Cyber security:

Day1: Understanding Cyber Security Basics & Attack Surface

1.what is cybersecurity? And CIA triad?

Cyber security is a practice of protecting data from an unauthorised entity or a unknown person or AI who is trying to authorize the protected data.

CIA Triad: (Cybsec core objective)

- **Confidentiality**

It ensures that data is accessible only to authorized users.

Example: Bank account details visible only to the account holder

WhatsApp messages protected using end-to-end encryption

Passwords stored in encrypted form

- **Integrity**

It ensures that data is accurate and not altered without authorization.

Examples: Bank balance should not change during data transmission

Marks in an exam database should not be modified by attackers

- **Availability**

It ensures that systems and data are accessible when needed.

Examples: Banking apps working during peak hours

Email servers not going down due to attacks

Types of Cyber Attackers

1. Script Kiddies

- Beginners using ready-made tools/scripts
- No deep technical knowledge
- Motivation: fun, curiosity

2. Insiders

- Employees or trusted users
- Have legitimate access
- Very dangerous due to internal knowledge

3. Hacktivists

- Politically or socially motivated
- Target governments or organizations
- Example: Website defacement

4. Cyber Criminals

- Financial motivation
- Phishing, ransomware, fraud
- Organized crime groups

5. Nation-State Attackers

- Government-sponsored
- Highly skilled and funded
- Target critical infrastructure, defense, power grids

4. What is an Attack Surface?

An attack surface is the total number of points where an attacker can try to enter or extract data from a system.

Larger attack surface = higher risk

5. Common Attack Surfaces

1. Web Applications

- Login forms
- APIs
- File uploads
- Admin panels

2. Mobile Applications

- Insecure storage
- Weak authentication
- Hardcoded credentials

3. APIs

- Broken authentication
- Excessive data exposure
- No rate limiting

4. Network

- Open ports
- Weak firewall rules
- Unsecured Wi-Fi

5. Cloud Infrastructure

- Misconfigured S3 buckets
- Weak IAM permissions
- Publicly exposed services

6. OWASP Top 10 (Why It Matters)

OWASP Top 10 lists the most critical security risks in web applications.

Some key vulnerabilities:

- SQL Injection
- Broken Authentication
- Cross-Site Scripting (XSS)
- Security Misconfiguration
- Insecure Deserialization

Why important?

- Industry standard
- Used by companies during security audits
- Frequently asked in interviews

7. Mapping Daily Applications to Attack Surfaces

Example: Banking App

- Login page → Brute force / credential stuffing
- API → Injection attacks
- Database → Data breach
- Network → Man-in-the-middle attack

Example: Email

- Phishing emails
- Malicious attachments
- Account takeover

8. Data Flow (User → Application → Server → Database)

1. User enters data (username/password)

2. Application sends request to server
3. Server processes request
4. Database stores/retrieves data
5. Response sent back to user

9. Where Attacks Can Happen in This Flow

Stage	Possible Attacks
User	Phishing, keylogging
Application	XSS, CSRF
Server	Authentication bypass
Database	SQL Injection
Network	MITM, sniffing

Summery:

Cyber security helps protect the data and their are many types of attacks and attackers from which the data should be protected and every single day many new attacking techniques and defending techniques are found and these can be studied from many knowledge bases like MITRE, OWASP and a lot of CYBERsec communities, so these make strong awareness for how everything happens.