

Task 1: Understanding Cyber Security Basics & Attack Surface

1. What is Cyber Security?

Cyber security is the practice of protecting systems, networks, and data from digital attacks. These attacks aim to steal data, disrupt services, or gain unauthorized access.

The core principles of cyber security are explained using the CIA Triad.

2. CIA Triad

Confidentiality

Ensures that sensitive data is accessible only to authorized users.

Examples:

- Online banking passwords
- WhatsApp private chats
- Company confidential documents

How it is achieved:

- Encryption
 - Authentication
 - Access control
-

Integrity

Ensures that data is accurate and not altered without authorization.

Examples:

- Bank transaction amounts
- Exam results stored in databases
- Medical records

How it is achieved:

- Hashing

- Digital signatures
 - File permissions
-

Availability

Ensures systems and data are available when required.

Examples:

- Banking apps working 24/7
- Email servers accessible anytime

Threats to availability:

- DDoS attacks
 - Server crashes
 - Power failures
-

3. Types of Cyber Attackers

1. Script Kiddies

- Beginners using ready-made tools
- No deep technical knowledge
- Example: Using downloaded DDoS tools

2. Insider Threats

- Employees or trusted users
- Misuse authorized access
- Example: Employee leaking company data

3. Hacktivists

- Attack for political or social causes
- Example: Website defacement to spread messages

4. Nation-State Attackers

- Sponsored by governments
 - Highly skilled and well-funded
 - Example: Cyber espionage, infrastructure attacks
-

4. What is an Attack Surface?

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

Common Attack Surfaces

- Web applications
 - Mobile applications
 - APIs
 - Networks
 - Cloud infrastructure
-

5. OWASP Top 10 (Why It Is Important)

OWASP Top 10 lists the most critical web application security risks.

Why it matters:

- Helps developers build secure apps
- Helps security teams prioritize risks
- Industry standard for web security

Examples of OWASP vulnerabilities:

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

6. Mapping Daily-Used Applications to Attack Surfaces

Application Possible Attack Surface

Email Phishing, malware attachments

WhatsApp Account takeover, OTP theft

Banking App Credential theft, MITM attacks

Social Media Password attacks, fake links

7. Data Flow Example

User → Application → Server → Database

Attack Points in Data Flow

- User side: Phishing, malware
 - Application: Input validation issues
 - Server: Misconfiguration
 - Database: SQL injection, data leakage
-

8. Difference Between Vulnerability, Threat, and Risk

- Vulnerability: Weakness in a system
(Example: Outdated software)
 - Threat: Potential danger that exploits a vulnerability
(Example: Hacker)
 - Risk: Probability of loss when threat exploits vulnerability
(Example: Data breach)
-

9. Interview Questions (Prepared Answers)

What is the CIA triad?

A model that represents Confidentiality, Integrity, and Availability.

What is an attack surface?

All entry points where an attacker can interact with a system.

Who are common cyber attackers?

Script kiddies, insiders, hacktivists, and nation-state actors.

Why is OWASP Top 10 important?

It highlights the most critical web security risks.

10. Final Summary

This task helped me understand core cyber security principles, attacker types, attack surfaces, and real-world threats. It built a strong foundation for identifying risks and protecting systems effectively.