Cyber security

1) Malware and Ransomware :-

Malware - a catchall term for any software that is designed to gain unauthorised access to computers or network equipment with goals of causing damage

Ransomware - form of malware

- Encrypts data and files on infected computer and instructs the user to recover their info

2) Phishing and smishing :-

phishing & smishing - social engineering attacks designed to trick user.

3) Business email compromise (BEC) :-

=> A cyber crime that can cost organizations a lot of money if they become victims.

=> They use hacked email accants.

=> considered as spear phishing

=> faking email senders

=> Payroll diversion

⇒ Protection :

- implementing email filtering controls
- Enabling Multi factor Authentication (MFA)

4) Botnets and DDoS attacks :

- ⇒ Botnet - a collection of computers or internet of things devices, which have been infected by malware, allowing a malicious actor to take remote control of them

⇒ Compromised system - part of botnets

- can't able to control their own actions.

⇒ DDoS - an attempt to make an online service.

- used for exortion

⇒ Protection :

- Firewalls or WAFs - used to detect and block unwanted and abnormal traffic.

* By using load balancers or CDNs -

Shares the traffic loads across servers in different locations to water down The DDoS attack.

* DDos defense system - specialize in protecting organizations from These attacks.

* Cloudfare for instance - provides a services to absorb DDoS traffic.

* A good network monitoring system -

detects unusual internet traffics

5) <u>zero - Day</u> attacks:

⇒ An exploit that target a vulnerability in software or hard ware unknown to the vendor and users.

⇒ leads to data breaches, financial loss, physical damage.

⇒ Mitigating : * updating softwares & systems

* Robust patch

* threat intelligence

* SIEM - analyse patterns and behaviours to spot anomalies.

6) AI -Based cyber attacks:

=) Criminals are leveraging advanced AI Software to execute a variety of cyber crimes such as deepfake audio and video attacks.

=) Can enhance phishing attacks.

7) Advanced persistent threats (APTs):

=) A prolonged and targeted cyber attack in which an intruder gains access to a network, and remains undetected for an extended period.

=) By passes security defenses.

=) Process : Reconnaissance → gain entry through Phishing → establishes a foothold → Escalate privileages → data exfilteration.

=) leads to data breaches, financial losses, reputational damage, risks to national security.

8) Insider threats:

⇒ Sabotage - to damage systems or destroy data.

⇒ Fraud - involves criminal transactions.

⇒ Espionage - steals sensitive data.

⇒ SIM - Collect and analyzes event logs activity from all your systems and helps to identify suspicious or malicious activity.

9) Unmanaged IoT Devices:

⇒ Source of major threats

⇒ Includes data leakage, DDoS, botnets

⇒ Protections :

* Network Scans (Nmap) - to know about systems and devices that are connected to our network

* Network segmentation - to identify your critical information assets.

* Blocking ports -