CYBER SECURITY INTERNSHIP – TASK 1

Understanding Cyber Security Basics & Attack Surface

1. What is Cyber Security?

Cyber Security refers to the practice of protecting **computer systems, networks, applications, and data** from digital attacks, unauthorized access, damage, or theft.
Its main goal is to ensure that information remains **secure, accurate, and available** only to authorized users.

Cyber security is essential in areas such as:

- Online banking
- Social media platforms
- Cloud storage
- E-commerce applications
- Government and defense systems

2. CIA Triad (Core Principles of Cyber Security)

The **CIA Triad** forms the foundation of cyber security.

a) Confidentiality

Ensures that information is accessible **only to authorized users**.

Examples:

- Password-protected email accounts
- OTP verification for banking apps
- Encryption of WhatsApp messages

Violation Example:
If a hacker accesses your bank account details without permission, confidentiality is broken.

b) Integrity

Ensures that data remains **accurate, complete, and unaltered**.

Examples:

- Transaction records in banking systems
- Exam results stored in college databases

Violation Example:
If a hacker modifies marks or transaction amounts, integrity is compromised.

---

c) Availability

Ensures that systems and data are **available when needed**.

Examples:

- Accessing online banking anytime
- Email services being reachable 24/7

Violation Example:
A **DDoS attack** that crashes a website affects availability.

---

3. Types of Cyber Attackers

1. Script Kiddies

- Beginners with little technical knowledge
- Use pre-written tools and scripts
- Attack systems for fun or curiosity

---

2. Insiders

- Employees or trusted users within an organization
- Have legitimate access
- May leak or misuse data intentionally or accidentally

---

3. Hacktivists

- Motivated by political or social causes
- Target governments or organizations
- Aim to spread messages or disrupt services

---

4. Nation-State Attackers

- Sponsored by governments
- Highly skilled and well-funded
- Target critical infrastructure, defense systems, or other countries

---

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, LAN)
- Cloud infrastructure
- Databases

The **larger the attack surface**, the higher the security risk.

---

5. OWASP Top 10 (Overview)

The **OWASP Top 10** is a list of the most critical security risks in web applications.

Some key vulnerabilities include:

1. Broken Access Control
2. Cryptographic Failures
3. Injection Attacks (SQL Injection)
4. Insecure Design
5. Security Misconfiguration
6. Vulnerable and Outdated Components
7. Identification and Authentication Failures
8. Software and Data Integrity Failures
9. Security Logging and Monitoring Failures
10. Server-Side Request Forgery (SSRF)

These vulnerabilities are dangerous because they can lead to:

- Data breaches
- Financial loss
- System takeover
- Reputation damage

6. Mapping Daily-Used Applications to Attack Surfaces

Application	Possible Attack Surface
Email	Phishing, malware attachments
WhatsApp	Account takeover, malicious links
Banking App	Credential theft, man-in-the-middle attack
Social Media	Fake logins, data scraping

7. Data Flow in an Application

User → Application → Server → Database

Explanation:

1. User enters data (login, message, transaction)
2. Application sends request to server
3. Server processes request
4. Database stores or retrieves data
5. Response is sent back to the user

8. Points Where Attacks Can Occur

- **User Level:** Phishing, fake websites
- **Application Level:** Injection attacks, broken authentication
- **Server Level:** Misconfigurations, malware
- **Database Level:** Data breaches, unauthorized access
- **Network Level:** Packet sniffing, MITM attacks

9. Vulnerability vs Threat vs Risk

Term	Description
Vulnerability	Weakness in a system
Threat	Potential danger that exploits a vulnerability
Risk	Probability of threat causing damage

Example:

- Weak password → Vulnerability
- Hacker → Threat

- Account compromise → Risk

---

10. Importance of OWASP Top 10

- Helps developers build secure applications
- Raises awareness about common vulnerabilities
- Acts as a security standard for web apps
- Reduces chances of cyber attack.

Final Summary

This task helped build a strong understanding of cyber security fundamentals, attacker types, attack surfaces, and real-world vulnerabilities. Knowing how data flows and where attacks occur is essential for protecting modern digital systems.