Cyber Security Internship – Task 1

Understanding Cyber Security Basics & Attack Surface

---

1. What is Cyber Security?

Cyber Security is the practice of protecting computers, applications, networks, and data from online attacks.
Today, we use the internet for banking, social media, emails, and shopping, which makes security very important.

The main purpose of cyber security is to ensure that information remains **safe, accurate, and accessible**.

---

2. CIA Triad (Core Cyber Security Concept)

Confidentiality

Confidentiality means that **only authorized users should be able to access data**.

Examples:

- Bank account details
- Email passwords
- Personal messages

If someone accesses this data without permission, confidentiality is violated.

Integrity

Integrity ensures that **data is not changed or modified without authorization**.

Examples:

- College exam marks
- Bank transaction amounts

Any unauthorized change in data leads to loss of integrity.

Availability

Availability ensures that **systems and services are available whenever users need them**.

Examples:

- Banking applications working 24/7
- Email services accessible at all times

Server failures or cyber attacks can affect availability.

---

3. Types of Cyber Attackers

Script Kiddies

Script kiddies are beginners who use **pre-built tools** to perform attacks.
They usually have limited technical knowledge.

Insider Attackers

Insiders are people within an organization who **misuse their access privileges**.

Example:
An employee leaking confidential company data.

Hacktivists

Hacktivists attack systems to support **political or social causes**.

Example:
Defacing government websites.

Nation-State Attackers

These attackers are backed by governments and conduct **high-level, well-planned cyber attacks**.

---

4. What is an Attack Surface?

An attack surface includes **all possible entry points** where an attacker can try to access a system.

Common Attack Surfaces:

- Web applications
- Mobile applications
- APIs
- Network connections
- Cloud infrastructure

---

5. Daily Used Applications and Their Attack Surfaces

Email Applications

- Phishing emails
- Weak passwords

Social Media Applications

- Fake links
- Account hijacking

Banking Applications

- Insecure networks
- Weak authentication mechanisms

---

6. OWASP Top 10 Overview

The OWASP Top 10 is a list of the **most common and critical web application security risks**.

Some important vulnerabilities include:

- SQL Injection
- Broken Authentication

- Sensitive Data Exposure
- Security Misconfiguration

The OWASP Top 10 helps developers and security professionals understand and prevent common attacks.

---

7. Data Flow in Applications

In most applications, data flows in the following way:

User → Application → Server → Database

Possible Attack Points:

- User input fields (Injection attacks)
- Network communication (Man-in-the-Middle attacks)
- Server configuration issues
- Database breaches

---

8. Vulnerability, Threat, and Risk

- **Vulnerability:** A weakness in the system
  Example: Weak password
- **Threat:** A potential attacker or harmful event
  Example: Hacker
- **Risk:** The possibility of loss when a threat exploits a vulnerability
  Example: Account compromise due to weak password

---

9. Conclusion

Through this task, I gained a clear understanding of cyber security fundamentals such as the CIA triad, different types of attackers, attack surfaces, OWASP Top 10 vulnerabilities, and how data flows in applications. This task helped me understand how cyber attacks occur and why security awareness is important in real-world systems.
