Cyber Security
Unit-1

Illustrate with examples why do cyber security is important. Briefly discuss the types of cyber-attacks.

Cybersecurity:
is the technique of protecting your systems, digital devices, networks and all of the data stored in the devices from cyber attacks.

importance:

1. **Protecting personal data**: safeguarding sensitive information by encryption & 2factor authentication
2. **Safeguarding business information**: safeguarding financial records to customer database by avoiding unathorised access by implementing robust cyber security measures
3. **Ensuring Online transaction Security**: Cyber security protocols, such as secure socket layer cerdificates & secure payment gateways. helps ensure the integrity & security of online transactions.
4. **Preventing unauthorised access**: cyber security countermeasures → strong password, multi factor authentication & intrusion detection systems.
5. **Mitigating the risks of cyber attacks**.
   Effective cyber security measures → regular software updates, security patches.
6. **Enhancing customer trust**
7. **Maintaining system integrity** → for smooth operation
   backup system, vulnerability management, regular system update
8. **Protecting nation security**
   Govt will invest heavily in CS measures to defend against cyber attacks

Cybersecurity Attacks Types:

(1) **Malware**: Malicious s/w such as viruses, worms and spyware that infiltrate & damage systems
Eg: WannaCry ransomware attack

(2) **Phishing**: Fraudulent communication, often emails, that trick users into revealing sensitive information
Eg: emails pretending to be from banks asking for login details.

(3) **Man-in-the-Middle (MitM) Attacks**: Interception of communication between two parties to steal or alter data
Eg: Eavesdropping on public Wi-Fi networks

(4) **Denial of services (DOS)**: Overloading a system to make it unavailable to users
Eg: Botnets used to flood a website with traffic

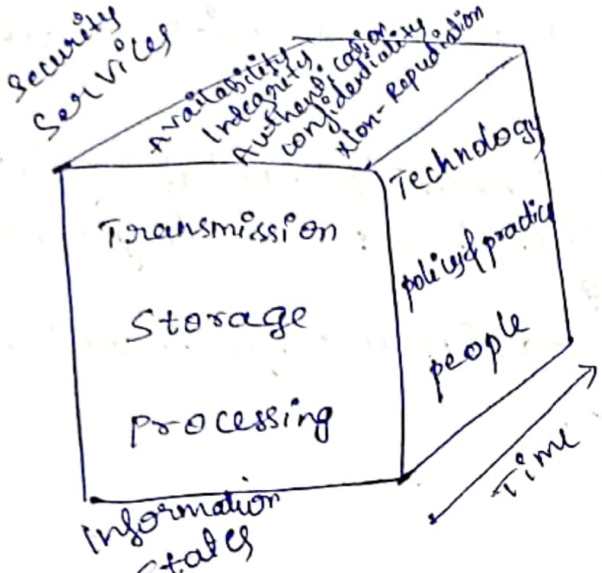
(5) **SQL Injection**: Exploiting vulnerabilities in SQL databases to access or manipulate data.
Eg: theft of sensitive customer info from poorly secured websites

(6) **Zero-Day Exploits**: Attacks on vulnerabilities unknown to s/w developers.
Eg: Stuxnet malware targeting industrial systems

(7) **Insider Threats**: Attacks from within an organization often by disgruntled employees.
Eg: Employees stealing or leaking sensitive company data

(8) **Social engineering**: Manipulating individuals to divulge confidential information
Eg: Pretending to be IT support to gain access to login credentials

Describe the principles of Confidentiality, Integrity & Availability with a neat diagram depicting cyber cube.



① Confidentiality: Ensures information is accessed only by authorized individuals. Protects sensitive data from unauthorized access or accidental disclosure through encryption, strong passwords & two-factor authentication.
Eg: Encrypting email content to restrict access to intended users.

② Integrity: Guarantees data accuracy & protection from unauthorized modification or deletion. Maintained using backups, and cryptographic checksums.
Eg: Verifying email content remains unaltered during transit using cryptography

③ Availability: Ensures constant, reliable access to data for authorized users, even during system failures or attacks. Maintained through robust recovery systems & infrastructure improvement
Eg: Ensuring uninterrupted email service access

④ Authentication: validates the identity of users access specific information. Uses single or multi factor methods like passwords, tokens or biometrics

Eg: Logging into a website with a username & password.

⑤ Non-Repudiation: Prevents denial of involvement in data transmission by providing proof of sending & receiving

Eg: SMS with delivery confirmation & sender details.

Discuss information assurance fundamentals essential in cyber security

IA is critical to safeguarding an organization's information and ensuring the security of its systems. IA ensures that sensitive data is protected from unauthorized access, modification, destruction, or loss. The framework focuses on more strategic, policy driven actions, as opposed to just infrastructure.

Key fundamentals of IA in CS:

1. Confidentiality
2. Integrity
3. Availability
4. Authentication
5. Non-Repudiation
6. Security countermeasures;

- **People**: involvement of both admin & user in safeguarding the info sys is essential. They must be aware of policies, follow best practices & act appropriately to protect sensitive data.
- **Policies & practices**: organizations must establish and enforce rules & procedures for handling sensitive data, ensuring compliance & taking action in case of breaches.
- **Technology**: Employing the right technologies both such as firewalls, routers, intrusion detection system (IDS) and anti-malware s/w is crucial for defending against cyber ~~attacks~~ threats.

(7) Time :

The time dimension refers to ensuring that Diffe
& systems are secure throughout their entire
lifecycle, from creation & storage to transmiss
& disposal.

→ both online & offline states; risk of unauthorized access is minimized

→ continious monitoring, Incident Respons Patch Management

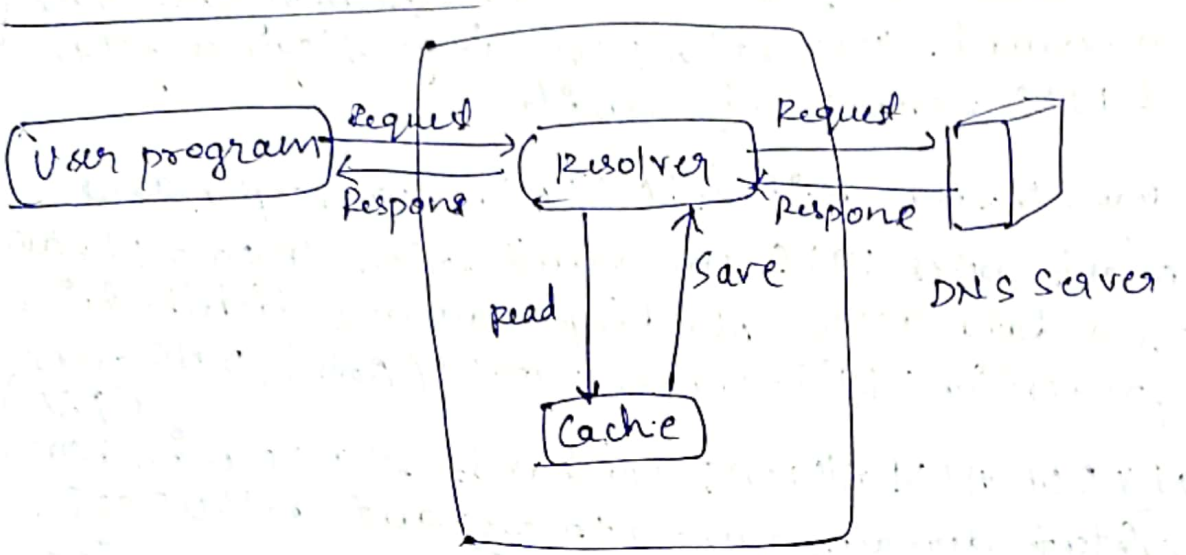
(8) Information states :

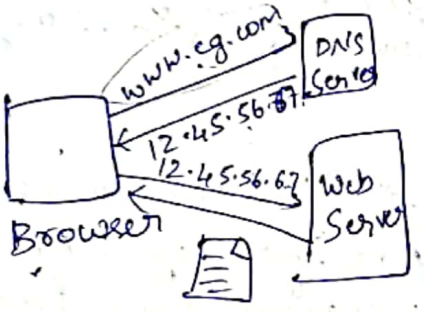
- Transmission : defines time wherin data is between processing steps
- Storage : defines time during which data is saved on medium such as hard drive
- Processing : It defines time during which data is in processing state

Difference between Information Assurance & Information Security

Information Assurance	Information Security
(1) Focuses on managing risks & threats to the organization's data & information system	(1) Focuses on protecting data through measures like encryption & access controls
(2) More concerned with the overall risks to data & systems	(2) Prevents unauthorized access, modification, and destruction of data.
(3) Five pillars: CIA, Authentication, Non-repudiation	(3) 3 main motives: CIA
(4) Emphasizes the appl^{n} of organizational standards and policies.	(4) Focuses on developing technologies & tools for securing data
(5) A broader framework that works with Information security to protect data	(5) Subset of Information assurance focused on securing data
(6) Includes risk management, restoration of information systems and more.	(6) Achieved through security technologies & processes
(7) Focuses on organizational risk management & data quality.	(7) Focuses on providing methods to reduce risks of unauthorised access
(8) Involves security audits, network architecture, compliance & policy enforcement	(8) Involves penetration testing, vulnerability management & technology solutions.

Illustrate with a neat diagram concept of DNS and associated attacks





Attacks:

① DNS Spoofing (Cache Poisoning): Redirects traffic to malicious servers by injecting false DNS info. Impact: Data theft, malware distribution. It is prevented by using DNSSEC, secure resolvers & clear cache

② Denial of Service (DoS) & Distributed Denial of Service (DDoS): floods system with traffic to overload & crash servers, Impact: service downtime, system crashes. It is prevented using Rate limiting DDoS mitigation services & Anycast routing

③ Fast Flux: Rapidly changes IP addresses to hide the attacker's location, Impact: Hides malicious activities, prolonging exploitation. It is prevented using monitor unusual DNS patterns block suspicious activity.

(4) Reflected Attacks & Reflective Amplification DoS: Spoofs victim's IP and redirects large responses overload the systems. Impact: System infrastructure overload. Prevention: Use ingress/egress filtering & DNS response size limits.

(5) Man-in-the-Middle (MITM): Intercepts and manipulates DNS communication Impact: Unauthorized data access, phishing, malware distribution, prevention: DNS-over-HTTPS (DoH), DNS-over-TLS (DoT)

(6) NXDOMAIN Attacks: Bombards servers with non-existent domain queries to exhaust resources. Impact: Delayed/dropped legitimate queries prevention: DNS firewalls, anomaly detection & rate limiting

(7) Domain Hijacking: Altering DNS records or seizes domain control. Impact: Loss of domain control, brand damage. Prevention: Two-factor authentication & domain locking,

Illustrate with examples the following terms of the characteristics in each case with respect to damage they create in cyber security arena.

(i) Virus: A virus is a type of malicious sw prog. designed to replicate itself & spread from one computer to another by attaching itself to a legitimate program or file.

characteristics: → Requires user action to activate
→ It can corrupt / delete files
→ inject files by spreading

Eg: Melissa virus → spread through email attachments

(ii) Worm: is a self-replicating malicious program that spreads without user intervention. Unlike a virus, a worm does not need to attach itself to an existing program.

characteristics: → self-replicating
→ spread autonomously across N/W
→ cause N/W congestion
→ slow down systems
→ Open backdoors for attackers

Eg: Blaster worm → targeted windows OS, computers get crashed & allowing remote control access to attackers

(iii) Trojan Horse: is a malicious program that disguises itself as a legitimate or useful software to deceive users. It doesn't replicate like a virus or worm

characteristics: → delivered via phishing emails or fake S/W downloads
→ creates backdoors, steal data, monitor user activity,
→ Install other malware

Eg: Zeus Trojan → primarily for banking fraud

(iv) Logic Bomb: is a piece of code deliberately inserted into a system that triggers a harmful action when specific conditions are met (eg: a certain date/time)

characteristics → lies dormant until triggered by an external event / time-based condition
→ used by disgruntled employees / hackers for sabotage / espionage
→ damage is usually hidden, and the attack might only be discovered after it causes damage.

Eg: A logic bomb planted by an employee in a financial company could trigger the deletion of critical data / transfer sensitive info to 3rd party after the employee leaves the company.

(v) Boot sector virus: As a type of virus that infects the boot sector of a computer's hard drive or a removable storage device (eg: USB drive)

characteristics: → infects area of a disk / drive that loads the OS causing computer to boot with malicious code instead of legitimate OS
→ causing data loss which will make difficult to recover without specialized tools.

Eg: Stone virus → infects floppy disks.

efine Symmetric Encryption? Discuss in detail the working principles involved in the design of public key encryption technique with an example.

Symmetric encryption: is a type of encryption where the same key is used for both encry & decry data. The key must remain secret between the sender & receiver & the security of encry relies on the confidentiality of this shared key

Working principle of Symmetric Encryption:

① Key generation: A secret key is generated, often a random chosen no. or string of characters.

② Encryption: plaintext → ciphertext using cryptographic algo & the secret key

③ Decryption: recipient uses the same secret key to decrypt the ciphertext → plaintext

⇒ Algo: AES Adv Encry Standard
DES Data Encry standard
RC4

Public Key Encryption (Asymmetric Encryption):

also known as asymmetric encryption uses a pair of keys → one public + one private for encry & decryption process.

public key → encry
private key → decryption

private key is kept secret by the owners
public key shared freely

Working principle

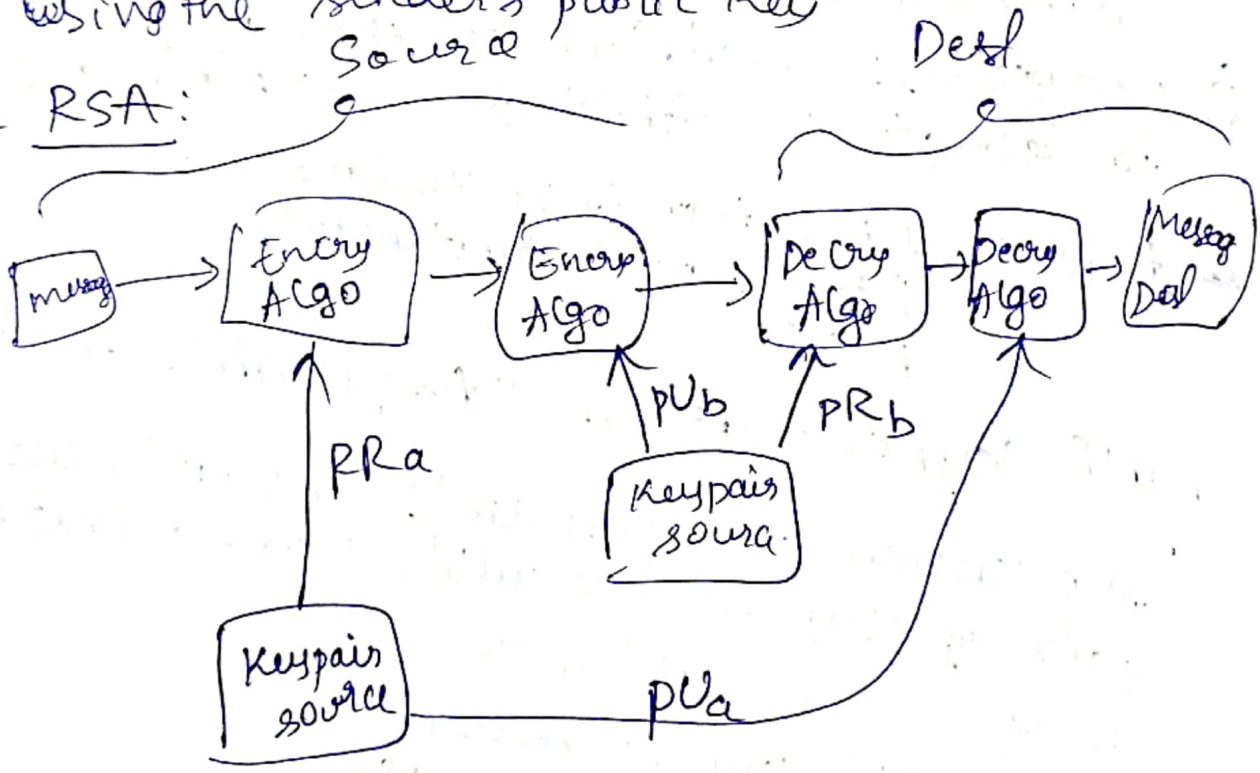
(1) Key pair generation
each participants generate keypair → public key, Private key

(2) Encryption process
sender uses the recipient's public key to encript the message

(3) Decryption process :
recipient uses private key to decrypt the encry messg

(4) Digital signature (Optional in Public Key Encryption)
public key systems can also be used for digital signatures, which verify the authenticity of the sender. The sender uses their private key to create signade, and the recipient can verify it using the sender's public key

Eg RSA:



bob & Alice Eg:

Quiz:

(1) phising is an activity on the internet of the victim, gather all information in the background, and send it to someone else

(2) Antivirus.s/w is a type of software designed to help the user's computer detect viruses & avoid them

(3) Define cryptanalyst?
is someone who specializes in breaking or analysing encrypted data or systems to reveal its content without the original key.

(4) three key elements of CIA triad
Confidentiality, Integrity, Availability

(5) It can be a s/w program or a hardware device that filters all data packets coming through the internet, a network etc. it is known as the Firewall

(6) Define Piracy, Plagiarism
Piracy refers to the unauthorized use or reproduction of someone else's work
plagarism is the act of copying someone else's works & passing it off as your own.

(7) Digital Ethics refers to exploring the appropriate ethical behaviors related to the online environment and digital media platform

(8) Denial of service (DOS) refers to the violation of the principle a computer is no more accessible

(9) Malware is also referred to as malicious s/w

(10) In Wi-Fi security, name the protocol which is used often? WPA2 (Wi-Fi Protected Access 2)

(11) The response time and transit time is used to measure the performance of a network

(12) CIA → Confidentiality, Integrity, Availability

(13) It can be a s/w program or a hardware device that filters all data packets coming through the internet, a network etc. it is known as the firewall.

(14) piracy, plagiarism

(14) When was the first computer virus created?

→ first computer virus → creeper
created in 1971

(15) In the computer networks, the encryption techniques are primarily used for improving the security of data transmitted over the network

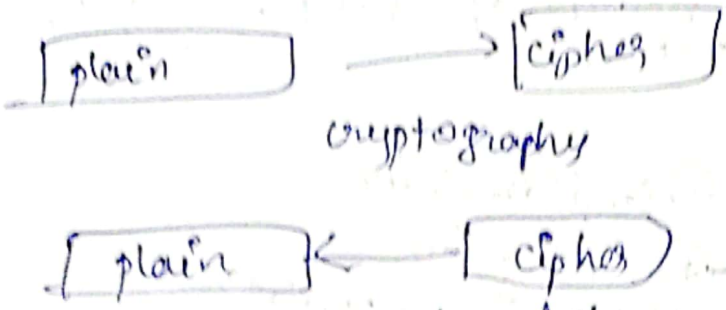
Describe the principles of basic cryptography (features)

Feature/principles:
1. Confidentiality
2. Integrity
3. Non-repudiation
4. Authentication

Types of cryptography:
1. Symmetric Key Cryptography
2. Hash functions → used for passwd encryption → hash value with fixed length per plaintext
3. Asymmetric Key Cryptography

Appln of cryptography:
1. Computer passwords
2. Digital currencies → prevent fraud transaction
3. Secure web browsing → to prevent eavesdrop → Man-in-middle
4. Electronic signature → handwritten → digital sign
5. Authentication
6. Crypto currencies → Bitcoins → safeguard transaction
7. End-to-End Encryption

Adv:
1. Access control
2. Secure communication
3. Protection against attacks
4. Compliance with legal requirements



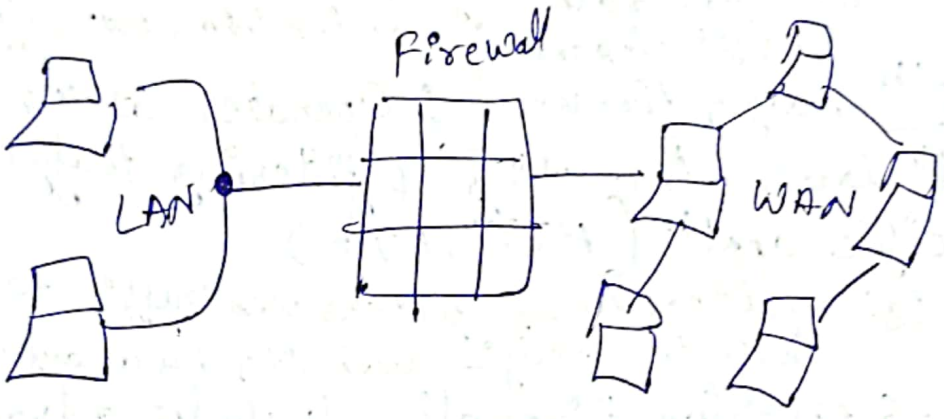
→ cryptology is parent of cryptography

cryptography	cryptology
① process of conversion of plain ⟶ cipher text	① plain ⟶ cipher text & vice versa
② called as studies of encryption	② studies of encryption & decryption
③ takeplace on sender side	③ sender & receiver side
④ sender sends msg to receiver	④ both send msg to each other
⑤ is child of cryptology	⑤ pareent of cryptography
⑥ deals with techniques of secure comm^{n}	⑥ Study of secure comm^{n}
⑦ focuses on practice of hiding info	⑦ focuses on theoritical & mathematical aspects of information security
⑧ involves encry+decrypt authentication technique	⑧ Involves study of codes, ciphers & cryptanalysis
⑨ is concerned with developing algorithms & protocols	⑨ concerned with analysing & breaking existing encryption methods
⑩ utilized in various fields such as finance, e-commerce and national security	⑩ utilized in academia & research to understand & improve encryption
⑪ Cryptography includes application such as secure messaging, secure file transfer, and digital signature	⑪ includes appl^{n} such as cryptanalysis, code breaking & mathematical Analysis of encryption methods

Symmetric	Asymmetric
(1) 1 Key ← both Enc, Dec	(1) 2 Keys
(2) ciphertext same/smaller than OG text	(2) same/larger
(3) encry → fast	(3) slow
(4) large amount of data can be transfered	(4) small amt
(5) only → confidentiality	(5) → confi → authenticity → Non-repudiation
(6) security less	(6) security more
(7) AES, DES	(7) RSA, DSA, Diffie-Hellman
$P = D(K, E(K, P))$	$P = D(K_d, E(K_e, P))$

Illustrate with a neat diagram concept of Firewalls and types of firewalls with examples.

A firewall is a network security device, either h/w or s/w which monitors all incoming & outgoing traffic and based on a defined set of security rules accepts, rejects or drops that specific traffic



A firewall is essentially the wall that separates a private internal network from the open internet

its very basic level

→ Access Control List

↓

not able to analyse the Nature of packet

Types:

① Packet filtering Firewall: Filters traffic based on src/dst IP addresses, ports & protocol, Inspects traffic at 1st three layer of OSI

Eg: blocking incoming packets from a specific networks/services, home router firewall

② Stateful Inspection Firewall: Tracks the stateful active connections, makes filtering decisions based not only on predefined rules but also history of packets in the connection state table

Eg: Cisco ASA → tracks state of connection

③ S/W Firewall: Installed locally ~~or~~ on cloud servers to control data packet inflow & outflow. Typically slower and more time-consuming to config

Eg: Windows Firewall on PC → block specific pgm from accessing the internet

④ Hardware Firewall: A physical appliance that protects the N/W by blocking malicious data b/fr it reaches end point

Eg: FortiGate → for business → protects entire N/W by filtering traffic coming into & out, blocking malicious tk

⑤ Appl^n Layer firewall: Operates at the OSI appl^n layer, inspecting & filtering traffic for specific appl^n (HTTP, FTP)

Eg: Squid proxy → filters web traffic to block access to specific websites by analysing HTTP traffic

⑥ Next-Generation Firewall: Includes advanced features like deep packet inspection, appl^n inspection and SSL/SSH inspection, provides protection against modern, sophisticated threats

Eg: Palo Alto NGFW → filter traffic + inspects the content of malware

⑦ Proxy service Firewall: Filters traffic at the appl^n layer acting as a gateway btw 2 N/W for specific appl^n

eg: Blue Coat ProxySG → gateway btw company internal N/W & the internet

⑧ Circuit level gateway Firewall: Operates at the session layer of the OSI model establishing TCP conn^n without inspecting the data packets. Less effective in blocking malware if the conn^n are correctly established

Eg: Checkpoint Firewall → controls sessions btw trusted devices

→ Host based firewall ⇒ individual device
⇒ entire device
⇒ windows Firewall

→ N/W base firewall ⇒ N/W perimeter
⇒ entire N/W / org
→ deployed btw org internal N/W & Internet

ate with examples attackers techniques &

sations

phishing
) DoS | DDoS
) SQL Injection
) Man-in-the-Middle
) Malware (Ransomware, Trojans, Viruses)

Motivations:

① Financial Gain
② Revenge / Personal Vendetta
③ Political or Ideological motivations (Hacktivism)
④ Intellectual property theft
⑤ Espionage - military advantage

Discuss Virtual Machine Obfuscation related to cyber security? Justify how it is useful in a virtual env. to mitigate modern threats?

VM Obfuscation is a technique used to hide the internal structure and behaviour of a virtual machine to protect it from being analyzed or attacked. This is specially important in environments like cloud computing where VM are shared & vulnerable to cyber threats

How it works: Obfuscation modifies the VM's code, process and configuration to make it harder for attackers to understand or reverse-engineer. This makes it difficult for malicious actors to exploit vulnerabilities or target the VM with specific attacks

Benefits in Mitigating Modern Threats:

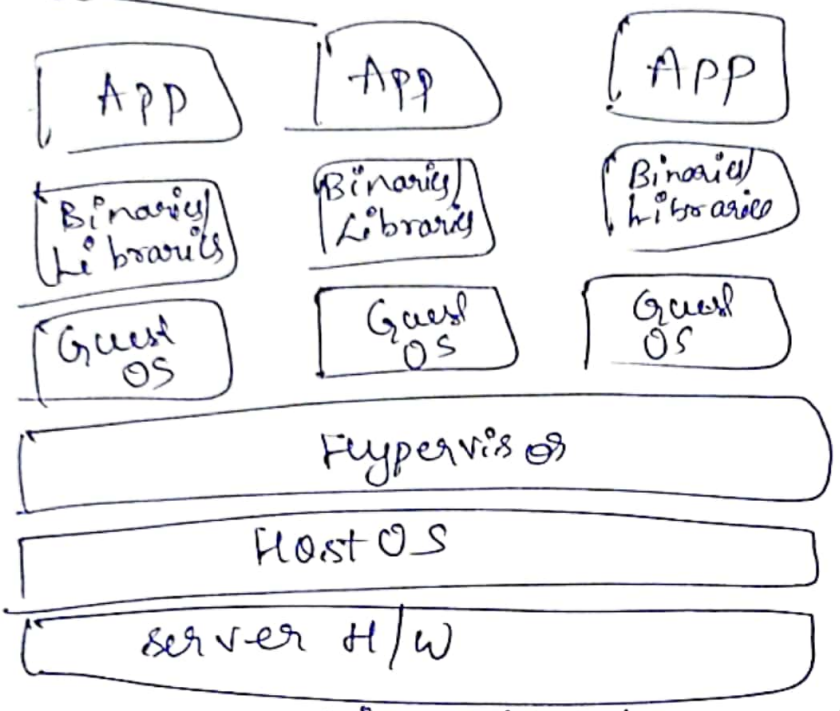
(1) Prevent Reverse Engineering: Obfuscation makes it difficult for attackers to analyze malware or VM vulnerabilities, reducing the risk of successful attacks.

(2) Protect Cloud Systems: In cloud env., where multiple users share resources, obfuscation prevents malicious users from accessing or affecting other VMs

(3) Evasion & Detection: Security tools may find it harder to detect hidden threats because the VM's processes are disguised, making attacks harder to spot.

(4) Defense Against Advanced Attacks: Obfuscation disrupts advanced attackers who use stealth techniques to infiltrate systems, increasing the complexity & their efforts.

Virtualization



Drawbacks:
- High initial Investment
- Learning new Infrastructure
- Risk of data

Characteristics
- Increase Security
- Managed Execution
- sharing
- Aggregation (Resource aggregation)

Benefits:
- Flexible / efficient allocation of resources
- Enhance dev productivity
- Lower cost of IT infrastructure
- Remote access & rapid scalability
- High availability & disaster recovery
- Pay per use of the IT infrastructure on demand
- Enables running multiple OS

Types:
- Application
- Network (Switches, Routers, VPN, firewall)
- Desktop
- Storage
- Server
- Data