1. Introduction to Cyber Security

Cyber security refers to the practice of protecting systems, networks, applications, and data from cyber attacks. These attacks aim to access, alter, or destroy sensitive information, extort money, or disrupt normal business operations.

---

2. CIA

Confidentiality

Confidentiality ensures that information is accessible only to authorized individuals.

Examples:

- Online banking login credentials
- Personal messages on WhatsApp
- Aadhaar and PAN details

Protection methods:

- Encryption
- Strong passwords
- Authentication and access control

Integrity

Integrity ensures that data remains accurate, complete, and unaltered during storage or transmission.

Examples:

- Bank transaction amounts
- Student examination results

Protection methods:

- Hashing
- Checksums
- Digital signatures

Availability

Availability ensures that systems and data are accessible to users whenever required.

Examples:

- 24/7 availability of banking apps
- Continuous access to email services

Threats to availability:

- DDoS attacks
- Server failures
- Power outages

---

3. Types of Cyber Attackers

1 Script Kiddies

- Beginners using pre-built hacking tools
- Motivated by curiosity or fun

2 Insiders

- Employees or trusted users
- Misuse authorized access

3 Hacktivists

- Attack systems for political or social reasons
- Often perform website defacement or data leaks

4 Cyber Criminals

- Financially motivated attackers
- Conduct phishing, ransomware, and fraud

5 Nation-State Attackers

- Government-sponsored attackers
- Target critical infrastructure and national security

---

4. Attack Surface

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

Common Attack Surfaces

- Web applications
- Mobile applications
- APIs
- Networks (Wi-Fi, routers)
- Cloud infrastructure
- Databases

A larger attack surface increases security risks.

---

5. OWASP Top 10

OWASP Top 10 is a list of the most critical security risks affecting web applications.

Examples of OWASP vulnerabilities:

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

Importance of OWASP Top 10:

- Industry-standard security guideline
- Helps developers build secure applications
- Widely asked in interviews

---

6. Mapping Daily-Use Applications to Attack Surfaces

Email Applications

- Phishing attacks
- Malware attachments
- Weak passwords

WhatsApp

- Account takeover

- Malicious links
- SIM swapping

Banking Applications

- Credential theft
- Man-in-the-middle attacks
- Insecure APIs

---

7. Data Flow in an Application

User → Application → Server → Database

Possible Attack Points

- User level: phishing, social engineering
- Application level: XSS, SQL injection
- Server level: misconfiguration
- Database level: unauthorized access

---

8. Vulnerability, Threat, and Risk

- **Vulnerability:** A weakness in a system
- **Threat:** A potential danger exploiting the vulnerability
- **Risk:** The impact when a threat successfully exploits a vulnerability