers or other remote computers, edit an existing remote desktop connection (. rdp) configuration file, and migrate legacy connection files that were created with the client connection manager to

the newer .rdp connection file type.

QUESTION 160
Your company is concerned about the possibility of power fluctuations that may occur and cause a small increase in the input power to their server room. What condition is this known as?

A. Power spikes
B. Power failure
C. Under-voltage event
D. Power surge

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.5: An extended over-voltage event is known as a power surge. A power surge is basically an increase in your electr ical current . A power surge often has levels of 10-30% above the normal line voltage and lasts from 15 milliseconds up to several minutes. An under-voltage eve·nt is a reduction in or restriction on the availability of electrical power in a particular area. The irregular power supply during an under-voltage event can ruin your computer and other electronic devices. Electronics are created to operate at specific voltages, so any f luctuations in power (both up and down) can damage them. To protect against an under-voltage event, you can use either a battery backup or a line conditioner. A significant over-voltage event that occurs for a very short t ime is known as a power spike. A power spike is a very short pulse of energy on a power line. Power spikes can contain very high voltages up to and beyond 6000 volts but usually last only a few milliseconds instead of longer but lower voltage power surges. A power loss or power failure is a tot al loss of power in a particular area. To prot ect against a power loss or power failure, a battery backup should be used.

QUESTION 161
Jason is building an inexpensive workstation for one of the employees at Dion Training. The workstation will utilize an Intel x86 processor. Which of the following editions of Windows will support installation on this workstation?

A. Windows 11 Home
B. Windows 10 Enterprise
C. Windows 11 Pro
D. Windows 10 Pro

Correct Answer: BD
Explanation

Explanation/Reference:
OBJ-1.1: All editions of Windows 10 are available in either x86 (32-bit) or x64 (64-bit) versions. When using a 32-bit version of Windows 10, a maximum of 4GB of RAM is supported. All editions of Windows 11 only support x64 (64-bit) processors due to the higher minimum memory requirements. All Windows 11 editions require a minimum of 4 GB of memory to operate.

QUESTION 162
You attempt to boot a Windows 10 laptop and receive an "Operating System Not Found" error on the screen. You can see the hard disk listed in the UEFI/BIOS of the system. Which of the following commands should you use to repair the boot sector of the hard disk?

A. bootrec /rebuildbcd
B. bootrec /fixboot
C. diskpart list
D. bootrec /fixmbr

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.1: To repair the drive's boot sector, you should use the command "bootrec /fixboot" and reboot the computer. If the disk cannot be detected, enter the system setup and t ry modifying settings (or even resetting the default settings). If the system firmware reports the disk's presence, but Windows sti ll will not boot, use a startup repair tool to open a recovery mode command prompt and use the bootrec tool to repair the drive's boot information. The "bootrec /fixmbr" command is used to attempt a repair of the master boot record of a drive. The "bootrec /rebuildbcd" command is used to add missing Windows installations to the Boot Configuration Database (BCD). The diskpart command is a command-line diskpartitioning utility available for Windows that is used to view, create, delete, and modify a computer's disk partitions.

QUESTION 163
Dion Training wants to implement a new wireless network using WPA3 in their offices. Which of the following features of WPA3 is used to provide a password-based authentication using the dragonfly handshake instead of the older WPA 4- way handshake?

A. Management protection frames
B. AESGCMP
C. SAE
D. Enhanced open

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.2: Simultaneous Authentication of Equals (SAE) is a password-based authentication and password-authenticated key agreement method used in WPA3 that replaced the 4-way handshake used in WPA-based wireless networks. The SAE handshake is also known as the dragonfly handshake. Enhanced Open enables encrypt ion for traffic being sent and received over a wireless network when still using open authentication. AES Galois Counter Mode Protocol (GCMP) is a high-performance mode of operation for symmetric encryption that supports authent icated encryption with associated data (AEAD). Management protection frames protect unicast and multicast management action frames to protect against eavesdropping and forgery in WPA3-based wireless networks.

QUESTION 164
A programmer is writing a script to display all the numbers from 1 to 100 to the screen. Which of the following should they use in their script?

A. Branch
B. Constant
C. loop
D. Comment

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.8: A loop deviates from the init ial program path to s.ome sort of logic condition. In a loop, t he computer repeats t he task until a condition is met. Often implemented with For or While statements. For example, a short script like (For i=1 to 100, print I, next) would print the numbers from 1 to 100 to the screen. A constant is a specific identifier t hat contains a value that cannot be changed within t he program. For example, the value to convert a number f rom F to Cis always 5/9 because the formula is C = (F -32) * 5/9. A comment is written into the code to help a human understand the init ial programmer's logic. In Python, for example, you can use the# symbol to comment on a line of code. Anything on the line after the# is ignored by the computer when the script is being executed. A branch is used to control the flow within a computer program or script, usually

based on some logic condition. Often, these are implemented with IF THEN ELSE statements.

QUESTION 165
Which of the following types of software CANNOT be updated via the Windows Update program?

A. Security patches
B. Critical fixes
C. Driver updates
D. Firmware updates

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.8: The Windows Update program can download critical fixes, security patches, and driver updates. The Windows Update program cannot download and install firmware updates because the firmware must be updated before the Windows operating system begins running during the boot process.

QUESTION 166
What does the command "shutdown /h" do on a Windows workstation?

A. Shutdown the workstation
B. Log off the workstation
C. Enter sleep mode
D. Reboot the workstation

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.2: The shutdown command allows a user or administrator to shut down or restart local or remote computers, one at a time. Using the /r option will reboot the computer. Using the /s option will shut down the computer. Using the /1 option will log off the current user. Using the /h option will enter sleep or hibernation mode.

QUESTION 167
Which of the following pairs of authentication factors should you choose to meet the requirements associated with MFA?

A. Thumbprint and retina scan
B. Username and pin
C. Thumbprint and password
D. Username and password

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.1: Multi-factor authentication (MFA) requires a user to provide at least two different forms of authentication:
something you know (username, password, pin), something you have (token, key fob, smartphone), something you are (fingerprint, retina scan), something you do (the way you speak a phrase or sign your name), or somewhere you are (location factor based on IP address or geolocation).

QUESTION 168
What is the minimum amount of RAM needed to inst all Windows 10 on a 32-bit system?

A. 4GB
B. 8GB
C. 2GB
D. 1GB

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.7: For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1GB of RAM, and at least 16GB of hard drive space.

QUESTION 169
Which of the following commands is used on a linux system to search for lines t hat match a pattern within a file?

A. pwd
B. vi
C. apt-get
D. grep

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.11: The grep is a command-line utility for searching plain-text data sets for lines that match a regular expression. The grep command works on Unix, Linux, and macOS operating systems. Grep is an acronym that stands for Global Regular Expression Print. The vi (visual) utility is a popular screen-oriented text editor in Linux, Unix, and other Unix-like operating systems. When using vi, the terminal screen acts as a window into the editing buffer. Changes made to the editing buffer shall be reflected in the screen display, and the position of the cursor on the screen will indicate the position within the editing buffer. The pwd command displays t he present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen. Tlhe apt-get util ity is a powerful package management command-line program that works with Ubuntu's APT (Adlvanced Packaging Tool) library to install new software packages, remove existing software packages, upgrade existing software packages, and even upgrade the entire operating system. The apt-get utility works with Ubuntu and Debian-based Linux distributions.

QUESTION 170
Jack has asked you for a recommendation on which word processing software they should insta ll. There are four different software packages they are considering, and ea,ch uses a different licensing type. Jack states he wants to get a copy of Microsoft Word so their son can create reports for school. Which of the following would MOST likely be the best option for them?

A. Enterprise
B. Open-source
C. Personal
D. Business

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.6: A personal license is an option for private individuals who purchase a license with their own funds and solely for their own use. Personal licenses are not to be purchased, refunded, or in any way financed by

companies. A business license is the standard licensing option for organizations and business entities. With Microsoft, a company can purchase anywhere from 1 to 300 user licenses under the business license program. An enterprise license is like a business license, but for an unlimited number of users and is designed for large corporate and government networks. Open-source is software that also makes the program code used to design it available. Generally, open-source software is free to use and distribute, but you may need to pay for ongoing support if you have technical issues. The idea is that other programmers can invest igate the program and make it more stable and useful. An open-source license does not forbid commercial use of applications derived from the original, but it is likely to impose the same conditions on further redistributions.

QUESTION 171
Which of the following open-source remote access tools allows users to connect to their desktop remotely, see what is on their screen, and control it with their mouse and keyboard?

A. RDP
B. Telnet
C. VNC
D. SSH

Correct Answer: C
Explanation

Explanation/Reference:
Explanat ion
OBJ-4.9: VNC (virtual network computing) is a remote access tool and protocol. It is used for screen sharing on Linux and macOS. RDP is not open-source. SSH and tel net are text-based remote access tools. Remote Desktop Protocol (RDP) uses port 3389 and is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection. Secure Shell (SSH) uses port 22 to securely create communication sessions over the Internet for remote access to a server or system. Tel net uses port 23 to provide a bidirectional interactive text-oriented communication facility using a virt ual terminal connection but sends its data in plaintext making it an insecure protocol.

QUESTION 172
Which of the following types of mobile device screen loclks uses biometrics to securely unlock the device?

A. FaceiD
B. Swipe
C. Passcode
D. TouchiD

Correct Answer: AD
Explanation

Explanation/Reference:
OBJ-2.7: The FaceiD and TouchiD screen locks rely upon biometric data to securely unlock the device. Face ID is a facial recognition system designed and developed by Apple. Touch ID is an electronic fingerprint recognition feature designed and released by Apple. Since biometrics are body measurements and calculations related to human characteristics, the use of a person's face or fingerprint is classified as a biometric authentication system. A swipe lock is a term for unlocking a device by tracing a predetermined on-screen pattern or joining dots on the screen. This was commonly used in Android devices until biometric methods li'ke fingerprint scanners and facia l recognition became more prevalent. A passcode unlock is a term for unlocking a device by entering a 4 to 6 digit pin.

QUESTION 173
You have decided to have DNA genetic testing and analysis performed to determine your exact ancestry composition and possibly find some lost relatives through their database. Which of the following types of data should this be classified?

A. CUI
B. Pll
C. IP
D. PHI

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.6: Protected health information (PHI) refers to medical and insurance records, plus associated hospital and laboratory test results. Data collected by genetic mapping and heredity companies include t he subject's DNA, making it PHI. Personally identifiable information (P II) is data that can be used to identify, contact, or locate an individual. Information such as social security number (SSN), name, date of birth, email address, telephone number, street address, and biometric data is considered PI I. Proprietary information or intellectual property (IP) is information created and owned by the company, typically about the products or services that they make or perform. Controlled Unclassified In formation (CUI) is federal non-classified information t hat must be safeguarded by implementing a uniform set of req uirements and information security controls to secure sensitive government information.

QUESTION 174
Which of the following data types would be used to store the number 21?

A. String
B. Integers
C. Boolean
D. Floating point

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.8: An integer stores a whole number, such as 21, 143, or 1024. An integer data type usually consumes 8 bytes of storage. A floating-point number stores a fractional or decimal number, such as 3.14, 45.5, or 333.33. A f loating-point number data type usually consumes 4 to 8 bytes of storage. A boolean stores a value of TRUE (1) or FALSE (0). It usually consumes only 1 bit of storage (a zero or a one). A string stores a group of characters, such as He·llo, PYTHON, or JasonDion. A string data type usually consumes as much storage as necessary. Each character in the string usually requires 1 byte of storage.

QUESTION 175
Which of the following Control Panel sections would allow a technician to add or remove an external scanner from a Windows 10 computer?

A. Programs and Features
B. System
C. Device Manager
D. Devices and Printers

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.4: The Devices and Printers section of the Control Panel allows a technician to manage the printers, scanners, and other external devices connected to a Windows computer. The System section of tfhe Control Panel allows a te,chnician to see information about the workstation, including the processor type, amount of memory, and operating system version installed on the computer. The Device Manager is used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is

not working so that a technician can repair or replace it. The Programs and Features section of the Control Panel allows a technician to install or remove applications, software packages, and features in the Windows operating system.

QUESTION 176
The video editor at Dion Training is having issues with her workstation. The workstation is running Windows 10 and is failing to boot up properly. A technician wants to replace the existing operating system files with a new copy of the same version. The technician has been told to ensure the user's data and applications are not modified or deleted during the upgrade or installation. Which types of upgrades or installations should the technician use?

A. Clean install
B. Repair installation
C. Refresh installation
D. In-place upgrade

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.9: Repair installation is a type of installation that attempts to replace the existing version of the operating system files with a new copy of the same version. A repair installation is useful when trying to repair a Windows computer that will not boot or when you believe the system f iles have become corrupted. A repair installation will only affect the system files and not any of the user's settings, customizations, or applications. A clean install is an installation of the new operating system on a new computer or a computer that has been recently formatted. A clean install will completely replace the operating system software on the computer with the new operating system. During a clean install, all ofthe user's data, settings, and applications will be deleted. An in-place upgrade is an installation of the new operating system on top of an existing version of the operating system. An in-place upgrade will preserve the applications, user settings, and data files that already exist on the computer. A refresh installation is a type of installation that will recopy the system files and revert most system settings to their default configuration while preserving user personalization settings, data files, and applications installed through the Windows Store. Any applications installed outside of the Windows Store, though, will be deleted if you use a refresh installation.

QUESTION 177
A new corporate policy dictates that all access to network resources will be controlled based on the user's job functions and tasks within the organization. For example, only people working in Human Resources can access employee records, and only the people working in finance can access customer payment histories. Which of the following security concepts is BEST described by this new policy?

A. Directory permissions
B. Permission creep
C. Least privilege
D. Blacklists

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.1: Least privilege is the concept and practice of restr icting access rights for users, accounts, and computing processes to only those resources absolutely required to perform routine, legitimate activities. Privilege itself refers to the authorization to bypass certain security restraints. Permissions Creep, also known as privilege creep, is what happens when an employee moves between roles in an organization and keeps the access or permissions of the previous role. Directory permissions are used to determine which us,ers can access, read, write, and delete files or directories within a given directory. A blacklist is a list of IP addresses, ports, or applications that are not allowed to be run or used on a given system.

QUESTION 178
An employee at Dion Training complains that every time airplane mode is enabled on their lapt op, their external mouse and headphones stop working. Which of the following technologies is being disabled by airplane mode and likely causing the issues experienced by this user?

A. Wireless
B. GPS
C. Cellular
D. Bluetooth

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.4: Bluetooth is a wireless connectivity method that is usually used by external mice and wireless headphones. When airplane mode is enabled, the GPS, cellular, wireless, and Bluetooth radios are usually disabled in smartphones, tablets, or laptops. If the Bluetooth radio is turned off/disabled, it will cause issues with Bluetooth-connected devices like mice and headphones. Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the industrial, scientific, and medical radio bands from 2.402 GHz to 2.480 GHz and building a personal area network (PAN). Bluetooth is commonly used when connecting wireless devices like mice, trackpads, headphones, and other devices. A GPS (global positioning system) device is used to determine a reoeiver's position on the Earth based on information received from 24 GPS satellites, which operate in a constellation in Medium Earth Orbit (MEO). lhe receiver must have a line-of-sight to four of the GPS satellites continuously to accurately determine its position on the earth (latitude, longitude, and altitude). A cellular radio is a component in a mobile device capable of switching frequencies automatically when moving between network cells without losing the connection. Wi-Fi is the IEEE 802.11 standard for wireless networking based on spread spectrum radio transmission in the 2.4 GHz and 5 GHz bands. The standard has six main iterations (a, b, g, n, ac, and ax), describing different modulation techniques, supported distances, and data rates.

QUESTION 179
You are troubleshooting a Windows 10 laptop that is infected with malware. You have already identified the type of malware on the laptop. What should you do NEXT? (Select THREE)

A. Disable System Restore in Windows
B. Educate the end user
C. Schedule scans and run system updates
D. Update the anti-malware software
E. Enable System Restore in Windows
F. Disconnect the laptop from the network

Correct Answer: ADF
Explanation

Explanation/Reference:
OBJ-3.3: The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update antimalware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 180
A user with an older laptop running Windows 7 that has only 2GB of RAM, 32GB of SSD, and a 1.7 GHz 64-bit processor. The user would like to upgrade to a newer OS since Windows 7 is now considered end-of-life. Which of the following operating systems should the technician recommend to ensure the BEST performance on this computer?

A. Windows8.1
B. Windows 11
C. Windows 10
D. Windows8

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.9: The user should update their laptop to Windows 10 since it is not considered end-of-life yet and will support being installed on a laptop with only 2GB of RAM. Windows 10 minimum requirements for a 32-bit operating system are a 1 GHz processor, 1GB of RAM, and at least 16GB of hard drive space. Windows 10 minimum requirements for a 64-bit operating system are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space. Windows 11 requires a 1 GHz processor, 4GB of RAM, and 64GB of hard drive space. Windows 8 and Windows 8.1 are considered end-of-lif,e and should not be installed.

QUESTION 181
Which of the following Windows tools can a technician use to display information about the performance of hardware and software resources in real-time?

A. dxdiag.exe
B. resmon.exe
C. devmgmt.msc
D. msinfo32.exe

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.3: Resource monitor (resmon.exe) is a utility used to display information about the use of hardware (CPU, memory, disk, and network) and software (file handles and modules) resources in real-time. The resource monitor helps check the performance counters of specific resources and decide a course of action to improve the performance. System information (msinfo32.exe) is a utility that gathers information about your computer and displays a comprehensive list of hardware, system components, and the software environment that can be used to diagnose computer issues. The DirectX diagnostic (dxdiag.exe) utility is used to collect info about devices to help troubleshoot problems with DirectX sound and video. It is a diagnostics tool used to test DirectX functionality and troubleshoot video-related or sound-related hardware problems. DirectX diagnostic can save text files with the scan results. Device manager (devmgmt.msc) is a utility used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it.

QUESTION 182
Which of the following policies or plans would dictate the complexity requirements for a wireless network's shared secret key?

A. Acceptable use policy
B. Password policy
C. Data loss prevention policy
D. Remote access policy

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.6: A password policy is a set of rules created to improve computer security by motivating users to

create dependable, secure passwords and then store and utilize them properly. This document promotes strong passwords by specifying a minimum password length, complexity requirements, requiring periodic password changes, and placing limits on ithe reuse of passwords. An acceptable use policy (AUP) is a set of rules applied by the owner, creator, or administrator of a network, website, or service, that restrict how the network, website, or system may be used and sets guidelines as to how it should be used. A data loss prevention policy is a document that defines how organizations can share and protect data. It guides how data can be used in decision-making without it being exposed to anyone who should not have access to it. The goal of a data loss prevention policy is to minimize accidental or malicious data loss. A remote access policy is a document that outlines and defines acceptable methods of remotely connecting to the internal network.

QUESTION 183
Your Android device's battery is advertised to last 12 hours, but it drains almost completely within 90 minutes. What should you do FIRST to try and solve this problem?

A. Enable airplane mode to save battery
B. Check which apps are using the most battery life
C. Dim your phone's display
D. Reboot your phone

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: If your battery is dying faster than in t he past, see whether apps are using too much battery. You can force stop or uninstall problem apps. If your device is infected with malware, this can also drastically reduce your battery life, and the malware should be removed. The display on a smartphone is normally one of the largest users of battery life, but even a brightly lit display will not consume the entire battery in only 90 minutes.

QUESTION 184
Which of the following types of backup would require the MOST time to complete?

A. Full
B. Differential
C. Synthetic
D. Incremental

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.3: A full backup creates a copy of all the selected data regardless of when it was previously backed up. It takes the most time to complete a backup but is the fastest when conducting a restoral of all the data on a hard drive. A differential backup only creates a copy of the selected data that has been modified since the last full backup. It is a good compromise in speed between a fu ll backup (which takes the longest to backup and the least to restore) and an incremental backup (which takes the least to backup and the longest to restore). An incremental backup only creates a copy of new files and files modified since the last full, incremental, or differential backup. Therefore, it takes the least amount of time to complete a backup. Unfortunately, it also takes the most time to r,estore since you have to first restore the full backup, then any differentijal and incremental backups until all your data is restored. Synthetic backup is the process of generating a file from a complete copy of a file created at some past time and one or more incremental copies created at later times. The expression synthetic in this context refers to the fact that the assembled file is not a direct copy of any single current or previously created file. Instead, a synthetic file is merged or synthesized by a specialized application program from the original file and one or more modifications to it.

QUESTION 185
Which of the following is used to communicate da,ta and preferences to child processes within a script or batch f ile?

A. Constants
B. Environmental variables
C. Comments
D. Variables

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.8: Shell scripts and batch files use environment variables to communicate data and preferences to child processes. They can also be used to store temporary values for reference later in a shell script. A variable is a placeholder in a script containing a number, character, or string of characters. Variables in scripts do not have to be declared (unlike in programming languages) but can be assigned a value. Then, the variable name is referenced throughout the script instead of the value itself. A comment is written into the code to help a human understand the initial programmer's logic. In Python, for example, you can use the # symbol to comment on a line of code. Anything on the line after the # is ignored by the computer when the script is being executed. A constant is a specific identifier that contains a value that cannot be changed within the program. For example, the value to convert a number from F to Cis always 5/9 b,ecause the formula is C = (F -32) * 5/9.

QUESTION 186
Tim has created a new iOS application that he wants to install on an iPad without having to install it through the official App Store. To save some money, he has not purchased a developer certificate from Apple since he isn't planning to sell this app to others. Which of the following would allow Tim to install this unofficial app on his own iPad for testing?

A. Jailbroken device
B. APK installer
C. Developer mode
D. Rooted device

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.5: Jailbreaking is conducted on an iOS device to remove manufacturer restrictions on the device and allow other software, operating systems, or networks to work with a device. An android application package (APK) is a third-party or custom program that is installed direct ly on an Android device to give users and business the flexibility to install apps directly on Android devices. Android supports sideloading through the APK package format. An APK file contains all of that program's code, including .dex files, resources, assets, certificates, and manifest files. A rooted device is an Android device that has been hacked to provide the user with administrative rights to install unapproved apps, update OS, delete unwanted apps, underclock or overclock the processor, replace firmware and customize anything else. A rooted device is not required just to install an APK outside of the Play Store, though, on an Android device. Devleoper mode is used on an Android device to show additional diagnostic information when using apps or making network connections.

QUESTION 187
Which of the following is the MOST secure wireless security and encryption protocol?

A. WPA2
B. WPA
C. WPA3
D. WEP

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.2: Wi-Fi protected access version 3 (WPA3) has replaced WPA2 as the most secure wireless encryption method. WPA3 uses the simultaneous authentication of equals (SAE) to increase the security of preshared keys. WPA3 provides the enhanced open mode that encrypts transmissions from a client to the access point when using an open network. WPA3 Enterprise mode supports the use of AES with the Galois/ counter mode protocol (GCMP-256) for the highest lev,els of encryption. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.11 i se,curity standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption. Wi-Fi protected access (WPA) is an improved encryption scheme for protecting Wi-Fi communications designed to replace WEP. WPA uses the RC4 cipher and a temporal key int,egrity protocol (TKIP) to overcome the vulnerabilities in the older WEP protection scheme. Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks that can break its encryption. WEP relies on the use of a 24-bit initializat ion vector to secure its preshared key.

QUESTION 188
Which of the following concepts is the MOST important for a company's long-term health in the event of a disaster?

A. Implementing an acceptable use policy
B. Off-site backups
C. Uninterruptible power supplies
D. Vulnerability scanning

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.3: In case of a disaster, you must protect your data. Some of the most common strategies for data protection include backups made to tape and sent off-site at regular intervals or the use of cloud-based backup solutions. All of the other options are good, too, but the MOST important is a good backup copy of your company's data.

QUESTION 189
Joanne is having a drink at the coffee shop near her office. She takes out her Windows 10 laptop and connects it to the coffee shop's wireless network to check her email. Which type of network should she select to hide their computer from other devices on the network and prevent file sharing with other patrons of the coffee shop?

A. Home
B. Work
C. Public
D. Private

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1 .6: Joanne should select the public network type when connecting to this coffee shop's wireless network. The Network and Sharing Center in the Control Panel allows a technician to see information and modify the configuration settings of the network adapters in the workstation. The Network and Sharing Center is used to connect to a network using broadband, dial-up, or VPN connection, or add/remove file and printer sharing over the network on the workstation. When connecting to a network for the first time, the user must select if it is a public or private network. A public network will hide your computer from other devices on the network and prevent file and printer sharing. A private network is considered trusted, allows the computer to be

discoverable to other devices on the network, and supports the use of file and printer sharing. In older versions of Windows, there were also Home and Work network types, but those have since been merged into public and private network types, as well.

QUESTION 190
You are troubleshooting a network connectivity issue and need to determine the packet's flow path from your system to the remote server. Which of the following tools would best help you identify the path between the two systems?

A. netstat
B. tracert
C. nbtstat
D. lpconfig

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .2: The tracert (trace route) diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination. In these packets, tracert uses varying IP TimeTo- Live (TTL) values. When the TTL on a packet reaches zero (0), the router sends an ICMP "Time Exceeded" message back to the source computer. The ICMP "Time Exceeded" messages that intermediate routers send back show the route. The ipconfig tool displays all current TCP/IP network configuration values on a given system. The netstat tool is a command-line network utility that displays network connections for Transmission Control Protocol, routing tables, and some network interface and network protocol statistics on a single system. The nbtstat command is a diagnostic tool for NetBIOS over TCP/IP used to troubleshoot NetBIOS name resolution roblems.

QUESTION 191
You are working at the Dion Training headquarters in Puerto Rico. The island just suffered a power outage due to a hurricane. The server room in the headquarters has power, but the rest of the office does not. You verify that the diesel generator is running at full electrical load capacity. Which of the following solutions should you recommend to Dion Training to allow them to continue working during a long-term power outage?

A. Purchase a 1500VA battery backup for each workstation in the office
B. Migrate their servers to the cloud whenever a hurricane is approaching
C. Replace all the lightbulbs in the building with LEOs to reduce the electrical load
D. Increase the capacity of their backup generator to support a larger load

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.5: When a hurricane causes a power outage on an island, it can be hours, days, or even months before the power is fully restored. Since the Dian Training headquarters is located in Puerto Rico, they should have a large capacity diesel generator to power their entire office during a long-term power outage. After Hurricane Maria in 2017, some parts of Puerto Rico went without grid power for nine-month. We have multiple redundant and highcapacity power sources at the Dion Training offices to ensure we can remain online and work even without any grid power available.

QUESTION 192
Which of the following macOS features is the equivalent of the Taskbar in Windows?

A. Mission Control
B. Dock
C. Finder

D. BootCamp

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.1 0: Dock is a macOS feature for managing applications from the desktop that is similar to the Windows taskbar. A technician can change the way the dock behaves by right-clicking near the vertical line at the right of the dock. For example, they can configure the dock to autohide or position itself on another edge of the screen. Mission Control is an application for facilitating multiple desktops in the macOS environment. The Finder is the first tlhing that you see when your Mac finishes starting up. It opens automatically and stays open as you use other apps. It includes the Finder menu bar at the top of the screen and the desktop below that. It uses windows and icons to show you the contents of your Mac, iCioud Drive, and other storage devices. According to Apple, it is called the Finder because it helps you to find and organize your files. Boot Camp is used to allow dual booting on a Macintosh computer. It allows the user to boot into either macOS (OS X) or Windows as the computer is rebooted. Boot Camp is only supported on lntel-based macOS systems, though.

QUESTION 193
Samantha works in the human resource department in an open floorplan office. She is concerned about the possibility of someone conducting shoulder surfing to read sensitive information from employee files while accessing them on her computer. Which of the following physical security measures should she implement to protect against this threat?

A. Badge reader
B. Privacy screen
C. Biometric lock
D. Hardware token

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.1: A privacy screen is a fi lter placed on a monitor to decrease the viewing angle of a monitor. This prevents the monitor from being viewed from the side and can help prevent shoulder surfing. The standard type of antiglare filter consists of a coating~ that reduces the reflection from a glass or plastic surface. A biometric lock is any lock that can be activated by biometric features, such as a fingerprint, voiceprint, or retina scan. Biometric locks make it more difficult for someone to counterfeit the key used to open the lock or a user's account. A smart card is a form of hardware token. A smart card, chip card, or integrated circuit card is a physical, electronic authorization device used to control access to a resource. It is typically a plastic credit card-sized card with an embedded integrated circuit chip. In high-security environments, employee badges may contain a smart card embedded chip that must be inserted into a smart card reader to log in or access information on the system. A badge reader is used to read an employee's identification badge using a magnetic stripe, barcode, or embedded RFID chi .

QUESTION 194
Maria is trying to log in to her company's webmail and is asked to enter her username and password. Which type of authentication method is Maria using?

A. Multifactor
B. Single-factor
C. RADIUS
D. TACACS+

Correct Answer: B
Explanation

Explanation/Reference:

OBJ-2.2: Single-factor authentication (SFA) is a process for securing access to a given system, such as a network or website, that identifies the party requesting access through only one category of credentials (something you know, something you have, something you are, something you do, or somewhere you are). The most common example of single-factor authentication occurs when a user is prompted to enter their username and password to authenticate. Multifactor authentication requires credentials that include at least 2 of the 5 authentication factors. The Remote Authentication Dial-in User Service (RADIUS) is used to manage remote and wireless authentication infrastructure. Users supply authentication information to RADIUS client devices, such as wireless access points. The client device then passes the authentication data to an AAA (Authentication, Authorization, and Accounting) server that processes the request. The Terminal Access Controller Access Cont rol System (TACACS+) is a proprietary alternative to RADIUS developed by Cisco for handling authentication.

QUESTION 195
Which of the following commands is used on a Linux system to convert and copy files from one hard disk to another?

A. ls
B. mv
C. dd
D. Cd

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.1 1: The dd command is used to convert and copy files. On Unix and Unix-like operating systems like Linux, almost everything is treated as a file, even block devices like a hard disk drive. This makes dd useful to clone disks or wipe data from a drive. The mv command is a command-line utility that moves files or directories from one place to another. The mv command supports moving single files, multiple files, and directories. The mv command can prompt before overwriting files and will only mov,e files that are newer than the destination. When the mv command is used, the file is copied to the new directory and removed from the old directory. The ls command lists the files or directories in the current path of a Unix, Linux, or Mac operating system. When invoked without any arguments, ls lists the files in the current working directory. The cd command is used to change the directory. If used with the "cd .. "option, it will move up one directory in the file system's directory structure. If used with the "cd ."

QUESTION 196
Your Windows 10 workstation is currently running version 1909 and was flagged by the cybersecurity team as a threat to the network due to its outdated operating system. Which of the following actions should be performed to remediate this issue?

A. Disable the Windows Update service to prevent future issues
B. Use the Windows Update to install the latest OS version
C. Rollback any system updates or changes
D. Enable System Restore in Windows

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.1: Windows Update hosts critical updates and security patches (code to fix security vulnerabilities in Windows and its associated software) plus optional software and hardware updates to add or change features or drivers. There is also a complementary program, called Microsoft Update, which can be used to keep Microsoft Office software patched at the same time. If you are working on a small network, you will likely use Windows Update to keep your systems patched and secure. If you work for a large organization, you will likely use the Microsoft Endpoint Configuration Manager (MECM) to conduct patch management across all your devices, instead.

QUESTION 197
A cybersecurity analyst is applying for a new job with a penetration testing firm. He received the job application as a secured Adobe PDF file, but unfortunately, the firm locked the file with a password so the potential employee could not fill in the application. Instead of asking for an unlocked copy of the document, the analyst decides to write a script in Python to attempt to unlock the PDF file by using passwords from a list of commonly used passwords until he can find the correct password or attempts every password in his list. Based on this description, what kind of cryptographic attack did the analyst perform?

A. Brute-force attack
B. Session hijacking
C. Dictionary attack
D. On-path attack

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.4: A dictionary attack is a technique for defeating a cipher or authentication mechanism by trying to determine its decryption key or passphrase by trying hundreds or sometimes millions of likely possibil ities, such as words in a dictionary. The key to answering this question is that they were using passwords from a list. A brute-force attack consists of an attacker submitting many passwords or passphrases with the hope of eventually guessing correctly. A session hijacking attack compromises the session token by stealing or predicting a valid session token to gain unauthorized access to the webserver. An on-path attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are d irectly communicating witth each other.

QUESTION 198
Which of the following file types are commonly used by scripts in a Linux command line environment?

A. sh
B. ps1
C. vbs
D. js

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.8: A shell script is a file that contains a list of commands to be read and executed by the shell in Linux and macOS. A .sh file is used for a shell script and its first line always begins with #!/bin/bash that designates the interpreter. This line instructs the operating system to execute the script. Shell scripts allow you to perform various functions. These functions include automation of commands and tasks of system administration and troubleshooting, creating simple applications, and manipulating text or files. VBScript is a scripting language based on Microsoft's Visual Basic programming language. Network administrators often use VBScript to perform repetitive administrative tasks. With VBScript, you can run your scripts from either the command-line or the Windows graphical interface. Scripts that you write must be run within a host environment. Windows 10 provides Internet Explorer, I iS, and Windows Script Host (WSH) for this purpose. Windows PowerShell enables you to perform management and administrative tasks in Windows 7 and later. It is fully integrated with the operating system and supports both remote execution and scripting. Microsoft provides the Windows PowerShell Integrated Scripting Environment (ISE) to help create and manage your Windows PowerShell scripts. If you want to save a series of PowerShell commands in a file to rerun them later, you effectively create a PowerShell script by creating a text file with a .ps1 extension. The file can contain a series of PowerShell commands, with each command appearing on a separate line. JavaScript is a scripting language that is designed to create interactive web-based content and web apps. The scripts are executed automatically by placing the script in the HTML code for a web page so that when the HTML code for the page loads, the script is run. JavaScript is stored in a .js file or as part of an HTML file.

QUESTION 199
A customer runs frantically into your computer repair store. He says that his smartphone fell into a puddle, and now it won't turn on. He excitedly t ells you that he needs the smartphone working again "right now" and cannot wait. What should you do?

A. Tell the customer to calm down because it is just a phone
B. Explain to the customer that the repairs may take several days
C. Post about the experience on Facebook after the customer leaves
D. Offer the customer the option to replace his phone

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.7: In this case, you should offer the customer the option to replace his phone. It is important to set and meet expectations and timelines when dealing with a customer. If you cannot meet the timeline needed, you should offer different repair/replacement options (if applicable). The other options violate the principles of good customer service: (1) Do not argue with customers and/or become defensive; (2) Avoid dismissing customer problems; (3) Avoid being judgmental; (4) Clarify customer statements (ask open-ended questions to narrow the problem's scope, restate the issue, or question to verity understanding); and (5) Do not disclose experiences via social media outlets.

QUESTION 200
You are working as a military defense contractor a1nd have been asked to dispose of 5 laptop hard drives used in systems that processed classified information. Which of the following physical data destruction and disposal methods is MOST appropriate to ensure the data cannot be recovered?

A. Degaussing of the HODs
B. Low-level formatting of the HODs
C. Standard formatting of the HODs
D. Drill/hammer the HOD platters

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.8: The best option is to use degaussing on the hard drives. Degaussing exposes the disk to a powerful electromagnet that disrupts the magnetic pattern that stores the data on the disk surface. This renders the data on the disk inaccessible, but the disk will become unusable for other purposes. If the drive needs to be reused, repurposed, or recycled, you should not use degaussing. If the drive contains sensitive or classified information, then it should be degaussed or shredded. Standard formatting of the drives could allow the data to be restored and make the data vulnerable to exposure. Low-level formatting is a hard disk operation that will make recovering data from your storage devices difficult once the operation is complete.

QUESTION 201
You are working as part of a penetration testing team during an assessment of Dion Training's headquarters. Your boss has requested that you search the company's recycling bins for any information that might be valuable during the reconnaissance phase of your attack. What type of social engineering method are you performing?

A. Dumpster diving
B. Whaling
C. Phishing
D. Impersonation

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.4: Dumpster diving involves searching through publicly accessible garbage cans or recycling bins to find discarded paper, manuals, or ot her valuable types of information from a targeted company. This is often done as part of the reconnaissance phase before an attack is performed. Whaling is an email-based or web-based form of phishing that targets senior executives or wealthy individuals. Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Impersonation is the act of pretending to be someone or something else. Malicious actors often couple pretexting and impersonation to craft a believable scenario and impersonate people in authority during a social engineering attack.

QUESTION 202
Which of the following data types would be used to store the value of TRUE?

A. Boolean
B. Integers
C. Floating point
D. String

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.8: A boolean stores a value of TRUE (1) or FALSE (0). It usually consumes only 1 bit of storage (a zero or a one). An integer stores a whole number, such as 21, 143, or 1024. An integer data type usually consumes 8 bytes of storage. A floating-point number stores a fractional or decimal number, such as 3.14, 45.5, or 333.33. A floating-point number data type usually consumes 4 to 8 bytes of storage. A string stores a group of characters, such as Hello, PYTHON, or JasonDion. A string data type usually consumes as much storage as necessary. Each character in the string usually requires 1 byte of storage.

QUESTION 203
Jason wants to configure his Windows 10 workstation to automatically block pop-ups when searching for websites online. Which of the following Control Panel sections should he use to achieve this?

A. Internet Options
B. Indexing Options
C. Power Options
D. File Explorer Options

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.4: The Internet Options section of the Control Panel allows a technician to manage the Internet settings for their computers, including the security settings, access settings, and add-on control settings. Using Internet Options, a technician can set the homepage of the browser, set up the proxy server connection details, and change the trust and security settings used by the system. The Indexing Options is used to configure the method used by Windows when searching for content within the storage devices. When indexing is properly configured, the system will catalog the information on the computer using the words within the files and their met adata to more easily find the content when requested by a user. The Power Options section of the Control Panel allows technicians to customize how a computer manages its power to either conserve energy at the expense of performance or to maximize performance at the expense of energy savings by creating a power plan. The File Explorer Options section of the Control Panel allows technicians to customize the display of files and folders. For example, the File Explorer Options can enable or disable the ability to show hidden files, hide file extensions, and more.

QUESTION 204
Which of the following IP addresses is considered an APIPA address?

A. 1 0.5.34.15
B. 172.16.13.12
C. 169.254.125.154
D. 192.168.2.14

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.6: Private IP addresses are any addresses in a specified range that are not allowed to be routed over the Internet. This allows companies to use these private IP addresses in their local area networks without having to purchase them from an internet registry. The class A private IP address range contains the addresses from 10.0.0.0 to 10.255.255.255.255. The class B private IP address range contains the addresses from 172.16.0.0 to 172.31.255.255. The class C private IP address range contains the addresses from 192.168.0.0 to 192.168.255.255. The APIPA/link-local autoconfiguration range is from 169.254.0.0 to 169.254.255.255.

QUESTION 205
A customer is complaining that there is are intermittent problems with their PC. As a technician, you don't know exactly what the errors are, so which tool should you use to determine what errors have previously occurred?

A. Device Manager
B. Event Viewer
C. System Information
D. Performance Monitor

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.3: You should use the Event Viewer to read the log entries within Windows to determine what errors have occurred in the past. Logs are a treasure trove of information on any workstation or server. The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a usefu l tool for troubleshooting all kinds of different Windows problems. If you use the Event Viewer, you can identify what was occurring at or around 2:35am each day before t he server crashed and use this to troubleshoot the problem. Performance monitor (perfmon.msc) is a performance monitoring and system monitoring utility in Windows that is used to monitor the activities on CPU and memory activity on a computer. The performance monitor is used to view performance data either in real-time or from a log file. The performance monitor can only monitor the resource utilization, but it cannot manage or terminate those processes. System information (msinfo32.exe) is a utility that gathers information about your computer and displays a comprehensive list of hardware, system components, and the software environment that can be used to diagnose computer issues. Device manager (devmgmt.msc) is a utility used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it.

QUESTION 206
Which of the following tools is used to duplicate all of the files in one directory to another in the Windows command line?

A. dir
B. format
C. xcopy

D. Netstat

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.2: The xcopy tool copies all of the f iles from one directory to another. The format command creates a new root directory and file system for the disk. It can check for bad areas on the disk, and it can delete all data on the disk. To use a new disk, you must first use the format command to format the disk. The dir command is used to list a directory's files and subdirectories. If used without parameters, this command displa1ys the disk's volume label and serial number, followed by a list of directories and files on the disk (including their names and the date and time each was last modified). The netstat command is used to display active TCP connections, ports on which the computer is listening, Ethernet statistics, the IP routing table, 1Pv4 statistics, and 1Pv6 statistics on a Windows machine.

QUESTION 207
Chris just downloaded a new third-party email client for his smartphone. When Chris attempts to log in to his email with his username and password, the email client generates an error messaging stating that "Invalid credentials" were entered. Chris assumes he must have forgotten his password, so he resets his email username and password and then reenters them into the email client. Again, Chris receives an "Invalid credentials" error. What is MOST likely causing the "Invalid credentials" error regarding Chris's email client?

A. His email account requires a strong password to be used
B. His email account is locked out
C. His smartphone has full device encryption enabled
D. His email account requires multi-factor authentication

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.7: If a user or system has configured their email accounts to require two-factor authentication (2FA) or multifactor authentication, then even if they enter their username and password correctly in the third- party email client, they will receive the "Invalid credentials" error message. Some email servers will allow the user to create an application-specific password to bypass the multifactor authentication requirement to overcome this. llf not, then the user will have to use an email client that supports multifactor authentication. His email account is not locked out or requiring a stronger password, otherwise, those issues would have been solved when he reset the password. Full device encryption on the smartphone would not affect the use of the email client since the device is unencrypted once a user enters their PIN, password, TouchiD, or FaceiD as authentication.

QUESTION 208
Whkh file system type is used to mount remote storage devices on a Linux system?

A. NTFS
B. exFAT
C. NFS
D. APFS

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.8: The Network File System (NFS) is used to mount remote storage devices into the local file system on a Linux system. It allows you to mount your local file systems over a network and remote hosts to interact with them while mounted locally on the same system. The extensible file allocation table (exFAT) is a file system optimized for external flash memory storage devices such as USB flash drives and SD cards. exFAT supports a maximum volume size of up to 128 PB with a recommended maximum volume size of 512 TB for the best

reliability. The Apple file system (APFS) is the default file system for Mac computers using macOS 10.13 or later and features strong encryption, space sharing, snapshots, fast directory sizing, and improved file system fundamentals. The NT file system (NTFS) is a Windows file system that supports a 64-bit address space and can provide extra features such as file-by-file compression and RAID support as well as advanced file attribute management tools, encryption, and disk quotas. NTFS can support a maximum volume size of up to 8 PB.

QUESTION 209
Gina just installed a 4 TB HOD into her Windows 10 computer and wants to assign the drive letter "M" to store her media files. Which type of partition should Gina use if she wants to mount the drive as a single partition?

A. GPT
B. FAT32
C. ISO
D. MBR

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.1: GPT is a newer way to partition disks that allows partition sizes over the 2 TB limit imposed by MBR. The GUID partition table (GPT) is a modern disk partitioning system allowing large numbers of partitions and very large partition sizes. The GPT is used in modern computers that support the UEFI standard and can support a maximum capacity of up to 9.7 ZB and up to 128 partitions. The master boot record (MBR) is a sector on a hard disk storing information about partitions configured on the disk. The MBR holds the information on how the logical partitions that contain the file systems are organized on the physical disk. Systems that rely on BIOS utilize the MBR to determine which partitions are on a given hard disk. MBR partition tables have a maximum capacity of 2 TB and only 4 separation partitions. An optical disc image (ISO) file is a file that contains all of the contents from an optical disc in a single file which can be mounted to the file system as though it were a physical optical drive. An ISO is a disk image that contains everything that would be written to an optical disc, disk sector by disc sector, including t he optical disc file system. The file allocation table 32-bit (FAT32) is the 32-bit file system supported by Windows, macOS, and Linux computers. FAT32 can support maximum volume sizes of up to 2 TB and maximum file sizes of up to 4 GB.

QUESTION 210
Which command-line tool is used on a Linux system to display a list of the files and directories within the current path?

A. chkdsk
B. sfc
C. ls
D. Pwd

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.1 1: The Is command lists the files or directories in the current path on a Linux system. When invoked without any arguments, Is lists the files in the current working directory. The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen. The chkdsk command is used to check the file system and file system metadata of a volume for logical and physical errors. The system file checker (SFC) command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from the command line.

QUESTION 211
A laptop is running Windows 10 with Windows Defender on it. A user believes their laptop may have become infected with malware, so they install a second antivirus program that supposedly includes realtime protection.

Now, the laptop is sluggish and sometimes non-responsive. Which of the following should you do FIRST to resolve this problem?

A. Enable real-time protection in Windows Defender
B. Install and run Spybot Search & Destroy on the laptop
C. Run the Windows Update utility
D. Uninstall the real-time protection antivirus

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.2: You should not have two antivirus or antimalware solutions running simultaneously on a single computer. Since the issues began for the user when they installed t he real -time protection scanner, it should be uninstalled FIRST. Then, you could enable real-time protection in Windows Defender to provide this functionality. While you can have two antivirus and antimalware solutions installed, you should only have one set up for real time protection at a time. The other could be used to scan the computer during the bootup process if desired. Windows Defender, by default, already has real -time protection enabled. This is why the installation of the second real-time protection service was causing issues on this laptop.

QUESTION 212
Which of the following security controls provides Windows system administrators with an efficient way to deploy system configuration settings across many devices?

A. Patch management
B. HIPS
C. Anti-malware
D. GPO

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.1: Microsoft's Group Policy Object (GPO) is a collection of Group Policy settings that defines what a system will look like and how it will behave for a defined group of users. A Group Policy is the pri'mary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, Group Policy is applied to users or computers based on their membership in sites, domains, or organizational units. A host-based intrusion detection system (HIDS) is a device or software application that monitors a system for malicious activity or policy violations. Any malicious activity or violation is typically reported to an administrator or collected centrally using a security information and event management system. Anti-malware software is a program that scans a device or network for known viruses, Trojans, worms, and other malicious software. Patch management is the process of distributing and applying updates to the software to prevent vulnerabilities from being exploited by an attacker or malware. Proper patch management is a technical control that would prevent future outbreaks.

QUESTION 213
Which of the following tools should a technician use to modify the HOSTS file on a Windows 10 system to solve a website address resolution issue?

A. Reg edit
B. MMC
C. Services
D. Notepad

Correct Answer: D

Explanation

Explanation/Reference:
OBJ-3.2: Browser redirection usually occurs if the browser's proxy is modified or the hosts.ini file is modified. If the redirection occurs only for a smal l number of sites or occurs in all web browsers on a system, it is most likely a maliciously modified hosts.ini file. The hosts.ini file is a local text file that allows a user to specify specific domain names to map to particular addresses. It can be edited using any basic text editor, such as notepad. It works as an elementary DNS server and can redirect a system's internet connection. For example, if your children are overusing YouTube, you can change YouTube.com to resolve to YourSchool.edu for just your child's laptop. The Microsoft management console (MMC) is a utility that uses snap-ins for various Windows tools such as disk management, computer management, performance monitor, print management, and others to perform operations on a local or networked computer. The task manager is an advanced Windows tool that has 7 tabs that are used to monitor the Processes, Performance, App History, Startup, Users, Details, and Services on a computer. By clicking the Services tab, the technician can list all of the services installed on the computer, display their status, and start/stop/restart those services. The registry editor (Reg Edit) allows you to view and make changes to system files and programs that you wouldn't be able to access otherwise. The registry is a database made up of hives and keys that control various settings on a Windows system. ly editing the Registry can permanently damage your computer, so it is important to be very careful when modifying the registry using Re Edit.

QUESTION 214
Which of the following encryption types was used by WPA to better secure wireless networks than WEP?

A. CCMP
B. TKIP
C. AES
D. IV

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.2: Wi-Fi protected access (WPA) is an improved encryption scheme for protecting Wi-Fi communications designed to replace WEP. WPA uses the RC4 cipher and a temporal key integrity protocol (TKIP) to overcome the vulnerabilities in the older WEP protection scheme. Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks that can break its encryption. WEP relies on the use of a 24-bit initialization vector to secure its preshared key. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authent ication protocol (CCMP) for enc tion.

QUESTION 215
Jason has built a custom Android application that he wants to install on an Android tablet without having to install it through the Play Store. Which of the following would be required to allow him to install the app's APK on the device?

A. Jailbroken device
B. Developer mode
C. Rooted device
D. Sideloading

Correct Answer: D
Explanation

Explanation/Reference:

OBJ-3.5: An android application package (APK) is a third-party or custom program that is installed directly on an Android device to give users and business the flexibility to install apps directly on Android devices. Android supports sideloading through the APK package format. An APK file contains all of that program's code, including .dex files, resources, assets, certificates, and manifest files. Jailbreaking is conducted on an iOS device to remove manufacturer restrictions on the device and allow other software, o perating systems, or networks to work with a device. A rooted device is an Android device that has been hacked t o provide the user with administrative rights to install unapproved apps, update OS, delete unwanted apps, underclock or overclock the processor, replace f irmware and customize anythirng else. A rooted device is not required just to install an APK outside of the Play StoreJ though, on an Android device. Devleoper mode is used on an Android device to show additional diagnostic information when using apps or making network connections.

QUESTION 216
A file currently has permissions of 755. Which of the following commands would change file permission to r-xr--r--?

A. chmod r-wr--r-- filename
B. chmod 544 filename
C. chmod u-rx,go-r filename
D. chmod u+w,go+x filename

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .1 1: The chmod command is used to change a file or directory's permissions from the command line or terminal. A technician can either use u+ to add user permission and g+ to add group permissions, or they can use the octal value. In this case, the octal value of r-wr--r-- is 544. In Linux, you can convert letter permissions to octal by giving 4 for each R, 2 for each W, and 1 for each X. R is for read-only, W is for write, and X is for execute. The permissions strings are written to represent the owner's permissions, the group's permissions, and the other user's permissions.

QUESTION 217
A developer uses a MacBook Pro when working from home, but they need access to both a Windows and macOS system to test their programs. Which of the following tools should be used to allow both operating systems to exist on their MacBook Pro?

A. Device Manager
B. Boot Camp
C. Mission Control
D. Terminal

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.1 0: Boot Camp is used to allow dual booting on a Macintosh computer. It allows the user to boot into either macOS (OS X) or Windows as the computer is rebooted. Boot Camp is only supported on Intel- based macOS systems, though. The terminal in macOS is the equivalent to the Windows Command Prompt window. The terminal is used to run network troubleshooting utilities such as the ping command and other advanced commands to modify the macOS environment. Mission Control is an application for facilit ating multiple desktops in the macOS environment. The Device Manager is used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it.

QUESTION 218
An employee's inbox is now f illed with unwanted emails after their email password had been compromised last week. You helped them reset their password and regain access to their account. Many of the emails are

coming from different email addresses ending in spamyou.com. Which of the following actions should you take to help reduce the amount of spam this and other users in your organization are receiving?

A. Create a domain-based email filter
B. Click the unsubscribe button of each email
C. Establish an allow list of trusted senders
D. Mark each email as spam or junk

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.2: Email filtering is any technique used to prevent a user from being overwhelmed with spam or junk email. By creating a domain-based email filter, all emails from the spamyou.com domain could be blocked and prevented from being delivered to the user. Spam can be blocked from reaching an organization using a mail gateway to fi lter messages. At the user level, the software can redirect spam to a junk folder or similar. Anti-spam filtering needs to balance blocking illegitimate traffic with permitting legitimate messages. Anti -spam techniques can also use lists of known spam servers by establishing a blacklist If an allow list is used, only a small number of senders could send emails to the user.

QUESTION 219
A workstation at Dion Training's office is taking a long time to boot up. Once it finishes booting to the Windows 10 desktop, which of the following tools can a technician use to diagnose and fix the boot issues?

A. msinfo32.exe
B. resmon.exe
C. msconfig.exe
D. perfmon.msc

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.3: System configuration (msconfig.exe) is a system utility to t roubleshoot the Microsoft Windows startup processes. MSConfig is used to disable or re-enable software, device drivers, and Windows services that run at startup, or to change boot parameters. PerfMon is a performance monitoring and system monitoring ut ility in Windows that is used to monitor the activities on CPU and memory activity on a computer. Performance monitor is used for viewing performance data either in real-time or from a log file. The performance monitor can only moniitor the resource utilization, but it cannot manage or terminate those processes. Resource monitor is a utility used to display information about the use of hardware (CPU, memo ry, disk, and network) and software (file handles and modules) resources in real-time. The resource monitor helps check the performance counters of specif ic resources and decide a course of action to improve the performance. System information (msinfo32.exe) is a utility that gathers information about your computer and displays a comprehensive list of hardware, system components, and t he software environment that can be used to diagnose computer issues.

QUESTION 220
Karen, a salesperson in your company, is currently on travel this week. She calls your company's help desk and is yelling because she cannot connect to her email using her hotel room's WiFi. Her laptop shows that it is connected to the "HoteiWiFi" network, but Windows states it has "Limited or no connectivity." What action should Karen perform to fix this issue?

A. Disable and enable her wireless adapter
B. Purchase an ethernet cable and use her room's wired connection
C. Open a web browser and agree to the hotel's capture page AUP
D. Reboot into Safe Mode and perform an antivirus scan

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.5: The "Limited or no connect ivity" message appears when a computer detects that the wireless network is present and operating, but the system cannot connect to the Internet. This is a common occurrence when connecting to a hotel or other public wireless networks. Many of these networks have a capture page that requires the user to agree to the company's privacy policy or acceptable use policy before connecting the device to the internet. If the capture page doesn't appear aut omatically, the user should open their web browser and visit any website to force the page to load.

QUESTION 221
Which of the following options in Windows 10 would create a small hibernation file saved on the storage device before shutting down the computer so that it reduces the time to boot up when powered on?

A. Sleep mode
B. Fast startup
C. USB selective suspend
D. Lock mode

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.4: Fast startup is a mode in between a full shutdown and a hibernation mode. With a fast startup, the computer will log out of the computer close all of its open files when being shut down. Before the system powers off, though, a small hibernation file is created to help speed up the bootup process when the computer is powered on again. The USB selective suspend feature allows the hub driver to suspend an individual port without affecting the operation of the other ports on the hub. Selective suspension of USB devices is helpful when using a laptop computer as it helps to conserve battery power by powering off USB ports that are not needed at the time. Sleep or standby mode is used to save the current session to memory and put the computer into a minimal power state to save battery life when the system is not being used. The computer takes less time to start up again from the sleep or standby mode than it does from the hibernate mode. A lock will secure the desktop with a password while leaving programs running.

QUESTION 222
Which of the following types of encryption uses a 128-bit encryption key but is considered weak due to its use of a 24-bit init ialization vector?

A. WEP
B. WPA2
C. WPA
D. WPS

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.2: Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks t hat can break its encryption. WEP relies on the use of a 24- bit initialization vector to secure its preshared key. Wi- Fi protected access (WPA) is an improved encryption scheme for protecting Wi-Fi communications designed to replace WEP. WPA uses the RC4 cipher and a temporal key integrity protocol (TKIP) to overcome the vulnerabilities in the older WEP protection scheme. Wi- Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is st ill available forr home and small office networks.

WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption. The Wi- Fi Protected Setup (WPS) is a mechanism for auto-configuring a WLAN securely for home users. On compatible equipment, users push a button on the access point and connect adapters to associate them securely. WPS is subject to brute force attacks against the PIN used to secure them, making them vulnerable to attack.

QUESTION 223
Your boss from work just sent you an important email, but you are not in the office. You tried to open the email from your smartphone, but it is encrypted and won't open. What should you do?

A. Open the email using your device's web browser and your corporate webmail
B. Ask your boss to resend the email to your Gmail account instead
C. Verify the digital certificate is installed on the device
D. Ask your boss to resend the email in an unencrypted format

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.5: If an encrypted email does not open in your mail app, you most likely need to verify that your digital certificates are properly installed on the device as these are used to decrypt encrypted emails. If the email was sent to your Gmail account, it would be sent unencrypted. You should not ask for the email to be sent unencrypted since it removes the confidentiality and privacy of the email. Regardless of whether you are using the email client or the mobile web browser, if the digital certificate is not properly installed then the encrypted email will not be able to be read.

QUESTION 224
Which of the following backup rotation schemes requires backups to be stored to at least two different types of media?

A. FIFO Ba1ckup
B. Grandfather-father-son
C. 3-2-1 backup
D. Tower of Hanoi

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.3: The 3-2-1 backup rule states that an organization should create (3) one primary backup and two copies of the data, (2) save the backups to two different types of media, and (1) keep at least one backup copy off-site. The grandfather-father-son (GFS) backup rotation scheme is widely used to combine full and incremental backups to reduce backup time and enhance storage security. The grandfather is a full backup that is stored offsite once per month. The father is a weekly full backup that is conducted. The son is an incremental or differential backup conducted each day. For example, each Monday a fu ll backup can be conducted which becomes the father. Then, each day of the week a son is created by performing an incremental or differential backup. Once per month, a full backup is conducted to become t he grandfather. The Tower of Hanoi is a backup rotation scheme that rotates backup media sets throughout the backup process to minimize wear and failure of tape backup media. For example, when using this method with fou r backup tapes labeled A, B, C, and D, a total of 16 days of backups can be maintained with just 4 tapes. Tape A is used every odd-numbered day for 16 days. Tape B is used on days 2, 6, 10, arnd 14. Tape Cis used on days 4 and 12. TapeD is used on days 8 and 16. This allows Tape A to be overwritten every other day, while Tapes B is overwritten every four days and Tapes C and Dare overwritten every 8 days. The First In First Out (FIFO) backup scheme uses a set number of tapes and overwrites the oldest tape with the newest information. For example, if there are 7 tapes in use, every evening a new backup is conducted over the previous week's daily backup. To have a longer amount of days of backups, a technician simply needs to increase the number of tapes from 7 to 14 or 21.

QUESTION 225
You are working as a mobile device technician for a large corporation's enterprise service desk. A user complains that every time they attempt to launch the company's mobile email application, it crashes and displays an error message of Code123. This is the third user with this error on an Android (model DTA) smartphone. The same app is working on your smartphone, but it is a model DTX. Which of the following should you do FIRST to attempt to solve this problem?

A. Rollback the app to an earlier version
B. Clear the app's cache
C. Update the smartphone's OS
D. Reinstall the email app

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.4: Normally, your first step would be to uninstall and reinstall the application. But, since this issue is occurring on multiple devices with the same model, it would be a better first step to update the smartphone's OS. Based on the scenario, you know that the app works on a different smartphone model. With Android devices, the OS is usually modified by the smartphone manufacturer, specifically for their devices. If the app doesn't work on one model, but it does on another, it may be an operating system issue.

QUESTION 226
You are troubleshooting a network printer when a document is printed with sensitive employee data on it. Which of the following actions should you take?

A. Leave the document in the output tray
B. Remove the document and shred it
C. Continue to troubleshoot the printer
D. Take the document to the office manager

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.7: The document contains sensitive employee information; therefore, you should not leave it on the printer. Instead, it would be best if you took it to the office manager so they can deliver it to the owner or they can securely dispose of it.

QUESTION 227
Which of the following is the LEAST secure wireless security and encryption protocol?

A. WEP
B. WPA2
C. WPA3
D. WPA

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.2: Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks that can break its encryption. WEP relies on the use of a 24- bit initialization vector to secure its preshared key. Wi-Fi protected access (WPA) is an improved encryption scheme for protecting Wi-Fi communications that was designed to replace WEP. WPA uses the

RC4 cipher and a temporal key integrity protocol (TKIP) to overcome the vulnerabilities in the older WEP protection scheme. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the complet ion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption. Wi- Fi protected access version 3 (WPA3) has replaced WPA2 as the most secure wireless encryption method. WPA3 uses the simultaneous authentication of equals (SAE) to increase the security of preshared keys. WPA3 provides the enhanced open mode that encrypts transmissions from a client to the access point when using an open network. WPA3 Enterprise mode supports the use of AES with the Galois/counter mode protocol (GCMP-256) for the highest lev,els of encryption.

QUESTION 228
Your company has just finished replacing all of its computers with brand new workstations. Colleen, one of your coworkers, has asked the company's owner if she can have the old computers that are about to be thrown away. Colleen would like to refurbish the old computers by reinstalling a new operating system and donating them to a local community center for disadvantaged children in the neighborhood. The owner thinks this is a great idea but is concerned that the private and sensitive corporate data on the old computer's hard drives might be placed at risk of exposure. You have been asked to choose the best solution to sanitize or destroy the data while ensuring the computers w'ill still be usable by the community center. What type of data destruction or sanitization method do you recommend?

A. Shredding
B. Wiping
C. Purging
D. Degaussing

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.8: Data wiping or clearing occurs by using a software tool to overwrite the data on a hard drive to destroy all electronic data on a hard disk or other media. Data wiping may be performed with a 1x, 7x, or 35x overwriting, with a higher number of times being more secure. This allows the hard drive to remain functional and allows for hardware reuse. Degaussing a hard drive involves demagnetizing a hard drive to erase its stored data. You cannot reuse a hard drive once it has been degaussed. Therefore, it is a bad solution for this scenario. Purging involves removing sensitive data from a hard drive using the device's internal electronics or an out side source such as a degausser, or by using a cryptographic erase function if the drive supports one. Shredding involves the physical dest ruction of the hard drive. This is a secure method of destruction but doesn't allow for device reuse.

QUESTION 229
What is the FIRST step of the seven-step malware removal process?

A. Update the applications and the operating system
B. Quarantine the infected system
C. Enable System Restore and create a restore point in Windows
D. Investigate and verify malware symptoms

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.3: The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 230
What is the FIFTH step of the seven-step malware removal process?

A. Schedule scans and run updates
B. Remediate the infected systems
C. Investigate and verify malware symptoms
D. Enable System Restore and create a restore point in Windows

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.3: The seven steps of the malware removal procedures are 0) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 231
Your smartphone's battery has been draining quickly. You have looked at the applications that are causing the drain and notice that a free game runs in the background, collecting GPS data even when you aren't using it. Which of the followi1ng threats is this an example of?

A. Unauthorized microphone activation
B. Unintended Bluetooth pairing
C. Unauthorized account access
D. Unauthorized location tracking

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.4: While location-based data can be valuable when using maps and trying to find sites, it can also give away sensitive information if accessed by someone who should not have it. You can optimize your battery life and protect yourself by turning off Locat ion Services. On an iPhone, turn it off in Settings > Privacy > Location Services. There you will see each app listed along with its permission setting. Apps that recently used location services have an indicator next to the on/off switch, and you can configure them accordingly. Unauthorized account access can give users access to personal files and data they should not have access to. Therefore, you should closely monitor your account usage. When files are accessed without authorization from your cloud storage service, it can lead to the leaking of your personal files and data. The microphone can be activated remotely and allow a troublemaker to spy on you. It is suggested that, when not in authorized use, you cover the microphone of your device to keep them from providing any data if remotely accessed. When anonymous devices are allowed to connect to Bluetooth-enabled devices, this is known as unintended Bluetooth pairing, and it represents a security threat. Mobile security policies should be created and enforced that prevent this from occurnn .

QUESTION 232
Malware infected Natalie's iMac. The malware has deleted numerous files from the system and corrupted the operating system. Natalie needs to access some of her files from the computer that have been deleted by the malware. Which of the following built-in utilities could restore access to those files?

A. System Restore
B. Snapshot
C. Time Machine
D. Keychain

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.1 0: Time Machine is the built-in backup feature of the macOS operating system. Time Machine aut omatically backs up all of the system's files, including apps, music, photos, email, documents, and system files. Once a user has a valid backup in Time Machine, they can restore files from the backup if the original files are ever corrupted or deleted on their Mac or if the hard disk (or SSD) is erased or replaced. A snapshot is used to backup virtual machines by creating a state of the disk at a particular point in time. Snapshots allow a technician to roll back any changes made to a VM during a session if needed. System restore is a Windows feature that creates configuration backups of the operating system. If there are any changes or file corruptions that damage the information in the registry or if the technician needs to reverse changes made when t hey installed an application or device driver, then System restore can be used to reset the configuration to an earlier point in time. Keychain is a macOS app for managing passwords cached by the OS and supported browser/web applications.

QUESTION 233
You are working as a defense contractor for the U.S. Army. The Army is looking to purchase Microsoft Office for all of its employees to use. Which of the following licenses would be BEST for this sized organization to purchase?

A. Enterprise
B. Personal
C. Business
D. Open-source

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.6: An enterprise license is like a business license, but for an unlimited number of users and is designed for large corporate and government networks. A business license is the standard licensing option for organizations and business entities. With Microsoft, a company can purchase anywhere from 1 to 300 user licenses under the business license program. A Personal license is an option for private individuals who purchase a license with their own funds and solely for their own use. Personal licenses are not to be purchased, refunded, or in any way financed by companies. Open source is software that also makes the program code used to design it available. Generally, open-source software is free to use and distribute, but you may need to pay for ongoing support if you have technical issues. The idea is that other programmers can investigate the program and make it more stable and useful. An open-source license does not forbid commercial use of applications derived from the original, but it is likely to impose the same conditions on further redistributions.

QUESTION 234
Dion Training wants to upgrade its employees' workstations from Windows 10 to Windows 11. All of the employees' data and files are saved to the company's shared drive. The technician has been told to choose an installation type that will delete all of the existing data, settings, and applications on the workstations during the upgrade. Which of the following types of upgrades or installlations should you perform on the workstations?

A. Refresh installation
B. Repair installation
C. In-place upgrade
D. Clean install

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.9: A clean install is an installation of the new operating system on a new computer or a computer that has been recently formatted. A clean install will completely replace the operating system software on the computer with the new operating system. During a clean install, all of the user's data, settings, and applications will be deleted. An in-place upgrade is an installation of the new operating system on top of an existing version of the operating system. An in-place upgrade will preserve the applications, user settings, and data files that already exist on the computer. A refresh installation is a type of installation that will recopy the system files and revert most system settings to their default configuration while preserving user personalization :sett ings, data files, and applications installed through the Windows Store. Repair installation is a type of installation that attempts to replace the existing version of the operating system files with a new copy of the same version. A repair installation is useful when trying to repair a Windows computer that will not boot or whern you believe the system files have become corrupted since it will keep all of the existing user data, settings, and applications during the re a1r.

QUESTION 235
When Jonathan opens the web browser on his computer, the initial page loads up to a search engine that he does not recognize. Jonathan attempts to use the search engine, but the results are abysmal, and the browser creates numerous pop-ups. Jonathan asks for your assistance in fixing this issue. Which TWO of the following actions do you recommend Jonathan perform first?

A. Reset the web browser to the default settings and configuration
B. Tell Jonathan to switch to a different web browser
C. Reboot Jonathan's computer and install a second anti-virus program
D. Uncheck any unapproved applications from the Startup tab in the Task Manager
E. Delete the web browser's cache, temporary files, and cookies
F. Update Jonathan's web browser to the latest version

Correct Answer: AD
Explanation

Explanation/Reference:
OBJ-3.2: Browser redirection and pop-ups are common symptoms of malware being installed on a computer. It is recommended that the web browser be reset to its default settings and configurations to remove any redirection settings that the malware may have made to the browser. Additionally, any unapproved applications should be unchecked from the Startup tab in Task Manager to ensure the malware isn't reloaded during the next reboot.

QUESTION 236
Which of the following types of screen locks uses a biometric authentication mechanism that relies upon mapping the geography of a user's eyes, nose, mouth, and other features before granting access to a mobile device?

A. Passcode
B. Swipe
C. TouchiD
D. FaceiD

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.7: Apple developed FaceiD as a facial recognition biometric authentication system. It creates a map of a user's face using an infrared image. This also accounts for changes in a user's appearance, such as wearing sunglasses, makeup, or even changes in the lighting of the environment. With over 30,000 individual, invisible dots that create the mapping of the user's face, the FaceiD system is extremely secure. Based on tests, it has a false positive rate of less than 1 in 1 million attempts. Touch ID is an electronic fingerprint recognition feature

designed and released by Apple. A swipe lock is a term for unlocking a device by tracing a predetermined onscreen pattern or joining dots on the screen. This was commonly used in Android devices until biometric methods like fingerprint scanners and facial recognition became more prevalent. A passcode unlock is a term for unlocking a device by entering a 4 to 6 digit pin.

QUESTION 237
Which command would a Linux user need to enter to change their password?

A. pwd
B. passwd
C. ps
D. Chown

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.1 1: The passwd command changes passwords for user accounts. A normal user may only change the password for their account, while the superuser may change the password for any user. The chown command is used to change the owner of the file, directory, or link in Linux. The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen. The ps command is used to list the currently running processes, and their PIDs and some other information depend on different options. It reads the process information from the virtual files in the /proc file system. The /proc directory contains virtual files and is known as a virtual file system.

QUESTION 238
What does the command "shutdown /s" do on a Windows workstation?

A. Log off the workstation
B. Shutdown the workstation
C. Enter sleep mode
D. Reboot the workstation

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.2: The shutdown command allows a user or administrator to shut down or restart local or remote computers, one at a time. Using the /r option will reboot the computer. Using the /s option will shut down the computer. Using the /l option will log off the current user. Using the /h option will enter sleep or hibernation mode.

QUESTION 239
Which of the following Control Panel options should a technician configure to automatically adjust the volume of different sounds when the computer is being used to place or receive telephone calls?

A. Sound
B. Programs and Features
C. Ease of Access
D. USB selective suspend

Correct Answer: A
Explanation

Explanation/Reference:

OBJ-1.4: The Sound section of the Control Panel allows technicians. to configure settings for the playback, recording, and sound effects on the computer. Under the communications tab of the Sound section, a technician can adjust whether or not the computer should adjust the volume of other sounds when a telephone call is occurring. The Ease of Access section of the Control Panel brings together the functionality for the accessibility features in Windows, including visual, tactile input, and speech recognition settings to assist those with disabilities. The USB selective suspend feature allows the hub driver to suspend an individual port without affecting the operation of the other ports on the hub. Selective suspension of USB devices is helpful when using a laptop computer as it helps to conserve battery power by powering off USB ports that are not needed at the time. The Programs and Features section of the Control Panel allows a technician to install or remove applications, software packages, and features in the Windows operating system.

QUESTION 240
What is the BEST way to update an app purchased from the Mac App Store on a Macbook?

A. Download the latest version from the manufacturer's website
B. Open the Mac App Store and select the Updates button
C. Open the terminal and use the "apt-get update" command
D. Open the app and run the "Download Update" command

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.1 0: You can open the Mac App Store and click the Updates button to see any applications that require a software update. This will work for all macOS software, built-in apps like Safari, and third- party apps downloaded from the App Store. You can use the Software Update tool in the System Preferences area of your system to update these apps. The apt-get utility is a powerful package management command-line program that works with Ubuntu's APT (Advanced Packaging Tool) library to install new software packages, remove existing software packages, upgrade existing software packages, and even upgrade the entire operating system. The apt-get utility works with Ubuntu and Debian-based Linux distributions.

QUESTION 241
What type of structure is "IF THEN ELSE" in scripting?

A. Branch
B. Variable
C. Loop
D. Constant

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.8: A branch is used to control the flow within a computer program or script, usually based on some logic condition. Often, these are implemented with IF THEN ELSE statements. A variable is a placeholder in a script containing a number, character, or string of characters. Variables in scripts do not have to be declared (unlike in programming languages) but can be assigned a value. Then, the variable name is referenced throughout the script instead of the value itself. A loop deviates from the initial program path to some sort of logic condition. In a loop, the computer repeats the task until a condition is met. Often implemented with For or While statements. For example, a short script like (Fori =1 to 100, print I, next) would print the numbers from 1 to 100 to the screen. A constant is a specific identifier that contains a value that cannot be changed within the program. For example, the value to convert a number from F to Cis always 5/9 because the formula is C = (F - 32) * 5/9.

QUESTION 242
What kind of attack is an example of IP spoofing?

A. ARP poisoning
B. On-path attack
C. SQL injections
D. Cross-site scripting

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: An on-path attack (formerly known as a man- in-the-middle attack) intercepts communications between two systems. For example, in an HTTP t ransaction, the· target is the TCP connection between client and server. Using different techniques, the attacker splits the original TCP connection into 2 new connections, one between the cllient and the attacker and the other between the attacker and the server. This often uses IP spoofing to trick a victim into connecting to the attack. SQL injection is a code injection technique used to attack data-driven applications. Malicious SQL statements are inserted into an entry field for execution, such as dumping the database contents to the attacker. An on- path attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other. ARP Poisoning, also known as ARP Spoofing, is a type of cyber attack carried out over a Local Area Network (LAN) that involves sending malicious ARP packets to a default gateway on a LAN to change the pairings in its IP to MAC address table. Cross-Site Scripting (XSS) attacks are a type of injection in which malicious scripts are injected into otherwise benign and trusted websites. XSS attacks occur when an attacker uses a web application to send malicious code, generally in a browser side script, to a different end-user.

QUESTION 243
Which of the following file types are commonly used by scripts in a web page?

A. sh
B. js
C. vbs
D. ps1

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.8: JavaScript is a scripting language that is designed to create interactive web-based content and web apps. The scripts are executed automatically by placing the script in the HTML code for a web page so that when the HTML code for the page loads, the script is run. JavaScript is stored in a js file or as part of an HTML file. VBScript is a scripting language based on Microsoft's Visual Basic programming language. Network administrators often use VBScript to perform repetitive administrative tasks. With VBScript, you can run your scripts from either the command-line or the Windows graphical interface. Scripts that you write must be run within a host environment. Windows 10 provides Internet Explorer, liS, and Windows Script Host (WSH) for this purpose. Windows PowerShell enables you to perform management and administrative tasks in Windows 7 and later. It is fully integrated with the operating system and supports both remote execution and scripting. Microsoft provides the Windows PowerShell Integrated Scripting Environment (ISE) to help create and manage your Windows PowerShell scripts. If you want to save a series of PowerShell commands in a file to rerun them later, you effectively create a PowerShell script by creating a text file with a .ps1 extension. The file can contain a series of PowerShell commands, with each command appearing on a separate line. A shell script is a file that contains a list of commands to be read and executed by the shell in Linux and macOS. A .sh file is used for a shell script and its first line always begins with #!/bin/bash that designates the interpreter. This line instructs the operating system to execute the script. Shell scripts allow you to perform various functions. These functions include automation of commands and tasks of system administration and troubleshooting, creating simple applications, and manipulating text or files.

QUESTION 244
You run the command ipconfig on your laptop and see that you have been assigned an IP address of

169.254.0.56. Which category of 1Pv4 address is this?

A. Public
B. Static
C. Private
D. APIPA

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.5: APIPA stands for Automatic Priv.ate IP Addressing and is a feature of Windows operating systems. When a client computer is configured to use automatic addressing (DHCP), APIPA assigns a class B IP address from 169.254.0.0 to 169.254.255.255 to the client if the DHCP server is unavailable. A static IP address is used when the DHCP server is disabled and clients are configured manually to join the network properly. A public IP address is the outward-facing (public-facing) IP address assigned to a client. A private IP address lets a router correctly direct traffic within its network and allows devices within a network to communicate with one another, but private I P addresses cannot be used to route traffic across the internet.

QUESTION 245
Which of the following file types are commonly used to create applications that can be run on Linux, macOS, and Windows?

A. vbs
B. ps1
C. sh
D. py

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.8: Python is a general-purpose programming language that can develop many different kinds of applications. It is designed to be easy to read, and the programs use fewer lines of code compared to other programming languages. The code runs in an interpreter. Python is preinstalled on many Linux distributions and can be installed on Windows. Python scripts are saved using the .py extension. A shell script is a file that contains a list of commands to be read and executed by the shell in Linux and macOS. A .sh file is used for a shell script and its first line always begins with #!/bin/bash that designates the interpreter. This line instructs the operating system to execute the script. Shell scripts allow you to perform various functions. These functions include automation of commands and tasks of system administration and troubleshooting, creating simple applications, and manipulating text or files. VBScript is a scripting language based on Microsoft's Visual Basic programming language. Network administrators often use VBScript to perform repetitive administrative tasks. With VBScript, you can run your scripts from either the command-line or the Windows graphical interface. Scripts that you write must be run within a host environment. Windows 10 provides Internet Explorer, liS, and Windows Script Host (WSH) for this purpose. Windows PowerShell enables you to perform management and administrative tasks in Windows 7 and later. It is fully integrated with the operating system and supports both remote execution and scripting. Microsoft provides the Windows PowerShellIntegrated Scripting Environment (ISE) to help create and manage your Windows PowerS hell script s. If you want to save a series of PowerS hell commands in a file to rerun them later, you effectively create a PowerShell script by creating a t ext file with a .ps1 extension. The file can contain a series of PowerShell commands, with each command appearing on a separate lijne.

QUESTION 246
Karen lives in an area that is prone to hurricanes and other extreme weather conditions. She asks you to recommend an electrical conditioning device that will prevent her files from being corrupted if the building's power is unstable or lost. Additionally, she would like the computer to maintain power for up to an hour of uptime to allow for a graceful shutdown of her programs and computer. Which of the following should you

recommend?

A. Power distribution unit
B. Line conditioner
C. Uninterruptible power supply
D. Surge protector

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.5: An uninterruptible power supply or uninterruptible power source (UPS) is an electrical apparatus that provides emergency power to a load when the input power source becomes too low or the main power fails. A UPS provides near-instantaneous protection from input power interruptions by using a battery backup. The onbattery run-time of most uninterruptible power sources is usually short (less than 60 minutes) but sufficient to properly shut down a computer system. A line conditioner is a device that adjusts voltages in under-voltage and overvoltage conditions to maintain a 120 V output. Line conditioners raise a sag or under-voltage event back to normal levels, but they cannot protect the line from a complete power fai lure or power outage. A surge protector defends against possible voltage spikes that could damage your electronics, appliances, or equipment. A power strip will not protect against voltage spikes. A UPS or line conditioner could protect against voltage spikes, but they cost much more than a surge protector. A power distribution unit (PDU) is a device designed to provide power to devices that require power, and may or may not support remote monitoring and access.

QUESTION 247
A programmer is writing a script to calculate the disk space needed to perform a daily backup. The programming needs to store the amount of disk space in a temporary placeholder within the program that can be updated and changed during the script 's execution. Which of the following would be used to store the value of the disk space needed?

A. Loop
B. Comment
C. Constant
D. Variable

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.8: A variable is a placeholder in a script containing a number, character, or string of characters. Variables in scripts do not have to be declared (unlike in programming languages) but can be assigned a value. Then, the variable name is referenced throughout the script instead of the value itself. A constant is a specific identifier that contains a value that cannot be changed within the program. For example, the value to convert a number from F to Cis always 5/9 because the formula is C = (F -32) * 5/ 9. A loop deviates from the initial program path to some sort of logic condition. In a loop, the computer repeats the task until a condition is met. Often implemented with For or While statements. For example, a short script like (For i=1 to 100, print I, next) would print the numbers from 1 to 100 to the screen. A comment is written into the code to help a human understand the initial programmer's logic. In Python, for example, you can use the# symbol to comment on a line of code. Anything on the line after the# is ignored by the computer when the script is being executed.

QUESTION 248
Which command-line tool could you use on a Windows system to enable an inactive administrator account?

A. net user
B. robocopy
C. taskkill

D. Gpresult

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.2: There are several net command utilities that you can use to view and configure shared resources on a Windows network. The net userr command allows system administrators to manage user accounts on Windows PCs. You can use the command to display account information or make changes to user accounts. It can be used, among other things, to enable the inactive administrator account of a Windows system. The robocopy tool is used to mirror or synchronize directories and their contents. Robocopy will check the destination directory and remove files no longer in the main tree. It also checks the files in the dest ination directory against the files to be copied and doesn't waste time copying unchanged mes. The taskkill command is used to end one or more tasks or processes on a Windows system. Processes can be ended by process ID or image name. You can use the tasklist command to determine the process ID (PI D) for the process to be ended. The gpresult command is used to display the Resultant Set of Policy (RSoP) information for a remote user and computer. Because you can apply overlapping policy settings to any computer or user, the Group Policy feature generates a resulting set of policy settings when the user logs on. The gpresult command displays the resulting set of policy settings that were enforced on the computer for the specified user when the user logged on.

QUESTION 249
While troubleshooting the reason that the File Explorer is crashing on a Windows 10 machine, you determine that some of its files may have become corrupt. Which of the following utilities should you use to correct this?

A. dxdiag
B. gpupdate
C. sfc
D. Reg edit

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.1: The system file checker (SFC) command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from the command line. System files (and shared program files) are maintained and version-controlled in the WINSxS system folder. Since the File Explorer is part of the Windows 10 operating system files, it would be repaired or replaced by running the system file checker (SFC). The registry editor (Reg Edit) allows you to view and make changes to system files and programs that you wouldn't be able to access otherwise. The registry is a database made up of hives and keys that control various settings on a Windows system. ly editing the Registry can permanently damage your computer, so it is important to be very careful when modifying the registry using Reg Edit. The gpupdate command-line tool is used to update the group policy settings on a Windows system. For an administrator to force a background update of all Group Policy settings regardless of whether they have changed, t hey need to run "gpupdate /force" from the command line. The DirectX diagnostic (dxdiag.exe) utility is used to collect info about devices to help troubleshoot problems with DirectX sound and video. It is a diagnostics tool used to test DirectX functionality and troubleshoot video-related or sound-related hardware problems. DirectX diagnostic can save text files with the scan results.

QUESTION 250
You are helping to set up a backup plan for your organization. The current plan states that all of the organization's Linux servers must have a daily backup conducted. These backups are then saved to a local NAS device. You have been asked to recommend a method to ensure the backups will work when needed for restoration. Which of the following should you recommend?

A. Create an additional copy of the backups in an off-site datacenter
B. Attempt to restore to a test server from one of the backup files to verify them

C. Frequently restore the server from backup files to test them
D. Set up scripts to automatically reattempt any failed backup jobs

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.3: The only way to fully ensure that a backup will work when needed is to restore the files from the backups. To do that, it is best to restore them to a test server since this will not affect your production en vi ron ment.

QUESTION 251
How would you represent r-xrw-r-- in octal notation?

A. 624
B. 754
C. 564
D. 541

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.6: R-X is 5, RW- is 6, and R-- is 4. In Linux, you can convert letter permissions to octal by giving 4 for each R, 2 for each W, and 1 for each X. R is for read-only, W is for write, and X is for execute. The permissions strings are written to represent the owner's permissions, the group's permissions, and the other user's permissions.

QUESTION 252
A network technician is tasked with designing a firewall to improve security for an existing FTP server on the company network. The FTP server must be accessible from the Internet. The security team is concerned that the FTP server could be compromised and used to attack the domain controller hosted within the company's internal network. What is the BEST way to mitigate this risk?

A. Configure the firewall to utilize an implicit deny statement
B. Upgrade the FTP server to an SFTP server since it is more secure
C. Migrate the FTP server from the internal network to a screened subnet
D. Add a deny rule to the firewall's ACL that blocks port 21 outbound

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: A screened subnet (formerly called a demilitarized zone or DMZ) is a perimeter network that protects an organization's internal local area network (LAN) from untrusted traffic. A screened subnet is placed between the public internet and private networks. Public servers, such as the FTP server, should be installed in a screened subnet so that additional security mitigations like a web application firewall or application-aware firewall can be used to protect them. SFTP (Secure File Transfer Protocol) is a file transfer protocol that leverages a set of utilities that provide secur,e access to a remote computer to deliver secure communications by leveraging a secure shell (SSH) connection to encrypt the communication between the client and the server. This will prevent an attacker from eavesdropping on the communications between the SFTP server and a client, but it will not prevent an attacker from exploiting the SFTP server itself. An implicit deny is when a user or group is not granted specific permission in the security settings of an object, but they are not explicitly denied either. This is a best practice to enable, but the FTP server would still have some open ports, such as ports 20 and 21, to operate. Thes,e ports could then be used by the attacker to connect to the FTP server and exploit it. Adding a deny rule to the firewall's ACL that blocks port 21 outbound would simply prevent internal

network users and servers from accessing external FTP servers. This would in no way prevent the exploitation of the company's FTP server since it has port 21 open and listening for inbound connections.

QUESTION 253
You are working as a mobile device technician for a large corporation's enterprise service desk. A user complains that every time they attempt to launch the company's mobile email application, it crashes and displays an error message of Code123. Which of the following should you do FIRST to attempt to solve this problem?

A. Reinstall! the email app
B. Rollback the app to an earlier version
C. Update the smartphone's OS
D. Clear the app's cache

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.4: If an app is not loading, you should uninstall and reinstall the app. This will ensure the app is not corrupted and has the latest version. If this doesn't work and the app used to work before being updated to the latest version, you can attempt to roll back the app to an older version on an Android device by sideloading the a

QUESTION 254
Which command is used to create a new disk partition on a Windows system?

A. dd
B. diskpart
C. chkdsk
D. Format

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.2: The diskpart command is a command-line disk-partitioning utility available for Windows that is used to view, create, delete, and modify a computer's disk partitions. The chkdsk command is used to check the file system and file system metadata of a volume for logical and physical errors. If used without parameters, chkdsk displays only the status of the volume and does not fix any errors. If used with the /f, /r, /x, or /b parameters, it fixes errors on the volume. The format command creates a new root directory and file system for the disk. It can check for bad areas on the disk, and it can delete all data on the disk. To use a new disk, you must first use the format command to format the disk. The dd command is a Linux utility that is used to copy and convert raw data from one source to another such as a hard disk to an image file.

QUESTION 255
Your mother says there is something wrong with her computer, but unfortunately, she doesn't know how to fix it. She asks if you can remotely connect to her computer and see if you can fix it. Which of the following technologies would BEST allow you to remotely access her computer and interact with her Windows 10 laptop?

A. RDP
B. SSH
C. Telnet
D. VPN

Correct Answer: A

Explanation

Explanation/Reference:
OBJ-4.9: Remote Desktop Protocol (RDP) is a Microsoft protocol designed to facilitate application data transfer security and encryption between client user devices and a virtual network server. It enables a remote user to add a graphical interface to the desktop of another computer. Whether across the house or the country, you can now help solve your mother's computer probllems anytime with RDP. Telnet should not be used in a network due to its weak security posture. Tel net transmits all of the data in plain text (without encryption}, including usernames, passwords, commands, and data files. For this reason, it should never be used in production networks and has been replaced by SSH in most corporate networks. SSH (Secure Shell) is used to remotely connect to a network's switches and routers to configure them securely. SSH is typically used for logging into a r,emote machine and executing commands, but it also supports tunneling, forwarding TCP ports, and X11 connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model. A remote-access VPN connection allows an individual user to connect to a private network from a remote location using a laptop or desktop computer connected to the internet. A remote-access VPN allows individual users to establish secure connections with a remote computer network. Once established, the remote user can access the corporate network and its capabilities as if they were accessing the network from their own office spaces.

QUESTION 256
What is the minimum processor required to install Windows 10 {x64) on a device?

A. 2 GHz single-core processor
B. 2 GHz dual-core processor
C. 1 GHz single-core processor
D. 1 GHz dual-core processor

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.7: For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64GB of hard drive space.

QUESTION 257
You have just completed a repair for a customer's smartphone that took you three days. The customer complained that the repair took too long and began to question you about the steps you took to repair the device. What should you do NEXT?

A. Become defensive and explain why each step was necessary to repair the device
B. Provide documentation of the repair to the customer and thank them for their patience
C. Listen to the customer's complaints with concern and then post about the encounter on Facebook
D. Clearly tell the customer that if they had been more careful with the device then it wouldn't have needed to be fixed in the first place

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.7: When dealing with a difficult customer or situation, you should follow five key principles: (1) Do not argue with customers and/or become defensive; (2) Avoid dismissing customer problems; (3) Avoid being judgmental; (4) Clarify customer statements (ask open-ended questions to narrow the problem's scope, restate the issue, or question to verify understanding); and (5) Do not disclose experiences via social media outlets. The only option provided that follows these principles is to provide documentation of the repair to the customer

and thank them for their patience. The other three options all violate these principles.

QUESTION 258
What is the minimum amount of memory required to install Windows 10 (x86) on a device?

A. 2GB
B. 1GB
C. 4GB
D. 8GB

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.7: For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20 GB of hard drive space. For the Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64GB of hard drive space.

QUESTION 259
Dion Training has configured Windows Defender Firewall on all of its corporate Windows 10 workstations. When connected to a private network, the firewall has been configured to only allow inbound connections that match an existing rule and to only allow outbound connections that do not match any existing rules.
What type of security posture has Dion Training implemented?

A. Implicit allow for inbound, implicit allow for outbound
B. Implicit allow for inbound, explicitly allow for outbound
C. Explicit allow for inbound, implicit allow for outbound
D. Explicit allow for inbound, explicit allow for outbound

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.4: The Windows Defender Firewall is a software-based firewall that is installed by default on Windows workstations. The Windows Defender firewall is used to prevent hackers and malicious software from gaining access to the workstation over the Internet or the local area network. Explicit allow refers to a security posture where the system will only allow an item to traverse the firewall if the traffic matches an existing rule. Implicit allow refers to a security posture where the system will allow all traffic to traverse the firewall unless there is a specific rule to prevent it.

QUESTION 260
Which attack utilizes a wirele.ss access point made to look as if it belongs to the network by mimicking the corporate network's SSID to eavesdrop on the wireless traffic?

A. Shoulder surfing
B. Evil twin
C. Rogue access point
D. WEP attack

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: An evil twin is meant to mimic a legitimate hotspot provided by a nearby business, such as a coffee

shop that provides free Wi-Fi access to its patrons. An evil twin is a type of rogue wireless access point that masquerades as a legitimate Wi-Fi access point so that an attacker can gather personal or corporate information without the user's knowledge. This type of attack may be used to s.teal the passwords of unsuspecting users by monitoring their connections or phishing, which involves setting up a fraudulent website and luring people there. A rogue access point is an access point installed on a network without the network owner's permission. For example, if an employee connected a wireless access point to a wall jack in their office so that they can use their smartphone or tablet, this would be considered a rogue access point. Therefore, an evil twin is the better answer to this question since it is specifically being made to look like it belongs on the network by mimicking the SSID of the corporate network. A WEP attack is a brute force password attack conducted against a wireless network that relies on WEP for its encryption and security. Shoulder surfing is a type of social engineering technique used to obtain information such as personal identification numbers, passwords, and other confident ial data by looking over the victim's shoulder.

QUESTION 261
Sally was checking her email when she noticed that she has several automated replies from emails she doesn't remember sending. What type of attack was Sally MOST likely the victim of?

A. Vishing
B. Phishing
C. Spear phishing
D. Hijacked email

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.2: Sally is MOST likely the victim of hijacked email. Hijacked email occurs when someone takes over your email account and sends out messages on your behalf. Hijacked emails can trigger automated replies indicating that the intended recipient's messages were rejected or that the recipient was out of the office. These "bounce back" emails indicate to the victim that they have lost control of their email account. Phishing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people. Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to induce targeted individuals to reveal confidential information. Vishing is a social-engineering attack where the attacker extracts information while speaking over the phone or leveraging IP-based voice messaging services (VoiP).

QUESTION 262
Dion Training will be hiring 10 college students as interns to work over the summer. Each year, the same interns will work for the company for 8 weeks, but then they will return to school. Next summer, they will return to the company and will need to reaccess their accounts. What is the BEST policy to use so that the interns can use the accounts during the summer but cannot log in during the school year?

A. Reset the user accounts at the end of each summer
B. Restrict the user accounts using login hours
C. Disable the user accounts at the end of each summer
D. Delete the user accounts at the end of each summer

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.6: If the accounts are disabled at the end of the· summer, the interns will be unable to log in again until their accounts are enabled again when they return next summer. This is the best method since deleting the accounts would require the interns to get new accounts each summer, and they would lose all their data and config urations.

QUESTION 263
Your company has just installed a brand new email server, but you determined that the server cannot send emails to another server during your initial testing. You decide to check the firewall's ACL to see if the server's outgoing email is being blocked. Which of the following ports should you ensure is open and not blocked by the firewall?

A. 25
B. 22
C. 143
D. 110

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.1: The Simple Mail Transfer Protocol (SMTP) uses port 25 and is an internet standard communication protocol for electronic mail transmission. Internet Message Access Protocol (I MAP) uses port 143 and ·is an Internet standard protocol used by email cl ients to retrieve email messages f rom a mail server over a TCP/IP connection. Post Office Protocol version 3 (POP3) uses port 110 and is an application-layer Internet standard protocol used by e-mail clients to retrieve e-mail from a mail server. Secure Shell (SSH) uses port 22 to securely create communication sessions over the Internet for remote access to a server or system.

QUESTION 264
Which of the following contains virtual memory that can supplement the physical system memory in a Linux system?

A. ext4
B. ext3
C. Swap partition
D. NFS

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.8: The swap partition on a Linux system is a portion of the hard disk formatted with a minimal kind of file system and used in situations when the operating system runs out of physical memory and needs more of it. It can only be used by the memory manager and not for the storage of ordinary data files. The third extended filesystem (ext3) is a journaled file system commonly used by the Linux kernel. The ext3 file system can support a maximum volume size of up to 32 TB. The fourth extended filesystem (ext4) is a journaled file system that is used natively by modern Linux operating systems such as Debian and Ubuntu. The ext4 file system can support a maximum volume size of up to 1 EB. The network file system (NFS) is used to mount remote storage devices into the local file system on a Linux system. It allows you to mount your local file systems over a network and remote hosts to interact with them while mounted locally on the same system.

QUESTION 265
Which of the following is considered a form of regulated data?

A. DRM
B. Pll
C. DMCA
D. AUP

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.6: The four forms of regulated data covered by the exam are PII (Personally Identifiable Informat ion), PCI (Payment Card Industry), GDPR (General Data Protection Regulation), and PHI (Protected Health Information). Personally identifiable information (PII) is data used to identify, contact or locate an individual. Information such as social security number (SSN), name, date of birth, email address, telephone number, street address, and biometric data is considered Pll. An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network or the Internet. While some items in the AUP might help prevent a malware infection (such as not allowing users to download and run programs from the internet), it is considered an administrative control, and choosing a technical control like patch management would better protect the network. Digital rights management (DRM) is a copyright protection technology for digital media. DRM solutions usually try to restrict the number of devices allowed for playback of a licensed digital fi le, such as a music t rack or ebook. The Digital Millennium Copyright Act (DMCA) is a 1998 United States copyright law that implements two 1996 treaties of the World Intellectual Property Organization that criminalizes production and dissemination of technology, devices, or services intended to circumvent measures that control access to copyrighted works.

QUESTION 266
A recently hired security employee at a bank was asked to perform daily scans of the bank's intranet to look for unautho:rized devices. The new employee decides to create a script that sca1ns the network for unauthorized devices every morning at 2:00am. Which programming language would work best to create this script?

A. PHP
B. Python
C. C#
D. ASP.NET

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.8: Python is a commonly used scripting language used in cybersecurity. Python is at general-purpose programming language that can develop many different kinds of applications. It is designed to be easy to read, and the programs use fewer lines of code compared to other programming languages. The code runs in an int erpreter. Python is preinstalled on many Linux distributions and can be installed on Windows. Python scripts are saved using the .py extension. PHP is used as a scripting language for web applicat ions. C# and ASP. NET are both compiled languages, not scripting languages.

QUESTION 267
Your home network is configured with a long, strong, and complex pre-shared key for its WPA2 encryption. You noticed that your wireless network has been running slow, so you checked the list of "connected clients" and see that "Bob's Laptop" is connected to it. Bob lives downstairs and is the maintenance man for your apartment building. You know that you never gave Bob your password, but somehow he has figured out how to connect to your wireless network. Which of the following actions should you take to prevent anyone from connecting to your wireless network without the proper WPA3 password?

A. Disable WPA3
B. Enable WEP
C. Disable SSID broadcast
D. Disable WPS

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.9: WPS was created to ease the setup and configuration of new wireless devices by allowing the router to aut omatically configure them after a short eight-digit PIN was entered. Unfortunately, WPS is vulnerable to a brute-force attack and is easily compromised. Therefore, WPS should be disabled on all wireless networks. If

Bob could enter your apartment and press the WPS button, he could have configured his laptop to use your wireless network without your WPA3 password. While disabling the SSID broadcast could help prevent someone from seeing your network, the issue was someone connecting to your network without having the password. Disabling the SSID broadcast would not solve this issue.

QUESTION 268
A user contacts the help desk and complains they are getting an error when they attempt to open a 4GB .dmg file on their Windows 10 workstation. Which of the following should you tell them?

A. "Your hard drive must not have enough free space"
B. "Your workstation need to have 16GB of RAM to open the file"
C. "You must be an administrator to open that file"
D. "You need to use macOS to open DMG files"

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.2: A .dmg file is a disk image file on a macOS computer. These file types normally are used to download and install applications for macOS. Essentially, a .dmg file on a macOS computer is like a .iso file on a Windows computer. Windows cannot open .dmg files without using special software tools.

QUESTION 269
A system administrator is assigned an approved change request with a change window minutes. After 90 minutes. the change is stuck on step five of a five-step change. The server manager decides to initia1te a rollback. Which describes what the system administrator should do next?

A. Request additional time since the change is near completion
B. Leave the change as is and inform users of a workaround
C. Return the system to step four since this was the last working step
D. Return the system to the original state before the change

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.2: By performing a rollback, the administrator will change everything back to the last known good configuration before the change is started. Every change should be accompanied by a rollback (or backout) plan so that the change can be reversed if it has harmful or unforeseen consequences. Changes should also be scheduled sensitively if they are likely to cause system downtime or other negative impacts on the workflow of the business units that depend on the IT system being modified. Most organizations have a scheduled maintenance window period for authorized downtime.

QUESTION 270
A small doctor's office has asked you to configure their network to use the highest levels of wireless security and desktop authentication. The office only uses cloud-based SaaS applications to store their patient's sensitive data. Which TWO of the following protocols or authentication methods should you implement for the BEST security?

A. WPS
B. SSO
C. WPA2
D. WEP
E. RADIUS
F. Multifactor

Correct Answer: CF
Explanation

Explanation/Reference:
OBJ-2.2: Since everything is being stored within a cloud-based SaaS application, the doctor's office needs to ensure their network connection uses the highest encryption level (WPA2), and their desktop authentication should use a multifactor authentication system. Multifactor authentication relies on using at least 2 of the following factors: something you know (password or pin), something you have (smart card or key fob), something you are (fingerprint or retinal scan), or something you do (draw a pattern or how you sign your name). Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the complet ion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption. Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks t hat can break its encryption. WEP relies on the use of a 24- bit initialization vector to secure its preshared key. The Wi- Fi Protected Setup (WPS) is a mechanism for autoconfiguring a WLAN securely for home users. On compatible equipment, users push a button on the access point and connect adapters to associate them securely. WPS is subject to brute force attacks against the PIN used to secure them, making them vulnerable to attack. The Remote Authentication Dial-in User Service (RADIUS) is used to manage remote and wireless authentication infrastructure. Users supply authentication information to RADIUS client devices, such as wireless access points. The client device then passes the authentication data to an AAA (Authentication, Authorization, and Accounting) server that processes the request. Single sign-on (SSO) is a type of mutual authentk ation for multiple services that can accept the credential from one domain or service as authentication for other services.

QUESTION 271
You have been asked to configure your neighbor's SOHO network. Your neighbor wants to build a Minecraft server :so that all their friends can play together over the internet. When configuring their firewall, where should you place the server?

A. Perimeter network
B. WAN
C. MAN
D. LAN

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.9: A perimeter network (formerly called a Demilitarized Zone or DMZ) is a portion of a private network connected to the Internet and protected against int rusion. Certain services may need to be made publicly accessible from the Internet (such as a web, email, or Minecraft server) and they should be installed in the perimeter network instead of in your intranet. If communication is required between hosts on either side of a perimeter network, then a host within the perimeter network will act as a proxy to take the request. If t he request is val id, it re-transmits it to the destination. External hosts have no idea about what is behind the perimeter network so that the intranet remains secure. A perimeter network can be implemented using either two firewalls (screened subnet) or a single three-legged firewall (one with three network ports). In this SOHO network, it would use a single three- legged firewall approach to separate the perimeter network from the LAN and WAN. A local area network (LAN) is a network where all the nodes or hosts participating in the network are directly connected with cables or short-range wireless media. A wide area network (WAN) is a network that spans multiple geographic locations such as the internet. A metropolitan area network (MAN) is a network that covers a geographical area equivalent to a city or municipality.

QUESTION 272
Your supervisor has requested remote access to a particular server to check on specific data and processes in the evenings and weekends. You are concerned that the server could become infected and want to take some precautions. Which of the following is the MOST important thing to do before granting remote access to the

server to your supervisor?

A. Disable internet access from the server outside of normal business hours
B. Educate your supervisor on safe internet browsing techniques
C. Install the latest security updates and patches to the server
D. Set the server's anti-virus software to automatically update itself and perform a full scan every Saturday night

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.6: To prevent infection, it is important that all servers and workstations remain patched and up to date on their security updates. After t hat, the next best thing would be to set up the anti-virus to update itself daily and run a full scan nightly automatically. Beyond that, educating your supervisor would be a good idea, as well. Disabling the internet access outside of normal business hours would not work since this would block your supervisor from accessing the server from their home.

QUESTION 273
Matt has verified that a user's system has symptoms of being infected with malware. According to the malware removal procedures~ what should Matt do NEXT?

A. Educate the end user about how to avoid malware in the future
B. Quarantine the infected system by removing its network connectivity
C. Enable System Restore and create a restore point in Windows
D. Update the anti-virus software and run a full system scan

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.3: The seven steps of the· malware removal procedures are 0) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 274
A technician needs to add new features to an existing router on the network. Which of the following should be performed to add the new features?

A. Firmwa1re update
B. Migrating to 1Pv6
C. Vulnerability patchiing
D. Clone the router

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.9: A firmware update wil ~ upgrade your device with advanced operational instructions without needing a hardware upgrade. A firmware update can provide new features or functions to an existing device, or patch vulnerabilities in the existing firmware code. Firmware· is a specific class of computer software that provides lowlevel control for a device's specific hardware. Internet Protocol version 6 (1Pv6) is the most recent version of the Internet Protocol, the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. 1Pv6 will not add any new features to an existing

hardware device. Some devices may require a firmware upgrade to support t he new 1Pv6 protocols. Cloning is a process that involves setting up the operating system, drivers, software, and patches on a single computer, then automatically replicat ing this same setup on other computers using specialized software. Routers, unlike computers, cannot be cloned. Routers can be backed up and then restored, though. Vulnerability patching is the process of checking your operating systems, software, applications, and network components for vulnerabilities that could allow a malicious user to access your system and cause damage, and then applying a security patch or reconfiguring the device to mitigate the vulnerabilities found. Vulnerability patching will mitigate software bugs, but it will not add new features to an existing device.

QUESTION 275
A small business network was recently infected by a piece of malware from a USB drive that copied sensitive data from a computer, infected the system, and then spread across the network by infecting other systems. Which of the following actions could have prevented this type of attack from occurring?

A. Replacing the default credentials on the system
B. Disabling AutoRun on the computer
C. Enforcing the use of complex passwords
D. Enabling full disk data encryption

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.6: The Windows AutoRun feature is turned on by default on most Windows versions, allowing programs to run from an external device as soon as it is attached to a comput er. Malware can exploit the AutoRun feature and allow it to spread its payload from your external USB device to a comput er. For this reason, users should disable the AutoRun feature. While the other options are all good security practices, they would not have prevented the issue stated in the scenario.

QUESTION 276
Tim connects his Windows 10 laptop to his office's wireless network to print out a report for his boss. Which type of network should he select to discover the printer on the office's wireless network?

A. Private
B. Home
C. Work
D. Public

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.6: Tim should select the private network type when connecting to the wireless network in his office so that he can access the networked printer. The Network and Sharing Center in t he Control Panel allows a technician to see information and modify the configuration settings of the network adapters in the workstation. The Network and Sharing Center is used to connect to a network using broadband, dial-up, or VPN connection, or add/remove file and printer sharing over the network on the workstation. When connecting to a network for the first time, t he user must select if it is a public or private network. A public network will hide your computer from other devices on the network and prevent file and printer sharing. A private network is considered trusted, allows the computer to be discoverable to other devices on the network, and supports the use of file and printer sharing. In older versions of Windows, there were also Home and Work network types, but those have since been merged into public and private network types, as well.

QUESTION 277
A technician at Dion Training wants to identify which version and build of Windows 10 is installed on a laptop. Which of the following commands should the technician enter at the command line?

A. path ping
B. winver
C. net user
D. Gpresult

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.2: The winver command is a Windows command-line tool that is used to display the name, version, and build of the operating system on a workstation. The gpresult command is used to display the Resultant Set of Policy (RSoP) information for a remote user and computer. Because you can apply overlapping policy settings to any computer or user, the Group Policy feature generates a resulting set of policy settings when the user logs on. The gpresult command displays the resulting set of policy settings that were enforced on the computer for the specified user when the user logged on. The pingpath command is a Windows command -line tool that is used to locate spots that have network latency and network loss between a client and a destination. The advantages of Path Ping over ping and traceroute are that each node is pinged as the result of a single command and that the behavior of nodes is studied over an extended period, rather than the defau lt ping sample of four messages or default traceroute single route trace. The net user command allows system administrators to manage user accounts on Windows PCs. You can use the command to display account information or make changes to user accounts. It can be used, among other things, to enable the inactive administrator account of a Windows system.

QUESTION 278
You are working as a desktop repair technician for a large corporation. The company uses the exact same desktop hardware for all of its user's workstations. Today, you have received multiple calls from users complaining that their screen becomes filled with static when moving their mouse. You believe the video card driver may be at fault. Which log would you review to determine if the video card driver has been updated recently?

A. System log
B. Application log
C. Setup
D. Security log

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: If the driver was recently updated and is now causing issues, it will most likely be documented in the system log. The system log contains information about service load failures, hardware conflicts, driver load failures, and more. The file (system.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a usef ul tool for troubleshooting all kinds of different Windows problems. The application log contains information regarding application errors. The file (application.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The setup log contains a record of the events generated during the Windows installation or upgrade process. The file (setup.evtx) is stor,ed in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The security log contains information regarding audit data and security on a system. For example, the security log contains a list of every successful and failed login attempt. The file (security.evtx) is stored in the %System Root%\System32\ Winevt\Logs\ folder and can be opened using the Event Viewer.

QUESTION 279
Dion Training is creating troubleshooting guides and frequently asked questions for its new customer service technicians. Which of the following would MOST likely contain these documents?

A. Network topology diagrams
B. Password policy
C. Asset management database
D. Knowledge base articles

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.1: A Knowledge Base (KB) is a reference document that is used to assist a technician when they are installing, configuring, and troubleshooting hardware and software. A knowledge base article might be created by a vendor to support their products, too. A company might create an internal KB, populated with guidelines, procedures, information, and frequently asked questions from their service tickets. A network topology is the shape or structure of a network in a physical or logical format as depicted in a network diagram. Physical network topologies include the actual appearance of the network layout. Logical network topologijes include the flow of data across the network. A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. It contains items like password complexity, password age, and password history requirements. An asset management database identifies each asset and records its location, attributes, and value in a database.

QUESTION 280
Which of the following commands is used to display the amount of disk space available on the f ile system in Linux?

A. df
B. Is
C. pwd
D. Cat

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.1 1: The df command is used to display the amount of disk space available on the file system containing each file name argument. If no filename is provided, then the space available on all currently mounted file systems is displayed. The cat (short for "concatenate") command is one of the most frequently used commands in Linux/Unix. The cat command allows the creation of single or multiple files, view file contents, concatenate files, and redirect output in the terminal to a file. The Is command lists the files or directories in the current path of a Linux operating system. When invoked without any arguments, Is lists the files in the current working directory. The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen.

QUESTION 281
Which of the following commands is used on a Linux system to edit a text file on a server?

A. vi
B. chown
C. pwd
D. Ps

Correct Answer: A
Explanation

Explanation/Reference:

OBJ-1.1 1: The vi (visual) utility is a popular screen-oriented text editor in Linux, Unix, and other Unix-like operating systems. When using vi, the terminal screen acts as a window into the editing buffer. Changes made to the editing buffer shall be reflected in the screen displlay, and the position of the cursor on the screen will indicate the posit ion within the editing buffer. The ps command is used to l ist the currently running processes, and their PIDs and some other information depend on different options. It reads the process information from the virtual files in the / proc file system. The /proc directory contains virtual files and is known as a virtual file system. The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory struct ure, type "pwd" and hit enter to display the path to the screen. The chown command is used to change the owner of the file, directory, or link in Linux.

QUESTION 282
You want to enable a security feature that would remember the Layer 2 address first connected to a particular switch port to prevent someone from unplugging a workstation from the switch port and connecting their ,own SOHO wireless router to that same switch port. Which of the following security features would BEST accomplish t his goal?

A. Firewall
B. Login script
C. Single sign-on
D. Port security

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.5: Port secu rity enables an administrator to configure individual switch ports to allow only a specified number of MAC addresses to use that port. Port Security helps secure the network by preventing unknown devices from forwarding packets. When a link goes down, all dynamically locked addresses are freed. A firewall is used to prevent hackers and malicious software from gaining access to the workstation over the Internet or the local area network. Single sign-on (SSO) is a type of mutual authentication for multiple services that can accept the credential from one domain or service as authentication for other services. A login script is a text f ile with commands and settings to configure a user's environment that runs when the user logs on to a computer.

QUESTION 283
A user contacts the service desk and states that Microsoft Excel crashed while they were in the middle of updating their spreadsheet. Which of the following log files should you review to determine the cause of the c1rash?

A. System log
B. Security log
C. Setup
D. Application log

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.1: The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems. The application log contains informat ion regarding application errors such as those caused by Microsoft Excel. The file (application.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The setup log contains a record of the events generated during the Windows installation or upgrade process. The fi le (setup.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The system log contains information about service load failu res, hardware conflicts, driver load failures, and more. The file (system.evtx) is stored in the %System Root%\System32

\Winevt\Logs\ folder and can be opened using the Event Viewer. The security log contains information regarding audit data and security on a system. For example, the security log contains a list of every successful and failed login attempt. The f ile (security.evtx) is stored in the %System Root%\System32\ Winevt\Logs\ folder and can be opened using the Event Viewer.

QUESTION 284
One of your Windows services is failing to start when you boot up your laptop. You have checked the service in the Windows Services tool and verified it is set to Automatic. What should you attempt to do NEXT to get the service to startup?

A. Run chkdsk on the system
B. Restore from backup
C. Update the operating system
D. Reboot into Safe Mode and see if the service starts

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.1: Windows Services typically start when the computer is booted and run quietly in the background until it is shut down. For the Windows operating system to run smoothly, Windows Services must start when required. Many times, non-Microsoft services or Drivers can interfere with the proper functioning of System Services. If you boot into Safe Mode, this will load the operating system with the most basic set of drivers, and this could identify if there is a conflict causing the service start failure.

QUESTION 285
Which of the following types of screen locks uses a secret PIN or password to prevent access to a mobile device?

A. Swipe
B. FaceiD
C. TouchiD
D. Passcode

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.7: A passcode lock relies upon something a user memorizes, known as a knowledge factor in authentication. This could be a PIN, password, or passphrase. This is the least secure mechanism of locking a mobile device as the PIN, password, or passphrase could be compromised by shoulder surfing or technical means. A swipe lock is a term for unlocking a device by tracing a predetermined on-screen pattern or joining dots on the screen. This was commonly used in Android devices until biomet ric methods like fingerprint scanners and facial recognition became more prevalent. The FaceiD and TouchiD screen locks rely upon biometric data to securely unlock the device. Since biometrics are body measurements and calculations related to human characteristics, the use of a person's face or fingerprint is classified as a biometric authentication system.

QUESTION 286
Regardless of what website Michelle types into her browser, she is being redirected to "malwarescammers.com." What should Michelle do to fix this problem?

A. Restart the network services
B. Update the anti-virus software and run a full system scan
C. Rollback the application to the previous version
D. Reset the web browser's proxy setting

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.2: When a browser redirect occurs, it usually results from a malicious proxy server setting being added to the browser. Michelle should first check her web browser's configuration for any malicious proxies under the Connections tab under Internet Options in the Control Panel. Next, she should check the hosts.ini file to ensure that single sites ar,e not being redirected.

QUESTION 287
Which of the following should you use to fix an issue with a graphics card's drivers in Windows 10?

A. Devices and Printers
B. System
C. Event Viewer
D. Device Manager

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.4: The Device Manager is used to view and cont rol the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it. The event viewer shows a log of application and system messages, including errors, information messages, and warnings. The Devices and Printers section of the Control Panel allows a technician to manage the printers, scanners, and other external devices connected to a Windows computer. The System section of the Control Panel allows a technician to see information about the workstation, including the processor type, amount of memory, and operating system version installed on the computer.

QUESTION 288
Judith is installing Windows 10 (64-bit) in a virtual machine on her macOS laptop. The installation is continually failing and producing an error. Judith has configured the virtual machine with a dual-core 1 GHz processor, 2GB of memory, a 15 GB hard drive, and a 1024x768 screen resolution. Which item in the virtual machine should be increased to fix the installation issue experienced?

A. Amount of memory
B. The screen resolution
C. Number of CPU cores
D. Amount of hard drive space

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1 .7: For the Windows 10 (64- bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20 GB of hard drive space. Since the virtual machine only has 15GB of hard drive space allocated, this has caused errors with the installation and must be increased.

QUESTION 289
Dion Training's offices are frequently experiencing under-voltage events, sags, and power failures. Which of the following solutions would protect their servers from these issues?

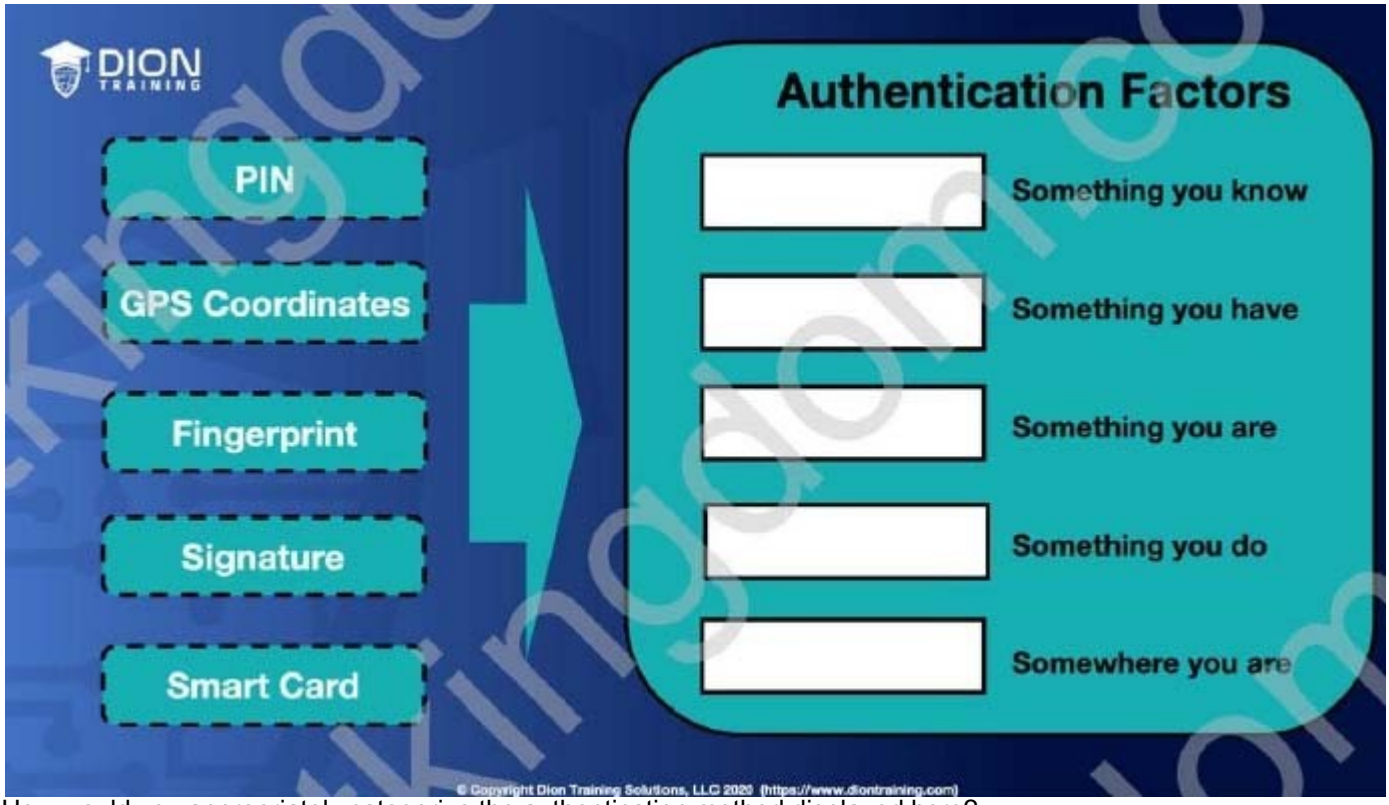
A. Uninterruptible power supply
B. Line conditioner
C. Diesel generator

D. Surge suppressor

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.5: A uninterruptible power supply (UPS) is a battery backup. It is used to protect one server or workstation from under-voltage events, sags, and power fa ilures. If there is a loss of power, system operation can be sustained for a few minutes or hours using a battery backup, depending on the load. A diesel generator is a mechanical device that converts rotational motion created by a diesel motor into electrical energy. Generators take 30-60 seconds to turn on and have the electrical load transferred to them. Generators are useful for longduration power loss events, not under-voltage events. A line conditioner is a device that adj usts voltages in under-voltage and overvoltage conditions to maintain a 120 V output. Line conditioners raise a sag or undervoltage event back to normal levels, but they cannot protect the line from a complete power failure or power outage. A surge protector defends against possible voltage spikes that could damage your electronics, appliances, or equipment. A power strip will not protect against vo ltage spikes

QUESTION 290
(Sample Simulation- On the real exam for this type of question, you would drag and drop the authenitication factor into the spot for the correct category.)



How would you appropriately categorize the authentication method displayed here?

A. Smart card, Signature, GPS Coordinates, PIN, Fingerprint
B. PIN, Signature, Fingerprint, Smart Card, GPS Coordinates
C. PIN, Smart Card, Fingerprint, Signature, GPS Coordinates
D. Fingerprint, PIN, GPS Coordinates, Smart Card, Signature

Correct Answer: C
Explanation

Explanation/Reference:

OBJ-2.1: For the exam, you need to know the different factors of authentication. If you use two or mor·e of these factors, you are using multi-factor authentication. The five factors are something you know (knowledge), something you have (possession), something you are (biometrics), something you do (action), and somewhere you are (location).

QUESTION 291
You are cleaning out the closet in your office and find several bottles of cleaner that need to be disposed of. Which of the following should you consult to determine the proper method of disposal?

A. sow
B. UPS
C. MSDS
D. MOU

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.5: The Material Safety Data Sheet (MSDS) is a document that contains information on the potential hazards (health, fire, reactivity, and environmental) and how to work safely with the chemical product. The MSDS is an essential starting point for the development of a complete health and safety program that includes the directions for proper handling and disposal of the chemicals. An uninterruptible power supply or uninterruptible power source (UPS) is an electrical apparatus that provides emergency power to a load when the input power source becomes too low or the main power fails. A UPS provides near-instantaneous protection from input power interruptions by using a battery backup. A memorandum of understanding (MOU) is a preliminary or exploratory agreement to express an intent to work together that is not legally binding and does not involve monetary exchange. A statement of work (SOW), or a scope of work, is a document that outlines all the work that is to be performed, as well as the agreed-upon deliverables and t imelines.

QUESTION 292
During a disaster recovery, which of the following statements is true?

A. A virtual machine has more downtime than a physical server
B. Both a virtual machine and a physical server has the same downtime
C. A virtual machine has less downtime than a physical server
D. A virtual machine cannot be used for redundancy or load balancing

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.3: A virtual machine can usually be restored much faster than a physical server. Physical servers must be modified to fit the right drivers for the disk drives, NIC, and other necessary components whenever they must be rebuilt after a crash. Often, a new physical server will also be required to replace a faulty one, and then the right drivers are needed to ensure a smooth transition. Conversely, a virtual machine can be recreated using another instance, clone, or restoration from a backup in much less time. Therefore, the downtime associated with virtual machines and their restoral is much lower.

QUESTION 293
You were troubleshooting a recently installed NIC on a workstation and decided to ping the NIC's loopback address. Which of the following 1Pv4 addresses should you ping?

A. 172.1 6.1 .1
B. 10.0.0.1
C. 127.0.0.1
D. 192.168.1.1

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.6: The loopback address is 127.0.0.1 in 1Pv4, and it is reserved for troubleshooting and testing. The loopback address is used to receive a test signal to the NIC and its software/drivers to diagnose problems. Even if the network cable is unplugged, you should be able to ping your loopback address successfully. The other three IP addresses presented as options are private Class A, Class B, or Class C addresses, and not the loopback address.

QUESTION 294
Which of the following commands is used on a Linux system to safely turn off a server?

A. rm
B. kill
C. shutdown
D. Ps

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1 .11: The shutdown command brings the system down in a secure way. When the shutdown is initiated, all logged-in users and processes are notified that the system is going down, and no further log ins are allowed. You can shut down your system immediately or at the specified time. The ps command is used to list the currently running processes, and their PIDs and some other information depend on different options. It reads the process information from the virtual files in the /proc file system. The /proc directory contains virtual files and is known as a virtual file system. The kill command sends a signal to specified processes or process groups, causing them to act according to the signal. When the signal is not specified, it defaults to -15 (-TERM), which terminates the specified process by gracefully stopping it. If "kill -9" is used instead, it will immediately kill the process. The rm command is a command-line utility for removing files or directories. To remove a file, pass the name of a file or files to the rm command, and those files will be removed immediately from the file system.

QUESTION 295
Which of the following Windows tools should a technician use to import and install data in the x.509 format?

A. RDS
B. Device manager
C. Group policy editor
D. Certif icate manager

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.3: The x.509 format is used to define a public key certificate used by TLS/SSL and other internet protocols. Certificate manager (certmgr.msc) is a uti lity used to manage digital certificates on a Windows system. The certificate manager can list, search, open, delete, import, and export digital certificates on a computer. Device manager (devmgmt.msc) is a utility used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it. Group policy editor (gpedit.msc) is a utility used to define and control how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, a group policy is applied to users or computers based on their membership in sites, domains, or organizational units. Remote desktop services (RDS) is used to connect to a remote desktop session host servers or other remote computers, edit an existing remote desktop connection (.rdp)

configuration file, and migrate legacy connection fi les that were created with the client connection manager to the newer .rdp connection file type.

QUESTION 296
A user's workstation is running slowly and cannot open some larger program files. The user complains that they often get a warning that states memory is running low on their Windows 10 workstation. Which of the following should you configure until more memory can be installed to help alleviate this problem?

A. Increase the pagefile size
B. Defragment the hard disk
C. Enable the swap file
D. Disable the visual effects

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: Pagefile in Windows 10 is a hidden system file with the .sys extension stored on your computer's system drive (usually C:\). The Pagefile allows the computer to perform smoothly by reducing the workload of physical memory. Simply put, every time you open more applications than the RAM on your PC can accommodate, the programs already present in the RAM are automatically transferred to the Pagefile. This process is technically called Paging. Because the Pagefile works as a secondary RAM, it is often referred to as Virtual Memory. Adding more physical memory will allow the computer to run faster, but increasing the pagefile size is an acceptable short-term solution.

QUESTION 297
A system administrator has noticed that an employee's account has been attempting to log in to multiple workstations and servers across the network. This employee does not have access to these systems, and the login attempts are unsuccessful. Which of the following actions should the administrator do to this employee's account in Active Directory?

A. Disable the user's account
B. Reset the password of the user's account
C. Lock the user's account
D. Delete the user's account

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.1: The system administrator should disable the user's account to prevent further login attempts. The system administrator should notify security, who will investigate whether the employee or another malicious actor is taking the actions. An administrator can disable an account, but they cannot lock it. A lockout occurs when the preconhgured threshold for the number of failed login attempts is met. Resetting the password would not solve this issue, and deleting the account would remove the user and their files from the system.

QUESTION 298
Your Windows 10 machine has just crashed. Where should you look to identify the cause of the system crash and how to fix it?

A. MAC
B. POST
C. BSOD
D. DDOS

Correct Answer: C

Explanation

Explanation/Reference:
OBJ-3.1: A stop error, commonly called the blue screen of death, blue screen, or BSoD, is an error screen displayed on a Windows computer system following a fatal system error. It indicates a system crash, in which the operating system has reached a condition where it can no longer operate safely. Each BSOD displays a "stop code" that can research the cause of the error and how to solve it. A Media Access Control (MAC) address is a unique physical hardware address for each Ethernet network adapter that is composed of 12 hexadecimal digits. A Distributed Denial of Service (DDoS) at tack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. The Power On Self Test (POST) is a built-in diagnostic program that checks t he hardware to ensure the components required to boot the PC are present and functioning correct ! .

QUESTION 299
Which of the following commands can a technician use on a Linux server to verify the IP address associated with diontraining.com?

A. netstat
B. grep
C. dig
D. apt-get

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.1 1: The dig command is used to qllery the domain name system (DNS) to obtain information about host addresses, mail exchanges, nameservers, and related information. The netstat command is used to display the network statistics. The grep is a command-line utility for searching plain-text data sets for lines that match a regular expression. The grep command works on Unix, Linux, and macOS operating systems. Grep is an acronym that stands for Global Regular Expression Print. The apt-get utility is a powerful package management commandline program that works with Ubuntu's APT (Advanced Packaging l ool) library to install new software packages, remove existing software packages, upgrade existing software packages, and even upgrade the entire operating system. The apt-get utility works with Ubuntu and Debian-based Linux distributions.

QUESTION 300
Which of the following Control Panel sections would allow a technician to see which version and build of Windows 10 is installed on a computer?

A. Programs and Features
B. System
C. Device Manager
D. Devices and Printers

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .4: The System section of the Control Panel allows a technician to see information at>out the workstation, including the processor type, amount of memory, and operating system version installed on the computer. The Device Manager is used to view and cont rol the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it. The Prog rams and Features section of the Control Panel allows a technician to install or remove applications, software packages, and features in the Windows operating system. The Devices and Printers section of the Control Panel allows a technician to manage the printers, scanners, and other external devices connected to a Windows computer.

QUESTION 301
A user is attempting to pay for their morning coffee using Apple Pay on their iPhone. The user quickly taps their phone against the payment terminal, but it fails to process. Which of the f ollowing should the user do to properly use N FC for payment?

A. Turn on airplane mode and then try again
B. Hold the phone 5 inches above the payment terminal
C. Manually select a card from your Apple Wallet and try again
D. Hold the phone on the payment terminal for at least 3 seconds

Correct Answer: CD
Explanation

Explanation/Reference:
OBJ-3.4: NFC usually takes a few seconds to process when the phone is placed on the terminal, so quickly tapping may not work properly. Sometimes, even holding the phone next to the payment terminal won't work if the terminal's NFC reader hasn't properly detected Apple Pay. If you find that simply holding your phone up to the terminal doesn't work, try selecting a card manually. To do this, go into the Wallet app, then select the card you want to use. Near-Field Communication (NFC) is a set of communication protocols for communication between two electronic devices over a distance of 4 em or less. NFC offers a low-speed connection with a simple setup that can be used to bootstrap more capable wireless connections. NFC is used with payment systems like Apple Pay, Samsung Pay, and Google Pay since it supports two-way communication, unlike RFID which only supports one-way data transfers.

QUESTION 302
Dion Training is creating a new security policy that states all access to system resources will be controlled based on the user's job functions and tasks within the organization. For example, only people working in Human Resources can access employee records, and only the people working in finance can access customer payment histories. Which of the following policies or security practices is BEST described by this new policy?

A. Separation of duties
B. Mandatory vacation
C. Least privilege
D. Job rotation

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.1: Least privilege is a security policy that states someone or something should be allocated the minimum necessary rights, privileges, or information to perform the specific role. Separation of duties is a security policy that states that duties and responsibilities should be divided among individuals to prevent ethical conflicts or abuse of powers. Job rotation is a security policy that prevents any one individual from performing the same role or tasks for too long. Job rotation is useful in deterring fraud and providing better oversight of the person's duties. Mandatory vacation is a security policy that states when and how long an employee must take time off from work so that their activities may be subjected to a security review by having another employee conduct their job functions.

QUESTION 303
One of the routers in your network just failed. You have been asked to replace it with the same model router from the spare inventory closet as part of an emergency change request. You f ind the new router in the clloset and notice it was signed into inventory 13 months ago. You install the router and attempt to enable HTTPS in the configuration to allow for remote access. The failed router had this capability, but this spare does not, even though they are the same model and were purchased at the same time. What should you do to enable HTTPS access for this router?

A. Perform a factory reset
B. Update the firmware
C. Enable HTTP instead
D. Reboot the router

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.9: Since the new router was pulled from your spare inventory closet, it is likely using an older and out-ofdate version of the firmware. You should update the firmware for this router and then check if the HTTPS can be enabled again. Firmware updates to switches and routers provide both security updates and additional features that were not initially available. Since the device has been in the supply closet for 13 months, it is possible the HTTPS configuration was not included in the initial version and has been included in an updated firmware that was not applied to the spare router.

QUESTION 304
Which of the following commands is used on a Linux system to delete a f ile from a directory?

A. rm
B. kill
C. mv
D. Cp

Correct Answer: A
Explanation

Explanation/Reference:
OBJ- 1.11: The rm command is a command-line utility for removin9 files or directories. To remove a file, pass the name of a file or files to the rm command, and those files will be removed immediately from the file system. The cp command is a command-line utility for copying files and directories. It supports moving one or more files or folders with options for taking backups and preserving attributes. Copies of files are independent of the original fi le, unlike the mv command. The mv command is a command-line utility that moves files or directories from one place to anot her. The mv command supports moving single files, multiple files, and directories. The mv command can prompt before overwriting files and will only move files that are newer than the destination. When the mv command is used, the f ile is copied to the new directory and removed from the old directory. The kill command sends a signal to specified processes or process groups, causing them to act according to the signal. When the signal is not specified, it defa ults to -15 (-TERM), which terminates the specified process by gracefully stopping it. If "kill -9" is used instead, it will immediately kill the process.

QUESTION 305
Dion Training has an open wireless network so that their students can connect to the network d uring class without logging in. The Dion Training security team is worried that the customers from the coffee shop next door may be connecting to the wireless network without permission. If Dion Training wants to keep the wireless network open fo1r students but prevents the coffee shop's customers from using it, which of the following should be changed or modified?

A. Firewall
B. Default SSID
C. Signal strength or power level
D. MAC filtering

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: Since Dian Training wants to keep the wireless network open, the BEST option is to reduce the signal strength of the net work's power level. This will ensure the wireless network can only be accessed from within its classrooms and not from the coffee shop next door. Changing the SSID won't prevent the coffee shop 's customers from accessing the network. While MAC filt ering could be used to create an approved allow list of MAC addresses for all Dian Training's students, this would also require it to be continuously updated with each class of students that is very time-intensive and inefficient. Therefore, the BEST solution is to reduce the signal stren · th.

QUESTION 306
Barbara has connected her personal wireless router to a network jack inside her office. The router cannot get a DHCP address even though her corporate laptop can get a DHCP address when connected to the same jack. Barbara checked the router's configuration to ensure it is set up to obtain a DHCP address. Which of the following is the MOST likely reason that the router is not getting a DHCP address?

A. DHCP requests that. originate from access points are blocked
B. The wir·eless router's MAC address is blacklist by the network
C. Only allow listed MAC addresses can connect to the network
D. DHCP s1nooping is enabled on the network

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: Allow lists specify MAC addresses as a securit y measure implemented by the administrator to only grant access to a specific user. It avoids a person with malicious intentions to access the corporate network. Since the router has a different MAC address, it is blocked from connecting to the wired network. Allow listed MAC addresses can be implemented automatically using different forms of port security on a network switch.

QUESTION 307
Tim has requested to install a security update to the Dion Training web server during the next maintenance window. At the change control board meeting, Tim presents t he requested change and gains approval from the change board. Before Tim installs the update, which of t he following should be documented as a result of the change board's approval?

A. Risk level of the change
B. Date and time of the change
C. Affected systems/impact of the change
D. Purpose of the charnge

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.2: The approved date and time of t he change needs to be documented as a result of the change board's approval. The change board will approve all changes per the change management procedures in the organization. To get a change approved, a technician must submit a request form that lists the purpose of the change, the scope of the change, affected systems and impact of the change, the risk analysis and resulting risk level of the change, and the proposed date/time of the change. Once the change board approves the change at the change control board meeting, the technician or the change board needs to document the approved date and time for the change to be implemented.

QUESTION 308
What is the maximum amount of memory used in a 32-bit version of the Windows operating system?

A. 2GB

B. 1GB
C. 8GB
D. 4GB

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.1: A 32-bit operating system can only access up to 4GB of memory. Every byte of RAM requires its address, and the processor limits the length of those addresses. A 32-bit processor uses addresses that are 32 bits long. There are only 4,294,967,296, or 4GB, possible 32-bit addresses. This 4GB limit applies to the total system memory, so if the system has memory dedicated to the graphics, it is also considered a part of this 4GB total limit.

QUESTION 309
A user's workstation is infected with malware. You have quarantined it from the network. When you attempt to boot it to the Windows 10 desktop, it fails. Which of the following should you do NEXT to begin remediating this system?

A. Disable System Restore and reinstall Windows 10
B. Format the workstation and reinstall Windows 10
C. Restore the workstation from the last system restore point
D. Restart into Safe Mode and conduct an antivirus scan

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.3: The system should be rebooted into Safe Mode and an antivirus scan conducted. Safe Mode starts Windows in a bask state, using a limited set of files and drivers. If a problem doesn't happen in Safe Mode, then the default settin9s and basic device drivers aren't causing the issue. Observing Windows in safe mode enables you to narrow down the source of a problem and can help you troubleshoot problems on your PC. Safe Mode will allow you to restore an earlier System Restore point, but it will not allow you to disable System Restore. Restoring to the last system restore point may not restore the system to the time before the malware infection. Formatting and reinstalling Windows would lead to data loss for the user. Therefore, you should attempt to remediate the malware infection from Safe Mode first. The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected syst ems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 310
You are applying for a job at a cybersecurity firm. The application requests you enter your social security number, date of birth, and email address to conduct a background check as part of the hiring process. Which of the following types of information have you been asked to provide?

A. IP
B. PHI
C. Pll
D. CUI

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.6: Personally identifiable information (PII) is data used to identify, contact, or locate an individual.

Information such as social security number (SSN), name, date of birth, email address, telephone number, street address, and biometric data is considered PII. Protected health information (PHI) refers to medical and insurance records, plus associated hospital and laboratory test results. Proprietary information or intellectual property (IP) is information created and owned by the company, typically about the products or services that they make or perform. Cont rolled Unclassified Information (CUI) is federal non-classified information that must be safeguarded by implementing a uniform set of requirements and information security controls to secure sensitive government information.

QUESTION 311
You need to move a new desktop computer to another desk. Which of the following actions should you take?

A. Ask a coworker to team lift it with you
B. Lift with your legs and not your back
C. Lift with your back and not your legs
D. Open the box and carry each piece individually

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.4: You should always lift with your legs and not your back. The leg muscles are much stronger than the back muscles. If you carry heavy objects with your back, you will injure yourself. If the object is greater than 50 pounds, you should ask another coworker to assist you in a team lift to carry the object to prevent injury. Team lifting is when two or more peo ple work together to pick up a heavy or bulky object. When you need to lift or carry items, be aware of what your weight limitations are, as well as any restrictions and guidance outlined in your job descript ion or site safety handbook. Weight limitations will vary depending on context.

QUESTION 312
Dion Training uses DHCP to assign private Class C IP addresses to its Windows 10 workstations. Which of the following IP addresses is a Class C address?

A. 10.5.34.15
B. 192.168.2.14
C. 169.254.125.154
D. 172.16.13.12

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .6: Private I P addresses are any addresses in a specified range that are not allowed to be routed over the Internet. This allows companies to use these private IP addresses in their local area networks without having to purchase them from an internet registry. The class A private IP address range contains the addresses from 10.0.0.0 to 10.255.255.255.255. The class B private IP address range contains the addresses from 172.1 6.0.0 to 172.31.255.255. The class C private IP address range contains the addresses from 192.168.0.0 to 192.168.255.255. The APIPA/link- local autoconfiguration range is from 169.254.0.0 to 169.254.255.255.

QUESTION 313
Joseph contacted the service desk because his Windows 10 desktop is acting strangely. He cannot use his mouse, speakers, or printer connected to his workstation by USB. Yesterday, everything worked normally. He attempted to reboot the computer to fix the issue, but it remains. Which of the following actions should be performed NEXT?

A. Rollback any system updates or changes since yesterday
B. Rollback the printer's device driver in the Device Manager

C. Disable System Restore in Windows
D. Disable the Windows Update service to prevent future issues

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: Since the machine worked yesterday without any issues but is now having issues this morning, the workstation likely received a system update or security patch last night. Most corporate networks push patches and updates overnight to prevent disrupting users during the workday. Since the issue affects more than just the printer, rolling back the printer drivers would not fully solve this issue. Instead, any system updates or changes since yesterday should be rolled back to solve this issue.

QUESTION 314
Which of the following types of remote access technologies should NOT be used in a network due to its lack of security?

A. SSH
B. VPN
C. Telnet
D. RDP

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.9: Telnet should not be used in a network due to its weak security posture. Telnet transmits all of the data in plain text (without encryptiorn), including usernames, passwords, commands, and data files. For this reason, it should never be used in production networks and has been replaced by SSH in most corporate networks. Remote Desktop Protocol (RDP) is a Microsoft protocol designed to facilitate application data transfer security and encryption between client user devices and a virtual network server. It enables a remote user to add a graphical interface to the desktop of another computer. SSH (Secure Shell) is used to remotely connect to a network's switches and routers to configure them securely. SSH is typically used for logging into a remote machine and executing commands, but it also supports tunneling, forwarding TCP ports, and X11 connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model. A remote-access VPN connection allows an individual user to connect to a private network from a remote location using a laptop or desktop computer connected to the internet. A remote-access VPN allows individual users to establish secure connections with a remote computer network. Once established, the remote user can access the corporate network and its capabilities as if they were accessing the network from their own office s aces.

QUESTION 315
Dion Consulting Group has been hired by a large security operations center (SOC) to build a Windows 2019 domain environment. The SOC has a total of 150 Windows 10 Professional edition workstations that will connect to the domain for authentication, administration, and access to networked resources. Which of the following types of network models is being used by this security operations center in the domain environment?

A. Client/server
B. Hub-and-spoke
C. Mesh
D. Peer-to-peer

Correct Answer: A
Explanation

Explanation/Reference:

OBJ-1.1: A domain is a Microsoft client/server network model that groups computers together for security and to centralize administration. Domain members have access to a central user account database so that users can log on to any computer within the domain. A workgroup is a Microsoft peer-to-peer network model in which computers are connected together with access to shared resources for organizational purposes. Hub-and-spoke and mesh are networking models that are not used for workgroups or domains.

QUESTION 316
Which of the following commands is used on a Linux system to terminate an unresponsive system process?

A. kill
B. ls
C. grep
D. Ps

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .11: The ki ll command sends a signal to specified processes or process groups, causing them to act according to the signal. When the signal is not specified, it defaults to -15 (-TERM), which terminates the specified process by gracefully stopping it. If "kill -9" is used instead, it will immediately ki ll the process. The ls command lists the f iles or directories in the current path of a Unix, Linux, or Mac operating system. When invoked without any arguments, ls lists the files in the current working directory. The ps command is used to list the currently running processes, and their PIDs and some other information depend on different options. It reads the process information from the virtual files in the /proc file system. The / proc directory cont ains virtual f iles and is known as a virtual file system. The grep is a command-line utility for searching plain-text data sets for lines that match a regular expression. The grep command works on Unix, Linux, and macOS operating systems. Grep is an acronym that stands for Global Regular Expression Print.

QUESTION 317
Your companies share drive has several folders that have become encrypted by a piece of ransomware. During your investigation, you found that only the Sales department folders were encrypted. You continue your investigation and find that a salesperson's workstation was also encrypted. You suspect that this workstation was the original source of the infection. Since it was connected to the Sales department share drive as a mapped S:\ drive, it was also encrypted. You have unplugged the network cable from this workstation. What action should you perform NEXT to restore the company's network to normal operation?

A. Schedule a full disk anti-malware scan on the workstation
B. Restore the Sales department folders from backups
C. Schedule weekly scans and enable on-acc,ess scanning
D. Disable System Restore on the workstation

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.3: Since the share drive affects multiple users, not just t his one salesperson, it should be prioritized for recovery first. Sinoe the workstation has been quarantined from the network, it is no longer a threat to the shared drive dat a. Therefore, you should restore the latest backup of the Sales folders to the share drive. This will enable the rest of the Sales department to get back to normal operat ions. Then, you should focus on remediating this workstation. The next step for that remediation would be to disable System Restore, remediate the infected workstation by updating the anti-malware software, and conduct scans. The seven steps of the malware removal procedures are (1) Invest igate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 318
A user has reported that their workstation is running very slowly. A technician begins to investigate the issue and notices a lot of unknown processes running in the background. The technician determines that the user has recently downloaded a new application from the internet and may have become infected with malware. Which of the following types of infections does the workstation MOST likely have?

A. Trojan
B. Keylogger
C. Rootkit
D. Ransomware

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.3: A trojan is a type of malware that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. The most common form of a trojan is a Remote Access Trojan (RAT), which allows an attacker to control a workstation or steal information remotely. To operate, a trojan will create numerous processes that run in the background of the system. Ransomware is a type of malware designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Once infected, a system or its files are encrypted, and then the decryption key is withheld from the victim unless payment is received. A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. A rootkit is generally a collection of tools that enabled administrator-level access to a computer or network. They can often disguise themselves from detection by the operating system and anti-malware solutions. If a rootkit is suspected on a machine, it is best to reformat and rei mage the system. A keylogger actively attempts to steal confidential information by capturing t he data when entered into the computer by the user. This is done by recording keystrokes entered into a web browser or other application. A software keylogger can be run in the background on a victim's computer. A hardware keylogger may be placed between the USB port and the wired keyboard.

QUESTION 319
Tony works for a company as a cybersecurity analyst. His company runs a website that allows public postings. Recently, users have started complaining about the website having pop-up messages asking for their username and password. Simultaneously, your security team has noticed a large increase in the number of compromised user accounts on the system. What type of attack is most Ukely the cause of both of these events?

A. Cross-site request forgery
B. Rootkit
C. Cross-site scripting
D. SQL injection

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.4: This scenario is a perfect example of the effects of a cross-site scripting (XSS) attack. If your website's HTML code does not perform input validation to remove scripts that may be entered by a user, t hen an attacker can create a popup window that collects passwords and uses that information to compromise other accounts further. A cross-site request forgery (CSRF) is an attack that forces an end user to execute unwanted actions on a web applicat ion in which they are currently authenticated. An XSS will allow an attacker to execute arbitrary JavaScript within the victim's browser (such as creating pop-ups). A CSRF would allow an attack to induce a victim to perform actions they do not intend to perform. A rootkit is a set of software tools that enable an unauthorized user to control a computer system without being detected. SQL injection is the

placement of malicious code in SQL statements via web page input. None of the things described in this scenario would indicate a CSRF, rootkit, or SQL injection.

QUESTION 320
Dion Training has several Windows 10 Professional workstations with an internal 2 TB hard disk drive. The company wants to use full disk encryption to protect the contents of this hard drive. Which of the following security settings can be used to encrypt this storage device?

A. Bitlocker to Go
B. Bitlocker
C. Encrypting File System
D. FileVault

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.5: Bitlocker performs full disk encryption of the internal hard drive or solid-state device on a Windows 10 system. Bitlocker to Go performance fu ll disk encryption of external storage devices such as external hard drives and flash drives. The encrypting file system (EFS) is used in NTFS to encrypt files or folders to ensure the privacy of the data. EFS encrypted files can only be opened by the user who encrypted them. FileVault is a full disk encryption program used in the macOS environment.

QUESTION 321
A technician wants to conduct a vulnerability scan on a server ,every morning at 3:00 am. Which of the following tools should the technician use?

A. Task scheduler
B. Event viewer
C. MSConfig
D. PerfMon

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .3: Task scheduler is a tool included with Windows that allows predefined actions to be automatically executed whenever a certain set of conditions is met. For example, you can schedule a task to run a vulnerability scanning script every night or send you an email whenever a certain system event occurs. The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It 's a useful tool for troubleshooting all kinds of different Windows problems. If you use the Event Viewer, you can identify what was occurring at or around 2:35 am each day before the server crashed and use this to troubleshoot the problem. MSConfig is a system utility to t roubleshoot the Microsoft Windows startup processes MSConfig is used to disable or re-enable software, device drivers, and Windows services that run at startup, or to change boot parameters. PerfMion is a performance monitoring and system monitoring utility in Windows that is used to monitor the activities on CPU and memory activity on a computer. Performance monitor i's used for viewing performance data either in real -time or f rom a log file. The performance monitor can only monitor the resource utilization, but it cannot manage or terminate those processes.

QUESTION 322
You have been asked to recycle 20 of your company's old laptops. The laptops will be donated to a local community center for underprivileged children. Which of the following data destruction and disposal methods is MOST appropriate to allow the data on the drives to be fully destroyed and the drives to be reused by the community center?

A. Degaussing of the HODs

B. Standard formatting of the HODs
C. Low-level formatting of the HODs
D. Drill/hammer the HOD platters

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.8: Low-level formatting is a hard disk operation that should make recovering data from your storage devices impossible once the operation is complete. It sounds like something you might want to do if giving away a hard disk or discarding an old computer that may have contained useful and important private information. Standard formatting of the drives could allow the data to be restored and make the data vulnerable to exposure. Drilling or hammering the HDD platters would physically destroy the drives and the data, making the laptops useless for the community center. Degaussing the drives would also render the drives useless to the community center. Therefore, the safest method is a low-level format since it fu lly destroys the data and allows the drives to be reused by the community center.

QUESTION 323
A user reports that every time they try to access https://www.diontraining.com, they receive an error stating "Invalid or Expired Security Certificate." The technician attempts to connect to the same site from other computers on the network, and no errors or issues are observed. Which of the following settings needs to be changed on the user's workstation to fix the "Invalid or Expired Security Certificate"' error?

A. User access control
B. Logon times
C. Date and time
D. UEFI boot mode

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.1: There are two causes of the "Invalid or Expired Security Certificate." The first is a problem with your computer, and the second occurs when the certificate itself has an issue. Since the technician can succ·essfully connect to the website from other computers, it shows that the error is on the user's computer. One of the common causes of an Invalid or Expired Security Certificate error is the clock on the user's computer being wrong. The website security certificates are issued to be valid within a given date range. If the certificate's date is too far outside the date on the computer, the web browser will give you an invalid security certificate error because the browser thinks something is wrong. To fix this, set the computer's clock to the correct date and time.

QUESTION 324
You are trying to open your company's internal shared drive from your Windows 10 laptop but cannot reach it. You open your web browser and can connect to DionTraining.com without any issues. Which of the following commands should you use to determine if the internal shared drive is mapped to your computer properly?

A. tracert
B. net use
C. ping
D. Chkdsk

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.2: The net use command is used to connect to, remove, and configure connections to shared resources

such as mapped drives and network printers. For example, "net useS: \\SERVER\DATA /persistent:yes" would map the DATA folder on the SERVER to your localS: drive on a Windows computer. The chkdsk command is used to check the file system and file system met adata of a volume for logical and physical errors. The ping command is used to test a host's reachability on an Internet Protocol network. The t racert (trace route) diagnostic utility determines the route to a destination by sending Internet Control Message Protocol (ICMP) echo packets to the destination.

QUESTION 325
What does the command "shutdown l r" do on a Windows workstation?

A. Log off the workstation
B. Reboot the workstation
C. Enter sleep mode
D. Shutdown the workstation

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .2: The shutdown command allows a user or administrator to shut down or restart local or remote computers, one at a time. Using the /r option will reboot the computer. Using the /s option will shut down the computer. Using the /l option will log off the current user. Using the /h option will enter sleep or hibernation mode.

QUESTION 326
Sam and Mary both work in the accounting department and use a web-based SaaS product as part of their job. Sam cannot log in to the website using his credentials from his computer, but Mary can log in with her c1redentials on her computer. Sam asks Mary to login into her account from his computer to see if the problem is with his account or computer. When Mary attempts to log in to Sam's computer, she receives an error. Mary noticed a pop-up notification about a new piece of software on Sam's computer when she attempted to log in to the website. Which TWO of the following steps should Mary take to resolve the issue with logging in from Sam's computer?

A. Have Sam attempt to log on to another website from Sam's computer to see if it works
B. Verify Sam's computer has the correct web browser configuration and settings
C. Ask Sam about the pop-up notification and determine what new programs he installed on his computer
D. Have Sam clear his browser cache on his computer and then attempt to log on to the website again
E. Ask Sam for his username/password to log on to the website from Mary's computer
F. Install a new web browser, reboot Sam's computer, and attempt to log on to the website again from Sam's computer

Correct Answer: BC
Explanation

Explanation/Reference:
OBJ-3.2: Since Mary was able to log in to the website from her computer but not from Sam's, this indicates an issue with Sam's computer and/or web browser. The pop-up notification about the new program being installed indicates that something exists on Sam's computer that doesn't exist on Mary's computer. Therefore, it could be the cause and should be investigated further. Additionally, the browser's configuration should be checked to ensure the correct settings are being used.

QUESTION 327
A coworker is creating a file containing a script. You look over their shoulder and see "net use s:\ \fileserver\videos" in the file. Based on this, what type of file extension should this script use?

A. .vbs

B. .bat
C. .js
D. . py

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.8: Batch scripts run on the Windows operating system and, in their simplest form, contain a list of several commands that are executed in a sequence. A .bat file is used for a batch script. You can run the file by calling its name from the command line or double- clicking the file in File Explorer. Generally, batch file scripts run from end to end and are limited in branclhing and user input. Python is a general-purpose programming language that can develop many different kinds of applications. It is designed to be easy to read, and the programs use fewer lines of code compared to other programming languages. The code runs in an interpreter. Python is preinst alled on many Linux distributions and can be installed on Windows. Python scripts are saved using the .py extension. JavaScript is a scripting language that is designed to create interactive web-based content and web apps. The scripts are executed automatically by placing the script in the HTML code for a web page so that when the HTML code for the page loads, the script is run. JavaScript is stored in a Js file or as part of an HTML file. VBScript is a scripting language based on Microsoft's Visual Basic programming language. Network administrators often use VBScript to perform repetitive administrative tasks. With VBScript, you can run your scripts from either the command-line or the Windows graphical interface. Scripts that you write must be run within a host environment. Windows 10 provides Internet Explorer, liS, and Windows Script Host (WSH) for this purpose.

QUESTION 328
A user has asked you for a recommendation for a word processing program for their home computer. The user doesn't want to pay for a license to be able to use the word processor. Based on this, what type of license would you recommend to the user?

A. Corporate license
B. Personal license
C. Open license
D. Enterprise license

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.6: An open license or free license is the legal statement that allows free content and free software to be f ree. Since the customer doesn't want to pay for a license, the user must get a word processing program that uses an open license to not pay for their software. For example, OpenOffice is an open license-based software that provides a word processor that can be used on Windows, Linux, or OS X for free. A Personal license is an option for private individuals who purchase a license with their own funds and solely for their own use. Personal licenses are not to be purchased, refunded, or in any way financed by companies. A business license is the standard licensing option for organizations and business entities. With Microsoft, a company can purchase anywhere from 1 to 300 user licenses under the business license program. An enterprise license is like a business license, but for an unlimited number of users and is designed for large corporate and government networks.

QUESTION 329
Which of the following could be used to meet regulatory compliance requirements associated with the monitoring of employee actions on their work computer by providing a customizable dialog box wit h a textual warning to the user before they log in to their Windows 10 workstation?

A. Splash screen
B. Change request form

C. Request form
D. Chain o·f custody

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.1: A splash screen or interactive login screen is a graphical co ntrol element consisting of a window containing an image, a logo, or textual content. In Windows 10, system administrators can configure the textual content of the interactive logon dialog box to display a warning or the terms of an acceptable use policy to meet regulatory requirements. This interactive log on dialog is commonly used by organizations to notify their employees that they are subject to monitoring while using their work computers.

QUESTION 330
Dion Training uses a patch management server to control the distribution and installation of security patches. A technician needs to configure a new Windows 10 workstation to not perform Windows Updates automatically. Which of the following fea1tures in the Task Manager should the technician use to disable the Windows Update service?

A. Services
B. Performance
C. Startup
D. Processes

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.3: The task manager is an advanced Windows tool that has 7 tabs that are used to monitor the Processes, Performance, App History, Startup, Users, Details, and Services on a computer. By clicking the Services tab, the technician can list all of the services installed on the computer, display their status, and start/ stop/restart those services. The Processes tab in the task manager is helpful to quickly see how system resources are utilized, help troubleshoot applications, or find out why the computer is performing slowly. The task manager can identify and stop processes that use excessive system resources and keep the computer operating at higher speeds. By clicking the Startup tab, the technician can see every program configured to start up when Windows is booted up. Tlhis can be used to disable unwanted programs from launching during the boot-up process. By clicking the Processes tab, the technician can manage and terminate running apps and services.

QUESTION 331
Which of the following is required for evidence to be admissible in a court of law?

A. Order of volatility
B. Chain of custody
C. Right to audit
D. Legal hold

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.6: Chain of custody forms list every person who has worked with or who has touched the evidence that is a part of an investigation. These forms record every action taken by each individual in possession of the evidence. Depending on the organization's procedures, manipullation of evidence may require an addit ional person to act as a witness to verify whatever action is being taken. A legal hold is a process that an organization uses to preserve all forms of potentially relevant information when litigation is pending or

reasonably anticipated. A right to audit is a clause in a contract or service agreement that allows a company the authority to audit the systems and information processed. Order of volatility refers to the order in which you should collect evidence.

QUESTION 332
A user's workstation is opening up browser windows without any action from the user. A technician attempts to troubleshoot the workstation, but the machine is extremely slow when in use. Which of the following actions should the technician perform?

A. Enable the pop-up blocker in the web browser
B. Format and reinstall the operating system
C. Update the Windows operating system
D. Perform an anti-ma1lware scan of the workstation

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.2: Based on the symptoms of the pop-up windows occurring without any user action, this indicates a virus or other malware infection on the workstation. Therefore, the technician should perform an anti-malware scan of the workstation to identify the infection's source and then remediate it. If the pop-ups were occurring as the user was browsing the internet, t hen enabling the pop-up blocker in the web browser would be the first step to take. Updating the Windows operating system would not remove malware that already exists on the system. Formatting and re1i nstalling the operating system would solve this issue, but it would also erase all of the user's applications, data, and configuration settings so it is not the best action to attempt first.

QUESTION 333
Which command-line tool in Windows would you use to end one or more processes that have begun hung on the system?

A. gpupdate
B. sfc
C. net use
D. taskkill

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.2: The taskkill command is used to end one or more tasks or processes on a Windows system. Processes can be ended by process ID or image name. You can use the tasklist command to determine the process ID (PI D) for the process to be ended. The system file checker (SFC) command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from t he command line. The net use command is used to connect to, remove, and configure connections to shared resources such as mapped drives and network printers. The gpupdate command-line tool is used to update the group policy settings on a Windows system. For an administrator to force a background update of all Group Policy settings regardless of whether they have changed, they need to run "gpupdate /force" from the command line.

QUESTION 334
You noticed that your personal files in your Dropbox had been accessed while you were sleeping. Which of the following threats is this an example of?

A. Unauthorized location tracking
B. Unauthorized microphone activation
C. Unintended Bluetooth pairing
D. Unauthorized account access

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.5: Unauthorized account access can give users access to personal files and data they should not have access to. Therefore, you should closely monitor your account usage. When files are accessed without authorization from your cloud storage service, it can lead to the leaking of your personal files and data. When anonymous devices are allowed to connect to Bluetooth-enabled devices, this is known as unintended Bluetooth pairing, and it represents a security threat. Mobile security policies should be created and enforced that prevent this from occurring. The microphone can be activated remotely and allow a t roublemaker to spy on you. It is suggested that, when not in aut horized use, you cover the microphone of your device to keep them from providing any data if remotely accessed. While location-based data can be valuable when using maps and trying to find sites, it can also give away sensit ive information if accessed by someone who should not have it. You can optimize your battery life and protect yourself by turning off Location Services. On an iPhone, t urn it off in Settings > Privacy > Location Services. There you will see each app listed along with its permission setting. Apps that recent ly used locat ion services have an indicator next to the on/off switch, and you can configure them accordingly.

QUESTION 335
You need to determine the best way to test operating system patches in a lab environment befo re deploying them to your automated pa1tch management system. Unfortunately, your network has several different operating systems in use, but you only have one machine available to test the patches on. What is the best environment to utilize to perform the testing of the patches before deployment?

A. Virtualization
B. Sandboxing
C. Purchase additional workstations
D. Bypass testing and deploy patches directly into the production environment

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.2: When you have a limited amount of hardware resources to utilize but have a requirement to test multiple operating systems, you should set up a virtualized environment to test the patch across each operating system before deployment. You should never deploy patches directly into production without testing them f irst in the lab. Virtualization will allow the organization to create a lab environment without significant costs. Purchasing additional workstations would be costly and more time-consuming to configure.

QUESTION 336
Jason checks the Dion Training server room and finds that it currently has over 80% humidity. Which of the following risks to the servers could occur due to this high humidity level?

A. An over-voltage event
B. Corrosion of the servers
C. Accidental static discharge
D. An under-voltage event

Correct Answer: B
Explanation

Explanation/Reference:
Expla nation
OBJ-4.5: When humidity is high, corrosion is the biggest threat. When humidity is high, the water in the air can react with the components in the servers and cause corrosion. When humidity is low, static electricity is built up and can lead to an accidental release which damages components. In a computer server room or work area,

the humidity should be kept between 40-60% to prevent electrostatic d ischarge from low humidity and corrosion from high humidity. An electrostatic discharge (ESD) is the release of a charge from metal or plastic surfaces that occurs when a potential difference is formed between the charged object and an oppositely charged conductive obj ect. This electrical discharge can damage silicon chips and computer components if they are exposed to it.

QUESTION 337
Your Windows 10 system is booting up very slowly. Which of the following should you do to speed up the boot process?

A. Reboot the system into Safe Mode
B. Rebuild your Windows profile
C. Disable unnecessary programs from automatically starting up
D. Reinstall! Windows

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.1: While many of these solutions may decrease the boot time, the first t hing to attempt is to disable unnecessary applications from automatically starting up. System configuration (msconfig .exe) is a system utility to troub leshoot the Microsoft Windows startup processes. MSConfig is used to disable or re-enable software, device d rivers, and Windows services that run at startup, or to change boot parameters. The task manager is an advanced Windows tool that has 7 tabs that are used to monitor the Processes, Performance, App Hist ory, Startup, Users, Details, and Services on a computer. By clicking the Startup tab, the technician can see every program configured to start up when Windows is booted up. This can be used to disable unwanted programs from launching d uring the boot-up p rocess.

QUESTION 338
Which of the following data types would be used to store the number 3.14?

A. Integers
B. String
C. Boolean
D. Floating-point

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.8: A float ing- point number stores a fractional or decimal number, such as 3.14, 45.5, or 333.33. A floating point number data type usually consumes 4 to 8 bytes of storage. An integer stores a whole number, such as 21, 143, or 1024. An integer data type usually consumes 8 bytes of storage. A boolean stores a value of TRUE (1) or FALSE (0). It usually consumes only 1 bit of storage (a zero or a one). A st ring stores a group of characters, such as Hello, PYTHON, or JasonDion. A string data type usually consumes as much storage as necessary. Each character in t he string usually requires 1 byte of storage.

QUESTION 339
You are configuring a wireless access point (WAP) in a large apartment building for a home user. The home user is concerned that their neighbor may try to connect to their Wi-Fi and wants to prevent it. Which THREE of the following actions should you perform to increase the wireless network's security?

A. Disable the SSID broadcast
B. Enabled WEP encryption
C. Enable WPA3 encryption
D. Disable the DHCP server

E. Reduce the channel availability
F. Reduce the transmission power

Correct Answer: ACF
Explanation

Explanation/Reference:
OBJ-2.9: To BEST secure this wireless network in a large apartment building, you should first reduce the t ransit power. This will ensure t he network's radio frequency signals remain within the apartment itself. You should then disable the SSID broadcast since this will prevent the home user's neighbor from seeing t he network as available. Finally, the home user should use WPA3 encryption since it is the strongest encryption method for Wi-Fi networks. Reducing the channel availability would minimize the bandwidth available for t he users. Disabling the DHCP server will prevent users from automatically getting their IP configuration settings when connecting to the network. WEP is considered a weak form of encryption and should not be used.

QUESTION 340
Which of the following is the purpose of an ESD mat?

A. Protects equipment against accidental static discharge
B. Protects equipment from dust or dirt
C. Protects the technician from accidental shocks
D. Protects casings from scratches and dents

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.4: An electrostatic discharge (ESD) mat is made from materials that dissipate static to protect sensitive electronic equipment and components. An electrostatic discharge (ESD) is the release of a charge from metal or plastic surfaces that occurs when a potential difference is formed between the charged object and an oppositely charged conductive object. This electrical discharge can damage silicon chips and computer components if they are exposed to it.

QUESTION 341
Which of the following commands would a technician use to find the comprehensive documentation for any command from the Linux terminal?

A. yum
B. grep
C. man
D. apt-get

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1 .1 1: The man command in Linux is used to display t he user manual of any command from the terminal. The grep is a command-line utility for searching plain-text data sets for lines that match a regular expression. The grep command works on Unix, Linux, and macOS operating systems. Grep is an acronym that stands for Global Regu1lar Expression Print. The apt-get utility is a powerful package management command-line program that works with Ubuntu's APT (Advanced Packaging Tool) library to install new software packages, remove existing software packages, upgrade existing software packages, and even upgrade the entire operating system. The aptget utility works with Ubuntu and Debian-based Linux distributions. The yum command is a package manager used with RPM-based Linux distributions to install new software packages, remove existing software packages, upgrade existing software packages, and even upgrade the entire operating system.

QUESTION 342
Your router has been turning itself off and on again for a few weeks. You begin to think back to when these issues began to occur and remember that each time it happened the lights also dimmed momentarily. You hook up a device to monitor the power being supplied to the router and identify that brownouts are frequently occurring, resulting in the router's power cycling. What should you (a network technician) do to solve t his problem?

A. Install an upgraded 1router
B. Install a new electrical outlet
C. Install a UPS
D. Install a surge protector

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.5: The best solution would be to install a UPS. Since you are a network technician and not an electrician, you should not install a new electrical circuit. The primary funct ion of UPS is to provide battery backup when the electrical power fails or drops to an unacceptable voltage level. It ensures that your electrical equipment gets a consistent current so damage and device power cycling do not occur. A surge protector defends against possible voltage spikes that could damage your electronics, appliances, or equipment. A network technician is not qualified to install a new electrical outlet since that is a j ob for an electrician. The scenario presents issues that focus on the power levels, therefore installing an upgraded router would not solve these issues.

QUESTION 343
Marta's organization is concerned with the vulnerability of a user's account being vulnerable for an extended period of time if their password was compromised. Which of the following controls should be configured as part of their password policy to minimize this vulnerability?

A. Minimum password length
B. Password complexity
C. Password expiration
D. Password history

Correct Answer: C
Explanation

Explanation/Reference:
Explanat ion
OBJ-2.6: A password expiration control in the policy would force users to change their passwords at specific time intervals. This will t hen locks out a user who types in the password or create an alter that the user's account has been potentially compromised. While the other options are good components of password security to prevent an overall compromise, they are not effective against the vulnera bility described in this particular scenario. It states the issue is based on time. Password history is used to determine t he number of unique passwords a user must use before using an old password again. The Passwords must meet complexity requirements policy setting determines whether passwords must meet a series of guidelines that are considered important for a strong password. Maximum password length creates a limit to how long the password can be, but a longer password is considered strong·er against a brute force attack.

QUESTION 344
A user's computer was running out of storage space, so they decided to install a new second 1 TB hard disk drive (HOD) into their Windows 10 computer. Whenever they attempt to boot up the computer, an error' of "No Operating System Found" is displayed on their screen. You unplugged the new 1 TB HOD, and then the computer boots up without any errors. You have just reconnected the 1 TB HOD. What step should you attempt NEXT to fix this issue?

A. Reboot the computer into safe mode
B. Format the 1 TB HOD
C. Verify the boot order in the BIOS/UEFI
D. Reinstall Windows to the 1 TB HOD

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.1: If more than one hard drive is connected to the computer, it is important to verify the correct boot order is listed in the BIOS/UEFI. In this scenario, it sounds like the system is configured to boot fi rst from the 1 TB HDD and then from the original HDD. If this order is switched in the boot order, the system will boot without generating the error message. Formatting the HDD will not solve this problem since a formatted drive does not have an operating system installed by default. Rebooting the computer into safe mode will not work either, since the 1 TB HDD doe.s not have an operating system installed. There is no need to reinstall Windows to the 1 TB HDD since this drive will only be used for file storage, therefore the boot order should be changed to boot from the older HDD first.

QUESTION 345
You are concerned that your servers could be damaged during a power failure or under-voltage event. Which TWO devices would protect against these conditions?

A. Surge suppressor
B. Battery backup
C. Grounding the server rack
D. Line conditioner

Correct Answer: BD
Explanation

Explanation/Reference:
OBJ-4.5: A power lloss or power fa ilure is a total loss of power in a particular area. An under-voltage event is a reduction in or restriction on the availability of electrical power in a particular area. The irregular power supply during the under-voltage event can ruin your computer and other electronic devices. Electronics are created to operate at specific voltages, so any fluctuations in power (both up and down) can damage them. To protect against an under-voltage event, you can use either a battery backup or a line conditioner. To protect against a power loss or power failure, a battery backup or generator should be used. Therefore, the best answer to this question is a battery backup and a line conditioner.

QUESTION 346
You are working for a brand new startup company that allows you to use your laptop, tablet, or other devices while at work. The company does provide some rules and guidelines that you must follow based on their policy. Which of the following policies should you look at to ensure you understand these rules and guidelines?

A. SLA
B. NDA
C. MOU
D. BYOD

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.7: BYOD (Bring Your Own Device) refers to the policy of permitting employees to bring personally owned devices to their workplace and to use those devices to access privileged company information and

applicat ions. A memorandum of understanding (MOU) is important because it defines the responsibilities of each party in an agreement, provides the scope and authority of the agreement, clarifies terms, and outlines compliance issues. A non-disclosure ag reement (NDA) is a legal contract or part of a contract between at least two parties that outlines confident,ial material, knowledge, or informat ion that the parties wish to share for certain purposes, but wish to restrict access to. A service level agreement (SLA) is a commitment between a service provider and a client for particular aspects of the service, such as quality, availability, or responsibilit ies.

QUESTION 347
A user contacts the service desk after they just finished attempting to upgrade their laptop to Windows 10. The upgrade failed, and the user asks you to explain why. Which of the following log files should you review to determine the cause of the upgrade failure?

A. Application log
B. Security log
C. System log
D. Setup

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.1: The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems. The setup log contains a record of the events generated during the Windows installation or upgrade process. The file (setup.evtx) is sto r~ed in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The application log contains information regarding applicat ion errors. The file (application.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The system log contains information about service load failures, hardware conflicts, driver load failures, and more. The fi le (system.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The security log contains information regarding audit data and security on a system. For example, the security log contains a list of every successful and failed login attempt. The file (security.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer.

QUESTION 348
You have just installed a second monitor for a salesperson's workstation. The user wants to clone the display so that both monitors show the exact same image. This will allow them to see one of the displays while their customer sees the other from across their desk. When you connect the second monitor and clone the display. the second monitor displays text twice as large as the other monitor. Which of the following settings should you configure?

A. Extended mode
B. Resolution
C. Refresh rate
D. Color depth

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.1: Most mo11itors have a default or native resolution. When you first connect a monitor to a Windows workstation, this native resolution is detected, and Windows attempts to configure itself automatically. If this creates an imbalance between the two monitors, a technician can adjust the screen's resolution by changing it in the Display settings area of Windows 10. Color depth defines how many unique colors can be displayed by the projected image at once. Refresh rate is the measure of how fast an image can be updated on a monitor or display. If a monitor has a lower refresh r.ate, then blurring and ghosting can occur. The extended mode allows

the Windows output to be stretched across two or more monitors as if they were a single· monitor. This can be configured under the Display settings in Windows 10.

QUESTION 349
Which of the following types of installations would you use on a system with slow performance or one that you cannot isolate a single cause of the system's issues?

A. Image deployment
B. In-place upgrade
C. Repair installation
D. Remote network installation

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.9: Repair installation is a type of installation that attempts to replace the existing version of the o perating system files with a new copy of the same version. A repair installation is useful when trying to repair a Windows computer that will not boot or when you believe the system files have become corrupted. An image deployment is a type of installation that use·s a clone of an existing installation stored in an image file to perform the installation. The image can contain the base OS and configuration settings, service packs and updates, applications software, and whatever else is required. An image can be stored on DVD or USB media or can be accessed over a network. A remote network installation connects to a shared folder containing the installation fi les. During the remote network installation, the target PC will boot to a Preboot eXecution Environment (PXE) and then copy the files to a temporary location on its hard drive before fully installing them to the target PC. Most commonly, a remote network installation will be combined with an image deployment for a more efficient installation across the network. An in-place upgrade is an installation of the new operating system on top of an existing version of the operating system. An in-place upgrade will preserve the applications, user settings, and data files that already exist on the computer.

QUESTION 350
The administrator would like to use the strongest encryption level possible using PSK without utilizing an additional authentication server. What encryption type should be implemented?

A. WPA personal
B. WEP
C. MAC filtering
D. WPA2 Enterprise

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.2: Since he wishes to use a pre-shared key and not require an authentication server, WPA personal is the most secure choice. If WPA2 Personal were an option, it would be more secure, though. WPA2 Enterprise is since the requirement was for a PSK, whereas WPA2 Enterprise requires a RADIUS authentication server to be used with individual usernames and passwords for each client. MAC filtering does not use a password or preshared key. WEP uses a pre-shared key to secure a wireless network, but WPA uses a stronger encryption standard than WEP.

QUESTION 351
Which of the following commands is used to edit a text file on a Linux server?

A. grep
B. nano
C. pwd

D. Cat

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.11: The nano utility is an easy-to-use command-line text editor for Linux systems. Nano includes the functionality of a regular text editor, as well as syntax highlighting, multiple buffers, search and replace with regular expression support, spellchecking, UTF-8 encoding, and more. The cat (short for "concatenate") command is one of the most frequently used commands in Linux/Unix. The cat command allows the creation of single or multiple files, view file contents, concatenate files, and redirect out put in the terminal to a fi le. The grep is a command-line utility for searching plain-text data sets for lines that match a regular expression. The grep command works on Unix, Linux, and macOS operating systems. Grep is an acronym that stands for Global Regular Expression Print. The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen.

QUESTION 352
Which of the following commands is used on a Linux system to change the ownership of a file or directory on a system?

A. passwd
B. pwd
C. chown
D. Chmod

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1 .1 1: The chown command changes user ownership of a file, directory, or link in Linux. Every file is associated with an owning user or group. The chmod command sets the permissions of files or directories on a Linux system. A set of flags associated with each file determines who can access that file and how they can access it. These flags are called file permissions or modes. The command name chmod stands for change mode and it restricts the way a file can be accessed. The passwd command changes passwords for user accounts. A normal user may only change the password for their account, while the superuser may change the password for any user. The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen.

QUESTION 353
A user's personal settings are not showing up on their computer. You suspect that their profile has become corrupted within Windows. You attempt to look at their profile file but cannot find it in their profile directory. Which of the following options do you need to configure to see this file?

A. Folder Options
B. Display Settings
C. User Accounts
D. Internet Options

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: The File Explorer Options section of the Control Panel allows technicians to customize the display of files and folders. For example, the File Explorer Options can enable or disable the ability to show hidden files, hide file extensions, and more. General options allow a technician to configure the folders to open in a new

window or the same window, to use a single-click or double-click when opening a file or program using its icon, and the ability to show or hide re,cently used files and folders in the Quick Access pane of the File Explorer window. The View options tab allows more customized control in terms of hiding and displaying files and folders, as well as the customization of the File Explorer window. If you configure view hidden files, you will see system files such as the ntuser.dat file that are hidden from users by default. The Internet Options section of the Control Panel allows a technician to manage the Internet settings for their computers, including the security sett ings, access settings, and add-on control settings. The User Accounts section of the Control Panel allows technicians to add user accounts, remove user accounts, change account types, reset account passwords, and other settings relevant to user accounts and their security. Display settings are used to modify the resolution, color depth, clone/extended mode, and refresh rate of a monitor or display panel.

QUESTION 354
You are working at the service desk when you receive a call from an upset user because their workstation cannot receive any emails. Which of the following should you use to document this phone call?

A. Incident report
B. Asset management database
C. Network topology diagrams
D. Knowledge base articles

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.1: An incident report is used to document any issues, problems, or incidents in the network. Incident reports are often consolidated into an incident database known as a trouble ticket system. The system should document the number of the incident, the point of contact for the workstation, the priority of the incident, the problem description, and a history of work performed to resolve the incident for the user. An asset management database tracks the number of assets deployed, on order, and in storage. A Knowledge Base (KB) is a reference document that is used to assist a technician when they are installing, configuring, and troubleshooting hardware and software. A knowledge base article might be created by a vendor to support their products, too. A company might create an internal KB, po pulated with guidelines, procedures, information, and freq uently asked questions f rom their service tickets. A network topology is the shape or structure of a network in a physical or logical format as depicted in a network diagram. Physical network topologies include the actual appearance of the network layout. Logical network topologies include the flow of data across the network.

QUESTION 355
Your company's wireless network was recently compromised by an attacker who utilized a brute force attack against the network's PIN to gain access. Once connected to the network, the attacker modified the DNS settings on the router and spread additional malware across the entire network. Which TWO of the following configurations were most likely used to allow the attack to occur?

A. Router with outdated firmware
B. WPS enabled
C. WPA2 encryption enabled
D. Guest network enabled
E. Default administrative login credentials
F. TKIP encryption protocols

Correct Answer: BE
Explanation

Explanation/Reference:
OBJ-2.9: Wireless networks that rely on a PIN to connect devices use the Wi-Fi Protected Setup (WPS). It is a wireless network security standard that tries to make connections between a router and wireless devices faster

and easier. WPS relies on an 8-digit PIN, but it is easily defeated using a brute force attack due to a poor design. Once connected to the network using the WPS PIN, the attacker may have logged into the router using the default administrative login credentials and then modified the router/gateway's DNS. Commonly, many network administrators forget to change the default username/password of their devices, leaving an easy vulnerability for an attacker to exploit.

QUESTION 356
You are working in a doctor's office and have been asked to set up a kiosk to allow customers to check in for their appointments. The kiosk should be secured, and only customers to access a single appllication used for the check-in process. You must also ensure that the computer will automatically log in whenever the system is powered on or rebooted. Which of the following types of accounts should you configure for t his kiosk?

A. Administrator
B. Remote Desktop User
C. Guest
D. Power lJser

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.5: A Windows guest account will let other people use your computer without being able to change PC settings, install apps, or access your private files. A Guest account is a Microsoft Windows user account with limited capabilities, no privacy, and is disabled by default. An administrator account is a Microsoft Windows user account that can perform all tasks on the computer, including installing and uninstalling apps, setting up other users, and configuring hardware and software.

QUESTION 357
A technician is trying to locate a protected .dll file to edit, but they cannot see it in the System32 folder. Which Control Panel utility should the technician use to find the file?

A. Indexing Options
B. Programs and Features
C. File Explorer Options
D. System

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1 .4: The File Explorer Options section of the Control Panel allows technicians to customize the display of fi les and folders. For example, the File Explorer Options can enable or d isable the ability to show hidden files, hide file extensions, and more. General options allow a technician to configure the folders to open in a new window or the same window, to use a single-click or double-click when opening a file or program using its icon, and the ability to show or hide recently used files and folders in the Quick Access pane of the File Explorer window. The View options tab allows more customized control in terms of hiding and displaying files and folders, as well as the customization of the File Explorer window. The Indexing Options is used to configure the method used by Windows when searching for content within the storage devices. When indexing is properly configured, the system will catalog the information on the computer using the words within the files and their metadata to more easily find the content when requested by a user. The System section of the Control Panel allows a technician to see information about the workstation, including the processor type, amount of memory, and operating system version installed on the computer. The Programs and Features section of the Control Panel allows a technician to install or remove applications, software packages, and features in the Windows operating system.

QUESTION 358
Which command- line tool is used on a Windows system to display a list of the files and directories within the

current directory or path?

A. sfc
B. dir
C. ls
D. Chkdsk

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .2: The dir command is used to list a directory's files and subdirectories. If used without parameters, this command displays the disk's volume label and serial number, followed by a list of directories and files on the disk (including their names and the date and time each was last modified). For files, this command displays the name extension and t he size in bytes. This command also displays the total number of files and directories listed, their cumulative size, and the free space (in bytes) remaining on the disk. The ls command is used on a Linux system to list a directory's files and subdirectories. The ls command only works on a Windows system when you are using PowerShell, not the command lline. The system file checker (SFC) command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from the command line. The chkdsk command is used to check the file system and file system metadata of a volume for logical and physical errors. If used without parameters, chkdsk displays only the status of the volume and does not fix any errors. If used with the /f, /r, /x, or /b parameters, it fixes errors on the volume.

QUESTION 359
Which of the following will close all of a user's open programs and services before powering off their Windows 10 computer?

A. Lock
B. Hibernate
C. Sleep
D. Shutdown

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1 .4: The shutdown option will close all open prog rams and services before powering off the comput er. The user should save changes in any open files first but will be prompted to save any open files during shut down. Once powered down, the computer or laptop uses no energy. The time from a computer being fully shut down to returning to operations is longer than sleep or hibernate. Hibernate mode is used to save the current session to disk before powering off the computer to save battery life when the system is not being used. The computer takes longer to start up again from hibernate mode than it does from the sleep or standby mode. Sleep or standby mode is used to save the current session to memory and put the computer into a minimal power state to save battery life when the system is not being used. The computer takes less time to start up again from the sleep or standby mode than it does from the hibernate mode. A lock will secure the desktop with a password while leaving programs running without powering off the computer.

QUESTION 360
Jonni is installing Windows 11 (64-bit) in a virtual machine on his Linux desktop. The installation is continually failing and producing an error. Jonni has configured the virtual machine with a dual-core 1.2 GHz processor, 4GB of memory, a 32GB hard drive, and a 1920 x 1080 screen resolution. Which item in the virtual machine should be increased to fix the installation issue experienced?

A. Amount of memory
B. Amount of hard drive space
C. Number of CPU cores

D. The screen resolution

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.7: The amount of storage space needs to be increased. For the Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64GB of hard drive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space.

QUESTION 361
An ethical hacker has been hired to conduct a physical penetration test of a company. During the first day of the test, the ethical hacker dresses up like a plumber and waits in the building's main lobby until an employee goes through the main turnstile. As soon as the employee enters his access number and proceeds to go through the turnstile, the ethical hacker follows them through the access gate. What type of attack did the ethical hacker utilize to access the restricted area of the building?

A. Spoofing
B. Shoulder surfing
C. Social engineering
D. Tailgating

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.4: Based on t he description, the ethical hacker conducted a very specialized type of social engineering attack known as t ailgating. Sometimes on a certification exam, there are two correct answers, but one is more correct. This question is an example of that concept. Tailgating involves someone who lacks the proper authentication following an employee into a restricted area. Social engineering uses deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. Shoulder surfing is a type of social engineering technique used to obtain personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder. Spoofing is the act of disguising a communication from an unknown source as being fro m a known, trusted source.

QUESTION 362
Dion Training is looking to purchase Microsoft Office for all of its employees to use. Which of tlile following licenses would be BEST for this small company to purchase?

A. Enterprise
B. Personal
C. Business
D. Open-source

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.6: A business license is the standard licensing option for organizations and business entities. With Microsoft, a company can purchase anywhere from 1 to 300 user licenses under the business license program. An enterprise license is like a business license, but for an unlimited number of users and is designed for large corporate and government networks. A Personal license is an option for private individuals who purchase a license with their own funds and solely for their own use. Personal licenses are not to be purchased, refunded, or in any way financed by companies. Open source is software that also makes the program code used to design it available. Generally, open-source software is free to use and distribute, but

you may need to pay for ongoing support if you have technical issues. The idea is that other programmers can investigate the program and make it more stable and useful. An open-source license does not forbid commercial use of applications derived from the original, but it is likely to impose the same conditions on further redistributions.

QUESTION 363
You are installing a new wireless network in your office building and want to ensure it is secure. Which of the following configurations would create the MOST secure wireless network?

A. WPA2 and RC4
B. WPA and MAC filtering
C. WPA2 and AES
D. WEP and TKIP

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.2: The most secure wireless network configuration utilizes WPA2 with AES encryption. WPA2 is the most secure wireless encryption standard listed as an option and has replaced both WPA and WEP. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption. Wi- Fi protected access (WPA) is an improved encryption scheme for protecting Wi-Fi communications designed to replace WEP. WPA uses the RC4 cipher and a temporal key integrity protocol (TKIP) to overcome the vulnerabilities in the older WEP protection scheme. Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks that could probably break its encryption. WEP relies on the use of a 24-bit initialization vector to secure its preshared key. MAC filtering is the application of an access control list to a switch or access point so that only clients with approved MAC addresses connect.

QUESTION 364
Bradley has been authorized to work from home every Friday. Normally, he can use his work laptop home from home while still accessing the company's internal network shares, but for some reason, it isn't working today. What is MOS'f likely the cause of Bradley's issue today?

A. The corporate MOM policy
B. Missing OS security patches
C. An inactive VPN connection
D. Outdated anti-malware software

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.9: To connect from Bradley's home to the corporate internal network, Bradley would need to use a VPN connection. A VPN connection will create a secure tunnel from Bradley's laptop over the internet to the corporate internal network, which will make his laptop act as if he is connected directly to the office network. If the VPN connection is inactive, then Bradley's laptop is simply connecting directly to the internet and cannot access any of the company's internal network resources (like the network shares). Patch management is the process of distributing and applying updates to the software to prevent vulnerabilities from being exploited by an attacker or malware. Mobile device management (MDM) software suites are designed to manage the use of smartphones and tablets within an enterprise. Anti-malware software is a program that scans a device or network for known viruses, Trojans, worms, and other malicious software.

QUESTION 365

Jason is using a Windows 10 workstation in the Dion Training conference room. The workstation is acting extremely slow and he suspects there are other accounts logged on to the workstation. Which of the following features in the Task Manager should he use to identify if anyone else is currently logged on to the workstation?

A. Processes
B. Performance
C. Users
D. Services

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.3: The task manager is an advanced Windows tool that has 7 tabs that are used to monitor the Processes, Performance, App History, Startup, Users, Details, and Services on a computer. By clicking the Users tab, the technician can see a list of signed-in users and their running processes on the workstation. The Processes tab in the task manager is helpful to quickly see how system resources are utilized, help troubleshoot applications, or find out why the computer is performing slowly. The task manager can identify and stop processes that use excessive system resources and keep the computer operating at higher speeds. By clicking the Processes tab, the technician can manage and terminate running apps and services. By clicking the Services tab, the technician can list all of the services installed on the computer, display their status, and start/stop/restart those services.

QUESTION 366
John is setting up 100 Windows 10 computers for a new corporate office. He wants to ensure that no one can change the boot order and boot from an unauthorized operating system. What feature should he ensure is enabled?

A. BIOS password required
B. RAM integrity checking
C. Secure Boot
D. Full disk encryption

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.6: John should utilize the BIOS to set up a password to prevent unauthorized access to the Basic Input/Output System (BIOS) by other users. The BIOS is software that utilizes a small memory chip on the motherboard to hold the settings specialized for an organization to prevent access and tampering, thus reducing the workstations' overall attack surface and the network. Full disk encryption is used to encrypt the user and system data stored in the device's internal storage. RAM integrity checking is conducted by default on most systems during the initial boot process but it doesn't prevent a user from booting the system or changing the boot order. The purpose of Secure Boot is to prevent malicious and unauthorized apps from loading into the operating system (OS) during the startup process. Secure Boot is enabled by default in Windows 10. When the PC starts, the firmware checks the signature of each piece of boot software, including UEFI firmware drivers (also known as Option ROMs), EFI applications, and the operating system. If the signatures are valid, the PC boots and the firmware gives control to the operating system.

QUESTION 367
What is the minimum amount of hard drive space needed to install Windows 10 on a 64-bit system?

A. 20GB
B. 64GB
C. 16GB
D. 32GB

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .7: For the Windows 10 (64- bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For t he Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64 GB of hard drive space.

QUESTION 368
The Chief Financial Officer has asked Maria for a recommendation on how the company could reduce its software licensing costs while still maintaining the ability to access its application server remotely. Which of the following should Maria recommend?

A. Use a Virtual Network Client (VNC) on a Windows 2019 server
B. Install and deploy Windows 10 Home edition on each user's thick client
C. Use a Remote Desktop Protocol (RDP) application on a Windows 10 desktop
D. Install and deploy thin clients without an operating system for each user

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.6: A thin client is a small device that can operate with or without an operating system installed on the client device. Instead, it can boot directly from a network-based operating system on a common server and access applications on the company's application server. This type of architecture can drastically reduce the need for operating system licenses and rreduce deployment costs. A thin client runs from resources stored on a central server instead of a localized hard drive. Thin clients work by connecting remotely to a server-based comput ing environment where most applications, sensitive data, and memory are stored.

QUESTION 369
A home user brought their Windows 1 0 laptop to the electronics store where you work because they suspect it has a malware infection. You have directly observed symptoms that indicate the system is infected with malware. Which of the following actions should you perform NEXT?

A. Remediate the infected system
B. Disable System Restore
C. Enable System Restore
D. Quarantine the affected system

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.3: After you have investigated and verified the malware symptoms, you should next quarantine the infected system. Malware such as worms can propagate over networks. This means that one of the first actions should be to disconnect the network link. Infected f iles could have been uploaded to network servers or cloud services, though these systems should have server-side scanning software to block infected files. Move the infected system to a physically or logically secure work area. You might nee·d network access to tools and resources to remediate the system, but you cannot risk infecting the production network. You should also ensure that the infected computer is not used until it has been cleaned up. (Note, for the exam you should never assume any information. Many students have assumed the laptop is already quarantined since the user brought it to the store. To observe the malware symptoms, though, you may need to connect the laptop to the internet. Since you do not know whether or not the laptop is currently connected to a network, you should quarantine the affected system, or verify that the system is quarantined.)

QUESTION 370
What is the SIXTH step of the seven-step malware removal process?

A. Quarantine the infected system
B. Enable System Restore and create a restore point in Windows
C. Educate the end user
D. Update the applications and the operating system

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.3: The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 371
A Windows 2019 server is crashing every evening at 2:35 am, but you are not sure why. Which of the following tools should you use to identify the cause of the system crash?

A. Performance monitor
B. Event viewer
C. System information
D. Registry editor

Correct Answer:
Explanation

Explanation/Reference:
OBJ-1.3: The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems. If you use the Event Viewer, you can identify what was occurring at or around 2:35 am each day before the server crashed and use this to troubleshoot the problem. The registry editor (Reg Edit) allows you to view and make changes to system files and programs that you wouldn't be able to access otherwise. The registry is a database made up of hives and keys that control various settings on a Windows system. ly editing the Registry can permanently damage your computer, so it is important to be very careful when modifying the registry using Reg Edit. PerfMon is a performance monitoring and system monitoring utility in Windows that is used to monitor the activities on CPU and memory activity on a computer. Performance monitor is used for viewing performance data either in real -time or from a log file. The performance monitor can only monitor the resource utilization, but it cannot manage or terminate those processes. System information (msinfo32.exe) is a utility that gathers information about your computer and displays a comprehensive list of hardware, system components., and the software environment that can be used to diagnose computer issues.

QUESTION 372
Whic.h of the following remote access tools is a command-line terminal emulation program operating on port 23?

A. RDP
B. SSH
C. VNC
D. Telnet

Correct Answer: D

Explanation

Explanation/Reference:
OBJ-4.9: Telnet is a TCP/IP application protocol supporting remote command-line administration of a host (terminal emulation). Telnet is unauthenticated, which means it sends data such as the username and password in plain text. For this reason, it should not be used, and SSH should he used instead. Tel net runs over TCP port 23. Virtual Network Computing (VNC) is a cross-platform screen sharing system that was created to remotely control another computer from a distance by a remote user from a secondary device as though they were sitting right in front of it. Secure Shell (SSH) uses port 22 to securely create communication sessions over the Internet for remote access to a server or system. Remote Desktop Protocol (RDP) uses port 3389 and is a proprietary protocol developed by Microsoft which provides a user with a graphical interface to connect to another computer over a network connection.

QUESTION 373
Which of the following workstation operating systems are Ubuntu and Red Hat considered?

A. macOS
B. Android
C. Windows
D. Linux

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.8: Ubuntu and Red hat ar·e common distributions of the Linux operating system. The Linux operating system has over 500 different distributions of Linux available. Windows is a desktop operating system created by Microsoft. macOS is a desktop operating system created by Apple. Android is a mobile operating system created by Google. Windows, macOS, and Android are not considered vers.ions of Linux.

QUESTION 374
When Jason needs to log in to his bank, he must use a hardware token to generate a random number code automatically synchronized to a code on the server for authentication. What type of device is Jason using to log in?

A. Key fob
B. Smart card
C. PIV card
D. Biometric lock

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.1: A key fob is a hardwar,e token that generates a random number code synchronized to a code on the server. The code changes every 60 seconds or so. This is an example of a one-time password. A SecureiD token is an example of a key fob that is produced by RSA. A smart card, chip card, PIV card, or integrated circuit card is a physkal, electronic authorization device used to control access to a resource. It is typically a plastic credit cardsized card with an embedded integrated circuit chip. In high-security environments, employee badges may contain a smart card embedded chip that must be inserted into a smart card reader to log in or access information on the system. A biometric lock is any lock that can be activated by biometric features, such as a fingerprint, voiceprint, or retina scan. Biometric locks make it more difficult for someone to counterfeit the key used to open t he lock or a user's account. A smart card is a form of hardware token.

QUESTION 375
Your company is concerned about the possibility of power fluctuations that may occur and cause a small dip in the input power to their server room for an extended period of t ime. What condition is this known as?

A. Power spikes
B. Power surge
C. Under-voltage event
D. Power failure

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.5: An under-voltage event is a reduction in or restriction on the availability of electrical power in a particular area. The irregular power supply during an under-voltage event can ruin your computer and other electronic devices. Electronics are created to operate at specific voltages, so any fluctuations in power (both up and down) can damage them. To protect against an under-voltage event, you can use either a battery backup or a line conditioner. If the reduction lasts for minutes or hours, as opposed to short-term voltage sag (or dip). A significant over-voltage event that occurs for a very short period of time is known as a power spike. A power spike is a very short pulse of energy on a power line. Power spikes can contain very high voltages up to and beyond 6000 volts but usually last only a few milliseconds instead of longer but lower voltage power surges. An extended over-voltage event is known as a power surge. A power surge is basically an increase in your electrical current. A power surge often has levels of 10-30% above the normal line voltage and lasts from 15 milliseconds up to several minutes.

QUESTION 376
You are installing a new file server at the offices of Dion Training. The entire building has a diesel generator installed to protect it from power outages. The file server must have zero downtime once placed into production. Which of the following power sources should the file server utilize?

A. A surge protector
B. A line conditioner
C. A surge protector connected to a UPS
D. An uninterruptible power supply {UPS)

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.5: An uninterruptible power supply (UPS) is a redundant power system that provides minutes to hours of power from an internal battery unit. Since the entire office has a backup diesel generator, the file server only needs power for about a minute until the generator can restore the power to the building. The UPS will also serve as a line conditioner to prevent issues caused by under-voltage events if the generator is operating too slowly. When power is lost, it usually takes 30-60 seconds for a generator to start up, reach normal operating speeds, and begin providing power to its electrical distribution and loads. A surge protector defends against possible voltage spikes that could damage your electronics, appliances, or equipment. Electronics are created to operate at specific voltages, so any fluct uations in power (both up and down) can damage them. A line conditioner is a device that adjusts voltages in under-voltage and overvoltage conditions to maintain a 120 V output. Line conditioners raise a sag or under-voltage event back to normal levels, but they cannot protect the line from a complete power failure or power outage.

QUESTION 377
You want to ensure that only one person can enter or leave the server room at a time. Which of the following physical security devices would BEST help you meet this requirement?

A. Thumbprint reader
B. Cipher lock
C. Access control vestibule
D. Video monitoring

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.1: An access control vestibule is a physical security access control system comprising a small space with two sets of interlocking doors, such that the first set of doors must close before the second set opens. Video monitoring is a passive security feature, so it won't prevent two people from entering at once. The thumbprint reader or cipher lock will ensure that only an authorized user can open the door, but it won't prevent someone from piggybacking and entering with them.

QUESTION 378
Which file system type should you format a 4 TB USB flash drive to use with both Windows and macOS laptops?

A. FAT32
B. APFS
C. NTFS
D. exFAT

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.8: The extensible file allocation table (exFAT) is a file system optimized for external flash memory storage devices such as USB flash drives and SD cards. exFAT supports a maximum volume size of up to 128 PB with a recommended marximum volume size of 512 TB for the best reliability. exFAT is supported natively by both Windows and macOS. The NT file system (NTFS) is a Windows file system that supports a 64-bit address space and can provide extra features such as file-by-file compression and RAID support as well as advanced file attribute management tools, encryption, and disk quotas. NTFS can support a maximum volume size of up to 8 PB. NTFS is not supported natively by macOS. The Apple file system (APFS) is the default file system for Mac computers using macOS 10.13 or later and features strong encryption, space sharing, snapshots, fast directory sizing, and improved file system fundamentals. APFS is not supported natively by Windows. The file allocation table 32-bit (FAT32) is the 32-bit file system supported by Windows, macOS, and Linux computers. FAT32 can support maximum volume sizes of up to 2 TB and maximum file sizes of up to 4GB.

QUESTION 379
You need to connect to a Linux server to conduct some maintenance. The server is located in a remote office about 50 miles away. You decide to connect the server remotely instead of driving to the location to save some time, but you want to ensure you do this securely. The Linux server has VNC installed, but it isn't configured to provide an encrypted connection. Which of the following should you use to secure the VNC connection to the remote server?

A. RDP
B. HTTPS
C. SSHintunnel mode
D. WPA2

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.9: Since you want to use the existing VNC server to make the connection and it is unencrypted, you should tunnel the VNC protocol through a secure SSH connection to encrypt it. While an SSH client connects to a Secure Shell server, which allows you to run terminal commands as if you were sitting in front of another computer, it can also allow you to "tunnel" any port or protocol between your local system and a remote SSH

server through its own encryption process. This allows you to add a layer of encryption and security to an unsecured protocol or application, like VNC. Remote Desktop Protocol (RDP) is a Microsoft protocol designed to facilitate application data transfer securrity and encryption between client user devices and a virtual network server. It enables a remote user to add a graphical interface to the desktop of another computer. The hypertext transfer protocol secure (HTIPS) is a secure protocol used to provide web content to browsers using SSL/TLS encryption over TCP port 443. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption.

QUESTION 380
Which of the following commands can be used to install software on a Linux system?

A. grep
B. cat
C. yum
D. Nano

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.11: The yum command is a package manager used with RPM-based Linux distribut ions to install new software packages, remove existing software packages, upgrade existing software packages, and even upgrade the entire operating system. The cat (short for "concatenate") command is one of the most frequently used commands in Linux/Unix. The cat command allows the creation of single or multiple files, view file contents, concatenate fi les, and redirect output in t he terminal to a file. The nano utility is an easy-to-use command-line text editor for Linux systems. Nano includes the functionality of a regular text editor, as well as syntax highlight ing, mult ilple buffers, search and replace with regular expression support, spellchecking, UTF-8 encoding, and more. The grep is a command-line utility for searching plain-text data sets for lines that match a regular expression. The grep command works on Unix, Linux, and macOS operating systems. Grep is an acronym that stands for Global Regular Expression Print.

QUESTION 381
During the recon1naissance phase of a penetration test, you have determined that your client's employees all use iPhones that connect back to the corporate network over a secure VPN connection. Which of the following methods would MOST likely be the best method for exploiting these?

A. Use social engineering to trick a user into opening a malicious APK
B. Use a tool like ICSSPLOIT to target specif ic vulnerabilities
C. Identify a jail broken device for easy exploitation
D. Use web-based exploits against the devices web interfaces

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.5: When targeting mobile devices, you must first determine if the company uses iPhones or Android-based devices. If they are using an iPhone, it becomes much more difficult to attack since iPhone users can only install trusted apps from the App Store. If the user has j ail broken their phone, they can sideload apps and other malware. After identifying a j ail broken device, you can use social engineering to trick the user into installing your malicious code and then take control of t heir device.

QUESTION 382
Which edition of Windows 10 does not have the group policy editor enabled?

A. Pro for Workstations
B. Pro
C. Enterprise
D. Home

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.1: The Grou[p Policy Editor gpedit.msc is only available in Professional .and Enterprise editions of the Windows 10 operating systems. A Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, Group Policy is applied to users or computers based on their membership in sites, domains, or organizational units.

QUESTION 383
Your company is setting up a system to accept credit cards in t heir retaU and online locations. Which of the following compliance types should you be MOST concerned with dealing with c1redit cards?

A. PHI
B. PCI-DSS
C. GDPR
D. Pll

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.6: The Payment Card Industry Data Security Standard (PCI-DSS) applies to companies of any size that accept credit card payments. If your company intends to accept card payment and store, process, and transmit cardholder data, you need to securely host your data and follow PCI compliance requirements. The General Data Protection Regulat ion (GDPR) is a regulation created in the European Union that creates provisions and requirements to protect the personal data of European Union (EU) citizens. Transfers of personal data outside the EU Single Market are restricted unless protected by like-for-like regulations, such as the US's Privacy Shield requirements. Personally identifiable information (PI I) is data used to identify, contact, or locate an individua l. Information such as social security number (SSN), name, date of birth, email address, telephone number, street address, and biometric data is considered PI I. Protected health information (PHI) refers to medical and insurance records, plus associated hospital and laboratory test results.

QUESTION 384
You have connected your laptop to the network using a CAT Se cable but received an IP address of 169.254.13.52 and cannot connect to www.DionTraining.com. What is most likely the cause of this issue?

A. Poisoned ARP cache
B. Failed DNS resolution
C. Duplicate IP address
D. DHCP failure

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.5: A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to clients' broadcast queries. Since you have received an APIPA address (169.254.113.52), this signifies a DHCP failure. If a user is unable to access a

website by using its domain name but can by its IP address, then this indicates a DNS resolution issue instead. ARP caches rely on layer 2 addresses known as MAC addresses, not IP addresses. Duplicate IP addresses will create an error on the screen instead of issuing an APIPA address as shown in this example.

QUESTION 385
Which of the following components presents the largest risk of electrical shock to a technician?

A. CRT monitor
B. Laptop battery
C. LCD monitor
D. Hard drive

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.4: A CRT monitor is an older-style computer monitor that contains large capacitors which retain high levels of electricity even after being disconnected. A CRT should be disposed of carefully. A technician should never open a CRT monitor or stick anything into its int erior for fear of electrocution. Hard drives, LCD monitors, and laptop batteries do not contain high voltage levels.

QUESTION 386
What type of wireless security measure can easily be defeated by a hacker by spoofing their network interface card's hardware address?

A. WPS
B. WEP
C. Disable SSID broadcast
D. MAC filtering

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.9: Wireless access points can utilize MAC filtering to ensure only known network interface cards are allowed to connect to the network. If the hacker changes their MAC address to a trusted MAC address, they can easily bypass this security mechanism. MAC fi ltering is considered a good security practice as part of a larger defense- in-depth strategy, but it won't stop a skilled hacker for long. MAC addresses are permanently burned into the network interface card by the manufacturer and serve as the device's physical address. WEP is the Wired Equivalent Privacy encryption standard, which is considered obsolete in modern wireless networks. WEP can be broken using a brute force attack within j ust a few minutes by an attacker. Another security technique is to disable the SSID broadcast of an access point. While this prevents the SSID broadcast, a skilled attacker can still find the SSID using discovery scanning techniques. WPS is the WiFi Protected Setup. WPS is used to connect and configure wireless devices to an access point easily.

QUESTION 387
You are installing a new firewall for Dion Training·s corporate network. Which of the following documents should you update FIRST?

A. Incident database
B. Password policy
C. Knowledge base articles
D. Network topology diagrams

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.1: A network topology is the shape or structure of a network in a physical or logical format as depicted in a network diagram. Physical network topologies include the actual appearance of the network layout. Logical network topologies include the flow of data across the network. A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. It contains items like password complexity, password age, and password history requirements. A Knowledge Base (KB) is a reference document that is used to assist a technician when they are installing, configuring, and trroubleshooting hardware and software. A knowledge base article might be created by a vendor to support their products, too. A company might create an internal KB, populated with guidelines, procedures, information, and f requently asked questions from their service tickets. An incident database is used to document any issues, problems, or incidents in the network. An incident database is oft:en called a trouble ticket system. The system should document the number of the incident, the point of contact for the workstation, the priority of the incident, the problem description, and a history of work performed to resolve the incident for the user.

QUESTION 388
A home user contacts the help desk and states that t heir desktop applications are running very slowly. The user also says that they have not received any emails all morning, but they normally get at least 5-10 emails each day. The help desk technician gets permission from the home user to remotely access their computer and runs some diagnostic scripts. The technician determines that the CPU performance is normal, the system can ping the local rout er/gateway, and the system can load websites slowly, or they fail to load completely. During the diagnosis, the technician also observes the remote connection dropping and reconnecting intermittently. Which of the following should the technician attempt to perform NEXT to resolve the user's issue?

A. Empty the web browser's cache, send a test email to the technician's personal account, and open the Explorer to check the file system
B. Boot into the BIOS setup, enable TPM, reboot into safe mode, and perform a System Restore
C. Reboot into safe mode, uninstall the last OS update, and run a CHKDSK against the hard
D. Update the anti-virus software, run a full scan of the system, and verify the web browser's and email client's settings

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.2: Based on the symptoms, it appears that the system may be infected with malware. Therefore, it would be best to attempt to remediate the system by updating the anti-virus, performing a full system scan, and verifying that the web browser and email cl ient's settings are correct. There is no indication that a recent OS update was performed, so there is no need to reboot into safe mode and roll back that update. Enabling TPM would not help with this issue since TPM is used to store encryption keys for a Bitl ocker encrypted hard disk. A technician should never send test emails to their personal account as it is considered unprofessional.

QUESTION 389
A user receives the following error me.ssage: "Windows Update cannot current ly check for updates because the service is not running." The user calls the help desk to report the error they received. A support technician uses a remote connection tool to log in to the computer remotely, quickly identifies the issue, and fixes the issue. Which of the following should the technician do NEXT?

A. Restart the network services
B. Reboot the computer
C. Register the Windows Update service's DLL files
D. Rollback the device drivers

Correct Answer: B

Explanation

Explanation/Reference:
OBJ-3.2: If any of the .DLL files involved with Windows Update are not correctly registered, you may also encounter this problem. To solve it, open services.msc and stop the Windows Update service. Then, open a Command Prompt as the administrator and use regsvr32 for each of the 6 Windows Update DLL files (wuapi.dll, wuaueng.dll, wups.dll, wups2.dll, wuwebv.dll, and wucltux.dll). Then, open services.msc and restart the Windows Update service. Finally, restart your computer for t hese changes to take effect.

QUESTION 390
A home user brought their Windows 1 0 laptop to the electronics store where you work because they suspect it has a malware infection. You have finished remediating the infected system. Which of the following steps should you NEXT?

A. Identify and research malware symptoms
B. Schedule scans and run updates
C. Quarantine infected systems
D. Educate the end user

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.3: The next step is to schedule scans and run updates, which is the f ifth step of the malware removal process. These scans can be configured as on-access scans or scheduled scans. The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 391
Susan, an executive at Dion Training, will be traveling to Italy for a conference next week. She is worried about remaining connected to the internet while overseas and plans to use the WiFi in her hotel room and the local coffee shop with her laptop. Which of the following should she purchase and configure before leaving for Italy to ensure her communications remain secure regardless of where she is connecting from?

A. VPN
B. Local SliM card for her smartphone
C. Local mobile hotspot
D. International data roaming plan on her cellphone

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.9: While WiFi is available almost everywhere these days, it is not safe to use it without first configuring and using a VPN. A Virtual Private Network (VPN) connects the components and resources of two (private) networks over another (public) network. This utilizes an encryption tunnel to protect data being transferred to and from her laptop to the Dion Training servers and other websites. The other options are all focused on connecting her cellphone but would still not be considered safe without a VPN being utilized. A local mobile hotspot should be used to provide internet connectivity to the laptop (if she uses this instead of the hotel and coffee shop WiFi). Still, for best security, it should also use a VPN when using this connection.

QUESTION 392
Your company recently suffered a small data breach caused by an employee emailing themselves a copy of the current customer's names, account numbers, and credit card limits. You are determined that something

like this shall never happen again. Which of the following logical security concepts should you implement to prevent a trusted insider from stealing your corporate data?

A. MOM
B. Firewall
C. Strong [passwords
D. DLP

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.1 : Data loss prevention software detects potential data breaches/ data ex-filtration transmissions and prevents them by monitoring, detecting, and blocking sensitive data while in use (endpoint actions), in-motion (network traffic), and at rest (data storage). Since the user was an authorized user (employee), changing your password policy, reconfiguring the firewall, or setting up an MDM solution would not solve this problem. Instead, a DLP solution must be implemented.

QUESTION 393
David is troubleshooting a new Android applicat ion his company is creating. He has installed the app on an Android tablet and needs to see observe diagnostic information about the app and its network connections while it is running to identify and correct a software bug. Which of the following should David enable on the device?

A. Jailbreak
B. Sideloading
C. Rooting
D. Developer mode

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.5: Developer mode is used on an Android device to show additional diagnostic information when using apps or making network connections. An android application package (APK) is a t hird-party or custom program that is installed directly on an Android device to give users and businesses the flexibility to install apps directly on Android devices. Android supports sideloading through the APK package format. An APK file contains all of that program's code, including .dex files, resources, assets, certificates, and manifest files. Jailbreaking is conducted on an iOS device to remove manufacturer restrictions on the device and allow other software, operating systems, or networks to work with a device. A rooted device is an Android device t hat has been hacked to provide the user with administrative rights to install unapproved apps, update OS, delete unwanted apps, underclock or overclock the processor, rep'lace the firmware and customize anything else. A rooted device is not required just to install an APK outside of the Play Store, though, on an Android device.

QUESTION 394
You recently moved 1.5 TB of data from your office's file server to a new 16 TB NAS and decommissioned the old file server. You verified all users had been given the same permissions to the new file shares on the NAS as they had on the old server. The users are receiving an error stating, "Windows cannot access \ \server1 0 \shared\" every time they d ick the Share drive icon on their desktop. What is MOST likely the source of this error?

A. The users are using the password for the new server
B. The users are still mapped to the old share drive
C. The users need administrative permission to access the new NAS
D. The users are outside the authorized hours set in the GPO

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.6: Based on the error shown, it appears that the users are sti II mapped to the old server and not the new NAS. This is a common issue and oversight that occurs when companies migrate from one server to another. Even if every computer has an S:\ (share drive) shown,. it is just a link to a network resource (like \ \server1 0\shared\). If the new server is not named "server1 0" and is called "server11 ", then the mapping needs to be redone to reflect \\server11\sharedl, for example.

QUESTION 395
You are configuring a SOHO network that will contain 7 devices, but you only have a single public IP address. Which of the following concepts should be configured to allow the 7 devices to share that single IP when connecting to the internet?

A. NAT
B. DHCP
C. UPnP
D. Perimeter network

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.9: Network address translation (NAT) is a network service provided by a router or proxy server to map private local addresses to one or more publicly accessible IP addresses. NAT can use static mappings but is commonly implemented as network port address translation (PAT) or NAT overloading, where a few public IP addresses are mapped to multiple LAN hosts using port allocations. The dynamic host control protocol (DHCP) is a protocol used to allocate IP addresses to a host when it joins a network. Universal plug-and-play (UPnP) is a protocol framework allowing network devices to autoconfigure services, such as allowing a games console to request appropriate settings from a firewall. A perimeter network (formerly called a Demilitarized Zone or DMZ) is a portion of a private network connected to the Internet and protected against intrusion. Certain services may need to be made publicly accessible from the Internet (such as a web, email, or Minecraft server) and they should be installed in the perimeter network inst ead of in your intra net. If communication is required between hosts on either side of a perimeter network, then a host within the perimeter network will act as a proxy to take the request.

QUESTION 396
Which command-line entry would be used on a Windows system to test if your system can reach diontraining.com?

A. ipconfig diontraining.com
B. net use diontraining.com
C. sfc diontraining.com
D. ping diontraining.com

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.2: The ping command is used to test a host's reachability on an Internet Protocol network. Type "ping diontraining.com" to send a series of ICMP packets will be sent to the Dion Training server. If they are received successfully, your system will receive an echo reply. Your system will then report if the calli and response were successful and how long it took in milliseconds. The system file checker (SFQ command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from the command line. The net use command is used to connect to, remove, and configure connections to shared resources such as mapped drives and network printers. The ipconfig tool displays all current TCP/IP network configuration values on a

given s stem.

QUESTION 397
Dion Consulting Group has been hired by a small real estate office to build its network. The office has 4 computers running Windows 10 Professional edit ion configured in a workgroup to access a shared file server. Which of the following types of network models is being used by this real estate office?

A. Peer-to-peer
B. Hub-and -spoke
C. Mesh
D. Client/server

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.1: A workgroup is a Microsoft peer-to-peer network model in which computers are connected together for access to shared resources for organizational purposes. A domain is a Microsoft client/server network model that groups computers together for security and to centralize administration. Domain members have access to a central user account database so that users can log on to any computer within the domain. Hub-and-spoke and mesh are networking models that are not used for workgroups or domains.

QUESTION 398
Last week, a technician remediated a malware infection on Karen's laptop. Today, she shows up at the service desk, frustrated because her laptop appears to have been infected again. What step of the malware remediation process did the technician MOST likely forget to complete?

A. Investigate and verify malware symptoms
B. Educating the end user
C. Enabling System Restore
D. Quarantining the infected laptop

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.3: The technician most likely neglected to educate Karen on safe web browsing techniques and how to avoid reinfection. This includes educating the users about not running attachments, as this will prevent files such as executables and Office macros from being allowed to run. By educating the end user, you can prevent reinfection more effectively than using technical controls alone. The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 399
Which of the following commands is used on a Linux system to copy a file to a new directory and then remove the original file from the previous directory?

A. ls
B. cp
C. rm
D. mv

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.1 1: The mv command is a command-line utility that moves files or directories from one place to another. The mv command supports moving single files, multiple files, and directories. The mv command can prompt before overwriting files and will only move files that are newer than the destination. When the mv command is used, the file is copied to the new directory and removed from the old directory. The cp command is a commandline utility for copying files and directories. It supports moving one or more files or folders with options for taking backups and preserving attributes. Copies of files are independent of the original file, unlike the mv command. The cp command will copy your f ile(s) while the mv one will move them and delete the original files from the old location. The rm command is a command-line utility for removing files or directories. To remove a file, pass the name of a file or files to the rm command, and those files will be removed immediately from the file system. The Is command lists the files or directories in the current path of a Unix, Linux, or Mac operating system. When invoked without any arguments, Is lists the files in the current working directory.

QUESTION 400
Which of the following types of screen locks uses a biometric authentication system to prevent access to a mobile device?

A. Pattern lock
B. TouchiD
C. Passcode
D. Swipe

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.7: TouchiD is a feature developed by Apple that uses fingerprint biometric information to grant access to the device. It is a form of biometric authentication. A swipe lock is a term for unlocking a device by tracing a predetermined on-screen pattern or joining dots on the screen. This was commonly used in Android devices until biometric methods like fingerprint scanners and facial recognition became more prevalent. A pattern lock is another name for a swipe lock. A passcode unlock is a term for unlocking a device by entering a 4 to 6 digit pin.

QUESTION 401
Which of the following is a connectionless protocol that utilizes on UDP?

A. HTTP
B. TFTP
C. FTP
D. HTTPS

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.1: The user datagram protocol (UIDP) is a protocol in the TCP/IP suite that operates at the transport layer to provide connection less, non-guaranteed communication with no sequencing or flow control. UDP is faster than TCP, but it does not provide reliable delivery of the packets. The trivial file transfer protocol (TFTP) is a protocol used to get a file from a remote host or put a file onto a remote host. TFTP is commonly used with embedded devices or systems t hat retrieve firmware, configuration information, or a system image during the boot process. TFTP operates over UDP port 69. The hypertext transfer protocol (HTTP) is a protocol used to provide web content to browsers using TCP port 80. The hypertext transfer protocol (HTTP) is a protocol used to provide web content to browsers using TCP port 80. The hypertext transfer protocol secure (HTTPS) is a secure protocol used to provide web content to browsers using SSL/TLS encryption over TCP po1rt 443.

QUESTION 402
Which of the following commands is used on a Linux system to copy a file from one directory to another directory?

A. cp
B. ls
C. mv
D. Rm

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.1 1: The cp command is a command- line utility for copying files and directories. It supports moving one or more files or folders with options for taking backups and preserving attributes. Copies of files are independent of the original file, unlike the mv command. The mv command is a command-line utility that moves files or directories from one place to another. The mv command supports moving single files, multiple files, and directories. The mv command can prompt before overwriting files and will only move files that are newer than the destination. When the mv command is used, the file is copied to the new directory and removed from the old directory. The rm command is a command-line utility for removing files or directories. To remove a file, pass the name of a file or files to the rm command, and those files will be removed immediately from the file system. The ls command lists the files or directories in the current path of a Unix, Linux, or Mac operating system. When invoked without any arguments, ls lists the files in the current working directory.

QUESTION 403
How would you represent the Linux permissions rwxr-xr-- in odal notation?

A. 724
B. 742
C. 754
D. 624

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.6: RWX is 7, R-X is 5, and R-- is 4. In Linux, you can convert letter permissions to octal by giving 4 for each R, 2 for each W, and 1 for each X. R is for read-only, W is for write, and X is for execute. The permissions strings are written to represent the owner's permissions, the group's permissions, and the other user's permissions.

QUESTION 404
Which of the following techniques would be the most appropriate solution to implementing a multifactor authentication system?

A. Password and security question
B. Fingerprint and retinal scan
C. Smartcard and PIN
D. Username and password

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.1: Multi-factor authentication (MFA) creates multiple security layers to help increase the confidence that the user requesting access is who they claim to be by requiring two distinct factors for authentication. These

factors can be something you know (knowledge factor), something you have (possession factor), something you are (inheritance factor), something you do (action factor), or somewhere you are (location factor). By selecting a smartcard (something you have) and a PIIN (something you know), you have implemented multi-factor authentication. Choosing a fingerprint and retinal scan would instead use only one factor (inheritance). Choosing a username, password, and security question would also be only using one factor (knowledge). For something to be considered mullti-factor, you need items from at least two different authentication factor categories:
knowledge, possession, inheritance, locat ion, or action.

QUESTION 405
Your company has just installed 50 new LCD monitors to replace some older CRT monitors. How should you properly dispose of the old CRT monitors?

A. Give them to charity
B. Follow local government regulations and handling procedures
C. Haul them to the landfill
D. Recycle them

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.5: When disposing of a CRT monitor, cel lphone, tablet s, toner, and batteries, you should follow your local government regulations for the proper d isposal of these items as t hey are considered toxic waste. They may be recycled or reused, but consult your local regulations before making that decision.

QUESTION 406
Your company is concerned about the possibility of power fluctuations that may occur and cause a large increase in the in[put power to their server room. What condition is this known as?

A. Under-voltage event
B. Power spikes
C. Power failure
D. Power surge

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.5: A significant over-voltage event that occurs for a very short period of time is known as a power spike. A power spike is a very short pulse of energy on a power line. Power spikes can contain very high voltages up to and beyond 6000 volts but usually last only a few milliseconds instead of longer but lower voltage power surges. An extended over-voltage event is known as a power surge. A power surge is basically an increase in your electrical current. A power surge often has levels of 10-30% above the normal line voltage and lasts from 15 milliseconds up to several minutes. An under-voltage event is a reduction in or restriction on the availability of electrical power in a particular area. The irregular power supply during an under-voltage event can ruin your computer and other electronic devices. Electronics are created to o perate at specific voltages, so any fluctuations in power (both up and down) can damage them. To protect against an under-voltage event, you can use either a battery backup or a line conditioner. A power loss or power failure is a total loss of power in a particular area. To protect against a power loss or power failure, a battery backup should be used.

QUESTION 407
A user is complaining that when they attempt to access Google's homepage, it appears in a foreign language even though they are located in the United States. The user claims they are not using a VPN to access the internet. You have run a full anti-malware scan on the workstation and detected nothing unusual. Which of the following actions should you attempt NEXT?

A. Disable the Windows Firewall
B. Verify the user's date and timezone are correctly listed in Windows
C. Remove any proxy servers configured in their web browser
D. Download the latest security updates for Windows

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.2: A proxy server is a web server that acts as a gateway between a client application. A malicious actor could have reconfigured this user's web browser to use a particular proxy server in a foreign country to conduct a man- in-the-middle attack. An anti-malware scanner would not detect this since the use of a proxy server could also be for legitimate purposes. In fact most large companies use their own proxy servers that users connect to when using the internet. Google would be detecting the language for the proxy server's location. If the malicious proxy server were located in Italy (for example), your Google homepage would be displayed in Italian even if your workstation is in the United States.

QUESTION 408
Which of the following types of encryption should be selected on a SOHO access point if you are running a coffee shop and want all of your customers to be able to join it by default?

A. WEP
B. WPA
C. WPA2
D. Open

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.2: An "open" wireless network is one in which no password or encryption is being used. If you have a public hotspot, such as in a library or coffee shop, then you may wish to configure it as "open." Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks that can break its encryption. WEP relies on the use of a 24-bit initialization vector to secure its preshared key. Wi-Fi protected access (WPA) is an improved encrypt ion scheme for prote·ct ing Wi- Fi communications designed to replace WEP. WPA uses the RC4 cipher and a temporal key integrity protocol (TKIP) to overcome the vulnerabilities in the older WEP protection scheme. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is st ill available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption.

QUESTION 409
A factory worker suspects that a legacy workstation is infected with malware. The workstation runs Windows XP and is used as part of an ICS/SCADA system to control industrial factory equipment. The workstation is connected to an isolated network that cannot reach the internet. The workstation receives the patterns for the manufactured designs through a USB drive. A technician is dispatched to remove the malware from this workstation. After its removal, the technician provides the factory worker with a new USB drive to move the pattern files to the workstation. Within a few days, the factory worker contacts the technician again to report the workstation appears to be reinfected with malware. Which of the following steps did the technician MOST likely forget to perform to prevent reinfection?

A. Enable System Restore and create a restore point in Windows
B. Remediate the infected systems
C. Disable System Restore in Windows

D. Quarantine the infected system
E. Investigate and verify malware symptoms
F. Update the anti-malware solution

Correct Answer: F
Explanation

Explanation/Reference:
OBJ-3.3: Since the workstation is isolated from the internet the anti-malware solution will need to be manually updated to ensure it has the latest virus definitions. Without the latest virus definitions, the system can easily become reinfected. The seven steps of the malware removal proced ures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 410
Dion Training's offices are frequently experiencing brownouts and sags. Which of the following solutions would protect all of their workstations and servers from these under-voltage events?

A. Diesel generator
B. Surge suppressor
C. Line conditioner
D. Uninterruptible power supply

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.5: Line conditioners are used to protect an entire power circuit from under-voltage events and power sags. Line conditioners raise a sag or under-voltage event back to normal levels, but it cannot protect the line from a complete power failu re or power outage. These are also known as voltage regulators and power distribution units (PDUs). Because the question's requirement must protect all of the workstations, a line conditioner is t he best option. A surge protector or surge suppressor can defend against possible voltage spikes that could damage your elect ronics, appliances, or equipment. An uninterruptible power supply or uninterruptible power source (UPS) is an electrical apparatus that provides emergency power to a load when the input power source becomes too low or the main power fails. A UPS provides near- instantaneous protection from input power interruptions by using a battery backup. A diesel generator is a mechanical device that converts rotational motion created by a diesel motor into electrical energy. Generators take 30-60 seconds to turn on and have the electrical load transferred to them. Generators are useful for long-duration power loss events, not under-voltage events.

QUESTION 411
You attempt to boot a Windows 10 laptop and receive an "Operating System Not Found" error on the screen. You can see the hard disk listed in the UEFI/BIOS of the system. Which of the following commands should you use to repair the first 512-byte sector on the hard disk?

A. bootrec /fixmbr
B. diskpart list
C. bootrec /fixboot
D. bootrec /rebuildbcd

Correct Answer: A
Explanation

Explanation/Reference:

OBJ-3.1: The master boot record (MBR) is the first 512-byte sector on a hard disk. It contains the partitioning information for a drive. To repair the master boot record (MBR), you should use the command "bootrec / fixmbr" and reboot the computer. If the disk cannot be detected, enter the system setup and try modifying settings (or even resetting the default settings). If the system firmware reports the disk's presence, but Windows still will not boot, use a startup repair tool to open a recovery mode command prompt and use the bootrec tool to repair the drive"s boot information. The "bootrec /fixboot" command is used to attempt a repair of the boot sector of a drive. The "bootrec /rebuildbcd" command is used to add missing Windows installations to the Boot Configuration Database (BCD). The diskpart command is a command-line disk-partitioning utility available for Windows that is used to view, create, delete, and modify a computer's disk partitions.

QUESTION 412
On your lunch break, you walked down to the coffee shop on the corner. You open your laptop and connect to their wireless network. After a few minutes of surfing the Internet, a pop-up is displayed on your screen. You close the pop-up, finish your lunch break, shut down the laptop, and put it back into your backpack. When you get back to the office, you take out the laptop and turn it on, but instead of your normal desktop background, you are greeted by a full-screen image with a padlock and a message stating you have to pay 0.1 BTC to regain access to your personal files. What type of malware has infected your laptop?

A. Trojan
B. Spyware
C. Rootkit
D. Ransomware

Correct Answer: D
Explanation

Explanation/Reference:
Explanat ion
OBJ-2.3: This scenario is describing a ransomware attack. Your personal files are being held hostage and will not be released unless you pay a ransom (in this case, 0.1 BTC). Ransomware is a type of malware designed to deny access to a computer system or data until a ransom is paid. Ransomware typically spreads through phishing emails or by unknowingly visiting an infected website. Once infected, a system or its files are encrypted, and t hen the decryption key is withheld from the victim unless payment is received. A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. A rootkit is generally a collection of tools that enabled administrator- level access to a computer or network. They can often disguise themselves f rom detection by the operating system and anti-malware solutions. If a rootkit is suspected on a machine, it is best to reformat and reimage the system. Spyware is a program that monitors user activity and sends the information to someone else. It may be installed with or without the user's knowledge. It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data firms, or external users. A trojan is a type of malware that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. The most common form of a trojan is a Remote Access Trojan (RAT), which allows an attacker to control a workstation or steal information remotely. To operate, a trojan will create numerous processes that run in the background of the system.

QUESTION 413
During a penetration test of your company's network, the assessor came across a spreadsheet with the passwords being used for several servers. Four of the passwords recovered are listed below. Which one is the weakest password and should be changed FIRST to increase the password's complexity?

A. P@$$w0rd
B. paSSword
C. P@$$WORD
D. PaSSwOrd

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.6: Password policies often enforce a mixture of standard character types, including uppercase let ters, lowercase letters, rnumbers, and symbols. The option 'paSSword' is the weakest choice since it only includes lowercase letters and numbers. The option 'PaSSwOrd ' is slightly more complex since it includes uppercase letters, lowercase letters, and numbers. The option 'P@$$WOIRD is also similar in complexity since it includes uppercase letters, numbers, and special characters. The most secure option is 'P@S$w0rd' since it includes a mixture of uppercase letters, lowercase letters, numbers, and special characters.

QUESTION 414
A corporate user has called the enterprise service desk because they believe their computer has become infected with malware. When you arrive at their desktop to troubleshoot the issue, you notice it was powered down. You press the power button, the system loads without any issues. When you open Google Chrome, you notice that mult iple pop-ups appear almost immediately. Which of the following actions should you take NEXT?

A. Document the pop-ups displayed and take a screenshot
B. Clear the browser's cookies, history, and enable the pop-up blocker
C. Reinstall or reimage the operating system
D. Quarantine the machine and report it as infected to your company's cybersecurity department for investigation

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.3: This is a tricky question because many technicians might try to fix the issue by clearing the browser or reinstalling/reimaging the machine. If this were a home user's machine, this would be an appropriate response, but you should follow the company's procedures since this is a corporate workstation. Most companies require any machines suspected of mallware infection to be scanned/analyzed by the cybersecurit y department before remediating or reimaging them. Therefore, the best thing to do is to remediate the system. This also follows the malware removal process since the technician just investigated and verified the malware symptoms. The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti malware software, scan the system, and use removal techniques (e.g., safe mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 415
A programmer is writing a script to calculate the temperature in Fahrenheit when it receives input in celsius. The conversion factor used is 5/9. Which of the following would be used to store this fixed conversion factor in the script?

A. Comment
B. Constant
C. Variable
D. Loop

Correct Answer:
Explanation

Explanation/Reference:
OBJ-4.8: A constant is a specific identifier that contains a value that cannot be changed within the program. For example, the value to convert a number from F to C is always 5/9 because the formula is C = (F -32) * 5/9. A comment is written into the code to help a human understand the initial programmer's logic. In Python, for example, you can use the# symbol to comment on a line of code. Anything on the line after the# is ignored by the computer when the script is being executed. A variable is a placeholder in a script containing a number,

character, or string of characters. Variables in scripts do not have to be declared (unlike in programming languages) but can be assigned a value. Then, the variable name is referenced throughout the script instead of the value itself. A loop deviates from the initial program path to some sort of logic condition. In a loop, the computer repeats the task until a condition is met. Often implemented with For or While statements. For example, a short script like (For i=1 to 100, print I, next) would print the numbers from 1 to 100 to the screen.

QUESTION 416
The customer service manager at Dion Training is having issues with her Windows 10 laptop. A technician believes that the operating system may have been corrupted by a piece of malware. The technician has removed the malware and wants to perform an installation or upgrade that will recopy the system files and revert most of the system settings to their default configurations while still preserving the user's personalization settings, data files, and any applicat ions installed through the Windows store. The technician has been told that they may delete any applications installed by the user, though, since they may have been irnfected by the malware. Which of the following types of upgrades or installations should the technician use?

A. In-place upgrade
B. Refresh installation
C. Clean install
D. Repair installation

Correct Answer:
Explanation

Explanation/Reference:
OBJ-1.9: A refresh installation is a type of installation that will recopy the system files and revert most system settings to their default configuration while preserving user personalization settings, data files, and applications installed through the Windows Store. A clean install is an installation of the new operating system on a new computer or a computer that has been recently formatted. A clean install will completely replace the operating system software on the computer with the new operating system. During a clean install, all of the user's data, settings, and applications will be deleted. An in-place upgrade is an installation of the new operating system on top of an existing version of the operating system. An in-place upgrade will preserve the applications, user settings, and data files that already exist on the computer. Repair installation is a type of installation that attempts to replace the existing version of the operating system files with a new copy of the same version. A repair installation is useful when trying to repair a Windows computer that will not boot or when you believe the system files have become corrupted.

QUESTION 417
Which of the following Control Panel sections would allow a technician to turn on Hyper-Von a Windows 10 Pro workstation?

A. Devices and Printers
B. Device Manager
C. Programs and Features
D. System

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.4: The Progrrams and Features section of the Control Panel allows a technician to install or remove applications, software packages, and features in the Windows operating system. Hyper-Vis considered an additional feature in Windows 10 Pro and can be enabled from the Windows Features section of the Programs and Features tool. The Devices and Printers section of the Control Panel allows a technician to manage the printers, scanners, and other external devices connected to a Windows computer. The System section of the Control Panel allows a technician to see information about the workstation, including the processor type, amount of memory, and operating system version installed on the computer. The Device Manager is used to view and control the hardware attached to the computer. The device manager will highlight a piece of

hardware that is not working so that a t echnician can repair or replace it.

QUESTION 418
Which of the following commands is used on a Linux system to display the current working directory's full pathname to the screen?

A. chmod
B. pwd
C. chown
D. Passwd

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .11 : The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen. The passwd command changes passwords for user accounts. A normal user may only change the password for their account, while the superuser may change the password for any user. The chown command is used to change the owner of the fi le, directory, or link in Linux. The chmod command sets the permissions of fi les or directories on a Linux system. A set of flags associated with each file determines who can access that file and how they can access it. These flags are called file permissions or modes. The command name chmod stands for change mode and it rest ricts the way a file can be accessed.

QUESTION 419
What is the minimum amount of memory required to install Windows 10 (x64) on a device?

A. 2GB
B. 8GB
C. 4GB
D. 1 G8

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .7: For the Windows 10 (64- bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64GB of hard drive space.

QUESTION 420
A Windows laptop is malfunctioning, and you believe that some system files are missing or corrupted. Which of the following commands should you use to verify this and, if needed, repair the files?

A. chkdsk
B. sfc
C. xcopy
D. Gpupdate

Correct Answer: B
Explanation

Explanation/Reference:

OBJ-1.2: The system file checker (SFC) command is a uti lity in Windows that allows users to scan for and restore corrupted Windows system files from the command line. The gpupdate command-line tool is used to update the group policy settings on a Windows system. For an administrator to force a background update of all Group Policy settings regardless of whether they have changed, they need to run "gpupdate /force" from the command line. The chkdsk command is used to check the file system and file system metadata of a volume for logical and physi(al errors. If used without parameters, chkdsk displays only the status of the volume and does not fix any errors. If used with the If, / r, /x, or /b parameters, it fixes errors on the volume. The xcopy tool copies all of the files from one directory t o another. To meet your boss's requireme,nts to synchronize the two hard drive's contents, you must use robocopy since it will also remove files from the second drive that were removed from the first drive, too.

QUESTION 421
A user's smartphone has become unresponsive since installing the latest iOS update. Which of the following should a technician do to restore the smartphone's performance?

A. Reimage the device
B. Rollback the iOS update
C. Update the applications
D. Perform a factory reset

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: If an update causes problems, you can try to uninstall it and roll back the device. Every change should be accompanied by a rollback (or backout) plan so that the change can be reversed if it has harmful or unforeseen consequences. The applications cannot be updated while the device is unresponsive. Reimaging is not a valid option for smartphones, only for desktops and laptops. Performing a factory reset would revert the phone to the initial operating system it came with when purchased. The issue is this may be several generations old and extremely insecure, so it is better to roll back to the last working iOS version.

QUESTION 422
You are writing a script that will take an employee's name as the input. Which of the following data types would the employee's name be stored in?

A. String
B. Integer
C. Float
D. Boolean

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.8: A string stores a group of characters, such as Hello, PYTHON, or JasonDion. A string data type usually consumes as much storage as necessary. Each character in the string usually requires 1 byte of storage. An integer stores a whole number, such as 21, 143, or 1024. An integer data type usually consumes 8 bytes of storage. A floating-point number stores a fractional or decimal number, such as 3.14, 45.5, or 333.33. A floatingpoint number data type usually consumes 4 to 8 bytes of storage. A boolean stores a value of TRUE (1) or FALSE (0). It usually consumes only 1 bit of storage (a zero or a one).

QUESTION 423
Which attack method is MOST likely to be used by a malicious employee or insider trying to obtain another user's passwords?

A. Tailgating

B. Shoulder surfing
C. On-path attack
D. Phishing

Correct Answer: B
Explanation

Explanation/Reference:
OBJ ~2.4: While a malicious employee or insider could use all of the methods listed to obtain another user's passwords, shoulder surfing is the MOST likely to be used. Shoulder surfing is a type of social engineering technique used to obtain personal identification numbers (PINs), passwords, and other confidential data by looking over the victim's shoulder. Since a malicious employee or insider can work close to their victims (other users), they could ,easily use this technique to collect t he victimized users' passwords. An on-path attack is an attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other. The attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection. The attacker will intercept all relevant messages passing between the two victims and inject new ones. Tailgating is a social engineering technique to gain access to a building by following someone unaware of their presence. Phishing is an email-based social engineering attaclk in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Phishing attacks target an indiscriminate large group of random people.

QUESTION 424
A user's Android smartphone is becoming sluggish and slow to load applications. Which of the following should you perform FIRST to fix this problem?

A. Turn off the smartphone's Bluetooth and Wifi
B. Conduct a factory restore of the smartphone
C. Close all of the running applications
D. Update the smartphone's firmware

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.4: If the smartphone becomes sluggish and slow, you should first close out of all running applications. Many applications continue to operate in the background, even if t hey are not actively being used. If closing all the applications doesn't free up enough resources, there may be other background processes in use. To clear these, you would then fully shut down and restart the smartphone.

QUESTION 425
You are assisting a network administrator with updating the firmware of a Cisco iOS-based router. This router is the only border router for your organization, and it co nnects them to the internet. A request for change (RFC) is being written and contains the purpose, plan, scope, and risk analysis of the proposed change. Which of the following should be added to the RFC before its approval?

A. Configure a secondary route during the maintenance window
B. Update the asset management database with the new router's asset ID
C. Document a backout plan if the update is not successful
D. Extend the maintenance windows from 1 hour to 8 hours

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.2: A backout plan or rollback plan is a plan defined ahead of making any moves, adds, or changes so

that if unforeseen problems arise when the change is made, there is a plan to put things back as they were before making the change. A firmware update of a router usually takes between 5-15 minutes to implement. If it is unsuccessful, the backout plan should revert to the previous firmware version and configuration. There is no secondary route that could be configured in this scenario. This is the only border router that the organization has connected to the internet, as described in the question. The asset management database should not be updated until after the firmware upgrade is completed, not before.

QUESTION 426
Which of the following provides accounting, authorization, and authentication via a centralized privileged database, as well as challenge/response and password encryption?

A. TACACS+
B. Network access control
C. ISAKMP
D. Multi-factor authentication

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.2: TACACS+ is a AAA (accounting, authorizat ion, and authentication) protocol to provide AAA services for access to routers, network access points, and other networking devices. TACACS+ is a remote authentication protocol, which allows a remote access server to communicate with an authentication server to validate user access onto the network. TACACS+ allows a client to accept a username and password, and pass a query to a TACACS+ authentication server. Multifactor authentication is an authentication scheme that works based on something you know, something you have, something you are, something you do, or somewhere you are. These schemes can be made stronger by combining them (for example, prot ecting the use of a smart card certificat ion [something you have] with a PIN [something you know]). Network Access Control (NAC) is a means of ensuring endpoint security by ensuring that all devices connecting to the network conform to a health policy such as its patch level, antivirus/firewall configuration, and other factors. Internet Security Association and Key Management Protocol (ISAKMP) is used for negotiating, establishing, modification, and deletion of SAs and related parameters in the IPSec protocol.

QUESTION 427
You are working on a Windows 10 workstation with a 1 TB HOD and 16GB of memory that is operating slowly when reading large files from its storage device. Which of the following commands should you use to speed up this workstation?

A. ipconfig
B. format
C. diskpart
D. chkdsk

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1 .2: The chkdsk command is used to check the file system and file system metadata of a volume for logical and physical errors. If used without parameters, chkdsk displays only the status of the volume and does not fix any errors. If used with the / f, / r, j x, or /b parameters, it fixes errors on the volume. The format command creates a new root directo ry and file system for the disk. It can check for bad areas on the disk, and it can delete all data on the disk. To use a new disk, you must first use the format command to format the disk. The diskpart command is a command-line disk-partitioning utility available for Windows that is used to view, create, delete, and modify a computer's disk partitions. The ipconfig tool displays all current TCP/IP network configuration values on a given s stem.

QUESTION 428

A network technician determines that two dynamically assigned workstations have duplicate IP addresses. What command should the technician use to correct this issue?

A. ipconfig /renew
B. ipconfig /dhcp
C. ipconfig /all
D. ipconfig /release I ipconfig /renew

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.2: The ipconfig tool displays all current TCP/IP network configuration values on a given system. The ipconfig also can release and renew a DHCP-received IP on a workstation. The first thing to do is release the IP address using the command ipconfig /release. Next, the technician should dynamically assign another IP address using the command ipconfig /renew. These commands could be each entered individually or combined using the pipe <D syntax as shown in this question. The ipconfig /all option would be used to display the assigned IP addresses. The ipconfig /renew option would be used to renew an existing DHCP lease and not request a new IP address.

QUESTION 429
Christina is attempting to install Windows 10 (32-bit) on an older netbook-style laptop. The installation is continually failing and producing an error. The device has a 1.1 GHz processor, 1 GB of memory, an 8GB hard drive, and a 720p display. Which component would need to be fixed to allow Windows 10 (64-bit) to be in.stalled on this device?

A. Amount of memory
B. Amount of hard drive space
C. Number of CPU cores
D. The screen resolution

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .7: The amount of hard drive space needs to be increased. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space. For the Windows 11 {64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4 GB of RAM, and at least 64 GB of hard drive space.

QUESTION 430
Which of the following types of attacks occurs when an attacker attempts to gain confidential information or login credentials by sending targeted emails to a specific set of recipients within an organization?

A. Phishing
B. Zero-day
C. Spear phishing
D. Spoofing

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.4: Spear phishing is the fraudulent practice of sending emails from a seemingly known or trusted sender to induce targeted individuals to reveal conf idential information. The key to answering this question is

that the attack was focused on a targeted set of people, not j ust an indiscriminate large group of random people. Phish ing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from t he victim. A zero-day vulnerability is when the vendor is aware of a security flaw, but a patch has not been developed or applied on an affected system. At this point, a malicious actor can craft an attack and take advantage of the zero-day vulnerability. Spoofing is a type of attack that disguises a communication from an unknown source as being from a known, trusted source. Spoofing can occur using different methods, such as MAC spoofing, IP spoofing, call spoofing, and ot hers.

QUESTION 431
Which of the following commands would you use to duplicate the file c:\Users\Jason\Downloads\newfile.docx to c:\Users\Jason\Desktop\newfile.docx from the command line?

A. diskpart
B. copy
C. chkdsk
D. net user

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.2: The copy command is used to copy one or more files from one location to another. The copy command cannot copy files that are 0 bytes long or for copying all of a directory's files and subdirectories. The diskpart command is a command-line disk-partitioning utility available for Windows t hat is used to view, create, delete, and modify a computer's disk partitions. The chkdsk command is used to check the file system and file system metadata of a volume for logical and physical errors. If used without parameters, chkdsk displays only the status of the volume and does not fix any errors. If used with the /f, /r, /x, or /b parameters, it fixes errors on the volume. The net user command allows system administrators to manage user accounts on Windows PCs. You can use the command to display account information or make changes to user accounts.

QUESTION 432
Jennifer decided that the licensing cost for a piece of video editing software was too expensive. Instead, she decided to download a keygen program to generate a license key and install a pirated version of the editing software. After she runs the keygen, a license key is created, but her system performance becomes very sluggish, and her antimalware suite begins to display numerous alerts. Which type of malware might her computer be infected with?

A. Adware
B. Trojan
C. Logic bomb
D. Worm

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.3: A trojan is a program in which malicious or harmful code is contained inside a harmless program. In this example, the harmless program is the key generator (which does create a license key). It also has malicious code inside it causing the additional alerts from the antimalware solution. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. The most common form of a trojan is a Remote Access Trojan (RAT), which allows an attacker to control a workstation or steal information remotely. To operate, a t rojan will create numerous processes that run in the background of the system. A worm is a standalone malware computer program that replicates itself to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. A worm can spread on its own, whereas a virus needs a host program or user interaction to propagate itself. A logic bomb is a malicious program that is triggered when a logical condition is

met, such as after a number of transactions have been processed, or on a specifi,c date. Adware is software that displays unwanted advertisements on your computer.

QUESTION 433
Sally just purchased a new iPhone and AirPods to listen to her music. After setting up the new iPhone, she can get online and watch YouTube, but her wireless headphones aren't working. Which of the following is MOST likely the problem?

A. Cellular is not enabled
B. Bluetooth is not enabled
C. The phone is in airplane mode
D. WiFi is not enabled

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: Since Sally can connect to the internet, either her cellular or WiFi is enabled, and the phone would not be in airplane mode. Since AirPods work over Bluetooth, it is most likely that the Bluetooth is not enabled on the new phone and should be turned on. Once Bluetooth is enabled, the Airpods will need to be paired to the device to begin using them.

QUESTION 434
Which of the following types of attacks occurs when an attacker attempts to gain confidential information or login credentials by sending targeted emails to a specific set of recipients within an organization?

A. Vishing
B. Spear phishing
C. Phishing
D. Whaling

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: Spear phishing is the f raudulent practice of sending emails from a seemingly known or trusted sender to induce targeted individuals to reveal confidential information. The key to answering this question is that the attack was focused on a targeted set of people, not just an indiscriminate large group of random people. Phish ing is an email-based social engineering attack in which the attacker sends an email from a supposedly reputable source, such as a bank, to try to elicit private information from the victim. Whaling is an email -based or web~based form of phishing that targets senior executives or wealthy individuals. Vishing is a social~engi neering attack where the attacker extracts information while speaking over the phone or leveraging IP-based voice messaging services (VoiP).

QUESTION 435
A user attempted to go to their favorite social media website this morning from their laptop. When they typed in Facebook.com, their browser redirected them to MalwareInfect.com instead. You asked the user to clear their cache, history, and cookies, but the problem remains. What should you do NEXT to solve this problem?

A. Conduct an antivirus scan
B. Upgrade their web browser
C. Check the host.ini file
D. Disable System Restore

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.2: The hosts.ini file is a local plain text file that maps servers or hostnames to IP addresses. It was the original method to resolve hostnames to a specific IP address. The hosts file is usually the first process in the domain name resolution procedure. When a user requests a webpage, the hosts.ini fi le is first checked for the IP address. If the IP address isn't found in the hosts.ini file, then the workstation requests the IP address from the DNS server. Attackers often modify host.ini files to redirect users to a malicious webpage instead of one they would commonly use like Google, Facebook, and others.

QUESTION 436
An increased amount of web traffic to an e-commerce server is observed by a network administrator but without increasing the number of financial transactions. Which kind of attack might the company be experiencing?

A. ARP spoofing
B. Bluejacking
C. Phishing
D. DoS

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.4: A DoS attack or denial-of-service attack works by overloading a server with multiple requests (more than it can handle), thus eventually knocking the server offline. When a denial-of-service attack occurs, there will be an increase in the amount of web traffic on the server, but since that traffic is not being sent by legitimate customers there will be no financial transactions occurring. ARP spoofing is a type of attack in which a malicious actor sends falsified ARP (Address Resolution Protoco l) messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. Phishing is a type of social engineering where an attacker sends a fraudulent email designed to trick a human victim into revealing sensit ive information to the attacker or to deploy malicious software on the victim's infrastructure like ransomware. Bluejacking is the sending of unsolicited messages over Bluetooth to Bluetooth-enabled devices such as mobile phones, PDAs, or laptop computers, sending a vCard which typically contains a message in the name field to another Bluetooth-enabled device via the OBEX protocol.

QUESTION 437
Your company is expanding its operations in the European Union and is concerned about additional governmental regulations that may apply. Which of the following regulations applies when processing personal data within the European Union?

A. PCI
B. PHI
C. Pll
D. GDPR

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.6: The General Data Protection Regulation (GDPR) is a regulation created in the European Union that creates provisions and requirements to protect the personal data of European Union (EU) citizens. Transfers of personal data outside the EU Single Market are restricted unless protected by like-for-like regulations, such as the US's Privacy Shield requirements. Personally identifiable information (PII) is data used to identify, contact, or locate an individual. Information such as social security number (SSN), name, date of birth, email address, telephone numberr, street address, and biometric data is considered PI I. Protected health information (PHI) refers to medical and insurance records, plus associated hospital and laboratory test results. The peripheral component interconnect (PCI) bus is used to provide low-speed co nnectivity to expansion

cards but has been mostly replaced by the faster PCie bus. The Payment Card Industry Data Security Standard (PCI-DSS) applies to companies of any size that accept credit card payments. If your company intends to accept card payment and store, process, and transmit cardholder data, you need to securely host your data and fol low PCI compliance requirements.

QUESTION 438
Fail to Pass Solutions has requested that its employees have a mobile device so that they can respond to questions when they are out of the off ice. Each employee is responsible for buying their Android smartphone and cellular plan service. To access the corporate network and its data, the employees need to install a company-provided APK on their device. This app contains access to their company-provided email, cloud storage, and customer relationship management (CRM) database. Which of the following policies BEST describes Fail to Pass's mobile device deployment model?

A. BVOD
B. COBO
C. COPE
D. CVOD

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.7: Bring Your Own Device (BYOD) is a mobile device deployment model that facilitates the use of personally owned devices to access corporate networks and data. Corporate Owned Business Only (COBO) is a mobille device deployment model that provides the employee with a corporate-owned device that may only be used for official work functions and purposes. Corporate Owned Personally Enabled (COPE) is a mobile device deployment model where the device remains the property of the organization, but certain personal use, such as private email, social networking, and web browsing, is also permitted. Choose Your Own Device (CYOD) is a mobille device deployment model where employees are offered a selection of corporate devices for work and, optionally, private use.

QUESTION 439
Which of the following installlation types would allow a single technician to quickly install Windows 10 Enterprise on 50 workstations simultaneously?

A. Refresh install
B. Image deployment
C. In-place upgrade
D. Repair installation

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.9: An image deployment is a type of installation that uses a done of an existing installation stored in an image file to perform the installation. The image can contain the base OS and configuration settings, service packs and updates, applications software, and whatever else is required. An image can be stored on DVD or USB media or can be accessed over a network. Repair installation is a type of installation that attempts to replace the existing version of the operating system files with a new copy of the same version. A repair installation is useful when trying to repair a Windows computer that will not boot or when you believe the system files have become corrupted. A refresh installation is a type of installation that will recopy the system files and revert most system settings to their default configuration while preserving user personalization settings, data files, and applications installed through the Windows Store. An in-place upgrade is an installation of the new operating system on top of an existing version of the operating system. An in-place upgrade will preserve the applications, user settings, and data files that already exist on the computer.

QUESTION 440

A printing company uses an isolated Windows XP workstation to print out large format banners for its customers on a custom printer. Unfortunately, the printer does not support newer versions of Windows and would cost $50,000 to replace it. To mitigate this risk, the workstation is not connected to the internet or a local area network. When a customer needs a banner printer, the technician takes a copy of their PDF file and moves it to the Windows XP workstation using a USB thumb drive. The workstation recently became 1infected with malware when printing a customer's file. The technician remediated the issue~ but the wo1rkstation became infected again three weeks later. Which of the following actions did the technician forget to perform?

A. Manually update the antivirus on t he workstation and set it to perform on-access scans
B. Connect the workstation to the Internet t·o receive the latest Windows XP patches
C. Perform a data wipe operation on the USB thumb drive before its next use
D. Disable System Restore and remove the previous restore points

Correct Answer: A
Explanation

Explanation/Reference:
Expla nation
OBJ-2.4: This is a legacy workstation since it is running Windows XP. Since Windows XP is considered end-of-life, there are no security patches or updates available for it. To mitigate this risk, the workstation should be run only as an isolated worlkstation. Since the workstation is not connected to a network and receives files through the connection of a USB thumb drive, this would be the only way a piece of malware could enter the system. The technician most likely neglected to update the antivirus/antimalware software on this workstation during the remediation. The technician should manually update the antivirus/antimalware definitions weekly. The workstation should also be configured to conduct on-access/on-demand scanning, as well.

QUESTION 441
A user's Android smartphone is sluggish in responding when the user tries to open any of its apps. The smartphone has 2 GB of memory and a 16 GB internal storage device. The technician saw that the smartphone currently has 1.7GB of memory in use and 412MB of free storage space on the internal storage device. Which of the following should t he technician perform to improve the device's performance?

A. Replace the device's screen
B. Replace the device's battery
C. Upgrade the internal storage device
D. Uninstall any unneeded apps

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.5: The smartphone is likely running out of memory, attempting to move data from the memory to the swap file, and the swap file is running low on space due to the internal storage device being almost full. Most smartphones do not allow the internal storage to be upgraded by technicians or end users. Some Android devices will have an external memory card slow that can be used for additional storage, but that was not an option presented in this scenario. To increase the performance of the smartphone, the technician should find any unnecessary applications and uninstall them with the consent of the user to free up additional internal storage s ace.

QUESTION 442
Whic·h command is used in the Linux terminal to change the permissions of a file?

A. chmod
B. sudo
C. chown
D. Pwd

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .1 1: The chmod command sets the permissions of files or directories on a Linux system. A set of f lags associated with each file determines who can access that file and how they can access it. These flags are called file permissions or modes. The command name chmod stands for change mode and it restricts the way a f ile can be accessed. The chown command is used to change the owner of the file, directory, or link in Linux. The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen. The sudo command allows programs to be executed as a superuser (known as the root user) or another user. The command's name is an abbreviation of the phrase "superuser do" and works on all Unix- based operating systems.

QUESTION 443
Jason checks the Dion Training server room and finds that it currently has only 10% humidity. Which of the following risks to the servers could occur due to this low humidity level?

A. Corrosion of the servers
B. An over-voltage event
C. An under-voltage event
D. Accidental static discharge

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.5: When humidity is low, stat ic discharge is the biggest threat. When humidity is low, static electricity is built up and can lead to an accidental release which damages components. When humidity is high, the water in the air can react with the components in the servers and cause corrosion. In a computer server room or work area, the humidity should be kept between 40-60% to prevent electrostatic discharge from low humidity and corrosion from high humidity. An electrostatic discharge (ESD) is the release of a charge from metal or plastic surfaces that occurs when a potent ial difference is formed between the charged object and an oppositely charged conductive object. This elect rical discharge can damage silicon chips and computer components if they are exposed to it.

QUESTION 444
Dion Training uses DHCP to assign private Class B IP addresses to its W~ndows 10 workstations. Which of the following IP addresses is a Class B address?

A. 1 0.5.34.15
B. 192.168.2.14
C. 172.16.13.12
D. 169.254.12 5.154

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.6: Private IP addresses are any addresses in a specified range that are not allowed to be routed over the Internet. This allows companies to use these private IP addresses in their local area networks without having to purchase them from an internet registry. The class A private IP address range contains the addresses from 10.0.0.0 to 10.255.255.255.255. The class B private IP address range contains the addresses from 172.1 6.0.0 to 172.31.255.255. The class C private IP address range contains the addresses from 192.168.0.0 to 192.168.255.255. The APIPA/link-local autoconfiguration range is from 169.254.0.0 to 169.254.255.255.

QUESTION 445
Nicole's smartphone works fine when she is at work or the mall, but she has limited bandwidth on the device when she is in her apa1rtment building. Nicole has asked you to help her. What is the FIRST step you should take in troubleshooting this issue?

A. Reset the data usage statistics on the smartphone
B. Update the smartphone's applications or OS
C. Reset the smartphone's wireless network settings
D. Verify the smartphone has adequate signal strength

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.4: The smartphone likely has lower signal strength when she· is in the apartment building. If she has 1 or 2 bars of signal at home, but 4 to 5 bars of signal at work or the mall, then she will have significantly reduced bandwidth when operating over the cellular network from her apartment. To solve this issue, the user will need to use a Wi-Fi connection instead or use a cellular signal booster in her apartment. A cellular signal boost er is a device that acts as a micro-cellular tower and connects to a user's home network to provide better cellular service 1n an area.

QUESTION 446
Edua1rdo is installing Windows 11 (64-bit) in a virtual machine on his macOS desktop. The installation is continually failing and producing an error. Eduardo has configured the virtual machine with a 2.2 GHz processor, 4 GB of memory, a 64GB hard drive, and a 1280 x 720 screen resolution. Which item in the virtual machine should be increased to fix the installation issue experienced?

A. Number of CPU cores
B. The screen resolution
C. Amount of memory
D. Amount of hard drive space

Correct Answer: A
Explanation

Explanation/Reference:
OBJ- 1.7: The number of CPU co res needs to be increased. For the Windows 11 (64 -bit) operating system, the minimum requirements are a d ual-core 1 GHz processor, 4GB of RAM, and at least 64GB of hard drive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processo r, 2GB of RAM, and at least 20GB of hard drive space.

QUESTION 447
Which of the following network configurations is used to identify your computer's individual host identifier and your computer's network identifier?

A. Gateway
B. WINS
C. Subnet mask
D. DNS

Correct Answer: C
Explanation

Explanation/Reference:

OBJ-1.6: The sub net mask is used to identify the host identifier and the network identifier uniquely in combination with the IP address. The subnet mask is used by the TCP/IP protocol to det errmine whether a host is on the local subnet or a remote network. The default gateway parameter is the IP add ress of a router to which packets destined for a remote network should be sent by default. This setting is not required, but if you do not have one included, your network traffic can never leave the local area network. Windows Internet Name Service (WINS) is a legacy computer name registration and resolution service that maps computer NetBIOS names to IP addresses. The domain name system (DNS) protocol is the protocol used to provide names for an IP address based on their mappings in a database using TCP/UDP port 53.

QUESTION 448
Which of the following commands is used on a Linux system to switch t:o another user's account?

A. chown
B. ps
C. su
D. Passwd

Correct Answer: C
Explanation

Explanation/Reference:
OBJ- 1.1 1: The su command, which stands for substitute user, is used by a computer user to execute commands with the privileges of another user account. When executed, it invokes a shell without changing the current working directory or the user environment. When the command is used without specifying the new user id as a command-line argument, it defaults to using the system's superuser account (user id 0). The command sudo is related and executes a command as another user but observes a set of constraints about which users can execute which other users can execute. The chown command is used to change the owner of the file, directory, or link in Linux. The ps command is used to list the currently running processes, and their PIDs and some other information depend on different options. It reads the process information from the virtual files in the /proc file system. The /proc directory contains virtual files and is known as a virtual file system. The passwd command changes passwords for user accounts. A normal user may only change the password for their account, while the superuser may change the password for any user.

QUESTION 449
Which of the following data types would be used to store a user's name?

A. Integers
B. St ring
C. Floating point
D. Boolean

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.8: A string stores a group of characters, such as Hello, PYTHON, or JasonDion. A string data type usually consumes as much storage as necessary. Each character in the string usually requires 1 byte of storage. A boolean stores a value of TRUE (1) or FALSE (0). It usually consumes only 1 bit of storage (a zero or a one). An integer stores a whole number, such as 21, 143, or 1024. An integer data type usually consumes 8 bytes of storage. A floating-point number stores a fractional or decimal number, such as 3.14, 45.5, or 333.33. A floating-point number data type usually consumes 4 to 8 bytes of storage.

QUESTION 450
Dion Training is building a new computer for its video editor to use. The new computer will use four physical Intel Xeon processors, 128GB of DDR4 memory, and a RAID 0 with two 2 TB SSDs for optimal performance. Which of the following editions of Windows 10 would support all of this computer's resources properly?

A. Home
B. Education
C. Pro for Workstations
D. Pro

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.1: Microsoft Windows 10 Pro for Workstations is designed to run on devices with high-performance configurations, including server-grade Intel Xeon and AMD Opteron processors. Windows 10 Pro for Workstations and Windows 10 Enterprise both support up to four physical CPUs and 6 TB of RAM. Windows 10 Pro and Windows 10 Education both only support two physical CPUs and 2 TB of RAM. Windows 10 Home only supports one physical CPU and up to 128 GB of RAM.

QUESTION 451
Dion Training has recently replaced the batteries in their rack-mounted UPS in their data center. Which of the following should their technicians do to dispose of the depleted batteries?

A. Research local regulations for toxic waste disposal in their area
B. Review the material safety data sheet for disposal instructions
C. Wrap the batteries in plastic and place them in the trash
D. Place the batteries in the recycle bin behind their office building

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.5: UPS batteries are considered a form of toxic waste and their disposal will be dictated by local regulations in the company's geographic area. Normally, there will be specific landfills or disposal sites that can accept depleted batteries for recycling or other methods of disposal. Technicians should not place toxic waste in the recyde bin or trash.

QUESTION 452
Tamera just purchased a Wi-Fi-enabled Nest Thermostat for her home. She has hired you to install it, but she is worried about a hacker breaking into the thermostat since it is an IoT device. Which of the following is the BEST thing to do to mitigate Tamera's security concerns? (Select TWO)

A. Configure the thermostat to use a segregated part of the network by installing it into a screened sub net
B. Configure the thermostat to connect to the wireless network using WPA2 encryption and a long, strong password
C. Configure the thermostat to use the WEP encryption standard for additional confidentiality
D. Upgrade the firmware of the wireless access point to the latest version to improve the security of the network
E. Enable two-factor authentication on the device's website (if supported by the company)
F. Disable wireless connectivity to the thermostat to ensure a hacker cannot access it

Correct Answer: AB
Explanation

Explanation/Reference:
OBJ-2.9: The BEST options are to configure the thermostat to use the WPA2 encryption standard (if supported) and place any Internet of Things (IoT) devices into a DMZ/screened subnet to segregate them from the production network. While enabling two-factor authentication on t he device's website is a good practice, it will not increase the IoT device's security. While disabling the wireless connectivity to the thermostat will

ensure it cannot be hacked, it also will make the device ineffective for the customer's normal operational needs. WEP is considered a weak encryption scheme, so you should use WPA2 over WEP whenever possible. Finally, upgrading the wireless access point's firmware is good for security, but it isn't specific to the loT device's security. Therefore, it is not one of the two BEST options.

QUESTION 453
Which of the following BEST describes the process of documenting everyone who has physical access or possession of evidence?

A. Legal hold
B. Financial responsibility
C. Chain of custody
D. Secure copy protocol

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.6: Chain of custody refers to documentation that identifies all changes in the control, handling, possession, ownership, or custody of a piece of evidence. The chain of custody is an important part of documenting the evidence collected during an incident response. A legal hold is a process that an organization uses to preserve all forms of relevant information when litigation is reasonably anticipated. If a legal hold notice has been given to the backup service, they will not destroy the old backup tapes until the hold is lifted. Financial responsibility is the process of managing money and other kinds of assets in a way that is productive and works in the best interest of an organization. Secure copy protocol (SCP) is a means of securely transferring comput er files between a local host and a remote host or between two remote host s.

QUESTION 454
Which of the following wireless technologies allows a wireless device to automatica1lly be configured for a SOHO wireless network with the push of a button?

A. WEP
B. WPA2
C. WPS
D. WPA

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: The Wi- Fi Protected Setup (WPS) is a mechanism for auto-configuring a WLAN s~ecu rely for home users. On compatible equipment, users push a button on the access point and connect adapters to associate them securely. WPS is subject to brute force attacks against the PIN used to secure them, making them vulnerable to attack. Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks t hat can break its encryption. WEP relies on the use of a 24-bit initialization vector to secure its preshared key. Wi-Fi protected access (WPA) is an improved encryption scheme for protecting Wi- Fi communications designed to replace WEP. WPA uses the RC4 cipher and a temporal key integrity protocol (TKIP) to overcome the vulnerabilities in the older WEP protect ion scheme. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for enc tion.

QUESTION 455
Which of the following remote access protocols should you use to connect to a Windows 2019 server and control it with your mouse arnd keyboard from your workstation?

A. VNC
B. RDP
C. Telnet
D. SSH

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.9: The RDP (remote desktop protocol) is a Windows feature that allows a remote user to initiate a connection at any time and sign on to the local machine using an authorized account. This connection allows a Windows administrator to see and control what is on a remote computer's screen. RDP authentication and session data are allways encrypted. This means that a malicious user with access to the same network cannot intercept credentials or interfer,e or capture anything transmitted during the session. Secure Shell (SSH) uses port 22 to securely create communication sessions over the Internet for remote access to a server or system. Tel net uses port 23 to provide a bidirectional interactive text-oriented communication facility using a virtual terminal connection but sends its data in plaintext making it an insecure protocol. Virtual Network Computing (VNC) is a cross-platform screen sharing system that was created to remotely control another computer from a distance by a remote user from a secondary device as though they were sitting right in front of it.

QUESTION 456
Which of the following allows users to save their current session to disk and before powering down their Windows 10 laptop?

A. Sleep
B. Lock
C. Hibernate
D. Shutdown

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1 .4: Hibernate mode is used to save the current session to disk before powering off the computer to save battery life when the system is not being used. The computer takes longer to start up again from hibernate mode than it does from the sleep or standby mode. Sleep or standby mode is used to save the current session to memory and put the computer into a minimal power state to save battery life when the system is not being used. The computer takes less time to start up again from the sleep or standby mode than it does from the hibernate mode. Shutdown mode completely powers off the computer and does not save the current user session to disk. Instead, the shutdown will close all open files and log out the user during the shutdown process. A lock will secure the desktop with a password while leaving proograms running.

QUESTION 457
Which of the following MacOS features allows the user to create a user account that is used to sign in to the App Store, iCioud, and iTunes?

A. Passwd
B. Apple ID
C. Spotlight
D. Keychain

Correct Answer: B
Explanation

Explanation/Reference:

OBJ-1 .1 0: When first setting up an Apple Mac, the user will be assigned an Apple ID based on the sign-in email address. An Apple ID is a user account on an Apple device based on the sign-in email address that is used to sign in to the App Store, access iCioud, and other Apple features and functions. Spotlight is the file system search feature in the macOS environment. Keychain is a macOS app for managing passwords cached by the OS and supported browser/web applications. The passwd command changes passwords for user accounts on Unix, Linux, and macOS systems. A normal user may only change the password for their account, while the superuser may change the password for any user.

QUESTION 458
A customer is complaining that they cannot connect to the local network share drive. You run the command 'ipconfig /all' from their workstation, and it returns an IP of 169.254.34.12. Which of the following is the problem with this workstation?

A. The workstation couldn't reach the proxy server
B. The workstation couldn't reach the DHCP server
C. The workstation couldn't reach the DNS server
D. The workstation couldn't reach the gateway

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.4: Since the customer's IP address is 169.254.34.12, it is an APIPA address. Since the workstation has an APIPA address, it means the DHCP server was unreachable. Automatic Private IP Addressing (APIPA) is a feature of Windows-based operating systems that enables a computer to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function. APIPA serves as a DHCP server fail over mechanism and makes it easier to configure and support small local area networks (LANs). If no DHCP server is currently available, either because the server is temporarily down or because none exists on the network, the computer selects an IP address from a range of addresses (from 169.254.0.0 - 169.254.255.255) reserved for that purpose.

QUESTION 459
Which command would be used to display the network address and subnet mask for the wired network connection on a Linux system?

A. ipconfig
B. nslookup
C. ip
D. Nets tat

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.1 1: The ip command is used to display informat ion about the current wired network connection on a Linux system, including its IP address, subnet mask, and MAC address. The nslookup command is used to display and troubleshoot DNS records. The netstat command is used to display the network statistics. The ipconfig tool displays all current TCP/IP network configuration values on a Windows system.

QUESTION 460
You have discovered that an employee has been conducting illegal activities using his workplace computer. You have taken possession of the employee's laptop according to your company's procedures and are waiting to give it to law enforcement authorities. Wha1t should you do when turning over the laptop to the police?

A. Maintain the chain of custody
B. Quarantine the system

C. Preserve the evidence
D. Document the changes

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.6: The chain of custody is the chronological documentation or paper t rail that records the sequence of custody, control, t ransfer, analysis, and disposition of physical or electronic evidence. The chain of custody must be maintained from when you arrived at the laptop until you turn it over to law enforcement officials. As first responders, our job is to collect the evidence and maintain the chain of custody.

QUESTION 461
Which of the following Control Panel sections contains various tools like computer management, disk cleanup, print management, and the registry editor?

A. Devices and Printers
B. Device Manager
C. System
D. Administrative Tools

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.4: The Administrative Tools section of the control panel is used to collect various tools on the computer that are commonly used by system administrators. These tools include computer management, disk defragmentation, disk cleanup, the event viewer, the performance monitor, print management, the registry editor, the resource monitor, services, system configuration, system information, the task scheduler, and ot hers. The Device Manager is used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technidan can repair or replace it. The System section of the Control Panel allows a technician to see information about the workstation, including the processor type, amount of memory, and operat ing system version installed on the computer. The Devices and Printers section of the Control Panel allows a technician to manage the printers, scanners, and other external devices connected to a Windows computer.

QUESTION 462
You just installed a flat panel television in a conference room in your office building. The facilities manager is concerned that a lightning strike could damage it. The company is not worried about the threat of power outages because the conference room is only used a few times per week. Which of the following should be installed to BEST mitigate the facilities manager's concerns without spending too much money?

A. Power strip
B. UPS
C. Line conditioner
D. Surge suppressor

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.5: A surge suppressor defends aga inst possible voltage spikes that could damage your electronics, appliances, or equipment. A power strip will not protect against voltage spikes. A UPS or line condit ioner could protect against voltage spikes, but they cost much more than a surge suppressor. A surge suppressor should be used to meet the requirements of this question best. A line conditioner is a device that adjusts voltages in undervoltage and overvoltage conditions to maintain a 120 V output. Line conditioners raise a sag or under-

voltage event back to normal levels, but they cannot protect the line from a complete power failure or power outage. An uninterruptible power supply or uninterrupti ble power source (UPS) is an electrical apparatus that provides emergency power to a load when the input power source becomes too low or the main power fails. A UPS provides near-instantaneous protection from input power interruptions by using a battery backup. The onbattery run-time of most uninterruptible power sources is usually short (less than 60 minutes) but sufficient to properly shut down a computer system. A UPS or line conditioner could protect against voltage spikes, as well.

QUESTION 463
An employee was recently moved from the Human Resources department into the Sales department. Which of the following should you check to ensure they no longer have access to the employee data stored in the Human Resource department share drives?

A. Security Groups
B. Credential Manager
C. Group Policy
D. Home Folder

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.2: A security group is a collection of user accounts that can be assigned permissions in the same way as a single user object. Security groups are used when assigning permissions and rights, as it is more efficient to assign permissions to a group than to assign them individually to each user. You can assign permissions to a user simply by adding t he user to the appropriate group. In most corporate environments, security groups control access to share drives, mailing lists, and other network resources.

QUESTION 464
Which of the following commands is used on a Linux system to delete all the files and directories in a Linux system's filesystem?

A. rm -rf * .*
B. rm -rf I
C. rm *.*
D. rm/

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.1 1: The rm command is a command-line utility for removing~ files or directories. The "rm -rf /" is the most dangerous command to issue in Linux. The rm -rf command is one of the fastest ways to delete a folder and its contents. But a little typo or ignorance may result in unrecoverable system damage. The -r option means that the command will recursively delete the folder and its subfolders. The -f option means that even read-only files will be removed without asking the user. The use of I indicates that the remove command should begin at the root directory(/) and recursively force all files and folders to be deleted under the root. This would delete everything on the system. The*.* would only begin deleting from the current working directory and then delete all files and folders further down the directory structure, not the entire file system.

QUESTION 465
A co-worker just sent you a macro-enabled Microsoft Word document. After you opened the fi le, your computer began to delete the photos stored in your c:\photos directory. What type of malware did you MOST likely receive?

A. Virus

B. Trojan
C. Rootkit
D. Worm

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.3: A virus is malicious software designed to infect computer files or disks when it is activated. A virus may be programmed to carry out other malicious actions, such as deleting files or changing system settings. A t rojan is a type of malware that looks legitimate but can take control of your computer. A Trojan is designed to damage, disrupt, steal, or in general, inflict some other harmful action on your data or network. The most common form of a trojan is a Remote Access Trojan (RAT), which allows an attacker to control a workstation or steal information remotely. To operate, a trojan will create numerous processes that run in the background of the system. A worm is a standalone malware computer program that replicates itself to spread to other computers. Often, it uses a computer network to spread itself, relying on security failures on the target computer to access it. A worm can spread on its own, whereas a virus needs a host program or user interaction to propagate itself. A rootkit is a clandestine computer program designed to provide continued privileged access to a computer while actively hiding its presence. A rootkit is generally a collection of tools that enabled administrator-level access to a computer or network. They can often disguise themselves from detection by the operating system and antimalware solutions. If a rootkit is suspected on a machine, it is best to reformat and reimage the system.

QUESTION 466
You have been asked to help a user upgrade their laptop from Windows 10 to Windows 11. The user has asked that all of their applications, user profiles, documents, and PST files be preserved during the upgrade. Which of the following types of upgrades or installations should you perform on this laptop?

A. Clean installation
B. Unattended installation
C. In-place upgrade
D. Repair upgrade

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.1: An in-place upgrade will preserve all of the user's files and applications during the upgrade process from Windows 10 to Windows 11. An in-place upgrade is an installation of the new operating system on top of an existing version of the operating system. An in-place upgrade will preserve the applications, user settings, and data files that already exist on the computer. A clean install is an installation of the new O[perating system on a new computer or a computer that has been recently formatted. A clean install will completely replace the operating system software on the computer with the new operating system. During a clean install, all of the user's data, settings, and applications will be deleted. An unattended installation is a software or operating system installation where the configuration information is derived from an input file. Repair installlation is a type of installation that attempts to replace the existing version of the operating system files with a new copy of the same version. A repair installation is useful when trying to repair a Windows computer that will not boot or when you believe the system files have become corrupted.

QUESTION 467
Which of the following Windows tools can a technician use to gather information about a workstation and create a comprehensive list of hardware, system components, and the software environment used by that workstation?

A. devmgmt.msc
B. dxdiag.exe

C. msinfo32.exe
D. resmon.exe

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.3: System information (msinfo32.exe) is a utility that gathers information about your computer and displays a comprehensive list of hardware, system components, and the software environment that can be used to diagnose computer issues. Resource monitor (resmon.exe) is a utility used to display information about the use of hardware (CPU, memory, disk, and network) and software (file handles and modules) resources in real-time. The resource monitor helps check the performance counters of specific resources and decide a course of action to improve the performance. The DirectX diagnostic (dxdiag.exe) utility is used to collect info about devices to help troubleshoot problems with DirectX sound and video. It is a diagnostics tool used to test DirectX functionality and troubleshoot video-related or sound-related hardware problems. DirectX diagnostic can save text files with the scan results. Device manager (devmgmt.msc) is a utility used to view and control the hardware attached to the computer. The device manager will highlight a piece of hardware that is not working so that a technician can repair or replace it.

QUESTION 468
Whic.h of the following types of attacks involves changing the system's MAC address before it connects to a wireless network?

A. DDoS
B. Spoofing
C. Zombie
D. Botnet

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.4: Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing is an attack where the attacker disguises their identity. Examples of spoofing include changing their MAC address (MAC spoofing), their IP address (IP spoofing), or their email address (commonly used during a phishing campaign). A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources. A botnet is many internet-connected devices, each of which is running one or more bots. Botnets can be used to perform distributed denial -of-service (DDoS) attacks, steal data, send spam, and allow the attacker to access the device and its connection. A zombie (also known as a bot) is a computer or workstation that a remote attacker has accessed and set up to forward transmissions (including spam and viruses) to other computers on the internet.

QUESTION 469
Michael, a salesman, is on a business trip and is trying to access his corporate email over the hotel's Wi-Fi network. Michael's laptop appears to be connected to the hotel's wireless network, but his email client cannot download any new messages and states, "Network Offline." Michael contacts the help desk for assistance. What action should the help desk technician tell Michael to perform to solve this issue?

A. Open a web browser, enter google.com, and see if a redirect page is displayed
B. Disable and reenable the wireless network adapter on his laptop
C. Disconnect and reconnect to the hotel's wireless network
D. Perform a full system scan for malware on his laptop

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .6: Many hotels use a captive portal with a redirect page with their wireless networks. When users connect to the wireless network, they have to open a web browser and are then redirected to the hotel 's Acceptable Use Policy page. Until t he user accepts the terms and cond itions, none of their network traffic will be routed to the int ernet. If the redirect page is shown, Michael can then accept the terms and conditions, and his email client will be able to download his mail again.

QUESTION 470
What is the THIRD step of the seven-step malware removal process?

A. Quarantine the infected system
B. Disable System Restore in Windows
C. Enable System Restore and create a restore point in Windows
D. Update the applications and the operating system

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.3: The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe mode, pre-inst allation environment), (5) Schedule scans and run updat es, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 471
What is the minimum amount of storage space required to install Windows 10 (x86) on a device?

A. 64GB
B. 32GB
C. 20GB
D. 16GB

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1 .7: For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20 GB of hard drive space. For the Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64 GB of hard drive space.

QUESTION 472
Which of the following technologies would you use to securely access the command line interface of a network's switches and routers remotely for configuration?

A. RDP
B. Telnet
C. HTTPS
D. SSH

Correct Answer: D
Explanation

Explanation/Reference:

OBJ-4.9: SSH (Secure Shell) is used to remotely connect to a network's switches and routers to configure them securely. SSH is typically used for logging into a remote machine and executing commands, but it also supports tunneling, forwarding TCP ports, and X1 1 connections; it can transfer files using the associated SSH file transfer (SFTP) or secure copy (SCP) protocols. SSH uses the client-server model. The hypertext transfer protocol secure (HTTPS) is a secure protocol used to provide web content to browsers using SSL/TLS encrypt ion over TCP port 443. Tel net should not be used in a network due to its weak security posture. Tel net t ransmits all of the data in plain text (without encryption), including usernames, passwords, commands, and data fi les. For this reason, it should never be used in production networks and has been replaced by SSH in most corporate networks. Remote Desktop Protocol (RDP) is a Microsoft protocol designed to facilitate application data transfer security and encryption between client user devices and a virtual network server. It enables a remote user to add a graphical interface to the desktop of another computer.

QUESTION 473
Which of the following backup rotation schemes overwrites the oldest media with the current backup being performed?

A. Grandfather-father-son
B. FIFO Batckup
C. 3-2-1 backup
D. Tower of Hanoi

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.3: The First In First Out (FIFO) backup scheme uses a set number of tapes and overwrites the oldest tape with the newest information. For example, if there are 7 tapes in use, every evening a new backup is conducted over the previous week's daily backup. To have a longer amount of days of backups, a technician simply needs to increase the number of tapes from 7 to 14 or 21. The grandfather-father-son (GFS) backup rotation scheme is widely used to combine full and incremental backups to reduce backup time and enhance storage security. The grandfather is a full backup that is stored off-site once per month. The father is a weekly full backup that is conducted. The son is an incremental or differential backup conducted each day. For example, each Monday a full backup can be conducted which becomes the father. Then, each day of the week a son is created by performing an incremental or differential backup. Once per month, a fu ll backup is conducted to become the grandfather. The 3-2-1 backup rule states that an organization should create (3) one primary backup and two copies of the data, (2) save the backups to two different types of media, and (1) keep at least one backup copy off-site. The Tower of Hanoi is a backup rotation scheme that rotates backup media sets throughout the backup process to minimize wear and failure of tape backup media. For example, when using this method with four backup tapes labeled A, B, C, and D, a total of 16 days of backups can be maintained with just 4 tapes. Tape A is used every odd-11umbered day for 16 days. Tape B is used on days 2, 6, 10, and 14. Tape C is used on days 4 and 12. Tape D is used on days 8 and 16. This allows Tape A to be overwritten every other day, while Tapes B is overwritten every four days and Tapes C and Dare overwritten every 8 days.

QUESTION 474
Dion Training uses DHCP to assign private Class A IP addresses to its Windows 10 workstations. Which of the following IP addresses is a Class A address?

A. 192.168 .. 3.5
B. 172.18.2 1.252
C. 1 0.1.2.3
D. 169.254.1.52

Correct Answer: C
Explanation

Explanation/Reference:

OBJ-1 .6: Private IP addresses are any addresses in a specified range that are not allowed to be routed over the Internet. This allows companies to use these private IP addresses in their local area networks without having to purchase them from an internet registry. The class A private IP address range contains the addresses f rom 10.0.0.0 to 10.255.255.255.255. The class B private IP address range contains the addresses from 172.16.0.0 to 172.31.255.255. The class C private IP address range contains the addresses from 192.168.0.0 to 192.168.255.255. The APIPA/link-local autoconfiguration range is from 169.254.0.0 to 169.254.255.255.

QUESTION 475
A network administrator receives a call asking for assistance with connecting to the network. The person on the phone asks for the IP address, subnet mask, and VLAN required to access the network. What type of attack might this be?

A. Zero-day attack
B. VLAN hopping
C. Spoofing
D. Social engineering

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.4: Social engineering is a type of attack on a network in which an attacker uses their confidence and their victims' gullibility to gain access. It is the only type of attack on a network that is directed towards the human element. The human interaction with the network administrator makes the other three answers . Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. A zero-day attack happens once that flaw, or software/hardware vulnerability, is exploited, and attackers release malware before a developer has an opportunity to create a patch to fix the vulnerability, hence the term zero-day. VLAN hopping is a method of attacking networked resources on a virtual LAN to gain access to traffic on other VLANs that would normally not be accessible.

QUESTION 476
Your company has just installed a new proxy server and has asked you to configure all of the Windows workstations to use it. Which of the following Internet Options tabs in the Windows Control Panel should you configure?

A. General
B. Content
C. Privacy
D. Connections

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.4: The Connections tab in the Internet Options is used to set up the dial-up and VPN settings and the LAN settings. Under the LAN settings, you can configure the proxy server settings for the system.

QUESTION 477
Which of the following types of backup requires the LEAST time to complete a backup?

A. Incremental
B. Synthetic
C. Full
D. Differential

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.3: An incremental backup only creates a copy of new files and files modified since the last full, incremental, or differential backup. Therefore, it takes the least amount of t ime to complete a backup. Unfortunately, it also takes the most time to restore since you have to first restore the full backup, then any differential and incremental backups until all your data is restored. A full backup creates a copy of all the selected data regardless of when it was previously backed up. It takes the most time to complete a backup but is the fastest when conducting a restoral of all the data on a hard drive. A differential backup only creates a copy of the selected data that has been modified since the last full backup. It is a good compromise in speed between a full backup (which takes the longest to backup and the least to restore) and an incremental backup (which takes the least to backup and the longest to restore). Synthetic backup is the process of generating a file from a complete copy of a file created at some past time and one or more incremental copies created at later times. The expression synthetic in this context refers to the fact that the assembled file is not a direct copy of any single current or previously created file. Instead, a synthetic file is merged or synthesized by a specialized application program from the original file and one or more modifications to it.

QUESTION 478
You need to move a 75-pound box with a rack-mounted UPS in it. Which of the following actions should you take?

A. Open the box and carry up the UPS in pieces
B. Ask a coworker to team lift it with you
C. Lift with your legs and not your back
D. Lift with your back and not your legs

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.4: Since the box is over 50 pounds, you should ask a coworker to team lift the box with you. Team lifting is when two or more people work together to pick up a heavy or bulky object. When you need to lift or carry items, be aware of what your weight limitations are, as well as any restrictions and guidance outlined in your job description or site safety handbook. Weight limitations will vary depending on context. When lifting objects, always lift using your legs and not your back. A rack-mounted UPS is a self-contained unit, making it impossible to carrry up in multiple pieces.

QUESTION 479
Your company wants to provide a secure SSO solution for accessing both the corporate wireless network and its network resources. Which of the following technologies should be used?

A. WEP
B. WPA2
C. WPS
D. RADIUS

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.2: With RADIUS and SSO configured, users on the network can provide their user credentials one time when they initially connect to the wireless access point or another RADIUS client and are then automatically authenticated to all of the network's resources. The Remote Authentication Dial-in User Service (RADIUS) is used to manage remote and wireless authentication infrastructure. Users supply authentication information to RADIUS client devices, such as wireless access points. The client device then passes the authentication data to an AAA (Authentication, Authorization, and Accounting) server that processes the request. The Terminal

Access Controller Access Control System (TACACS+) is a proprietary alternative to RADIUS developed by Cisco for handling authentication. The Wi-Fi Protected Setup (WPS) is a mechanism for auto-configuring a WLAN securely for home users. On compatible equipment, users push a button on the access point and connect adapters to associate them securely. WPS is subject to brute force attacks against the PIN used to secure them, making them vulnerable to attack. Wired equivalent privacy (WEP) is an older mechanism for encrypting data sent over a wireless connection. WEP is considered vulnerable to attacks that can break its encryption. WEP relies on the use of a 24-bit initialization vector to secure its preshared key. Wi-Fi protected access version 2 (WPA2) replaced the original version of WPA after the completion of the 802.11 i security standard. WPA2 features an improved method of key distribution and authentication for enterprise networks, though the pre-shared key method is still available for home and small office networks. WPA2 uses the improved AES cipher with counter mode with cipher-block chaining message authentication protocol (CCMP) for encryption.

QUESTION 480
You attempt to boot a Windows 10 laptop and receive an "Operating System Not Found" error on the screen. You can see the hard disk listed in the EFI/BIOS of the system. Which of the following commands should you use to add the Windows installation to the boot manager?

A. bootrec /fixboot
B. bootrec /rebuildbcd
C. diskpart list
D. bootrec /fixmbr

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.1: The Boot Configuration Data (BCD) stores the list of known Windows installations that can be booted from a hard drive. If the Windows installation is not listed, the computer will be unable to boot into W'indows. To add a missing Windows installation to the Boot Configuration Database (BCD), you should use the command "bootrec /rebuildbcd" and reboot the computer. If the disk cannot be detected, enter the system setup and try modifying settings (or even resetting the default settings). If the system firmware reports the disk's presence, but Windows still will not boot, use a startup repair tool to open a recovery mode command prompt and use the bootrec tool to repair the drive's boot information. The "bootrec /fixmbr" command is used to attempt a repair of the master boot record of a drive. The "bootrec /fixboot" command is used to attempt a repair of the boot sector of a drive. The diskpart command is a command-line disk-partitioning utility available for Windows that is used to view, create, delete, and modify a computer's disk partitions.

QUESTION 481
You have just finished installing a new workstation for a user in your office. They need to be able to see the other workstations on the company's workgroup. Which of the following settings should you ensure is enabled?

A. Enable an RDP connection
B. Enable network discovery
C. Enable file and folder sharing
D. Enable Bitlocker

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1.6: Network discovery allows Windows 10 to find other comput ers and devices on a network. This feature is automatically tumed on when connected to private networks like the one in your home or workplace. Network discovery is turned off when you're connected to public networks that shouldn't be trusted, and you should not allow your PC to be discoverable on those networks. If your Windows 10 computer or device can't view other computers on the network, two things are probably at fault: either the network profile is assigned (public instead or private), or network discovery is disabled. Remote desktop protocol (RDP) is used to

connect to a remote desktop session on a host computer or server. File and folder sharing is enabled to allow other users on a network to access files and folders on a computer or server. Bitlocker is used on a Windows 10 Pro, Education, or Enterprise edition workstation to perform full disk encryption on the operating systems storage devices.

QUESTION 482
An employee at Dion Training is complaining that every time they reboot their Windows 10 workstation a music application is loaded. Which of the following commands would you use to disable the program from starting up each time Windows reboots?

A. Event viewer
B. User account control
C. System information
D. Task manager

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.3: The task manager is an advanced Windows tool that has 7 tabs that are used to monitor the Processes, Performance, App History, Start up, Users, Details, and Services on a computer. If you click on the Startup tab, you will see every program configured to start up when Windows is booted up. This can be used to disable unwanted programs from launching during the boot-up process. System information (msinfo32.exe) is a utility that gathers information about your computer and displays a comprehensive list of hardware, system components, and the software environment that can be used to diagnose computer issues. The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems. User account control (UAC) is used to prevent malware from damaging a PC by blocking the automatic installation of unauthorized apps and preventing inadvertent changes to system settin s.

QUESTION 483
John is a PC technician. To perform his job, he needs to be able to install and remove programs, modify system f iles, and change user permissions on the Windows workstation in his office. Which of the following types of user account types should he have to perform his role?

A. Guest
B. Power User
C. Remote Desktop User
D. Administrator

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.5: An administrator account is a Microsoft Windows user account that can perform all tasks on the computer, including installing and uninstalling apps, setting up other users, and configuring hardware and software. By default, the rights and permissions that are granted to the Power Users group include those rights and permissions that are required to allow members of the Power Users group to install devices and to install programs that do not modify the operating system files. They have some of the permissions of an administrator but without the ability to change everything in a Windows workstation. A Windows guest account will let other people use your computer without being able to change PC settings, install apps, or access your private files. A Guest account is a Microsoft Windows user account with limited capabilities, no privacy, and is disabled by default. A remote desktop user is a user role that enables the account to log in to a system remotely using RDP.

QUESTION 484
Your Windows 10 workstation is attempting to boot up when it receives the following error, "BOOTMGR is

missing; Press Ctri+Ait+Del to restart." To fix this, you insert your Windows installation disc and reboot into the Command Prompt under the System Recovery Options. Which of the following commands should you enter in the command prompt?

A. bootrec /fixboot
B. chkdsk /repair
C. sfc /fixboot
D. diskpart /repair

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: The partition boot sector is stored on the hard disk drive and contains the necessary code to start the Windows boot process. If this partition is corrupt or not properly configured during a Windows install, it would lead to "BOOTMGR is missing or corrupt" errors at startup. You should reboot into the command Prompt under the System Recovery Options using the Windows installation disc to fix this. Then, you should enter bootrec / fix boot. If the master boot record is corrupted, you can also run bootrec /fixmbr and the bootrec /fixboot to solve this issue. The diskpart command is a command-line disk-partitioning utility available for Windows that is used to view, create, delete, and modify a computer's disk partitions. The chkdsk command is used to check the file system and file system metadata of a volume for logical and physical errors. If used without parameters, chkdsk displays only the status of t he volume and does not f ix any errors. If used with the /f, / r, / x, or /b parameters, it fixes errors on the volume. The system file checker (SFC) command is a utility in Windows that allows users to scan for and restore corrupted Windows system files from the command line.

QUESTION 485
What is the minimum processor required to install Windows 11 (x64) on a device?

A. 2 GHz dual-core processor
B. 1 GHz single-core processor
C. 1 GHz dual-core processor
D. 2 GHz single-core processor

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.7: For the Windows 11 (64- bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4GB of RAM, and at least 64GB of hard dr ive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16 GB of hard drive space. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space.

QUESTION 486
Which of the following commands is used on a Linux system to change a user's password on the system?

A. passwd
B. chmod
C. chown
D. Pwd

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.1 1: The passwd command is used to change a user's account password on a Linux system. A normal

user can run passwd to change their password, and a system administrator (the superuser) can use passwd to change another user's password or define how that account's password can be used or changed. The chmod command sets the permissions of files or directories on a Linux system. A set of flags associated with each file determines who can access that file and how they can access it. These flags are called file permissions or modes. The command name chmod stands for change mode and it restricts the way a file can be accessed. The chown command is used to change the owner of the file, directory, or link in Linux. The pwd command displays the present working directory (current directory) path to the terminal or display. If you are working on a Linux system and are unsure of where you are in the directory structure, type "pwd" and hit enter to display the path to the screen.

QUESTION 487
Which of the following devices should you NEVER disassemble during troubleshooting due to the risk of electrocution?

A. Power supply
B. Tablet
C. LCD display
D. Printer

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.4: A power supply contains large capacitors that could retain high electricity levels even after being disconnected. A power supply is considered a field -replaceable part. It should not be fixed. It should simply be replaced. A technician should never open a power supply or stick anything into its interior for fear of electrocution. Printers, tablets, and LCD displays all have field replaceable parts that a technician can install, remove, or replace.

QUESTION 488
Which of the following components presents the largest risk of electrical shock to a technician?

A. Solid-state device
B. LCD monitor
C. Power supply
D. Laptop battery

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.4: A power supply contains large capacitors that could retain high electricity levels ~even after being disconnected. A power supply should be disposed of carefully. A technician should never open a power supply or stick anything into its interior for fear of electrocution. Solid-state devices, LCD monitors, and laptop batteries do not contain high voltage levels.

QUESTION 489
A user is complaining that the touchscreen on their smartphone is not responding to their touch. What is the FIRST step you recommend to solve this issue?

A. Reinstall! the OS
B. Have the user restart the device
C. Enable and disable airplane mode
D. Replace the defective touchscreen

Correct Answer: B

Explanation

Explanation/Reference:
OBJ-3.4: If a smartphone's touchscreen is unresponsive, the first step is to restart (or reboot) the device. This will cause the operating system and its device drivers to be reloaded and normally restore the touchscreen's funct ionality if it is a software issue. If this doesn't work, the technician may need to reinst all the OS if it is a software issue. If it is a hardware issue, then the touchscreen would need to be replaced. Airplane mode should not affect the touchscreen's operation.

QUESTION 490
After a company rolls out software updates, Ann, a lab researcher, can no longer use the lab equipment connected to her PC. The technician contacts the vendor and determines there is an incompatibility with the latest version of the drivers. Which of the following should the technician perform to get the researcher back to work as quickly as possible?

A. Downgrade the PC to a working patch level
B. Restore Ann's PC to the last known good configuration
C. Reset Ann's equipment configuration from a backup
D. Rollback the drivers to the previous version

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.1: By rolling back the drivers, Ann would be able to use her lab equipment again. To roll back a d river in Windows means to return the driver to the version that was last installed for the device. Every change should be accompanied by a rollback (or backout) plan so that the change can be reversed if it has harmful or unforeseen consequences. If you are experiencing problems with a device and you have recently updated the driver, Windows also provides a Roll B,ack Driver feat ure. A new driver may not work properly because it has not been fully tested or it may not work on your particular system. Driver rollback can recover a system speedily and easily where this has occurred. You can use Device Manager to revert to the previous driver. Right-click the device and select Properties. Click the Driver tab then click the Roll Back Driver button.

QUESTION 491
Jason wants to configure his Windows 10 laptop to more quickly find files when he is searching its hard drive. Which of the following Control Panel sections should he use to configure his laptop for optimal searching performance?

A. File Explorer Options
B. Internet Options
C. Indexing Options
D. Power Options

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.4: The Indexing Options is used to configure the method used by Windows when searching for content within the storage devices. When indexing is properly configured, the system will catalog the information on the computer using the words within the files and their metadata to more easily find the content when requested by a user. The File Explorer Options section of the Control Panel allows technicians to customize the display of files and folders. For example, the File Explorer Options can enable or disable the ability to show hidden files, hide file extensions, and more. The Internet Options section of the Control Panel allows a technician to manage the Internet settings for their computers, including the security settings, access settings, and add-on control settings. The Power Options section of the Control Panel allows technicians to customize how a computer manages its power to either conserve energy at the expense of performance or to maximize performance at the expense of energy savings by creating a power plan.

QUESTION 492
Your son just attempted to start up three programs at once on his Windows 10 Home laptop. The system appears to be unresponsive, and a spinning circle has replaced his mouse cursor on the screen. What is the BEST solution to this problem?

A. Kill the unresponsive task
B. Restart the network services
C. Disable the applicat ion startup
D. Reboot the system

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: When an application becomes unresponsive, it is best to either wait or kill the process. To kill a task or process, open the Task Manager, and click More Details. Then, select the unresponsive task and cl ick End Task. The task manager is an advanced Windows tool that has 7 tabs that are used to monitor the Processes, Performance, App History, Startup, Users, Details, and Services on a computer. The Processes tab in the task manager is helpful to quickly see how system resources are utilized, help troubleshoot applications, or find out why the computer is performing slowly. The task manager can identify and stop processes that use excessive system resources and keep the computer operating at higher speeds.

QUESTION 493
You are troubleshooting a workstation and want to check if any S.M.A.R.T. errors are being reported. Which of the following tools should you use to troubleshoot this workstation?

A. Disk management
B. DxDiag
C. Performance monitor
D. Task scheduler

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.1: The disk management tool is used to display the drive status, mount the drive, initialize the drive, and create/split/extend/shrink drive partitions. The utility displays a summary of any fixed and removable drives attached to the system. From the Disk Management console, you can see the S.M.A.R.T. status of each hard disk. The task scheduler is a tool included with Windows that allows predefined actions to be automatically executed whenever a certain set of conditions is met. For example, you can schedule a task to run a backup script every night or send you an email whenever a certain system event occurs. The DirectX diagnostic (dxdiag.exe) utility is used to collect info about devices to help troubleshoot problems with DirectX sound and video. It is a diagnost ics tool used to test DirectX functionality and troubleshoot video-related or sound-related hardware problems. DirectX diagnostic can save text fi les with the scan results. Performance monitor (perfmon.msc) is a performance monit oring and system monitoring utility in Windows that is used ito monitor the activities on CPU and memory activity on a computer. The performance monitor is used to view performance data either in real-time or from a log file. The performance monitor can only monitor the resource utilization, but it cannot manage or terminate those processes.

QUESTION 494
Which of the following features allows a Linux server to provide file-sharing services to a company's Windows 10 workstations?

A. Yum
B. Samba

C. Keychain
D. Pathping

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .11: Samba is used by Linux computers to enable the sharing and access of resources with Windows-based networks. Samba can also be used by Linux servers to provide file-sharing services to Windows clients. The ping path command is a Windows command-line tool that is used to locate spots that have network latency and network loss between a client and a destination. The advantages of PathPing over ping and traceroute are that each node is pinged as the result of a single command and that the behavior of nodes is studied over an extended period, rather than the default ping sample of four messages or default traceroute single route trace. The yum command is a package manager used with RPM-based Linux distribut ions to install new software packages, remove existing software packages, upgrade existing software packages, and even upgrade the entire operating system. Keychain is a macOS app for managing passwords cached by the OS and supported browser/web applications.

QUESTION 495
You are troubleshooting a user's laptop that is unable to print a document. You have verified the printer is working and properly connected to the workstation by USB. Which of the following actions should you attempt to f ix the problem in Windows 1 0?

A. Rollback the USB drivers
B. Restart Windows Defender
C. Restart the print spooler service
D. Disable/enable the wireless network adapter

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.1: Based on the issue described, it is likely that the print spooler service is not started or has become hung. To fix this issue, an administrator should restart the print spooler service. The Print Spooler is software built into the Windows operating system that temporarily stores print jobs in the computer's memory until the printer is ready to print them. In some circumstances, you may need to stop and/or restart the service. To access the Print Spooler, you must open the Local Services console. If restarting the print spooler doesn't fix the issue, the technician should check the driver and determine if it is fau lty and needs to be rolled baclk or upgraded.

QUESTION 496
You have just set up a Minecraft server on a spare computer within your network and want your friends to connect to it over the internet. What do you need to configure in your SOHO router to allow your friends to connect to the new Minecraft server you created?

A. Update the firmware
B. Enable DHCP
C. Configure port forwarding
D. Configure your Wi-Fi to use Channel11

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: Port forwarding occurs when a router takes requests from the Internet for a particular application, such as HTTP/port 80), and sends them to a designated host on the local area network. This question did not

mention that Wi- Fi was being used in the 2.4 GHz frequency range, therefore using channels 1, 6, and 11 is not required to minimize interference. The dynamic host control protocol (DHCP) is a protocol used to allocate IP addresses to a host when it joins a network. DHCP does not need to be configured to use a server and most servers use static IP addresses instead of dynamic ones. The firmware is a set of software instructions stored semi-permanently (embedded) on a hardware device. Modern types of f irmware are stored in flash memory and can be updated more easily than legacy programmable Read-Only Memory (ROM) types.

QUESTION 497
Which of the following policies should be created to provide employees with the guidelines and limitations they must follow when using company-provided email, computers, and network access?

A. Group policy
B. Local security policy
C. Acceptable use policy
D. Password policy

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-4.1 : An acceptable use policy (AUP) governs employees' use of company equipment and Internet services. Enforcing an acceptable use policy is important to protect the organization from the security and legal implications of employees (or customers) misusing its equipment. Typically, the policy will forbid the use of equipment to defraud, defame, or obtain illegal material. It is also likely to prohibit unauthorized hardware or software installation and explicitly forbid actual or attempted intrusion (snooping). An organization's acceptable use policy may forbid the use of Internet tools outside of work-related duties or restrict such use to break times. A local security policy is a set of policies relating to log on, passwo rds, and other security issues that can be enforced or disabled on the local machine. On domains, security policy is configured centrally using Group Policy Objects (GPO). A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. It contains items like password complexity, password age, and password history requirements. A Group Policy is the primary administrative tool for defining and controlling how programs, network resources, and the operating system operate for users and computers in an organization. In an active directory environment, Group Policy is applied to users or computers based on their membership in sites, domains, or organizational units.

QUESTION 498
You are working as a forensic investigator for the police. The police have a search warrant to capture a suspect's workstation as evidence for an ongoing criminal investigation. As you enter the room with the policeman, he arrests the suspect and handcuffs him. What should you do FIRST?

A. Implement the chain of custody
B. Turn off the workstation
C. Document the scene
D. Secure the area

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.6: As a forensic investigator, you should always 'secure the area' before taking any other actions. This includes ensuring that no other people are in the area to disrupt your forensic collection (such as the suspect or their accomplices), ensuring the workstation isn't unplugged from the network or the power, and other actions to prevent the evidence from being tampered with. Once the area is secure, then you should document the scene, begin your evidence collection, and implement the chain of custody.

QUESTION 499

You are working for a government contractor who requires all users to use a PIV device when sending digitally signed and encrypted emails. Which of the following physical security measures is being implemented?

A. Keyfob
B. Cable lock
C. Biometric reader
D. Smart card

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.1 : A smart card is used in applications that need to protect personal information and/or deliver fast, secure transactions, such as transit fa re payment cards, government, and corporate ident ification cards, documents such as electronic passports and visas, and financial payment cards. Often, smart cards are used as part of a multifactor authentication system in which the smart card and a PIN need to be entered for system authentication to occur. Biometrics are identifying features stored as digital data that can be used to authenticate a user. Typical features used include facial pattern, iris, retina, or fingerprint pattern, and signature recognition. This requires a relevant scanning device, such as a fingerprint reader, and a database of biomet ric information for authentication to occur. The Kensington lock is a small hole found on almost every portable computer or laptop made after 2000. It allows a cable lock to be attached to a portable computer or laptop to lock it to a desk and prevent theft. These locks often use a combination lock or padlock type of locking system. These locks do not affect the user's ability to use the laptop or device. It only prevents them from moving the laptop from the area. A key fob generates a random number code synchronized to a code on the server. The code changes every 60 seconds or so. This is an example of a one-time password. A SecureiD token is an example of a key fob that is produced by RSA.

QUESTION 500
A user contacts the service desk and states a hardware conflict error is showing in their Device Manager. Which of the following log files should you review to determine the source of the conflict?

A. Security log
B. Setup
C. System log
D. Application log

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.1: The event viewer shows a log of application and system messages, including errors, information messages, and warnings. It's a useful tool for troubleshooting all kinds of different Windows problems. The system log contains information about service load failures, hardware conflicts, driver load failures, and more. The file (system.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The security log contains information regarding audit data and security on a system. For example, the security log contains a list of every successful and failed login attempt. The file (security.evtx) is stored in the %System Root%\System32\ Winevt\Logs\ folder and can be opened using the Event Viewer. The application log contains information regarding application errors. The file (applicat ion.evtx) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer. The setup log contains a record of the events generated during the Windows installation or upgrade process. The file (setup.evt x) is stored in the %System Root%\System32\Winevt\Logs\ folder and can be opened using the Event Viewer.

QUESTION 501
Which version should you use when installing a Linux operating system and are concerned with end-oflife support?

A. L TS release
B. Beta release
C. Rolling release
D. Developer release

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .8: The LTS (Long-Term Support) release is well-supported and will be regularly updated by the Linux distribution to support new hardware, performance, and security improvements. These LTS releases are supported for a long time (app roximately 10 years), so they are great to use in production systems like servers. A beta release is a pre-release of a software product that is given out to a large group of users to try under real conditions. Beta versions have gone through alpha testing in-house and are generally fairly close in look, feel and function to the final product. A developer release is a pre-release of a software product that is given out to software developers to test and modify their existing products to the upcoming version of an operating system or application. Rolling release is a concept in software development where an application is frequently updated through the release of new features over time.

QUESTION 502
Dion Training utilizes a federation authentication model for all of its internal and external services. If an employee needs to access one of the company's web applications from their smartphone, they use a username and pa1ssword to log in to the main website. They then are transferred and authenticated to all of the other sites and services automatically. Which of the following type of authentication is this known as?

A. MFA
B. FaceiD
C. TouchiD
D. SSO

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.5: Single Sign-on (SSO) is an authentication technology that allows users to authenticate once and receive authorizations for multiple services. The advantage of single sign-on is that each user does not have to manage multiple user accounts and passwords. The disadvantage is that compromising the account also compromises multiple services. Multifactor authentication is an authentication scheme that relies on at least two of the five factors: something you know, something you have, something you are, something you do, and somewhere you are. Since only a u.sername and password are used in this scenario, it is not considered multi-factor authentication. Face ID is an Apple device feature t hat uses a face lock to grant access to the device. Face ID is considered a form of biometric authentication. Touch ID is an Apple device feature that uses fingerprint biometric information to grant access to the device.

QUESTION 503
A network technician must allow HTTP traffic from the Internet over port 80 to an internal server running HTTP over port 81. Which of the following is this an example of?

A. Static NAT
B. Port forwarding
C. Dynamic DNS
D. Dynamic NAT

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.9: Port forwarding is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are t raversing a network gateway, such as a router or firewall. Port Address Translation (PAT) is a type of dynamic NAT that can map multiple private IP addresses to a single public IP address by using port forwarding. Static NAT (Network Address Translation) is a one-to-one mapping of a private IP address to a public IP address. Dynamic NAT can be defined as mapping a private IP address to a public IP address from a group of public IP addresses known as the NAT pool. Dynamic NAT establishes a one-to-one mapping between a private IP address to a public IP address. Dynamic DNS (DDNS) is a method of automatically updating a name server in the Domain Name System (DNS), often in real-time, with the active DDNS configuration of its configured hostnames, addresses, or other information. Since this question focused on the relationship between port 80 at the gateway or public IP address being mapped to port 81 on the internet server, this is an example of port forwarding that was configured on the gateway or firewall of this network.

QUESTION 504
You are configuring a SOHO network and only denying specific IP addresses from accessing the network while allowing any IP addresses not found on the list. Which of the following should be implemented?

A. Allow list
B. MAC filtering
C. Blocklist
D. Port forwarding

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.9: A blacklist is a form of protection where only the items identified specifically on the list are blocked, whereas all others are allowed. For example, if you create an access control list that relies on blacklisting, it would allow every IP address not found in the allow list. An allow list is a form of protection where only the items identified specifically on the list are allowed, whereas all others are denied. For example, if you create an access control list that relies on an allow list, it would block every IP address that is not found in the allow list. MAC filtering is the application of an access control list to a switch or access point so that only clients with approved MAC addresses connect. Port forwarding allows a router to take requests from the Internet for a particular application and send them to a designated host on the LAN.

QUESTION 505
Which of the following file system formatting types should be used with a DVD?

A. FAT32
B. CDFS
C. UDF
D. NTFS

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1 .8: The Universal Disk Format (UDF or ISO 13346) is an updated file system for optical media supporting multisession writing. It is the standard used by Windows, referred to as the Live File System, for CD and DVD recordable and rewritable discs. There are several different versions of UDF, with 2.01 being the default in Windows. Blu-ray reading and writing requires version 2.5 and third-party software. The CD file system (CDFS or ISO 9660) is a legacy file system used for CD optical disc media (CD-ROM and CD- R). CDFS supports two main data writing modes: mode 1 has better error correction, whereas mode 2 allows more data to be written to the disc. Joliet is an extension to CDFS that enables long filename support and Unicode characters in file names. The NT file system (NTFS) is a Windows file system that supports a 64-bit address space and can provide extra features such as file-by-file compression and RAID support as well as

advanced file attribute management tools, encryption, and disk quotas. NTFS can support a maximum volume size of up to 8 PB. The file allocation table 32- bit (FAT32) is the 32-bit file system supported by Windows, macOS, and Linux computers. FAT32 can support maximum volume sizes of up to 2 TB and maximum file sizes of up to 4 GB.

QUESTION 506
Which of the following is an APIPA or link-local address?

A. 192.168 .. 1.34
B. 33.52.7.83
C. 127.0.0.1
D. 169.254.64.23

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.5: IP addresses are either public, private, localhost, or APIPA addresses. Automatic Private IP Addressing (APIPA) is a feature of Windows-based operating systems that enables a computer to automatically assign itself an IP address when there is no Dynamic Host Configuration Protocol (DHCP) server available to perform that function. When a host uses an APIPA address, it can communicate with other hosts on the same network using APIPA. Still, it cannot reach other networks or communicate with hosts who have managed to obtain a valid DHCP lease. Any address from 169.254.1.0 to 169.254.254.255 is considered an APIPA address. An APIIPA address is also referred to as a link-local address. A private IP address is in the range of 10.x.x.x, 172.1 6-31.x.x, or 192.168.x.x. A localhost IP is 127.0.0.1. All others are considered public IP addresses.

QUESTION 507
Tamera trying to install Windows 11 (64-bit) on an older laptop she found in her closet. The installation is continually failing and producing an error. The laptop has a dual-core 1.2 GHz processor, 2GB of memory, a 250 GB hard drive, and a 1280 x 720 screen resolution. Which item in the laptop must be upgraded to meet the minimum requirements for installing Windows 11?

A. The screen resolution
B. Amount of hard drive space
C. Number of CPU cores
D. Amount of memory

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1 .7: The amount of memory needs to be increased. For the Windows 11 (64-bit) operating system, the minimum requirements are a dual-core 1 GHz processor, 4 GB of RAM, and at least 64GB of hard drive space. For the Windows 10 (32-bit) operating system, the minimum requirements are a 1 GHz processor, 1 GB of RAM, and at least 16GB of hard drive space. For the Windows 10 (64-bit) operating system, the minimum requirements are a 1 GHz processor, 2GB of RAM, and at least 20GB of hard drive space.

QUESTION 508
David is a brand new help desk technician. To perform his job, he needs to install programs and printers but should not have full access to change everything on a Windows workstation. Which of the following types of user accounts should David be given to perform his job as a help desk technician?

A. Administrator
B. Power User
C. Guest

D. Remote Desktop User

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.5: By default, the rights and permissions that are granted to the Power Users group include those rights and permissions that are required to allow members of the Power Users group to install devices and to install programs that do not modify the operating system files. They have some of the permissions of an administrator but without the ability to change everything in a Windows workstation. A Windows guest account will let other people use your computer without being able to change PC settings, install apps, or access your private files. A Guest account is a Microsoft Windows user account with limited capabilities, no privacy, and is disabled by default. An administrator account is a Microsoft Windows user account that can perform all tasks on the computer, including installing and uninstalling apps, setting up other users, and configuring hardware and software. A remote desktop user is a user role that enables the account to log in to a syst,em remotely using RDP.

QUESTION 509
You just received your monthly smartphone bill. As you review your charges, you notice that this month shows three times as much data usage as a normal month. You don't remember changing your usage pattern, so there should not have been a large increase in data used. Which of the following should you do Fl RST to determine the source of the increased usage?

A. Configure your applications to only download large files over WiFi
B. Check network permissions and data usage for any applications installed within the last month
C. Conduct a factory restore of the smartphone and reload your applications
D. Enable biometric login for the lock screen to ensure no one else uses your device

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.5: You should FIRST check your network permissions and data usage for any applications installed within the last month. Some applications use background processes and daemons to download data over the network, even if you are not using the device. If there is a large increase in your data usage from one month to the next, you should check what may have changed during that month. This includes your usage patterns (which the question states haven't changed) and any applications you may have updated or installed.

QUESTION 510
Which of the following backup rotation schemes uses a complex mathematical puzzle to extend the number of unique days of backups stored with the least amount of tapes?

A. Tower of Hanoi
B. Grandfather-father-son
C. 3-2-1 backup
D. FIFO Backup

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.3: The Tower of Hanoi is a backup rotation scheme that rotates backup media sets throughout the backup process to minimize wear and failure of tape backup media. For example, when using this method with four backup tapes labeled A, B, C, and D, a tot al of 16 days of backups can be maintained with just 4 tapes. Tape A is used every odd-numbered day for 16 days. Tape B is used on days 2, 6, 10, and 14. Tape Cis used on days 4 and
12. Tape Dis used on days 8 and 16. This allows Tape A to be overwritten every other day, while Tapes B is

overwritten every four days and Tapes C and Dare overwritten every 8 days. The grandfather-father-son (GFS) backup rotation scheme is widely used to combine fu ll and incremental backups to reduce backup time and enhance storage security. The grandfather is a full backup that is stored off-site once per month. The father is a weekly full backup that is conducted. The son is an incremental or differential backup conducted each day. For example, each Monday a full backup can be conducte,d which becomes the father. Then, each day of the week a son is created by performing an incremental or differential backup. Once per month, a fu ll backup is conducted to become the grandfather. The 3-2-1 backup ru le states that an organization should create (3) one primary backup and two copies of the data, (2) save the backups to two different types of media, and (1) keep at least one backup copy off-site. The First In First Out (FIFO) backup scheme uses a set number of tapes and overwrites the oldest tape with the newest information. For example, if there are 7 tapes in use, every evening a new backup is conducted over the previous week's daily backup. To have a longer amount of days of backups, a technician simply needs to increase the number of tapes from 7 to 14 or 21.

QUESTION 511
Jason wants to configure his Windows 10 laptop to suspend individual USB ports when not in use. Which of the following Control Panel sections should he use to set the USB selective suspend feature?

A. Indexing Options
B. Power Options
C. File Explorer Options
D. Internet Options

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-1 .4: The USB selective suspend feature is located in the Power Options section of the Control Panel. The Power Options section of the Control Panel allows technicians to customize how a computer manages its power to either conserve energy at the expense of performance or to maximize performance at the expense of energy savings by creating a power plan. The USB selective suspend feature allows the hub driver to suspend an individual port without affecting the operation of the other ports on the hub. Selective suspension of USB devices is helpful when using a laptop computer as it helps to conserve battery power by powering off USB ports that are not needed at the time. The File Explorer Options section of the Control Panel allows technicians to customize the display of files and folders. The Indexing Options is used to configure the method used by Windows when searching for cont,ent within the storage devices. When indexing is properly configured, the system will catalog the information on the computer using the words within the files and their metadata to more easily find the content when requested by a user. The Internet Options section of the Control Panel allows a technician to manage the Internet settings for their computers, including the security settings, access settings, and add-on control settings.

QUESTION 512
Which of the following would NOT be included in a company's password policy?

A. Password age
B. Password style
C. Password complexity requirements
D. Password history

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.6: A password policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. A password policy is often part of an organization's official regulations and may be taught as part of security awareness training. It contains items like password complexity, password age, and password history requirements.

QUESTION 513
Which of the following operating systems cannot be run on a laptop?

A. Linux
B. Windows
C. iOS
D. Android

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.8: Apple's iOS can only be run on iPhones and iPads, not on laptops. Linux, Windows, macOS (OS X), and Android can all be run on laptops. Android is unique because it was originally designed to be run only on smartphones and tablets but has since been installed on many inexpensive laptops and desktops. Linux and Windows are both commonly installed on laptops and desktops.

QUESTION 514
Which of the following types of wireless connections requires a pin to be entered as part of the pairing process before it is utilized?

A. Radiofr·equency
B. NFC
C. Bluetooth
D. Infrared

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-3.4: Wireless devices with Bluetooth radios must be paired with each other before they can communicate. This involves making them discoverable and entering a PIN as part of the pairing process. The pairing process works with Bluetooth profiles, and each device has to be compatible. For example, you can only pair a mouse or keyboard with a device that's been designed to work with that type of accessory. Bluetooth is a wireless technology standard used for exchanging data between fixed and mobile devices over short distances using UHF radio waves in the industrial, scientific, and medical radio bands from 2.402 GHz to 2.480 GHz and building a personal area network (PAN). Infrared (IR) was a wireless networking standard supportin9 speeds up to about 4 Mbps with a direct line of sight for communications. Infrared sensors are used in mobile devices and with IR blasters to control appliances. While infrared (IR) used to be commonly used to connect wireless mice and keyboards to a laptop in the 1990s, it has fallen out of favor in the last 10-15 years since Bluetooth is more reliable and does not require a direct line of sight between the device and the laptop. Near-field communication (NFC) is a set of communication protocols that enable two electronic devices, one of which is usually a portable device such as a smartphone, to establish communication by bringing them within 4 em of each other. This is commonly used for contactless payment systems, transferring contacts, or transferring a f ile from one device to another. Radiofrequency (RF) is the propagation of radio waves at different frequencies and wavelengths. For example, Wi-Fi network products use a frequency of either 2.4 GHz or 5 GHz.

QUESTION 515
Your company is concerned about the possibility of power fluctuations that may occur and cause an immediate loss of power for several minutes to their server room. To prevent this condition, they are installing a large rack-mounted UPS to protect the server. Which type of condition are they trying to prevent using this UPS?

A. Under-voltage event
B. Power surge
C. Power spikes
D. Power failure

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.5: A power loss or power failure is a total loss of power in a particular area. To protect against a power loss or power failure, a battery backup should be used. A significant over-voltage event that occurs for a very short period of time is known as a power spike. A power spike is a very short pulse of energy on a power line. Power spikes can contain very high voltages up to and beyond 6000 volts but usually last only a few milliseconds instead of longer but lower voltage power surges. An extended over-voltage event is known as a power surge. A power surge is basically an inuease in your electrical current. A power surge often has levels of 10-30% above the normal line voltage and lasts from 15 milliseconds up to several minutes. An under-voltage event is a reduction in or restriction on the availability of electrical power in a particular area. The irregular power supply during an under-voltage event can ruin your computer and other electronic devices. Electronics are created to operate at specific voltages, so any fluctuations in power (both up and down) can damage them. To protect against an under-voltage event, you can use either a battery backup or a line conditioner.

QUESTION 516
You are configuring a new printer for a small real estate office. There are only 4 computers in the network, and they are all connected to a single 4-port switch/router/cable modem device. There are no additional open ports on the device and no servers configured within the network. All the computers operate as part of a single workgroup with no domain controller. You need to configure the printer to allow all 4 computers to print to it as long as they are connected to the switch. Which of the following methods would BEST allow the users to print to the printer based on this network's configuration?

A. Configure it as a shared printer connected to one of the four workstations
B. Configure the printer to support Bluetooth printing
C. Configure the printer to support cloud printing
D. Configure a print server and connect the printer to it

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1 .6: Due to the small size of the network and the lack of additional open switch ports, it would BEST to connect the printer to one of the workstations and configure it as a shared printer. This will allow any of the other workstations to print to the shared printer via the connected workstation. This allows the workstation to act as a print server, which means that the computer must always be left on or the rest of the users would be unable to print. Bluetooth printing is set up as a one-to-one pai ring between a single computer and a single printer that is located within 10 f eet. Since thus is a small office, they do not have a dedicated server to configure for use as a print server. Cloud printing is only supported by some printers and the question doesn't specify if this printer supports this feature.

QUESTION 517
Which editions of Windows 10 can you connect to using Remote Desktop?

A. Enterprise
B. Pro
C. Education
D. Home

Correct Answer: ABC
Explanation

Explanation/Reference:
OBJ-1 .1: A technician can connect to computers running Windows 10 Education, Pro, Pro for Workstations, or

Enterprise editions. Remote Desktop is not supported on computers running Windows 10 Home edition and requires third-party software to provide remote assistance to these computers. Remote desktop services (RDS) is used to connect to a remote desktop session host servers or other remote computers, edit an existing remote desktop connection (.rdp) configuration file, and migrate legacy connection files that were created with the client connection manager to the newer .rdp connection file type.

QUESTION 518
What is the symbolic representation of the octal numeric permission 644?

A. r--rw-rw-
B. rw--- ----
C. rw-r--r--
D. rwx-r-xr-x

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.6: RW- is 6 and R-- is 4. In Linux, you can convert letter permissions to octal by giving 4 for each R, 2 for each W, and 1 for each X. R is for read -only, W is for write, and X is for execute. The permissions strings are written to represent the owner's permissions, the group's permissions, and the other user's permissions.

QUESTION 519
Which of the following policies should be created to provide employees with the guidelines and limitations they must follow when using company-provided email, computers, and network access?

A. AUP
B. Pll
C. GDPR
D. DLP

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.1: An acceptable use policy (AUP) governs employees' use of company equipment and Internet services. Enforcing an acceptable use policy is important to protect the organization from the security and legal implications of employees (or customers) misusing its equipment. Typically, the policy will forbid the use of equipment to defraud, defame, or obtain illegal material. It is also likely to prohibit unauthorized hardware or software installation and to forbid actual or attempted intrusion (snooping) explicitly. An organization's acceptable use policy may forbid the use of Internet tools outside of work-related duties or restrict such use to break times. Data loss prevention (DLP) is a software solution that detects and prevents sensitive information from being stored on unauthorized systems or transmitted over unauthorized networks. Personally identifiable information (PII) is data used to identify, contact, or locate an individual. Information such as social security number (SSN), name, date of bi rth, email address, telephone number, street address, and biometric data is considered PI I. The General Data Protection Regulation (GDPR) is a regulation created in the European Union that creates provisions and requirements to protect the personal data of European Union (EU) citizens. Transfers of personal data outside the EU Single Market are restricted unless protected by like-for-like regulations, such as the US's Privacy Shield requirements.

QUESTION 520
You work for Dion Training as a physical security manager. You are concerned that the physical security at the entrance to the company is not sufficient. To increase your security, you are determined to prevent piggybacking. What technique should you implement first?

A. Install an RFID badge reader at the entrance

B. Install CCTV to monitor the entrance
C. Install an access control vestibule at the entrance
D. Require all employees to wear security badges when entering the building

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.1: An access control vestibule, or mantrap, is a device that only allows a single person to enter per authentication. This authentication can be done by RFID, a PIN, or other methods. Once verified, the mantrap lets a single person enter t hrough a system, such as a turnstile or rotating door. CCTV will not stop piggybacking, but it could be used as a detective control after an occurrence. Wearing security badges is useful, but it won't stop piggybacking by a skilled social engineer. RFID badges may be used as part of your entry requirements, but it won't stop a determined piggyback who follows an employee into t he building after their authenticated RFID access has been performed.

QUESTION 521
You are working as a desktop repair technician for a large corporation. The company uses the exact same desktop hardware for all of its user's workstations. Today, you have received multiple calls from users complaining that their screen becomes f illed with static when moving their mouse. You noticed that the systems all received a security patch and other updates from the Microsoft Endpoint Configuration Management (MECM) server last night. Which of the following actions should you take to resolve this issue?

A. Disable the DirectX service in services.msc
B. Use SFC to ensure all system files are correct and not corrupted
C. Reboot the system into Safe Mode and allow the user to continue their work
D. Rollback the video card driver and wait for a new driver to be released

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.1: Since the issue first appears after the systems received their latest security patch and updates, the video card driver was likely updated last night. Therefore, you should roll back the driver and verify that this solves the issue. If it does, then you should wait for a new version of the video card driver to be released by the manufacturer or submit a trouble ticket to the manufacturer to let them know there is an issue with their current driver's version. According to the CompTIA Troubleshooting Methodology, you should always question the obvious and ask yourself what has recently changed.

QUESTION 522
You are working at the service desk and j ust received the following email from an end-user who believes it is suspicious

How should you classify this email?

A. Zero-day
B. Spoofing
C. Spear phishing
D. Phishing

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-2.4: This is an example of a phishing campaign. Phishing refers to obtaining user authentication or financial information through a fraudulent request for information. Phishing is specifically associated with emailing users with a link to a faked site (or some other malware that steals the information they use to try to authenticate). Spear phishing is an email or electronic communications scam targeted towards a specific individual, organization, or business. In this example, the specific user wasn't targeted by their name or by their association with a particular store, company, or website. Spoofing is a type of attack that disguises a communication from an unknown source as being from a known, trusted source. Spoofing can occur using different methods, such as MAC spoofing, IP spoofing, calli spoofing, and others. A zero-day vulnerability is when the vendor is aware of a security flaw, but a patch has not been developed or applied on an affected system. At this point, a malicious actor can craft an attack and take advantage of the zero-day vulnerability.

QUESTION 523
Which of the following operating systems are NOT used in modern smartphones or tablets?

A. macOS
B. Android
C. iPadOS
D. Ios

Correct Answer: A
Explanation

Explanation/Reference:

OBJ-1.8: macOS is only supported on Apple desktops, laptops, and servers. Apple released iOS for smartphones and iPadOS for their tablets. Android was developed as a mobile operating system for use in smartphones and tablets.

QUESTION 524
A client contacts the service desk and complains that their smartphone is warm to the touch and their battery only lasts 4 hours a day, not t he 10 hours advertised by your company. You ask them fo,r the status of their location settings, which a re summarized below: * Storage (49 GB Used, 15 GB Free, 64 GB Total) * Mail Client (Corporate account set to push, Personal account set to pull hourly) * Display (Auto brightness, Lock after 30 minutes, Night mode disabled) * Calls (33 minutes used during last 24 hours) * Data (52MB used during last 24 hours) * Location (All apps set to "a llow while using") Based on the information provided, what should be changed to resolve this client's problem?

A. Display settings
B. Storage settings
C. Location settings
D. Mail settings

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.5: The display option is currently set to auto-brightness (this. is acceptable), lock after 30 minutes (this is not recommended), and night mode disabled (this is optional based on the user's preference). The display setting of a lock after 30 minutes will keep the smartphone's display on for 30 betweens after the phone is last used or touched by the user. This will waste a lot of battery power and cause the device to become warm to the touch. The d isplay is one of the largest users of battery power on a smartphone. This setting should be set to 1-3 minut es to help extend the device's battery life.

QUESTION 525
Which low power mode is used witn Windows 10 laptops to save power, but it takes longer to turn back on and resume where the user left off?

A. Hibernate
B. Sleep
C. Power saver
D. Balanced

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-1.4: Hibernate mode is used to save the current session to disk before powering off the computer to save battery life when the system is not being used. The computer takes longer to start up again from hibernate mode than it does from the sleep or standby mode. Sleep or standby mode is used to save the current session to memo ry and put the computer into a minimal power state to save battery life when the system is not being used. The computer takes less time to start up again from the sleep or standby mode than it does from the hibernate mode. The high-performance power plan favors performance over energy savings. The balanced power plan adjusts the performance to conserve energy on capable hardware.

QUESTION 526
You are troubleshooting an issue with a Windows desktop and need to display the machine's active TCP connections. Which of the following commands should you use?

A. ping
B. net use

C. ipconfig
D. netstat

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-1.2: The netstat command is used to display active TCP connect ions, ports on which t he computer is listening, Ethernet statistics, the IP routing table, 1Pv4 stat istics (for the IP, ICMP, TCP, and UDP protocols), and 1Pv6 statistics (for the 1Pv6, ICMPv6, TCP over 1Pv6, and UDP over 1Pv6 protocols) on a Windows machine. This is a useful command when determining if any malware has been installed on the system and maybe maintaining a remote connection wit h a command and control server. The ipconfig tool displays all current TCP/IP network configuration values on a given system. The ping command is used to test a host's reachability on an Internet Protocol network. The net use command is used t o connect to, remove, and configure connections to shared resources such as mapped drives and network printers.

QUESTION 527
Fail To Pass Systems has just been the victim of another embarrassing data breach. Their database administrator needed to work from home this weekend, so he downloaded the corporate database to his work laptop. On his way home, he left the laptop in an Uber, and a few days later, the data was posted on the internet. Which of the following mitigations would have provided the greatest protection against this data breach?

A. Require data at rest encryption on all endpoints
B. Require a VPN to be utilized for all telework employees
C. Require all new employees to sign an NDA
D. Require data masking for any information stored in the database

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-2.6: The greatest protection against this data breach would have been to require data at rest encryption on all endpoints, including this laptop. If the laptop were encrypted, the data would not have been readable by others, even if it was lost or stolen. While requiring a VPN for all telework employees is a good idea, it would not have prevented this data breach since the laptop's loss caused it. Even if a VPN had been used, the same data breach would have still occurred if the employee copied the database to the machine. Remember on exam day that many options are good security practices, but you must select the option that solves the issue or problem in the question being asked. Similarly, data masking and NDAs are useful techniques, but they would not have solved this particular data breach.

QUESTION 528
What is the FOURTH step of the seven-step malware removal process?

A. Enable System Restore and create a restore point in Windows
B. Quarantine the infected system
C. Update the applications and the operating system
D. Remediate the infected systems

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-3.3: The seven steps of the malware removal procedures are (1) Investigate and verify malware symptoms, (2) Quarantine the infected systems, (3) Disable System Restore in Windows, (4) Remediate the infected systems, update anti-malware software, scan the system, and use removal techniques (e.g., safe

mode, pre-installation environment), (5) Schedule scans and run updates, (6) Enable System Restore and create a restore point in Windows, and (7) Educate the end user.

QUESTION 529
An offsite tape backup storage facility is involved with a forensic investigation. The facility has been told they cannot recycle their outdated tapes until the conclusion of the investigation. Which of the following is the MOST likely reason for this?

A. The process of discovery
B. A notice of a legal hold
C. A data transport request
D. A chain of custody breach

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.6: A legal hold is a process that an organization uses to preserve all forms of relevant information when litigat ion is reasonably anticipated. If a legal hold nohce has been given to the backup service, they will not destroy the old backup tapes until the hold is lifted. The process of discovery is the formal process of exchanging information between the parties about the witnesses and evidence they will present at trial. The chain of custody is the chronological documentation or paper trail that records the sequence of custody, control, transfer, analysis, and disposition of materials, including physical or electronic evidence. A data transport request is a formalized request to initiate a data transfer by establishing a circuit or connection between two networks.

QUESTION 530
Which of the following password policies defines the number of previous passwords that cannot be reused when resetting a user's password?

A. Password complexity
B. Password history
C. Password expiration
D. Password length

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.6: Password history is used to determine the number of unique passwords a user must use before using an old password again. This prevents password reuse and also helps protect authentication services from brute force attacks. A password expiration control in the policy would force users to change their passwords at specific time intervals. The passwords must meet the complexity requirements which determines whether passwords must meet a series of guidelines that are considered important for a strong password. Maximum password length creates a limit to how long the password can be, but a longer password is considered stronger against a brute force attack.

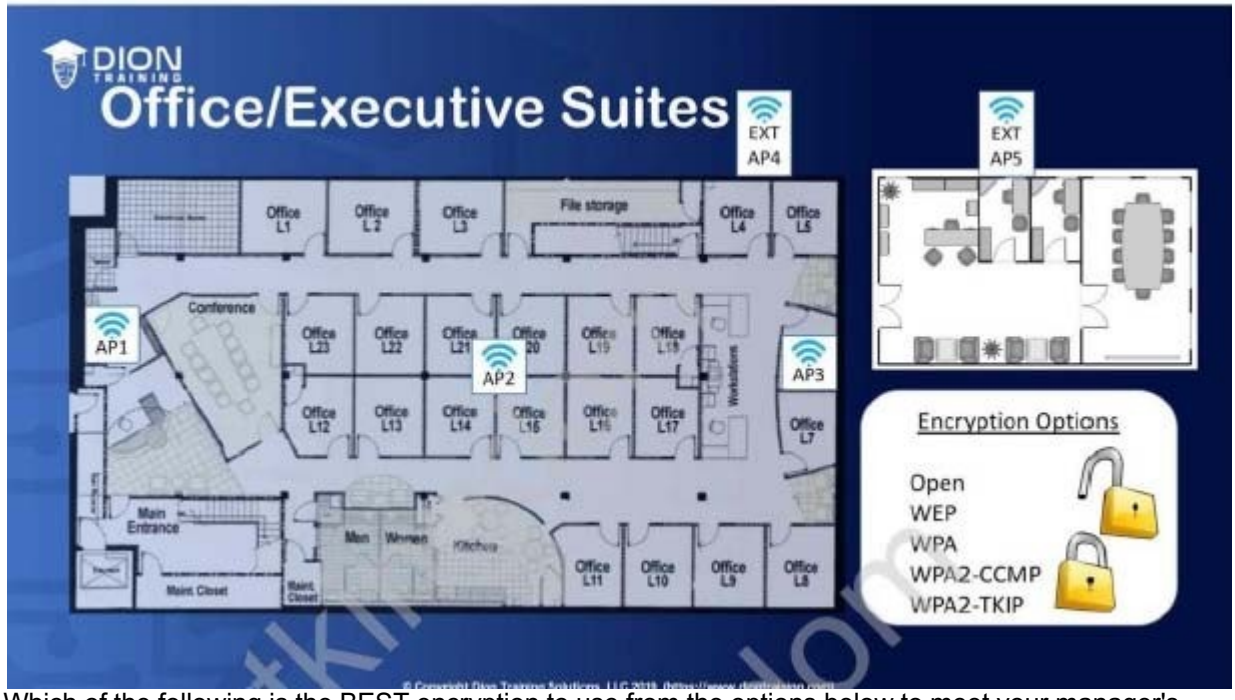
QUESTION 531
What anti-malware solution is installed as a dedicated on-premise appliance to scan all incoming traffic and prevent malware from being installed on any of your clients without requiring the installatiton of any software on your clients?

A. Signature-based anti-malware
B. Host-based anti-malware
C. Network-based anti-malware
D. Cloud-based anti-malware

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.3: The network-based anti-malware can help prevent malware attacks by scanning all incoming data to prevent malware from being installed and infecting a computer. Network-based anti-malware solutions can be installed as a rack-mounted, in- line network appliance in your company's on-premise datacenter to protect every client and server on the network without having to install software on each of the clients. Network-based antimalware solutions often come as part of a unified threat management (UTM) appliance. Cloud antivirus is a programmatic solution that offloads ant ivirus workloads to a cloud-based server, rather than bogging down a user's computer with a complete antivirus suite. Cloud-based solutions do not use on-premise appliances as part of their installation. Host-based anti-malware relies upon the installation of an agent to detect threats such as viruses, spam, and rootkits to protect the client it is installed upon. Host-based malware often uses signatures to detect and remove malicious code. Signature-based anti-malware is a generic category of malware that may be implemented through host-based, network-based, or cloud-based anti-malware solutions. Anti-malware either operates using signature-based detection, behavioral- based detect ion, or heuristic-based detection.

QUESTION 532
(This is a simulated Performance-Based Question. If this was the real certification exam, you would be asked to drag-and-drop the correct encryption onto the APs.)
Your company has purchased a new office building down the street for its executive suite·s. You have been asked to choose the BEST encryption for AP1, AP2, and AP3 to establish a wireless connection inside the main building for visitors to use. Your boss has stated that the main building's internal wireless network is only going to be used by visitors and should not require the visitors to set up any special configuration on their devices to connect.



Which of the following is the BEST encryption to use from the options below to meet your manager's requirrements for the new visitors' Wireless Network?

A. WEP
B. Open
C. WPA-CCMP
D. WPA2-I"KIP
E. WPA

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-2.9: Since your manager has required that the visitors not be required to configure anything on their devices to connect, the only option you can choose is Open. This option presents no security for the visitor's wireless network, but it also requires no setup on the user's devices. All of the other options would require a pre-shared key and set up to allow the visitor to use the network. This wireless network should act as a guest network, be segmented from your corporate network, and only allow the visitors to access the internet directly using this network.

QUESTION 533
A small business rrecently experienced a catastrophic data loss due to flooding from a recent hurricane. The customer had no backups, and flooding destroyed all of the hardware associated with the small business. As part of the rebuilding process, the small business contracts with your company to help create a disaster recovery plan to ensure this never reoccurs again. Which of the following recommendations should you include as part of the disaster recovery plan?

A. Local backups should be verified weekly to ensure no data loss occurs
B. Backups should be conducted to a cloud-based storage solution
C. Purchase waterproof devices to prevent data loss
D. Local backups should be conducted

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-4.2: While losing the hardware is a problem for the business, t heir insurance will replace the hardware if flooding destroyed it. The data involved is more of a concern. Therefore, backups should be the primary concern. Local backups are risky since a flood might also destroy them; therefore, using a cloud -based storage solution would be ideal and prevent future data loss.

QUESTION 534
A client contacts the service desk and complains that their smartphone is warm to the touch and their battery only lasts 4 hours a day, not t he 10 hours advertised by your company. You ask them for the status of several settings: Email (neve r), Maps (always), Calender (while using), Messages (while using), Photos (never), App Store (while using), Bank (while using), and Weather (while using). Based on the information provided, what should be changed to resolve this client's problem?

A. Change the App Store to never
B. Change the Maps setting to while using
C. Change the Email setting to while using
D. Change the Weather setting to always

Correct Answer: B
Explanation

Explanation/Reference:
OBJ-3.5: The location setting is found under privacy settings on most smartphones. If the location setting is set to always, then the app will continue to check the background's GPS location. This will occur even if the smartphone is in standby mode. When a smartphone is checking its location, it uses both the GPS received and the cellular modem to triangular its position. This can waste a lot of battery life. Instead, it is better to set the apps to only use the location feature while using the app or to never, in the case of an app that shouldn't need to r·ely on a user's location.

QUESTION 535

Jason's iPhone has not received any emails or SMS messages in the few 4 hours. Which of the following is the most cause of these issues?

A. Internet connectivity failure
B. OS update failure
C. Mail client error
D. Bluetooth connectivity failure

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.5: Based on the symptoms, the most likely cause is an internet connectivity failure . . Apple iPhones use internet connectivity and data to send their text messages by default. If the smartphone's internet connection is offline, then the phone will not receive emails or SMS messages from other iPhone users. If an Android user sends a text message to an iPhone, it willl be delivered over the cellular network without using an internet connection. Based on the symptoms, this is not a mail client error since it also affects SMS messages. This is not a Bluetooth connectivity issue since emails and SMS messages are not delivered using Bluetooth. There is no indication that it was an OS update issue since the scenario does not mention that a recent update was attempted by the user.

QUESTION 536
Every new employee at Dion Training must sign a document to show they understand the proper rules for using the company's computers. This document states that the new employee has read the policy that dictates what can and cannot be done from the corporate workstations. Which of the following documents BEST describes this policy?

A. AUP
B. MOU
C. SLA
D. SOW

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-4.1 : An acceptable use policy (AUP) is a document stipulating constraints and practices that a user must agree to for access to a corporate network or the internet. For example, an AUP may state that they must not attempt to break any computer network security, hack other users, or visit pornographic websites from their work computer. A service level agreement (SLA) is a contract that outlines the detailed terms under which a service is provided, including reasons the contract may be terminated. A statement of work (SOW), or a scope of work, is a document that outlines all the work that is to be performed, as well as the agreed-upon deliverables and timelines. A memorandum of understanding (MOU) is a preliminary or exploratory agreement to express an intent to work together that is not legally binding and does not involve monetary exchange.

QUESTION 537
Which partition of the hard drive is concealed from the user in the File Explorer within Windows 10 and is only used when imaging the computer back to its factory default state?

A. Primary
B. Swap
C. Recovery
D. Extended

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-1.9: The recovery partition is a disk partition that is accessible via the startup sequence that contains an image of the system partition as produced by the PC vendor. This can be used to recover the PC to its factory state by performing a repair install but will erase any user data or installed programs. The· swap partition on a Linux system is a portion of the hard disk formatted with a minimal kind of file system and used in situations when the operating system runs out of physical memory and needs more of it. It can only be used by the memory manager and not for the storage of ordinary data files. Primary partitions are limited to only four primary partitions on a system using MBR. To overcome this limitat ion, extended partitions can be used. An extended partition is a partition that can be divided into additional logical drives. Unlike a primary partition, you don't need to assign it a drive letter and install a file system.

QUESTION 538
What is the name of a program that monitors user activity and sends that information to someone else?

A. Rootkit
B. Keylogger
C. Spyware
D. Virus

Correct Answer: C
Explanation

Explanation/Reference:
OBJ-2.3: Spyware is a program that monitors user activity and sends the information to someone else. It may be installed with or without the user's knowledge. It invades the device, steals sensitive information and internet usage data, and relays it to advertisers, data fi rms, or external users. A vi rus is malicious software designed to infect computer files or disks when it is activated. A virus may be programmed t o carry out other malicious actions, such as deleting files or changing system settings. A rootkit is a clandest ine computer program designed to provide continued privileged access to a computer while actively hiding its presence. A rootkit is generally a collection of tools that enabled administrator- level ac,cess to a computer or network. They can often disguise themselves from detection by the operating system and anti-malware solutions. If a rootkit is suspected on a machine, it is best to reformat and reimage the system. A keylogger actively attempts to steal confidential information by capturing the data when entered into the computer by the user. This is done by recording keystrokes entered into a web browser or other application. A software keylogger can be run in the background on a vict im's computer. A hardware keylogger may be placed between the USB port and the wired keyboard.

QUESTION 539
A user's SOHO wireless network appears to have significantly slowed down today. Normally, they can download files at 900 Mbps or more, but today, they only averaged 23 Mbps when downloading. You check their wireless settings and see the following: Network SSID: DionTraining Security: WPA2 Password: diontraining Mode: AC ISP: Fiber1 Gbps Which of the following is MOST likely the problem?

A. Other users have connected to the WiFi due to a weak password
B. WPA2 reduces download speeds and the user should switch to WPA3
C. Additional transmission power is needed for the wireless signal
D. The WAN type needs to be upgraded to DSL or cable

Correct Answer: A
Explanation

Explanation/Reference:
OBJ-3.5: Other users have likely connected to this wireless network since the SSID being broadcast and the password are both similar. The additional usage by those users could drastically slow down this user's overall connection speed. For example, some attackers will look for open WiFi or wireless networks with weak passwords. When they find them, they will connect servers with illicit files on them for others to download. This

would reduce the connection speed for legitimate users. The WAN type is displayed as a Fiber connection at 1 Gbps, therefore it does not need to be upgraded or changed. WPA2 and WPA3 are forms of encryption and do not affect the overall speed of the network drastically. There is no indication in the scenario that there is a weak signal or a low signal-to-noise ratio that would require additional transmission power to be added.

QUESTION 540
Which of the following file types are commonly used to create simple scripts in the Windows commandline environment?

A. .py
B. .sh
C. .js
D. .bat

Correct Answer: D
Explanation

Explanation/Reference:
OBJ-4.8: Batch scripts run on the Windows operating system and, in their simplest form, contain a list of several commands that are executed in a sequence. A .bat file is used for a batch script. You can run the file by calling its name from the command line or double-clicking the file in File Explorer. Generally, batch file scripts run from end to end and are limited in branching and user input. A shell script is a file that contains a list of commands to be read and executed by the shell in Linux and macOS. A .sh file is used for a shell script and its first line always begins with #!/bin/bash that designates the interpreter. This line instructs the operating system to execute the script. Shell scripts allow you to perform various functions. These functions include automation of commands and tasks of system administration and t roubleshooting, creating simple applications, and manipulating text or files. Python is a general-purpose programming language that can develop many different kinds of applications. It is designed to be easy to read, and the programs use fewer lines of code compared to other programming languages. The code runs in an interpreter. Python is preinstalled on many Linux distributions and can be installed on Windows. Python scripts are saved using the .py ext ension. JavaScript is a scripting language that is designed to create interactive web-based content and web apps. The scripts are executed automatically by placing the script in the HTML code for a web page so that when the HTML code for the page loads, the script is run. JavaScript is stored in a .js file or as part of an HTML file.