CYBER SECURITY INTERNSHIP – TASK 1 REPORT

Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security

Cyber Security refers to the practice of protecting computers, networks, applications, and data from unauthorized access, attacks, damage, or theft. In today's digital world, almost all activities such as banking, communication, shopping, education, and healthcare depend on digital systems. Because of this dependency, cyber security plays a critical role in ensuring safe and reliable use of technology.

Cyber security focuses on protecting information from cyber threats such as hacking, malware, phishing, and data breaches. The main goal is to ensure that data remains secure, trustworthy, and accessible only to authorized users.

2. CIA Triad (Confidentiality, Integrity, Availability)

The CIA Triad is the foundation of cyber security. It represents three core principles that must be protected in any secure system.

2.1 Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized individuals. It prevents unauthorized users from viewing or stealing data.

Examples:

- Banking applications protect account details using passwords and encryption.
- WhatsApp messages are end-to-end encrypted so that only the sender and receiver can read them.
- Email services use authentication to ensure only the owner can access emails.

2.2 Integrity

Integrity ensures that data is accurate, complete, and not altered by unauthorized users. It protects data from being modified, deleted, or tampered with.

Examples:

- Transaction amounts in online banking must not change during transfer.
- Exam results stored in databases must remain accurate.
- Hashing is used to verify that files are not modified.

2.3 Availability

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

Examples:

- Banking services should be available 24/7.
- Email servers must remain accessible without downtime.
- Protection against Denial-of-Service (DoS) attacks helps maintain availability.

3. Types of Cyber Attackers

Different types of attackers exist based on their skills, motivation, and objectives.

3.1 Script Kiddies

Script kiddies are beginners who use pre-written tools or scripts without understanding how they work. Their goal is usually fun, curiosity, or gaining attention.

3.2 Insider Attackers

Insiders are employees or trusted individuals who misuse their access to steal data or damage systems. Insider attacks are dangerous because insiders already have authorized access.

3.3 Hacktivists

Hacktivists perform cyber attacks to promote political, social, or ideological causes. They often target government websites or organizations.

3.4 Nation-State Attackers

Nation-state attackers are highly skilled groups sponsored by governments. They target critical infrastructure, defense systems, and other countries for espionage or cyber warfare.

4. Attack Surface

An attack surface refers to all possible entry points where an attacker can try to gain access to a system. A larger attack surface increases the chances of security breaches.

Common Attack Surfaces:

- Web applications (login forms, input fields)
- Mobile applications
- APIs
- Networks (Wi-Fi, routers, firewalls)
- Cloud infrastructure

Reducing the attack surface is an important security strategy.

5. OWASP Top 10

OWASP Top 10 is a widely recognized list of the most critical security risks to web applications. It helps developers and security professionals understand common vulnerabilities.

Some common OWASP risks include:

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

OWASP Top 10 is important because it provides awareness, improves secure coding practices, and helps prevent common cyber attacks.

6. Mapping Daily Applications to Attack Surfaces

Example 1: Email Application

- User enters login credentials
- Data travels through the internet
- Stored on email server and database
- Attack points: phishing, weak passwords, insecure servers

Example 2: WhatsApp

- User sends message via mobile app
- Data travels through encrypted channels
- Stored temporarily on servers
- Attack points: compromised device, malware, fake apps

Example 3: Banking Application

- User logs in and performs transactions
- Data sent to bank servers and databases
- Attack points: fake apps, man-in-the-middle attacks, insecure networks

7. Data Flow and Possible Attack Points

Data Flow:

User → Application → Server → Database

Possible Attack Locations:

- User side: phishing, malware
- Application layer: SQL injection, XSS
- Network layer: packet sniffing, MITM attacks
- Database: unauthorized access, data leakage

8. Conclusion

This task helped in understanding the fundamentals of cyber security, attacker types, attack surfaces, and common vulnerabilities. It provides a strong foundation for advanced cyber security concepts.