The #QuarantineSec Security+ Study Guide

EXAM NUMBER: SY0-501

Need editing access?

Dm Marcus on Twitter !!!! (@marcusjcarey)

Email Frank The Tank (tankeazy@gmail.com)
Austin (mullins.austin@gmail.com)
Geovani(geovanijnpierre2@gmail.com)

Want to get ignored?
Email Marcus (seriouslydontemailmarcus@gmail.com)

Need to be on the zoom calls? Fill this form out.

1.0 Threats, Attacks and Vulnerabilities

1.1 Given a scenario, analyze indicators of compromise and determine the type of malware.

- **Viruses**

  Malware that requires a host application to activate.

- **Crypto-malware**

  Malware that uses a targeted PC to mine cryptocurrency.

- **Ransomware**

  A type of malware that either blocks access to or threatens to publish a users data unless a ransom is paid.

- **Worm**

  Malware that is capable of self-replicating without human interaction or a host application.

- **Trojan**

  A Trojan horse, or Trojan for short, is a piece of malware that pretends to be something benign, such a media player, an emailed file, a smartphone app or even a Web page.

- **Rootkit**

  Software designed to provide continued privileged access to a computer while also remaining hidden.

- **Keylogger**

  Malicious software installed on a computer to capture a user's keystrokes.

- **Adware**

  Malicious software that inundates the user with pop-up ads or browser redirects to advertising.

- **Spyware**

  A type of malware that is used to gather information on a user as well as spy on a users activities. A keylogger is a type of spyware.

- **Bots/Botnet**

  When an attacker takes over unknowing targets to perpetrate an attack on an intended target. A botnet is a collection of devices, typically IoT devices, all running bots.

- **RAT**

  Remote Access Tool - a piece of code running on a remote machine that provides access to the attacker

- **Logic bomb**

  A logic bomb is malware that is triggered by a response to an event, such as launching an application or when a specific date/time is reached. Attackers can use logic bombs in a variety of ways.

- **Backdoor**

  A set of conditions (e.g. user added, web interface exposed) that provides an alternate route for an attacker into the system

1.2 Compare and contrast types of attacks.

- **Social engineering**

    - **Phishing**
      An attack when an attacker attempts to acquire confidential information by tricking the target individual through email. Socially-engineering someone to click a link, or download something, often impersonating a boss or another authoritative body.

    - **Spear phishing**
      Phishing targeting a specific individual or group of people

    - **Whaling**
      Spear-phishing targeting high-level employees (C-suite, sys admin, etc)

    - **Vishing**
      A form of phishing but using the telephone.

    - **Tailgating**
      Waiting until someone makes a legitimate entry to a building and following in after them - e.g. people will hold the door to be polite

    - **Impersonation**
      Pretending to be a legitimate person or institution. Using the identity of a trusted or authorized individual to lure a victim into providing sensitive information is the basis of impersonation.

    - **Dumpster diving**
      Searching through discarded materials and machines for information that has not been properly destroyed

    - **Shoulder surfing**
      The act of looking over someone's shoulder while they enter a username and password to steal the information.

    - **Hoax**
      A malicious attack similar to phishing but can be used to spread false information leading the audience to believe and act according to the intentions of the hoax maker.

- **Watering hole attack**
  An attack where malware is installed on a frequently visited website to steal information from the victim(s) or target them with malware.

- **Principles (reasons for effectiveness)**
  - Authority - The psychological principle that humans are motivated and open to persuasion from people in positions of authority.
  - Intimidation - The psychological principle that humans are motivated by fear of repercussions if they do not comply with an attacker's request. This usually works well with an authority pretext.
  - Consensus - The psychological principle that humans tend to look for consensus from others or "social proof" when making decisions. "If other people are doing it then it must be OK."
  - Scarcity - The psychological principle that humans are motivated to act when there is a fear that something may soon be made unavailable or become difficult to get. The perception that if something is hard to get then it must be more valuable.
  - Familiarity - The psychological principle that humans are more willing to comply with requests from someone they know and trust.
  - Trust - Same as above.
  - Urgency - The psychological principle that humans will more easily comply with requests when there is a perceived deadline or urgency to making their decision. The fear of missing out on something is a motivational factor.

● Application/service attacks

- **DoS or DDoS**
  Target to disrupt the services ping of death & ping flooding. Goal is to overwhelm target system with junk traffic so as to deny service to legitimate users.

- **Man-in-the-middle**
  The attacker inserts themself between the victim and their intended communication destination - can view and alter data in transit

- **Buffer overflow**
  If code variables are not carefully defined, it may be possible to input content for them that exceeds the memory available for the variable by default. In this event, it may be possible to crash into other parts of the software that were never meant to be accessed this way and to overwrite or execute them out of order

- **Injection**
  the attacker is able to provide malicious code (SQL queries, CLI commands, shell code) and have the program execute it, potentially with privileged access

- **Cross-site scripting -** A code injection attack where an attacker is able to execute a script in the forms of an application or web site, or anywhere else in an application.

  - Non-persistent/reflected
    An XSS attack that does not stay in the target application or web site. Usually a user will need to click on a link to activate the malicious script, like with a search box.

  - Persistent/stored
    When an XSS attack is stored in a web site or application and anyone who accesses it is vulnerable.

  - DOM
    When an XSS attack alters the Document Object Model to influence the behaviour of the webpage

- **Cross-site request forgery**
  Code on one site makes a request on behalf of the victim on another site (e.g. code on malicious site attempts bank transaction in another tab/window) - limited by same origin policy and CSRF tokens

- **Privilege escalation**
  Taking advantage of misconfigurations to gain access to resources as a more privileged user (e.g. root/admin)

- **ARP poisoning**
  Providing malicious ARP information to the victim's ARP cache - may allow MitM attacks as victim now thinks attacker is their intended connection

- **Amplification**
  The attacker sends out relatively small service requests (e.g. asking an NTP server what the time is in timezone X?) that result in a larger response - many small requests from the attacker can put a much greater load on the target receiving the responses, which can be any machine by way of IP spoofing (i.e. pretending to be that machine when making the request)

- **DNS poisoning**

Same as ARP poisoning but affecting the DNS cache of the victim or the DNS server(s) they rely upon

- **Domain hijacking**
  Theft of control of a domain by changing the registration of the domain without permission of owner

- **Man-in-the-browser**
  a MitM attack that specifically affects the contents of the browser using a proxy Trojan horse

- **Zero day**
  An exploit that has not been used or publicly disclosed, yet, and has therefore been available for 0 days - no patches or mitigations will be in place until it is revealed and identified

- **Replay**
  Especially relevant in wireless communications (open broadcast domain) - the attacker is able to replay sensitive traffic that they have recorded from a legitimate user's action

- **Pass the hash**
  Some systems rely entirely on the password hash to authenticate - it is possible to provide them with the hash only, rather than the user's password

- **Hijacking and related attacks**

  - Clickjacking
    By overlaying a transparent object on an area of a web page that the user wishes to click on, the attacker can get the user to click on their transparent object instead to run code or direct the user to another page

  - Session hijacking
    following authentication, it is possible for the attacker to use captured session credentials to act as though they were the authenticated user

  - URL hijacking
    the attacker causes the victim's URL to be removed from search results and replaced with their own malicious site URL

  - Typosquatting
    By registering domains that are common typographic errors of popular domains (e.g. goggle.com instead of google.com) they can receive traffic

from people who make those typos or they can use the domains in phishing emails, relying on people not to look too closely at the URL they are clicking on

- **Driver manipulation**
  - Shimming
    a small software library that intercepts API calls and executes them itself potentially with changes or redirects
  - Refactoring
    identifying and modifying the flow of code to produce a malicious effect without alerting the victim
- **MAC spoofing**
  the attacker provides a MAC address that is not theirs in order to impersonate the machine that legitimately bears that MAC
- **IP spoofing**
  as MAC spoofing, but the IP address is impersonated

Wireless attacks

- **Replay**
  the attacker is able to replay sensitive traffic that they have recorded from a legitimate user's action
- **IV**
  Initialisation Vector - poor implementation of the IV in encryption allows the attacker to predict key rotation
- **Evil twin**
  a rogue AP pretending to be a legitimate AP, by mimicking its SSID and potentially actively disassociating current valid connections, in order to provide MitM access to the attacker
- **Rogue AP**
  an Access Point in the local environment that should not be there - can be malicious (e.g. Evil Twin) or legitimate (e.g. neighbour)
- **Jamming**

flooding the wireless environment with radio noise to prevent any communications from occurring

- **WPS**
  Wireless Protected Setup - quick, easy connection between device and AP (e.g. press button instead of entering secret) - relied on 8-digit identification number (actually 7, plus a checksum digit)

- **Bluejacking**
  the attacker connects to a BlueTooth device and takes control of it

- **Bluesnarfing**
  the attacker sniffs BlueTooth traffic and gains information communicated from the victim to the device

- **RFID**
  Radio Frequency Identification - typically quite simple antennae and transmitter powered by the radio signal from the RFID reader - limited range, but often vulnerable to cloning and replay attacks

- **NFC**
  Near Field Communications - similar to RFID but the range is <=4cm and the communication can be more active and support encryption

- **Disassociation**
  typical of Evil Twin attacks - in order to get the victims to connect (associate) with the malicious AP, they are first sent a disconnect (disassociation) signal pretending to be the legitimate AP - the Evil Twin can then take up that freed connection to the legit AP, and can answer the victim's request to reconnect

Cryptographic attacks

- **Birthday**
  exploits probability theory - while the probability space may be quite large to permit vast numbers of different keys/hashes/etc, there may actually be a relatively high probability that the same key/hash/etc is generated more than once - the analogy is the probability of two students in a classroom having the same birthday

- **Known plain text/cipher text**

Given both the original unencrypted text and the resulting cypher text, it may be possible to reverse engineer the encryption keys and algorithms involved

- **Rainbow tables**
  These are large tables of pre-computed hashes using many different protocols (and/or salts) used to speed up the hash cracking process

- **Dictionary**
  a refinement on the brute-force attack, the dictionary attack tries each password in a large list of known passwords

- **Brute force**
  the attacker attempts every possible combination within a given keyspace at each possible length until the password is guessed

  - Online vs. offline
    online password cracking may be limited by connection speeds, attempt rates, and attempt limits - offline attacks can make use of high-powered computing resources and make far more attempts in the same time

- **Collision**
  it is possible, though highly unlikely, that two inputs could have the same hashed output
  - What attackers try to do with Hashes so it messes up data
  - A Weakness

- **Downgrade**
  the attacker may be able to force the victim machine to downgrade its encryption or authentication restrictions - often takes advantage of backwards compatibility for less secure systems

- **Replay**
  the attacker is able to replay sensitive traffic, including encrypted authentication traffic, that they have recorded from a legitimate user's action

- **Weak implementations**
  use of weak cryptographic implementations (e.g. obsolete algorithms, vulnerable key transmission methods, lower-bit encryption)

1.3 Explain threat actor types and attributes.

- ## Types of actors

    - **Script kiddies**
      attackers with an incomplete understanding of the tools they use - often just hacking for mischief or exploration. Downloads and runs “scripts” written by other, and may or may not understand how they work.

    - **Hacktivist**
      attackers with a political or ideological goal

    - **Organized crime**
      Actors who do crime for economic gain.

    - **Nation states/APT**
      nations and the Advanced Persistent Threats they form and fund - these attackers have extensive resources at their disposal

    - **Insiders**
      may be malicious (e.g. disgruntled employee) or simply ignorant

    - **Competitors**
      attackers interested in industrial espionage - typically focussed on proprietary information exfiltration but may engage in sabotage

- ## Attributes of actors

    - **Internal/external**
      actors may be internal to the organisation, which permits them increased access to sensitive resources, contacts, and information - external actors will generally have much less sensitive access, but have less concern about detection

    - **Level of sophistication**
      attackers can range, from script kiddies who may not know or care what their tools do, to highly-trained (even professionally-trained) APT groups

    - **Resources/funding**

attackers may range, from having little to no funding and few resources (although internet access alone is a huge resource), to having the resources of whole nations behind them

- **Intent/motivation**
  attacker motivations range from curiosity to economic gain to ideological and political agendas to nationalist superiority

- **Use of open-source intelligence**

  Openly accessible information abounds in the form of social media, Google dorks, public DNS, Shodan, Censys, and more, and can often be gathered without the target being aware they are being examined. Often referred to as OSINT.

1.4 Explain penetration testing concepts.

- **Active reconnaissance**

  You are actively communicating with the assets that you are trying to test. (NMAP, Vulnerability Scan, Ping, etc)

- **Passive reconnaissance**

  Reconnaissance that does not touch the target infrastructure. Using sites like Shodan, Hunter.io, etc.

- **Pivot**

  Accessing internal machines through another machine you have already compromised.

- **Initial exploitation**

  How an attacker initially compromises a system/network. These attacks change frequently.

- **Persistence**

  Keeping access on a network/system. This can be accomplished through creating new accounts, installing backdoors and/or stealing additional credentials.

- **Escalation of privilege**

  Exploitation of a vulnerability to gain super user or higher privileges than the current user.

- **Black box**

  A penetration test where you know nothing about the target machine.

- **White box**

  A penetration test where you know everything about the target machine.

- **Gray box**

  A penetration test where only some things are known about the target machine.

- **Penetration testing vs. vulnerability scanning**

  Vulnerability scanning is used to find potential exploits, penetration testing actively uses/tests the exploits.

1.5 Explain vulnerability scanning concepts.

- **Passively test security controls**

  grabbing traffic headers to identify service type and version

- **Identify vulnerability**

  cross-referencing header info with CVEs (Common Vulnerabilities and Exposures) to identify services with known vulnerabilities

- **Identify lack of security controls**

  testing simple security controls such as authentication without credentials or with default credentials

- **Identify common misconfigurations**

  tests for presence of known misconfigurations such as use of HTTP instead of HTTPS

- **Intrusive vs. non-intrusive**

  intrusive tests require access to the system (e.g. due to lacking security controls), non-intrusive tests do not attempt access to the system being tested

- **Credentialed vs. non-credentialed**

  user and/or admin credentials may be supplied to the scanner to allow it access to the internals of the system - to see if vulnerabilities exist once an attacker has gained access to the system

- **False positive**

  the scanner has identified a possible vulnerability where none actually exists - all vulnerability scan results should be ground-truthed by an analyst

1.6 Explain the impact associated with types of vulnerabilities.

- **Race conditions**

  the system may process different activities at different times, allowing an attacker to take advantage of settings or information that should no longer be in place - e.g. attacker uploads a valid file, but between the time of upload and the time it is rendered for them, the attacker is able to replace it with a malicious file.

- **Vulnerabilities due to:**
  - **End-of-life systems**
    for a variety of business and technical reasons it may be necessary to retain equipment past the end of its supported life - in this case, it is important to set up up-to-date protections around such a system to prevent exploitation of its outdated system

  - **Embedded systems**

very little security control has been placed in embedded systems, often due to their reduced processing power - the rise of IoT/IIoT makes these vulnerabilities increasingly important

- **Lack of vendor support**
  insufficient support in configuring and maintaining equipment due to lack of vendor support may result in misconfigurations, outdated software and poor security control implementation

- **Improper input handling**

  input should be sanitised to prevent the inclusion of characters and commands that the system may interpret as code instead of data

- **Improper error handling**

  error messages and even differences in timing between successful and unsuccessful actions can provide an attacker with information they require to exploit the system

- **Misconfiguration/weak configuration**

  failure to configure a system with adequate security controls will expose the system to exploitation

- **Default configuration**

  default configurations, and especially default passwords, are easily discovered in product documentation and reverse engineering efforts and can provide an attacker with a backdoor to the system

- **Resource exhaustion**

  the attacker may be able to overload the system to the extent that it hangs or crashes - this may be part of a DoS attack or may be desired to trigger a restart that executes their code or exposes some other vulnerability

- **Untrained users**

  untrained users are the greatest threat to system security - their use and reuse of weak passwords, their exposure to phishing efforts, and their circumvention of security policies, procedures, and equipment provide attackers with many avenues of attack

- **Improperly configured accounts**

  accounts should be configured with as little privilege as the user requires on a daily basis to do their job (principle of least privilege) - service accounts and privileged accounts can be exploited to gain access to sensitive systems and information

- **Vulnerable business processes**

  business processes may also provide attackers with a means to exploit the human side of the system - e.g. failure to gain out-of-bound confirmation for large withdrawal requests by email

- **Weak cipher suites and implementations**

  use of weak and outdated encryption may allow an attacker to easily decrypt sensitive traffic

- **Memory/buffer vulnerability**

  - **Memory leak**
    a flaw in the software causes a section of memory to be exposed to the attacker - may be improper error handling or a flaw that outputs memory directly

  - **Integer overflow**
    the result of an arithmetic operation exceeds the allowed size of the integer variable storing it - may provide access to areas of memory beyond those intended for the storage of a valid result

  - **Buffer overflow**
    a flaw in the software that allows the attacker to write more data than is expected into an area of memory - may cause the program to crash, leak memory, or access other sensitive portions of the program or memory

- **Pointer dereference**
  by removing or changing the reference pointer, the attacker may be able to jump to parts of the code that they should not be able to access

- **DLL injection**
  by modifying or replacing required software libraries that are called upon by software and services, the attacker may be able to execute code with the privilege of the executing service/software

- **System sprawl/undocumented assets**

  undocmented or poorly managed assets may become lost or stolen without the organisation's knowledge - if those assets contain sensitive information or access to the system they can be used by an attacker

- **Architecture/design weaknesses**

  the design of the system may not lend itself to strong security - e.g. flat networks, absent DMZs, etc

- **New threats/zero day**

  an exploit or vulnerability that has not been publicly disclosed, yet, and has therefore been available for 0 days - no patches or mitigations will be in place until it is revealed and identified

- **Improper certificate and key management**

  many modern systems rely on PKI (Private Key Infrastructure) to authenticate users, services, and systems - attacker access to the private keys can completely expose the system and its traffic

2.0 Technologies and Tools

2.1 Install and configure network components, both hardware and software-based, to support organizational security.

- **Firewall**
  - **ACL**
    Access Control List - identifies and limits the transmission of certain types of traffic between certain areas of the network and hosts

  - **Application-based vs. network-based**
    - **Network-based (OSI Layer 4)**
      - Filter traffic by port number
      - Encrypt traffic travelling into or out of the network
      - Sometimes performs proxy or router functions

    - **Application-based (OSI Layer 7)**
      - Establish rules and control traffic based on the application used
      - MS SQL server, Twitter and YouTube can each have separate rules

  - **Stateful vs. stateless**
    - **Stateless Firewall**
      - Does not keep track of traffic flows
      - Each packet is individually examined, regardless of its past history
      - Traffic sent outside of an active session will traverse a stateless firewall

    - **Stateful Firewall**
      - Stateful firewalls remember the “state” of a session
      - All packets within a valid session are allowed

  - **Implicit deny**
    - If a packet does not match one of the explicit rules in the ACL, it is dropped by default - it is implicitly denied.

- **VPN concentrator**
    - **Remote access vs. site-to-site** - A remote access VPN is a VPN used by organizations to provide remote network access for employees and other authorized parties. A site-to-site VPN is used to provide a connection between two organization locations.

    - **IPSec**
        - **Tunnel mode** - The more popular way to use IPSec. With this mode the original IP header is encrypted and a new one is created.

        - **Transport mode** - Less-used mode where the IP header is not encrypted, so routing information could be seen by a sniffer.

        - **AH - Authentication Header** - A mostly obsolete protocol that encapsulates authentication and integrity via hashing in IPSec. It does not provide encryption. It takes the payload, TCP and IP headers and puts them through a hash, but if NAT is being used that could change the IP header and be a problem.

        - **ESP - Encapsulating Security Payload** - A protocol that encapsulates both authentication, integrity, and encryption for communicating with IPSec. It takes the payload and TCP header and puts them through a hash, that way it's easier to use NAT.

    - **Split tunnel vs. full tunnel** - With a split tunnel configuration all traffic that is not part of the VPN's network will be routed outside of the encrypted tunnel. With a full tunnel configuration all traffic, regardless of destination, will traverse the encrypted tunnel and the VPN concentrator will route it.

    - **TLS** - An encryption protocol that is used with remote-site VPNs and popular because most routers will have port 443 open for outbound traffic.

    - **Always-on VPN** - A security configuration that prevents traffic from being sent without a VPN. If the VPN is down then access to the Internet or other networks will be cut off until the VPN is working properly.

- **NIPS/NIDS**
    - **Signature-based** - When the system looks for traffic that matches signatures belonging to malicious exploits and techniques.

- **Heuristic/behavioral** - When the system uses AI to identify different attributes that indicate an attack.

- **Anomaly** - When a system looks for something outside of the usual baseline of behavior.

- **Inline vs. passive** - Inline monitoring is when an IPS has direct access to all incoming traffic before it reaches the rest of the network. Passive monitoring is when the system uses port mirroring/Switched port analyzer (SPAN) to look at traffic, and it can't really do much to block the traffic.

- **In-band vs. out-of-band** - And in-band response is when the system is using inline monitoring, spots malicious traffic, and drops it. An out-of-band response is when a system is passively monitoring traffic and sends a TCP RST flag to stop a malicious connection. This doesn't work so well with UDP.

- **Rules** - The criteria set by administrators that determines what happens with specific traffic. There can be thousands of rules relating to traffic and they can be customized into groups.

- **Analytics**
  - False positive - An action that is identified as malicious but is not.

  - False negative - A malicious action that does exist but is not found by the system.

Router

- **ACLs** - Access Control Lists identify interesting traffic and permit or deny it according to the rules in the ACL

- **Antispoofing** - How a router blocks address spoofing attempts. One method is to block all RFC 1918 private addresses on interfaces that are connected to the Internet. Another is to use Reverse Path Forwarding (RPF), which means inbound traffic will only be responded to on the interface it came in on.

Switch

- **Port security** - Protecting switch ports on the network. This can be done by disabling the ports or by using 802.1x authentication. You could also check for duplicate MAC addresses to stop spoofing attempts.

- **Layer 2 vs. Layer 3** - Layer 2 switches are standard switches and layer 3 switches have packet routing capabilities.

- **Loop prevention** - Using STP or RTP to prevent DoS outages caused by broadcast storms and redundant switch links.

- **Flood guard** - When an administrator configures a set number of MAC addresses that can be assigned to each interface to avoid flooding attacks that overwhelm the switch's Content Addressable Memory (CAM).

- **Proxy** - Intermediary systems for which clients separately connect to the destination host.

  - **Forward and reverse proxy**

    - **Forward Proxy**
      - Located on the inside of a network; sits between a workstation and the Internet

      - How it works:
        - User makes a request to a destination on the Internet
        - This request is first sent to the proxy, which forwards the user's request to the intended destination on the user's behalf
        - The destination sends its response back to the proxy (intended for the user), which analyzes the response for security and integrity
        - If everything looks good, the response is forwarded to the user

      - Also has URL filtering functionality
        - If a user requests a URL to a site they're not allowed to visit, the proxy will immediately respond and notify the user that they don't have permission to visit that URL

    - **Reverse Proxy**

      - Sits between the Internet and a server on an internal network
        - Anyone who wants access to an internal service (like a web server) must first connect to the proxy
      - How it works:

        - Proxy receives communication from sources on the Internet
        - Then, the proxy forwards that request to the web server on the source's behalf
        - Web server sends its response to the external source through the proxy, which forwards the response on the web server's behalf
    - Useful as a security device for large network configurations
        - Make sure outside connections are secure before they can communicate with internal resources

- **Transparent** - A transparent proxy does not require a special configuration or modify traffic. A non-transparent proxy is more difficult to implement but it's better for modifying and filtering traffic.

- **Application/multipurpose**
    - Application-based proxies operate at OSI Layer 7
        - Must be specifically written to understand how their associated applications will operate
            - As such, an application proxy may only work with one type of application
                - Ex: HTTP proxy may only work with HTTP-based applications
            - May need to enable additional features or use multiple proxies to support multiple application types

- **Load balancer** - A device that manages traffic and routes it to specific servers. They can provide TCP handshake offloading, SSL handshake offloading, caching, QoS, and prioritization.

    - **Scheduling**

        - Affinity
          Web applications often like to communicate with one server as opposed to being kicked around. Load balancers can assign specific users an affinity to the same server, which is organized through IPs and session ids.

        - Round-robin
          The way traffic is distributed to servers. The standard Round Robin has each server take a turn. A weighted Round Robin allows an admin to

choose servers that will be used more than others, and dynamic Round Robin monitors the load on all of the servers and routes traffic to the server with the lightest load.

- **Active-passive** - When some load balancing servers are active and some are on standby in case one goes offline.
- **Active-active** - When all load balancing servers are active and can be used at any time.
- **Virtual IPs** - A virtual IP address is used for the load-balancing instance where users send their traffic.

● Access point

- **SSID** - Service Set Identifier - The name given to and broadcast by a particular wireless LAN.
- **MAC filtering** - The process of restricting access to a local network based on a list of approved MAC addresses (whitelisting) or banned MAC addresses (blacklisting)
- **Signal strength** - A measure of the broadcast power of a network, measured in dB.
- **Band selection/width** - The frequency at which a WLAN is broadcasting. The two most prevalent bands are 2.4GHz and 5GHz, which can be further subdivided into channels of varying width. Channels with greater width occupy a broader range of frequency. Neighbouring channels can be combined to provide greater throughput. Channel selection in the 2.4GHz range is important due to channel overlap causing interference.
- **Antenna types and placement** - Most antennas are omnidirectional dipole antennas, but parabolic and Yagi antennas can also be used to focus a signal in one particular direction. Should be placed with minimal distance and physical blockage between them and hosts, but centralized enough to not leak outside of the client's work area.
- **Fat vs. thin** - Thin access points are essentially repeaters of a particular broadcast. Fat access points have fuller features, such as support for configuring

ACLs, blacklists, etc.

- **Controller-based vs. standalone** - A standalone access point is not controlled via a wireless controller, meaning that it must be configured by directly accessing that point alone.

- **SIEM -** Security Information and Event Management - gathers logging information into a central database, correlates information from different parts of the network, and alerts on malicious behaviours

  - **Aggregation** - SIEMs normalize and aggregate logs for long-term storage. They often use syslog, a message logging protocol.

  - **Correlation** - How the SIEMs link different data types together.

  - **Automated alerting and triggers** - Along with storing logs, a SIEM also alerts the admin about certain events or actions happening on the network, based on a set of rules.

  - **Time synchronization** - When keeping logs it is very important to make sure all devices are set at the same time to avoid analysis errors. This can be accomplished with NTP.

  - **Event deduplication** - A way of filtering out a log event that happens many times. If a ton of interfaces go down or they are going back and forth between off and on states instead of 100 lines of the same event there will be one line with the event saying it happened 100 times.

  - **Logs/WORM** - With all of the logs a SIEM stores there needs to be a lot of disk space. WORM is Write Once Read Many, a drive technology that protects logs so they can't be overwritten. Like a DVD-R.

- **DLP -** Data Loss Prevention - strategies, software, and hardware that limit what data users can transfer

  - **USB blocking** - Disabling the use of USB external storage to stop data loss or theft. Employees could use a VPN instead for working from home.

    - **Cloud-based** - A DLP mechanism where there is a cloud proxy located between users and the internet that scans every byte, looks at file transfers and blocks certain strings.

    - **Email** - A DLP mechanism which could also be cloud based or on premise. It's a proxy that blocks keywords or quarantines inbound and outbound e-mail to prevent data loss.

- **NAC** - Network Access Control - software that ensures devices connecting to the network meet defined security and patching requirements

    - **Dissolvable vs. permanent** - A permanent agent will be installed on an end user's device and stay there, while a dissolvable agent runs on a end user's device (usually via a link) and is then terminated. Permanent is often used with enterprise-owned devices and dissolvable is often used when the devices do not belong to the enterprise.

    - **Host health checks** - A way to check that a device is in compliance with NAC. If it fails this posture assessment it will be put on a quarantine network where it is given just enough access to fix the issue and try again

    - **Agent vs. agentless** - An agent-based posture assessment takes place on the device while an agentless one is embedded in Active Directory and it is part of the login and logoff process.

- **Mail gateway**

    - **Spam filter** - Any way to filter unsolicited e-mail. With a *whitelist* everything is blocked except for specific e-mail that is allowed. There's *SMTP standards* checking. *Reverse DNS (rDNS)* is used to block mail where the sender's domain doesn't match their IP address. (Which probably means it has been spoofed). *Tarpitting* slows down sessions between an organization mail server and someone else's. *Recipient filtering* blocks all mail not addressed to valid recipients.

    - **DLP** - Gateways often include Data Loss Prevention capabilities - for example, recognising and restricting credit card numbers from being sent out.

    - **Encryption** - A method where the gateway requires encryption. It can encrypt all outgoing mail or only certain data. Can be certificate or password based. Varies from vendor to vendor.

- ## Bridge

  A bridge is a network segregation device that operates at layer 2 of the OSI model. It operates by connecting two separate network segments and allows communication between the two segments and forwards to the correct port based on the layer 2 address on a packet. Separates *collision* domains

- ## SSL/TLS accelerators

  The process of encrypting traffic per SSL/TLS protocols can be a computer-intensive effort. For large-scale web servers, this becomes a bottleneck in the throughput of the web server. Rather than continue to use larger and larger servers for web pages, organization with significant SSL/TLS neds use a specialized device that is specifically designed

- ## SSL decryptors

  Devices that temporarily decrypt TLS traffic on a local network for security reasons, kind of like a TLS proxy. Users on a local network use internal certificates with the decryptor. The decryptor then decrypts the traffic and forwards it by creating its own TLS session to go out to the Internet. Malware likes to hide in encrypted traffic. This allows an internal resource to decrypt it and examine it before it causes too much harm.

- ## Media gateway

  A device that converts traffic between one communications medium to another, like a VoIP network and the PSTN. Important to have security on these devices to avoid fraudulent outbound calls, DoS, or voice mail spying.

- ## Hardware security module

  Cryptography hardware that can handle the extra CPU workload that comes with encryption. Often used in large server environments. Can also be used for key backup and secure storage.

2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

- ## Protocol analyzer

  A protocol analyzer is simply a tool (either hardware or software) that can be used to capture and analyze traffic passing over a communications channel, such as a network.

- ## Network scanners

  A network scanner is a tool designed to probe a network or system for open ports, and hence machines that are on the network

  - **Rogue system detection**
    You should do rogue system detection on a regular basis, which you can do in two ways with a network scanner. First, you can do active scans of the network to detect any devices not authorized. Second, you can do a passive scan via an examination of packets to see if anyone is communicating who is not authorized. Many Wireless LAN Controllers (WLCs) have this functionality built-in to monitor and alert in real-time.

  - **Network mapping**
    Network mapping tools are another name for network scanners. Network mappers are designed to create network diagrams of how machines are connected.

- ## Wireless scanners/cracker

  You can use wireless scanner/crackers to perform analysis of the wireless side of your networks. The scanner can identify hosts and clients and the cracker (such as aircrack) can crack passwords being sent between them.

- ## Password cracker

  Software used to recover stored passwords, by repeatedly comparing passwords against either the account itself (through attempted login) or a stored cryptographic hash of the password. either from a large list of known passwords, or a list generated according to common password format rules.

This can be used to recover passwords for a locked account, or when it has simply been forgotten. You are able to demonstrate that a password is weak if the time it takes to crack it is very low. (if you can crack it, so can someone else).

- **Vulnerability scanner**

  Software that compares scanned servers/endpoints to a list of software with known vulnerabilities. From a defense standpoint, it can be used to quickly assess which servers/software need to be updated on your network, and what known risks there are to not performing those updates.

- **Configuration compliance scanner**

  Tools used to ensure that the network is following pertinent compliance standards.

- **Exploitation frameworks**

  Tools that provide exploits for common vulnerabilities - major open-source tools include the Metasploit Framework, Powershell Empire, Pacu for AWS, SET (Social Engineering Toolkit), and BeEF (Browser Exploitation Framework) - major paid tools include Cobalt Strike and Canvas Immunity

- **Data sanitization tools**

  All user input should be sanitised to remove symbols or strings that could be used to execute code where only data should be provided. Output should also be sanitised to prevent stored malicious code from executing when recalled by a user or service. May also include utilities for removing sensitive data from files (IP addresses, Usernames, Real Names, etc…).

- **Steganography tools**

  Steganography can be identified using tools like hex editors, EXIF tools, and least significant bit analysers. Tools like steghide can be used to hide or extract information from files.

- **Honeypot**

  A computer you intend on being compromised, for the purpose of gathering information on would-be attackers and their Tactics, Techniques, and Procedures.

- **Backup utilities**

  Tools for taking copies of your data and saving them elsewhere (external drives, storage array in your server room, or in the cloud) as a safeguard against ransomware (or just accidental deletions/destructions/corruptions).

- **Banner grabbing**

  Obtaining data on a target machine (Operating System and Version) from “banner” information the target machine hands out upon querying ports. This info can then be cross-referenced against vuln databases (i.e. we know that Apache Struts of version X is vulnerable to Y attack).

- **Passive vs. active**

  - **Active Reconnaissance** - You’re are actually touching their system, examples are vulnerability scans, Nmap, DNS enumeration

  - **Passive Reconnaissance** - Trying to find out information/weaknesses without actually touching their system/network, an example would be google hacking and DNS queries

- **Command line tools**

  - **Ping** - sends ICMP echo requests to verify system is connected to the network and reachable

  - **Netstat** - Lists all of the active TCP and UDP connections from the host to other hosts.

  - **Tracert** - traces the IP path from one host to another, showing each route hop along the route - it sends pings with increasing TimeToLive values - when the TTL reaches 0 (decreases at each hop), most routers will send an ICMP error

back to the sender to let them know - that provides the address of the hop. Some routers will be configured to not return an error to the sender - those hops are termed “black holes” (show up as stars in the tracert output).

- **nslookup/dig** - uses host DNS client to lookup DNS records for specific host or IP, can also search specified DNS server - dig can provide further information about the nameserver providing DNS and can even be used to copy the nameserver’s whole database if it is configured to allow zone transfers.

- **arp** - displays and modifies ARP table information for local host - this displays the MAC and IP addresses of all of the devices it can see on its network

- **ipconfig/ip/ifconfig** - displays current IP and MAC address and network information for PC (ipconfig), Linux (ip/ifconfig) and MacOS (ifconfig)

- **tcpdump** - packet capturing tool - similar to wireshark but without the GUI

- **nmap** - network mapper - maps out the network and services on its machine using ping, TCP handshake, and other communication protocols

- **Netcat** - Enables you to make a connection to any host on any port number or to listen for activity on any port number and see the results. This specific terminal program is unique to Linux, but alternatives for other OSes exist.

2.3 Given a scenario, troubleshoot common security issues.

- ### Unencrypted credentials/clear text

  Unencrypted credentials or cleartext credentials are unfortunately still a common security issue. When credentials are transferred from one machine to another, it is important to protect the transfer of this information from unauthorized observation.

- ### Logs and events anomalies

  Logs, or log files, are an everyday part of computing. What makes log files useful is the exercise of careful discrimination when choosing what is logged. The objective of logging is to record event anomalies. Event anomalies are conditions that differ from expected outcomes

- ## Permission issues

  Human error can cause permissions on a resource to be too restrictive or too permissive, resulting in loss of effort or data exposure.

- ## Access violations

  An access violation occurs if users access materials that they shouldn't.

- ## Certificate issues

  Certificates are means for carrying public keys and vouching for their authenticity. A common certificate issue is when a user attempts to use a certificate that lacks a complete chain of trust back to a trusted root, leaving the certificate hanging without any means of validation

- ## Data exfiltration

  Data is the primary target of most attackers. The value of the data can vary, making some data more valuable and, hence, more at risk of theft. Data exfiltration is where an attacker attempts to steal a copy of your data and export it from your system

- ## Misconfigured devices

  Misconfigured devices represent one of the more common security issues and can go completely unnoticed. Many security controls depend upon a properly configured device to function properly.

  - **Firewall** - Firewalls essentially are devices to enforce network access policy. Using a set of rules, a firewall either allows or blocks passage of packets. The key is the ruleset.

  - **Content filter** - Content filters are used to limit specific types of content across the Web to users. A common use is to block sites that are not work related, and to limit items such as Google searches and other methods of accessing content determined to be inappropriate.

  - **Access points** - Access points are the first line of defense, where access to a network is either granted or denied. Access points, whether RJ-45 physical jacks

or wireless, need a method of determining entry criteria, before allowing access to network resources.

- **Weak security configurations**

  Weak security configuration refers to the choice of a set of configuration parameters associated with a software application or operating system that results in greater than necessary security risk.

- **Personnel issues**

  - **Policy violation** - When employees violate policies that were agreed to. This could mean violating AUPs, NDAs, or other contracts.
  - **Insider threat** - When someone inside an organization tries to cause harm.
  - **Social engineering** - The psychological manipulation used to persuade employees to comply with requests that are malicious.
  - **Social media** - When employees publicly share information that could cause harm or assist an attacker.
  - **Personal email** - When employees use their personal email for work purposes or when they use their work email for personal business.

- **Unauthorized software**

  When network users download or use software that poses a security risk**.**

- **Baseline deviation**

  When a network or devices on a network are not acting normally and there are anomalies.

- **License compliance violation (availability/integrity)**

  When a license of a crucial application is violated in some way, which could lead to legal action or the application not working for users**.**

- **Asset management**

  When there is no inventory of devices or services that are used on a network. Can happen when administrators don't know about servers that are running or what hardware devices are being used (“shadow IT”).

- **Authentication issues**

  When authentication methods are vulnerable to exploits, are unencrypted, or will not allow users to access a system**.**

2.4 Given a scenario, analyze and interpret output from security technologies.

- **HIDS/HIPS**

  HIDS/HIPS relies on a learning pattern for both known and unknown types of malicious. activity. Rather than relying on signature matching for specific attacks, the behavior-based rules associated with HIDS/HIPS products monitor and deny malicious activity patterns

- **Antivirus**

  Malicious software, including viruses, is identified by signature detection (file hash matches hash of known malware) or by suspicious system behaviour (e.g. spawns new process, access registry keys, begins encryption processes, etc). Sandboxed environments may be used to activate and detect malware activity safely before allowing the user to access the file.

- **File integrity check**

  File integrity checks are done using a variety of hashing programs including command line tools. Usually you have a collection of known good hashes to compare to make sure the file hasn’t changed.

- **Host-based firewall**

  A Host-based firewall is a firewall located on a host system. Because of the firewall's proximity to a single system, you can tune it to the exact specification of that machine, making it highly specific in its granularity of function.

- **Application whitelisting**

  AWL (application whitelisting) controls the software that is allowed to run on a given system. Any application not specifically whitelisted (noted as safe) and allowed by the administrator is unable to be run.

- **Removable media control**

  Removable media provide a common route for the introduction of malware and the accidental or deliberate export of sensitive data. You should be clear about the business need to use removable media and apply appropriate security controls to its use.

- **Advanced malware tools**

  Advanced malware tools include tools such as Yara, a command-line pattern matcher that looks for indicators of compromise in a system. Yara assists security engineers in hunting down malware infections based on artifacts that the malware leaves behind in memory.

- **Patch management tools**

  Patch management can be a daunting task. Administrators have to consider patches not only for the operating system**,** but also for applications. In an enterprise with multiple machines that have different configurations, the task of maintaining software in a patched state is a significant chore. Patch management tools assist administrators by keeping lists of the software on a system and alerting users when patches become available.

- **UTM**

  Unified threat management (UTM) is a marketing term used to describe all-in-one devices employed in network security**.** UTM devices typically provide a wide range of

services, including switching, firewall, IDS/IPS, anti-malware, anti-spam, content filtering, and traffic shaping.

- **DLP**

  Data loss prevention (DLP) refers to technology employed to prevent transfers of data across an enterprise. Employed at key locations, DLP technology can scan packets for specific data patterns.

- **Data execution prevention**

  Data execution protection (DEP) is the protection of specific memory areas as non executable in a Windows system. Implemented post Windows XP DEP combines with other technologies to prevent attackers from changing the operation of a program through code injection into a data storage location and then subsequently executing the code.

- **Web application firewall**

  A web application firewall (WAF) analyzes at the application layer, allowing a high degree of security tuning and logging based on expected behavior. Requires significant user acceptance testing to deploy properly. If tuned improperly, the application may not function as expected, or vulnerabilities may still be able to be exploited.

2.5 Given a scenario, deploy mobile devices securely.

- **Connection methods**
  - **Cellular** - Method of communication using radio propagation and wired networks that is used on mobile devices. LTE, LTE-A, 5G.
  - **WiFi** - Method of radio communication to interconnect local networks. 2.4 Ghz and 5Ghz.
  - **SATCOM** - Satellite communications with a transceiver. Can be used for Internet service, but can be affected by weather and possible lagging speed.
  - **Bluetooth** - Radio communication often used for PANs. 2.4Ghz.
  - **NFC -** Short-range radio communication (4cm or less) used with mobile devices. Based on RFID.
  - **ANT** - A proprietary wireless technology often used in fitness products.
  - **Infrared** - Wireless communication that uses infrared light. It is often used for commands, like with a remote control.

- **USB** - A connection protocol for portable devices.

● Mobile device management concepts

- **Application management -** When an MDM restricts what applications can be installed on a mobile device.
- **Content management** - When an MDM or organization restricts what content or web sites can be accessed on a mobile device.
- **Remote wipe** - A security mechanism that allows a user to delete all of the data on a mobile device remotely if it should get lost or stolen.
- **Geofencing** - Restricting access or authorization based on the physical location of the user.
- **Geolocation** - Identifying where a user's device is using GPS or wireless network locations - connection from some regions may require greater security measures (e.g. MFA) - connection from unexpected or unrealistic locations (e.g. suddenly jumped from New York to Beijing) may be prevented altogether
- **Screen locks** - Mechanisms that lock the screen until proper authentication.
- **Push notification services** - Services that send an alert to the user's mobile device screen.
- **Passwords and pins** - Methods of authentication used by users of mobile devices.
- **Biometrics -** Another method of authentication that can be used to access a mobile device, often based on the user's fingerprint or face.
- **Context-aware authentication** - A type of authentication that relies on a number of different attributes set by the administrator. These can include location, operating system and IP addresses.
- **Containerization** - A virtualization method of allowing the user to access certain resources in a predetermined virtual environment - containers run only the minimum of required resources and dependencies rather than an entire operating system

- **Storage segmentation -** Segmenting how data is stored on mobile devices and networks. Like in a cloud as opposed to on a phone.

- **Full device encryption -** When a mobile device's disk is encrypted by default in an effort to prevent tampering with the device.

- **Enforcement and monitoring for:**

  - **Third-party app stores** - Being aware of what a user is downloading, or filtering what a user can download to prevent the installation of malicious programs.

  - **Rooting/jailbreaking -** Using 3rd party software to gain root access over a device.

  - **Sideloading** - to prevent malicious DLL libraries from being loaded by services, it is possible to sign the libraries to demonstrate they come from a trusted source

  - **Custom firmware -** Using and installing firmware that was not produced by the manufacturer.

  - **Carrier unlocking -** Refers to the practice of locking cell-network-enabled devices to a particular carrier (AT&T, Verizon, etc). A carrier can unlock a device, removing this restriction.

  - **Firmware OTA updates -** Over the air updates to a mobile device's firmware.

  - **Camera use -** How a camera is used in a restricted environment. Some MDMs will disable cameras in certain areas.

  - **SMS/MMS** - How text messaging is used. MDMs can prohibit texting to stop exfiltration of data from a restricted area. While not recommended, text messages can also be used as an additional authentication factor.

  - **External media** - Any portable media, including phones, digital cameras, or USB disks.

  - **USB OTG** - USB On-the-go - Specification that allows mobile devices to host USB external devices.

- **Recording microphone** - Often MDMs can disable recording of audio in restricted locations.

- **GPS tagging -** metadata within a file containing GPS coordinates, most commonly in photos to show where they've been taken. Monitoring uploads to strip out this metadata before posting is common practice to preserve privacy.

- **WiFi direct/ad hoc -** The ability for mobile devices to communicate over WiFi or other wireless protocols. MDMs can disable this.

- **Tethering -** using one device to share/chain access to a network, most commonly using a cell phone connected to a laptop.

- **Payment methods** - How financial transactions are made and what security mechanisms are being used for payment.

● Deployment models

- **BYOD -** Bring Your Own Device - When an employee's personal device is used in the workplace. Usually minimum requirements must be met, like with a NAC. Employee owns the device. Can be difficult to secure.

- **COPE -** Corporate Owned, Personally Enabled - When a company keeps full control of the device. Information is protected by company policies.

- **CYOD -** Choose Your Own Device - When an employee gets to pick their corporate-owned device.

- **Corporate-owned -** The device is owned and managed by the company, rather than the individual employee. Allows the company greater control over the security of the devices, but carries the expense of ownership. It is also not necessarily preferred by employees who wish to use their preferred device.

- **VDI -** Virtual Desktop Infrastructure - A virtualization environment where applications are completely separated from the mobile device. The device is basically a window. Data is centralized somewhere else, and there is minimal risk if the device is lost.

2.6 Given a scenario, implement secure protocols.

- **Protocols**
    - **DNSSEC -** A protocol that validates DNS responses with public key cryptography. DNSSEC does not provide confidentiality of data; all DNSSEC responses are authenticated but not encrypted.
    - **SSH** - Secure Shell, uses TCP port 22, authenticates entities, provides for encryption - replaces unencrypted Telnet
    - **S/MIME** - Secure/Multipurpose Internet Mail Extensions - standard for signing and encrypting email using public key cryptography
    - **SRTP** - Secure Real-time Transport Protocol - VoIP protocol that provides encryption and authentication, and integrity. It uses AES for encryption, and HMAC-SHA1 is the hash used for integrity.
    - **LDAPS** - LDAP Secure, a directory protocol that is used with Active Directory, which is encrypted with TLS via port 636.
    - **FTPS** - FTP Secure - FTP with SSL/TLS, where there are still command and data channels. SSL command channel is 990 and data channel is 989.
    - **SFTP** - Secure FTP - FTP over SSH - there are not two separate channels as in FTP - all over port 22
    - **SNMPv3** - A more secure version of Simple Network Management Protocol that does not use plain text community strings. Provides confidentiality, integrity, and authentication.
    - **SSL/TLS** - Secure Sockets Layer, Transport Layer Security - Protocol that manages encrypted communication - currently SSL and TLS 1.1 have been deprecated - useful TLS is at version 1.2/1.3.
    - **HTTPS -** A secure HTTP protocol that uses encryption with TLS.
    - **Secure POP/IMAP -** Mail client protocols that use TLS. POP (995), IMAP (993).

- **Use cases**

    - **Voice and video** - Voice and video calls could use SRTP to encrypt traffic and ensure conversations are confidential.

    - **Time synchronization -** NTPSec is a project that is trying to make time synchronization more secure, but it's a work in progress.

    - **Email and web** - Email clients could use POP or IMAP with TLS, or for transferring mail SMTP with TLS could be used. Using a mail gateway that enables encryption is one solution or signatures could be used to ensure integrity.

    - **File transfer** - SFTP can be used in conjunction with SSH to transfer files or FTPS could be used so that file transfers are not shown in plain text.

    - **Directory services** - There is LDAPS or SASL - Simple Authentication and Security Layer - which provides authentication for other protocols.

    - **Remote access -** SSH could be used to encrypt remote sessions.

    - **Domain name resolution** - DNSSEC can be used by a host to make sure that queries are validated - some people have also chosen to use DNS over HTTPS (DoH) and DNS over TLS (DoT) to encrypt their DNS requests for privacy, which causes issues for packet inspection at firewall unless the firewall acts as a proxy (decrypting, inspecting, and re-encrypting the packets)

    - **Routing and switching** - LDAPS can be used for directory services. SSH can be used to remotely log into a network device. And SNMPv3 can be used to get baseline information from the devices.

    - **Network address allocation** - In Active Directory, DHCP servers must be authorized. Some switches will have "trusted interfaces" that are identified as having trusted DHCP servers attached to them. All other interfaces will be blocked to stop rogue DHCP servers. With Cisco this is called DHCP snooping.

    - **Subscription services** - Anti-virus, IPSs, and malware databases all use different methods for constant updates. An administrator might be able to improve security by requiring encryption/setting up encryption with certificates.

3.0 Architecture and Design

3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.

- **Industry-standard frameworks and reference architectures**
    - **Regulatory** - Frameworks that are regulated by a government or trade group.
    - **Non-regulatory** - Frameworks that are suggested but not legally enforced.
    - **National vs. international -** National frameworks and architectures are regulated/suggested in a specific country or nation state, while international ones apply globally.
    - **Industry-specific frameworks -** NIST - National Institute of Standards and Technology. COBIT - Control Objectives for Information and related Technology. ITIL - Information Technology Infrastructure Library.

- **Benchmarks/secure configuration guides**
    - **Platform/vendor-specific guides**
        - Web server - Vendor guides that explain the steps to take to lock down a web server. Don't leak banners or directories, don't have non-privileged accounts with bad file permissions, use certificates, and manage log files.
        - Operating system - Vendor/manufacturer guides that explain how to lock down and harden a user's operating system. Install updates, lock down user accounts, implement password policies, have limited network access and monitoring.
        - Application server **-** Steps a user can take to better secure all the services and hardware used on an application server. Disable all unused services, install updates/patches, use and audit file permissions and access controls.
        - Network infrastructure devices - Any guides that inform an administrator how to lock down and harden all the elements in a network topology. Limit access to the devices, use authentication like 802.1x, and update

firmware.

- **General purpose guides** - Non-specific guides that explain how to operate a network or device in a more secure environment.

- **Defense-in-depth/layered security**
  - **Vendor diversity** - When an administrator purchases devices from multiple vendors as to not have too many devices serviced by the same vendor. That way if there is a problem or vulnerability with one brand of devices it will not affect the entire network.

  - **Control diversity**
    - Administrative - Security controls that are based on policies and procedures.
    - Technical - Security controls that are are implement with technical equipment, hardware and software.

  - **User training** - Providing training to end users and members of an organization to enhance security practices. This would be an administrative control.

3.2 Given a scenario, implement secure network architecture concepts.

- **Zones/topologies**

  - **DMZ** - DeMilitarised Zone - devices are placed in a position between the firewall and the Internet (possibly with their own firewall) to reduce exposure of the network to the Internet while allowing external access to some services (e.g. web server)

  - **Extranet** - A network set up between an internal organization and external entities, such as partners or customers.

  - **Intranet** - the internal network of the organisation (i.e. the LAN or WAN)

  - **Wireless -** A concept where a wireless network topology is secured. Using a WLC for centralized maintenance, using WPA2 encryption, limiting the signal range, using 801.x authentication and not a pre-shared key (PSK).

- **Guest** - A network topology where guest users are segmented on another network away from an organization's internal network.

- **Honeynets** - A network of computers to lure attackers in the same fashion that honeypots are used.

- **NAT -** NAT is a basic proxy and can provide address translation and address filtering to block malicious inbound traffic.

- **Ad hoc**
  Devices associate and communicate with one another directly without central management by a networking device

● Segregation/segmentation/isolation

- **Physical**
  This is the most difficult method but also the most secure. In this method each segment must have its own Internet connection, physical wiring and firewall.

- **Logical (VLAN)**
  - **Hosts can be isolated from each other, restricting lateral movement, while also allowing discrete networks to span and co-occupy multiple switches and routers**
    - Not accepted as a compliant segmentation methodology by PCI-DSS
    - https://www.tylercybersecurity.com/blog/network-segmentation-considerations-for-design

- **Virtualization**
  Some or all of the network endpoints and networking devices are virtualised and networked in software. The flexibility, scalability, and easy of central management makes this a very popular option.

- **Air gaps**
  - A security measure employed on one or more computers to ensure that a secure computer network is physically isolated from unsecured networks. It means a computer or network has no network interfaces connected to other networks

- **Tunneling/VPN**
  - **Site-to-site** - A VPN that is used to provide a connection between two locations.

- **Remote access -** A VPN used by organizations to provide remote network access to employees and other authorized parties

● Security device/technology placement

- **Sensors** - Sensors gather information from network devices that is used for data aggregation and analysis.
- **Collectors** - Proprietary consoles that collect data, they may include correlation engines to compare data.
- **Correlation engines** - A mechanism that analyzes large amounts of sensor data and uses the data to send alerts.
- **Filters** - A tool used to filter packets that can be placed between any source and destination.
- **Proxies** - An intermediate server that can handle both forward and reverse traffic. Often placed in a DMZ or on the perimeter of a server farm.
- **Firewalls** - Placed in DMZ or on the perimeter of a network. Sometimes there are internal firewalls, like if you want to stop users from having access to a data center for example.
- **VPN concentrators** - Placed anywhere between a client and a server, or between to sites.
- **SSL accelerators** - Often used in a DMZ or on the perimeter of a server farm.
- **Load balancers** - Located in a DMZ, or between servers and the Internet.
- **DDoS mitigator** - A service (oftentimes 3rd party) meant to fight DoS attacks and other malicious traffic. They are often located between the Internet and a network. They can be cloud-based or onsite.
- **Aggregation switches** - The middle layer of switches that hold everything together. There's the access layer, the distributed switches, and then the core or backbone.
- **Taps and port mirror** - They can be anywhere on a network where traffic monitoring is needed, and can be software or hardware based.

● SDN

Software Defined Networking - rather than relying on hardware, the network connectivity (i.e. its connections, its routing, its ACLs, etc) is virtualised in software - this is how some on-prem virtual environments and all cloud-based networks are designed and managed

3.3 Given a scenario, implement secure systems design.

- **Hardware/firmware security**
  - **FDE/SED** - Full Disk Enryption FDE - Software programs like BitLocker, FileValut, or Linux Unified Key Setup (LUKS). Self Encrypting Disk SED - Where encryption it is built into the circuitry to encrypt; with SED you don't need the software
  - **TPM** - Trusted Platform Module - Cryptographic processor used for secure boot and attestation services.
    - Persistent memory - Where unique keys are burned into memory during production.
    - Versatile memory -Volatile memory that holds keys and hardware information (when powered off volatile memory goes away).
  - **HSM** - Hardware Security Module - device used for secure key storage, part of load balancer or stand alone box and used as crypto accelerator in large environments.
  - **UEFI/BIOS** - Software used by a device to boot up. These days it comes with a number of features, including password settings, boot order and secure boot.
  - **Secure boot and attestation** - A UEFI setting where only software (OSs, bootloaders) signed with approved keys (from the TPM) are allowed to execute and boot. Guards against any malicious attacks that can happen before an OS boots. Attestation makes sure secure boot is working properly by measuring each step of the boot process and storing it externally, then an attestation service on the remote device will attest that the boot process is secure and no changes have been made.
  - **Supply chain** - Whatever happens from when the device is manufactured to when it arrives at its final destination.
  - **Hardware root of trust** - A source that can always be trusted within a cryptographic system. Like from a TPM.
  - **EMI/EMP** - ElectroMagnetic Interference/Pulse - Data can leak based off of EMI emissions and be used to determine keystrokes. You could also inject EMI for a DoS or to change sensor data and other input.

- **Operating systems**
  - **Types**
    - Network - A system that has specific networking capabilities.
    - Server - A system that is specially made to provide services to hosts.
    - Workstation - A system that is meant to be used as an end device.
    - Appliance - A system that operates different house-hold or industrial appliances.

        - Kiosk - A workstation system that has limited operating capabilities for a specific purpose.
        - Mobile OS - A system that is meant to support portable devices.

    - **Patch management** - The process of keeping patches updated. Planning, testing, and implementing.
    - **Disabling unnecessary ports and services** - Deactivating any ports or services that are not needed on a device.
    - **Least functionality -** Not running any services that aren't crucial to operations.
    - **Secure configurations** - Making sure there are consistent and secure configurations for devices on a network. Often used with security templates.
    - **Trusted operating system** - Any operating systems that are rated no lower than a Evaluation Assurance Level 4 (EAL-4). EAL is a numerical system that rates the security level of technologies and services with respect to the Common Criteria standards.
    - **Application whitelisting/blacklisting** - Allowing or banning certain applications.
        - Application hash - Only certain executables can run.
        - Certificates - An application can run only if it's signed by a vendor, like Microsoft for example.
        - Path to executables - only application executables in certain paths can run
        - Network zone - Applications can only run in particular areas or subnets of a network, like a corporate office network.
    - **Disable default accounts/passwords -** Getting rid of easily guessed passwords and vulnerable accounts.

- **Peripherals**
    - **Wireless keyboards** - Wireless traffic can be sniffed and many keyboards do not use encryption.
    - **Wireless mice** - Wireless traffic can be sniffed and mouse movements are not always encrypted.
    - **Displays** - Electromagnetic radiation or emissions could be used to view images on a screen or eavesdrop through walls. Firmware hacks are also a possibility. Attackers could log info on the screen, or put ransomware on the display.
    - **WiFi-enabled MicroSD cards** - Storage devices that can also communicate over 802.11 and have authentication vulnerabilities or open APIs. Attackers could see files on the card.
    - **Printers/MFDs** - Printers and multifunction devices. Most have local storage and network connectivity. They could be used for reconnaissance with unauthorized access, attackers could use spool files to see what's been printed.
    - **External storage devices** - Exfiltration concerns and vulnerable firmware.

- **Digital cameras** - Exfiltration concerns and vulnerable firmware.

3.4 Explain the importance of secure staging deployment concepts.

- **Sandboxing**

  Used as a tool to isolate discovered attacks and learn about the nature of how these attacks work. May also be used to safely test incoming files for malware triggers and behaviours.

- **Environment**
  - **Development** - Secure environment where code gets written, where a sandbox would be used.
  - **Test** - Where all the pieces get put together, functional tests, QA, to see if an application is ready for production.
  - **Staging** - Simulating the real world if an application were live. When it's almost ready for rollout. Performance tests, usability and features.
  - **Production** - When the application is live.

- **Secure baseline** - Making sure an application runs securely. Where the security of an application environment is well defined, with firewall settings, patch levels, and OS file versions.

- **Integrity measurement** - Integrity measurements check for secure baselines and should be performed often, with failure requiring immediate correction.

3.5 Explain the security implications of embedded systems.

- **SCADA/ICS**

  Supervisory Control And Data Acquisition / Industrial Control Systems - ICS networks control industrial processes on plant/factory scale - SCADA systems control ICS network on larger regional/national scales

- **Smart devices/IoT (Internet of Things)**

    - **Wearable technology**
      Examples are smart watches or health monitors. Important things to keep in mind for security are where is the location being stored and who has access to that sensitive data.

    - **Home automation**
      Examples are automated door bell systems, garage door openers, automated lights, etc. These devices are all connected to the internet, and know when the owner is in the house, if someone compromises one of these devices, they could gain access to the entire house.

- **HVAC**

  Heating, ventilation, and cooling systems that are now being connected to the corporate network so that they can automate the controls in the building. This involves third party vendors within the network creating a new risk layer.

- **SoC**

  Stands for System on a Chip where most activities take place in one piece of silicon. With this system, it is hard to do security patches because usually the entire machine needs to be replaced if this is not upgraded from one single chip.

- **RTOS**

  Real-time operating system. This reacts to an input within a certain time frame. Very common within embedded systems.

- **Printers/MFDs**

  Printers and MultiFunction Devices (e.g. printer/scanner/photocopier) are infrequently patched, may have lax security controls, and may have vulnerabilities of their own.

- **Camera systems**

  Cameras might reveal sensitive information and well as intellectual property. They can also function as a pivoting or access point. Often they have outdated certificates, hardcoded default credentials, and other vulnerabilities

- **Special purpose**

  - **Medical devices**
    Devices that can monitor patients in real-time, easily access patient records, and deliver data remotely. Examples are insulin pumps, pacemakers, and MRI machines.

  - **Vehicles**
    Cars are run by code; most cars now have internet connections. This is also software that needs protection.

  - **Aircraft/UAV**
    If a flying device is compromised while in flight, the device could potentially fall out of the sky and cause harm to anyone around. UAVs may also be used to spy on offices, deliver rogue APs into proximity with sensitive floors, etc.

3.6 Summarize secure application development and deployment concepts.

- **Development life-cycle models**

  Ways to go from an idea to a full application.

  - **Waterfall vs. Agile**

    - Waterfall
      Sequential design process, step one to step two, etc. Framework: document requirements, analyze models, pick software architecture to design, code the application, test it and then install and support.
    - Agile
      Perform tasks simultaneously, working together and communicating. Get code completed quickly, then evolve it. Lots of communication and collaboration between devs and customers, resulting in fast changes.

- ## Secure DevOps

  Combining the development and operations units, everyone is a part of one team and more deployments can be met in a shooter amount of time.

  - **Security automation -** Integrate with automated tests, less manpower and can be set early on in process to test against known vulnerabilities and penetration tests

  - **Continuous integration -** Code is constantly generated, so need a base set of security baseline checks to catch issues during development. Full security analysis is run during testing.

  - **Baselining -** Basic set of security checks, a bare minimum that can be used to catch anything during development.

  - **Immutable systems -** Code is put into production and cannot be altered there. Changes can only be made in development, and sent to production following testing and validation.

  - **Infrastructure as code -** Software in the cloud, relying on automation to roll out software. Instead of deploying hardware and software, deploy everything virtually so the organization can focus on the application's needs, and you know what security tools are needed.

- ## Version control and change management

  - **Version Control -** Able to track changes made and the ability to revert to a previous version. Identify modifications made to important files. Confidential data is contained in previous versions, so bad actors could access this to gather information or earlier versions of files.

  - **Change management -** A formal process for managing change; Avoid downtime, confusion, and mistakes. Plan for a change, estimate the risk associated with the change, have a recovery plan if the change does not work, test before making the change, document all to get approval and implement the change.

- ## Provisioning and deprovisioning

    - **Provisioning -** Making something available. For example, deploying an application. With that we will need to provision a web server, a database server, a workstation, certificates and other necessary components. Security components will need to be added as well (firewall rules, VLAN configurations, or up to date VPN access)

    - **Orchestration -** A way of provisioning through automation via the cloud. Application deploys in a click of a button and no need to deploy any physical servers. All security components are deployed through automation as well.

    - **Follow-The-Sun -** Instances of applications can be provisioned around the world as needed - only paying for resources as needed. At daytime the application is provisioned, at night time it is deprovisioned.

    - **Deprovisioning -** Just as important as provisioning, it is the process of removing an application. We want to completely dismantle the product. We want to make sure we do not leave any open holes and close any holes we made initially. Basically remove the rules we created during the provision of the application.

- ## Secure coding techniques

    - **Proper error handling** - Errors must not provide more information than is strictly necessary to diagnose the problem. Improper error handling reveals information to attackers (e.g. username is valid but password is wrong, version information of server, etc.) that they can exploit

    - **Proper input validation -** Fix input data before it is handled by the application to make sure it does not have unintended, negative effects, such as being interpreted as code.

    - **Normalization -** The process of standardising input data to its simplest known form to aid in validation/sanitisation

    - **Stored procedures -** On a SQL database queries can be stored. When an application needs output that one of these stored queries can provide, the application sends a call to that query to get what it needs. This avoids the application from making queries that could be manipulated.

- **Code signing -** To sign an individual executable or interpreted code digitally so that users have confidence the code they run is the actual code from the developer.

- **Encryption -** If you can see the source code. You can look for security holes. Development platforms should use encryption. Encrypt important data.

- **Obfuscation/camouflage -** Can be applied to code so that someone viewing the code sees what looks like gibberish.

- **Code reuse/dead code -**
  Code reuse - If the original code that is being reused has a security concern, then using that code will bring that security issue over to the new application.

  Dead code - Code whose results or output are never used in an application. Removing dead code makes the application more secure.

- **Server-side vs. client-side execution and validation**

  Server-side execution and validation - Input validation that uses the server to perform the validation. Regardless of client-side validation, server-side validation should always be performed - proxies allow changes to data after client-side validation.

  Client-side execution and validation - Input validation that is performed by the user's web browser. Client-side validation is primarily about efficiency, by reducing the chance of the server receiving invalid data and wasting cycles processing and returning an error - this can be done more efficiently on the client side. Client-side validation does not replace server-side validation.

- **Memory management -** Never trust input data. It should be sanitized and checked. Ex: Buffer overflows, some built in features aren't as secure as they could be, so write code to take care of potential security concerns.

- **Use of third-party libraries and SDKs -** These libraries and SDKS could have security vulnerabilities in them.

- **Data exposure -** This needs to be taken into account when developing an application and it should be limited.

- **Code quality and testing**
    - **Static code analyzers -** A tool that simply read through the source code trying to document security vulnerabilities.
    - **Dynamic analysis (e.g., fuzzing) -** Send random input to an application to see if it can handle the data or have any other problems.
    - **Stress testing -** Determines what happens on your web site when greater numbers of users access the site.
    - **Sandboxing -** Test environment looks and works exactly like production. No production systems are used and no production data is used. You can overload and try to break the sandbox environment instead of your actual production systems.
    - **Model verification -** A test used to ensure that the projected application meets all specifications at that point.

- **Compiled vs. runtime code -** Compiled code is high-level instructions (more human-readable) that has been converted in advance to low-level machine language (i.e. binary). Run-time code is also high-level instructions, but they are converted to machine language on the fly at the time of running. Compiled code runs faster at the time of execution, but is less accessible (changes require source code and recompiling for the intended CPU architecture).

3.7 Summarize cloud and virtualization concepts.

- **Hypervisor**

    - **Type I -** hypervisor that is actually an OS that sits on top of a bare metal server. This provides the best performance for large environments. Examples include ESXi, MSFT Hyper-V and VMware vSphere.

    - **Type II -** hypervisor that is installed on top of an existing OS such as Windows, Linux or MacOS. Typically seen in smaller environments. Examples of Type II hypervisor include Oracle VirtualBox, Parallels for Mac and VMware Workstation

    - **Application cells/containers -** Application cells are virtualized containers. They can be thought of as very simple virtual machines. However, containers do not

run/mimic a full OS. Rather, they have enough functionality to run a program or function.

- **VM sprawl avoidance**
  - Ref:https://thwack.solarwinds.com/t5/Geek-Speak-Blogs/Strategies-for-Avoiding-VM-Sprawl-at-Your-Agency/ba-p/496156
  - Define processes and policies that include steps such as defining authority for the creating of VMs that are proportionate to the business need. Also, create a second line of defense in Operations to ensure order in a production environment.

- **VM escape protection**
  - **VM escape protection** - To prevent attackers from accessing the underlying hypervisor make sure that the hypervisor is properly updated and patched.

- **Cloud storage**

  Is a method of storing data in a remote location with access via the internet.

- **Cloud deployment models**
  - **SaaS** - Software as a Service. Running on top of IaaS and PaaS. SaaS is a method of software delivery where the software is accessed online via subscription rather than bought and installed on individual computers. Most of the security responsibility is borne by the Cloud Service Provider (CSP) - client mostly just needs to ensure strong passwords and least privileges are used.
  - **PaaS** - Platform as a Service. Running on top of IaaS. PaaS allows complete development and deployment in the cloud of products from simple cloud based apps to enterprise level applications. An intermediate amount of security responsibility is borne by both the client and CSP - client responsible for security of the code they develop and run on the platform
  - **IaaS** - Infrastructure as a Service. Is instant computing infrastructure(server, storage and networking) created and provisioned over the internet - much more responsibility for security rests on the client - similar to responsibility of on-prem infrastructure, but not most of the physical security.

- **Private** - Private cloud consists of computer assets owned by just one company.
- **Public** - Public cloud is a term for cloud computing service offered to anyone over the public internet.
- **Hybrid** - Hybrid cloud is a term used to describe a cloud computing environment in which some combination of private cloud, public cloud, and/or on-premises infrastructure are used together.
- **Community** - Community cloud is a cloud infrastructure shared by several organizations.

● On-premise vs. hosted vs. cloud

With an On-premise solution you purchase the compute infrastructure & sw licenses. Also, you maintain the hardware and software. With a cloud solution you pay a fee (ex user/per month) and the cloud solution provider maintains the hardware and software. A hosted solution lies in the middle. You purchase and maintain the software. In the hosted solution someone else provides the server on which the software runs.

- **VDI/VDE**
  VDI - Virtual Desktop Infrastructure/Virtual Desktop Environment is a technology that supplies hosted desktop images to remote users from a central server.

- **Cloud access security broker**
  - Ref: https://www.skyhighnetworks.com/cloud-security-university/what-is-cloud-access-security-broker/
  - Cloud access security brokers (CASBs) are on-premises or cloud-hosted software that sit between cloud service consumers and cloud service providers to enforce security, compliance, and governance policies for cloud applications. CASBs help organizations extend the security controls of their on-premises infrastructure to the cloud.

- **Security as a service**
  - Security as service - is a delivery method to deliver cybersecurity services via the cloud, including remote log storage. Remote SIEM, and remote SOC monitoring.

3.8 Explain how resiliency and automation strategies reduce risk.

- **Automation/scripting**
    - Automated courses of action **-** When there are many automated tasks happening in a cloud. This includes orchestration.
    - Continuous monitoring **-** Because there are so many tasks it's important to continuously monitor and audit them.
    - Configuration validation **-** It's important to audit the automated tasks to make sure they are configured correctly and do not pose security risks.

- **Templates**

  Templates are preconfigured master copies of virtual machines (VM) that can be used for multiple VM deployments. They preserve the VM configurations, which are assigned for specific purposes and which can be based on the organization's parameters or on industry standards.

- **Master image**

  Scripts typically start with a master image, also known as golden or parent image, which is a copy of the reference system (such as the operating system and the enterprise-wide components and settings). Master images can be applied to both physical environments (e.g., hard disks and servers) and virtual ones (e.g., a virtual machine or virtual desktop).

- **Non-persistence** - The cloud is always in motion and changing and can be a non-persistent environment.
    - Snapshots **-** Help capture current configurations of data during an application/cloud instance.
    - Revert to known state **-** Snapshots can be used to go back to a known state in a cloud environment.
    - Rollback to known configuration **-** Snapshots can be used to go back to a previously known state in a cloud environment.
    - Live boot media **-** Snapshots can also be used to run instances on live boot media.

- **Elasticity**

  Elasticity is the ability to reduce or expand resources dynamically as the loads change. It's different from scalability because you can automatically and quickly scale both in and out.

- **Scalability**

  Scalability can be vertical, scaling up within the system by making the existing machine or system more powerful; or it can be horizontal, which means scaling out by adding more nodes or systems. Scalability is one of the key benefits of cloud computing and allows an organization to meet its expected demands.(https://resources.infosecinstitute.com/category/certifications-training/securityplus/sec-domains/architecture-and-design-in-security/how-resiliency-and-automation-strategies-reduce-risk/)

- **Distributive allocation**

  Distributive allocation refers to how system resources (storage, processing power, etc.) are spread across multiple servers.

- **Redundancy**

  Redundancy is the presence of multiple identical instances of data, mass storage, systems, or networks to ensure that these resources can be available if the primary instance fails.

- **Fault tolerance**

  The ability of a system to continue operating in the event of failure of some of its components.

- **High availability**

  High availability systems are able to provide a particular level of performance (typically uptime) for a greater-than-normal period. Availability can refer to the user's ability to obtain a good/service, submit new work, update existing work, or simply access the system.

- **RAID**
  A common strategy for fault tolerance is RAID, which is an acronym for redundant array of inexpensive disks. RAID takes several disk drives (hard drives) and organizes them into one logical unit. There are different types, or levels, of RAID, with each configuration providing a different type of redundancy. For example, level 1 RAID achieves fault tolerance — it mirrors data to a second disk, providing a hundred percent redundancy.

3.9 Explain the importance of physical security controls.

- ## Lighting

  Lighting can be an effective deterrent against nighttime threats. Should be placed along perimeters, gates, door entrances, foyers, entryways, and sidewalks. Effective lighting also increases the value of footage from security cameras.

- ## Signs

  Signage can both deter would-be intruders and provide important safety information to employees, such as the location of hazards or exits.

- ## Fencing/gate/cage

  A substantial physical deterrent that demarcates the entry/exit points to a facility. Clearly defined entry/exit points increase an organization’s control over who enters/exits a facility.

- ## Security guards

  Human guards can make split-second, intelligent decisions to react to live threats that can cover a broader range of scenarios than an automated solution. However, they require extensive training and equipment to do their job effectively and are vulnerable to social engineering attacks.

- ## Alarms

  Alert organizations to the presence of an intruder, allowing security personnel to respond to and subdue the threat.

- ## Safe

  Allows for secure storage of sensitive materials, but can be vulnerable to lockpicking, cutting, or physical removal from the facility.

- **Secure cabinets/enclosures**

  A physical barrier to prevent unauthorized physical access to servers and other sensitive computing/networking equipment.

- **Protected distribution/Protected cabling**

  An aspect of facility design that ensures that cables cannot easily be severed, damaged, or eavesdropped upon. The facility design should also be such that termination points and end-user connection points are also protected from unauthorized physical access.

- **Airgap**

  "The concept represents nearly the maximum protection one network can have from another (save turning the device off). The only way to transfer data between the outside world and the air-gapped system is to copy data on a removable storage medium such as a removable disk or USB flash drive and physically carry the storage to the other system." https://en.wikipedia.org/wiki/Air_gap_%28networking%29

- **Mantrap**

  A small room or compartment with two individually locked doors. Individuals are intended to enter a mantrap one at a time, with the entry door locking upon entry. The exit door will only unlock once the user has been authenticated and authorized.

- **Faraday cage**

  "Faraday cages, more specifically dual paired seam Faraday bags, are often used in digital forensics to prevent remote wiping and alteration of criminal digital evidence." (https://en.wikipedia.org/wiki/Faraday_cage/) - Faraday cages prevent radio signals from entering or leaving an area

- **Lock types**

  Locks can be generally divided into mechanical locks (including combination locks, padlocks, and device locks) and electronic locks (PIN-based locks, which can be integrated into a biometric or smart card system).

- **Biometrics**

  A physical authentication method that can include thumbprint scans, palm scans, voice recognition, or retinal/iris scans. Often used as part of a multifactor authentication

scheme.

- **Barricades/bollards**

  A physical block to prevent unauthorized access to a facility. Bollards are individual poles that typically surround parking lots and drive-through areas to prevent vehicles from exiting those parts of the perimeter.

- **Tokens/cards**

  A form of authentication typically using RFID, barcodes, or other physical coding on the card to provide information regarding an individual's identity.

- **Environmental controls**

  - **HVAC** - Heating, Ventilation, and Air Conditioning - The systems that regulate the heat and air quality of a facility to ensure that humans and devices can function properly.

  - **Hot and cold aisles** - Aisles of equipment racks in a facility that alternate between hot aisles (where hot air is pulled away from them) and cold aisles (where cooler air is blown into equipment).

  - **Fire suppression** - A combination of smoke alarms, temperature sensors, sprinklers, or foam-dispensing systems used to mitigate fire damage to a facility, its personnel, and equipment.

- **Cable locks**

  A device-level lock that typically loops secures the device against a sturdy or difficult-to-move object to prevent easy theft.

- **Screen filters**

  A thin filter placed over a screen that narrows the field of vision on that screen in order to mitigate shoulder surfing.

- **Cameras**

  Video surveillance systems (closed-circuit television) that record video and transmit it to central monitoring stations. Often integrated with motion sensors, alarms, and security personnel.

- **Motion detection**

  A security system, often using light beams, to trigger an alarm based on motion in a given area.

- **Logs**

  Records of security-relevant events occurring on a host system.

- **Infrared detection**

  A motion detection system that uses beams of infrared light. When that beam is disrupted, the alarm is triggered.

- **Key management**

  The ability of an organization to manage digital authentication via cryptographic keys and digital certificates. The management process involves reissuing, suspending, revoking, renewing, creating, and destroying these keys.

4.0 Identity and Access Management

4.1 Compare and contrast identity and access management concepts.

- **Identification, authentication, authorization and accounting (AAA)**
    - **Authentication** - the process used to uniquely identify an individual account
    - **Authorization** - the rights and capabilities of each identified account
    - **Accounting** - logging each access and action taken by individual accounts

- **Multifactor Authentication**
    - **Something you are** - The use of unique physical characteristics to identify and authenticate a person (known as the inherence factor).
    - **Something you have** - The use of a physical object for authentication, including cards or tokens (known as the possession factor).
    - **Something you know** - The use of something that only one individual should know for authentication, such as a username/password or a security question (known as the knowledge factor).
    - **Somewhere you are** - The use of physical locations (e.g. requiring a user to authenticate from a specific room) or logical locations (e.g. requiring authentication from a certain device with a certain digital cert) to authenticate a user (known as the location factor).
    - **Something you do** - The use of a physical action (e.g. drawing a pattern) to authenticate a user.

- **Federation**

  The use of a common authentication system and credentials database across multiple entities.

- **Single sign-on**

  The use of a single set of user credentials to access resources across an enterprise.

- **Transitive Trust**

  An indirect method of authentication in scenarios with more than two entities. In a transitive trust relationship, when entity A trusts entity B's authentication system, entity A will also trust the authentication systems of any entity trusted by entity B.

4.2 Given a scenario, install and configure identity and access services.

- **LDAP**

  Lightweight Directory Access Protocol, a hierarchical directory information system, is an application protocol working with IP networks to manage a distributed information service.

- **Kerberos**

  Windows authentication protocol for AD - uses shared secrets for auth -> NTLM hash (password hash for account) - to authenticate to anything you need a TGT (ticket-granting ticket)

- **TACACS+** - Terminal Access Controller Access Control System - Similar to RADIUS. Family of protocols that support authentication. TACACS+ is the latest version. It is not backwards compatible with other protocols.

- **CHAP**

  Challenge Handshake Authentication Protocol, sends a challenge to a client: the client encrypts the challenge using its password as the key and sends the ciphertext by decrypting the challenge with the user password.

- **PAP**

  Password Authentication Protocol authenticates passwords in clear text.

- **MSCHAP**

- **RADIUS**

  Remote Authentication Dial-In User Service (RADIUS) is a networking protocol, operating on port 1812, that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. https://en.wikipedia.org/wiki/RADIUS

- **SAML**

- **OpenID Connect**

- **OAUTH**

- **Shibboleth**

- **Secure token**

  A small hardware device that the owner carries to authorize access to a network service. It could be a smart card or embedded in a commonly used object like key fob. A secure token provides an extra layer of protection using two factor authentication.

- **NTLM**

4.3 Given a scenario, implement identity and access management controls.

- **Access control models**
    - **MAC**
        - MAC - Mandatory Access Control
        - Operating system limits the access a user has to a particular object
            - Access limits are based on clearance levels
        - Every object that someone may need to use is assigned a label
            - Ex: Confidential, Secret, Top Secret, etc.
                - Each user's access rights are directly related to the level associated with their account
        - Clearance levels are assigned by an administrator
            - Users cannot change their own access level
    - **DAC**
        - DAC - Discretionary Access Control
        - Commonly used with shared documents like Google Docs or spreadsheets
            - The document owner determines who else can have access to the document and also what type of access they have
            - Very flexible; the owner can modify access rights at any time
        - Although DAC is flexible, the owner is the single point-of-failure
            - They are responsible for setting up proper security features and managing access
    - **ABAC**
        - ABAC - Attribute-based Access Control
        - Determine access rights based on application use and the data used within that application
            - Called the next generation of authorization due to its context awareness
        - Evaluate and combine multiple parameters to determine access rights
            - IP address, time of day, geographical location, etc.
    - **Role-based access control**
        - Broader form of access control based on the person's role in the organization

        - Manager Director, Team Lead, Project Manager, etc.
    - An administrator determines the level of access assigned to a particular role
        - They can also configure implicit access rights
            - If an admin provides access of an object to Managers, and Directors are also included in the Managers group, Directors will also have access to that object
    - Commonly implemented in Windows using Windows Groups

- **Rule-based access control**
    - Access is based on a set of predefined rules; usually set by an administrator
    - Firewalls are a good example of rule-based access control
        - Examples of firewall access rules
            - Allow network access to the lab during business hours; deny access at all other times
            - Only allow Chrome-based browsers to access and complete a particular web form

Physical access control

- **Proximity cards**
    - Card containing a close-range reader, such as RFID
        - Passive device; usually powered by a proximity reader
    - No large data storage inside the card itself
        - A small chip on the card contains ID data, but authentication data used by the reader is stored elsewhere

- **Smart cards**
    - More intelligent cards containing an integrated circuit
        - Can physically connect to a device (like a chip reader slot)
        - Can also be contactless
    - Smart cards may contain a digital certificate as an authentication factor
        - Can be combined with a PIN, biometric or other authentication factor to support 2FA or multi-factor authentication
    - Many modern credit cards have smart card technology

Biometric factors

- **Fingerprint scanner** - Evaluates one or more of the person's fingerprints

        - Usually, fingerprint data is stored as a mathematical representation of the fingerprint rather than the actual pattern

    - **Retinal scanner** - Evaluates the unique capillary structure in the back of the eye

    - **Iris scanner -** Evaluates the texture and color of the iris

    - **Voice recognition -** Evaluates the person's voice; Sometimes called a "voiceprint"

    - **Facial recognition -** Evaluates facial shape and unique features

    - **False acceptance rate** - Likelihood that an unauthorized user will be accepted

    - **False rejection rate** - Likelihood that an authorized user will be rejected

    - **Crossover error rate** - Used to quantitatively compare biometric systems
        - Goal: Adjust sensitivity/configuration of the biometric system to equalize both FAR and FRR values

- **Tokens**
    - **Hardware -** physical device that generates the token - e.g. a Yubikey.

    - **Software**

    - **HOTP/TOTP**
        - HOTP - HMAC-based One-Time Password
            - HMAC - keyed-Hash Message Authentication Code
                - Calculated based on a secret key and an **incremental** counter
            - A form of token-based authentication
                - The calculated hash is a different result each time
            - A combination of hardware and software is required to implement HOTP

        - TOTP - Time-based One-Time Password
            - Determined using a secret key and a **timestamp** counter
                - Secret key is configured ahead of time
                - Timestamp counter changes every 30 seconds
                    - Timestamps are synchronized by NTP

        - Each time the timestamp counter changes, a new TOTP is generated
    - More commonly used OTP method
        - Used by Google, Facebook, BattleNet, Twitch, etc. for 2FA

- **Certificate-based authentication**

    - **PIV/CAC/smart card**
        - Smart cards can contain a digital certificate which authorizes the user
            - PIV (Personal Identity Verification Card)
                - Smart card used by the U.S. Federal Government
            - CAC (Common Access Card)
                - Smart card used by the U.S. Department of Defense
            - Both PIVs and CACs contain the person's picture and ID information on the outside of the card; stored digital certificate inside the card

    - **IEEE 802.1x= Authentication for port-based network access control includes EAP.**

- **File system security**

- **Database security**

4.4 Given a scenario, differentiate common account management practices.

- **Account types**

    - **User account**
      A user level account often prevents the installation of new applications, changes to global settings or rules, and limits other functions or files, focusing on core business functionality.

- **anShared d generic accounts/credentials**
  A shared account, sometimes known as a generic account, is one that can be utilized by more than one assigned user. This account type is often used by teams that share similar functions – known as group-based access – or by casual users that need access to a system in a limited capacity.

- **Guest accounts -** used to grant limited access to users who do not have an account, i.e. guests.

- **Service accounts** - Control the privileges and functions of an application.

- **Privileged accounts** - Administrative functions of a system that require global access – whether they be management, maintenance, or monitoring

General Concepts

- **Least privilege**
  - **Only give access needed to operate systems.**
- **Onboarding/offboarding**
- **Permission auditing and review**
- **Usage auditing and review**
- **Time-of-day restrictions**
- **Recertification**
- **Standard naming convention**
- **Account maintenance**
- **Group-based access control**
- **Location-based policies**

Account policy enforcement

- **Credential management**
- **Group policy**
  - **Users are provisioned as a group of users.**
- **Password complexity**
  Make sure the password is composed of upper letters, lower letters, numbers and special characters
- **Expiration**
  - **Account expires after non-usage**
- **Recovery**
- **Disablement**
  Account disabled after multiple failed attempts. A customer service call is needed to restore access.

- **Lockout**
  Account is locked after multiple failed attempts. Usually 3. The lockout can go from 1 minutes to 24hrs.
- **Password history**
  Verify that the same password hasn't been used in the past year at least.
- **Password reuse**
  New password is not the same as the old password. Some companies test the password use against HaveIBeenPwned to make sure they have not been compromised.
- **Password length**
  Password is at least 10 characters long per recent standard.

5.0 Risk Management

5.1 Explain the importance of policies, plans and procedures related to organizational security.

- **Standard operating procedure**

- **Agreement types**
  - **BPA: Blanket Purchase Agreement.** An Agreement that allows the organization to order and purchase supplies and services from approved vendors multiple times a year.

  - **SLA: Service Level Agreement.** A commitment between service provider and a client. Aspects of the service - quality, availability, responsibilities - are agreed upon between the service provider and client. Services should be provided to the customer as they were agreed upon.

  - **ISA: Interconnection Security Agreement.** An agreement between the organizations that own and operate connected IT systems to document the technical requirements of the interconnection. *Example from NIST Security Guide for Interconnecting Information Technology Systems page A-6*
    "The requirements for interconnection between "Organization A" and "Organization B" are for the express purpose of exchanging data between "System A," owned by Organization A, and "System B," owned by Organization B. Organization B requires the use of Organization A's "XYZ database" and Organization A requires the use of Organization B's "ABC database," as approved and directed by the Secretary of "Agency" in "Proclamation A," dated (date). The expected benefit is to expedite the processing of data associated with "Project R" within prescribed timelines."

  - **MOU/MOA: Memorandum of Understanding Agreement.** The organizations that own and operate the connected systems should establish a Memorandum of Understanding (or Agreement) (MOU/A) (or an equivalent document) that defines the responsibilities of both parties in establishing, operating, and securing the interconnection. This management document should not contain technical details of the interconnection. Those details should be addressed separately in the Interconnection Security Agreement (ISA) *from NIST Security Guide for Interconnecting Information Technology Systems page B-1*

- **Personnel management**
  - **Mandatory vacations:** Good mentally and physically to take time off. Can help develop leaders and it can help spot fraud or other trouble spots before they become too much of a problem.

  - **Job rotation:** Employees move between 2 or more job functions at a company. It helps expose employees to different aspects of the company, cross trains them, and can enhance job satisfaction.

  - **Separation of duties:** Policy where no person is given responsibility for more than 1 related function. Example, the person purchasing items isn't also paying for the same items.

  - **Clean desk:** Policy where employees must clear their desks of all documents, removable media, notes or business cards from their desk. This is to help prevent theft, fraud, or any breaches from information left on desks.

  - **Background checks:** The act of reviewing both public and confidential information to investigate a person's history to make sure they are who they say they are and don't have any history that may reflect poorly on the employer.

  - **Exit interviews:** Interview that should provide candid information from the leaving employee which helps the employer recognize any issues it may not have seen.

  - **Role-based awareness training**: ex vendors: KnowBe4, Ninjio, Security Innovation. Often combined with phishing exercises and training to detect for when being phished/smished.

  - **Data owner:** Entity that can deny or authorize access to certain data, and is responsible for its accuracy, integrity and timeliness. *business dictionary*

  - **Systems administrator:** A person who is responsible for the upkeep, configuration, and reliable operation of computer systems; especially multi-user computers, such as servers. *wikipedia*

  - **System owner:** an organizational official responsible for the procurement, development, integration, modification, operation, maintenance, and disposal of an information system.

- **User**
- **Privileged user**
- **Executive user**
- **NDA:** Non-disclosure agreement
- **Onboarding**
- **Continuing education:** Courses for employees to educate them on advancements in their field of work and help build on their expertise.
- **Acceptable use policy/rules of behavior**
- **Adverse actions**

- **General security policies**
  - Social media networks/applications
  - Personal email

5.2 Summarize business impact analysis concepts.

- **RTO/RPO**
  - **RPO(Recovery Point Objective)** represents a business' acceptable loss (as measured in dollars, terabytes, customer interactions, etc.) during the aftermath of a disaster/setback.
  - **RTO(Recovery time Objective)** describes the amount of time a company has to restore operations after an undesirable event before falling apart (including troubleshooting, recovery, and testing phases).
    - https://toggl.com/business-impact-analysis/

- **MTBF**

  Mean time between failures (MTBF) is the predicted elapsed time between inherent failures of a mechanical or electronic system, during normal system operation.

- **MTTR**

  Mean time to repair (MTTR) is a basic measure of the maintainability of repairable items. It represents the average time required to repair a failed component or device.

- **Mission-essential functions**

- **Identification of critical systems**

- **Single point of failure**

  A single point of failure (SPOF) is a person, facility, piece of equipment, application, or another resource for which there is no redundancy in place. If such a resource goes down, any system or process of which it is an essential part will come to a halt.

- **Impact**
  - Life
  - Property
  - Safety
  - Finance
  - Reputation

- **Privacy impact assessment**

  A Privacy Impact Assessment is a process which assists organizations in identifying and managing the privacy risks arising from new projects, initiatives, systems, processes, strategies, policies, business relationships etc.

- **Privacy threshold assessment**

  The purpose of the Privacy Threshold Analysis (PTA) is to help a company's departments gauge their system's information, and determine how to appropriately treat data that has been acquired by the organization. PTAs primarily focus on two main areas: Business data and business processes within each business unit.

5.3 Explain risk management processes and concepts.

- **Threat assessment**
  - Environmental
  - Manmade
  - Internal vs. external

- **Risk assessment**
  - **Exposure Factor (EF)= The amount or percentage of value that would be lost if a single event occurred.**
  - SLE= Single loss expectancy, the financial value lost when a single security event occurs. SLE is expressed :- SLE = Asset X EF
  - ALE= Annualized loss expectancy, the amount of money expected to be lost by a given event occurring one or more times per year. It is expressed as: ALE = SLE X ARO
  - ARO
    - Annual Rate of Occurrence, that is the average number of times a given security event is expected to occur per year.
      -
  - Asset value
  - Risk register
  - Likelihood of occurrence
  - Supply chain assessment
  - Impact
  - Quantitative risk analysis= Provides a numeric (dollar) values to provide for more exact value of risk.
  - Qualitative risk analysis: Assigns priority levels to risk, such as high, medium or low.
  - Testing
    - Penetration testing authorization
    - Vulnerability testing authorization
  - Risk response techniques
    - Accept = After evaluating risk and possible countermeasures, we accept the risk because the benefits of the practice are great and the cost of the countermeasures exceed the perceived risk value.
    - Transfer= Allowing another entity to handle the risk. For example Insurance.
    - Avoid = Not taking on a project, because the risks are too great.
    - Mitigate = using countermeasure to reduce the risk.

- **Change management**
    - Maintains consistent operational security, by understanding, managing and controlling changes. Best handled through a change control board which evaluates consequences of each proposed change. Change must be submitted, recorded, approved and tested.

5.4 Given a scenario, follow incident response procedures.

- **Incident response plan**
    - Documented incident types/category definitions
    - Roles and responsibilities

      At its core, an IR team should consist of:

        - Incident Response Manager
          The incident response manager oversees and prioritizes actions during the detection, analysis, and containment of an incident.

        - Security Analysts
          Security analysts work directly with the affected network to research the time, location, and details of an incident.

        - Threat Researchers
          Threat researchers complement security analysts by providing threat intelligence and context for an incident. They are constantly combing the internet and identifying intelligence that may have been reported externally.

    - Reporting requirements/escalation

    - Cyber-incident response teams

    - Exercise

- **Incident response process**
    - Preparation
    - Identification
    - Containment

- Eradication
- Recovery
- Lessons learned

5.5 Summarize basic concepts of forensics.

- **Order of volatility**

  Order of volatility refers to the order in which you should collect evidence. Highly volatile data is easily lost, such as data in memory when you turn off a computer. Less volatile data, such as printouts, is relatively permanent and the least volatile**.**

- **Chain of custody**

  Can also be referred to as the forensic link, the paper trail, or the chronological documentation of electronic evidence. It also documents each person who handled the evidence, the date/time it was collected or transferred, and the purpose for the transfer.

- **Legal hold**

  A legal hold, also known as a litigation hold, is the process that must occur to preserve data potentially relevant to anticipated, pending or active litigation, investigations or other legal disputes.

- **Data acquisition**

  The process of making a forensic image from computer media such as a hard drive, thumb drive, CDROM, removable hard drives, thumb drives, servers and other media that stores electronic data including gaming consoles and other devices.
  - Capture system image
  - Network traffic and logs
  - Capture video
  - Record time offset
  - Take hashes
  - Screenshots
  - Witness interviews

- ## Preservation

  The isolation and protection of digital evidence exactly as found without alteration so that it can later be analyzed.

- ## Recovery

  Data recovery typically refers to the process of salvaging data from media that is either corrupted or physically damaged.

- ## Strategic intelligence/ counterintelligence gathering

  - **Strategic intelligence (STRATINT)** pertains to the collection, processing, analysis, and dissemination of intelligence that is required for forming policy and military plans at the national and international level. ... Understanding what motivates people is based upon another ability, personality intelligence

  - **Counterintelligence** is an activity aimed at protecting an agency's intelligence program against an opposition's intelligence service. It likewise refers to information gathered and activities conducted to counter sabotage or other intelligence activities

  - **Active logging** - an active logging strategy can help an organization gather a significant amount of data on attackers. An active logging strategy increases the amount of logged data collected on a routine basis.

- ## Track man-hours

  A man-hour is the amount of work performed by the average worker in one hour. It is used for estimation of the total amount of uninterrupted labour required to perform a task. You should document every action taken by end users and the incident-response/investigation teams. This tracking will serve as an audit trail to retrace the actions taken and the events that occurred during the incident.

5.6 Explain disaster recovery and continuity of operations concepts.

- **Recovery sites**
  - Hot site= Fully equipped with near real-time data backup providing for very quick full recovery. Very expensive option.
  - Warm site= Fully equipped with all equipment and applications, but no data providing for MTD of one to three days. Less expensive option.
  - Cold site= A facility that provides no equipment. Least expensive standby facility.

- **Order of restoration**

- **Backup concepts**
  - Differential = Backs up all data changed since last full backup.
  - Incremental= Backup all data changed since last full or incremental backup.
  - Snapshots
  - Full= Backs up all data. (Does not look at archive bit and resets archive bit)

- **Geographic considerations**
  - Off-site backups
  - Distance
  - Location selection
  - Legal implications
  - Data sovereignty

- **Continuity of operations planning**
  - Exercises/tabletop
  - After-action reports
  - Failover
  - Alternate processing sites
  - Alternate business practices

5.7 Compare and contrast various types of controls.

- **Deterrent**
  - **Controls that mitigate risks by discouraging potential attackers.**

- **Preventive**
  - **Taking measures to stop the threat or attack from exposing a vulnerability in the computer system prevention occurs BEFORE the attack occurs.**

- **Detective**
  - **Determination that an event has occurred.**

- **Corrective**
  - **Fixes a system or component after an event has occurred.**

- **Compensating**
  - **Provide an alternative method for controlling a risk. For example if a fence rather than expensive security guards.**
  -

5.7.1: Control Categories

- **Technical =** Also known as logical security controls, technical controls use technology to provide for protection against compromises to confidentiality, integrity and availability.

- **Administrative=** Provide for policies, standards, procedures,guidelines, baselines and all other non technical nor physical control.

- **Physical=** Provide for protection against physical harm such as fire, flood, heat and other environmental controls; provides controls to restrict physical access.

5.8 Given a scenario, carry out data security and privacy practices.

- **Data destruction and media sanitization**
  - Burning
  - Shredding= Preferred method as information is literally impossible to recover from a shredded drive or (other media)
  - Pulping=
  - Pulverizing
  - Degaussing= The process of demagnetizing media using a super strong magnet. Another preferred method.
  - Purging
  - Wiping/overwriting/zeroizing = The process of overwriting media should be overwritten many times (NIST standard is seven times) Another preferred method, particularly when is repurposed.

- **Data sensitivity labeling and handling**
  - Confidential=
  - Private
  - Public
  - Proprietary
  - PII
  - PHI

- **Data roles**
  - Owner
  - Steward/custodian
  - Privacy officer

- **Data retention**

- **Legal and compliance**

6.0 Cryptography and PKI

6.1 Compare and contrast basic concepts of cryptography.

- **Symmetric algorithms**

  encryption that uses a single key to encrypt and decrypt a message. DES, 3DES, AES, BLOWFISH, TWOFISH, RC4

- **Modes of Operation**

- **Asymmetric algorithms**
  - Different key on each side (private/public)

- **Hashing**
  - What is it?
    - Math for Integrity Checking
    - One way operation
  - Uses
    - Verify Passwords
    - Verify Download wasn't tampered with
    - Only Used for Integrity of Files

- **Salt, IV, nonce**

- **Elliptic curve**

- **Weak/deprecated algorithms**

- **Key exchange**

- **Digital signatures**

- **Diffusion**

  Means that a single bit change in the plaintext will cause multiple changes in the ciphertext.

- **Confusion**

  A characteristic of cryptography where the relationship between plaintext and ciphertext is as random as possible. Confusion is provided by substitution.

- **Collision**

  Where two hashes have the same value.

- **Steganography**

  Steganography is the practice of concealing a file, message, image, or video within another file, message, image, or video.

- **Obfuscation**

  Taking something and making it harder to understand or unclear

- **Stream vs. block**

- **Key strength**

- **Session keys**

- **Ephemeral key**

- **Secret algorithm**

- **Data-in-transit**

- **Data-at-rest**

  Data not being transferred, often considered to be less vulnerable, designed to protect inactive data.

- **Data-in-use**

- **Random/pseudo-random number generation**

- **Key stretching**

- **Implementation vs. algorithm selection**
  - Crypto service provider
  - Crypto modules

- **Perfect forward secrecy**

  PFS, is a feature of specific key agreement protocols that gives assurances that session keys will not be compromised even if the private key of the server is compromised.

- **Security through obscurity**

  Security through obscurity is a design that relies on secrecy to remain secure. It is considered a poor practice as truly secure designs could be openly published and remain secure.

- **Common use cases**
  - Low power devices
  - Low latency
  - High resiliency
  - Supporting confidentiality
  - Supporting integrity
  - Supporting obfuscation
  - Supporting authentication
  - Supporting non-repudiation
  - Resource vs. security constraints

6.2 Explain cryptography algorithms and their basic characteristics.

- **Symmetric algorithms**
  - AES : Advanced Encryption Standard,
  - DES : Data Encryption Standard,
  - 3DES
  - RC4 : Stream Cipher, Designed by RSA Data Security
  - Blowfish/Twofish

- **Cipher modes**
  - CBC : “Cipher Block Chaining”
  - GCM
  - ECB
  - CTR
  - Stream vs. block

- **Asymmetric algorithms**
  - RSA : Develops 1024/2048/4096 bit keys [Used in the Transport Layer]
  - DSA : Uses a public key cryptography and a hash function
  - Diffie-Hellman :Uses a shared secret key, over a public insecure channel
    - Groups
    - DHE
    - ECDHE
  - Elliptic curve
  - PGP/GPG

- **Hashing algorithms**
    - Protect (Hash) the data/files
        - Don't do it for password files
            - Keep track of file integrity
                - If a file changes from expected state, Hash won't match anymore

    - **MD5**
      The MD5 message-digest algorithm is a widely used hash function producing a 128-bit hash value. Although MD5 was initially designed to be used as a cryptographic hash function, it has been found to suffer from extensive vulnerabilities. It can still be used as a checksum to verify data integrity, but only against unintentional corruption. Reference: https://en.wikipedia.org/wiki/MD5

    - **SHA**
      The Secure Hash Algorithms are a family of cryptographic hash functions published by the National Institute of Standards and Technology (NIST)
      Reference: https://en.wikipedia.org/wiki/Secure_Hash_Algorithms

    - **HMAC**
      An HMAC (sometimes expanded as either keyed-hash message authentication code or hash-based message authentication code) is a specific type of message authentication code (MAC) involving a cryptographic hash function and a secret cryptographic key. As with any MAC, it may be used to simultaneously verify both the data integrity and the authenticity of a message.
      Reference: https://en.wikipedia.org/wiki/HMAC

    - **RIPEMD**

- **Key stretching algorithms**

  One way to use a stronger type of encryption using this weak key is to send it through multiple processes. So you might hash a password, and then hash the hash of the password, and then hash the hash of the hash of the password, and so on. (https://www.professormesser.com/security-plus/sy0-501/key-stretching-algorithms/)

    - **BCRYPT**
        - A library that will create hashes from passwords by going through multiple rounds of the Blowfish cipher to make that original process much, much stronger.
    - **PBKDF2**
        - Password-Based Key Derivation Function 2

- Library that's part of the RSA public key cryptography standards, and it can also help strengthen or stretch your keys.

- **Obfuscation**
  - **XOR**
    - Exclusive OR
    - A cipher to make data less readable
      - Comparing two different types of input to be able to create a single output. If both of those inputs are different, then we mark them as true. If both of those inputs are the same, then we mark them as false. (https://www.professormesser.com/security-plus/sy0-501/obfuscation/)
  - **ROT13**
    - Rotate by 13 Places
      - A standard form of the Caesar cipher
      - Substitute a letter with the other. For example, URYYB substituted 13 places is the same as hello. (https://www.professormesser.com/security-plus/sy0-501/obfuscation/)
  - **Substitution ciphers**
    - A method of encrypting by which units of plaintext are replaced with ciphertext, according to a fixed system.
      - The "units" may be single letters (the most common), pairs of letters, triplets of letters, mixtures of the above, and so forth. The receiver deciphers the text by performing the inverse substitution. https://en.wikipedia.org/wiki/Substitution_cipher

6.3 Given a scenario, install and configure wireless security settings.

- **Cryptographic protocols**
  - WPA: Wi-Fi Protected Access
  - WPA2: Wi-Fi Protected Access 2
  - CCMP: Counter Mode Cipher Block Chaining Message Authentication Protocol
    - Standard encryption protocol for use with WPA2.

        - Provides: Data confidentiality, Authentication, & Access Control.
    - TKIP: Temporal Key Protocol

- **Authentication protocols**
    - EAP = Extensible Authentication Protocol, a framework describing many different authentication protocols, provides port-based authentication at Layer 2.
    -
    - PEAP = (Protected Extensible Authentication Protocol) provides for secure authentication data, including outdated password-based protocols, via 802.11 Wi-Fi networks.
    - EAP-FAST
    - EAP-TLS
    - EAP-TTLS
    - IEEE 802.1x
    - RADIUS Federation

- **Methods**
    - PSK vs. Enterprise vs. Open
    - WPS
    - Captive portals

6.4 Given a scenario, implement public key infrastructure.

- **Components**

    - **CA: Certificate Authority**
        - Verifies that an organization has control over a domain

    - **Intermediate CA: Intermediate Certificate Authority**
        - Supplies chaining to a trusted root CA Certificate

    - **CRL: Certificate Revocation List**
        - List of digital certificates revoked by the issuing CA before their scheduled expiration

    - **OCSP: Online Certificate Status Protocol**
        - Used for obtaining the revocation status of a X.509 digital certificate
        - Alternative to CRL

- **CSR: Certificate signing request**
  - Message sent from an applicant to a certificate authority in order to apply for a digital identity certificate.

- **Certificates**
  - Small data file to bind cryptographic key to an organization/site.

- **Public key**
  - One half of a key pair. It is distributed as part of your ssl certificate. Anyone with the public key can verify that the digital signature is authentic without knowing the private key.

- **Private key**
  - One half a key pair. This key is secret and stays with the key initiator.

- Object identifiers (OID)

Concepts

- Online vs. offline CA
- Stapling
- Pinning
- Trust model
- Key escrow
- Certificate chaining

Types of certificates

- Wildcard: a wildcard certificate is a public key certificate which can be used with multiple sub-domains of a domain.
- SAN
- Code signing
- Self-signed
- Machine/computer
- Email
- User
- Root
- Domain validation
- Extended validation

- **Certificate formats**
    - https://blogs.getcertifiedgetahead.com/understanding-certificate-formats/
    - https://knowledge.digicert.com/generalinformation/INFO4448.html

    - DER
        - Distinguished Encoding Rules
            - A format specifically designed for X.509 certificates.
            - The DER format is the binary form of the certificate
            - All types of certificates & private keys can be encoded in DER format
            - Do not contain the "BEGIN CERTIFICATE/END CERTIFICATE" statements
            - DER formatted certificates most often use the ‘.cer’ and '.der' extensions
            - DER is typically used in Java Platforms

    - PEM
        - Privacy Enhanced Mail
            - It is the most common format used for certificates
            - Most servers (Ex: Apache) expects the certificates and private key to be in a separate files
            - Usually they are Base64 encoded ASCII files
            - Extensions used for PEM certificates are .cer, .crt, .pem, .key files
            - Apache and similar server uses PEM format certificates

    - PFX
    - CER
    - P12
    - P7B

Security+ Acronyms

Acronym	Spelled Out
3DES	Triple Digital Encryption Standard
AAA	Authentication, Authorization, and Accounting
ABAC	Attribute-based Access Control
ACL	Access Control List
AES	Advanced Encryption Standard
AES256	Advanced Encryption Standards 256bit
AH	Authentication Header
ALE	Annualized Loss Expectancy
AP	Access Point
API	Application Programming Interface
APT	Advanced Persistent Threat
ARO	Annualized Rate of Occurrence
ARP	Address Resolution Protocol
ASLR	Address Space Layout Randomization
ASP	Application Service Provider
AUP	Acceptable Use Policy
AV	Antivirus
AV	Asset Value
BAC	Business Availability Center
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BIOS	Basic Input/Output System
BPA	Business Partners Agreement
BPDU	Bridge Protocol Data Unit
BYOD	Bring Your Own Device
CA	Certificate Authority
CAC	Common Access Card
CAN	Controller Area Network
CAPTCHA	Completely Automated Public Turing Test

	to Tell Computers and Humans Apart
CAR	**Corrective Action Report**
CASB	**Cloud Access Security Broker**
CBC	**Cipher Block Chaining**
CCMP	**Counter-Mode/CBC-Mac Protocol**
CCTV	**Closed-circuit Television**
CER	**Certificate**
CER	**Cross-over Error Rate**
CERT	**Computer Emergency Response Team**
CFB	**Cipher Feedback**
CHAP	**Challenge Handshake Authentication Protocol**
CIO	**Chief Information Officer**
CIRT	**Computer Incident Response Team**
CMS	**Content Management System**
COOP	**Continuity of Operations Plan**
COPE	**Corporate Owned, Personally Enabled**
CP	**Contingency Planning**
CRC	**Cyclical Redundancy Check**
CRL	**Certificate Revocation List**
CSIRT	**Computer Security Incident Response Team**
CSO	**Chief Security Officer**
CSP	**Cloud Service Provider**
CSR	**Certificate Signing Request**
CSRF	**Cross-site Request Forgery**
CSU	**Channel Service Unit**
CTM	**Counter-Mode**
CTO	**Chief Technology Officer**
CTR	**Counter**
CYOD	**Choose Your Own Device**
DAC	**Discretionary Access Control**
DBA	**Database Administrator**
DDoS	**Distributed Denial of Service**
DEP	**Data Execution Prevention**

DER	**Distinguished Encoding Rules**
DES	**Digital Encryption Standard**
DFIR	**Digital Forensics and Investigation Response**
DHCP	**Dynamic Host Configuration Protocol**
DHE	**Data-Handling Electronics**
DHE	**Diffie-Hellman Ephemeral**
DLL	**Dynamic Link Library**
DLP	**Data Loss Prevention**
DMZ	**Demilitarized Zone**
DNAT	**Destination Network Address Translation**
DNS	**Domain Name Service (Server)**
DoS	**Denial of Service**
DRP	**Disaster Recovery Plan**
DSA	**Digital Signature Algorithm**
DSL	**Digital Subscriber Line**
DSU	**Data Service Unit**
EAP	**Extensible Authentication Protocol**
ECB	**Electronic Code Book**
ECC	**Elliptic Curve Cryptography**
ECDHE	**Elliptic Curve Diffie-Hellman Ephemeral**
ECDSA	**Elliptic Curve Digital Signature Algorithm**
EF	**Exposure Factor**
EFS	**Encrypted File System**
EMI	**Electromagnetic Interference**
EMP	**Electro Magnetic Pulse**
EOL	**End of Life**
ERP	**Enterprise Resource Planning**
ESN	**Electronic Serial Number**
ESP	**Encapsulated Security Payload**
EULA	**End User License Agreement**
FACL	**File System Access Control List**
FAR	**False Acceptance Rate**
FDE	**Full Disk Encryption**

FRR	**False Rejection Rate**
FTP	**File Transfer Protocol**
FTPS	**FTP over SSL**
GCM	**Galois Counter Mode**
GPG	**Gnu Privacy Guard**
GPO	**Group Policy Object**
GPS	**Global Positioning System**
GPU	**Graphic Processing Unit**
GRE	**Generic Routing Encapsulation**
HA	**High Availability**
HDD	**Hard Disk Drive**
HIDS	**Host-based Intrusion Detection System**
HIPS	**Host-based Intrusion Prevention System**
HMAC	**Hashed Message Authentication Code**
HOTP	**HMAC-based One-Time Password**
HSM	**Hardware Security Module**
HTML	**Hypertext Markup Language**
HTTP	**Hypertext Transfer Protocol**
HTTPS	**Hypertext Transfer Protocol over SSL/TLS**
HVAC	**Heating, Ventilation and Air Conditioning**
IaaS	**Infrastructure as a Service**
ICMP	**Internet Control Message Protocol**
ICS	**Industrial Control Systems**
ID	**Identification**
IDEA	**International Data Encryption Algorithm**
IDF	**Intermediate Distribution Frame**
IdP	**Identity Provider**
IDS	**Intrusion Detection System**
IEEE	**Institute of Electrical and Electronic Engineers**
IIS	**Internet Information System**
IKE	**Internet Key Exchange**
IM	**Instant Messaging**
IMAP4	**Internet Message Access Protocol v4**

IoT	**Internet of Things**
IP	**Internet Protocol**
IPSec	**Internet Protocol Security**
IR	**Incident Response**
IR	**Infrared**
IRC	**Internet Relay Chat**
IRP	**Incident Response Plan**
ISA	**Interconnection Security Agreement**
ISP	**Internet Service Provider**
ISSO	**Information Systems Security Officer**
ITCP	**IT Contingency Plan**
IV	**Initialization Vector**
KDC	**Key Distribution Center**
KEK	**Key Encryption Key**
L2TP	**Layer 2 Tunneling Protocol**
LAN	**Local Area Network**
LDAP	**Lightweight Directory Access Protocol**
LEAP	**Lightweight Extensible Authentication Protocol**
MaaS	**Monitoring as a Service**
MAC	**Mandatory Access Control**
MAC	**Media Access Control**
MAC	**Message Authentication Code**
MAN	**Metropolitan Area Network**
MBR	**Master Boot Record**
MD5	**Message Digest 5**
MDF	**Main Distribution Frame**
MDM	**Mobile Device Management**
MFA	**Multifactor Authentication**
MFD	**Multi-function Device**
MIME	**Multipurpose Internet Mail Exchange**
MITM	**Man-in-the-Middle**
MMS	**Multimedia Message Service**
MOA	**Memorandum of Agreement**

MOTD	**Message of the Day**
MOU	**Memorandum of Understanding**
MPLS	**Multi-Protocol Label Switching**
MSCHAP	**Microsoft Challenge Handshake Authentication Protocol**
MSP	**Managed Service Provider**
MTBF	**Mean Time Between Failures**
MTTF	**Mean Time to Failure**
MTTR	**Mean Time to Recover or Mean Time to Repair**
MTU	**Maximum Transmission Unit**
NAC	**Network Access Control**
NAT	**Network Address Translation**
NDA	**Non-disclosure Agreement**
NFC	**Near Field Communication**
NGAC	**Next Generation Access Control**
NIDS	**Network-based Intrusion Detection System**
NIPS	**Network-based Intrusion Prevention System**
NIST	**National Institute of Standards & Technology**
NTFS	**New Technology File System**
NTLM	**New Technology LAN Manager**
NTP	**Network Time Protocol**
OAUTH	**Open Authorization**
OCSP	**Online Certificate Status Protocol**
OID	**Object Identifier**
OS	**Operating System**
OTA	**Over The Air**
OVAL	**Open Vulnerability Assessment Language**
P12	**PKCS #12**
P2P	**Peer to Peer**
PaaS	**Platform as a Service**
PAC	**Proxy Auto Configuration**
PAM	**Pluggable Authentication Modules**

PAP	**Password Authentication Protocol**
PAT	**Port Address Translation**
PBKDF2	**Password-based Key Derivation Function 2**
PBX	**Private Branch Exchange**
PCAP	**Packet Capture**
PEAP	**Protected Extensible Authentication Protocol**
PED	**Personal Electronic Device**
PEM	**Privacy-enhanced Electronic Mail**
PFS	**Perfect Forward Secrecy**
PFX	**Personal Exchange Format**
PGP	**Pretty Good Privacy**
PHI	**Personal Health Information**
PII	**Personally Identifiable Information**
PIV	**Personal Identity Verification**
PKI	**Public Key Infrastructure**
POODLE	**Padding Oracle on Downgrade Legacy Encryption**
POP	**Post Office Protocol**
POTS	**Plain Old Telephone Service**
PPP	**Point-to-Point Protocol**
PPTP	**Point-to-Point Tunneling Protocol**
PSK	**Pre-shared Key**
PTZ	**Pan-Tilt-Zoom**
RA	**Recovery Agent**
RA	**Registration Authority**
RAD	**Rapid Application Development**
RADIUS	**Remote Authentication Dial-in User Server**
RAID	**Redundant Array of Inexpensive Disks**
RAS	**Remote Access Server**
RAT	**Remote Access Trojan**
RBAC	**Role-based Access Control**
RBAC	**Rule-based Access Control**
RC4	**Rivest Cipher version 4**
RDP	**Remote Desktop Protocol**

REST	**Representational State Transfer**
RFID	**Radio Frequency Identifier**
RIPEMD RACE	**Integrity Primitives Evaluation Message Digest**
ROI	**Return on Investment**
RMF	**Risk Management Framework**
RPO	**Recovery Point Objective**
RSA	**Rivest, Shamir, & Adleman**
RTBH	**Remotely Triggered Black Hole**
RTO	**Recovery Time Objective**
RTOS	**Real-time Operating System**
RTP	**Real-time Transport Protocol**
S/MIME	**Secure/Multipurpose Internet Mail Extensions**
SaaS	**Software as a Service**
SAML	**Security Assertions Markup Language**
SAN	**Storage Area Network**
SAN	**Subject Alternative Name**
SCADA	**System Control and Data Acquisition**
SCAP	**Security Content Automation Protocol**
SCEP	**Simple Certificate Enrollment Protocol**
SCP	**Secure Copy**
SCSI	**Small Computer System Interface**
SDK	**Software Development Kit**
SDLC	**Software Development Life Cycle**
SDLM	**Software Development Life Cycle Methodology**
SDN	**Software Defined Network**
SED	**Self-encrypting Drive**
SEH	**Structured Exception Handler**
SFTP	**Secured File Transfer Protocol**
SHA	**Secure Hashing Algorithm**
SHTTP	**Secure Hypertext Transfer Protocol**
SIEM	**Security Information and Event Management**

SIM	**Subscriber Identity Module**
SIP	**Session Initiation Protocol**
SIPS	**Session Initiation Protocol Secure**
SLA	**Service Level Agreement**
SLE	**Single Loss Expectancy**
SMB	**Server Message Block**
SMS	**Short Message Service**
SMTP	**Simple Mail Transfer Protocol**
SMTPS	**Simple Mail Transfer Protocol Secure**
SNMP	**Simple Network Management Protocol**
SOAP	**Simple Object Access Protocol**
SoC	**System on Chip**
SPF	**Sender Policy Framework**
SPIM	**Spam over Internet Messaging**
SPoF	**Single Point of Failure**
SQL	**Structured Query Language**
SRTP	**Secure Real-Time Protocol**
SSD	**Solid State Drive**
SSH	**Secure Shell**
SSID	**Service Set Identifier**
SSL	**Secure Sockets Layer**
SSO	**Single Sign-on**
SSP	**System Security Plan**
STP	**Shielded Twisted Pair**
TACACS+	**Terminal Access Controller Access Control System Plus**
TCO	**Total Cost of Ownership**
TCP/IP	**Transmission Control Protocol/Internet Protocol**
TGT	**Ticket Granting Ticket**
TKIP	**Temporal Key Integrity Protocol**
TLS	**Transport Layer Security**
TOTP	**Time-based One-time Password**
TPM	**Trusted Platform Module**
TSIG	**Transaction Signature**

UAT	**User Acceptance Testing**
UAV	**Unmanned Aerial Vehicle**
UDP	**User Datagram Protocol**
UEFI	**Unified Extensible Firmware Interface**
UPS	**Uninterruptable Power Supply**
URI	**Uniform Resource Identifier**
URL	**Universal Resource Locator**
USB	**Universal Serial Bus**
USB OTG	**USB On The Go**
UTM	**Unified Threat Management**
UTP	**Unshielded Twisted Pair**
VDE	**Virtual Desktop Environment**
VDI	**Virtual Desktop Infrastructure**
VLAN	**Virtual Local Area Network**
VLSM	**Variable Length Subnet Masking**
VM	**Virtual Machine**
VoIP	**Voice over IP**
VPN	**Virtual Private Network**
VTC	**Video Teleconferencing**
WAF	**Web Application Firewall**
WAP	**Wireless Access Point**
WEP	**Wired Equivalent Privacy**
WIDS	**Wireless Intrusion Detection System**
WIPS	**Wireless Intrusion Prevention System**
WORM	**Write Once Read Many**
WPA	**WiFi Protected Access**
WPA2	**WiFi Protected Access 2**
WPS	**WiFi Protected Setup**
WTLS	**Wireless TLS**
XML	**Extensible Markup Language**
XOR	**Exclusive Or**
XSRF	**Cross-site Request Forgery**
XSS	**Cross-site Scripting**