CYBER SECURITY INTERNSHIP

Task 1: Understanding Cyber Security Basics & Attack Surface

---

1. Introduction

In today's digital era, almost every aspect of human life depends on technology. From online banking and social media to healthcare systems and government services, digital platforms handle massive amounts of sensitive data. Cyber Security is the practice of protecting systems, networks, applications, and data from cyber threats such as unauthorized access, attacks, damage, or data breaches.

This report provides a detailed understanding of cyber security fundamentals with a strong focus on the CIA Triad, types of attackers, attack surfaces, OWASP Top 10 vulnerabilities, and real-world data flow and attack points. The objective of this task is to build a strong foundational knowledge of cyber security concepts and threat awareness.

---

2. What is Cyber Security?

Cyber Security refers to the technologies, processes, and practices designed to protect computers, networks, software, and data from cyber attacks. These attacks often aim to: - Steal sensitive information - Disrupt business operations - Damage systems or infrastructure - Gain unauthorized access

Cyber security ensures that information remains safe and systems function reliably, even in the presence of attackers.

---

3. CIA Triad (Confidentiality, Integrity, Availability)

The CIA Triad is the foundation of cyber security principles. Every security control and policy is designed to protect one or more of these three pillars.

3.1 Confidentiality

Confidentiality ensures that sensitive information is accessed only by authorized users.

Examples: - Online banking passwords - Personal messages on WhatsApp - Medical records

How it is protected: - Encryption - Authentication (passwords, OTPs, biometrics) - Access control

Real-world example: If a hacker gains access to a user's bank account credentials, confidentiality is breached.

3.2 Integrity

Integrity ensures that data remains accurate, complete, and unaltered by unauthorized users.

Examples: - Bank transaction amounts - Exam results - Software source code

How it is protected: - Hashing - Digital signatures - File integrity monitoring

Real-world example: If a hacker modifies a bank transfer amount during transmission, integrity is compromised.

3.3 Availability

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

Examples: - Banking apps - Email services - E-commerce websites

How it is protected: - Redundant systems - Load balancing - Protection against DDoS attacks

Real-world example: If a banking website goes down due to a DDoS attack, availability is affected.

---

4. Types of Cyber Attackers

Understanding attackers helps in designing better defense strategies.

4.1 Script Kiddies

Script kiddies are inexperienced attackers who use ready-made tools and scripts without understanding how they work.

Motivation: Fun, curiosity, or recognition

4.2 Insider Threats

Insiders are employees or trusted individuals who misuse their authorized access.

Motivation: Revenge, financial gain, negligence

4.3 Hacktivists

Hacktivists attack systems to promote political or social causes.

Examples: Website defacement, data leaks

4.4 Organized Cyber Criminals

These attackers operate in groups and focus on financial gain.

Examples: Ransomware gangs, phishing campaigns

4.5 Nation-State Actors

Highly skilled attackers sponsored by governments.

Targets: Critical infrastructure, defense systems, financial institutions

---

5. Attack Surface

5.1 What is an Attack Surface?

An attack surface is the total number of entry points where an attacker can try to exploit a system.

Larger attack surface = higher risk

5.2 Common Attack Surfaces

- **Web Applications** (login pages, forms)
- **Mobile Applications**
- **APIs**
- **Networks** (open ports, insecure Wi-Fi)
- **Cloud Infrastructure**
- **Operating Systems**

---

6. OWASP Top 10 Overview

The OWASP Top 10 is a globally recognized list of the most critical web application security risks.

Key OWASP Top 10 Risks:

1. Broken Access Control
2. Cryptographic Failures
3. Injection (SQL Injection, Command 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)

Importance: - Helps developers build secure applications - Guides security testing - Reduces real-world breaches

---

7. Mapping Daily-Used Applications to Attack Surfaces

7.1 Email Applications

Attack Surfaces: - Phishing emails - Malicious attachments - Weak passwords

---

7.2 WhatsApp / Messaging Apps

Attack Surfaces: - Account takeover - Malware links - SIM swapping

---

7.3 Banking Applications

Attack Surfaces: - Login pages - APIs - Man-in-the-middle attacks

---

8. Data Flow in an Application

Typical Data Flow:

User → Application → Server → Database → Server → Application → User

---

Example: Online Banking

1. User enters login credentials
2. Application sends data to server
3. Server validates credentials

4. Server fetches data from database
5. Response is sent back to the user

---

9. Attack Points in Data Flow

- During user input (SQL Injection, XSS)
- During data transmission (MITM attacks)
- On server (authentication bypass)
- In database (data breaches)

---

10. Difference Between Vulnerability, Threat, and Risk

- **Vulnerability:** A weakness in a system
- **Threat:** A potential attacker or attack
- **Risk:** The likelihood of a threat exploiting a vulnerability

---

11. Interview Questions – Explained

What is the CIA Triad?

It is a security model focusing on confidentiality, integrity, and availability.

What is an attack surface?

All possible points where an attacker can try to gain access.

Why is OWASP Top 10 important?

It highlights the most critical web application security risks.

---

12. Conclusion

This task provided a strong foundation in cyber security concepts. Understanding the CIA Triad, attackers, attack surfaces, OWASP Top 10, and data flow helps in identifying threats and securing systems effectively. These concepts form the base for advanced cyber security learning and real-world security analysis.

Final Outcome: A clear understanding of cyber security fundamentals and threat awareness, essential for a career in cyber security.