• Computer Networking

→ A computer network is a system that connects numerous independent computers in order to share information (data) and resources.

• It can be established using either cable or wireless media.

• N/w and S/w are used to connect computers and nodes in any network.

• A computer network consists of various kinds of nodes.

• Servers, networking hardware, personal computers etc. → Host names and network addresses are used to identify them.

• Working of Computer N/ws.

→ It simply works using nodes and links.

→ Data communication equipment is simply termed as NODES.
Eg Modems, hubs, Switches etc.
Link :- In computer n/ws can be referred to as a connection b/w 2 nodes.
We have several types of links like cable wires, optical fibres etc.

When a computer Network is working, nodes have the work of sending and receiving data via the links.

Comp N/w provides some set of protocols that help in following the rules & protocols.

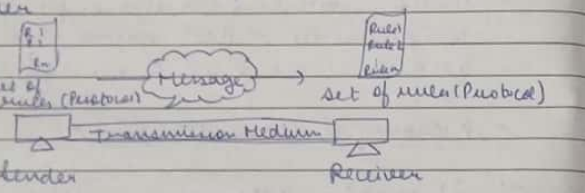
* Components of Data Communication System:

- Data Communication is defined as exchange of data between 2 devices via some form of transmission media such as a cable, wire etc.

- Data Communication System Components:

→ There are mainly 5 components of a data communication system.

[1] Message
[2] Sender
[3] Receiver
[4] Transmission Medium
[5] Set of rules (Protocol)



[1] Message

→ This is the most useful asset of a data communication system. It refers to a data or piece of information which is to be communicated. It could be in any form. Eg Text file, audio file, video file etc

[2] Sender

→ Sender plays a part of the source to transfer messages to destination in data communication system. It sends data message. Eg Computer, mobile, telephone, laptop, video camera, workstation etc

[3] Receiver

→ It acts as a destination where finally message sent by source has arrived. It is a device that receives message.
Eg. Computer, telephone, mobile, workstation etc

[4] Transmission Medium:

→ It acts as a bridge between sender and receiver. It is a physical path by which data or message travels from sender to receiver. It could be guided (with wires) or unguided (without wires).
Eg. Twisted pair cable, radio waves, microwaves etc.

[5] Set of rules (Protocol):

→ These are the set of rules that govern data communications ~~between computers on a n/w~~ → n/w Protocol
Communication between sender & receiver is not possible without protocol.
Elements of protocol:
① Syntax: It is the structure or the format of the data that gets exchanged

between the devices. It includes type of data, composition of message and sequencing of message
Starting 8 bits of data → address of the sender
Next 8 bits of data → address of the receiver
Remaining bits are considered as the message itself

(2) Semantics - It defines data transmitted between devices. It provides rules and norms for understanding message or data element values and actions.

(3) Timing - It refers to the synchronization and coordination b/w devices while transferring the data. Timing ensures at what time data should be sent and how fast data can be sent.
Eg. If a sender sends 100 Mbps of data but the receiver can only handle 1 Mbps, the receiver will overflow and lose data. Timing ensures data loss, collisions and other timing related issues.

(4) Sequence Control - It ensures proper ordering of data packets. It acknowledge the data while it gets received and the retransmission of lost data.
By following this mechanism the data is delivered in correct order.

(5) Flow Control - It regulates device data delivery. It limits the sender's data or asks the receiver if it's ready for more. It prevents data congestion and loss.

(6) Error Control - It detect and fix data transmission faults. It include error detection codes, data resend and error recovery. It detects and corrects noise, interference and other problems to maintain data integrity.

(7) Security - Network security safeguards data confidentiality, integrity and authenticity which includes encryption, authentication, access control. Network communication's privacy and trustworthiness are protected by security standards.

Example - of Data Communication system is sending an e-mail. The user which send email acts as a sender, message is data which user wants to send message, receiver is one whom user wants to send message, there are many protocols involved in this entire process, one of them is Simple Mail Transfer Protocol (SMTP), both sender and receiver must have an internet connection which uses a wireless medium to send & receive email.

Page No. 6
Date / /

- Cyber Security:

→ It is the technique of protecting internet-connected systems such as computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks.

Cyber Security → Cyber + Security

→ Cyber refers to the technology that includes systems, networks, programs, and data.

→ Security is concerned with the protection of systems, networks, application and information.

It is also called electronic Information Security or Information Technology security.

→ Types of Cyber Security:

- Every organization's assets are the combinations of a variety of different systems.
- These systems have a strong cybersecurity posture that requires coordinated efforts across all of its systems.

(1) Network Security:

① It involves implementing the hardware and software to secure a computer network from authorized access, intruders, attacks, disruption, and misuse.

② This security helps an organization to protect its assets against internal & external threats. It involves technologies such as

Page No. 7
Date / /

- Segmentation → It divides a computer network into smaller parts. Its purpose is to improve network performance & security.

(2) Application Security: Eg. Firewalls, Intrusion

→ It involves detection systems (IDS), Virtual Private networks (VPN), network segmentation.

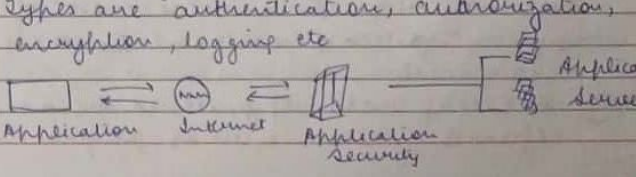
(a) Internal Threat	External Threat
① It refers to risks that originate from within an organization	① These are risks that arise from outside the organization.
② These can include action or oversights by employees, system vulnerabilities or operational failures	② These can include cyber attacks, natural disasters, economic fluctuations, or even regulatory changes.
③ Eg. Data breaches caused by employees mishandling sensitive information or unauthorized access to confidential data can be considered.	③ These threats are beyond the direct control of the organization, making it essential to identify and prepare for them proactively

(3) Application Security

→ ① It involves protecting the software & devices from unwanted threats.

② This protection can be done by constantly updating the apps to ensure they are secure from attacks.

③ Types are authentication, authorization, encryption, logging etc.



(3) Information or Data Security
→ It involves strong implementing a strong data storage mechanism to maintain the integrity and privacy of data, both in storage and transmit

Types:
(a) Access Controls:
(1) It includes both limiting both physical and digital access to critical systems and data
(2) It includes making sure all computers and devices are protected with mandatory login entry, and the physical spaces can only be entered by authorized personnel

(b) Authentication:
(1) It refers specifically to accurately identifying users before they have access to data.
(2) It includes things like password, PIN numbers, security tokens, swipe cards or biometrics

(c) Backups & Recovery:
(1) Good data security means a plan to securely access data in the event of system failure, disaster, data corruption, or breach.
(2) A backup data copy, stored on a separate format such as physical disks,

local network, or cloud to recover in case of failure

(d) Data Erasure
(1) Disposal of data properly on a regular basis is required
(2) Data erasure employs software to completely overwrite data on any storage devices and is more secure than data wiping
(3) It verifies that the data is unrecoverable and won't fall in wrong hands.

(e) Data Masking
(1) This software is used in hiding information by obscuring letters and numbers with proxy characters
(2) It effectively marks key information even if an unauthorized party gains access to it.
(3) The data changes back to its original form only when an authorized user receives it.

(f) Data Resiliency
(1) Data secure means that your systems can endure or recover from failures.
(2) Building resiliency into your hardware and software means that events like power outages or natural disasters won't compromise security.

(4) Encryption:
(1) A computer algorithm transforms text characters into an unreadable format via encryption keys.
(2) Only authorized users with the proper corresponding keys can unlock and access the information.

* Main Elements of Data security
(1) Confidentiality: It ensures that the data is accessed only by authorized users with proper credentials.

(2) Integrity: It ensures that all data stored is reliable, accurate, and not subject to unwarranted changes.

(3) Availability: It ensures that the data is readily and safely accessible and available for ongoing business needs.

(4) Identity Management
It deals with the procedure for determining the level of access that each individual has within the organization.

(i) Role-Based Access Control (RBAC):-
→ It assigns permissions based on predefined roles.

(ii) User-Based Access Control (UBAC)
→ It associates access permissions directly with individual users.

(iii) Biometric Access Control
→ It uses biometrics like fingerprints or facial recognition for authentication.

(iv) DaaS (Identity as a Service)
→ Cloud-based identity management with authentication and access control.

(5) Operational Security:
It involves processing and making decisions on handling and ~~security~~ securing data assets.

(1) Data Classification
→ Categorizing data based on sensitivity to prioritize security measures.

(2) Access Control
→ Managing who can access data and what actions they can perform.

(3) Backup & Recovery:
→ Regularly backing up data and having plans for data restoration.

(6) Mobile Security:
① It involves securing of the organizational and personal data stored on mobile devices such as cell phones, computers, tablets against various malicious threats.
② These threats are unauthorized access, device loss or theft, malware etc.

(7) Cloud Security:
① It involves in protecting the information stored in the digital environment or cloud architectures for the organization.
② It uses various cloud service providers such as AWS, Azure, Google etc. to ensure security against multiple threats.

(8) Disaster Recovery and Business Continuity Planning
① It deals with the processes, monitoring, alerts, and plans how an organization responds when any malicious activity is causing the loss of operation or data.
② Its policies dictate resuming the lost operation after any disaster happens to the same operating capacity as before the event.

(9) User Education
① It deals with the processes, monitoring, alerts, and plans to how an organization

responds when any malicious activity is causing the loss of operation or data.
② Its policies dictate ~~the~~ resuming the lost operation after any disaster happens to the same operating capacity as before the event.

* Need of Cyber Security:

① Protecting ~~An~~ Sensitive Data:
→ With the increase in digitalization, data is becoming more & more valuable. Cybersecurity helps protect sensitive data such as personal information, financial data, and intellectual property from unauthorized access and theft.
Common reasons of data breaches are:
(i) Weak & stolen credentials
(ii) Malicious insiders
(iii) Application vulnerabilities
(iv) Human Error

→ To prevent from data theft:
· ensure your device is secured by endpoint security
· lock down your system
· identify critical data
· use authentication

② To prevent virus and malware
→ Cyber security is important to protect from computer viruses and malware. A

computer virus or malware can corrupt or delete your sensitive data, damage your hard disk and it spreads from one computer to another using email program and others.

- To protect your computer from viruses:-

(a) Keep your software up to date.
(b) Use professional antivirus software
(c) Use a strong password
(d) Don't click suspicious email links
(e) Back up your computer data
(f) Browse only trusted & secured websites.

(3) To protect Personal Information
→ To prevent from cyber security risks you have to protect your personal information. IT security is one prime issue to protect your personal and others information.

- To keep your information secure:-

(a) Use an Antivirus Software.
(b) Update your computer Operating System
(c) Use strong & smart password
(d) Backup your sensitive data
(e) Lock your computer for safety
(f) Avoid Phishing emails

National security

(4) To protect Organization Properties
→ Cyber attacks can be used to compromise national security by targeting critical infrastructure, government systems, and military installations.

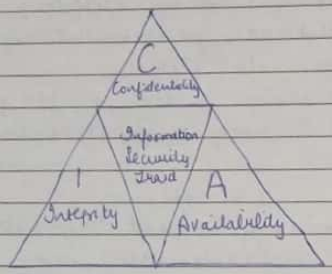
- Cyber security is critical for protecting national security and preventing cyber warfare.

(5) Safeguarding Critical Infrastructure
→ Critical infrastructure, ~~user~~ including power grids, transportation systems, healthcare systems, and communication networks, heavily relies on interconnected computer systems. Protecting these systems from cyber threats is crucial to ensure smooth functioning of essential services and prevent potential disruptions that could impact the public safety & national security.

- Objectives of Cyber Security:-
→ To protect information from being stolen, compromised or attacked. It can be measured by goals:-

(1) Protect the confidentiality of data.
(2) Preserve the integrity of data
(3) Promote the availability of data for authorized users.

- Basics of all security Programs are CIA (Confidentiality, Integrity, Availability).



(1) Confidentiality

→ It is equivalent to privacy and avoids the unauthorized disclosure of information.

→ It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about its content.

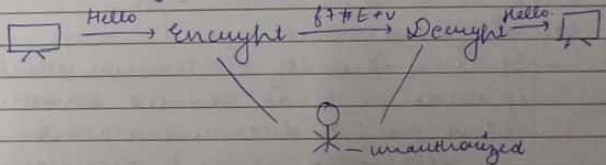
→ It prevents essential information from reaching the wrong people while making it sure that the right people can get it.

Eg Data Encryption

Tools: Encryption
Access Control
Authentication
Authorization
Physical security

(a) Encryption:

- It is the process of converting data into unreadable text using an algorithm and a secret encryption key.
- This ensures that only those with corresponding decryption key can decipher the information.
- It safeguards sensitive data like credit card numbers, with symmetric key and asymmetric-key encryption.



(b) Access Control:

- It sets rules and (regulations) policies for regulating system or resource access.
- It involves granting users access and privileges based on presented credentials like username or serial number.
- Security is enhanced when credentials are non-transferable, ensuring proper access control in both physical & virtual systems.

(c) Authentication:

- It confirms a user's identity via something.
- It is a process that ensures and confirms a user's identity or roles that someone has.

It can be done in a
(a) Something the person has (like a smart card or radio key for storing secret key)
(b) something the person knows (like a password)
(c) Something the person is (like a human with a fingerprint)

- It is crucial for security, permitting only authorized users to access protected resources like systems, networks, and databases in organizations.

(d) Authorization
- It is a security mechanism which gives permission to do or have something.
It is used to determine a person or system is allowed to access to resources based on an access control policy, including computer programs, files, services, data and application features.
- It is preceded by authentication
- System administrators are assigned permissions levels covering all system & user resources
- During authorization, a system verifies an authenticated user's access rules & either grants access or refuses resource access.

(e) Physical Security
- It describes measures designed to deny the unauthorized access of IT assets like

facilities, equipment, personnel, resources & other properties from damage.
- It protects these assets from physical threats including theft, fire and natural disasters.

(2) Integrity

→ (i) It refers to the methods of ensuring that data is real, accurate & safeguarded from unauthorized user modification.
→ It is the property that information has not be altered in an unauthorized way, and that source of information is genuine.

Tools: Backups, Checksums, Data Correcting Codes

(a) Backups
→ (i) It is the periodic archiving of data. It involves making copies of data for recovery in case of loss or damage.
(ii) It serves historical, statistical, and data retention purposes.
(iii) It have extension like .BAK.

(b) Checksums:
(i) It is a numeric value used to verify file or data integrity
(ii) It maps file content to a numerical value, detecting even minor changes
(iii) It is used to prepare data sets & ensure they match.

(c) Data Correcting Codes
→ It is a method for storing ~~for~~ data in such a way that small changes can be easily detected & automatically corrected.

(3) Availability

→ It is the property in which information is accessible and modifiable by those authorized to do so.
→ It is the guarantee of reliable and constant access to our sensitive data by authorized people.

Tools: Physical Protection
Computational Redundancies

(a) Physical Protection
→ Physical safeguard means to keep information available even in the event of physical challenges. It
It ensures sensitive information &

and critical IT are housed in secure areas

(b) Computational redundancies
→ It is applied to as fault tolerant against accidental faults.
→ It protects information computers and storage devices that serve as fallbacks in the case of failures.

	Confidentiality	Integrity	Availability
	The information is safe from accidental or intentional disclosure	The information is safe from accidental or intentional modification or alteration	The information is available to authorized users when needed
Eg.	(2) I send you a message and no one else knows what message is	I send you a message, and you exactly receive what I sent you (without any modification)	I send you a message, and you are able to receive it
Purpose	Data is not disclosed	Data is not tampered	Data is available
How you can achieve	Eg. Encryption	Eg. Hashing, Digital Signatures	Eg. Backups, redundant system
Opposite of CIA	Disclosure	Alteration	Destruction

* Utility

(1) It refers to a concept of data or information being useful and accessible.
(2) in, Breaches of utility occurs when data becomes inaccessible or unusable, like losing encryption keys or using inappropriate formats.

Eg - An employee was asked to send an encrypted copy of the company's employee database to a data mining company. They used an encrypting drive, assigned a key but then forgot it. The data mining company received the drive but couldn't access the data without the key.

* Thus availability ensures information is accessible but it doesn't guarantee its usefulness or practicality in its current form.

* Authenticity

→ It validates the source or origin of data and other file transfers through proof or identity.
→ It is important because it ensures that the message (email, payment transaction, digital file etc.) was not corrupted or intercepted during transmission.

(3) Users can verify their identities by providing specific credentials including
(1) Login information (username & password)
(2) Biometric data
(3) electronic or digital signatures
(4) Authentication Tokens
(5) Smart cards

- Passwords & tokens can be hacked or lost :- so we require one authentication factor with either 2FA (2-Factor authentication) or mfa (multi-factor authentication).

- Hashing
→ It is a common method for data security as it converts data into a unique, randomized hash value using algorithms.

- MAC & HMAC :- can also be used to ensure both authenticity and integrity.

MAC - A small value or short piece of information used to authenticate data.

HMAC :- A type of MAC obtained by using a cryptographic hash function combined with a cryptographic key.

Date / /

NON-REPUDIATION:

(1) It is the assurance that prevents either sender or receiver from denying a transmitted message or a transaction.

(2) When a message is sent, the receiver can prove that the alleged sender in fact sent the message or vice-versa. [i.e when a message is received, the sender can prove that the alleged receiver in fact received the message.]

(3) It aims to prevent disputes arising from claims of forgery, data tempering or denial of receipt.

* It is crucial for:

(a) Trust Assurance: Digital signatures build trust by confirming identities & data integrity in digital transaction.

(b) Accountability & Tracking: It establish accountability, creating a digital trail for dispute resolution and detecting malicious actions.

(c) Legal Requirements: Various sectors, like finance, healthcare, and government, mandate digital signatures for legal compliance.

Page No. 25.
Date / /

* Mechanisms to achieve Non-Repudiation:

(a) Digital Signatures
(b) Digital Timestamps

(A) Digital Signatures

→ Based on public key cryptography.
It is a mathematical algorithm that securely associates a signer with a document or a message.

Steps:

(a) Hashing:- The original msg is transformed into a fixed-size hash to maintain its integrity.

(b) Encryption:- The hash is encrypted using the sender's private key, creating a unique digital signature.

(c) Verification: The recipient uses the sender's public key to decrypt & verify the sender's identity and message authenticity.

(B) Digital Timestamps

→ These are used to prove the existence of a document or a message at a specific time.

→ A trusted timestamp authority (TSA) provides timestamp services, ensuring the integrity of the timestamp and preventing tampering.

* Working:

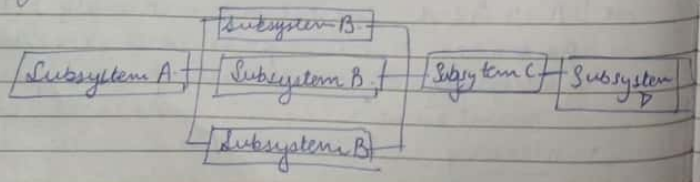
* Tampering - unauthorized or malicious changes including alteration, deletion or modifications.

(1) Hash Computation: Sender computes the document/message hash.
(2) TSA Timestamp: It provides a timestamp signing it with the hash. It sends to sender.
(3) Timestamp Proof: Sender can prove document/message existence at the timestamped time.

* RELIABILITY:

→ It is the degree to which a network is trustworthy, consistent, and dependable. The reliability of a network is measured by the frequency of failures it is undergoing and the time it takes to recover from failures. The robustness of the Network at times of catastrophic Calamities like earthquake, wildfire etc) events is measured to check how reliable the Network is.

- A reliability block diagram is a diagrammatic method for showing how component reliability contributes to the success or failure of a redundant.



(1) Representation of components → RBDs use blocks or switches to depict system components. Closed switches or II blocks indicate redundancy, enhancing reliability.
(2) Parallel Redundancy: Parallel blocks may require a specific number of components to succeed, thus providing fault tolerance.
(3) Series Path Vulnerability: In a series path, any failure along its lead to the entire series path failing, highlighting its vulnerabilities.

* Repudiation

(1) This type of attack is different from others because it is performed by one of the 2 parties in the communication: the sender or the receiver.
(2) The sender of the message might ~~to~~ later deny that she has sent the message; the receiver of the message might later deny that she has received the message.
(3) Example of denial by the sender would be a bank customer asking her bank to send some money to a third party but later denying that she has made such a request.
(4) Example of denial by the receiver could occur when a person buys a product from a manufacturer and pays for it electronically, but the manufacturer later denies having received the payment and asks to be paid.

Page No. 26.
Date / /

* ATTACKS:-

- A cyber attack is any attempt to gain unauthorized access to a computer, computing system or computer network with the intent to cause damage.
- Cyber attacks aim to disable, disrupt, destroy or control computer systems or to alter, block, delete, manipulate or steal the data held within these systems.
- Any individual or group can launch a cyber attack from anywhere by using one or more various attack strategies.

Cybercriminals:- People who carry out cyber attacks

Weaknesses or problems in the computer systems: Vulnerabilities

Why cyber attacks happen?

→ Cyber attacks are designed to cause damage. Objectives:

(a) Financial gain:- Cybercriminals often launch attacks to target sensitive data like credit card info. or personal details.
- They may lock systems and demand ransoms or engage in corporate spying to steal valuable data.

Threat actors or hackers :- Bad Actors

Page No. 27.
Date / /

(b) Disruption & Revenge:
- Aim to cause chaos, mistrust or embarassment.
- May seek revenge or tarnish an entity's reputation.
- It targets government, commercial or non profit organizations. Nation-state actors & hacktivists are often involved.
- Insider threats can come from malicious employees

Hacktivists:- They launch these types of attacks as a form of protest against the targeted entity. (more often to aid an ideological reason rather than financial gain)
Eg. Anonymous:- A secretive decentralized group of internationalist activists.

(c) Cyberwarfare:- Government around the world are also involved in cyber attacks, with many national governments acknowledging or suspected of designing & executing attacks against other countries as part of ongoing political, national economic & social disputes.

Threat actors use various techniques to launch cyber attacks:-

(1) Unexpected Attacks:- Bad actors try to break into as many devices as possible, seek software vulnerabilities that will enable them to gain access without being detected or blocked.

- They also use phishing emails to tempt recipients into clicking a link that downloads malicious code.

Dark Web :- Cybercriminals often create their own attack tools & share them on the dark web.

- Classification of Cyber Attacks :-

(1) Web-based attacks :
→ Attacks which occur on a website or web application.
Eg. SQL Injection, Brute Force, Phishing, Man-in-the-middle (MITM) attack.

(2) System-based attacks :
→ Attacks which are intended to compromise a computer or a computer network.
Eg :- Virus, Worm, Trojan horse, Backdoors.

Types of Cyber Security Threats :-

I MALWARE :-
→ It means malicious software.
→ It refers to any software that is designed to cause harm to computer systems, networks, or users.
→ Cybercriminals use it to extract data they can use against victims to their advantage in order to profit financially.

legitimate → genuine.

→ It is used to disrupt or damage a legitimate user's system.
Eg. financial information, medical records, personal emails, passwords etc.

Why do cybercriminals use malware??
Ans (1) Using deception to induce a victim to provide personal information for identity theft.
(2) Theft of customer credit card information or other financial information.
(3) Taking over several computers & using them to launch denial-of-service attacks against other networks.
(4) Using infected computers to mine for cryptocurrencies like Bitcoin.

→ Types of MALWARE :-

(1) Virus :-
→ It means Vital Information Resources Under Siege
important processed data under attack / threat

It implies that the critical information & data within a computer system or network are under attack or threat by malicious software or cyber threats. It emphasizes the idea that the integrity & availability of important information are being compromised or attacked.

VIRUS:-

→ Virus is a malicious executable code attached to another executable file. The virus spreads when an infected file is passed from system to system. Viruses can be harmless or they can modify or delete data.
Once a program virus is active, it will infect other programs on the computer.

(2) WORMS

→ It stands for Written Once Read Many Times.
→ It replicate themselves on one system, attaching themselves to different files and looking for pathways between computers, such as computer network that shares common file storage areas.
• Worms usually slow down networks. A virus needs a host program to run but worms can run by themselves. After a worm affects one host, it is able to spread very quickly over the network. Eg. ILOVEYOU.

(3) TROJANS:-(Trojan Horse Virus)

→ These are deceptive programs that appear to perform one function, but in fact perform another, malicious function. They might be disguised as free software, videos or music,

• bait → Website set up with intent to deceive visitors to download malware including personal info. or other harmful activities. They are designed to appear legitimate but their goal is to exploit or trick user.

on seemingly legitimate advertisements or file to fool us into downloading & running.
• Primary purpose → To corrupt or steal data from a device or do another harmful activity on a network.
• They are installed through social engineering techniques such as phishing or bait websites or user downloads a program whose publisher is unknown or unauthorized by organizations security policies.

(4) RANSOMWARE

→ Ransomware grasps a computer system or the data until it contains until the victim makes a payment.
→ It encrypts data in the computer with a key that is unknown to the user.
→ The user has to pay a ransom (price) to the criminals to retrieve data.
→ Once the amount is paid the victim can resume using his/her system.
Eg. Bitcoin

(5) SPYWARE

→ It performs certain tasks that include watching & tracking of user actions and collecting personal data. These programs generally install themselves

on users computers and provides profit to the third party by collecting data of users without his awareness. It steals passwords and personal information of the users by running in background in the system.

→ It cannot self-replicate & can be detected & removed by the antispyware program

Eg ⇒ It could capture credit card details that can be used by cybercriminals for unauthorized shopping, money withdrawing etc.

(6) ADWARE

→ It stands for Advertising-supported software designed to throw advertisements up on your screen, most often within a web browser.

→ It is a type of malicious software that secretly installs itself on your device & display unwanted advertisements and pop-ups.

→ It can even track your online behaviours & display personalized ads.

→ Eg Pop-up advertising, un-closable panels, other forms of harmful adware can infect PCs

- Objective: Generate revenue for its developers by showing unwanted ads to users.

How to Remove ADWARE?

(1.) Create a backup of your data

(2.) Download or update your security software

(3) Uninstall programs that are not in use

(4) Use an adware and PUAs (Potentially Unwanted Applications cleanup application to run a scan

(7) BOTNETS:

→ It stands for Robot Network.

→ It refers to a network of computers infected by malware that are under the control of a single attacking party called bot-herder.

→ Each individual machine under the control of bot-herder is known as a bot.

→ [Bot is also called zombie. & a botnet is referred to as a zombie Army]

→ Objectives:-

(1) Data Theft: Botnets can be used to steal sensitive data, such as login credentials or financial information, from infected computers.

(2) DDoS: Botnets are often used to launch DDoS attacks, where a large no. of infected computers flood a target server with traffic, rendering it unavailable

(3) Distributed Computing: Botnets are used for distributed computing tasks such as cryptocurrency mining or password cracking.

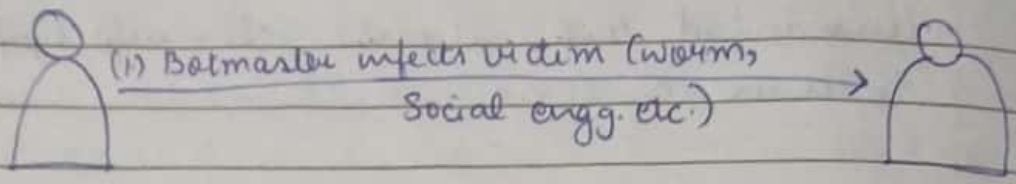
(4) Click Fraud: Botnets generate fraudulent clicks on online ads to generate revenue for the operator

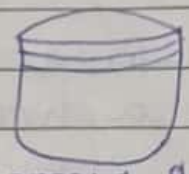
(5) Spam & Phishing: Botnets can send out massive volumes of spam emails or phishing attempts, spreading malware or attempting to steal information

⇒ Eg: Fraud Online Reviews: Where some fake reviews are posted on the device of the user.

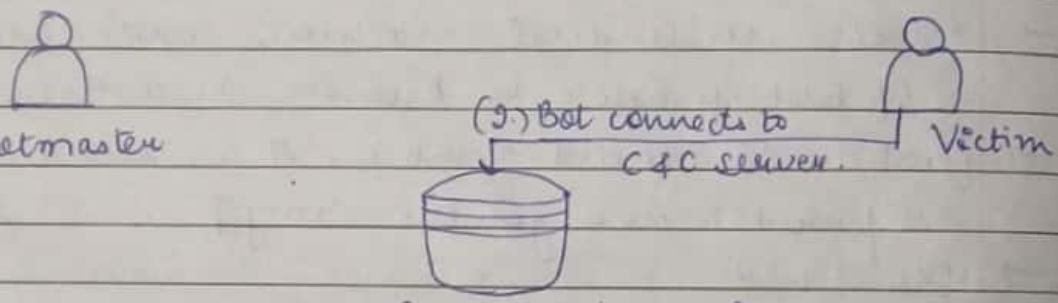
Botnet lifecycle:-

Stage (1)

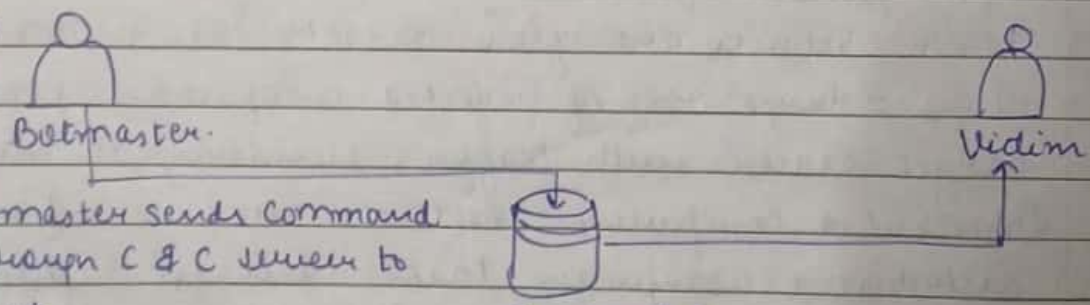




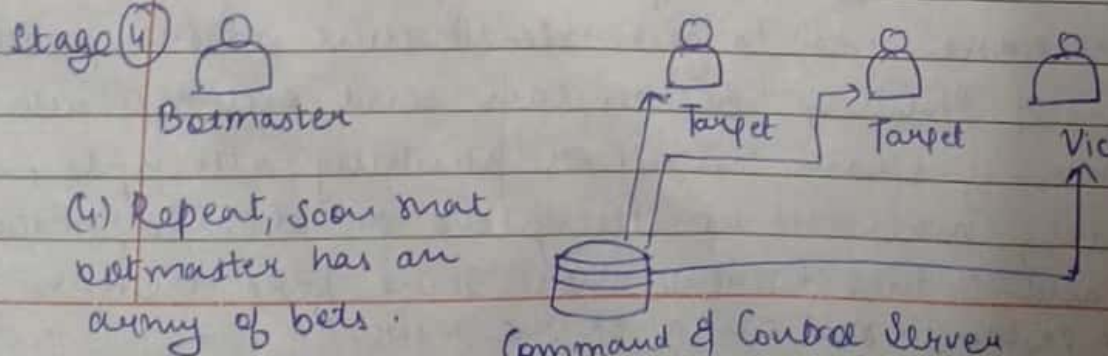
Stage (2)



Stage (3)



Stage (4)



II PHISHING:

→ In a phishing scam, a target is contacted by email, telephone or text messages by someone posing as a close personal contract or on behalf of a legitimate institution.

→ Objective:- To get people to reveal sensitive data such as their account numbers, home address, banking / credit card details and usernames / passwords.

→ The information is then used to access important accounts and can result in identity theft & financial loss.

Types of Phishing attacks:

(A) Email Phishing:
- Fraudsters send deceptive emails mimicking legitimate companies.
- Goal: Obtain sensitive financial & personal information
- Email contains links to fake websites for data collection.

(B) Voice Phishing (Vishing):
- Aims to obtain sensitive information via voice calls.
- Exploits trust, fear, greed, or helpfulness instincts.

(C) Text Phishing (Smishing)
- Uses text message or SMS for attacks.
- Often includes clickable links or return phone numbers.

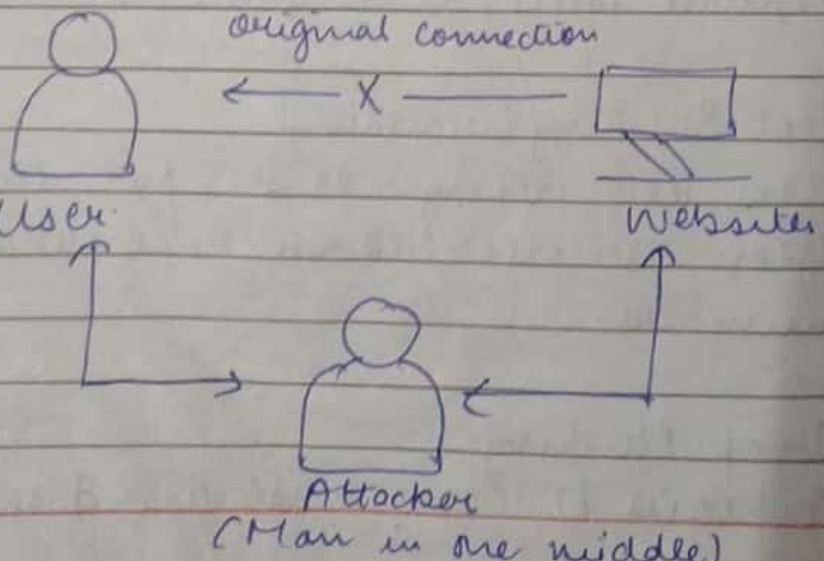
(D) Trap Phishing:
- Exploits IT team mistakes & security vulnerabilities

• eavesdropping: act of secretly listening to a conversation or private communication.
. Invasion of privacy.

Page No. 38.
Date / /

(E) Spear Phishing
. Targets specific individuals, like company system administrators.
. Uses personalized information to craft convincing emails for immediate action.

III Man-in-the-middle (MITM) Attacks:
→ It is a type of cyberattack where attackers intercept an existing conversation or data transfer, either by eavesdropping or by pretending to be a legitimate participant.
→ To the victim, it will appear as though a standard exchange of information is underway- but by inserting themselves into the "middle" of the conversation or data transfer, the attacker can quietly hijack information.
• Objective: To retrieve confidential data such as bank account details, credit card numbers, or login credentials to carry out further crimes like identity theft or illegal fund transfers.



ARP :- Address Resolution Protocol.

2 phases :- Interception & decryption.

[1.] Interception:

→ Attacker insert themselves as a "man in the middle" to intercept data. Creating fake public Wi-Fi hotspots is a common method.

- IP Spoofing → Manipulating IP packets to impersonate the victim
- ARP Spoofing → Linking attacker's MAC address to victim's legitimate IP.
- DNS Spoofing → Altering DNS servers to redirect traffic to fraudulent websites.

[2.] Decryption:

→ After the attacker gains access to the victim's encrypted data, it must be decrypted in order for the attacker to be able to read & use it. Methods used to decrypt. User's data without alerting the user or application:

(1.) HTTPS Spoofing → Sends false certificates to trick the victim's browser, redirecting data to the attacker's site.

(2.) SSL Hijacking → Intercepts reroutes from HTTP to HTTPS, accessing user-server communication.

(3.) SSL Stripping → Downgrades secure HTTPS connections to unsecure HTTP, exposing user activity to the attacker.

IV Distributed Denial of Service (DDoS)

→ It attempts to interrupt a service or network by flooding it with fake internet traffic, preventing user access and disrupting operations.

DDoS attacks are launched from multiple systems while (DOS) Denial of Service originate from just one system.

DDoS attacks are faster & harder to block than DoS attacks.

DoS attacks are easier to block because there is only one attacking machine to identify.

→ After building a massive botnet of million of compromised devices, a DDOS attacker remotely directs each bot to send requests to the target's IP address.

• Objective: Exceed the capacity limits of the victim's web resources with an overwhelming number of connection requests or data to ultimately crash main service.

3 Types:-

(1) Volume-based attacks:

→ Overwhelm with massive traffic.

(2) Protocol attacks:

→ Exploit network protocol weaknesses

(3) Application layer attacks:

→ They target specific online services, overwhelming them with fake requests to disrupt or take them offline.

V Brute Force Attacks:

→ A brute force attack uses a trial-and-error to guess the passwords, login info, or encryption keys to guess a combination correctly.

→ The attacker checks all possible passwords and passphrases until the correct one is found.

Brute force means attackers using excessively forceful attempts to gain access to user accounts.

• Types of Brute Force Attacks:-

(A) Dictionary Attack: Tries common passwords from a list.

(B) Credential Stuffing: Reuses stolen usernames and passwords.

(C) Hybrid Attack: Combines dictionary & brute force methods.

(D) Rainbow Table Attack: Uses precomputed tables to crack passwords.

(E) Online Vs Offline Attacks: Distinguishes between attacking a live system or offline data.

How to prevent brute force password hacking?

→ Enforce the use of strong passwords. Password should:

(1) Have as many characters as possible.
(2) Combine letters, numbers, and symbols.
(3) Avoid common patterns.
(4) Change your password periodically.
(5) Use strong & long password.
(6) Use multifactor authentication.

VI SQL Injection:

→ It is a type of an injection attack that makes it possible to execute malicious SQL statements.

→ These statements / scripts control a database server behind a web application.
It works on vulnerable web pages of apps that use a backend database like MySQL, Oracle, or MSSQL. It enable threat actors to add, update, or remove mis information, permanently altering the application's behaviour.

* Types of SQLi (Injection):

(1.) Classic SQLi: Exploits input fields for unauthorized database access.

Example: 'Select * FROM users WHERE ~~USERNAME~~ username = '' OR '1' = '1';

(2) Blind SQLi: Retrieve data without displaying it, based on true / false responses

Example: 'SELECT * FROM users WHERE username = 'admin' AND '1' = '1';

(3) Time-Based Blind SQLi: Delays database response for interference.

Example 'WAITFOR DELOY '0:0:5'--'

(4.) Out-of-Band SQLi: Exfiltrates data through a different channel.

Example: 'UNION SELECT username FROM users--'

(5.) Second-Order SQLi: Injects malicious code, which executes later.

Example:- Input is stored & executed on another page.

VII: Domain Name System (DNS) Attack:

→ It is a malicious action that targets the DNS architecture and exploits vulnerabilities in it.

DNS:- It translate user-friendly domain names into machine-readable IP addresses.

- Objectives:

(1.) Disruption & Data Theft:- To disrupt the normal functioning of DNS services, causing inconvenience or downtime for users, to intercept DNS queries & responses to gain access to sensitive data.

(2.) Website Manipulation: To redirect users to malicious websites or manipulate the content of legitimate ones.

* Types of DNS attacks:

(A.) DNS Spoofing (DNS Cache Poisoning):

→ Attacker manipulate DNS data to redirect users to malicious websites.

(B.) Domain hijacking:

→ Attackers gain control of a domain owner's

account of DNS records, allowing them to redirect traffic to malicious sites.

(C.) Fast-Flux DNS: Cybercriminals use a constantly changing network (location) of compromised hosts to hid malicious activities & make ~~traf~~ tracking difficult.