COMPTIA 501 SECURITY PLUS+ CERTIFICATION STUDY GUIDE

1.0 THREATS, ATTACKS AND VULNERABILITIES

1.1 GIVEN A SCENARIO, ANALYZE INDICATORS OF COMPROMISE AND DETERMINE THE TYPE OF MALWARE.

A) Viruses: An unsolicited and unwanted malicious program.
B) Crypto-malware: A malicious program that encrypts programs and files on the computer in order to extort money from the user.
C) Ransomware: Denies access to a computer system or data until a ransom is paid. Can be spread through a phishing email or unknowingly infected website.
D) Worm: A self-contained infection that can spread itself through networks, emails, and messages.
E) Trojan: A form of malware that pretends to be a harmless application.
F) Rootkit: A backdoor program that allows full remote access to a system.
G) Keylogger: A malicious program that saves all of the keystrokes of the infected machine.
H) Adware: A program that produces ads and pop ups using your browser, may replace the original browser and produce fake ads to remove the adware in order to download more malware.
I) Spyware: Software that installs itself to spy on the infected machine, sends the stolen information over the internet back to the host machine.
J) Bots: AI that when inside an infected machine performs specific actions as a part of a larger entity known as a botnet.
K) RAT: A remote access Trojan.
L) Logic bomb: A malicious program that lies dormant until a specific date or event occurs.
M) Backdoor: Allows for full access to a system remotely.

1.2 COMPARE AND CONTRAST TYPES OF ATTACKS.

A) Social engineering: Gathering information on an attack by exploiting the weakest part of security, people.
    a. Phishing: Sending a false email pretending to be legitimate to steal valuable information from the user.
    b. Spear phishing: Attacks that target specific users.
    c. Whaling: An attack on a powerful or wealthy individual.
    d. Vishing: An attack through a phone or voice communications.
    e. Tailgating: Closely following individuals with keys to get access to secure areas.
    f. Impersonation: Taking on the identity of an individual to get access into the system or communications protocol.
    g. Dumpster diving: Going through a business's or person's trash to find thrown away valuable information or possessions.

h. Shoulder surfing: Watching as a person enters information.
i. Hoax: False information that deceives the user into compromising security by making them believe they are at risk.
j. Watering hole attack: A security attack that targets a specific highly secured group by infecting a commonly visited website by the group's members.
k. Principles (reasons for effectiveness):
    i. Authority: The actor acts as an individual of authority.
    ii. Intimidation: Frightening or threatening the victim.
    iii. Consensus: Influenced by what others do, everyone else does it.
    iv. Scarcity: Limited resources and time to act.
    v. Familiarity: The victim is well known.
    vi. Trust: Gain their confidence, be their friend.
    vii. Urgency: Limited time to act, rush the victim.

B) Application/service attacks:
a. DoS (Denial of Service): Flooding a target machine or resource with many requests to overload the system and prevent use of its resources.
b. DDoS (Distributed Denial of Service): Multiple different sources attack one victim.
c. Man-in-the-middle: The attacker alters the communication between two parties who believe they are directly communicating.
d. Buffer overflow: A program attempts to write more data than can be held in fixed block of memory.
e. Injection: Occurs from processing invalid data, inserts code into the vulnerable computer program and changes the course of execution.
f. Cross-site scripting (XXS): Found in web applications, allows for an attacker to inject client-side scripts in web pages.
g. 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.
h. Privilege escalation: An attack that exploits a vulnerability that allows them to gain access to resources that they normally would be restricted from accessing.
i. ARP poisoning: The act of falsifying the IP-to-MAC address resolution system employed by TCP/IP.
j. Amplification: The amount of traffic sent by the attacker is originally small but then is repeatability multiplied to place a massive strain on the victim's resources, in an attempt to cause it to fail or malfunction.
k. DNS poisoning: Is a type of attack that exploits vulnerabilities in the domain name system (DNS) to divert Internet traffic away from legitimate servers and towards fake ones.
l. Domain hijacking: The act of changing the registration of a domain name without the permission of the victim.
m. Man-in-the-browser: A proxy Trojan horse that infects web browsers and capture browser session data
n. Zero day: The aim is to exploit flaws or vulnerabilities in targeted systems that are unknown or undisclosed to the world in general. Meaning that there is no direct or specific defense to the attack; which puts most systems vulnerable assets at risk.
o. Replay: Is a network-based attack where a valid data transmission is rebroadcasted, repeated, or delayed.

p. Pass the hash: An authentication attack that captures and uses the hash of a password. The attacker then attempts to log on as the user with the stolen hash. This type of attack is commonly associated with the Microsoft NTLM (New Technology LAN Manager) protocol.
q. Hijacking and related attacks:
    i. 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.
    ii. Session hijacking: An attack in which an attacker attempts to impersonate the user by using their legitimate session token.
    iii. URL hijacking: Redirects the user to a false website based on misspelling the URL, is also referred to typosquatting.
    iv. Typosquatting: An alternate name for URL hijacking.
r. Driver manipulation:
    i. Shimming: The process of injecting alternate or compensation code into a system in order to alter its operations without changing the original or existing code.
    ii. Refactoring: Rewrites the internal processing of code without changing its behavior.
s. MAC spoofing: The attacker falsifies the MAC address of a device.
t. IP spoofing: An intruder uses another site's IP address to masquerade as a legitimate site.

C) Wireless attacks:
a. 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.
b. IV (Initialization Vector): A random number used to increase security by reducing predictability and repeatability.
c. Evil twin: Has same SSID (Service Set Identifier) as a proper access point (AP). Once a user connects to it, all wireless traffic goes through it instead of the real AP.
d. Rogue AP (Access Point): An unauthorized WAP (Wireless Access Point) or Wireless Router that allows for attackers to bypass many of the network security configurations and opens the network and its users to attacks.
e. Jamming: Disabling a wireless frequency with noise to block the wireless traffic.
f. WPS (WiFi Protected Setup): Allows users to easily configure a wireless network, sometimes by using only a PIN. The PIN can be found through a brute force attack.
g. Bluejacking: Sending unauthorized messages to a Bluetooth device.
h. Bluesnarfing: Gaining unauthorized access to, or stealing information from a Bluetooth device
i. RFID (Radio Frequency Identifier): 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.
j. NFC (Near Field Communication): A wireless technology that allows for smartphones and other devices to establish communication over a short distance.
k. Disassociation: Removes clients from a wireless network.

D) Cryptographic attacks
a. Birthday: Used to find collisions in hashes and allows the attacker to be able to create the same hash as the user. Exploits that if the same mathematical function is performed on two values and the result is the same, then the original values are the same.
b. Known plain text/cipher text:
    i. Plain text: The attacker has both the plaintext and its encrypted version.
    ii. Cipher text: The attacker has access only to the encrypted messages.
c. Rainbow tables: Large pregenerated data sets of encrypted passwords used in password attacks.

d. Dictionary: A password attack that 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.
e. Brute force: A password-cracking program that tries every possible combination of characters through A to Z.
f. Online vs. offline:
    i. Online: Is against a live logon prompt.
    ii. Offline: The attack is working on their own independent computers to compromise a password hash.
g. Collision: When two different inputs produce the same hash value.
h. Downgrade: Forces a system to lessen its security, this allows for the attacker to exploit the lesser security control. It is most often associated with cryptographic attacks due to weak implementations of cipher suites. Example is TLS > SSL, a man-in-the-middle POODLE attack exploiting TLS v1.0 - CBC mode.
i. Replay: The attacker captures network packets and then retransmits them back onto the network to gain unauthorized access.
j. Weak implementations: The main cause of failures in modern cryptography systems are because of poor or weak implementations instead of a failure caused by the algorithm itself.

1.3 EXPLAIN THREAT ACTOR TYPES AND ATTRIBUTES.

A) Script kiddies: A person who uses pre-existing code and scripts to hack into machines, because they lack the expertise to write their own.
B) Hacktivist: An individual who is someone who misuses computer systems for a socially or politically motivated agenda. They have roots in the hacker culture and ethics. Hacker on a mission.
C) Organized crime: These are professionals motivated ultimately by profit. They have enough money to buy the best gear and tech. Multiple people perform specific roles: gathering data, managing exploits, and one who actually writes the code.
D) Nation states/APT: An APT is an advanced persistent threat, these are massive 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 or large security sites, they also frequently attack power plants.
E) Insiders: Someone who is inside the company 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.
F) Competitors: Rival companies, can bring down your network or steal information through espionage.
G) Internal/external: Internal is inside the company, can be intentional, unintentional, or an act of God. External is someone outside the company trying to get in.
H) Level of sophistication: Is the skill of the hacker and the complexity of the attack.
I) Resources/funding: The amount of money and the value of the tech and gear being used.
J) Intent/motivation: The reason for the attack, can be for political, monetary, or social reasons.
K) Use of open-source intelligence (OSINT): Data that is collected through publicly available information. This can be used to help make decisions. Can be used by threat actors to help find their next target or how to best attack their target. OSINT is also incredibly helpful for mitigating risks and for identifying new threat actors.

1.4 EXPLAIN PENETRATION TESTING CONCEPTS.

A) Active reconnaissance: Is the use of tools to send data to systems and then understanding their responses. Usually starts with various network and vulnerability scanners. Can be incredibly illegal and should not be engaged without being prepared and proper authorization.
B) Passive reconnaissance: You are not touching any of the target's equipment. Instead you are going through and gathering that is already available. Forums and social media are great sources for gathering information about the company and its employees.
C) Pivot: In penetration testing it is using a compromised machine to attack other machines on the same network. Attacking and gaining access to an area of lower security in order to be more likely to have a successful attack on an area of greater security. Is also referred to as island hopping.
D) Initial exploitation: Usually the hardest part. A vulnerability is taken advantage of to get into the network or system.
E) Persistence: Installing backdoors or methods to keep access to the host or networks.
F) Escalation of privilege: Allows for a user to get a higher-level access than what authentication allows for. Can be resolved through patching and updating. Typically related to a bug or vulnerability
G) Black box: You know nothing of the network, you have no prior knowledge.
H) White box: You are given a network map and you have full knowledge of the configurations allowing you to perform specific tests.
I) Gray box: Knowledge of the network but not incredibly detailed.
J) Penetration testing vs. vulnerability scanning: Penetration testing is an active attack on the network to exploit vulnerabilities, can assess potential damages and the potential of the exploits being found. Is done by a human. Vulnerability scans passively scans and identifies vulnerabilities. Is automated.

1.5 EXPLAIN VULNERABILITY SCANNING CONCEPTS.

A) Passively test security controls: Uses an automated vulnerability scanner. Observes and reports findings. Does not take down systems, applications, or services, and doesn't disrupt business.
B) Identify vulnerability: Understanding common attacks and taking inventory of vulnerabilities. Scanners can report: missing updates, misconfigured security settings, and known exploits.
C) Identify lack of security controls: Vulnerability scanners can identify missing patches or antivirus.
D) Identify common misconfigurations: Weak passwords, default usernames and passwords, and open ports.
E) Intrusive vs. non-intrusive: Intrusive testing can interrupt service, is much more detailed, and exploits vulnerabilities. Non-intrusive is more passive, does not exploit vulnerabilities, and does not disrupt service.
F) Credentialed vs. non-credentialed: Credentialed are done as though it is inside the network, 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.
G) False positive: A result which shows incorrectly that a condition or attribute is present. A false vulnerability.

1.6 EXPLAIN THE IMPACT ASSOCIATED WITH TYPES OF VULNERABILITIES

A) Race conditions: The behavior of a software, electronic, or another system's output is dependent on the timing, sequence of events, or a factor out of the user's control.
B) Vulnerabilities due to:
    a. End-of-life systems: No longer receives updates, and at a high risk to compromise.
    b. Embedded systems: Programs added for automation and/or monitoring. Can allow for malicious programs to gain access through the added programs.
    c. Lack of vendor support: Vendor does not support the product: does not update, improve, or protect the product.
C) Improper input handling: The system does not properly validate data, allows for an attacker to create an input that is not expected. Allows for parts of the system vulnerable to unintended data.
D) Improper error handling: The error messages display sensitive or private information that give the user too much data.
E) Misconfiguration/weak configuration:
F) Default configuration: Uses the unsecure out-of-box settings.
G) Resource exhaustion: A denial of service occurs, the amount of resources to execute an action are expended, making it unable for the action to be performed.
H) Untrained users: Users are not properly informed on how to use the systems. This means that mistakes will more likely occur and that the system's resources may be abused.
I) Improperly configured accounts: Users should only be allowed to access the parts that they need to complete their work.
J) Vulnerable business processes: All tasks, procedures, and functions should be properly assessed and the most valuable and vulnerable should be heavily protected.
K) Weak cipher suites and implementations: Use of older and less robust cryptographic algorithms. EX. DES, WEP
L) Memory/buffer vulnerability:
    a. Memory leak: Leaves the system unresponsive.
    b. Integer overflow: Large integer exceeds data storage capacity.
    c. Buffer overflow: Too much data for the computer's memory to buffer.
    d. Pointer dereference: Failed deference can cause memory corruption and the application to crash.
    e. DLL injection: Allows for the running of outside code.
M) System sprawl/undocumented assets: Lack of internal inventory and allowing unsecure devices and systems to connect to the network.
N) Architecture/design weaknesses: An insecure and poorly designed network. Ex. Not segmenting the systems or internal network.
O) New threats/zero day: A zero-day threat, is a flaw that is unknown to the teams patching and fixing flaws.
P) Improper certificate and key management: Allowing for unauthorized access to certificates and keys, which allows for sensitive data to be decrypted. And allowing for certificates to expire.

2.0 TECHNOLOGIES AND TOOLS INSTALL AND CONFIGURE NETWORK COMPONENTS,

2.1 HARDWARE AND SOFTWARE-BASED, TO SUPPORT ORGANIZATIONAL SECURITY.

A) Firewall: A network security system that monitors and controls incoming and outgoing network traffic based on predetermined security rules.
   a. ACL (Access control lists): A list of rules that can be used to control traffic based on networks, subnets, IP addresses, ports, and some protocols.
   b. Application-based vs. network-based:
      i. Application-based: Protects the user from applications and services by monitoring and potentially blocking the input, output, or system service calls that do not meet the configured policy of the firewall.
      ii. Network-based: Filtering traffic based on firewall rules and allows only authorized traffic to pass in and out of the network
   c. Stateful vs. stateless:
      i. Stateful: Stateful firewalls 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.
      ii. Stateless: Stateless firewalls uses rules within an ACL to identify allowed and/or block traffic through packet filtering.
   d. Implicit deny: The last rule in an ACL that indicates that, "all traffic that isn't explicitly allowed is implicitly denied".

B) VPN concentrator: A type of router device that allows for the secure creation of VPN connections and for the safe delivery of messages between VPN nodes. Allows for the handling of a large quantity of VPN tunnels.
   a. Remote access vs. site-to-site:
      i. Remote access: A user-to-LAN connection used by remote users.
      ii. Site-to-site: Allows multiple sites to connect to remote sites over the internet.
   b. 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.
   c. Tunnel mode: The default mode for IPSec, the entire pack is protected.
   d. Transport mode: Used for end-to-end communications in IPSec. Ex. encrypted Telnet or Remote Desktop session from a workstation to a server.
   e. Authentication Header (AH): IPsec protocol that authenticates that the packets received were sent from the source identified in the header.
   f. ESP (Encapsulating Security Payload): IPSec component that provides the same services as AH and also ensures confidentiality when sending data.
   g. Split tunnel vs. full tunnel:
      i. Split tunnel: Only some traffic over the secure VPN while the rest of the traffic directly accesses the internet.
      ii. Full tunnel: All of the traffic is sent over the secure VPN.
   h. TLS: The replacement of SSL to encrypt data-in-transit. Uses certificates issued by CAs.
   i. Always-on VPN: The user does not connect and disconnect and instead is always connected.

C) NIPS (Network Intrusion Prevention System)/NIDS (Network Intrusion Detection System):

a. Signature-based: Detects attacks based on known attack patterns documented as attack signatures.
b. Heuristic/behavioral: It detects attacks by comparing traffic against a baseline to find any anomalies.
c. Anomaly: Abnormal packets or traffic.
d. Inline vs. passive:
    i. Inline: Connected directly to the network and monitors the flow of data as it occurs.
    ii. Passive: Connected through a switch or port on the network and receives a copy of the flow of data as it occurs.
e. In-band vs. out-of-band:
    i. In-band: Sits in the network, can quickly warn of or prevent malicious traffic.
    ii. Out-of-band: Out the can only warn of malicious traffic.
f. Rules: Standards set to differentiate good traffic from suspicious traffic.
g. Analytics: Shows the amount, type and history of traffic coming through.
h. False positive: NIPS blocks legitimate incoming traffic.
i. False negative: NIPS allows harmful incoming traffic.

D) Router: A device that directs data traffic along specific routes.
a. ACLs (Access Control List): A list of permit or deny rules detailing what can or can't enter or leave the interface.
b. Anti Spoofing: A device with the intent of excluding packets that have invalid source addresses.

E) Switch: A networking device that connects devices together on a computer network
a. Port security: Requires a username and a password and authenticate before gaining access to any of the switch interfaces.
b. Layer 2 vs. Layer 3:
    i. Layer 2: Packets are sent to a specific switch port based on destination MAC addresses.
    ii. Layer 3: Packets are sent to a specific next-hop IP address, based on destination IP address.
c. 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.
d. Flood guard: Configuration that sets the maximum number of MAC addresses that could possibly be seen on any particular interface.

F) Proxy: Acts as an intermediary for requests from clients seeking resources from servers that provide those resources.
a. Forward and reverse proxy:
    i. Forward proxy: Forwards requests from internal clients to external servers.
    ii. Reverse proxy: Takes in requests from the Internet and forwards them to an internal web server.
b. Transparent: Accepts and forwards requests without performing any modifications on them.
c. Application/multipurpose: A type of proxy server that knows the application protocols that it supports.

G) Load balancer: 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.
a. Scheduling: Sends requests to servers using set rules.
b. Affinity: Sends client requests to the same server based on the client's IP address.
c. Round-robin: Sends requests in a predefined order.

d. Active-passive: Some servers are not active and only go active to take excess traffic or if an active server fails.
e. Active-active: All servers are actively processing requests
f. Virtual IPs: An IP address and a specific port number that can be used to reference different physical servers. Provides IP addresses that can float between two or more physical network nodes and provide redundancy.

H) Access point:
   a. SSID: Name of a wireless network.
   b. MAC filtering: A method of controlling access on a wired or wireless network by denying unapproved MAC address access to a device.
   c. Signal strength: The quality and distance of a signal.
   d. Band selection/width: Can be set between 2.4 GHz and 5 GHz depending on which 802.11 protocol is being used.
   e. Antenna types and placement:
   f. Fat vs. thin:
      i. Fat: Has everything necessary to handle wireless clients. If end-user deploys several Fat Wireless Access Points, each one needs to be configured individually.
      ii. Thin: Acts as a radio and antenna that is controlled by a wireless switch. If multiple thin wireless access points are deployed, the entire configuration takes place at the switch. This is the far cheaper option.
   g. Controller-based vs. standalone:
      i. Controller-based: Require a controller for centralized management and are not manually configured.
      ii. Standalone: Do not require a controller and are generally used in smaller environments.

I) SIEM (Security Information and Event Management):
   a. Aggregation: The gathering of log and event data from the different network security devices used on the network.
   b. Correlation: Relating various events to identifiable patterns. If those patterns threaten security, then action must be taken.
   c. Automated alerting and triggers: Sends messages based on configured rules based on events that occur within the log files.
   d. Time synchronization: Ensures that the time is the same across devices so that all security events are recorded at the same time using Network Time Protocol.
   e. Event deduplication: Trimming event logging so that the same event is not recorded over and over again, overflowing log space.
   f. Logs/WORM: Prevents alteration of logs and archives the source logs with write protection.

J) DLP (Data Loss Prevention): Policies and technologies that protect data loss through theft or destruction.
   a. USB blocking: Prevents the use of USBs
   b. Cloud-based: Prevents sensitive data from being stored on the cloud without proper encryptions and authorization.
   c. Email: Protects against email fraud and from valuable data from being sent through email.

K) NAC (Network Access Control): Enforces security policies on devices that access networks to increase network visibility and reduce risk.
   a. Dissolvable vs. permanent:
      i. Dissolvable: Disappears after reporting information to the NAC device.
      ii. Permanent: Resides on end devices until uninstalled.

b. Host health checks: Reports sent by network access control to gather information on installed devices.
c. Agent vs. agentless:
    i. Agent: Is installed on the end device.
    ii. Agentless: Is not installed on the device itself but instead is embedded within a Microsoft Windows Active Directory domain controller.

L) Mail gateway: Examines and processes all incoming and outgoing email.
    a. Spam filter: An on-premises software solution for filtering, well spam emails.
    b. DLP (Data Loss Prevention): Prevents certain information leaving the organization via email.
    c. Encryption: Encrypt and decrypts emails being sent and received across networks.
M) Bridge: Provides interconnection with other bridge networks using the same protocol.
N) SSL/TLS accelerators: The process of offloading processor-intensive public-key encryption for TLS or its SSL to a hardware accelerator.
O) SSL decryptors: Allows for the user to view inside of passing Secure HTTP traffic.
P) Media gateway: Converts media streams between disparate telecommunications technologies.
Q) Hardware security module: Safeguards and manages digital keys for strong authentication and provides cryptoprocessing.

2.2 GIVEN A SCENARIO, USE APPROPRIATE SOFTWARE TOOLS TO ASSESS THE SECURITY POSTURE OF AN ORGANIZATION.

A) Protocol analyzer: Hardware or software that captures packets to decode and analyze their contents. Allows for you to easily view traffic patterns, identify unknown traffic, and verify packet filtering and security controls.
    a. Big data analytics: Allows for the user to store large amounts of data and then easily go through it.
B) Network scanners: A computer program used for scanning networks to obtain user names, host names, groups, shares, and services.
    a. Rogue system detection: Find devices that are not supposed to be on the network, such as rogue AP's.
    b. Network mapping: Identifying all devices on a network along with a list of ports on those devices.
C) Wireless scanners/cracker:
    a. Wireless scanners: Is for wireless monitoring, it scans wireless frequency bands in order to help discover rogue APs and crack passwords used by wireless APs.
    b. Wireless cracker: Uses wireless attacks to test if an attacker could find the passwords to gain access to parts of your network.
        i. • WEP - Cryptographic vulnerabilities, is relatively straightforward.
        ii. • WPA1 PSK and WPA2 PSK, uses dictionary brute force and rainbow tables attacks.
D) Password cracker: A program that uses the file of hashed passwords, such as a rainbow table, and then attempts to break the hashed passwords of the network. Getting the hashes is the hardest part.
E) Vulnerability scanner: Attempts to identify vulnerabilities, misconfigured systems, and the lack of security controls such as up-to-date patches. They can be passive or active, either way they have little impact on a system during the test.

F) Configuration compliance scanner: A vulnerability scanner that verifies systems are configured correctly and meet the minimum-security configurations, it typically 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 logon process.
G) Exploitation frameworks: An already created set of exploits that already have all the major components designed, the user just needs to figure out how to inject them into the network. These toolsets can be used offensively by hackers or defensively by pen testers.
H) 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.
I) Steganography tools: Allows for the user to embed data into an image, video, sound files, or packets. It is security through obscurity.
J) Honeypot: Decoy systems or networks to gather information on the attacker.
K) Backup utilities: Important to protect data from being lost, downtime, or corrupted.
L) Banner grabbing: The process of capturing the initial message (the banner) from a network service. Often the banner discloses the application's identity, version information, and other sensitive information.
M) Passive vs. active:
    a. Passive: You are observing.
    b. Active: You are interacting with the network by sending traffic and trying to access parts of the network.
N) Command line tools:
    a. ping: The name is based on the sound made by sonar. Tests reachability, it is a primary troubleshooting tool.
    b. netstat (Network statistics):
        i. netstat -a: Show all active connections.
        ii. netstat -b: Show binaries, for Windows.
        iii. netstat -n: Does not resolve names.
    c. tracert (Windows)/traceroute (MacOS/Linux): Uses the ICMP (Internet Control Message Protocol) time to live (TTL) error message to map the path of a packet. Time in TTL is measured in hops, TTL = 1 for the first router, and 2 refers to the second router.
    d. nslookup/dig (Domain Information Groper):
        i. nslookup: Used to gather information from DNS servers, lookups names and IP addresses. Was replaced by dig.
        ii. dig (Domain Information Groper): More advanced than nslookup and shows more detailed domain information. Is for Linux but can be downloaded for windows.
    e. arp (Address Resolution Protocol): Used to view MAC addresses.
        i. Arp -a: Views the local arp table.
    f. ipconfig/ip/ifconfig:
        i. ipconfig: Shows the Windows TCP/IP configuration.
        ii. ip: Used to replace ifconfig on Linux. Shows and manipulates settings on the network interface card (NIC).
        iii. ifconfig: Shows the Linux interface configuration.
    g. tcpdump: A command-line packet analyzer that allows to capture packets from the command line.
    h. nmap: It is designed to scan a network and create a map, this is useful as a vulnerability scanner because it can find open ports and unsecured access points.
    i. netcat: Is used to safely connect to remote systems using command line instead of a front-end application. Can also be used for banner grabbing.

2.3 GIVEN A SCENARIO, TROUBLESHOOT COMMON SECURITY ISSUES.

A) Unencrypted credentials/clear text: All authentication must be encrypted. Unencrypted credentials can allow for the attacker to: elevate privileges, establish a foothold, maintain persistence, and move to other networks.
B) Logs and events 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 fixed.
C) Permission issues: Determine how much access a specific user needs to be able to complete their job. Confirm permissions on initial configurations, perform periodic audits, and provide a process for changes and updates.
D) Access violations: Segmentation fault, OS locks you out, or prevents access to restricted memory. A user is able to properly logon and then access systems they don't have proper authorization for.
E) Certificate issues: Certificates should be signed by someone trusted, be up to date, and be properly checked.
F) Data exfiltration: Data is your most important asset to and attackers.
G) Misconfigured devices:
    a. Firewall: Provide too much access, and to audit when using a large rule base,
    b. Content filter: URLs are not specific, and some protocols are not filtered.
    c. Access points: No encryption mechanisms and Open configurations from the wireless side.
H) Weak security configurations: Make sure to regularly upgrade equipment and update firmware. Using hash algorithms that are susceptible to collisions.
I) Personnel issues: The weakest link
    a. Policy violation: Transferring private data or visiting unsafe websites.
    b. Insider threat: Authenticated users have free reign. Assign correct user rights and permissions.
    c. Social engineering: Deceit can cause employees to give up personal or valuable data.
    d. Social media: Sharing private data or personal information.
    e. Personal email: Uses company resources and leaves the network vulnerable.
J) Unauthorized software: Don't know what it is: could conflict with company software, could be malware, or could be useful for work.
K) Baseline deviation: Everything is well documented, any changes to the norm should be noted, and no remote access until it matches the baseline.
L) License compliance violation (availability/integrity): Make sure licenses are up to date and valid.
M) Asset management: Identify and track assets to respond faster to security risks. Keep detailed records of the most valuable assets. Usually automated.
N) Authentication issues: The more factors the safer, makes sure the user is actually the correct person.

2.4 GIVEN A SCENARIO, ANALYZE AND INTERPRET OUTPUT FROM SECURITY TECHNOLOGIES.

A) HIDS/HIPS:
    a. HIDS (Host-based intrusion detection system): Runs on a single computer and alerts of potential threats to help warn of attacks against that host.
    b. HIPS (Host-based intrusion prevention system: Runs on a single computer and intercepts potential threats to help prevent attacks against that host.
B) Antivirus: Software that is specifically designed to detect viruses and protect a computer and files from harm.
C) File integrity check: An application that can verify that the files have not been modified using hash algorithms to authenticate the file.

D) Host-based firewall: A firewall that is on a single host that only restricts incoming and outgoing network activity for that host.
E) Application whitelisting: The practice of allowing only approved programs to run on a computer, computer network, or mobile device.
F) 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.
G) Advanced malware tools: Block malware from running by blocking file signature, heuristics/Anomalous behavior, sandboxing, virtualizing. Need to be routinely updated with the latest definitions to be secure and protect against current threats.
H) Patch management tools: Tools that aid in the: monitoring, evaluating, testing, and installing of the most current software patches and updates.
I) UTM (Unified Threat Management): A group of security controls combined in a single solution that can inspect data streams for malicious content and block it.
J) DLP (Data Loss Prevention): Systems that identify, monitor, and protect data: from unauthorized use, transfers, modification, or destruction.
K) 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.
L) Web application firewall: A firewall that looks monitors and filters packets carrying HTTP traffic using a set of communication rules.

2.5 GIVEN A SCENARIO, DEPLOY MOBILE DEVICES SECURELY.

A) Connection methods
    a. Cellular: Network used for mobile phones.
        i. Potential Risks: Cellular devices are susceptible to traffic monitoring, location tracking, and gain access to the device from anywhere in the world.
    b. WiFi: A local area network that uses high frequency radio signals to transmit and receive data over distances of a few hundred feet.
        i. Potential Risks: If the Wi-Fi connection is not encrypted it is vulnerable to eavesdropping. Jamming frequencies or interferences can cause a denial of service.
    c. SATCOM: Satellite Communications that is used for communications in remote areas and during natural disasters.
        i. Potential Risks: SATCOM devices are at risk of leaking geopositioning data and remote code execution, and are not easily updated remotely.
    d. Bluetooth: Allows electronic devices like cell phones and computers to exchange data over short distances using radio waves.
    e. NFC (Near Field Communication): Enable two electronic devices in short proximity to each other. Typically used as a payment system, but can also be used as an identity token and to help pair Bluetooth devices.
        i. 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. Can be vulnerable to relay and replay attacks.
    f. ANT: A wireless sensor protocol that uses a 2.4 GHz ISM (industrial, scientific, and medical) band to communicate. Used in heart monitors, sports and fitness sensors.
        i. Potential Risks: At risk of jamming band, and eavesdropping because encryption is vulnerable.

g. Infrared: Electromagnetic waves of frequencies lower than the red of visible light. Used to control entertainment devices and other IR devices.
h. USB (Universal Serial Bus): 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.
    i. Potential Risks: Mobile devices can appear as storage devices allowing for the exfiltration and theft of data.

B) Mobile device management concepts:
a. Application management: Limiting which applications can be installed on a device.
b. Content management: Limiting access to content hosted on company systems, and controlling access to company data stored on mobile devices.
c. Remote wipe: Allows for the deletion of all data and possibly even configuration settings from a device remotely.
d. Geofencing: Using GPS to define geographical boundaries where the app can be used.
e. Geolocation: The location of a device identified by GPS.
f. Screen locks: Prevents someone from being able to pick up and use a mobile device.
g. Push notification services: Using SMS texts to send messages to selected users or groups.
h. Passwords and pins: Keep the device safe with something you know.
i. Biometrics: Keep the device safe with something you are.
j. Context-aware authentication: Uses multiple elements to authenticate a user and a mobile device.
k. Containerization: isolating and protecting the application, including any data used by the application.
l. Storage segmentation: Separates the information on a device into partitions.
m. Full device encryption: Protects against loss of confidentiality

C) Enforcement and monitoring for:
a. Third-party app stores: Anything that isn't from the Apple's App Store or Google Play. More likely to be a risk to security.
b. Rooting/jailbreaking:
    i. Rooting: Android, the process of modifying the device to gain root-level (full administrator) access.
    ii. Jailbreaking: Apple, the process removing all software restrictions from the device.
c. Sideloading: The process of copying an application package to a mobile device.
d. Custom firmware: The removal of the pre-installed firmware and replacing it. This may remove bloatware included by the vendor or telco, add or remove features, and streamline the OS to optimize performance.
e. Carrier unlocking: Means the device can be used by any carrier. Most cellular devices only work with specific carriers.
f. Firmware OTA updates: The downloading of: upgrades, patches, and improvements to the existing firmware.
g. Camera use: A cable used to connect mobile devices to other devices.
h. SMS/MMS: Sending alerts through text messages.
i. External media: Disable it to prevent the transferring of files through physical ports.
j. USB OTG (Universal Serial Bus On-The-Go):
k. 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.

l. Recording microphone: Disable it to prevent people from being able to listen in on conversations.
m. GPS tagging: Adding GPS information to the video, photo giving its location
n. WiFi direct/ad hoc: Means for wireless devices to connect directly to each other without a wireless access point.
o. Tethering: The process of sharing an Internet connection from one mobile device to another.
p. Payment methods:

D) Deployment models:
   a. BYOD (Bring Your Own Device): Employees to connect their own personal devices to the corporate network to work.
   b. COPE (Corporate Owned, Personally Enabled): Are owned by the organization, but can be used personally by employees.
   c. CYOD (Choose Your Own Device): Employees can purchase devices on the list and bring them to work. The company then supports, monitors, and manages the device.
   d. Corporate-owned: Company owns and controls all aspects, no personal info at all, most secure for company.
   e. VDI (Virtual Desktop Infrastructure): A virtual desktop that is created so users can access their desktop from a mobile device.

2.6 GIVEN A SCENARIO, IMPLEMENT SECURE PROTOCOLS.

A) Protocols:
   a. DNS (Domain Name Service): Does not have any security in its original design. The hierarchical and decentralized naming system for computers, services, or other resources connected to a private network or the internet.
   b. DNSSEC (Domain Name Service Security Extensions): Primary purpose is to provide a reliable authorization service between devices when performing operations on the DNS. Must be digitally signed.
   c. SSH (Secure Shell): Replaces Telnet. TCP (Transmission Control Protocol) over Port 22. Allows for a securely encrypted terminal connection.
   d. S/MIME (Secure/Multipurpose Internet Mail Extensions): Digitally signed email content using public key encryption.
   e. SRTP (Secure Real-time Transport Protocol): Protected and encrypted voice communications.
   f. LDAPS (Lightweight Directory Access Protocol Secure): TCP ports 389 and 636. Protocol used for reading and writing directories over an IP network. Uses the X.500 specifications written by the International Telecommunications Union (ITU) over SSL/TLS.
   g. FTPS (File Transfer Protocol Secure): TCP Ports 989/990. File transfer using SSL/TLS.
   h. SFTP (Secure File Transfer Protocol): TCP Port 22. FTP over an SSH channel.
   i. SNMPv3 (Simple Network Management Protocol Version 3): Ports 161/162. Encrypted statistics gathering from a router.
   j. SSL (Secure Sockets Layer)/TLS (Transport Layer Security):
      i. SSL (Secure Sockets Layer): Encryption technology developed for web and email over the transport layer. Uses public keys to exchange symmetric keys.
      ii. TLS (Transport Layer Security): The replacement for SSL, is sometimes called SSL still. Used to encrypt the communication of servers in an organization.
   k. HTTPS (Hypertext Transfer Protocol Secure): TCP port 443. HTTP over SSL/TLS provides a secure connection between the server and web browser.

l. Secure POP (Post Office Protocol)/IMAP (Internet Message Access Protocol):
    i. Secure POP (Post Office Protocol): Sends from port 110 to 995. Encrypted email communications used for retrieving email from a mail server over SSL/TLS.
    ii. Secure IMAP (Internet Message Access Protocol): Sends from port 143 to 993. Is standard email protocol for storing email messages on a mail server over SSL/TLS.

B) Use cases:
    a. Voice and video: SRTP.
    b. Time synchronization: NTPsec.
        i. NTPsec (Secure network time protocol): Used to securely sync all the devices' clocks on the network.
    c. Email and web: S/MIME and HTTPS.
    d. File transfer: FTPS or SFTP.
    e. Directory services: LDAPS or SASL.
        i. SASL (Simple Authentication and Security Layer): Provides a source of additional authentication using many different methods, such as Kerberos or client certificates.
    f. Remote access: SSH.
    g. Domain name resolution: DNSSec.
    h. Routing and switching: SNMPv3, SSH, or HTTPS.
        i. SNMPv3: Provides continentality, integrity, and authentication.
        ii. HTTPS: Allows for browser-based management.
    i. Network address allocation: DHCP, there is no secure version it.
        i. DHCP starvation attack: Using spoofed MAC addresses to exhaust the amount of DHCP's pool. Can configure a switch to limit the number of MAC addresses on an interface.
    j. Subscription services: Anti-viruses and anti-malware are subscription based. Must check regularly for updates. Set up integrity checks to verify the updates are coming from the correct source.

3.0 ARCHITECTURE AND DESIGN

3.1 EXPLAIN USE CASES AND PURPOSE FOR FRAMEWORKS, BEST PRACTICES AND SECURE CONFIGURATION GUIDES.

A) Industry-standard frameworks and reference architectures:
   a. Framework: Is a collection of standardized policies, procedures and guides, meant to direct a: user, firm, or any organization.
   b. Regulatory: Is a framework that is based on mandated laws and regulations. HIPAA is an example of this.
   c. Non-regulatory: The common standards and best practices that the organization follows.
   d. National vs. international:
      i. National: Framework based on the laws of a single country.
      ii. International: Framework based on the laws of multiple countries.
   e. Industry-specific frameworks: Frameworks based on the standards and regulations of a certain industry.

B) 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.
   a. Platform/vendor-specific guides: Hardening guides that are specific to the software or platform, also you can get feedback from the manufacturer or internet interest groups. System default configurations are unsecured and at high risk for exploits.
   b. Web server: Web application firewall (WAF), DMZ, Reverse Proxy for incoming communication from the internet to the server.
   c. Operating system: Implement a change management policy.
   d. Application server: Securing an application server means using industry standard guides, vendor specific, locking down the server to only the ports it needs for its specific role.
   e. Network infrastructure devices: Use national vs international guides, regulatory/non-regulatory and general purpose guides for securing.
   f. General purpose guides: Security configuration guides that are generic in scope.

C) Defense-in-depth/layered security:
   a. Vendor diversity: The practice of implementing security controls from different vendors to increase security. Reduces the impact of company specific vulnerabilities.
   b. Control diversity: The use of technical controls, administrative controls, and physical controls to harden security.
   c. Administrative: Mandated standards set by organizational policies or other guidelines.
   d. Technical: Technologies that reduce vulnerabilities, examples of this are: encryption, antivirus software, IDSs/IPS, and firewalls.
   e. User training: Providing regular training to users on common threats, emerging threats, and social engineering in to raise awareness and help avoid attacks.

3.2 GIVEN A SCENARIO, IMPLEMENT SECURE NETWORK ARCHITECTURE CONCEPTS.

A) Zones/topologies:
   a. DMZ: Demilitarized Zone, additional layer of protection to protect one from the internet.
   b. Extranet: Private network that can only be accessed by authorized individuals. Links a company with its suppliers and customers.

c. Intranet: Network that exclusively for the use of the members of the organization, cannot be accessed by anyone outside the organization.
d. Wireless: Generally, requires a login, an example is an internal wireless network at work.
e. Guest: Network with access to the internet but no access to the internal network. Is useful in congested areas and is generally unsecured.
f. Honeynets: Dummy Network to attract and fool attackers.
g. NAT (Network Address Translation): Translates private IP addresses in to public and public IP addresses to private.
h. Ad hoc: A wireless network without an access point, the connected devices communicate directly.

B) Segregation/segmentation/isolation: Separation for performance, security, or compliance
   a. Physical: Devices are separate and cannot directly communicate unless physically connected. Does not scale well.
   b. Logical (VLAN): Separate areas are segmented for different networks, but still housed on the same switch. To connect them you need a layer 3 device, such as a router.
   c. 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.
   d. Air gaps: Network where the devices are physically separate from another and don't share any components to communicate. Great for security but be careful with removable media.

C) Tunneling/VPN:
   a. Site-to-site: Send data between two sites in an encrypted form. Done by installing a VPN on both sides. Data will reach the VPN and encrypt and then the other VPN will decrypt it for the receiving end.
   b. Remote access (Host to Site): Software is installed on the device that wants the VPN tunnel, then the encrypted tunnel is created to connect to the specific network.

D) Security device/technology placement:
   a. Sensors: Can give transactions, logs, or other raw data. Can be integrated or built-into switches, servers, firewalls, routers, or other network devices.
   b. Collectors: Could be a console or SIEM. Gathers all the data from sensors into one place and attempts to make sense of it.
   c. Correlation engines: Can be built in SIEM, tries to compare and correspond data collected from the sensors to determine if an attack is present.
   d. Filters: Follow the logical path, does not follow a state set of rules for traffic. Blocks harmful traffic.
   e. Proxies: Intermediary point between the client and the service. Ensures that the response arrives safely and that the traffic flow is correct.
   f. 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.
   g. VPN concentrators: Authenticates VPN clients and establishes between tunnels.
   h. SSL accelerators: Offloads the SSL process to a hardware accelerator. SSL handshake is complicated and time consuming.
   i. Load balancers: Takes requests from the internet, and spreads the requests over multiple servers, can also determine the health of servers.
   j. DDoS mitigator: Sits between the network and the internet. Identifies and blocks DDOS attacks in real time.

k. Aggregation switches:
l. Taps and port mirror: Physical tap sees what is happening in traffic packets, and software port mirror sends a copy of the traffic packets. Is better for light traffic.

E) SDN: Aims to separate the hardware layer from the control. The network is fully virtualized with software, and then separated into the control (configuration) and data plane (forwarding and firewalling). Directly programmable from a central location, often automatically.

3.3 GIVEN A SCENARIO, IMPLEMENT SECURE SYSTEMS DESIGN.

A) Hardware/firmware security:
   a. FDE (Full Disk Encryption)/SED (Self Encryption Drives): Programs and technologies that encrypt everything on the storage drive.
   b. TPM (Trusted Platform Module): A chip on the motherboard designed to protect hardware through integrated cryptographic keys.
   c. HSM (Hardware Security Module): Accelerates cryptographic operations and manages cryptographic keys, can be implemented as a physical device and used to accelerate RSA-based operations.
   d. UEFI (Unified Extensible Firmware Interface)/BIOS (Basic Input/Output System):
      i. UEFI (Unified Extensible Firmware Interface): A method used to boot some 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.
      ii. BIOS (Basic Input/Output System): Basic low-end firmware or software that provides a computer with the basic instructions on how to start.
   e. Secure boot and attestation: Processes that checks and validates system files during the boot process.
   f. Supply chain: The process of getting a product or a service from the beginning supplier to the user.
   g. 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.
   h. EMI (Electromagnetic Interference)/EMP (Electromagnetic Pulse):
      i. EMI (Electromagnetic Interference): Electromagnetic interferences caused by devices that can corrupt data or prevent data from being transferred.
      ii. EMP (Electromagnetic Pulse): A short burst of electromagnetic energy

B) Operating systems:
   a. Types:
      i. Network: Supports servers, workstations, and other network-connected devices.
      ii. Server: Designed to function as a server.
      iii. Workstation: Optimized for user applications such as email and office apps.
      iv. Appliance: A system designed to serve a purpose.
      v. Kiosk: A system or computer with a touch screen designed to provide information or directions.
      vi. Mobile OS: The OS of phones, tablets, and other handheld devices.
   b. Patch management: Keeping systems up to date to help improve stability and security.
   c. Disabling unnecessary ports and services: Disabling unnecessary ports 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.

d. Least functionality: Limiting the operating system to be able to perform what is necessary.
e. Secure configurations: Changing the unsecure default setting to protect the system.
f. Trusted operating system (TOS): provides sufficient support for multilevel security and evidence of correctness to meet high security standards.
g. Application whitelisting/blacklisting: Protects the system from potentially dangerous applications.
    i. Whitelisting: Applications allowed on the system.
    ii. Blacklisting: Applications blocked by the system.
h. Disable default accounts/passwords: Are easily guessable and must be changed immediately to prevent unauthorized access.

C) Peripherals:
a. Wireless keyboards: Operate in the clear allowing for the capturing of keystrokes with a receiver to be controlled remotely.
b. Wireless mice: Operate in the clear allowing for the capturing of movements or to be controlled remotely.
c. Displays: Vulnerable to shoulder surfing, firmware hacks, and eavesdropping.
d. WiFi-enabled MicroSD cards: Portable storage device that has access to 802.11 Wi-Fi file transfers.
e. Printers/MFDs (Multi-Function Devices): Reconnaissance can be performed by going through the saved logs.
f. External storage devices: No authentication allows for anyone to read, write and move files.
g. Digital cameras: Easy to steal data.

3.4 EXPLAIN THE IMPORTANCE OF SECURE STAGING DEPLOYMENT CONCEPTS.

A) 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.
a. Environment: Usually tested in the actual environment that the product will be used in.
b. Development: Uses a development environment, version control and change management control to track development.
c. Test: Rigid tests are performed to find bugs and errors. Does not simulate the full product.
d. Staging: Uses data that the real product would use. Late stage testing.
e. Production: Application is now live, and the updates will be rolled out.

B) Secure baseline: Defines the core of what the development team must do. Lays out what will need to be updated in the future.

C) Integrity measurement: Tests against the baseline to keep it secure.

3.5 EXPLAIN THE SECURITY IMPLICATIONS OF EMBEDDED SYSTEMS.

A) SCADA (Supervisory Control and Data Acquisition)/ICS (Industrial Control System): An ICS is a type of 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, and they require extensive network segmentation.

B) Smart devices/IoT (Internet of Things): A mobile device that allows the user: customizable options, applications to help make daily activities easier, and an AI to assist in tasks. The IoT is the class of devices that help provide automation and remote control of appliances and devices in the home or office.
    a. Wearable technology: Contains personal and health information on a person.
    b. Home automation: Technology in the home is not updated frequently and are susceptible to attacks.
C) HVAC: Heating, ventilation, and air conditioning.
D) SoC (System on a Chip): An embedded device where the entire system is on the chip.
E) RTOS (Real Time Operating System): Attempts to use predictability to see what happens to meet real time requirements, the guesses must be secured.
F) Printers/MFDs: Contains logs, documents, and sensitive information that can be accessed and stolen.
G) Camera systems: Videos recorders and cameras are IP devices. The risk is that they can be hacked.
H) Special purpose:
    a. Medical devices: Can be attacked leaving patients at risk.
    b. Vehicles: Contains onboard Wi-Fi vulnerable to threats.
    c. Aircraft/UAV: Can have communications intercepted.

3.6 SUMMARIZE SECURE APPLICATION DEVELOPMENT AND DEPLOYMENT CONCEPTS.

A) Development life-cycle models:
    a. Waterfall vs. Agile:
        i. Waterfall: Not flexible, done in stages, and cannot go back to a previous stage once the next stage is started.
        ii. Agile: Flexible: allows for collaboration between groups, and can go back and fix previous iterations.
B) Secure DevOps:
    a. Security automation: Tools that automatically tests security functions, penetration, and for vulnerabilities.
    b. Continuous integration: The basic set of security checks while developing.
    c. Baselining: Comparing current performance to previously set metric
    d. Immutable systems: Are locked and unable to change. To update the entire platform must be updated.
    e. Infrastructure as code: Turns the devices into code to allow for focusing on the application needs instead of based on available infrastructure.
C) Version control and change management: The ability to track change and ability to revert to previous versions.
D) Provisioning and deprovisioning: The adding and removing of assets over time. Installing new devices and uninstalling old ones.
E) Secure coding techniques:
    a. Proper error handling: Errors do not crash the system, allow for elevated privileges, or expose private information.
    b. Proper input validation: Sanitizing data to make sure it is correct and secure before using.
    c. Normalization: Applying rules to a database design to ensure that the proper information goes in the proper places.
    d. Stored procedures: A program in the database that enforces the business rules.
    e. Code signing: Assigning a digitally signed certificate to code.

f. Encryption: Converting readable code to unreadable garbage to make it secure.
g. Obfuscation/camouflage: Making code difficult to read.
h. Code reuse/dead code: Reusing code in multiple contexts. Code that cannot be executed.
i. Server-side vs. client-side:
    i. Server-Side: Code runs on the server.
    ii. Client-Side: Code runs in the browser, is highly vulnerable to attacks.

F) execution and validation:
a. Memory management: Checking and ensuring that the program does not use too much memory.
b. Use of third-party libraries and SDKs: Commonly used so is better understood by attackers.
c. Data exposure: Disclosing private information to attackers.

G) Code quality and testing:
a. Static code analyzers: Checks source code for: conformance to coding standards, quality metrics, and for data flow anomalies.
b. Dynamic analysis (e.g., fuzzing): Providing unexpected inputs to cause the application to crash.
c. Stress testing: Seeing how many users a program can handle at a time.
d. 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.
e. Model verification: Ensuring the program meets specifications and performs its purpose.

H) Compiled vs. runtime code:
a. Compiled Code: Code that is optimized by an application and converted into an executable.
b. Runtime Code: The code that is interpreted as it runs.

3.7 SUMMARIZE CLOUD AND VIRTUALIZATION CONCEPTS.

A) Hypervisor: A software, firmware or hardware that creates, manages, and operates virtual machines.
a. Type I: Known as bare metal, runs on the hardware.
b. Type II: Known as hosted, runs on top of the operating system.
c. Application cells/containers: Abstracting applications from the platform into containers allowing for applications to run without launching an entire virtual machine. This provides portability and isolation, and less overhead than VM.

B) VM sprawl avoidance: The avoiding of a VM getting 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.

C) VM escape protection:

D) Cloud storage: The process of storing data in an off-site location that is leased from a provider.

E) Cloud deployment models:
a. SaaS (Software as a Service): The customer uses software that is not locally stored, instead, all of that service is being provided in the cloud. Ex. Google docs or Gmail.
    i. Everything is managed by the provider.
b. PaaS (Platform as a Service): Also known as software as a service.
c. Managed by customer: Data, applications, and making sure apps run on the OS
    i. Managed by Provider: Runtime, middleware, OS, virtualization, servers, storage, and networking.
d. IaaS (Infrastructure as a Service): Also known as hardware as a service,
    i. Managed by customer: Software (applications, data, Runtime, middleware, and operating system).

ii. Managed by Provider: Hardware (virtualization, servers, storage, and networking).

e. Private: Deployed within the organization by the organization for the organization.
f. Public: Cloud is deployed by the provider within their organization for other organizations to use.
g. Hybrid: A combination of public and private replication.
h. Community: Private or public but only shared between trusted groups.

F) On-premise vs. hosted vs. cloud:
   a. On-premise: Built and managed by the company's data center. Allows for complete control over it. Has a high investment cost and operational cost.
   b. Hosted: Leasing the network and storage that is off site. Access and availability depends on the design. Has No investment cost, and a moderate operational cost
   c. Cloud: 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.

G) VDI (Virtual Desktop Infrastructure)/VDE (Virtual Desktop Environment): 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.

H) Cloud access security broker: Allows for the integration of security policies across all cloud-based applications. Let's the provider see that applications are in use and users associated with them. Can be installed on premise or on the cloud server.

I) Security as a service (SECaaS): The provider implements their security services into your environment via the cloud, such as: authentication anti-virus, anti-malware, IDS, and event management.

3.8 EXPLAIN HOW RESILIENCY AND AUTOMATION STRATEGIES REDUCE RISK.

A) Automation/scripting:
   a. Automated courses of action: Automated scripts that give a basis for secured configuration with a secured template. Can be configured to accommodate for constant changes or can be launched on a specific schedule.
   b. Continuous monitoring: Monitors IDS/ logs, networks, SIEMs, and other systems for changes and threats.
   c. Configuration validation: Reviewing the settings of the system to ensure that its security settings are configured correctly.

B) Templates: Gives a basis for secured configuration with a standard secured configuration.

C) Master image: Is crafted configuration of a software or entire system. Created after the target system is installed, patched, and configured.

D) Non-persistence: Changes are possible. Due to risks of unintended changes, multiple protection and recovery options must be established.
   a. Snapshots: A copy of the live current operating environment.
   b. Revert to known state: Is a recovery process that goes back to a previous snapshot.
   c. Rollback to known configuration: Just a collection of settings. Does not usually include software elements.
   d. Live boot media: A portable storage device that can boot a computer. Is read-to-run or a portable version of the OS.

E) Elasticity: The ability for the system to adapt to a workload by allocating and providing resources in an automatic manner.

F) Scalability: The ability to handle an ever-increasing workload and able to accommodate future growth.

G) Distributive allocation: Is providing resources across multiple services or servers as necessary instead of preallocation or concentrated resources based on physical system location.
H) Redundancy: Secondary or alternate solutions, it's an alternate means to complete tasks. Helps reduce single points of failure and boosts fault tolerance.
I) Fault tolerance: The ability for the: network, system, or computer to provide a service while withstanding a certain level of failures. Aids in avoiding a single point of failure, a SPoF is anything that is mission critical.
J) High availability: Refers to a system that is able to function for extended periods of time with little to no downtime.
K) RAID (Redundant Array of Independent Disks): Is a high availability solution. Employs multiple hard drives in a storage volume with a level of drive loss protection, except for RAID 0.

3.9 EXPLAIN THE IMPORTANCE OF PHYSICAL SECURITY CONTROLS.

A) Lighting: If the perimeter is properly lit it can deter thieves, break-ins, and other criminal activity.
B) Signs: Allows for controlled entry point, is a psychological deterrent, and helps new and visitors find their way. Informs of security cameras, safety warnings, and that an area is restricted.
C) Fencing/gate/cage: A fence sets the boundaries of the property and protects against casual intruders. Gates allow for controlled entry and exit. Cages protect assets from being accessed by unauthorized individuals.
D) Security guards: Humans are adaptable, can adjust to live events, and can react to real time intrusion events. Can intervene and control the security devices.
E) Alarms: Notify security personnel and the authorities of unauthorized activities.
F) Safe: Protects valuables from thieves and natural disasters.
G) Secure cabinets/enclosures: Restricts unauthorized personnel from accessing cabinets.
H) Protected distribution/Protected cabling: Is a standard on how to safely transmit unencrypted data. Protects from wire-taps.
I) Airgap: Ensure secure networks are physically isolated from unsecure networks.
J) Mantrap: Area between two doorways to identify and authenticate individuals.
K) Faraday cage: Metal screen to protect equipment from electrostatic and electromagnetic influences.
L) Lock types: Can use a key, key-pad, cards, or biometrics.
M) Biometrics: Uses physical characters to identify the individual.
N) Barricades/bollards: Stops and guides traffic, it can also prevent the entrance of vehicles.
O) Tokens/cards: Items necessary to gain access to secured areas of the building. Can contain information that can identify and authorize an individual.
P) Environmental controls:
    a. HVAC: Keeps servers from overheating and shutting down.
    b. Hot and cold aisles: Allows for air flow control and for the air to move through the data center strategically.
    c. Fire suppression: Protects the equipment from fire, smoke, corrosion, heat, and water damage. Early fire detection is vital for protecting personal and equipment from harm.
Q) Cable locks: Protects small equipment from theft.
R) Screen filters: Reduces the range of visibility to prevent shoulder suffering.
S) Cameras: Deters criminal activity and creates a record of events.
T) Motion detection: Senses movement and sound in a specific area.

U) Logs: Document visitor access, allows for the identifying and record keeping of everyone who has access to the premise.
V) Infrared detection: Detects and monitors changes in the temperature.
W) Key management: Ensure only authorized individuals only have access to the areas they need to complete their work

4.0 IDENTITY AND ACCESS MANAGEMENT

4.1 COMPARE AND CONTRAST IDENTITY AND ACCESS MANAGEMENT CONCEPTS

A) Identification, authentication, authorization and accounting (AAA):
    a. Identification: Finding the unique individual on the system.
    b. Authentication: The ability to tell if an individual is actually who they claim they are.
    c. Authorization: Determining what an individual can and cannot access on a system.
    d. Accounting: The tracking of an individual's actions on the system.
B) Multifactor authentication: Uses at least two of the factors of authentication.
    a. Something you are
    b. Something you have
    c. Something you know
    d. Somewhere you are
    e. Something you do
C) Federation: The authenticating and authorizing between two parties. Ex. Logging onto Facebook with Google account.
D) Single sign-on: Only uses one of the factors of authentication.
E) Transitive trust: There are more than two entities, one entity is trusted because they are trusted by someone the company trusts.

4.2 GIVEN A SCENARIO, INSTALL AND CONFIGURE IDENTITY AND ACCESS SERVICES.

A) LDAP (Lightweight Directory Access Protocol):
Queries information about the directory. Is a hierarchical structure; CN = Common Name, OU = Organizational Unit, DC = Domain Controller. Utilizes TCP/IP, TCP/UDP ports 389.
    a. Secure LDAP: LDAP over SSL/TLS, uses TCP on port 636. Does not send queries in plain text.
B) Kerberos: Developed by MIT, for mutual authorization between client and server. It uses a ticket granting system for authorization. Is a government standard.
C) TACACS+ (Terminal Access Controller Access Control System): Runs TCP over port 49, encrypts all parts of communication. Does not suffer due to security issues caused by RADIUS. Authorization and Authentication are separated for granular control.
D) CHAP (Challenge Handshake Authentication Protocol): 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 over the wire.
E) PAP (Password Authentication Protocol): Username and password are sent as plaintext and are no longer used.
F) MS-CHAP (Microsoft CHAP): Delivers a two-way, mutual authentication between the server and client. Separate keys are created for sent and received data. Is seen as weak due to it using a 5-bit encryption system, same as NTLM.
G) RADIUS (Remote Authentication and Dial-in User service): Combines authentication and authorization, only encrypts the passwords, each network device must contain an authorization configuration. There is

no command logging, and minimal vendor support. Uses ports 1812 for authentication and authorization and port 1813 for accounting functions.

H) SAML (Security Association Markup Language): Authenticates through a third-party source to gain access, the resource is not responsible for the authentication. The request is passed through a trusted third-party server.
    a. The three roles are: Principle (the user or client), identity provider (the one who assures the identity of the principle), and service provider (a web service of some type.)

I) OpenID Connect: OpenID Connect handles the authentication part of the identification process and uses OAuth for authorization.

J) OAUTH (Open Standard for Authorization): Token authorization happens in the background. Uses a logon from a larger trusted service.

K) Shibboleth: An open-source software that uses SAML to provide a third-party federated SSO authentication.

L) Secure token: An authentication mechanism that can be used to identify and authenticate, and to deny and allow access.

M) NTLM (New Technology LAN Manager): Used for authenticating in a Windows domain, was replaced by Kerberos for the most part.
    a. NTMLv2: Is the most common form used, is somewhat insecure.

4.3 GIVEN A SCENARIO, IMPLEMENT IDENTITY AND ACCESS MANAGEMENT CONTROLS.

A) Access control models:
    a. MAC (Mandatory Access Control): Based on classification rules. Objects are given sensitivity labels, subjects given clearance labels, and users obtain access by having the correct clearance. The classifications are hierarchical.-
    b. DAC (Discretionary Access Control): Is based on user identity. Users are granted access through ACLs placed on objects through the object's owner or creator.
        i. ACL (Access Control List): A security logical device attached to all objects and resources, it defines which users are granted or denied access.
    c. ABAC (Attribute Based Access Control): Assigning access and privileges through a scheme of attributes. Relations and criteria determine access; time of day, location, and/or IP address.
    d. Role-based access control: Access is based on the job and position of the user. Changing permissions of a group changes the permissions for all of the members. Not good for companies with high turn-over rates.
    e. Rule-based access control: Rules are created by the admin to monitor usage and if a user needs access they must meet the requirements of the rules. Rules are enforced regardless of the user.

B) Physical access control:
    a. Proximity cards: A smart card that does not require direct contact.
    b. 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).

C) Biometric factors: Verifies identity through physical features.
    a. Fingerprint scanner: Scans the unique patterns of the fingerprint to grant access.
    b. Retinal scanner: Blood vessels in the back of the retina.
    c. Iris scanner: Scans the Iris.
    d. Voice recognition: The identification and translation of spoken language for authorization of a user. Is vulnerable to impersonation.
    e. Facial recognition: The identification of an individual from a digital image or a video frame. Is vulnerable to impersonation.

f. False acceptance rate (FAR): Incorrectly identifies an unauthorized user as an authorized user. Type 2 error.
g. False rejection rate (FRR): Incorrectly identifies an authorized user as an unauthorized user. Type 1 error.
h. 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.

D) Tokens
   a. Hardware: A device that displays and constantly generates a pin or password.
   b. Software: An app or software that generates a token.
   c. HOTP/TOTP: Open source standards to generate one-time use passwords.
      i. HOTP (HMAC-based One-Time Password): Can be used only once before it expires.
      ii. TOTP (Time-based One-time Password): Only last for around 30 seconds before it expires.

E) Certificate-based authentication:
      i. PIV/CAC/smart card: Cards that have embedded certificates and a photo ID for authorization. The US DOD uses CAC/PIV.
      ii. PIV (Personal identity verification): Is for civilians working for the federal government.
      iii. CAC (Common access card): Is for Department of Defense members.
   b. IEEE 802.1x: Offers port-based authentication to wireless and wired networks to prevent rogue devices from connecting to secured ports.

F) File system security: The means of ensuring that files are encrypted and can only be used by properly authorized users have access to them or modify them.

G) Database security: MS and Oracle allow for the DB to be encrypted.

4.4 GIVEN A SCENARIO, DIFFERENTIATE COMMON ACCOUNT MANAGEMENT PRACTICES.

A) Account types:
   a. User account: An account that is a collection of information that identifies an individual and grants them specific areas of the network or system.
   b. Shared and generic: Multiple individuals sign into a single account. No workplace should have these, cannot distinguish the actions of the user.

B) accounts/credentials:
   a. Guest accounts: An anonymous shared logon account.
   b. Service accounts: Performs specific maintenance actions, such as a backup, account and server operators.
   c. Privileged accounts: Access is set to access rights, generally referred to as system or network administrative accounts.

C) General Concepts:
   a. Least privilege: Rights and permission are set to bare minimum.
   b. Onboarding/offboarding:
      i. Onboarding: Helps new employees learn all of the facets of their new job.
      ii. Offboarding: Helps leaving employees learn how to properly leave and potentially return to the company.
   c. Permission auditing and review:
   d. Usage auditing and review:
   e. Time-of-day restrictions: Certain privileges are permitted or restricted based on the time of day.
   f. Recertification: The action of regaining a certification due to the certification being expired.
   g. Standard naming convention: Allows for the easier identification of resource location and purpose. Reduces the amount of time needed for troubleshooting and training.

h. Account maintenance: Making sure that accounts have the proper privileges, and unused accounts are deleted. Generally done through scripts to save time and money.
i. Group-based access control: Every user in a group has the same privileges.
j. Location-based policies: Grants and denies access based on the user's location.
k. Account policy enforcement:
l. Credential management: Stores, manages, and tracks user credentials.
m. Group policy: Sets different privileges of the system and allows for these to be managed or set those across entire groups or even through the entire network and every computer within it.
n. Password complexity: The enforcing of complex and difficult to guess passwords.
o. Expiration: The amount of time that passes before a password is required to be changed.
p. Recovery: The ability to find lost passwords and usernames in case an employee forgets them.
q. Disablement: Disabling an account.
r. Lockout: Prevents login from specific individual after a set of failed login attempts, for a set period of time.
s. Password history: Remembers past passwords and prevents the reuse of passwords.
t. Password reuse: The ability to ever use the same password again.
u. Password length: The minimum amount of characters that can be used in a password.
v. Password age: A policy that sets how long a user can have a password before they are forced to change it.

6.0 CRYPTOGRAPHY AND PKI

6.1 COMPARE AND CONTRAST BASIC CONCEPTS OF CRYPTOGRAPHY.

A) Symmetric algorithms: A shared secret key used by the sender and receiver to encrypt and decrypt.
B) Modes of operation:
C) Asymmetric algorithms: There is a shared public key and a private secret key. Public key encrypts and the private key decrypts, private key to sign and public key verify.
D) Hashing: An algorithm that creates a unique one-way encryption, not plaintext.
E) Salt, IV, nonce:
    a. Salt: The adding of input to random data to function to make it more complicated. A small piece of data added to the end of a password when creating a hash
    b. IV (Initialization Vector): A random value used with an encryption key.
    c. Nonce: One-time use random value used for authentication.
F) Elliptic curve (ECC): Great for low powered machines. Uses curves for encryption instead of large prime numbers.
G) Weak/deprecated algorithms: Weak due to vulnerabilities (WEP) or weak key length (DES is on 56-bits) which is easy to brute force through.
H) Key exchange: Securely sending keys back and forth. Out-of-Band where the key is sent over the phone, in person, or any other way offline. In-Band is sent over the internet encrypted.
I) Digital signatures: Provides integrity, verifies that the original sender is actually the one who sent it. This can be done through asymmetric encryption, where there is a hash message then they will encrypt the hash using their private key, creating a digital signature that can only originate from them. To verify, the signature is decrypted with the public key, and the message is then hashed. If the two hashes match, then the digital signature is valid
J) Diffusion: Changing one character causes the plaintext to drastically change the outputted cipher.
K) Confusion: The cipher doesn't look anything like the plain text.
L) Collision: Two completely different pieces of data have the exact same hash.
M) Steganography: Hides messages or code inside of an image or another type of data. Impossible to decipher without the correct tools.
N) Obfuscation: Taking something and making it difficult for a human to understand, however it is not impossible to convert it back to the original form.
O) Stream vs. block:
P) Key strength: Larger keys and more bits are signs of better encryption and stronger keys.
Q) Session keys: Symmetric keys used to provide a secure and fast online connection. The server's public key is paired with a random key to produce a symmetric key, that the server uses to encrypt and the user to decrypt.
R) Ephemeral key: Session keys that only last temporarily and change frequently.
S) Secret algorithm: Is a symmetric encryption. Uses the same key for the sender to encrypt and the receiver to decrypt.
T) Data-in-transit: Data being transmitted over a network. Should be encrypted using TLS and IPSec.
U) Data-at-rest: Data in a storage device.
V) Data-in-use: Data being ran through RAM or CPU, is almost always decrypted to make it easier to use.
W) Random/pseudo-random:
    a. 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.
X) Key stretching: Hashing a password, and then hashing that hashed value. Protects a weak password from brute force attacks.
Y) Implementation vs. algorithm selection:

a. Crypto service provider: A library of cryptographic standards and algorithms.
b. Crypto modules: Hardware, firmware or software that provides the hash, HMAC, cipher, decipher, sign, and verify methods.

Z) Perfect forward secrecy (PFS): Prevents point of failure where a stolen private key can decrypt all connections by generating a new key each session. Protects past sessions against future compromises of secret keys.

AA) Security through obscurity: Relying on secrecy to protect and secure data.

BB) Common use cases:
a. Low power devices: Mobile phones and portable devices.
b. Low latency: Low amount of time occurs between input and output.
c. High resiliency: Larger key sizes and encryption algorithm quality.
d. Supporting confidentiality: Secrecy and privacy.
e. Supporting integrity: Preventing modification of data and validating contents with hashes.
f. Supporting obfuscation:
g. Supporting authentication: Password hashing and protecting the original password.
h. Supporting non-repudiation: Digital signature provides: authenticity, integrity, and non-repudiation.
i. Resource vs. security constraints: Limitations in providing strong cryptography due to the amount of available resources (time and energy) vs the security provided by cryptography.

6.2 EXPLAIN CRYPTOGRAPHY ALGORITHMS AND THEIR BASIC CHARACTERISTICS.

A) Symmetric algorithms:
a. AES (Advanced Encryption Standard): Symmetric, block cipher with 128-bit blocks, key sizes of 128-bit, 192-bit and 256-bit. It utilizes the Rijndael algorithm and is the U.S. government standard for the secure exchange of sensitive but unclassified data. It is also the encryption standard used today with WPA2.
b. DES (Data Encryption Standard): Symmetric, was common until replaced by AES, the block cipher is 64-bit and the key is 56-bit (very small), this means it can easily be brute forced.
c. 3DES: Symmetric, very secure and upgrade over DES with three separate keys and three passes over data. Not used in modern day either.
d. RC4: Symmetric, part of the original WEP standard with SSL, removed from TLS, key sizes of 40-bit to 2048-bit. Deprecated from biased output.
e. Blowfish/Twofish:
i. Blowfish: Symmetric, fast and has variable key-lengths from 1-bit to 448-bits, uses 64-bit block cipher. Not limited by patents.
ii. Twofish: Symmetric, uses a very complex key structure up to 256-bits but still similar to predecessor, works using 128-bit blocks. Again, not limited by patents.

B) Cipher modes:
a. CBC (Cipher Block Chaining): Symmetric, uses IV for randomization. Encryption that is dependent on the block before it. Slow.
b. GCM (Galois Counter Mode): Used by many. Provides data authenticity/integrity, hashes as well. Widely used.
c. ECB (Electronic Code Book): Mode of operation, simplest cipher mode, not recommended.
d. CTR (Counter Mode): Converts block into stream, uses IV. Widely used.
e. Stream vs. block:

C) Asymmetric algorithms:
a. RSA (Rivest, Shamir, Adleman): First practical use of public key cryptography, uses large prime numbers as the basis for encryption.

b. DSA (Digital Signature Algorithm): Standard for digital signatures and modifies Diffie-Hellman, follows usage of elliptic curves to create ECDSA.
c. Diffie-Hellman: An asymmetric standard for exchanging keys. Primarily used to send private keys over public (unsecured) networks.
    i. Groups: Diffie-Hellman (DH) groups determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require additional time to compute the key.
    ii. DHE (Diffie-Hellman Ephemeral): A Diffie-Hellman key exchange that uses different keys.
    iii. ECDHE (Elliptic Curve Diffie-Hellman Ephemeral): Key agreement protocol that allows 2 parties, each having an elliptic curve public-private key pair, to establish a shared secret over an insecure channel.
d. 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.
e. PGP (Pretty Good Privacy)/GPG (GNU Privacy Guard):
    i. PGP (Pretty Good Privacy): Asymmetric, used by many for emails and is used by IDEA algorithm.
    ii. GPG (GNU Privacy Guard): A free, open-source version of PGP that provides equivalent encryption and authentication services.

D) Hashing algorithms: Hashing provides integrity and authenticity.
a. MD5 (Message-Digest Algorithm v5): Hashing algorithm, 128-bit hash with strong security, collision was found in 1996 so it is not used as much nowadays.
b. SHA (Secure Hash Algorithm): Hashing algorithm, one-way 160-bit hash value with encryption protocol. Standard hash algorithm today, went from SHA-1 (160-bit digest, deprecated) to SHA-2 (512-bit digest, still used).
c. HMAC (Hash-Based Message Authentication Code): Hashing algorithm that combines itself with a symmetric key. Provides data integrity as well as authenticity, but is faster than asymmetric encryption.
d. RIPEMD (RACE Integrity Primitives Evaluation Message Digest): Hashing algorithm that is based on MD4, collisions were found so it now exists in versions of 160-bits, 256-bits, and 320-bits.

E) Key stretching algorithms: Lengthen key to make brute-force attacks harder.
a. Bcrypt: Key Stretching that helps protect passwords by repeating Blowfish cipher.
b. PBKDF2 (Password-Based Key Derivation Function 2): Key Stretching, applies RSA function to password to create stronger key.

F) Obfuscation: Making something unclear to read, but can still reverse it.
a. XOR (Exclusive OR): Mathematical operation that's a part of all symmetric operations, done by comparing bits of plaintext and a key (same=0, different=1). Can be reversed to get plaintext back.
b. ROT13 (Rotate by 13): Common substitution cipher, rotates each letter 13 places.
c. Substitution ciphers: Cipher that changes one symbol for another, like the Caesar Cipher. Easy to decrypt.

6.3 GIVEN A SCENARIO, INSTALL AND CONFIGURE WIRELESS SECURITY SETTINGS.

A) Cryptographic protocols:
a. WPA (Wi-Fi Protected Access): Uses RC4 with TKIP. Was replaced by WPA2.
b. WPA2 (Wi-Fi Protected Access v2): Uses CCMP for encryption.
c. CCMP (Counter Mode with Cipher Block Chaining Message Authentication Code Protocol): Is based on 128-bit AES is more secure than TKIP. Was advanced for its time.

d. TKIP (Temporal Key Integrity Protocol): Protocol that mixes a root key with an initialization vector, a new key for each packet.

B) Authentication protocols:
   a. EAP (Extensible Authentication Protocol): Is an authentication framework that provides general guidance for authentication methods.
   b. PEAP (Protected Extensible Authentication Protocol): An extension of EAP that is sometimes used with 802.1x, a certificate is required on the 802.1x server.
   c. EAP-FAST (EAP Flexible Authentication with Secure Tunneling): A Cisco-designed replacement for Lightweight EAP, supports certificates but are not required.
   d. EAP-TLS (EAP Transport Layer Security): This is one of the most secure EAP standards and is widely implemented on many networks. It uses PKI, so certificates are required on the 802.1x server and on the clients.
   e. EAP-TTLS (EAP Tunneled Transport Layer Security): 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.
   f. IEEE 802.1x: An authentication protocol used in VPNs, wired and wireless networks. In VPNs it is used as a RADIUS server, wired use it as a port-based authentication, and wireless use it in Enterprise mode. Can be used with certificate-based authentication.
   g. RADIUS Federation: Members of one organization can authenticate to the network of another network using their normal credentials.

C) Methods:
   a. PSK vs. Enterprise vs. Open:
      i. PSK (Pre-Shared Key): Uses WPA2 encryption along with a key that everyone needs to know to access the network.
      ii. Enterprise: Users to authenticate using a username and password, and uses 802.1X to provide authentication, server handles distribution of keys/certificates.
      iii. Open: Does not apply any security.
   b. WPS: Allows users to easily configure a wireless network, often by using only a PIN. Are susceptible to brute force attacks because they can discover the PIN.
   c. Captive portals: Forces clients using a web browser to complete a task before being able to access the network.

6.4 GIVEN A SCENARIO, IMPLEMENT PUBLIC KEY INFRASTRUCTURE.

A) Components:
   a. CA (Certificate Authority): A trusted third-party agency that is responsible for issuing digital certificates.
   b. Intermediate CA (Intermediate Certificate Authority): An entity that processes the CSR and verifies the authenticity of the user on behalf of a CA.
   c. CRL (Certificate Revocation List): A list of certificates that are: no longer valid, expired, or that have been revoked by the issuer.
   d. OCSP (Online Certificate Status Protocol): A request and response protocol that obtains the serial number of the certificate that is being validated and reviews revocation lists for the client.
   e. CSR (Certificate Signing Request): A user request for a digital certificate
   f. Certificate: Digitally signed statement that associates a public key to the corresponding private key.
   g. Public key: A key that is provided by the sender, used by anyone to encrypt with asymmetric.
   h. Private key: Key used to decrypt a message, only used by the person opening the message.
   i. Object identifiers (OID): A serial number that authenticates a certificate.

B) Concepts:
    a. Online vs. offline CA:
        i. Online CA: Is directly connected to a network, most common.
        ii. Offline CA: Is not directly connected to a network, often used for root certificates.
    b. 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.
    c. Pinning: The application has hard-coded the server's certificate into the application itself.
    d. Trust model: A complex structure of: systems, personnel, applications, protocols, technologies, and policies working together to provide protection.
    e. Key escrow: Private keys are kept by the users and a 3rd party as back-ups.
    f. Certificate chaining: Certificates are handled by a chain of trust, the trust anchor for the digital cert is the root CA.
C) Types of certificates:
    a. Wildcard: A Certificate that can be used with multiple subdomains of a given domain, by covering the all subordinate certificates to the root.
    b. SAN (Subject Alternative Name): The certificate has several uses, allows a certificate to be valid for multiple domains using multiple names.
    c. Code signing: Digitally signs written application code and makes sure that it adheres to policy restriction and usage.
    d. Self-signed: The root CA creates its own certificate.
    e. Machine/computer: Certificates that are assigned to a specific machine.
    f. Email: Secures emails, is used by S/MIME.
    g. User: Often for authentication or to access resources.
    h. Root: Used for root authorities, they usually are self-signed.
    i. Domain validation: Provides a secure communication with a specific domain and provides TLS, this is the most common form of certificate.
    j. Extended validation: Are more secure because they require more validation from the certification holder.
D) Certificate formats:
    a. DER (Distinguished Encoding Rules): Are common and designed for X.509 certificates, they are used to extend binary encoded certificates. Cannot be edited by a plain text editor. Used with java commonly.
    b. PEM (Privacy Enhanced Mail): Most common format in which certificates are issued. Multiple certificates and the private key can be included in one file. The file is encoded ASCII. PEM file extensions include .pem, .crt, .cer, and .key. Apache servers typically use PEM-format files.
    c. PFX: A precursor to P12, has the same usage. Administrators often use this to format on Windows to import and export certificates.
    d. CER (Certificate File): May be encoded as binary DER or as ASCII PEM.
    e. P12: Is a PFX extension used in windows
        i. PKS 12 (Public Key Cryptography Standards #12): Is part of the RFC standard. Stores many types of certificates and can be password protected.
        ii. RFC (Remote Function Call): A formal document describes the specifications for a particular technology, was drafted by the Internet Engineering Task Force.
    f. P7B: Is stored in Base64 ASCII, containing certificates and chains but not the private key.

.