CompTIA Security+ Cheat Sheet

Concepts, Controls and Tools

By Krystal Ballew

1.0 Threats, Attacks, and Vulnerabilities

- **Given a Scenario, Analyze Indicators of Compromise (IoC) and Determine the Type of Malware.**
  - **Virus:** An unsolicited and unwanted malicious program.
  - **Worm:** A self-contained infection that can spread itself through networks, E-mails, and messages.
  - **Crypto-Malware:** A malicious program that encrypts files on the computer to extort money from the user.
  - **Ransomware:** Denies access to a computer system or data until a ransom is paid. Can be spread through a phishing E-mail or an unknowingly infected website.
  - **Adware:** A program that produces ads and pop-ups using a browser. May replace the original browser and/or produce fake ads to "remove" the adware, which only downloads more malware.
  - **Spyware:** Software that installs itself to spy on the infected machine and sends stolen information back to the host machine.
  - **Keylogger:** A malicious program that records keystrokes from the infected machine.
  - **Logic Bomb:** A malicious program that lies dormant until a specific date or event occurs.
  - **Bots:** AI that performs specific actions as a part of a larger entity known as a *botnet*.
  - **Trojan:** A form of malware that pretends to be a harmless application.
  - **Remote Access Trojan (RAT):** A remotely operated Trojan.
  - **Rootkit:** A backdoor program that allows full remote access to a system.
  - **Backdoor:** Allows for full access to a system remotely.

- **Compare and Contrast Types of Attacks.**
  - **Social Engineering:** Gathering information by exploiting the weakest part of security, *people.*
    - **Phishing:** Sending false E-mails pretending to be legitimate to steal information from the user.
    - **Spear Phishing:** Attacks that target specific users.
    - **Whaling:** A targeted attack on a powerful or wealthy individual.
    - **Vishing:** An attack through a phone or voice communication.
    - **Smishing:** An attack through SMS.
    - **Tailgating/Piggybacking:** Closely following authorized individuals to get access to secure areas.
    - **Impersonation:** Taking on the identity of an individual to gain access to a system.
    - **Dumpster Diving:** Going through trash to find thrown-away valuable information or possessions.
    - **Shoulder Surfing:** Watching as a person enters information.
    - **Hoax:** Deceiving the user into compromising security by falsely making them believe they are at risk.
    - **Watering Hole:** Targets a group by infecting a website that is commonly visited by the members.
      - **Principles of Social Engineering/ Reasons for Effectiveness**
        - **Authority:** Behaving as an individual with authority.
        - **Intimidation:** Frightening or threatening the victim.
        - **Consensus:** Influencing others based on what peers do or are said to do.
        - **Scarcity:** Limiting resources or time to act.
        - **Familiarity:** Behaving like a familiar person to the victim.
        - **Trust:** Gaining the victim's confidence or being their "friend."
        - **Urgency:** Limiting time to act. Rushing the victim.
  - **Application and Service Attacks**
    - **Denial of Service (DoS):** Flooding a target machine to prevent the use of its resources.
    - **Distributed Denial of Service (DDoS):** Multiple different sources attack one victim.
    - **Man-in-the-Middle:** The attacker alters the communication between two parties who believe they are directly communicating.
    - **Buffer Overflow:** A program writes more data than can be held in a fixed block of memory.

  - **Injection:** Inserting code into a vulnerable computer program and changing the course of execution.
  - **Cross-Site Scripting (XXS):** Found in web applications. Allows for an attacker to inject client-side scripts into web pages.
  - **Cross-Site Request Forgery (XSRF):** Unauthorized commands are sent from a user that is trusted by the website. Allows the attacker to steal cookies and harvest passwords.
  - **Privilege Escalation:** Exploits a vulnerability that allows an attacker to gain access to resources that they normally would be restricted from accessing.
  - **ARP Poisoning:** The act of falsifying the IP-to-MAC address resolution system employed by *TCP/IP.*
  - **Amplification:** The amount of traffic sent by the attacker is originally small but then is repeatability multiplied in an attempt to cause the victim machine to fail or malfunction.
  - **DNS Poisoning:** Exploits vulnerabilities in the *Domain Name System (DNS)* to divert Internet traffic away from legitimate servers and towards fake ones.
  - **Domain Hijacking:** Changing the registration of a domain name without the victim's permission.
  - **Man-in-the-Browser:** A proxy Trojan horse that infects web browsers and captures session data.
  - **Zero Day:** Exploits for which there is no known defense.
  - **Replay:** Valid data transmission is rebroadcasted, repeated, or delayed.
  - **Pass-the-Hash:** An authentication attack that captures and uses password hashes. The attacker attempts to log on as the user with the stolen hash. This bypasses the need to decrypt passwords.
  - **MAC Spoofing:** The attacker falsifies the *MAC address* of a device.
  - **IP Spoofing:** An intruder uses another site's IP address to masquerade as a legitimate site.
- **Hijacking Attacks**
  - **Clickjacking:** Deceives the user into clicking on a malicious link by adding the link to a transparent layer over what appears to be a legitimate web page.
  - **Session Hijacking:** An attacker impersonates the user by using their legitimate session token.
  - **URL Hijacking/ Typo-squatting:** Redirects the user to a false website based on a misspelled URL.
- **Driver Manipulation**
  - **Shimming:** Injecting alternate or compensation code into a system in order to alter its operations without changing the original or existing code.
  - **Refactoring:** Rewrites the internal processing of code without changing its behavior.
- **Wireless Attacks**
  - **Replay:** This is a passive attack where the attacker captures wireless data, records it, and then sends it on to the original recipient without them being aware of the attacker's presence.
  - **Evil Twin:** An *Access Point (AP)* that has the same *Service Set Identifier (SSID)* as a legitimate Access Point. Once a user connects to it, all wireless traffic goes through it instead of the real AP.
  - **Rogue Access Point:** An unauthorized *Wireless Access Point (WAP)* or router that is designed to bypass network security configurations but opens the network and its users to attacks.
  - **Jamming:** Disabling a wireless frequency with noise to block the wireless traffic.
  - **Wi-Fi Protected Setup (WPS):** Allows users to easily configure a wireless network, sometimes by using only a PIN. The PIN can easily be found through a *brute force attack*.
  - **Bluejacking:** Sending unauthorized messages to a Bluetooth device.
  - **Bluesnarfing:** Gaining unauthorized access to or stealing information from a Bluetooth device.
  - **Radio Frequency Identifier (RFID):** Communicates with a tag placed in or attached to an object using radio signals. Can be jammed with noise interference, the blocking of radio signals, or removing/disabling the tags themselves.
  - **Near Field Communication (NFC):** A wireless technology that allows for smartphones and other devices to establish communication over a short distance.
  - **Disassociation:** Removes clients from a wireless network. A form of *Denial of Service (DoS).*
- **Cryptographic Attacks**
  - **Brute Force:** A password-cracking program that systematically guesses every possible combination of characters until the correct password is found.

        - **Dictionary:** Creates encrypted versions of common dictionary words and then compares them against those in a stolen password file. Guessing using a list of possible passwords.
        - **Rainbow Tables:** Large pre-generated data sets of encrypted passwords used in password attacks.
        - **Birthday:** Used to find collisions in hashes and allows the attacker to create the same hash as the user. Exploits the fact that if the same mathematical function is performed on two values and the result is the same, then the original values must be the same.
        - **Collision:** When two different inputs produce the same hash value.
        - **Replay:** The attacker captures network packets and then retransmits them back onto the network to gain unauthorized access.
        - **Weak Implementations:** The main cause of failure in modern cryptographic systems are due to poor or weak implementations as opposed to a failure caused by the algorithm itself.
        - **Downgrade:** Forces a system to lessen its security, allowing the attacker to exploit the lesser security control. It is most often caused by weak implementations or deprecated cipher suites.

- **Explain Threat Actor Types and Attributes.**
    - **Threat Actors**
        - **Script Kiddies:** A person who uses pre-existing code and scripts to hack into machines, because they lack the expertise to write their own.
        - **Hacktivist:** Someone who misuses computer systems for a socially or politically motivated agenda.
        - **Organized Crime:** Professionals motivated by profit. They have enough money to source the best gear, technology and talent. Multiple people perform specific roles; Gathering data, managing exploits, and writing unique code.
        - **Nation States/APT:** An APT is an *Advanced Persistent Threat*. These are major security risks that can cost companies and countries millions of dollars. Nation states have very sophisticated hacking teams that target the security of other nations. They often attack military organizations, large security sites or infrastructure such as power plants.
        - **Insiders:** Someone who has intricate knowledge of the company and how its network works. They can pinpoint a specific vulnerability and may even have access to multiple parts of the network.
        - **Competitors:** Rival companies can bring down a network or steal information through espionage.
    - **Attributes**
        - **Internal/External:** Insider threats can be intentional, unintentional, or an act of God. External is someone outside the company trying to get in.
        - **Level of Sophistication:** The skill of the hacker and the complexity of the attack.
        - **Resources/Funding:** The amount of money and the value of the technology being used.
        - **Intent/Motivation:** The reason for the attack. Can be for political, monetary, or social reasons.
        - **Use of Open-Source Intelligence (OSINT):** Data that is collected through publicly available information. Can be used by threat actors to help find their next target or how to best attack their target. OSINT is also helpful for mitigating risks and for identifying new threat actors.

- **Explain Penetration Testing Concepts.**
    - **Concepts**
        - **Active Reconnaissance:** The use of tools to send data to systems and analyze their responses. Usually starts with various network and vulnerability scanners. Illegal without proper authorization.
        - **Passive Reconnaissance:** Not directly interacting with the target's system. Instead, going through and gathering what is already available. Forums and social media are great sources for gathering information about the company and its employees.
        - **Pivoting:** Using a compromised machine to attack other machines on the same network. Attacking and gaining access to an area of lower security to increase the likelihood of initiating a successful attack on an area of greater security. Is also referred to as *island hopping*.
        - **Initial Exploitation:** A vulnerability is taken advantage of to get into the network or system.
        - **Persistence:** Installing backdoors or methods to keep access to the host or networks.

        - **Privilege Escalation:** Allows for a user to get a higher-level access than what authentication allows for. Typically related to a bug or vulnerability. Can be resolved through patching and updating.
        - **Black Box:** Knowing nothing about the network. No prior knowledge.
        - **White Box:** The *pen-tester* is given a network map and has full knowledge of configurations, allowing them to perform specific tests. They may have been given credentials.
        - **Gray Box:** Some knowledge of the network but not incredibly detailed.
        - **Penetration Testing vs. Vulnerability Scanning:** *Pen-testing* is actively attacking the network to exploit vulnerabilities. It assesses the likelihood of exploits being utilized, and potential damages to the network as a result. Performed by humans. *Vulnerability Scans* passively scan a network to identify vulnerabilities. Often automated.

- **Explain Vulnerability Scanning Concepts.**
    - **Passively Test Security Controls:** Uses an automated *Vulnerability Scanner.* Observes and reports findings. Does not take down systems, applications, or services, and does not disrupt business.
    - **Identify Vulnerabilities:** Understanding common attacks and taking inventory of vulnerabilities.
    - **Scanners Can Report:** Missing updates, misconfigured security settings, and known exploits.
    - **Identify Lack of Security Controls:** Vulnerability scanners can identify missing patches or antivirus.
    - **Identify Common Misconfigurations:** Weak or default usernames and passwords, and open ports.
    - **Intrusive vs. Non-Intrusive:** Intrusive scans can interrupt service. They are much more detailed and can exploit vulnerabilities. Non-intrusive scans are passive. They do not exploit vulnerabilities or disrupt service.
    - **Credentialed vs. Non-Credentialed:** Credentialed scans are done as though it is coming from inside the network. It emulates an insider attack. Non-credentialed are done as though it is outside the network. Emulates an outside attack. Shows what would be found if the network was scanned by an adversary.
    - **False Positive:** A result which incorrectly shows that a condition or attribute is present. A false vulnerability.

- **Explain the Impact Associated with Types of Vulnerabilities.**
    - **End-of-Life Systems:** No longer receives updates, and at a high risk of compromise.
    - **Lack of Vendor Support:** Vendor does not support, update, improve, or protect the product.
    - **Embedded Systems:** Programs added for automation and/or monitoring. Not easily patched.
    - **Race Conditions:** The behavior of a system output is dependent on the timing, sequence of events, or a factor out of the user's control.
    - **Improper Input Handling:** The system does not properly validate data. This allows an attacker to create an input that is not expected, which makes the system vulnerable to unintended data.
    - **Improper Error Handling:** Error messages display sensitive data that gives the user too much information.
    - **Misconfiguration/Weak Configuration:** Default configuration use the unsecure out-of-box settings.
    - **Resource Exhaustion:** The number of resources available to execute an action are expended. A *Denial of Service (DoS)* occurs.
    - **Untrained Users:** Users are not properly informed on how to use the systems. Mistakes will likely occur, and the system's resources are more likely to be abused.
    - **Improperly Configured Accounts:** Users should only be given access to necessary resources.
    - **Vulnerable Business Processes:** All tasks, procedures, and functions should be properly assessed and the most valuable and vulnerable should be heavily protected.
    - **Weak Cipher Suites and Implementations:** Use of less robust cryptographic algorithms, such as DES or WEP.
    - **Memory Leak:** Leaves the system unresponsive.
    - **Integer Overflow:** A large integer exceeds data storage capacity.
    - **Buffer Overflow:** Too much data for the computer's memory to buffer.
    - **Pointer Dereference:** Failed deference can cause memory corruption and the application to crash.
    - **DLL Injection:** Allows for the running of outside code.
    - **System Sprawl/Undocumented Assets:** Lack of internal inventory and allowing unsecure devices and systems to connect to the network.
    - **Architecture/Design Weaknesses:** An unsecure and poorly designed network. Not segmenting the systems or internal network.

- **Zero Day:** An exploit for which there is no known fix.
- **Improper Certificate and Key Management:** Allowing for unauthorized access to certificates and keys, which allows for sensitive data to be decrypted. Allowing for certificates to expire is also a risk.

2.0 Technologies and Tools: Install and Configure Network Components

- **Given a Scenario, Implement Hardware and Software-Based Tools to Support Organizational Security.**
  - **Switches:** A networking device that connects devices together on a computer network.
    - **Port Security:** Requires authentication before gaining access to any of the switch interfaces.
    - **Layer 2:** Packets are sent to a specific switch port based on the destination MAC address.
    - **Layer 3:** Packets are sent to a specific next-hop IP address, based on destination IP address.
    - **Loop Prevention:** Spanning-tree algorithms can determine the best path to a host while blocking all other paths to prevent *loops*. Loops can cause a Denial of Service (DoS).
    - **Flood Guard:** Configuration that sets the maximum number of MAC addresses that could possibly be seen on any particular interface.
  - **Routers:** A device that directs data traffic along specific routes.
    - **Access Control List (ACL):** A list of rules detailing what can enter or leave the interface.
    - **Anti-Spoofing:** A device with the intent of excluding packets that have invalid source addresses.
  - **Firewalls:** A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
    - **Access Control Lists (ACL):** A list of rules that can be used to control traffic based on networks, subnets, IP addresses, ports, and some protocols.
    - **Implicit Deny:** The last rule in an ACL indicates that, "all traffic that isn't explicitly allowed is implicitly denied".
    - **Stateless:** Use rules within an ACL to identify allowed and/or block traffic through packet filtering.
    - **Stateful:** Block traffic based on the state of the packet within a session. It adds and maintains information about a user's connections in a state table, referred to as a *connection table*.
    - **Network-Based:** Filtering traffic based on firewall rules and allows only authorized traffic to pass in and out of the network.
    - **Application-Based:** Protects the user by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall.
  - **Network Intrusion Prevention Systems (NIPS) and Network Intrusion Detection Systems (NIDS):** Security solutions that monitor network traffic for suspicious activity and potential security breaches.
    - **Rules:** Standards set to differentiate good traffic from suspicious traffic.
    - **Signature-Based:** Detects attacks based on known attack patterns documented as *attack signatures*.
    - **Heuristic/Behavior-Based:** Detects attacks by comparing traffic against a baseline to find anomalies.
    - **Anomaly-Based:** Abnormal packets or traffic when compared to a baseline.
    - **Analytics:** Shows the amount, type and history of traffic coming through.
    - **Inline:** Connected directly to the network and monitors the flow of data as it occurs.
    - **Passive:** Connected through a switch or port on the network and receives a copy of data as it occurs.
    - **In-Band:** Sits within the network and can quickly warn of or prevent malicious traffic.
    - **Out-of-Band:** Outside the flow of traffic. Can only warn of malicious traffic.
    - **False Positive:** Blocking or alerting against legitimate incoming traffic.
    - **False Negative:** Allowing actual harmful incoming traffic.
  - **VPN Concentrators:** A type of routing device that allows for secure VPN connections and for the safe delivery of messages between VPN nodes. Allows for the handling of a large quantity of VPN tunnels.
    - **Remote Access VPN:** A user-to-LAN connection used by remote users.
    - **Site-to-Site VPN:** Allows multiple sites to connect to remote sites over the Internet.
    - **Always-On VPN:** The user does not connect and disconnect and instead is always connected.

  - **IPSec:** A protocol suite for securing *Internet Protocol (IP)* communications. Encrypts and authenticates all of the packets in a session between hosts or networks. Secures more applications than SSL and TLS.
    - **Tunnel Mode:** The default mode for IPSec. The entire pack is protected.
    - **Transport Mode:** Used for end-to-end communications in IPSec.
    - **Authentication Header (AH):** IPsec protocol that authenticates that the packets received were sent from the source identified in the header.
    - **Encapsulating Security Payload (ESP):** IPSec component that provides the same services as AH and also ensures confidentiality when sending data.
    - **Full Tunnel:** All of the traffic is sent over the secure VPN.
    - **Split Tunnel:** Only some traffic is sent over the secure VPN while the rest of the traffic is sent over the Internet.
    - **TLS:** The replacement of SSL to encrypt data-in-transit. Uses certificates issued by CAs.
- **Proxies:** Acts as an intermediary for requests from clients seeking resources from servers.
  - **Forward Proxy:** Forwards requests from internal clients to external servers.
  - **Reverse Proxy:** Takes in requests from the Internet and forwards them to an internal web server.
  - **Transparent Proxy:** Accepts and forwards requests without performing any modifications on them.
  - **Application/Multipurpose:** A proxy server that knows the application protocols that it supports.
- **Load Balancers:** A reverse proxy that distributes network or application traffic across a number of servers. Designed to increase capacity of concurrent users and reliability of applications.
  - **Active-Active:** All servers are actively processing requests.
  - **Active-Passive:** Some servers are not active and only go active if a server fails.
  - **Scheduling:** Sends requests to servers using set rules.
  - **Affinity:** Sends client requests to the same server based on the client's IP address.
  - **Round-Robin:** Sends requests in a predefined order.
- **Access Points (APs)**: A network device that allows wireless devices to connect to a wired network, such as the Internet. APs are also known as wireless routers because they can act as both routers and firewalls.
  - **SSID:** Name of a wireless network.
  - **MAC Filtering:** A method of controlling access on a wired or wireless network by denying unapproved MAC address access to a device.
  - **Signal Strength:** The quality and distance of a signal.
  - **Band Selection/Width:** Can be set between 2.4 GHz and 5 GHz depending on which 802.11 protocol is being used.
  - **Controller-Based:** Requires a controller for centralized management. Not manually configured.
  - **Standalone:** Does not require a controller and are generally used in smaller environments.
  - **Fat:** Has everything necessary to handle wireless clients. If end-user deploys several *Fat Wireless Access Points (WAP)*, each one needs to be configured individually.
  - **Thin:** Acts as a radio and antenna that is controlled by a wireless switch. If multiple *Thin Wireless Access Points (WAP)* are deployed, the entire configuration takes place at the switch. This is the far cheaper option.
- **Security Information and Event Management (SIEM):** Combines both *Security Information Management (SIM)* and *Security Event Management (SEM)* into one security management system. SIEM technology collects event log data from a range of sources, identifies activity that deviates from the norm with real-time analysis, and takes appropriate action.
  - **Aggregation:** The gathering of log and event data from the different network security devices.
  - **Correlation:** Relating various events to identifiable patterns. If those patterns threaten security, then action must be taken.
  - **Automated Alerting and Triggers:** Sends alerts in response to events that occur within the log files.
  - **Time Synchronization:** Ensures that timing of all security events is synchronized and recorded using *Network Time Protocol (NTP).*

        - **Event Deduplication:** Trimming event logging so that the same event is not recorded more than once, preventing the overflow of log space.
        - **Logs:** Prevents alteration of logs and archives the source logs with write protection.
    - **Data Loss Prevention (DLP):** Policies and technologies that protect data loss through theft or destruction.
        - **USB Blocking:** Prevents the use of USBs.
        - **Cloud-Based:** Prevents sensitive data from being stored on the cloud without proper encryption and authorization.
        - **E-mail:** Protects against E-mail fraud and from valuable data from being sent through E-mail.
    - **Network Access Control (NAC):** Enforces security policies on devices that access networks to increase *network visibility* and reduce risk.
        - **Dissolvable:** Disappears after reporting information to the NAC device.
        - **Permanent:** Resides on end devices until uninstalled.
        - **Host Health Checks:** Reports sent by NAC to gather information on installed devices.
        - **Agent:** Installed on the end device.
        - **Agentless:** Not installed on the device itself but instead is embedded within a Microsoft Windows *Active Directory* domain controller.
    - **Mail Gateway:** Examines and processes all incoming and outgoing E-mail.
        - **Spam Filter:** An on-premises software solution for filtering spam E-mails.
        - **Data Loss Prevention (DLP):** Prevents data from leaving the organization via E-mail.
        - **Encryption:** Encrypts and decrypts E-mails being sent and received across networks.
    - **Bridge:** Provides interconnection with other bridge networks using the same protocol.
    - **SSL/TLS Accelerator:** Offloading intensive public-key encryption for to an SSL or TLS *hardware accelerator*.
    - **SSL Decryptor:** Allows the user to view unencrypted HTTPS traffic.
    - **Media Gateway:** Converts media streams between disparate telecommunications technologies.
    - **Hardware Security Module (HSM):** Manages and provides crypto-processing of *digital keys*.

- **Given a Scenario, Use Appropriate Software Tools to Assess the Security Posture of an Organization.**
    - **Protocol Analyzers:** Hardware or software that captures packets to analyze their contents. Allows for easy viewing of traffic patterns, identifying unknown traffic, and verifying packet filtering and security controls.
        - **Big Data Analytics:** Allows for the user to store large amounts of data and then easily go through it.
    - **Network Scanners:** A computer program used for scanning networks to obtain usernames, host names, groups, shares, and services.
        - **Rogue Device Detection:** Find unauthorized devices, such as *rogue AP's.*
        - **Network Mapping:** Identifying all devices on a network along with a list of ports on those devices.
            - **Passive:** Purely observational.
            - **Active:** Interacting with the network by sending traffic and trying to access parts of it.
    - **Wireless Scanners and Crackers:** Tools that helps troubleshoot and improve a wireless network. Can also help ensure that a Wi-Fi network is secure and encrypted.
        - **Wireless Scanners:** For wireless monitoring. It scans wireless frequency bands in order to help discover *rogue APs* and crack passwords used by wireless APs.
        - **Wireless Cracker:** Uses wireless attacks to test if an attacker could find the passwords to gain access to parts of your network.
            - **WEP:** Cryptographic vulnerabilities are relatively straightforward.
            - **WPA1 PSK and WPA2 PSK:** Susceptible to *dictionary, brute force* and *rainbow table attacks*.
    - **Password Crackers:** A program that uses the file of hashed passwords, such as a *rainbow table* to break the hashed passwords of the network. Getting the hashes is the hardest part.
    - **Vulnerability Scanners:** Identifies vulnerabilities, misconfigured systems, and a lack of security controls. They can be passive or active. Neither impact the system greatly during a test.
    - **Configuration Compliance Scanners:** A vulnerability scanner that verifies systems are configured correctly and meet the minimum-security configurations. It does this by comparing the system to a file that has the proper configurations. This is an ongoing task and can be integrated with the login process.

- **Exploitation Frameworks:** A set of pre-designed exploits. The user just needs inject them into the network. These toolsets can be used offensively by hackers or defensively by pen-testers.
- **Data Sanitization Tools:** Tools that overwrite data on hard drives so that it is unrecoverable. This only needs to be done once but some may do it multiple times to feel safe.
- **Steganography Tools:** Allows for the user to embed data into an image, video, sound file, or packet. It is an example of *security through obscurity*.
- **Honeypots:** Intentionally vulnerable decoy systems or networks to gather information on the attacker.
- **Backup Utilities:** Protects from data loss or corruption and protects systems from unintentional downtime.
- **Banner Grabbing:** Capturing the initial message (the banner) from a network service. The banner often discloses the application's identity, version information, and other sensitive information.
- **Command Line Tools**
  - **ping:** Tests reachability, it is a primary troubleshooting tool.
  - **Netstat:** Network Statistics.
    - **netstat -a:** Show all active connections.
    - **netstat -b:** Show binaries, for Windows.
    - **netstat -n:** Does not resolve names.
  - **tracert** (Windows)/**traceroute** (MacOS/Linux): Uses the *Internet Control Message Protocol (ICMP) Time to Live (TTL)* error message to map the path of a packet. TTL is measured in hops. TTL = 1 for the first router, and 2 refers to the second router.
  - **nslookup:** Gathers data from DNS servers; lookup names and IP addresses. Was replaced by **dig**.
  - **Dig:** *Domain Information Groper*. More advanced than **nslookup** and shows more detailed domain information. For Linux but can be downloaded for Windows.
  - **Arp -a:** Views the local ARP table.
  - **ipconfig:** Shows the Windows TCP/IP configuration.
  - **ifconfig:** Shows the Linux interface configuration.
  - **ip:** Replaced **ifconfig** on Linux. Shows and manipulates settings on the *Network Interface Card (NIC).*
  - **tcpdump:** A command-line packet analyzer that allows packet capture from the command line.
  - **nmap:** Scans a network and creates a map. Useful as a vulnerability scanner because it can find open ports and unsecured access points.
  - **netcat:** Used to safely connect to remote systems using a command line instead of a front-end application. Can also be used for *banner grabbing*.

- **Given a Scenario, Troubleshoot Common Security Issues.**
  - **Unencrypted Credentials/Clear Text:** All authentication must be encrypted. Unencrypted credentials allow the attacker to elevate privileges, establish a foothold, maintain persistence, and move to other networks.
  - **Logs and Event Anomalies:** Block all outside access until the issue is fixed. Backup and preserve the current logs, and if possible, restrict access to more sensitive data till the issue is resolved.
  - **Permissions Issues:** Determine the access a user needs to complete their job. Confirm Permissions on initial configurations, perform periodic audits, and provide a process for changes and updates.
  - **Access Violations:** A user is able to properly logon and then access systems they don't have proper authorization for. Segmentation fault. OS locks out or prevents access to restricted memory.
  - **Certificate Issues:** Certificates should be signed by a trusted party, be up to date, and be properly checked.
  - **Data Exfiltration:** Data is the most important asset to attackers. DLP helps prevent this.
  - **Misconfigured Devices:** Cybercriminals can exploit misconfigurations to gain access to systems or networks, steal sensitive data, or disrupt operations.
    - **Firewalls:** Provide too much access, and difficult to audit when using a large rule base.
    - **Content Filters:** URLs are not specific, and some protocols are not filtered.
    - **Access Points (APs):** No encryption mechanisms or open configurations.
  - **Weak Security Configurations:** Make sure to regularly upgrade equipment and update firmware. Using hash algorithms that are susceptible to collisions.
  - **Personnel Issues:** People are often the weakest link.

        - **Policy Violation:** Transferring private data or visiting unsafe websites.
        - **Insider Threat:** Authenticated users have free reign. Assign correct user rights and permissions.
        - **Social Engineering:** Deceit can cause employees to give up personal or valuable data.
        - **Social Media:** Sharing private data or personal information.
        - **Personal E-mail:** Uses company resources and leaves the network vulnerable.
    - **Unauthorized Software:** May be work-related but also conflict with company software. Could be malware.
    - **Baseline Deviation:** Everything is well-documented. Any changes to the norm should be noted, and no remote access should be allowed until the system matches the current baseline.
    - **License Compliance Violation:** Make sure licenses are up to date and valid.
    - **Asset Management:** Identify and track assets to respond faster to security risks. Keep detailed records of the most valuable assets. Usually automated.
    - **Authentication Issues:** The more factors the safer. Makes sure the user can be authenticated.

- **Given a Scenario, Analyze and Interpret Output From Security Technologies.**
    - **Host-Based Intrusion Detection System (HIDS):** Runs on a single computer and alerts administrators of potential threats. Warns of attacks against that host.
    - **Host-Based Intrusion Prevention System (HIPS):** Runs on a single computer and intercepts potential threats to help prevent attacks against that host.
    - **Antivirus:** Software that is designed to detect viruses and protect a computer and its files from harm.
    - **File Integrity Check:** An application that can verify that the files have not been modified using hash algorithms to authenticate the file.
    - **Host-Based Firewall:** On a single host that restricts incoming and outgoing network activity for that host.
    - **Application Whitelisting:** Allowing only approved programs on a computer, network, or mobile device.
    - **Removable Media Control:** Blocks users from using USB drives, CD/DVD drives or portable hard drives/flash drives to help prevent the installation of viruses, malware, and exfiltration of data.
    - **Advanced Malware Tools:** Block malware from running by blocking file signatures, heuristics, or anomalous behavior. Need to be routinely updated with the latest definitions to be secure against current threats.
    - **Patch Management Tools:** Tools that aid in the monitoring, evaluating, testing, and installing of the most current software patches and updates.
    - **Unified Threat Management (UTM):** A group of security controls combined in a single solution that can inspect data streams for malicious content and block it.
    - **Data Loss Prevention (DLP):** Systems that identify, monitor, and protect data from unauthorized use, transfers, modification, or destruction.
    - **Data Execution Prevention (DEP):** Memory regions are marked as non-executable which prevents code from being executed. This protects against memory abuse attacks such as *buffer overflows*.
    - **Web Application Firewall:** A firewall that looks monitors and filters packets carrying HTTP traffic using a set of communication rules.

- **Given a Scenario, Deploy Mobile Devices Securely.**
    - **Connection Methods**
        - **Cellular:** Network used for mobile phones. Potential risks: Cellular devices are susceptible to traffic monitoring, location tracking, and attackers can gain access from anywhere in the world.
        - **Wi-Fi:** A *Local Area Network (LAN)* that uses high frequency radio signals to transmit data over distances of a few hundred feet. Potential risks: If the connection is not encrypted, it is vulnerable to eavesdropping. Jamming frequencies or interferences can cause a *Denial of Service (DoS).*
        - **SATCOM:** *Satellite Communications* is used for communication in remote areas and during natural disasters. Potential risks: SATCOM devices are at risk of leaking geo-positioning data and remote code execution. They are not easily updated remotely.
        - **Bluetooth:** Allows electronic devices like cell phones and computers to exchange data over short distances using radio waves.
        - **Near Field Communication (NFC):** Enables the communication of two electronic devices in close proximity to each other. Typically used for payment systems, identity tokens, and to help pair

Bluetooth devices. Potential risks: Active devices can perform a remote capture up to a ten-meter range. Jamming frequencies or interferences can cause a *Denial of Service (DoS).* Can be vulnerable to *relay* and *replay attacks*.

  - **ANT:** A wireless sensor protocol that uses a 2.4 GHz *Industrial, Scientific, and Medical (ISM)* band to communicate. Used in heart monitors and fitness sensors. Potential risks: At risk of *band-jamming* and *eavesdropping* because encryption is vulnerable.
  - **Infrared:** Electromagnetic waves of frequencies lower than the red of visible light. Used to control entertainment devices and other IR devices.
  - **Universal Serial Bus (USB):** A cable used to connect mobile devices to other devices. Is comparatively safer than wireless because it requires a physical connection and data is not allowed to be transferred without being unlocked first. Potential risks: Mobile devices can act as storage devices allowing for the exfiltration and theft of data.
- **Mobile Device Management (MDM) Concepts**
  - **Application Management:** Limiting which applications can be installed on a device.
  - **Content Management:** Limiting access to content hosted on company systems and controlling access to company data stored on mobile devices.
  - **Remote Wipe:** Allows for the deletion of all data and configuration settings from a device remotely.
  - **Geofencing:** Using GPS to define geographical boundaries for where the app can be used.
  - **Geolocation:** The location of a device identified by GPS.
  - **Screen Locks:** Prevents someone from being able to pick up and use a mobile device.
  - **Push Notifications:** Using SMS texts to send messages to selected users or groups.
  - **Passwords/Pins:** Keep the device safe with *something you know*.
  - **Biometrics:** Keep the device safe with *something you are*.
  - **Context-Aware Authentication:** Uses multiple elements to authenticate a user and a mobile device.
  - **Containerization:** Isolating and protecting the application, and any data used by the application.
  - **Storage Segmentation:** Separates the information on a device into *partitions*.
  - **Full Device Encryption:** Protects against loss of confidentiality.
- **Enforcement and Monitoring**
  - **Third-Party App Stores:** Any app that isn't from the Apple App Store or Google Play is more likely to be a security risk.
  - **Rooting:** In Android, the process of modifying the device to gain *root-level* access.
  - **Jailbreaking:** In Apple, the process removing all software restrictions from the device.
  - **Sideloading:** The process of copying an application package to a mobile device.
  - **Custom Firmware:** The removal of the pre-installed firmware and replacing it. This may remove bloatware included by the vendor, add or remove features, and streamline the OS to optimize performance.
  - **Carrier Unlocking:** The device can be used by any carrier. Most cellular devices only work with specific carriers.
  - **Firmware Updates:** Downloading upgrades, patches, and improvements to the existing firmware.
  - **SMS/MMS:** Sending alerts through text messages.
  - **External Media:** Disable it to prevent the transferring of files through physical ports.
  - **Universal Serial Bus On-The-Go (USB-OTG):** A cable used to connect mobile devices to other devices. It is one of many methods that you can use to connect a mobile device to external media.
  - **Recording/Microphone:** Disable to prevent people from being able to listen in on conversations.
  - **GPS Tagging:** Adding GPS data to a video or photo, providing the location from which it was taken.
  - **Wi-Fi Direct/Ad Hoc Mode:** Means for wireless devices to connect directly to each other without a *Wireless Access Point (WAP).*
  - **Tethering:** The process of sharing an Internet connection from one mobile device to another.
- **Deployment Models**
  - **Bring Your Own Device (BYOD):** Employees connect their own personal devices to the corporate network for work.

        - **Corporate Owned, Personally Enabled (COPE):** Devices owned by the organization but can be used personally by employees.
          Choose Your Own Device (CYOD): Employees can purchase devices on the list and bring them to work. The company then supports, monitors, and manages the device.
        - **Corporate-Owned:** Company owns and controls all aspects of the device. No personal data allowed.
        - **Virtual Desktop Infrastructure (VDI):** A virtual desktop that is created so users can access their desktop from a mobile device.

- **Given a Scenario, Implement Secure Protocols.**
    - **Protocols**
        - **Domain Name Service (DNS):** The hierarchical and decentralized naming system for computers, services, or other resources connected to a private network or the Internet. Does not have any security in its original design
        - **Domain Name Service Security Extensions (DNSSEC):** Provides a reliable authorization service between devices when performing operations on the DNS. Must be digitally signed.
        - **Secure Shell (SSH):** Replaces *Telnet*. Uses *Transmission Control Protocol (TCP)* over port 22. Allows for a securely encrypted terminal connection.
        - **Secure/Multipurpose Internet Mail Extensions (S/MIME):** Digitally signed E-mail content using *public key encryption*.
        - **Secure Real-time Transport Protocol (SRTP):** Protected and encrypted voice communications.
        - **Lightweight Directory Access Protocol Secure (LDAPS):** Protocol used for reading and writing directories over an IP network. Uses TCP ports 389 and 636.
        - **File Transfer Protocol Secure (FTPS):** File transfer using SSL/TLS. Uses TCP ports 989 and 990.
        - **Secure File Transfer Protocol (SFTP):** FTP over an SSH channel. Uses TCP port 22.
        - **Simple Network Management Protocol Version 3 (SNMPv3):** Encrypted statistics gathering from a router. Uses ports 161 and 162.
        - **Secure Sockets Layer (SSL):** Encryption technology developed for web and E-mail over the transport layer. Uses public keys to exchange symmetric keys.
        - **Transport Layer Security (TLS):** The replacement for SSL. Used to encrypt the communication of servers in an organization.
        - **Hypertext Transfer Protocol Secure (HTTPS):** HTTP over SSL/TLS provides a secure connection between the server and web browser. Uses TCP port 443.
        - **Secure Post Office Protocol (POP):** Encrypted E-mail communications used for retrieving E-mail from a mail server over SSL/TLS. Sends from port 110 to 995.
        - **Secure Internet Message Access Protocol (IMAP):** The standard E-mail protocol for storing E-mail messages on a mail server over SSL/TLS. Sends from port 143 to 993.
        - **Simple Authentication and Security Layer (SASL):** Provides a source of additional authentication using many different methods, such as Kerberos or client certificates.
    - **Use Cases**
        - **Voice and Video:** SRTP.
        - **Time Synchronization:** NTPsec.
        - **E-mail and Web:** S/MIME and HTTPS.
        - **File Transfer:** FTPS or SFTP.
        - **Directory Services:** LDAPS or SASL.
        - **Remote Access:** SSH.
        - **Domain Name Resolution:** DNSSec.
        - **Network Address Allocation:** DHCP.
        - **Routing and Switching:** SNMPv3, SSH, or HTTPS.
            - **SNMPv3:** Provides confidentiality, integrity, and authentication.
            - **HTTPS:** Allows for browser-based management.

3.0 Architecture and Design

- **Explain Use Cases and Purposes for Frameworks, Best Practices, and Secure Configuration Guides.**
    - **Framework:** A collection of standardized policies, procedures and guides, to direct a user or organization.
        - **Regulatory:** A framework based on mandated laws and regulations. HIPAA is an example of this.
        - **Non-Regulatory:** The common standards and best practices that the organization follows.
        - **National:** Framework based on the laws of a single country.
        - **International:** Framework based on the laws of multiple countries.
        - **Industry-Specific Frameworks:** Based on the standards and regulations of a certain industry.
    - **Benchmarks/Secure Configuration Guides:** Instructions that have been developed over years that are designed to give organizations the best and most secure configurations for a particular system.
        - **Platform/Vendor-Specific Guides:** Hardening guides that are specific to the software or platform. System default configurations are unsecure and at high risk for exploits.
        - **General Purpose Guides:** Security configuration guides that are generic in scope.
        - **Web Server:** Use a *Web Application Firewall (WAF), DMZ*, and/or *Reverse Proxy* for incoming communication from the Internet to the server.
        - **Operating System:** Implement a *Change Management (CM)* policy.
        - **Application Server:** Use industry-standard guides that are vendor-specific. Lock down the server to use only the ports it needs for its specific role.
        - **Network Infrastructure Devices:** Use national or international guides, regulatory/non-regulatory and general-purpose guides for securing these devices.
    - **Defense-in-Depth/Layered Security:** A strategy that uses multiple layers of security measures to protect assets from threats.
        - **Vendor Diversity:** Implementing security controls from different vendors to increase security. Reduces the impact of company-specific vulnerabilities.
        - **Control Diversity:** The use of technical controls, administrative controls, and physical controls to *harden* security.
        - **Administrative Controls:** Mandated standards set by organizational policies or other guidelines.
        - **Technical Controls:** Technologies that reduce vulnerabilities. Examples of this are encryption, antivirus software, IDS/IPS, and firewalls.
        - **User Training:** Providing regular training to users on common threats, emerging threats, and social engineering to raise awareness and help avoid attacks.

- **Given a Scenario, Implement Secure Network Architecture Concepts.**
    - **Zones:** Different network *topologies.*
        - **Demilitarized Zone (DMZ):** Additional layer of protection to protect a network from the Internet.
        - **Extranet:** Private network that can only be accessed by authorized individuals. Links a company with its suppliers and customers.
        - **Intranet:** Network that exclusively for the use of the members of the organization, cannot be accessed by anyone outside of the organization.
        - **Wireless:** Requires a login. An example of this is an internal wireless network used for work.
        - **Guest:** Network with access to the Internet but no access to the internal network. This is useful in congested areas and is generally considered unsecure.
        - **Honeynets:** Dummy network to attract and fool attackers.
        - **Ad Hoc:** A wireless network where the connected devices communicate directly.
    - **Segregation/Segmentation/Isolation:** Separation for performance, security, or compliance.
        - **Physical:** Devices are separate and cannot directly communicate unless physically connected. Does not scale well.
        - **Logical (VLANs):** Separate areas are segmented for different networks, but still housed on the same switch. To connect them, a *Layer 3* device, such as a router, is needed.

        - **Virtualization:** The hardware to separate networks is virtualized, including routers, switches, and other devices apart from the infrastructure. Easier to manage from a security standpoint and everything can be segmented.
        - **Air Gaps:** Devices are physically separate from another and don't share any components to communicate. Great for security but must be mindful of removable media.
        - **Network Address Translation (NAT):** Translates private IP addresses to public addresses and public IP addresses to private.
    - **Tunneling/VPNs**
        - **Site-to-Site:** Send data between two sites in an encrypted form. Done by installing a VPN on both sides. Data will be encrypted at the first VPN and decrypted at the VPN on the receiving end.
        - **Host-to-Site (Remote Access):** Software is installed on the device that wants the VPN tunnel, then the encrypted tunnel is created to connect to the specific network.
    - **Security Device Placement**
        - **Sensors:** Can give transactions, logs, or other raw data. Can be integrated or built-into switches, servers, firewalls, routers, or other network devices.
        - **Collectors:** Could be a console or SIEM. Gathers all the data from sensors into one place and attempts to make sense of it.
        - **Correlation Engines:** Can be built in SIEM. Compares and corresponds data collected from the sensors to determine if an attack is present.
        - **Filters:** Follow the logical path. Does not follow a state set of rules for traffic. Blocks harmful traffic.
        - **Proxies:** Intermediary point between the client and the service. Ensures that the response arrives safely and that the traffic flow is correct.
        - **Firewalls:** Is state-based so that it can filter by content and more specific perimeters. Placed on the outgoing and inward edges of the network.
        - **VPN Concentrators:** Authenticates VPN clients and establishes between tunnels.
        - **SSL Accelerators:** Offloads the SSL process to a hardware accelerator. SSL handshake is complicated and time-consuming.
        - **Load Balancers:** Takes requests from the Internet and spreads them over multiple servers. Can also determine the health of servers.
        - **DDoS Mitigator:** Sits between the network and the Internet. Identifies and blocks DDoS attacks in real-time.
        - **Taps and Port Mirrors:** Physical tap sees what is happening in traffic packets. The software port mirror sends a copy of the traffic packets. Work well for light traffic.
    - **Software Defined Networking (SDN):** The network is fully virtualized with software, and then separated into the *control plane* (configuration) and *data plane* (forwarding and firewalling). Directly programmable from a central location, often automatically.

- **Given a Scenario, Implement Secure Systems Design.**
    - **Hardware/Firmware Security**
        - **Full Disk Encryption (FDE) and Self-Encrypting Drives (SED):** Programs and technologies that encrypt everything on the storage drive.
        - **Trusted Platform Module (TPM):** A chip on the motherboard designed to protect hardware through integrated cryptographic keys.
        - **Hardware Security Module (HSM):** Accelerates cryptographic operations and manages cryptographic keys. Implemented as a physical device and used to accelerate RSA-based operations.
        - **Basic Input/Output System (BIOS):** Basic low-end firmware or software that provides a computer with the basic instructions on how to start.
        - **Unified Extensible Firmware Interface (UEFI):** A method used to boot systems and is intended to succeed BIOS. Improves upon the BIOS design by allowing support for larger hard drives, having faster boot times, providing enhanced security features, and giving the user the ability to use a mouse when making system changes.

        - **Secure Boot and Attestation:** Checks and validates system files during the boot process.
        - **Hardware Root of Trust:** Shows that there was a secure starting point. This is proved by TPMs having a *private key* burned into the hardware.
    - **Operating Systems**
        - **Patch Management:** Keeping systems up to date to help improve stability and security.
        - **System Hardening:** Disabling unnecessary physical and logical ports and services improves security by preventing the users from being able to steal important data through physical storage or injecting viruses through USB. Unnecessary services leave the system vulnerable to viruses and exploits.
        - **Least Functionality:** Limiting the operating system to be able to perform only what is necessary.
        - **Secure Configurations:** Changing the unsecure default setting to protect the system.
        - **Trusted Operating System (TOS):** Provides sufficient support for multi-level security and evidence of correctness to meet high security standards.
        - **Application Whitelisting/Blacklisting:** Protects the system from potentially dangerous applications.
            - **Whitelisting:** Applications allowed on the system.
            - **Blacklisting:** Applications blocked by the system.
        - **Default Accounts and Passwords:** Are easily guessable and must be changed to prevent unauthorized access.
    - **Peripherals**
        - **Wireless Keyboards:** Operate in the clear, allowing for the capture of keystrokes.
        - **Wireless Mice:** Operate in the clear, allowing for the capture of movements or to be controlled remotely.
        - **Displays:** Vulnerable to shoulder surfing, firmware hacks, and eavesdropping.
        - **Wi-Fi-Enabled MicroSD Cards:** Portable storage devices that have access to 802.11 file transfers.
        - **Printers/ Multi-Function Devices (MFDs):** Reconnaissance can be performed via saved logs.
        - **External Storage Devices:** No authentication allows for anyone to read, write and move files.
        - **Digital Cameras:** Easy to steal data.

- **Explain the Security Implications of Embedded Systems.**
    - **Industrial Control System (ICS)/Supervisory Control and Data Acquisition (SCADA):** An ICS is a computer-management deceive that controls industrial procedures and machines. A SCADA is a system used over multiple industries. SCADAs can be protected with VLANs and NIPS. They require extensive segmentation.
    - **Smart Devices/Internet of Things (IoT):** A mobile device that allows the user customizable options, applications to help make daily activities easier, and AI to assist in tasks. IoT is a class of devices that help provide automation and remote control of appliances and devices in the home or office.
        - **Wearable Technology:** Contains personal and health information about a person.
        - **Home Automation:** In-home technology is not updated frequently and are susceptible to attacks.
    - **HVAC:** Heating, ventilation, and air conditioning.
    - **System on a Chip (SoC):** An embedded device where the entire system is on the chip.
    - **Real Time Operating System (ROTS):** Uses predictability to meet real-time requirements. The guesses must be secured.
    - **Printers/ Multi-Functional Devices (MFDs):** Contains logs, documents, and sensitive information that can be accessed and stolen.
    - **Camera Systems:** Video recorders and cameras are IP devices. They pose a hacking risk.
    - **Medical Devices:** Can be attacked, leaving patients at risk.
    - **Vehicles:** Contains onboard Wi-Fi. Vulnerable to threats.
    - **Aircraft/UAV:** Can have communications intercepted.

- **Explain the Importance of Secure Staging and Deployment Concepts.**
    - **Sandboxing:** Virtualizes a deployment process, allows for machines to be completely isolated from each other, and is similar to the environment that will be used.
        - **Environment:** Usually tested in the actual environment that the product will be used in.

        - **Development:** Uses a development environment, version control and change management control to track development.
        - **Test:** Rigid tests are performed to find bugs and errors. Does not simulate the full product.
        - **Staging:** Uses data that the real product would use. Late-stage testing.
        - **Production:** Application is now live, and the updates will be rolled out.
    - **Secure Baseline:** Defines the core of what the development team must do. Lays out what will need to be updated in the future.
    - **Integrity Measurement:** Tests against the baseline to keep it secure.

- **Summarize Secure Application Development and Deployment Concepts.**
    - **Development Life-Cycle Models**
        - **Waterfall:** Not flexible. Done in stages; Cannot revert to a previous stage once the next has begun.
        - **Agile:** Flexible. Allows for collaboration between groups and can go back and fix previous iterations.
    - **Secure DevOps**
        - **Security Automation:** Tools that automatically tests security functions for vulnerabilities.
        - **Continuous Integration:** The basic set of security checks while developing.
        - **Baselining:** Comparing current performance to previously set metric.
        - **Immutable Systems:** Locked and unable to change. To update, the entire platform must be updated.
        - **Infrastructure as Code (IaC):** The ability to deploy infrastructure quickly and automatically via code.
        - **Version Control and Change Management:** The ability to track changes and to easily revert to previous versions.
        - **Provisioning and Deprovisioning:** The adding and removing of assets over time. Installing new devices and uninstalling old ones.
    - **Secure Coding Techniques**
        - **Proper Error Handling:** Ensuring that errors do not crash the system, allow for elevated privileges, or expose private information.
        - **Proper Input Validation:** Sanitizing data to make sure it is correct and secure before using.
        - **Normalization:** Applying rules to a database design to ensure a proper baseline.
        - **Stored Procedures:** A program in the database that enforces the business rules.
        - **Code Signing:** Assigning a digitally signed certificate to code.
        - **Encryption:** Converting readable code to unreadable text to help make it secure.
        - **Obfuscation:** Making code difficult to read.
        - **Code Reuse:** Reusing code in multiple contexts.
        - **Dead Code:** Code that cannot be executed.
        - **Server-Side:** Code that runs on the server.
        - **Client-Side:** Code that runs in the browser and is highly vulnerable to attacks.
        - **Memory Management:** Ensuring that the program does not use too much memory.
        - **Third-Party Libraries and SDKs:** Commonly used so is better understood by attackers.
        - **Data Exposure:** Disclosing private information to attackers.
        - **Compiled Code:** Code that is optimized by an application and converted into an executable.
        - **Runtime Code:** The code that is interpreted as it runs.
    - **Code Quality and Testing**
        - **Static Code Analyzers:** Checks source code for conformance to coding standards, quality metrics, and data flow anomalies.
        - **Dynamic Analysis (Fuzzing):** Providing unexpected inputs to verify the application won't crash.
        - **Stress Testing:** Seeing how many users a program can handle at a time.
        - **Sandboxing:** Using a virtual machine to run the program in a simulated environment to determine if it will properly run. Does not affect production equipment.
        - **Model Verification:** Ensuring the program meets specifications and performs its purpose.

- **Summarize Cloud and Virtualization Concepts.**
    - **Virtual Machines**

        - **Hypervisor:** Software, firmware or hardware that creates, manages, and operates VMs.
            - **Type I:** Known as a *bare metal hypervisor* and runs on the hardware.
            - **Type II:** Known as a *hosted hypervisor* and runs on top of the operating system.
        - **VM Sprawl Avoidance:** VM networks can get too large for the admin to properly manage. To avoid, the admin should enforce a strict process for deploying VMs, have a library of standard VM images, archive or recycle under-utilized VMs, and implement a *Virtual Machine Lifecycle Management* tool.
    - **Containers:** Separating applications from the platform into containers, allowing for applications to run without launching an entire VM. This provides portability and isolation, and less overhead than VM.
    - **Cloud Storage:** The process of storing data in an off-site location that is leased from a provider. Leasing the network and storage that can be on or off site. Has no investment cost, and a low operational cost. Can be accessed anywhere, anytime, and has high mobility.
        - **Software as a Service (SaaS):** The customer uses software that is not locally stored, instead, all of that service is being provided in the cloud. Everything is managed by the provider.
        - **Platform as a Service (PaaS):** A cloud computing model that provides a flexible environment for developing, deploying, running, and managing applications. Managed by customer: Data, applications, and making sure apps run on the OS. Managed by Provider: Runtime, middleware, OS, virtualization, servers, storage, and networking.
        - **Infrastructure as a Service (IaaS):** Also known as *hardware as a service*. Managed by customer: Software (applications, data, Runtime, middleware, and operating system. Managed by Provider: Hardware, virtualization, servers, storage, and networking.
        - **Private:** Deployed within the organization by the organization for the organization.
        - **Public:** Cloud is deployed within an organization for other organizations to use.
        - **Hybrid:** A combination of public and private replication.
        - **Community:** Private or public but only shared between trusted groups.
        - **On-Premises:** Built and managed by the company's data center. Allows for complete control. Has high investment and operational costs.
        - **Hosted:** Leasing the network and storage that is offsite. Access and availability depend on the design. Has no investment cost, and a moderate operational cost.
    - **Virtual Desktop Infrastructure (VDI)/Virtual Desktop Environment (VDE):** The virtualization of a user's desktop where the applications are running in the cloud or in a data center. The user runs as little of the application as possible on the local device.
    - **Cloud Access Security Broker (CASB):** Allows for the integration of security policies across all cloud-based applications. Allows for visibility of applications, and users associated with them. Can be installed on premise or on the cloud server.
    - **Security-as-a-Service (SECaaS):** The provider implements security services such as, authentication, anti-virus, anti-malware, IDS, and event management into the cloud environment,

- **Explain How Resilience and Automation Strategies Reduce Risk.**
    - **Automation/Scripting:** Automated scripts that give a basis for secured configuration with a secured template. Can be configured to accommodate constant changes or can be launched on a specific schedule.
        - **Continuous Monitoring:** Monitors IDS/ logs, networks and SIEMs for changes and threats.
        - **Configuration Validation:** Reviewing the settings of the system to ensure that its security settings are configured correctly.
        - **Templates:** Gives a basis for secured configuration with a standard secured configuration.
        - **Master image:** Is a crafted configuration of a software or entire system. Created after the target system is installed, patched, and configured.
        - **Non-Persistence:** Changes are possible. Due to risks of unintended changes, multiple protection and recovery options must be established.
        - **Elasticity:** The ability for the system to adapt to a workload by allocating and providing resources in an automatic manner.
        - **Scalability:** The ability to handle an ever-increasing workload and to accommodate future growth.

        - **Distributive Allocation:** Providing resources across multiple services or servers as necessary instead of pre-allocation of concentrated resources based on physical system location.
    - **Snapshots:** A copy of the live current operating environment. Reverting to a *known state* is a recovery process that goes back to a previous snapshot. *Rollback to known configuration* includes only a collection of settings. Does not usually include software elements.
    - **Live Boot Media:** A portable storage device that can boot a computer. A ready-to-run version of the OS.
    - **Redundancy:** Secondary or alternate solutions. An alternate means to complete tasks. Helps reduce *single points of failure* and increases *fault tolerance*, the ability for the network, system, or computer to provide a service while withstanding a certain level of failure.
    - **High Availability:** A system that is able to function for extended periods of time with little to no downtime.
        - **Redundant Array of Independent Disks (RAID):** A *high availability* (HA) solution. Employs multiple hard drives in a storage volume with a level of drive loss protection (except for *RAID 0).*

- **Explain the Importance of Physical Security Controls.**
    - **Lighting:** If the perimeter is properly lit, it can deter thieves, break-ins, and other criminal activity.
    - **Signs:** Allows for a controlled entry point, is a psychological deterrent, and helps visitors find their way. Informs of security cameras, safety warnings, and that an area is restricted.
    - **Fencing/Gates/Cages:** Fences set the boundaries of the property and protect against casual intruders. Gates allow for controlled entry and exit. Cages protect assets from being accessed by unauthorized individuals.
    - **Security Guards:** Humans are adaptable, can adjust to live events, and can react to real-time intrusion events. Guards can intervene and control security devices.
    - **Alarms:** Notify security personnel and the authorities of unauthorized activities.
    - **Safes:** Protects valuables from thieves and natural disasters.
    - **Secure Cabinets/Enclosures:** Restricts unauthorized personnel from accessing cabinets.
    - **Protected Distribution/Protected Cabling:** A standard for safely transmitting unencrypted data. Protects from wiretaps.
    - **Airgaps:** Ensure secure networks are physically isolated from unsecure networks.
    - **Mantraps:** Area between two doorways to identify and authenticate individuals. Prevents *tailgating.*
    - **Faraday Cages:** Metal screen or bag that protects devices from electrostatic and electromagnetic influences.
    - **Lock Types:** Can use a key, keypad, cards, or biometrics.
    - **Biometrics:** Uses physical characters to identify the individual.
    - **Barricades/Bollards:** Stops and guides traffic. Can also prevent the entrance of vehicles.
    - **Tokens/Cards:** Items necessary to gain access to secured areas of the building. Can contain information that can identify and authorize an individual.
    - **HVAC:** Keeps servers from overheating and shutting down.
    - **Hot and Cold Aisles:** Allows for strategic air flow control throughout the data center.
    - **Fire Suppression:** Protects the equipment from fire, smoke, corrosion, heat, and water damage. Early fire detection is vital for protecting personnel and equipment from harm.
    - **Cable Locks:** Protects small equipment from theft.
    - **Screen Filters:** Reduces the range of visibility to prevent shoulder suffering.
    - **Cameras:** Deters criminal activity and creates a record of events.
    - **Motion Detection:** Senses movement and sound in a specific area.
    - **Logs:** Documents visitor access and allows for the identification and record-keeping of everyone who has access to the premise.
    - **Infrared Detection:** Detects and monitors changes in the temperature.
    - **Key Management:** Ensure that only authorized individuals have access to only the areas they need to complete their work.

4.0 Identity and Access Management

- **Compare and Contrast Identity and Access Management (IAM) Concepts.**
    - **Identification, Authentication, Authorization and Accounting (AAA)**

        - **Identification:** Finding the unique individual on the system.
        - **Authentication:** The ability to tell if an individual is actually who they claim they are.
        - **Authorization:** Determining what an individual can and cannot access on a system.
        - **Accounting:** The tracking of an individual’s actions on the system.
    - **Multifactor Authentication (MFA):** Uses *at least* two factors of authentication.
        - **Something You Are:** Biometrics.
        - **Something You Have:** Key or Hardware Token
        - **Something You Know:** Pin or Password.
        - **Somewhere You Are:** Current Location.
        - **Something You Do:** Gait or Keystrokes.
    - **Federation:** The authenticating and authorizing between two parties, such as logging onto Facebook with a Google account.
    - **Single Sign-On (SSO):** Only uses one of the factors of authentication.
    - **Transitive Trust:** There are more than two entities. One entity is trusted because they are trusted by someone the system trusts.

- **Given a Scenario, Install and Configure Identity and Access Services.**
    - **Lightweight Directory Access Protocol (LDAP):** Queries information about the directory. *Common Name (CN), Organizational Unit (OU),* and *Domain Controller (DC).* Uses TCP/UDP ports 389.
        - **Secure LDAP:** LDAP over SSL/TLS. Uses TCP on port 636. Does not send queries in plain text.
    - **Kerberos:** Mutual authorization between client and server. It uses a ticket-granting system for authorization and is a government standard.
    - **Terminal Access Controller Access Control System (TACACS+):** Encrypts all parts of communication. Does not suffer due to security issues caused by RADIUS. Authorization and authentication are separated for granular control. Uses TCP over port 49.
    - **Challenge Handshake Authentication Protocol (CHAP):** Authenticates PPP clients to the server. Uses a one-way hash based on a *shared secret* that is compared on the client and server end. Does not send plaintext.
    - **Password Authentication Protocol (PAP):** Username and password are sent as plaintext. Deprecated.
    - **Microsoft CHAP (MS-CHAP):** Delivers a two-way, mutual authentication between the server and client. Separate keys are created for sent and received data. Seen as weak due to it using a 5-bit encryption system.
    - **Remote Authentication and Dial-in User Service (RADIUS):** Combines authentication and authorization. Only encrypts the passwords. There is no command logging, and minimal vendor support. Uses ports 1812 for authentication and authorization and port 1813 for accounting functions.
    - **IEEE 802.1x:** Offers port-based authentication to wireless and wired networks to prevent rogue devices from connecting to secured ports.
    - **Security Association Markup Language (SAML):** Authenticates through a third-party to gain access. The resource is not responsible for authentication.
        - **Principle:** The user or client.
        - **Identity Provider:** The one who assures the identity of the principle.
        - **Service Provider:** A web service of some type.
    - **OpenID Connect:** Handles authentication but and uses OAuth for authorization.
    - **Open Standard for Authorization (OAUTH):** Token authorization happens in the background. Uses a logon from a larger trusted service.
    - **Shibboleth:** An open-source software that uses SAML to provide a third-party federated SSO authentication.
    - **Secure Token:** An authentication mechanism that can identify and authenticate, and allow or deny access.
    - **New Technology LAN Manager (NTLM):** Used for authenticating in Windows. Replaced by Kerberos.
        - **NTMLv2:** Is the most common form used, is somewhat unsecure.

- **Given a Scenario, Implement Identity and Access Management Controls.**
    - **Access Control Models**
        - **Mandatory Access Control (MAC):** Based on classification rules. Objects are given sensitivity labels, subjects are given clearance labels, and users obtain access by having the correct clearance.

  - **Discretionary Access Control (DAC):** Based on user identity. Users are granted access through ACLs placed on objects through the object owner or creator.
  - **Attribute Based Access Control (ABAC):** Assigning access and privileges through a scheme of attributes. Relations and criteria determine access; Time of day, location, and/or IP address.
  - **Role-Based Access Control:** Access is based on the user's position. Changing permissions of a group changes the permissions for all of the members. Not good for companies with high turn-over rates.
  - **Rule-Based Access Control:** Rules are created by the admin to monitor usage. If a user needs access, they must meet the requirements of the rules. Rules are enforced regardless of the user.
- **Physical Access Control**
  - **Proximity Cards:** A smart card that does not require direct contact.
  - **Smart Cards:** Cards that contain identification/authentication information in an integrated circuit chip. Often uses dual factor authentication; *Something you have* (the card), and *something you know* (a pin or password).
- **Biometric Factors:** Verifies identity through physical features. Stored as a mathematical representation.
  - **Fingerprint Scanner:** Scans the unique patterns of the fingerprint to grant access.
  - **Retinal Scanner:** Blood vessels in the back of the retina.
  - **Iris Scanner:** Scans the unique patterns in the Iris.
  - **Voice Recognition:** The identification and translation of spoken language for authorization of a user. Is vulnerable to impersonation.
  - **Facial Recognition:** The identification of an individual from a digital image or a video frame. Is vulnerable to impersonation.
    - **False Rejection Rate (FRR):** Incorrectly identifies an authorized user as an unauthorized user. *Type 1 error.*
    - **False Acceptance Rate (FAR):** Incorrectly identifies an unauthorized user as an authorized user. *Type 2 Error.*
    - **Crossover Error Rate (CER):** The point on a graph where the FAR and FRR meet. The lowest CER point is the most accurate biometric device for a body part.
- **Tokens**
  - **Hardware:** A device that displays and constantly generates a pin or password.
  - **Software:** An app or software that generates a token.
    - **HOTP/TOTP:** Open-source standards to generate one-time use passwords.
      - **HMAC-Based One-Time Password (HOTP):** Can be used only once before it expires.
      - **Time-Based One-time Password (TOTP):** Only last for a short time before it expires.
- **Certificate-Based Authentication**
  - **PIV/CAC/Smart Cards:** Cards that have embedded certificates and a photo ID for authorization. The US DoD uses CAC/PIV.
    - **Common Access Card (CAC):** Is for Department of Defense members.
    - **Personal Identity Verification (PIV):** Is for civilians working for the federal government.

- **Given a Scenario, Differentiate Common Account Management Practices.**
  - **Account Types**
    - **User Account:** An account that identifies an individual and grants them access to specific areas of the network or system.
    - **Shared and Generic:** Multiple individuals sign into a single account. No workplace should have these. Cannot distinguish the actions of the user.
    - **Guest Accounts:** An anonymous shared logon account.
    - **Service Accounts:** Performs specific maintenance actions. Account and server operators.
    - **Privileged Accounts:** Access is set to access rights, generally referred to as system or network administrative accounts.
      - **Least Privilege:** Rights and permission are set to bare minimum needed to complete work.
  - **Onboarding/Offboarding**

        - **Onboarding:** Helps new employees learn all of the facets of their new job.
        - **Offboarding:** Ensures exiting employees securely leave and without causing risk to the company.
    - **Permission Auditing and Review**
        - **Time-of-Day Restrictions:** Certain privileges are permitted or restricted based on the time of day.
        - **Recertification:** The action of regaining a certification due to the certification being expired.
        - **Standard Naming Conventions:** Allows for the easier identification of resource location and purpose. Reduces the amount of time needed for troubleshooting and training.
        - **Account Maintenance:** Making sure that accounts have the proper privileges, and unused accounts are deleted. Generally done through scripts to save time and money.
        - **Group-Based Access Control:** Every user in a group has the same privileges.
        - **Location-Based Policies:** Grants and denies access based on the user's location.
        - **Credential Management:** Stores, manages, and tracks user credentials.
        - **Group Policy:** Sets different privileges for entire groups.
        - **Password Policy:** A set of policies and procedures enforcing secure password practices.
            - **Password Complexity:** The enforcing of complex and difficult to guess passwords.
            - **Expiration:** The amount of time that passes before a password is required to be changed.
            - **Recovery:** The ability to find lost passwords or usernames if an employee forgets them.
            - **Disablement:** Disabling an account.
            - **Lockout:** Prevents login after a set of failed login attempts, for a set period of time.
            - **Password History:** Remembers past passwords and prevents the reuse of passwords.
            - **Password Reuse:** The ability to ever use the same password again.
            - **Password Length:** The minimum number of characters that can be used in a password.
            - **Password Age:** How long a user can have a password before they are forced to change it.

5.0 Cryptography and Public Key Infrastructure (PKI)

- **Compare and Contrast Basic Concepts of Cryptography.**
    - **Symmetric Algorithms:** A shared secret key used by the sender and receiver to encrypt and decrypt.
    - **Asymmetric Algorithms:** There is a *shared public key* and a *private secret key*. The public key encrypts and the private key decrypts. The private key is used to sign, and the public key is used to verify.
    - **Hashing:** An algorithm that creates a unique one-way encryption.
        - **Salt:** Adding random data to a function to make it more complicated.
        - **Initialization Vector (IV):** A random value used with an encryption key.
        - **Nonce:** A one-time, random value used for authentication.
    - **Weak or Deprecated Algorithms:** Weak due to vulnerabilities (WEP) or weak key length (DES uses 56-bits).
    - **Key Exchange:** Securely sending keys back and forth. *Out-of-Band* is where the key is sent over the phone, in person, or any other offline way. *In-Band* is where the key is encrypted and sent over the Internet.
    - **Digital Signatures:** Provides integrity and non-repudiation. Verifies that the original sender is actually the one who sent it.
    - **Diffusion:** Changing one character causes the plaintext to drastically change the ciphertext output.
    - **Confusion:** The cipher does not look anything like the plain text.
    - **Collision:** Two completely different pieces of data have the exact same hash.
    - **Steganography:** Hides messages or code inside of an image or another type of data. Impossible to decipher without the correct tools.
    - **Obfuscation:** Taking something and making it difficult for a human to understand. Not impossible to convert it back to the original form.
    - **Stream vs. Block Ciphers:** *Stream ciphers* convert plain text into cipher text by encrypting 1 byte at a time. *Block ciphers* convert the plain text into cipher text by encrypting larger blocks one by one.
    - **Key Strength:** Larger keys and more bits are signs of better encryption and stronger keys.
    - **Session Keys:** Symmetric keys provide a secure online connection. The server's public key is paired with a random key to produce a symmetric key. The server uses it to encrypt, while the user uses it to decrypt.

- **Ephemeral Key:** Session keys that only last temporarily and change frequently.
- **Data-in-Transit:** Data being transmitted over a network. Should be encrypted using TLS and IPSec.
- **Data-at-Rest:** Data in a storage device. Should be encrypted and backups should be performed.
- **Data-in-Use:** Data being ran through RAM or CPU. Almost always decrypted to make it easier to use.
- **Random/Pseudo-Random Number Generation:** Used to create random keys and salts. A computer is never truly random, so it relies on outside factors such as user input to create a more random number.
- **Key Stretching:** Hashing a password and hashing that value. Brute-force protection for weak passwords.
- **Perfect Forward Secrecy (PFS):** Generates a new key each session. Prevents a stolen private key from decrypting all previous and current connections. Protects past sessions against future compromises.
- **Security Through Obscurity:** Relying on secrecy to protect and secure data.
- **Common Use Cases**
  - **Low Power Devices:** Mobile phones and portable devices.
  - **Low Latency:** Short amount of time occurs between input and output.
  - **High Resiliency:** Larger key sizes and encryption algorithm quality.
  - **Confidentiality:** Secrecy and privacy.
  - **Integrity:** Prevents modification of data and validating contents with hashes.
  - **Obfuscation:** Makes plaintext more difficult to understand.
  - **Authentication:** Password hashing and protecting the original password.
  - **Non-Repudiation:** Digital signature provides authenticity, integrity, and non-repudiation.
  - **Resource vs. Security Constraints:** Limitations in providing strong cryptography due to the number of available resources (time and energy) vs the security provided by cryptography.

- **Explain Cryptography Algorithms and Their Basic Characteristics.**
  - **Symmetric Algorithms**
    - **Advanced Encryption Standard (AES):** A symmetric, block cipher with 128-bit blocks, key sizes of 128-bit, 192-bit and 256-bit. It is the U.S. government standard for the secure exchange of sensitive but unclassified data. It is also the standard used today with WPA2.
    - **Data Encryption Standard (DES):** A symmetric, block cipher with a 64-bit block size and a 56-bit key size. Susceptible to *brute force* attacks. Was commonly used until it was replaced by AES.
    - **3DES:** Symmetric. Very secure and an upgrade compared to its predecessor, DES. Three separate keys and three passes over data. Not used in modern day either.
    - **RC4:** Symmetric algorithm with key sizes of 40-bit to 2048-bit. Part of the original WEP standard with SSL. Deprecated from biased output.
    - **Blowfish:** Symmetric, block cipher with variable key-lengths from 1-bit to 448-bits and 64-bit block size. Fast and not limited by patents.
    - **Twofish:** Symmetric block cipher that uses a complex key structure up to 256-bits. Uses 128-bit blocks. Again, not limited by patents. Just as good as AES.
  - **Cipher Modes**
    - **Cipher Block Chaining (CBC):** Symmetric, uses IV for randomization. Encryption that is dependent on the block before it. Slow.
    - **Galois Counter Mode (GCM):** Provides data authenticity/integrity, hashes as well. Widely used.
    - **Electronic Code Book (ECB):** Simplest cipher mode. Not recommended.
    - **Counter Mode (CTR):** Converts block into stream, uses IV. Widely used.
  - **Asymmetric Algorithms**
    - **Rivest, Shamir, Adleman (RSA):** First practical use of public key cryptography. Uses large prime numbers as the basis for encryption.
    - **Digital Signature Algorithm (DSA):** Standard for *digital signatures*. Uses elliptic curves for ECDSA.
    - **Diffie-Hellman:** An asymmetric standard for exchanging keys. Primarily used to send private keys over public (unsecured) networks.
      - **Diffie-Hellman Ephemeral (DHE):** A Diffie-Hellman key exchange that uses different keys.

      - **Elliptic Curve Diffie-Hellman Ephemeral (ECDHE):** Key agreement protocol that allows two parties to establish a shared secret over an unsecure channel.
    - **Elliptic Curve Cryptography (ECC):** Asymmetric. Uses smaller key sizes and curve algorithms to secure data. Useful in portable devices because it uses less CPU power.
    - **Pretty Good Privacy (PGP):** Asymmetric. Used by many for E-mails and is used by IDEA algorithm.
    - **GNU Privacy Guard (GPG):** A free, open-source version of PGP that provides equivalent services.
  - **Hashing Algorithms:** Hashing provides integrity and authenticity.
    - **Message-Digest Algorithm v5 (MD5):** Hashing algorithm. 128-bit hash with strong security. A collision was found in 1996, so it is considered deprecated.
    - **Secure Hash Algorithm (SHA):** Hashing algorithm. One-way, 160-bit hash value with encryption protocol. Standard hash algorithm today.
    - **Hash-Based Message Authentication Code (HMAC):** Hashing algorithm that combines itself with a symmetric key. Provides data integrity and authenticity and is faster than asymmetric encryption.
    - **RACE Integrity Primitives Evaluation Message Digest (RIPEMD):** Hashing algorithm that is based on MD4. Collisions were found, so it now exists in versions with 160-bits, 256-bits, and 320-bits.
  - **Key Stretching Algorithms:** Lengthen keys to make brute-force attacks more difficult.
    - **Bcrypt:** Key Stretching that helps protect passwords by repeating the *Blowfish cipher*.
    - **PBKDF2:** *Password-Based Key Derivation Function 2.* Applies the RSA function to a password to create stronger key.
  - **Obfuscation:** Making something unclear to read. Can still reverse it.
    - **XOR:** *Exclusive OR*. Mathematical operation that's a part of all symmetric operations, done by comparing bits of plaintext and a key. Can be reversed to get plaintext back.
    - **ROT13:** *Rotate by 13.* Common substitution cipher that rotates each letter 13 places. *Substitution ciphers* change one symbol for another, like the **Caesar Cipher**. Easy to decrypt.

- **Given a Scenario, Install and Configure Wireless Security Settings.**
  - **Cryptographic Protocols**
    - **Wi-Fi Protected Access (WPA):** Uses RC4 with TKIP. Was replaced by WPA2.
    - **Wi-Fi Protected Access v2 (WPA2):** Uses CCMP for encryption.
      - **Temporal Key Integrity Protocol (TKIP):** Protocol that mixes a root key with an *Initialization Vector (IV),* a new key for each packet.
      - **Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP):** Based on 128-bit AES. More secure than TKIP. Was advanced for its time.
  - **Authentication Protocols**
    - **Extensible Authentication Protocol (EAP):** An authentication framework that provides general guidance for authentication methods.
    - **Protected Extensible Authentication Protocol (PEAP):** An extension of EAP that is sometimes used with 802.1x. A certificate is required on the 802.1x server.
    - **EAP Flexible Authentication with Secure Tunneling (EAP-FAST):** A Cisco-designed replacement for *Lightweight EAP (LEAP).* Supports certificates but are not required.
    - **EAP Transport Layer Security (EAP-TLS):** One of the most secure EAP standards. Widely implemented. It uses PKI. Certificates are required on the 802.1x server and on the clients.
    - **EAP Tunneled Transport Layer Security (EAP-TTLS):** Allows for systems to use older authentication methods, such as PAP, within a TLS tunnel. Certificate is required on the 802.1x server but not on the clients.
    - **IEEE 802.1x:** An authentication protocol used in VPNs, wired and wireless networks. In VPNs it is used as a RADIUS server. In wired networks, it is used as port-based authentication, and wireless networks use it in *Enterprise Mode.* Can be used with certificate-based authentication.
    - **RADIUS Federation:** Members of one organization can authenticate to the network of another network using their normal credentials.
  - **Configuration Methods**

        - **Open:** Does not apply any security.
        - **Pre-Shared Key (PSK):** Uses WPA2 encryption and a common key to access the network.
        - **Enterprise:** Users authenticate with a username and password and uses 802.1X to provide authentication. The server handles the distribution of keys and certificates.
        - **Wi-Fi Protected Setup (WPS):** Allows users to easily configure a wireless network, often by using only a PIN. Susceptible to *brute force attacks* because PINs are easily discovered.
        - **Captive Portals:** Forces clients using a web browser to complete a task before being able to access the network.

- **Given a Scenario, Implement Public Key Infrastructure.**
    - **Components of PKI**
        - **Certificate Authority (CA):** A trusted third-party that is responsible for issuing *digital certificates*.
        - **Certificate Signing Request (CSR):** A user request for a digital certificate.
        - **Intermediate CA:** An entity that processes CSRs and verifies user authenticity on behalf of the CA.
        - **Certificate Revocation List (CLR):** A list of certificates that are expired, or that have been revoked.
        - **Online Certificate Status Protocol (OSCP):** A request and response protocol that obtains the serial number of the certificate that is being validated and reviews revocation lists for the client.
        - **Certificate:** Digitally signed statement that associates a public key to the corresponding private key.
        - **Public Key:** A key that is provided by the sender and used by anyone to encrypt data.
        - **Private Key:** Key used to decrypt a message. Only used by the person opening the message.
        - **Object Identifiers (OID):** A serial number that authenticates a certificate.
    - **Certificate Concepts**
        - **Online CA:** Directly connected to a network. Most common.
        - **Offline CA:** Not directly connected to a network. Often used for root certificates for security.
        - **Trust Model:** A complex structure of systems, personnel, applications, protocols, technologies, and policies working together to provide protection.
        - **Key Escrow:** Private keys are kept by the users and a 3rd party as back-ups.
        - **OSCP Stapling:** Combining related items in order to reduce communication steps. The device that holds the certificate will also be the one to provide status of any revocation.
        - **Pinning:** The application has hard-coded the server's certificate into the application itself.
        - **Certificate Chaining:** Certificates are handled by a *chain of trust*. The *trust anchor* is the root CA.
    - **Certificate Types**
        - **Root:** Used for root authorities. They usually are self-signed.
        - **Self-Signed:** The root CA creates its own certificate.
        - **Machine/Computer:** Certificates that are assigned to a specific machine.
        - **E-mail:** Secures E-mails. Is used by S/MIME.
        - **User:** For authentication or to access resources.
        - **Domain Validation:** Provides a secure communication with a specific domain and provides TLS. This is the most common form of certificate.
        - **Code Signing:** Digitally signs written application code and makes sure that it adheres to policy restrictions and usage.
        - **SAN (Subject Alternative Name):** A certificate is valid for multiple domains using multiple names.
        - **Extended Validation:** More secure because they require stricter validation of the certificate holder.
        - **Wildcard:** A certificate that can be used with multiple subdomains of a given domain, by covering all subordinate certificates to the root.
    - **Certificate Formats**
        - **Distinguished Encoding Rules (DER):** Designed for X.509 certificates, they are used to extend binary encoded certificates. Cannot be edited by a plain text editor. Commonly used with Java.