Core domains of the CompTIA security +
1.0: General Security Concepts (12%)
2.0: Threats, Vulnerabilities, and Mitigations (22%)
3.0: Security Architecture (18%)
4.0: Security Operations (28%)
5.0: Security Program Management and Oversight (20%)

Notes:
Take advantage of the guide to gain hand-on experience.
Consistency is key. Stick to a study schedule.

1) General security concepts

Compare and contrast various types of security controls.
Security controls
To put it simply, security controls are mechanisms that secure computer systems and enforce the confidentiality, integrity, and availability of our assets.
There are four main categories of security controls
1) Technical controls
Also known as logical controls, they are basically implemented using technology either by hardware or software. Examples include firewalls, anti-virus software, and data encryption. **Firewalls** monitor incoming and outgoing data while **data encryption** converts information into a coded form which makes it non-readable for unauthorized individuals.
2)Managerial controls
They focus on the governance aspect of security and guide security professionals to enhance overall security protection. They are more about policies, guidelines, standards, and practices. Examples include assessing risks, providing performance reviews, and making comprehensive plans after classifying data.

Risk assessment aims to reduce potential risk exposure by identifying and making plans to mitigate threats and vulnerabilities.

3)Operational controls

They consist of procedures taken by security professionals through guidance by managerial controls to implement security mechanisms. Examples include awareness training programs, backup procedures, and incident response activities.

Awareness training programs aim to educate employees and foster a security-conscious environment merely to enhance their ability to protect assets and data. **Incident response activities** outline the steps to be taken in case of an attack.

4)Physical controls

This security control aims to protect computer systems and the assets they hold by using physical barriers such as locks, security cameras, and physical intrusion detection sensors/systems.

To understand the categorization better, keep in mind the concept of prevent, detect, and react.

Security control types

Based on their functions, security controls can be further classified into six main types

1) Preventive controls

They stand on the frontline against potential threats to avoid and prevent their occurrence. They operate before attacks happen. Examples include firewalls, multi-factor authentication methods, and access control lists.

2)Deterrent controls

They help discourage potential attackers from committing any cybercrime. For instance, a warning sign or even the presence of a security personnel can scare them off. Legal penalties are another example.

3)Detective controls

They are used to detect and identify malicious activities and issues. Detective controls operate during an intrusion or attack. Examples include system monitoring, intrusion detection systems, and log monitoring.

4)Corrective controls

Security controls that try to lessen the damage or eliminate the impact of an attack. Examples include patch management systems and back up systems that are able to restore data after an attack.

5)Compensating control

Due to various reasons, an organization may seek out alternative security methods that offer similar protection to their primary control counterparts to ensure protection of its assets. They may also be used to enhance already deployed primary controls.

6)Directive controls

They are more about directing individuals and offering them recommendations to help protect their assets.

1.2) Summarize fundamental security concepts

Simply put, the CIA triad unifies the cornerstone principles for security protection. It stands for confidentiality, integrity, and availability.

Confidentiality ensures that only authorized individuals have access to certain data and resources. Examples include password-protected files, encryption, secure communication channels, and access control.

Integrity ensures that data is accurate and trustworthy. It also manages data so that it is not altered or deleted. Examples include digital signatures and hashing algorithms.

Availability ensures that data and resources are timely available for users to access. Examples include backup systems, high availability configuration, and fault tolerance.

Non-repudiation ensures that entities of a transaction cannot deny that it had occurred. It ensures accountability and reliability.

Digital signatures: utilize cryptography to verify the sender's identity and ensure integrity. CAs issue digital certificates that certify the authenticity of the sender and link them with the public key and the integrity of the document sent.
Audit trails: it is a detailed record that tracks all changes and activities within a system. It can help detect security violations and intrusions as well as hold individuals accountable.
Access control:restricts resource access only to authorized entities
Identification is uniquely identifying an individual based on their information and data

Authentication, Authorization, and Accounting (AAA)
Authentication is the verification of a user's identity. It proves you are who you are.
Authorization determines what an authenticated user is allowed to access.
Accounting tracks the activity of users.

Authenticating people focuses on verifying the identity of users. The username and password inserted are compared to stored credentials in a database.
Authenticating systems

AAA protocols
Remote Authentication Dial-in User Service (RADIUS)
Radius is a network protocol used to provide AAA for network services
Diameter: It is an evolution of the RADIUS protocol.
Terminal Access controller Access Control System:

Gap analysis: It is a procedure which assesses the cybersecurity posture of an organization by comparing its existing security controls to particular desired standards. It helps them ensure their security controls are effective while identifying the need for additional ones.
Assessment is conducted to thoroughly understand the organization's policies and procedures.
Benchmarking is comparing their existing security controls to established industry standards.
Identification: Gaps are identified where security measures don't meet desired levels.
Prioritization: Gaps are ranked based on their potential impacts.
Remediation strategy: A comprehensive strategy is planned to enhance the organization's security posture.

Zero-trust : It is an information security concept which assumes no trust to any entity by default. It always verifies every user or device to ensure they meet the organization's policies before granting access. The zero trust architecture is split into two planes: the control plane and the data plane.

Control plane: it is an element of the network architecture which makes intelligent decisions based on policies and protocols.

Adaptive identity: Unlike traditional authentication methods, adaptive identity selects for each user a tailored authentication based on multiple factors including the user's activity, the device used, and their geographical location as well as other contextual factors. It is an essential implementation for zero trust.

Threat scope reduction: It aims to limit the avenue of threats by minimizing access rights for users so they only have permission to do what they need to do and nothing more.

Policy-driven access control: Access to a network and its resources is granted for users based on a predefined set of rules.

The policy engine (PE) grants or denies requests. It gathers the policies set along and defined by the PA with info from external systems such as Adaptive identity to make the final decision.
The policy administrator (PA) is responsible for defining and managing the policies that dictate how a subject can interact with a network resource.

Data plane: It primarily focuses on how data moves within a network. It is also where the actual process of forwarding of data happens. It is sometimes referred to as the forwarding plane.

Implicit trust zones: This refers to the zone or segment within a network where all communications are trusted which means that data can flow freely.

Subject/System: An entity which requests access to data and resources while the system is the computer.

Policy-enforcement point: It is a network component which enforces all of the access control policies when a subject attempts to access a resource. It gathers information regarding this subject and hands it over to the PDP to learn whether to grant access or not. It basically acts with compliance to policies within a network.
PA + PE= PDP

Physical security
It is a category of security controls by which physical implementations are put in place to limit physical risks to an organization’s assets. Without physical security, other controls are of no use if an attacker can get physical access to a system.

Bollards

They are short and sturdy physical barriers made out of metal, steel, or concrete. They are often dug deep into the ground and are used to prevent vehicle access to high-security areas. Some of them are mechanically controlled.

Access Control Vestibule

It is a secure entryway consisting of a set of doors that lead to a highly secure area. This adds a layer of protection as the doors to the highly secure area cannot be opened before the entrance to the ACV is closed which prevents unauthorized individuals from secretly following authorized individuals (piggybacking or tailgating). A manual ACV is also sometimes included where a guard is present in a one window room to manually unlock the second door after the entry of the authorized individual through the first door. Further, different unlocking mechanisms are used for each door.

Fencing

Fences are structures that enclose a highly-secure area to prevent intrusion. They are often made out of materials such as wood, metal, or wire. To prevent climbing, metal fences may be spiked and wired fences may be barbed. Some are even transparent and others are opaque which block all sight for privacy. There also exist ones that are electrified with a high voltage.

Video surveillance:

A video surveillance system is another physical security control which includes a network of cameras, monitors, and recorders. These elements of surveillance offer a wide range of features. With CCTV being the most well known, their video cameras record footage and transmit a video signal privately to a video room. The recorded footage is stored for criminal investigations later on. These systems may cause privacy concerns for some individuals.

Security guards:
Although other physical security controls can protect an organization's assets, trained security guards can never be replaced.
They are also needed at desk receptions to authenticate and authorize individuals. Their presence is also needed to monitor other controls such as video surveillance.

Access badges:
An access badge is a type of technology used to grant or deny access to a physical zone. It comes in the form of an ID card that stores unique data pertaining to its holder. These badges must be worn at all times to allow entry to a certain part of a building by scanning or swiping the relevant card as well as to help security guards identify someone based on the details found on them.

Lightning:
These are essential deterrent controls as potential attackers usually avoid lit areas in order not to be caught by surveillance. Motion based lighting that activates upon detecting movement can also help identify presence and alert security guards. It is important to study the placement of the lightning within the facility.

Sensors

Infrared
These sensors detect motion from emitted infrared radiation. They are able to detect movement in an area by sensing changes in temperature.

Pressure

These sensors detect changes in pressure. They are used to detect unauthorized access upon inflicting pressure on their surface. Pressure sensors can also be integrated into electronic locks or safes to detect attempts to force them open. They can also be placed under floor mats.

Microwave

These sensors emit microwave signals to detect the presence of someone. They operate by emitting microwaves and then detecting the reflections of those microwaves back to the sensor. They have a long detection range and are highly sensitive.

Ultrasonic

These sensors work by transmitting sound waves that aren't heard by humans and measuring the time it takes for the waves to reflect back. Using the time of the wave and the speed of sound, the sensors can calculate the distance of the object that the wave was reflected off.

Other things to note

All critical systems should be placed in a secure system rather known as the server room. This room should always be monitored and locked and must be placed in an area with limited personnel access.

Considering the safety of employees, the facility or building of an organization should be in an area where crime rates are low, natural disasters don't occur regularly, and emergency services aren't out of reach in case of incidents.

Entrances and exits must also be well lit. Alternatives such as emergency lighting units should be implemented incase of power outages to aid evacuations.

Highly secure environments should have security desks close by where security personnel always monitor incoming and outgoing individuals.

Entrance doors must be secured with hinges and pins.

Doors must have panic bars that provide easy entrance and exits in case of an emergency.
If a partition for walls or floors exists, an intruder is able to crawl in that space and access the secure area.
Ventilation ducts and utility tunnels may also be taken advantage of by intruders. Hence, they must be equipped with motion detectors.

Deception and Disruption Technologies

They are used to deceive attackers and disrupt their attacks. These technologies help security professionals learn more about attackers' techniques to build stronger defenses based on real world attacks.

Honeypots

It is when security teams set up a website similar to the legitimate website but with lower security. Honeypots record attack patterns, techniques, and commands which help security professionals gain insight and advance their defenses.

Honeynets

Essentially, they are a set of honeypots which form a bait network. They aid security professionals as they form a testing ground for them to analyze malicious activities used to exploit a network.

Honeyfile

They are files placed within honeypots or honeynets but can also be placed inside a legitimate system or network. Basically, they create the illusion of value for attackers to open them which signals their presence for the security team.

Honeytokens

Data or information used to lure attackers. These fake assets help security professionals track and identify attackers as they contain unique pieces of traceable data embedded within them.

There are many open sources to download to create a virtual world.
Some of the info gained by studying spammers and attackers is shared with other organizations.

1.3)Explain the importance of change management processes and the impact to security

Change is inevitable for all organizations. And for ones that heavily rely on technology, change management is significant to maintain security.

Business Processes Impacting Security Operation

Approval Process:

It looks at the proposed change and the purpose behind it while identifying its scope. This ensures that important modifications get formal approval from the right people who assess both the risks and benefits.

Ownership:

In security, ownership ensures that assets are consistently maintained, protected and updated.It refers to the person within a department who has asked for a change. Ownership ensures accountability and effective outcomes upon modifications. In terms of security, it may be handled by the Chief Information Security Officer (CISO).

Stakeholder:

Entities that impact and are impacted by how the security of an organization functions. They should be well informed throughout the process.

Impact analysis:

It is important to analyze the impacts of any modification within an organization before implementing it. This helps foresee potential security risks and address things before they become an actual issue. We determine both the risks of making and not making the change.

Test results:

Before implementing any security change, it should be tested to ensure it works as expected. It is done within a technological safe space.

Backout plan:

When conducting any change that is thought to be quite risky, a backout plan helps undo a change and return everything back to normal. A thorough outlined procedure should be created before the change.

Maintenance Window:

It is a scheduled time for implementing security changes or updates. By implementing these modifications during the maintenance window, security measures are smoothly applied with no disruptions.

Standard operating procedure:

It is a well documented rulebook that guides how a complex task should be executed. It consists of an outline of every critical step to make sure that these tasks are implemented accurately and consistently.

Technical Implications

Allow lists:

This list grants access merely to those on the list. This ensures that only approved applications and files can run on a system.

Deny lists:

This list denies access to what's on the list. It helps protect a computer system from harm.

Restricted activities:

Restricted activities prevent disruptions. Examples include unauthorized software installations, unauthorized system modifications, access to critical servers, access to sensitive data, and unauthorized data transfers.

Several other factors that impact change management:

Downtime:
This occurs when the system is down and not running due to maintenance or even due to cyberattacks. Potential revenue loss as it may cause disruptions. So, it must be scheduled during non-production hours. Or, there must be usage of a secondary system.
Service restart:
After implementing a change, the system has to restart. It is sometimes required.
Application restart:
When an application restarts, potential security weaknesses emerge. This can affect the integrity of the application and its security measures temporarily.
Legacy applications:
They are applications that have been used for a long time. These applications tend to have outdated security measures. It is also common for these legacy apps to no longer be supported by the developer.
Dependencies:
Another thing which complicates changes is their reliance on other system components. With dependencies, you have to make a change or upgrade an application or server before installing or upgrading another application or server.

Documentation:
Written material that includes user guides, technical specifications, or system descriptions. A detailed documentation of changes is crucial to ensure transparency and accountability. These documented modifications help identify who made that change and why. It enhances security as it ensures alterations are accounted for by authorized individuals. Maintaining documentation involves the following practices:

Updating diagrams:

Keeping system architecture diagrams up to date supports the changes and gives a better understanding of the current environment.
Accurate diagrams contribute to enhanced security management. They should be well written and up to date.

Updating policies:
Policies and procedures must be regularly updated to reflect changes and to ensure they provide correct guidelines that are also in compliance with regulations.

Version control
It ensures that only authorized modifications are implemented. It is a system which documents changes over time so that you can recall specific versions laters. By tracking changes, we can easily revert to previous settings.

1.4) Explain the importance of appropriate cryptographic solutions

Public Key Infrastructure (PKI)
The public key infrastructure refers to policies and procedures, hardwares, softwares, and individuals that create, distribute, manage, store, and revoke digital certificates.

Public key: the public key is distributed to the public and is used for the encryption of data and for the validation of digital signatures.

Private key: the private key is kept confidential (a secret) only known by its owner. It is often stored in digital or hardware-based cryptographic devices. It is used for the decryption of data. Also, it is used to generate digital signatures.

Key escrow: the escrow agent is a trusted third party responsible for storing private keys in an escrow which ensures that authorized entities can retrieve them later on. Specialized hardware such as the Hardware Security Model safeguard (HSM) these cryptographic keys.

Encryption: it is the conversion of information or data into a coded form which makes it unreadable for unauthorized individuals. It converts data from a plaintext to a ciphertext to uphold its secrecy and genuineness.

Level: the encryption level refers to the intricacy of the encryption algorithm and the cryptographic key used to safeguard information as well as the extent and scope by which data is transformed into a secure format.

Full disk encryption: it is a cryptographic security measure used to protect data and info stored on a computer hard drive. It encrypts an entire hard drive including data, files, the OS, and software programs. The trusted platform module is where keys can be stored.

Partition: it refers to separate portions of a disk that are independent of each other.

File: a file stores images, text, audio, and videos. File encryption allows for encryption at the level of a file which helps protect data especially in shared environments. The Encrypted File System is used to encrypt files where the keys are stored in the user's profile.

Volume: A Volume Level Encryption is used to encrypt large amounts of data across countless drives which enhances overall security. Bitlocker encrypts the entire volume while TPM securely stores encryption keys.

Database: securing a database usually involves database encryption. Practices include separating the database from the web servers, encrypting a backup of the database, ensuring physical security, and actively monitoring database activity.

Record: it is a technique which encrypts specific data (a row or a column) within a database. In this case, each record has its own key.

Transport/Communication: encryption of data in transit ensures a secure highway of transmission for data being exchanged.
Data at rest means that it is inactive; backed up or stored.
Data in transit is one flowing from its source or origin to its destination within a network.
Data in use or in processing means its undergoing constant change like data on a spreadsheet or a database

Asymmetric encryption: it utilizes a pair of keys: a public one for encryption and a private one for decryption

Symmetric encryption: employs a single key for both the encryption and decryption. It is more straightforward but less secure. It is an old technique that is still widely used.

Key exchange: It is a cryptographic process by which keys are exchanged between a sender and a receiver to exchange encrypted messages.

Algorithms: An algorithm is a mathematical cryptographic formula or equation which scrambles the plaintext. A set of algorithms is known as a ciphersuite which typically includes a key exchange algorithm, a bulk encryption algorithm, and a message authentication code. The key exchange algorithm is used to exchange a key between two devices. The bulk encryption encrypts the data. The MAC algorithm ensures the integrity of data in transit. Different types of ciphersuites exist, some which are better than others as they offer additional security requirements. We have stream ciphers and block ciphers.

Key length: It corresponds to the number of bits in an encryption algorithm's key. The strength of encryption relies on how difficult it is to discover the key which depends on key length and the cipher used. Longer keys are usually known to provide stronger encryption unlike their short counterparts that may be vulnerable to brute-force attacks.

Tools: specialized technologies and protocols which play a critical role in digital communications

Trusted Platform module: it is a cryptographic technology integrated into a computer's motherboard. A TPM chip is a processor which carries out cryptographic operations. It includes physical security mechanisms that make it resistant against tampering. It generates and stores cryptographic keys and limits their usage. It also carries out authentication and ensures integrity.

Hardware Security module: it is a physical computing device which provides cryptoprocessing. It generates and stores digital keys only for authorized individuals to access. The HSM strengthens encryption and decryption as well as payment security. Unlike a TPM, it is a removable unit within a computer. Some of the disadvantages of HSMs include their expensive costs and the software programs that have to be installed on a computer to use them.

Key management system: a system used to manage cryptographic keys including their generation, storage, distribution, use, destruction and so on. The central functions of a KMS are the generation of secure cryptographic keys while ensuring their strength and complexity, the secure storage of keys within a safe environment, the secure exchange of keys during transmission, the insurance of access control for key usage, and the key replacement over the long-term to maintain security.

Secure enclave: it is a unique hardware based feature which securely handles encryption and decryption. It is designed to resist software and hardware tampering as well as sophisticated digital attacks. Unlocking its data requires biometric information.

Obfuscation: transforming data into a confusing form to protect it. It includes various unique techniques and methods.

Steganography: it is the use of any digital medium to hide a secret message. You can embed a secret within a Microsoft word or Excel document. There are several applications that can be used for steganography including Xiao, Foremost, Steghide, and Concealment.

Audio steganography: data can also be hidden within audio files. This is a technique by which audio signals are modified to transmit hidden information. Embedding a secret message in an audio is harder to do. Audio steganography is made up of a carrier or audio file, a message, and a password. The carrier conceals the secret message. The message is anything the sender wants to remain hidden.

Video steganography: this technique hides secrets within a video file. A video is made up of several images or frames. By pulling out all of the frames from the video, we can store the secret data using least significant bit steganography and then put them back together with the secret message within.

Image steganography: it is used to hide data in an image file. There are three effective methods used to apply image steganography including least significant bit, blocking, and palette modification. The LSB

Tokenization: it is the process of protecting data at rest by which this data is replaced by or converted or generated into random and unique values/tokens and storing its mapping within a database. The tokenized data has the same length and format as the original data. The original data is stored in a secure token vault. When the og data is needed, its tokenized version is submitted to a vault which then compares it to existing data and returns with the actual data.

Data masking: it is hiding data/information with specific characters or other data to protect it. Substitution is used in data masking; you replace the actual data with an authentic looking value.You may also reveal only a portion of the actual data.

Hashing: it is a mathematical one-way function by which data is converted into fixed-length value. Hashing is a checksum. It ensures that data has not been altered or modified in storage or in transit.
Each hashing algorithm outputs a specific length. Each hash value is unique. If two different data sets produce the same hash value, the phenomenon is rather known as collision.

Salting: it is a cryptographic technique used to enhance password security. It involves adding a unique and random data string to a password before hashing it and storing it in a database. A salt is created by a cryptographic random number generator.

Digital signatures: it is a mathematical cryptographic technique used to verify a digital message's authenticity and integrity. They employ asymmetric encryption by which the digital signature scheme consists of three elements: a key generation algorithm which selects a random private key and a corresponding public key, a signing algorithm which produces a signature given a message and a private key, and a signature verifying algorithm which verifies the authenticity given a public key, the message, and the signature.

Key stretching: it is a cryptographic method used to make a weak password or passphrase more secure by increasing the resources needed to test each possible key. It involves converting a password to a longer and more random key. Key stretching typically includes a salt or a pepper (secret salt).

Blockchain: it is a type of database which stores information in blocks and chains them together in a chronological manner. It is basically tracking anything with value (mainly transactions). The chain contains details of each transaction. It is difficult to tamper with this technology as the blocks are cryptographically bound together. Further, a blockchain is a decentralized database which means it is managed by several individuals.

Open public ledger: it is a trusted medium/ system which organizes blocks of information to ensure secure transactions between a seller and a buyer. Anyone can access and verify the record keeping process which makes the ledger transparent and decentralized as it's shared over a network of nodes (computers).

Certificates: it is a digital document issued by a CA which establishes trust between individuals as it verifies their identities within the digital landscape.

Certificate authorities: an entity which issues digital certificates to users. In a PKI system, the CA is known as a trusted third party. Certificate authorities verify the authenticity of a domain or a website as they hand over identity credentials (certs) to authenticate entities or organizations. Any website with HTTPS has been verified by a CA which makes the internet a more secure place. Sometimes, a registration authority is used to verify requests for digital certificates.

Certificate revocation list: it is a list of certificates that are no longer valid and cannot be trusted as they have been revoked by the CA. The CRL is published every 24 hours.

Online certificate Status protocol: an internet protocol which serves as an alternative to the CRL as it checks whether digital certificates are valid or not. The OCSP requests is submitted to the issuer to validate a digital certificate. There are countless attributes found on a certificate.

Self-signed: a self-signed certificate typically uses its own private key to authenticate itself. It lacks trust as it's not validated by a trusted external party. A SAN certificate permits organizations to use several domains with one certificate only.

X.690 is a common standard which defines encoding formats. It was developed by the ITU-T

Basic encoding rule: it is a rule which sets governing for the encoding of ASN.1 data structure. Any data which is created is encoded using a type identifier, a length description, and the content's value. Encoding is expressing information as data elements.

ASN.1: it is a stand interface description language used to define data structures

Canonical encoding rule: it is a restricted version of BER which permits the usage of only one encoding type.
Distinguished encoding rule: it is also a restricted version of BER which allows the usage of only one encoding type. It has restrictions regarding length and other details.

Third-party: a third party certificate authority verifies individuals and issues digital certificates for them.

Root of trust: a source that is trusted within a cryptographic system

Certificate signing request: it is basically an application for a digital certificate. It is when a user sends their credentials along with their public key for the CA to verify them and issue a certificate to validate their authenticity.

Wildcard: it is when a single certificate is used to verify countless domains for an organization.

2)Threats, Vulnerabilities, and Mitigation

2.1)Compare and contrast common threat actors and motivations

Threat actors: aim to compromise the confidentiality, integrity, and availability of systems.

Nation state: they are often supported by the government. In such cases, the government is known as an advanced persistent threat. They have the highest level of resources.

Unskilled actor: has little to no technological knowledge. May copy and paste malicious code into a website. They are also referred to as script kiddies.

Hacktivist: comes from the words hack and activist. They are individuals who hack for social change or to promote a political agenda.

Insider threat: it refers to someone within an organization who abuses their authority and their access to data and resources to misuse data for malicious purposes.

Organized crime: cybercriminals who are part of an enterprise run by people motivated by money. They may be well funded and have a high level of sophistication.

Shadow IT: it is when someone within an organization uses systems, software, network devices, services, and applications without approval from the IT department. This may introduce vulnerabilities.

Attributes of actors
internal/external: someone within an organization(internal) may seek out to compromise the assets of said organization if they're motivated by money offered by someone outside the organization (external)

Resources/funding: nation-state actors and cybercriminals typically have more resources and fundings. Resources are the tools, technology, and information. Fundings refer to financial means.

Level of sophistication/capability: some hackers may have more access to sophisticated tools than others. Capabilities refer to the tools, techniques, procedures, and infrastructure which connects the adversary to the victim

Motivation: it is the reason which drives the actor to compromise a system. Some are more than mere financial gain schemes.

Data exfiltration: it is the unauthorized transfer of data from a computer
Espionage: spying to gain secrets or confidential information
Service disruption: temporarily or permanently causes the downfall of an information system. It is done intentionally.

Blackmail: threatening someone to reveal their secrets unless a demand is met
Financial gain: to increase one's wealth
philosophical/political beliefs: deeply held beliefs and views regarding politics and philosophy
Ethical: actions that conform to accepted standard behaviors
Revenge: the act of retaliation against wrongdoing
Disruption/chaos: causing confusion through disruptive activities

War: In cybersecurity, war is often referred to as cyber warfare. It encapsulates state-backed attacks that aim to sabotage critical infrastructures or to cause disruptions. These sophisticated state-sponsored threats may be APTs that demand high security measures. The digital landscape is sometimes used as a battlefield during wartime.

2.2)Explain common threat vectors and attack surfaces
Message based: attackers use a variety of strategies to take advantage of individuals that use message based communication.
Email: one of the most prevalent attack vectors for threat actors. Email is used to spread malicious links and attachments that download malware. There are also phishing emails by which an attacker pretends to be a trusted source and tricks users into disclosing confidential information.
SMS: Also known as text messaging, SMS is another threat vector commonly used. Attackers may use smishing attacks via SMS to trick users to disclose personal information. SMS is susceptible to several types of attacks.
Instant messaging (IM): instant messaging platforms are used by attackers to spread nefarious links, take advantage of holes in the software, and carry out phishing scams.
Spam and Spam over instant messaging: spam is unwanted digital communication sent in bulk. Although mainly referred to spam sent over email, it is not uncommon to encounter spam

messages across instant messaging platforms or social media sites.

Image-based: it is when an attacker exploits or manipulates digital images and their metadata to hide malware. It is also used by threat actors to execute phishing activities.

File-based: these threats use common files such as spreadsheets, documents, and PDFs to embed harmful scripts which may lead to adverse effects such as infecting systems and nets or unauthorized access.

Voice-call: these threats include deceptive acts such as vishing, unauthorized call interception, and ID fraud or spoofing.

Removable devices: portable devices such as USB drives, external hard drives, and memory cards are prone to damage by threat actors who use them to transmit malware. This can lead to data theft, system compromise, or malware execution.

Vulnerable software: it is a software which has weaknesses or flaws in its code or design.

Client-based security: requires the installation of a software (an agent) that actively monitors against malicious activities

Agentless security: doesn't require installation. It involves centrally monitoring and enforcing network policies virtually.

Unsupported systems and applications: ones that no longer receive updates, security patches, and technical support. These systems are prime targets for cybercriminals that take advantage of security flaws.