* Day 1 :->

No. 01
Date 31 · 08 · 25

• What is Cyber Security?

⇒ The body of techologies, Processes, Pratices and designed to protect networks, compoters, Programs and data from attack damage or unauthorized access or misuse of authorized assets.

⊙ Goals of Cyber Security :-

⊙ Reduce the risk of Cyber-attacks.

⊙ Protect organizations and individuals from intentional and unintentional exploitation of security weaknesses in systems, network, and technologies.

⊙ Maintain Confidentiality, Integrity & Availability of information.

⊙ Example :- Preventing unauthorized access to a banking system.

⊙ Scope :- Covers everything - computers, Phones, cloud, even IoT devices (i.e., Smart T.V)

⊙ Key Idea :- It's all about protecting data safe.

No.
Date

•) Threat :-

It is any potential danger or risk that can harm a system, network or data.

(Think of it like a storm approaching your digital house).

→ Can be intentional (hackers) or accidental (user mistake).

• Types of Threat :-

•1) Malware :- Nasty software designed to damage or steal data.

Eg:- Viruses spread by clicking bad links; Ransomware locks files (like Wanna cry in 2017).

•2) Ransomware :- Type of malware that encrypts your files and demands payment to unlock them.

•Note:- Never Pay - call experts himself!

•3) Social Engineering :- Tricking people into giving away sensitive info.

→eg:) Fake emails pretending to be your bank asking for password

No. 03
Date

•4) Insider Threats :- Harm caused by someone inside (e.g., employee or contractor).

→ Could be accidental (leaking data) or, intentional (selling secrets).

•5) Phishing :- A social engineering trick using fake emails or texts to steal info.

→ eg, "Click here to win prize" - don't fall for it.

•6) Denial-of-Service (DoS) :- Overloading a system to make it crash or unavailable.

→ e.g., "Flooding a website with traffic to shut it down."

•7) Quick Tip :- Circle "user mistakes" and think of examples (e.g., clicking phishing links) - it's a big source of threats!

•8) Man-in-the-Middle (MiTM) : When an attacker secretly intercepts and possibly alters communication between two parties

→ eg) Hackers listen to your Wi-Fi chat and steal passwords.

No.
Date

·9) SQL Injection :- A attack where malicious code is inserted into website's database query to steal or manipulate data

→eg) Hacker types bad code into a login box to access all user info.

·10) Zero-Day Exploit :- An attack using a flaw in software that's unknown to the vendor

→e.g., Hacker uses new bug in Window before a patch is out.

·11) Botnets :- Networks of infected devices (bots) controlled by an attacker to launch attacks.

eg) Thousands of hijacked computers send spam or DDoS traffic.

→ (Think of it like a Zombie Army).

12) APT (Advanced Persistent Threat) :- A long-term, targeted attack by a skilled group (eg nation-states) to steal data.

E.g., :- Spies infiltrate a company's

No. 05
Date

network over months.

(note :- very sneaky and hard to detect!)

·13) Drive-by Download :- Malware automatically downloaded to your device just by visiting a hacked website.

E.g., → You click a shady ad, and boom - virus installed.

⊙ Vulnerabilities :-

Weaknesses or flaw in systems, networks, software, or human practices that attackers can exploit to cause harm.

·Why it matters? These are the entry points for threats (eg, Malware) and can lead to data breaches or system crashes.

⊙ Characteristics :-

· Can be technical (e.g., software bugs) or human-related (e.g., errors).

· Often hidden until exploited.

⊙ TYPES OF VULNERABILITIES :-

① Software Vulnerabilities :- Bugs or errors in code that attackers can use.

- Examples :- ① Unpatched software (old Windows version with known bugs)

② Buffer Overflow (too much data crashes a program, letting hackers in).

Includes :- ① Unpatched software,
② Buffer Over Flow;

③ Input Validation Errors ; ⇒ Failure to sanitize user input., leads to SQL injection, XSS.

④ Broken Access Control :- Unauthorized users gaining higher privileges.
Example :- IDOR (Insecure Direct Object Reference).

⑤ Insecure APIs :- Poorly secured endpoints.
- eg> No authentication, rate limiting

⑥ Third-Party Components :- Vulnerable libraries or plugins in use.
Eg> Log4j Vulnerabilities.

② Network Vulnerabilities :-
Weaknesses in network setup or protocols that expose data.

- Examples :-
① Unencrypted Wi-Fi (e.g., Public → hotspots hackers can intercept).
② Misconfigured Firewalls (e.g., open ports letting attackers in).

→ Includes :- ① Outdated Protocols :- Using insecure protocols (eg, FTP, Telnet) ⇒ susceptible to interception and manipulation

② Missing Encryption :- Data Transmitted or stored in plain Text.
eg> HTTP instead of HTTPS.

③ Unpatched Software.

③ HUMAN Vulnerabilities :- Mistake, or behaviours by people that create risks.

- Examples :- ▸ Weak password (eg "password123")
▸ Phishing Clicks (eg Opening Fake bank mails).

⇒ Include ⇒ Social engineering.

④ Configuration Vulnerabilities :-
Errors in system or device settings that leave gaps.

Examples :- ① Default settings not changed (eg) Routers admin password as "admin").
② Open ports on a server (eg, unused services exposed).

Include :- ① Misconfigurations :- Default settings, open ports, excessive permissions
eg) S3 bucket publicly accessible.

② Insufficient Loggings :- Attack go on detected due to lack of visibility
→ Critical for incident response.

③ Default Credentials :- System deployed without changing factory credentials
• Example :→ Admin/admin on routers.

⑤ Hardware Vulnerabilities :- Physical or design flaws in devices that can be exploited.
eg) Outdated hardware (eg) Old routers with no security update).
→ USB attacks (eg) Plugging in an infected drive).

→ OWASP TOP 10 (2021) :-

→ OWASP ⇒ Open Worldwide Application Security Project.

→ It publishes the OWASP Top 10 list every 4 years.

→ Focus :- Raise awareness about top web application vulnerabilities.

→ Purpose :- Used by devs, auditors, and cybersecurity professionals to identify, prioritize and mitigate critical web application security risks.

List :- ① Broken Access Control :- Users can act outside intended permissions.
Eg) User changes URL to access another user's data.

② Cryptographic Failures :- Weak or missing encryption of sensitive data.
eg) Passwords stored without hashing.

③ Injection :- Untrusted input interferes with queries or commands.
eg) SQL Injection : ' OR '1'=1 .

4) Insecure Design :- Flawed security logic in application architecture.
example :- No rate limiting on login attempts.

5) Security Misconfiguration :- Improper settings or defaults left unchanged.
example :- Directory listing enabled on server.

6) Vulnerable and Outdated Components :- Using libraries or platforms with known flaws. eg) Unpatched Log4j library.

7) Identification and authentication Failures :- Weak or broken login/authentication mechanisms. eg) No 2FA, predictable session token.

8) Software and Data Integrity Failure :- → Code/data updates without integrity checks. Eg) App Auto updates from unsigned sources.

9) Security Logging and Monitoring Failures :- → Lacks of logs and alerts for suspicious activity. Example :- No alert for repeated login failures.

10) Server-Side Request Forgery (SSRF) :- Server makes requests to unintended destinations. Eg :- Attacker causes server to access internal IPs.

▶ RISK :- Cybersecurity risk is the potential for loss or damage when a threat exploits a vulnerability in a system, asset or process.

(Risk = Threat x Vulnerability x Impact)
If any factor is zero, Risk = 0.

• Key Terms :- ① Impact :- Consequence of successful attack (eg → data breach, downtime).
② Vulnerability :- Weakness that can be exploited.
③ Threat :- Anything that can cause harm.

• Types of Risks :-

① Operational Risk :- Risk from internal process, system, or human errors.

Example :- • Employee misconfiguring a server
→ Power outage disrupting operations.

② Strategic Risk :- Risks from buisness decisions or external changes affecting security.

Examples :- • Adopting new tech without security checks.

•) Competitor cyber attacks targeting your strategy.

③ Compliance Risk :- Risks from failing to meet legal or regulatory requirements.

Examples :- Not following GDPR data protection laws.
•) Missing audit deadlines.

④ Technical Risk :- Risks from hardware, software or network failures.

• Examples :- ① Outdated hardware crashing under load

•) Software bugs exploited by hackers.

5.) External Risk :- Risks from outside the organization, like natural disasters or cyber attacks.

•) Examples :- DDoS attack overwhelming a server.
•) Flood damaging data centers.

▸ Risk Assessment Process :-
A systematic method to identify, analyze, and prioritize risk to system, data and network to guide security decisions.

→ Helps to allocate resource effectively and prevent major incidents.

• Key Steps :-

① Identify Risk :- list Potential threat & vulnerabilities
• Tool → Vulnerability scanner
eg) Finding / spotting weak password policy of a company.

B) Analyze Risks :- Evalute the likelihood and impact of each risk.

→ Assign scores or use qualitative methods. (1-5 for likelihood) & (1-10 for impact).

eg: A DDoS attack is likely (4/5) and has impact (8/10) on a website.

C) Paioritize Risks :→ Rank risks on based analysis to focus on the most caitical ones.

→ Use a risk matrix (high likelihood + impact => top priority).

eg: Paioritizing Zero day exploit over a minor config mismatch.

D) ~~Migit~~ Mitigate Risk :- Develop and implement plans to reduce or eliminate risks.

→ Apply patches, train users, or add firewalls.

eg: Updating software to fix vulnerability

Risk Managment :-

The process of identifying, assessing and reducing risks to protect system data and networks from threats and vulnerabilities.

- Helps to prevent losses & ensure security

- Managment = Assess + Act + Check

Assessment is the analysis phase; Managment is the full phase to analyse, monitor and eliminate.

Risk Managment Steps :-

① Identify Risks,

② Assess Risks,

③ Mitigate Risks;

④ Monitor and Review :→ Continuously track risks and update the plan on new threats emerge.

Monitoring Tools :→ SIEM are used.

CIA-TRIAD :-

The foundational model of information security consisting of three key principles :-
① Confidentiality, ② Integrity, ③ Availability

→ Three pillars holding up cybersecurity.

⊙ Key Principles :-

ⓐ **Confidentiality** :- Ensuring data is accessible only to authorized people.

→ use encryption, strong password and access control.
Eg :→ Your bank PIN is hidden from hackers with encryption.

ⓑ **Integrity** :- Ensuring data remains accurate and unchanged unless authorized.
Use checksums, version control, and secure updates.
eg :→ A file's content stays intact, no sneaky edits by malware.

ⓒ **Availability** :- Ensuring system and data are accessible when needed.
Use backups, redundancy and DDoS protection.
• Eg :- A website stays online during a cyber-attack with load balancers.

∴ (C = Greenlock, I = Read seal, A = Blue door).

∴ A breach in any of individual, will show security failure.

• Extended Security Goals :-

→ Additional objectives beyond the CIA Triad to provide a more comprehensive security framework.
• Adding extra layers to cybersecurity.

→ Addresses modern threats and compliance needs not fully covered by Confidentiality, Integrity and Availability.

• Key Extended Goals :-

⊙ ⓐ **Non-Repudiation** :- Ensuring actions ∴ can be proven to have been done

by specific users, preventing denial.

- Use digital signatures, log and authentication
eg) A signed email proves you sent it, not a hacker

(B) Authentication :- Verifying the identity of users or devices before granting access.

Use passwords, biometrics, or multi-factor authentication (MFA).

Eg) logging into your bank with a password and a code from your phone.

(C) Authorization :- Ensuring users only access resources they're permitted to use.

Implement role-based access control (RBAC) or permissions.

- Eg:) An employee can't access HR files unless authorized.

(D) Accountability :- Tracking and holding individuals accountable for their actions in a system.

Use audit logs and monitoring tools

eg) Logs show who deleted a file, preventing blame-shifting.

:) While CIA focuses on data protection, NAAA ensures process and user security.

) Access Control & System Maintenance Basics :-

) Practices to manage who can access resources and keep system secure and updated.

- Think of it as the gatekeeper and mechanic for your digital world.

→ Prevents unauthorized access and ensure system run smoothly against threats.

) Subsections :-

a) File Permissions :- Rules that determine who can read, write, or execute files on a system.

(How)
→ Set using access control lists (ACLs) or Unix-style permissions (e.g., read=4, write=2, execute=1).

- Example :- Only the HR team (read/write) can access employee salary files, not interns (read-only).

- R=4, W=2, X=1.

(B) User Roles :- Defined levels of access or responsibilities assigned to users based on their job.

How: Implemented via Role-based Access Control (RBAC) or group policies.

- Example :- An admin can delete files, while a guest can only view them.

(C) Patch Managment :- The process of regularly updating software and system to fix vulnerabilities.

How → Use automated tools (eg- WSUS), and schedule updates (eg- monthly).

eg → Applying a Window patch to fix a zero-day exploit.

→ These ensure access is controlled (permissions, roles) and system are secure (patches).

TYPES OF HACKERS :-

- Hackers :- Categories of individuals or groups who use their skills to breach system with varying intentions.

- Understanding their motives helps in defending against them.

- Key Types :-

(A) White Hat Hackers :- Ethical hackers who test system with permission to improve security.
- Protect organization, earn a living.

eg → A security consultant finding vulnerabilities in bank's network.

(B) Black Hat Hackers :- Malicious hackers who break into system for personal gain.

→ motivation → steal data, money.
→ eg) Hackers stealing data of credit card detail from an e-commerce site.

(C) Gray Hat - Hackers :- Hackers who operate in a gray area, hacking without permission but sometimes reporting issues.

→ motivation → Curiosity or seeking reward, not always malicious.

→ eg) Hacker finds a bug and asks for payment to report it.

(D) Script Kiddies :- Amateur hackers using pre-written tools without deep knowledge.
→ motivation :- Fun, fame, or mindless disruption.

→ eg :- A teen using a downloaded script to crash a small website.

(E) Hacktivists :- Hackers who target system to promote a social or political cause.
[motive]
→ Protest or awareness.
→ eg) Group defacing a website to support a movement.

(F) State-Sponsored Hackers :- Hackers backed by governments for espionage or cyber warfare.
→ Motivation → National security.
→ eg) A Team infiltrating another country's infrastructure.

(G) # Insider Threat :- A security risk originating from within the organization by employees, contractors, or partners. Example :- A disgruntled employee leaking sensitive data.

→ It can cause data leaks, financial losses, or system damage.

Red

(A) ~~Green Hat~~ Team :- Offensive team ~~that~~ tests security by simulating attacks.

eg) Phishing test to find weak links.

" Green hats expose vulnerabilities with controlled attacks".

(B) Blue - ~~Hat~~ - Team :- Defensive team that monitors and responds to incidents.

eg) Using SIEM to stop an API.

→ Blue hats protect with real time monitoring.

(H) Green Hackers :- Inexperienced learners, not attackers. Curious to learn hacking

(I) Blue Hackers :- Not defenders. Typically use hacking for revenge, not part of security teams.

(C) Green Team :- Team of new learners or novices training in cybersecurity skills.

eg) Beginners practicing with basic tools

(D) Purple Team :- Hybrid team that combines Red & Blue efforts for collaborative defense.

eg) Red tests, Blue Responds & Purple aligns strategies.

(E) Orange Team :- Managment or oversight team ~~the~~ plans & evaluates security exercises.

eg) Examples :- Overseeing a Red/Blue drill and assessing results.

(F) Yellow Team :- Neutral team that referees exercises & enforces rules

eg) Setting boundaries for a Red/Blue team drill.

• Malwaare :-

→ Malicious softwaare designed to haam, exploit, oa disrupt system, netwaarks oa usea data.

→ Steals data, damage system, gain unauthaaized access oa extaat victim.

→ Understanding malwaare is caitical faa threat identification, paevention and mitigation in Cybea Secuaity.

• Malwaae's Type :-

① Viaus :- Attaches to legitimate paagaams, spaead when executed.
→ Caaupts files, slaws system.
•Eg) Macaa viauses in MS-OFFice doc.

② Waam :- Self-aeplicating, spaeads independently via netwaaks.
→ Consumes bandwidth, caeates backdaas.
•Eg) Wanna Cay Waam (2017).

③ Tiajan :- ~~Self-aeplicating, spaeads~~
→ Disguises aa legitimate softwaae to taick usaas.
→ Caeates backdaas, steals data.
•Eg) Emotet banking Tiajan.

④ Ransomwaae :- Encaypts data, demands aansom faa decayption.
→ Data loss, financial extaation
•Eg) Locky, Ryuk.

⑤ Spywaae :- Secaetly monitaas usea activity, collects data.
→ Paivacy violation, caedential theft.
•Eg) Pegasus Spywaae.

⑥ Adwaae :- Displays unwanted ads, aften bundled with faee softwaae.
→ Slaws system, tiacks usea behaviaa
•Eg) Baowsea toolbaa adwaae.

⑦ Rootkit :- Hides malicious paacesses, paavides paasistent access.
Conceals otaea malwaae, haad to detect.
•Eg) NTRootkit.

⑧ Botnet :- (Impact ⇒ Used faa Spam & Cayptomining).
Eg) Miaai Botnet.

ATTACK VECTORS :-

→ Path or method used by an attacker to gain unauthorized access to a system, network or data.

Types :- ① Phishing
② Malware, ③ Drive-by-download
④ SQL injection, ⑤ Man-in-the-middle.
⑥ Insider threats ⑦ Exploited Vulnerabilities (unpatched software).

② Brute Force :-
→ Repeatedly guessing credentials until access is gained.
Eg) Using automated tools to crack weak password.

⑨ Cross-Site Scripting (XSS) :-
→ Injecting malicious scripts into websites viewed by other users
Example) Script in a comment section steals session cookies.

Purpose :- ① Delivery of Payload

② Exploitation :- Gain access by leveraging weakness (SQL injection to by Pass authentication

Lateral movement :- Spread within a network (eg → Malware exploiting unpatched system).

Data Exfiltration :- Steal sensitive information (eg → MitM capturing credentials).

Relation to Threat :-

Attack Vectors :→ Method used to deliver attacks.

Threats : Actors (hacker) or events (malware infection) that exploit vectors

Example :-
Vector : Phishing email
Threat : Black hat hacker sending ransomware

Key Point :- Vectors enable threats, mitigating vectors reduces threat impact.

Advanced Persistent Threat (APT) :-

① Definition :- A sophisticated, targeted and prolonged cyber attack where an attacker gains unauthorized access to a network and remains undetected for an extended period.

- Key characteristics :-

- Advanced :- Uses complex techniques (eg → Zero day exploits).
- Persistent :- Long-term, stealthy presence to achieve goals.
- Threat :- Highly motivated actors (organized crimes) targeting specific organizations.

- Features :- ① Multistage :- Involves reconnaissance, initial breach, lateral movement & data exfiltration

① Purpose of APTs :-

① Espionage :- Steal sensitive data

② Sabotage :- Disrupt operation

③ Financial Gain :- Extort via ransomware or sell stolen data.

④ Lateral movement :- Expand control within networks for broader attacks.

- API - attack Lifecycle :-

1) Reconnaissance :- Gather info on target (eg) employee details via social media).

2) Initial Access :- Exploit attack vectors (Phishing).

3) Establish Foothold :- Install malware for access

4) Lateral Movement, ⑤ Data Exfiltration :- ↓ Steal sensitive data.

⑥ Maintain Presence :- Use rootkits or legitimate tools to remain undetected

⑦ Achieve Objective :- Espionage, sabotage or financial gain.

Example of APT's :-

① Stuxnet (2010) :- program via USB & Zero Day. Targeted Iran's Nuclear

② APT 28 (Fancy Bear) :- Russian Group using Phishing

③ Solar Winds (2020) :- Supply chain attack via compromised software updates.

- Defense Against APTs :-
- Tools :- ① EDR → Detects suspicious behaviour (Sentinel One).
② SIEM → Monitors logs for anomalies (eg → Splunk)
③ Threat Intelligence :- Tracks APT groups (Fire Eyes)
④ Fire Walls / IDS :- Block malicious traffic (Snort).
⑤ Antivirus :- Scans for known malware (Malwarebytes)

⊙ Kali Linux v/s Windows Architecture -

① Overview :-

Ⓐ Kali Linux :- Linux distro for penetration testing. Open-source, customizable, tool rich (eg) Nmap).

Ⓑ Windows :- Proprietary OS for general use. Common in enterprises. Limited built in security tools.

② Architecture Comparison

Aspect	Kali Linux	Windows
Base	Linux Kernel	NT Kernel
File System	Hierarchical, Btrfs	NTFS, FAT32
User Permission	Root/non-root	Admin/Standard
Security Tools	Pre-installed tools	Basic tools
Customization	Fully	Limited
Updates	manual	Automatic

③ Relevance :-

① Kali Linux :- Offensive

② Windows :- Defensive

No.

Date

- Kali Pros :- Free, Powerful tools, Ided for ethical hacking
- Kali Cons → Linux knowledge needed.
- Window Pros :- Familias, widely used
- Window Cons :- Frequent target, less security : focused by default.

(end)