220-1102 Security Study Guide

General Information - test devotes **25% (one-fourth) of its questions** to security concept assessment. More than half (**60%**) of the questions about security will begin with a **scenario**.

Security Measures - are practical concepts, both physical and logical, which are designed to maintain the integrity and security of a network, device, or program among others.

Physical Security - is important because no matter how many security measures you put in place on a device itself, physical security is the only thing that will stop a criminal from walking away with the entire device.

Access Control Vestibule - commonly known as a **mantrap**, is exactly what it sounds like. It's a trap used to prevent infiltration methods such as **tailgating** and **piggybacking**. The access control vestibule is a small area with a set of two locked doors, and it separates the outside world from a secured area. When entering, an individual will enter through the first door, but that door must then be closed behind them before the second door may be opened.

Badge Reader - Identification badges can be used as proof of access authorization. Badge readers can be implemented to help prevent unauthorized access. In this type of environment, employees are given badges, such as **proximity cards** or **smart cards**. When the employee scans the badge, he or she is allowed entry to the area.

Video Surveillance - is one of the most important aspects of physical security as it allows for the investigator to physically see what has occurred in the physical area. The two primary types of camera employed for video surveillance are the fixed and pan-tilt-zoom (PTZ) variety. A **fixed camera** is limited to the scope of the stationary camera and may create blind spots. The **PTZ camera**, however, has the capability of covering 360 degrees as well as zooming capabilities. The drawback of the PTZ camera, though, is that one camera is commonly employed to cover a large area, reducing the likelihood of the camera being pointed at the direction of the occurrence at the time.

Alarm Systems - can be installed to alert for potential unauthorized access. Alarm systems can be used to notify if an access control system has logged unauthorized access or for break-in response and detection. **Common sensors** found in an alarm system include video surveillance, motion detection devices, and magnetic contact sensors.

Motion Sensors - is a device that is programmed to detect motion in a space. The sensitivity of these sensors can be adjusted to fit the needs of the enterprise to avoid false alarms.

Door Locks - should be utilized whenever possible. Aside from locks preventing unauthorized entrance to the building, locks should also be utilized to protect rooms containing sensitive equipment (such as the server room or network closet).

Equipment Locks - are locks designed to secure a specific type or piece of equipment. For example, a cable lock can be used to help prevent a thief from walking off with laptops. A **cable lock** is used by looping the cable around a heavy (ideally immovable) object and then securing the lock to a small security hole on the side of the laptop. **Server locks** are used to secure servers, but are becoming obsolete since a rack-mounted enclosure provides more security for servers. **USB locks** are plastic pieces that can be inserted into a USB port to close the port. A specialty tool is needed to remove the lock.

Guards - Security guards are one of the few security controls that are considered not only **preventative** controls, but also **deterrent** and **detective** controls. This is because organizations with onsite security staff are less likely to be targeted for attacks than those with no security guards. Security guards have the ability to physically limit access to the premises or specific places within the premises to those without proper identification and authorization. They can also investigate if something seems amiss.

Bollards - is a physical security measure that is placed around the perimeter of an area and is used to prevent catastrophic entrance or access to the area. Bollards are very sturdy, usually made of concrete or steel, and are designed to keep vehicles such as cars or trucks from driving into a secured area.

Fences - are physical barriers designed to keep unauthorized persons out of an area or space. Fences are commonly the **first line of physical defense** against unauthorized access and work best when paired with other physical security measures, such as badge readers and security guards.

Physical Security for Staff - include methods of access control for sensitive areas or equipment that provide authentication for the user.

Key Fobs - are small security devices that store authentication information. They can easily be attached to a keyring or lanyard to provide both security and instant availability.

Smart Cards - are typically the size of your driver's license or credit card. The embedded memory and chipset in these cards can store identification and authentication information.

Keys - used to open a specific lock or set of locks. Keys are easily duplicated or stolen, and their usage is hard to control.

Biometrics - locks can add an additional layer of protection to an organization's physical security. Smart cards and proximity badges can be lost and possibly wind up in the wrong hands. Biometric locks **use an individual's features**, such as their retina or fingerprints, to authenticate them.
***Retina Scanner* -** compares the retinal scan of a person's eye against the markers on file to verify identity. Retinal scanners are considered to be **more intrusive** than other types of biometric authentication and the accuracy of the scan **can be limited** by diseases of the eye, such as cataracts, glaucoma, or severe astigmatism.
***Fingerprint Scanner* -** matches fingerprints to verified users. Fingerprint scanners are a common method of biometric authentication but **may cause bottlenecking** at high traffic locations or **lack accuracy** in high dirt environments.
***Palmprint Scanner* -** compares the scanned palmprint against the verified users and looks for such markers as lines, scars, and fingerprints. Palmprint scans tend to be **more accurate** than fingerprint scans due to the large surface area of the scan location allowing for more points of comparison.
Lighting - can impact the picture quality of video surveillance. To ensure high-quality video, the area should be properly lighted. Most video surveillance used today, however, includes **infrared (IR) capabilities** that allow for surveillance in low light or dark areas.
Magnetometers - known as a **metal detector**, can be used to detect metal objects. The metal detector can also be used as a security choke point. Metal detectors can also be used upon exiting if the enterprise is concerned about insider threats, but this is controversial as it can be considered to be infringing upon employee rights to privacy.
Logical Security - are concepts like security policies and software safeguards that are used to protect systems. You should be able to explain these.
Principle of Least Privilege - Permissions should only be given to a user if they absolutely need them to complete their job. This idea is known as the principle of least privilege. The fewer users who have access to sensitive files, the less likelihood that something bad will happen to those files.
Access-Control Lists (ACLs) - are used to specify **which traffic should be allowed** through a firewall and which traffic should be blocked. Using an ACL, traffic can be blocked or allowed based upon a number of items including source or destination port as well as source or destination IP address.
Multi-Factor Authentication (MFA) - Even the strongest passwords can be compromised. This is where MFA comes in. MFA requires two or more *different* authentication types. Authentication types are typically broken down into categories, such as **something you know** (password, PIN, security question), **something you have** (authenticator, token), and **something you are** (biometrics). Because MFA requires two or more *different types* of authentication, a user would not be able to use just a personal identification number (PIN) and a password, since they both fall into the category of something you know. Rather, the user would need a combination of the authentication types, such as a password and a token.
Email - can be used as a method of MFA, but it is the **least secure method** of MFA. Email can be helpful as a notification tool for unauthorized access by notifying the individual if suspicious activity has been detected.
Hard Token - or hardware token, is a physical device that the user must have on them to gain access to a network's resources. The drawback of a hard token is the **chance of losing** the token, which could then be used by an unauthorized user to authenticate to a system.
Soft Token - or software token is similar to a hardware token, except they come in the form of either a piece of software on your laptop or an app on your mobile device. A software token is more commonly used for MFA with applications such as Google Authenticator, where it acts as a hard token but is software based.
Short Message Service (SMS) - A can be used as a method of MFA by sending a **time sensitive code**, typically a five- to eight-digit code to the authorized users connected SMS number.
Voice Call - like an SMS, can be used to verify the user by placing an automated call to the contact number on file for the user. A verification code is thereby provided to the user for authentication purposes.
Authenticator Application - are technically soft tokens that act like hard tokens. An application is loaded onto a device and used for authentication, such as Google Authenticator.
Mobile Device Management (MDM) - policies are used to enforce security measures on mobile devices, such as cell phones and tablets. Many organizations require that their users access email or other business-related apps on their phone, but this can present security risks to the organization. MDM policies can help offset some of the risk. An example of an MDM policy would be an organization requiring anyone accessing business email or business apps to have a lock screen on their phone with a PIN.

Active Directory (AD) - is the Microsoft directory used to manage users, applications, computers, and much more. AD can be used to help implement security measures across an organization. AD is not an authentication protocol but acts as **storage for the authentication data** and works closely with **Kerberos**, which is the actual authentication protocol.
Login Script - can be thought of as a series of instructions given for a device to perform upon login. Login scripts can be set on the profile tab of a user in AD. Login scripts can be used to map network drives, log computer access, gather information from a computer, and much more.
Domain - Ensuring that all computers in an environment are in your domain helps ensure they will be given the proper security policies. When a computer is in your domain, you'll be able to see it and manage it within AD.
Group Policy/Updates - can be extremely **useful in securing an organization**. Group policies can be used to set password policies, block unwanted applications, and even block access to the internet entirely in some cases. They can also be used to push out security updates, which are important to keep an organization safe.
Organizational Units (OU) - are subdivisions of your domain within Active Directory. For example, if an organization has three separate locations, they may choose to have three organizational units within their domain.
Home Folder - can be set for each user in AD. If the home folder doesn't exist when it's added in AD, then AD will create the folder and set the permissions for you. By default, this folder can be accessed only by the user and the domain administrators. Home folders should be used by personnel to store their files on the server. Because computers can be lost or stolen, it's best for users to store their documents on the server in this way rather than store them locally on their own machines.
Folder Redirection - allows administrators (and, in some cases, users) to redirect the path of a specific folder to a new location. One popular implementation of this is to redirect a user's Documents folder (that is stored locally on their machine) to a network location, such as the home folder.
Security Groups - can be created to make assigning privileges and permissions to groups of users more efficient. Security groups are also helpful when auditing permissions. The security groups can be examined rather than the individual user.
Wireless Security Protocols and Authentication Methods - Wireless networks are inherently less secure than wired networks. However, there are several methods that can be used to secure wireless networks. You must be able to compare and contrast these protocols and authentication methods.
Protocols and Encryption - You should be able to differentiate between different protocols and encryption methods used with wireless networks.
Wi-Fi Protected Access 2 (WPA2) - improved upon WPA by using the Advanced Encryption Standard (AES). WPA2 is exploitable if the WPS service is enabled on the device.
WPA3 - is the successor to WPA2. It introduced 192-bit cryptographic strength in Enterprise mode and requires CCMP 128 as a minimum in personal mode. WPA3-Personal also uses Simultaneous Authentication of Equals (SAE) instead of the preshared key (PSK) exchange used in previous versions of WPA.
Temporal Key Integrity Protocol (TKIP) - provides a new encryption key for every sent packet. TKIP uses the RC4 encryption algorithm protocol for its cipher. An RC4 encryption algorithm encrypts plain text by bytes to produce a cipher stream. The key for the RC4 algorithm is based on the MAC address and initialization vector of the sending device and is used to check message integrity.
Advanced Encryption Standard (AES) - is a secure encryption method that is still used today. WPA2 uses AES in order to secure wireless networks.
Authentication - Wireless networks should never be left open, and they should always require some form of authentication. Let's look at a few wireless authentication methods.
Remote Authentication Dial-In User Service (RADIUS) - is an authentication method used to allow for centralized authentication and accounting. Although it gets its name from the days of dial-up internet, RADIUS is now the common method used to authenticate over virtual private networks (VPNs) and wireless networks.
Terminal Access Controller Access-Control System (TACACS) - (now TACACS+) was originally developed by Cisco, but was released as an open standard. These protocols are used for the authentication of users on network devices, such as routers and switches.
Kerberos - is an open standard for authentication that is used in conjunction with AD for authentication. Kerberos can also be used with the 802.1X protocol for direct authentication.
Multi-Factor - authentication requires a user to provide more than one authentication type, as discussed earlier in this study guide. A common implementation of multi-factor relating to wireless authentication is the Extensible Authentication Protocol-Transport Layer Security (EAP-TLS), which requires the user to not only have a password but also a certificate installed on the computer.

Detecting, Removing, and Preventing Malware - To succeed on questions about malware, you should be able to evaluate a given scenario, find malware, and remove it with effective tools and procedures. You should also know how to prevent malware in the future. Questions of this type will be scenario based.

Malware - is used to describe **any malicious software** that includes (but is not limited to) trojans, spyware, viruses, and worms. Let's take a deeper look at some of the different types of malware that exist today.

Trojan are malicious programs that **disguise themselves as valuable programs**. Imagine a scenario where a user downloads a program that they believe will allow them to listen to music or watch a movie for free. They downloaded the program because they believed it to be a valuable and legitimate program; however, when they run the program, they have actually installed malware on their device. This is an example of a trojan.

Rootkit - are malicious programs with the **goal of gaining privileged access** to a computer. Rootkits hide themselves by taking advantage of operating system (OS) functions, and they can attack operating systems, hypervisors, and firmware.

Virus - is defined as any malicious program that **replicates itself** and attempts to infect other computers. Viruses, unlike worms, **need human interaction** to spread. They are only able to replicate to other drives on the same computer and not across the network. Viruses are designed for many different goals, from corrupting data to stealing information.

Spyware - is a type of malware that **covertly collects data** on a user after it is installed on their computer. Spyware is typically a virus that **requires user interaction** to infect. For example, a user would have to click on a link in an email for the spyware to download. Spyware can be used for malicious purposes, such as stealing confidential data or credentials, or as a data collection device for advertising purposes.

Ransomware - is so named because it essentially **holds your files and data ransom** until you pay the attacker. As the popularity of cryptocurrency (e.g., Bitcoin) has grown, so has ransomware. Attackers can request Bitcoin as their method of payment to release the data after a ransomware attack, making the attackers more difficult to track down after the transaction.

Keylogger - come in both hardware and software forms. A keylogger will **track all the keystrokes** made on the computer running the keylogger. This information can then be transmitted over to the attack entity for them to parse for useful stolen information.

Boot Sector Virus - infects the master boot record (MBR) of a hard disk and is designed to load when a device is booted up, reinfecting the OS each time it is booted up. **Secure boot** can be used to identify a boot sector virus.

Cryptominers - are users who **perform cryptographic computations to create cryptocoins**. A cryptominer can infect others computers and use the other computer's processing power to perform the computations for the cryptominer.

Tools and Methods - that can be used to detect and prevent malware.. Multiple layers of **prevention, detection, and eradication** should be used to fully protect a system.

Recovery Mode - Microsoft Windows offers a suite of built-in recovery tools known as the **Windows Recovery Environment (WinRE)**. This console can be especially helpful if a computer has been infected by malware. Some of the tools in the recovery console will allow you to reset the operating system back to default or simply restore the computer to an earlier time, such as before the computer became infected.

Antivirus - Many threats described above can be mitigated simply by having an antivirus program installed. Antivirus software is made up of two main components, the antivirus engine and the antivirus database. The **antivirus engine** is responsible for real-time scanning. The **antivirus definitions database** is a repository of signatures that is used to detect known malware.

Anti-Malware - software is extremely similar to antivirus software, but it takes the detection a step farther. Anti-malware software can usually **check files outside of the Windows file systems**, such as those on malicious websites and those coming in via email.

Software Firewalls - When referring to software firewalls in this section, we are referring to firewalls that come as part of the operating system. Windows computers come with a built-in software firewall called **Windows Defender Firewall**. This firewall can help prevent worms and malicious inbound connections.

Anti-Phishing Training - is training of end users targeted specifically at understanding phishing techniques and tactics. This training may involve sending spoof phishing emails to end users to identify potential weak spots in users and training.

User Education - While there are plenty of wonderful tools out there to help protect against attacks, end user education is **one of the most important**. This is because antivirus software and spam filters are not perfect. It is important for users to understand what types of items they should download and not download, what types of websites they should *not* visit, and how to identify a phishing scam.

OS Reinstallation - For a highly corrupted OS, the OS may need to be reinstalled with a clean installation. This will remove all data previously attached to the old installation of the OS, including viruses and malware it may have been infected with.
Social Engineering Attacks, Threats, and Vulnerabilities - For this test you should be able to compare and contrast different types of threats, social engineering, and vulnerabilities.
Social Engineering - is the act of **manipulating individuals** into giving you unauthorized access to a building or room, or giving you private information.
Phishing - is the most common type of social engineering. In a phishing attack, the attacker sends a **fraudulent email** pretending to be from a legitimate source, such as a colleague, vendor, or even a user's bank. The goal of a phishing attempt is to get the unsuspecting user to give up their private information.
Vishing - is **phishing through Voice over Internet Protocol (VoIP) calls**. Vishing calls may attempt to elicit information from the recipient using social engineering techniques. For example, a caller may state that they are from the IRS and the recipient needs to provide back tax payment or risk further financial or legal penalties.
Shoulder Surfing - is the act of stealing a person's data by looking over their shoulder as they type private information on a computer or a code into a door or ATM.
Whaling - is phishing that specifically targets individuals high up in a company's hierarchy, such as CEOs and CFOs or other **high-value targets**.
Tailgating - or **follow another person** into a building. This means sneaking into a locked door right behind a person who has permission to enter. Sometimes, the social engineer may carry boxes so that an individual, who is just trying to be polite, will unlock and hold the door open for them.
Impersonation - pretend to be someone else to gain access to what they are looking for. One example of this would be an attacker pretending to be from your internet provider asking for access to your network closet.
Dumpster Diving - an attacker digs through the trash hoping to find private information that wasn't shredded.
Evil Twin - is an **imposter access point** that impersonates a legitimate access point in order to intercept data. For example, a user could connect to an access point at their local cafe that provides free Wi-Fi access under the name "Cafe Guest." The evil twin will create an imposter access point also named "Cafe Guest" and intercept data when the user connects to the evil twin.
Threats - are potential hazards to a network that can be either **physically or logically based**. A threat is an attack designed to interrupt, intercept, or damage data from a target. Threats can come from a single threat actor, such as a **script kiddie**, or numerous threat actors acting in coordination with one another, such as a **nation state**.
Denial of Service (DoS) - attack is one in which a **large amount of meaningless traffic** is directed toward a device or network in an attempt to overburden and bring it down.
Distributed Denial of Service (DDoS) - is a denial-of-service attack in which multiple computers (often a **botnet**) are used to send an abundance of traffic in an attempt to bring down a network's resources.
Zero-Day Attack - is one that **targets a vulnerability** that developers have not identified yet or for which they have not had time to release a patch or fix.
Spoofing - is a form of an **impersonation attack**. Some commonly spoofed items include a source IP address, source MAC address, source email address, and usernames.
On-Path Attack - previously known as a **man-in-the-middle (MITM)** attack, is an **eavesdropping** attack. The attacker will try to plant themself between two systems and intercept the traffic.
Brute-Force Attack - the attacker attempts to guess as many of the possible values as they can. Brute force is generally used as a method of **password cracking** but can be used in some other scenarios as well.
Dictionary Attack - One form of brute-force attack is known as a dictionary attack. Rather than the attacker trying to come up with passwords to guess themselves, they can use a **list of all leaked passwords** online (known as a dictionary).
Insider Threat - is a **threat from within the organization itself** and may be perpetrated by disgruntled employees or for personal gain. Insider threats are **more common than external threats** and can expose the organization to significant levels of damage as the threat has access to the network. An internal threat may be **more difficult to detect** since the threat is expected to be on the network.
Structured Query Language (SQL) Injection - is an attack in which the threat enters a series of malicious code with a SQL query to gain access to SQL databases.
Cross-Site Scripting (XSS) - is used to **embed malicious scripts** into a legitimate web page and is commonly used to hijack web pages to coax the end user to install malware.

Vulnerabilities - in cyber security are weaknesses in the OS or network that can be exploited for access. Threat actors leverage vulnerabilities to gain access to a network. While zero-day threats do occur, the majority of vulnerabilities have been previously identified with released patches. It is easier for a threat actor to try known vulnerabilities against a target to gain access to the network than to attempt to discover a new vulnerability.
Non-Compliant Systems - is a system or device that does not follow the standard security precautions as dictated by the system administrator. Non-compliant software or systems can pose a threat to an organization's network. It's important to fix non-compliant devices as soon as you notice them.
Unpatched Systems - Patches protect systems, software, or networks from known vulnerabilities. Unpatched systems leave the network or device open to exploitation through these known vulnerabilities.
Unprotected Systems - is a system that does not have the appropriate security measures in place, such as a device without an antivirus or anti-malware program installed or a system without a properly configured firewall.
End-of-Life (EOL) Operating Systems (OSs) - is an OS that is no longer supported by the vendor. This means that no new patches or updates will be released for vulnerabilities, leaving the OS open to exploitation.
Bring Your Own Device (BYOD) - policies allow users to use their own devices on a network and are therefore difficult to police and pose both a data leakage and data portability vulnerability. These devices may not be properly secured, both physically and logically, making them targets for threat actors.
Basic Security Settings in Microsoft Windows® OS - provides useful settings that can be used to enhance security. It is important that you know their names and how they are used. Questions on this subject will be scenario based.
Defender Antivirus - is the Windows OS's pre-installed antivirus software included in all recent versions of the OS.
Activate/Deactivate - Windows Defender can be activated and deactivated via the Virus and Threat Protection settings by clicking on Manage Settings. Specific aspects of the Defender can also be activated and deactivated as needed, such as real-time protection and cloud-delivered protection.
Updated Definitions - To maintain the most current malware definitions and signatures, Defender needs to be updated regularly. Windows Defender as well as its definitions are updated through the Windows Update process.
Firewall - Windows Defender Firewall is a host-based firewall designed to block access from the network. Defender Firewall can be specified to protect the domain network, private network, and public network separately.
Activate/Deactivate - Windows Defender Firewall can be activated or deactivated easily through Firewall and Network Protection. Windows Firewall blocks incoming connections by default.
Port Security - Windows Defender Firewall allows for the creation of specific rules for specific ports as needed, providing advanced port security.
Application Security - By default, the Windows Defender Firewall creates a pop-up when applications attempt to listen in on a port for incoming connections. If allowed, Firewall will create a new rule for the application, allowing it through. Allowed applications can be managed through Firewall and Network Protection.
Users and Groups - users will not all require the same level. **Windows permissions** is a critical part of access control.
Local vs. Microsoft Account - Using a Microsoft account on a device allows for **synchronization** between the device and all data stored in the Microsoft Cloud. A local account does not provide this synchronization and requires manual setup for synchronization.
Standard Account - Most users will fall into the standard account category. A standard account will have varying permissions based upon roles and groups set by the administrator.
Administrator - accounts have **complete power** over the OS. Administrator accounts should be reserved for those who absolutely require them. The more administrators that exist on a network, the more room for error. An administrator will have **access to everything**.
Guest User - on Windows is an account that exists on every Windows machine. It's a **very low-privilege account** that can be used for individuals who only need occasional access to the device.
Power User - account is **one step down from an administrator account**. It is the second most powerful account type within the Windows OS. Can be given read and write permissions but will not be able to change OS system files.
Login OS Options - The Window OS provides multiple methods of login options requiring various levels of authentication.
Username and Password - common method of authentication is this combination to identify the user and the permissions associated with the user.
Personal Identification Number (PIN) - is a password designed for simplifying the login process while still retaining security. A PIN is also often used in two-factor authentication (2FA) and multi-factor authentication (MFA).

Fingerprint - A fingerprint scanner is a biometric method of authentication that can be used as a stand-alone authentication method or in 2FA/MFA.
Facial Recognition - uses facial-scanning technology to identify a user and can be used as a standalone authentication method or in 2FA/MFA.
Single Sign-On (SSO) - is an authentication technique that uses a **single authentication method** to provide access to all applications and systems that the user may need, reducing the need for the user to remember multiple login and password credentials for various applications.
New Technology File System (NTFS) vs. Share Permissions - should be used whenever possible as it will provide the most control over data resources. The advantage of using NTFS permissions over share permissions is that they are applied to both local users and network users and they are based on the permissions granted to an individual user at the Windows logon. **Share permissions** are not applied to users who log in locally to the machine.
File and Folder Attributes - It's possible to encrypt individual files and folders on a computer using the **Encrypted File System (EFS)** that is built into professional versions of Windows. This can be done from the **Advanced Attributes** dialog box for the files and folders.
Inheritance - Rather than needing to specify permissions on each and every file and folder, administrators can configure inheritance. Inheritance allows files and folders within another folder to inherit the permissions of the top-level folder.
Run as Administrator vs. Standard User - Running the system as **administrator** allows for complete access and control while a **standard user** has more limited access and permissions. The administrator mode should only be used if absolutely necessary since running as administrator provides complete access to the system. The standard user should be used for daily activities.
User Account Control (UAC) - When a user wants to run a program that requires an administrator to run, they'll receive a UAC pop-up. This **pop-up** will request an administrator password before the program will run. UAC can be beneficial as it forces an administrator to approve a program before it is run or installed. This can come in handy when users who are not particularly tech savvy try to download or run programs that might end up being malicious.
Encrypting File System (EFS) - is a feature that is available in professional versions of Windows. EFS makes it possible to encrypt individual files and folders with just the click of a button. EFS can be configured in the Advanced Attributes dialog box of a file or folder.
BitLocker - is a program that offers **full drive encryption**. Unlike EFS, which encrypts individual files, BitLocker encrypts the entire drive. BitLocker relies on the computer having a **Trusted Platform Module (TPM)** chip to function.
BitLocker To Go - is an encryption method like BitLocker that allows you to encrypt removable/portable drives, such as external hard drives and USB drives. Unlike the full version BitLocker , BitLocker To Go does not require a TPM chip.
Workstation Security - During the test, you will need to be able to take a given scenario about a workstation and develop appropriate security measures on a "best practice" level to optimally secure that workstation. Here is some relevant information.
Data-At-Rest Encryption - For comprehensive security, it is recommended to **encrypt data at all times**, even when data is at rest. This protects data within the network in case of breach.
Password Best Practices - Passwords are one of the first lines of defense against an attacker. It's important to set strong and memorable passwords.
Complexity Requirements - that deter users from creating short, simple, and easily cracked passwords.
***Length* -** Setting longer password-length requirements increases the security of the passwords. Most security experts feel that a **12 character minimum** should be set, although many organizations use an eight-character length requirement.
***Character Types* -** Requiring multiple character types in a password increases its security. These character types may include **digits, upper and lowercase letters, or special characters**, such as % or @.
Expiration Requirements - Users should be required to change their password at **regular intervals**. This is enforced using a password-expiration policy. Common intervals are every 30, 60, or 90 days.
Basic Input/Output System (BIOS)/Unified Extensible Firmware Interface (UEFI) Passwords - can be set to prevent individuals from gaining unauthorized access to the BIOS configuration.
End-User Best Practices - Educating the end-user about cybersecurity best practices is critical to network security. It is important that *all* users receive this education.
Use Screensaver Locks - For individuals who use screensavers, it's a good idea to set a screensaver password. This will require a password to reenter the computer after the screensaver has come up. The screensaver then works similarly to locking the computer.

Log Off When Not in Use - Cybersecurity best practices include training end-users to log off of network-connected devices when not in use.
Secure/Protect Critical Hardware - Critical hardware (e.g., laptops) should be equipped with multiple security measures, such as logon time restrictions, time-out policies, and failed-login lockouts.
Secure Personally Identifiable Information (PII) and Passwords - can be easily extracted through end-user negligence, such as writing a password on a sticky note or leaving printouts with PII on printers in an easily accessible area. Users should be instructed *not* to do these things.
Account Management - Administrators are in charge of ensuring the security of workstations using various policies. They define these policies and monitor and enforce them. The following are important considerations regarding account management.
Restrict User Permissions - Organizations should always use the **principle of least privilege**. This means that users should only be given access to the resources that they need in order to complete their jobs and nothing more. Having strong permissions helps to prevent unauthorized access whether intentional or accidental.
Restrict Login Times - If your organization only has users working between certain hours of the day (for example, between 9 a.m. and 5 p.m.), one good security restriction to put in place is logon time restrictions. It's possible to put policies in place that restrict users from logging into a computer outside their **normal working hours**.
Disable Guest Account - immediately disable it. Even though it is a low-privilege account, attackers have ways to escalate privilege if they are given access to a machine.
Use Failed Attempts Lockout - A common way to combat brute-force password attacks is to implement a lock-out policy. After a specified number of failed attempts at logging in, the account will lock and an administrator will have to unlock it.
Use Screen Lock/Timeout - Leaving a computer unlocked while you are away is dangerous. Any person can come up and begin working on your computer without your knowledge. For this reason, organizations should implement a screen lock or screen timeout policy. This policy would force the computer to lock after a few minutes of inactivity.
Change Default Administrator's User Account/Password - It's best to immediately change default passwords or disable default accounts altogether and create new accounts.
Disable AutoRun - Certain programs or discs will run immediately when put into the computer. It is best practice to disable the AutoRun and AutoPlay features on the operating system. This is because it gives you time to evaluate the item before allowing it to run on the PC.
Disable AutoPlay - is disabled by default in the Windows OS. AutoPlay does not look in the autorun.inf file for permissions and will prompt the user to choose to execute or not.
Securing Mobile and Embedded Devices - have become an important part of business as we know it. Employees are expected to be available at all times via their phone. But with the new wave of mobile devices in business, organizations must consider the risks. You must be able to identify common methods for securing mobile and embedded devices.
Screen Locks - When a user has access to business resources via a mobile device, it's necessary to ensure that the mobile device is just as secure as a workstation would be. This means having a lock on the screen so that if the phone is lost or stolen, attackers don't have access to the business resources.
Facial Recognition - Screen locks can be enabled with facial recognition that uses biometric facial features to unlock a screen. Facial recognition is common on mobile devices but is prone to false negatives and, less commonly, false positives.
PIN Codes - can be set that must be entered correctly to gain access to the mobile device. A PIN code is often used in conjunction with a biometric authentication method for MFA to provide added security to a device.
Fingerprint - Some devices may use a fingerprint scan as authentication for mobile device access. Fingerprint scans are trending down in mobile devices with the advancements in facial recognition and the front-facing camera.
Pattern - A pattern lock is a method of authentication that requires the user to draw a specified pattern in a 3X3 matrix of dots for access to the mobile device. A pattern lock, like a PIN, can be used in conjunction with biometric authentication for MFA. Some users, however, may choose a very simple pattern to make accessing the device easier, which can be easily discovered, similar to using the word "password" as your password.
Swipe - A swipe lock is not an actual locking method. The swipe merely requires the user to swipe the screen to gain access and should not be used for securing mobile devices.
Remote Wipes - Organizations are able to remotely wipe devices after they are given remote administration control. This is useful if a user reports that their phone has been lost or stolen.

Locator Applications - can help individuals find their devices if they have been lost or stolen. These applications use GPS technology. The location services on the device must be turned on for these applications to work.
OS Updates - Whenever an update is available for a mobile device, it **should be installed**. Applications on the phone should also be kept up to date. When vulnerabilities are found, developers will put out updates to **fix the vulnerabilities**. This is why devices must be kept up to date.
Device Encryption - Mobile devices can also be encrypted to protect the data that is stored on the device. This adds another layer of protection in the case the device is lost or stolen.
Remote Backup Applications - Some organizations may choose to remotely back up the mobile devices that store data. Because mobile devices are typically used during travel, they are more likely to be lost or stolen.
Failed Login Attempts Restrictions - In the same way that you can lock a user's account on a computer, you can lock an account on a mobile device. Mobile devices should lock the ability to log in after a specified number of failed attempts.
Antivirus/Anti-Malware - In the same way that you should protect your computer from viruses and malware using antivirus and anti-malware software, you can download mobile antivirus and anti-malware applications. There are not as many providers for mobile antivirus and anti-malware as there are for computers, but the market is growing.
Firewalls - A mobile firewall acts as a screen between mobile devices and an organization's network. It will monitor all inbound network traffic before it is allowed to access the network system.
Policies and Procedures - should be put in place by an organization so that users understand exactly how to use mobile devices on the organization's network.
Bring Your Own Device (BYOD) vs. Corporate-Owned -
Corporate-owned devices are completely under the control of an organization. In this scenario, the organization can specify policies about which applications can be installed as well as what the device can be used for. However, many organizations are moving to a BYOD environment. **BYOD environments** are more complicated to manage because, while policies can be put in place for accessing *corporate resources*, ultimately, the *device* is owned by the end user.
Profile Security Requirements - When accessing an organization's resources, users must meet all profile security requirements set forth by the organization.
Internet of Things (IoT) - devices are notoriously difficult to secure. Personal IoT devices should not be kept on a separate network from the business network if possible.
Data Destruction and Disposal - As discussed earlier in this guide, dumpster diving is a method of obtaining private information or data from the trash. Let's look at how to properly dispose of computer equipment. Questions of this type will be scenario based.
Physical Destruction - One of the only ways to ensure that data is no longer accessible is to completely destroy the device the data is stored on. Physical destruction is used when the data on the device needs to be completely removed or destroyed.
Drilling - is a destruction method where a drill is used to physically put a hole into the device, destroying the internal components of the device.
Shredding - To prevent dumpster divers from stealing private information, organizations should have a shredding policy in place to shred all documents before throwing them in the trash.
Degaussing - Using an electromagnet is one way to wipe a hard drive. However, it's often still possible for individuals to pull data off of a hard drive even though it's been wiped. One wipe using a magnet is not enough. This process, known as degaussing, **must be done over and over** again.
Incinerating - Some organizations may choose to completely incinerate their devices to ensure that data can not be pulled off the devices.
Recycling or Repurposing - Rather than destroy the devices, many organizations will take the route of recycling or repurposing the devices. Best practices should be followed to ensure the safety of the data on the repurposed or recycled device.
Erasing/Wiping - Before recycling or reuse, all data should be completely wiped or erased to prevent data breach.
Note: Standard wiping or erasing of a drive does not actually remove the data from the drive or device, it merely marks the space being wiped or erased as available for overwriting. Data may still be recovered before it is actually overwritten. To fully wipe or erase a drive, the data needs to be **overwritten with zeros or nonsense** before being marked as available.
Low-Level Formatting - can be used to completely wipe a disk. This formatting method takes the drive back to the very beginning of drive controller chip and drive interaction and occurs prior to partitioning.

Standard Formatting - does not erase the data on the disk but marks the space the data occupies as available for use. Standard formatting is not a secure way of wiping a drive.
Outsourcing Concepts - Outsourcing data and device destruction is a valid method of data destruction but comes with considerations of its own.
Third-Party Vendor - can be contracted to destroy or recycle a device or drive. When using third-party vendors, be aware that there is a potential for data leakage either through a mismanaged wipe or insider threats in the vendor.
Certification of Destruction/Recycling - When an organization uses a third-party vendor to dispose and destroy their devices, they may receive a certificate of destruction stating that the items have been recycled and all data storage components have been wiped or destroyed pursuant to all applicable laws, including environmental and waste-management regulations.
Security for Small Office/Home Office (SOHO) Wireless and Wired Networks - It will also be important for you to manage a scenario related to a SOHO situation and devise best practice security measures for that environment, whether it is wired or wireless. Questions of this type will be scenario based.
Home Router Settings - Routers used in the home can be **configured for security** and best practices should be followed. While most home routers are considered to be plug and play, you should always access the router to change the default password and manage updates and other security settings prior to use.
Change Default Passwords - It is easy to do an online search and find the default usernames and passwords of wireless devices. When setting up a wireless network, ensure that the default passwords are not being used.
IP Filtering - also referred to as **firewall rules**, should be used on a home router to secure the internal network from an external network, such as the internet.
Firmware Updates - on a wireless device should be kept up to date. Whenever the latest updates are not installed on a device, that device is susceptible to attacks.
Content Filtering - Some wireless routers will come with built-in content filtering and **parental controls**. These can be used to block users from navigating to sites that could contain malware.
Physical Placement/Secure Locations - when setting up a wireless network, you want the network to span your entire building or workspace, without leaking outside of your organization. It's a difficult task to do perfectly, but it can be achieved by doing wireless network surveys and ensuring that your antennas and access points are placed in the right locations.
Dynamic Host Configuration Protocol (DHCP) Reservations - can be used to create a dynamically static-assigned IP address and is commonly used with network printers.
Static Wide-Area Network (WAN) IP - set a static IP address on your wireless router so that, in the event of an internet outage or power outage, the IP address will not change when the device is back online.
Universal Plug and Play (UPnP) - is designed to make connecting devices to a network simpler. To protect a SOHO, UPnP should be required to ask permission prior to connection to the SOHO network or network-connected device.
Screened Subnet - also referred to as a **demilitarized zone (DMZ)**, creates a separation between the exterior and interior of a network where a communication can take place without placing the interior of the network at risk.
Wireless-Specific - There are some security measures specific to wireless networks. Let's take a look at some of them.
Changing the Service Set Identifier (SSID) - Keeping the default SSID can provide a potential attacker with information they need to target you. For example, the default SSID may show exactly what type of wireless device you are using. It's best to change the SSID before you begin using the wireless network.
Disabling SSID Broadcast - is one way to prevent attackers from finding your wireless network. It requires a few extra steps for getting yourself and other users connected to the network, but it does add that additional layer of protection. Experienced hackers will still be able to locate hidden networks, but generally attackers go after the low-hanging fruit.
Encryption Settings - secures your wireless network with an authentication protocol. Wireless encryption requires both a password and an encrypted key when you connect. The encryption key can generally be located in the setup page of a wireless router.
Disabling Guest Access - While guest access is designed to allow minimal permissions, it can easily be exploited for privilege escalation.
Changing Channels - Wireless local area networks (WLANs) operate on two primary frequency channels, 2.4 GHz and 5 GHz. For security, the channel can be changed to reduce the possibility of overlap in the network.
Firewall Settings - As with other network-connected devices, firewalls should be configured to provide the **highest security possible** for wireless networks.
Disabling Unused Ports - can prevent unauthorized parties from plugging in and gaining access to the entire network.

Port Forwarding/Mapping - is the configuration of ports on a device to allow or block port access. Port forwarding/mapping can be configured on a wireless device in the same way that it is on a wired network.
Browser Security - Web browsers are one of the most used tools on the internet and require security considerations and best practices in and of themselves. Questions in this section will be scenario based.
Browser Download/Installation - Browsers can be downloaded either online or offline. An **online browser download** is an online link that installs a smaller installation application on a device. The installation application then pulls the needed data for the rest of the browser from the internet via a live internet connection. An **offline browser download** is a download of the complete installation package in a single file. The initial offline installation download does require an active internet connection. However, once the download is complete, it can be used to install the browser on additional devices without the need of an internet connection. With either method, care must be taken to install a clean version of the browser.
Trusted Sources - Browsers should be downloaded and installed only from trusted sources, preferably through the official distributor.
***Hashing* -** is one method of verifying the integrity of a downloaded browser installation. This method creates a secure hash algorithm of the executable that is stored in a separate location and can be compared to the executable if the browser needs to be reinstalled.
Untrusted Sources - or unverified sources should not be used for browser installation or download. To ensure a verified installation, go directly to the vendor page for the browser you wish to install. Do not follow links within a non-vendor page for installation.
Extensions and Plug-ins - are designed to make a browser more functional to the end user. However, care must be taken when installing extensions and plug-ins.
Trusted Sources - As with browser installation, trusted sources should be used when downloading and installing extensions and plug-ins.
Untrusted Sources - such as third-party links, should not be used for extension and plug-in installation. Verify the source prior to installation.
Password Managers - A or credential manager is offered by many browsers as a way to store credentials and passwords. Only use a password manager on a private and secure device.
Secure Connections/Sites—Valid Certificates - Web browsers identify secure connections through certificate validation. Try to avoid connections or sites with invalid certificates.
Settings - Like firewall settings, a web browser has browser-specific security settings that can be configured to provide the highest level of security.
Pop-Up Blocker - is designed to prevent pop-ups and pop-unders from appearing. Pop-ups are blocked by default on most browsers but may need to be allowed for specific websites that require pop-ups for functionality.
Clearing Browsing Data - removes the data that was stored during browsing and should be used to maintain data privacy. The frequency of clearing browser data is dependent upon the usage of the device. For example, if the browser is on your home computer that only you have access to, it is not as vital to clear browser data after browsing. However, if you are using a public browser, such as at the library, the browser history should be cleared upon each usage.
Clearing Cache - The browser cache is where data is placed when rendering a website for quick retrieval. The cache should be cleared frequently to maintain browser security.
Private-Browsing Mode - does not store any web browsing data and can be used for security as well as privacy. However, private-browsing mode is **not completely private**. Private-browsing mode merely keeps the browsing data on a device secret for that particular device. All visited websites will still receive any information that was collected by the website.
Sign-In/Browser Data Synchronization - allows for the synchronization of a user's browser across multiple devices. Caution should be used when synchronizing browsers. Do not synchronize on public devices or, if synchronization is required, remember to log off and delete the history and cache before leaving the browser.
Ad Blockers - are designed to prevent spam advertisements in browsers. Ad blockers work by comparing a URL to a set list of blacklisted or whitelisted URLs. If the URL is **blacklisted**, it is denied download on the browser. URLs can be **whitelisted** by users to allow them through the ad blocker. For example, an ad blocker may ask the browser if they want to see advertisements from ABC Company. If the user agrees, the URL for ABC Company is whitelisted and allowed access.