CYBER SECURITY INTERNSHIP – TASK 1
Topic: Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security
Cyber security is the practice of protecting systems, networks, programs, and data from digital attacks. It focuses on preventing unauthorized access, data breaches, cyber threats, and system damage.

In today's digital world, almost everything such as banking, social media, education, and business depends on technology. Therefore, cyber security plays a very important role in protecting sensitive information.

2. CIA Triad
The CIA Triad is the core model of cyber security. It stands for:

a) Confidentiality
Confidentiality means keeping sensitive information private and accessible only to authorized people.
Examples:
- Passwords stored in encrypted format
- Bank account details accessible only to the account holder

b) Integrity
Integrity ensures that data is accurate and not modified by unauthorized users.
Examples:
- A student's marks in a college database should not be altered
- Transaction details in banking systems must remain unchanged

c) Availability
Availability means that data and services should be accessible whenever needed.
Examples:
- Online banking should be available 24/7
- Email services like Gmail should always be accessible

Real-World Example of CIA Triad
In a banking application:
- Confidentiality → Your account details are private
- Integrity → Transaction records cannot be changed
- Availability → You can access your account anytime

3. Types of Cyber Attackers
Different attackers have different motives. Common types are:

1. Script Kiddies
- Beginners who use ready-made hacking tools
- Little technical knowledge
- Mostly attack for fun

2. Insider Attackers
- Employees or trusted people inside an organization
- Can misuse access for personal benefit

3. Hacktivists
- Attack systems for political or social reasons
- Target government or corporate websites

4. Nation-State Attackers
- Highly skilled hackers sponsored by governments
- Aim to steal sensitive national information

4. What is an Attack Surface?
An attack surface is all the possible points where an attacker can try to enter or exploit a system.

Common attack surfaces include:
- Web applications

- Mobile applications
- APIs
- Networks
- Cloud platforms
- Databases

Everyday Examples of Attack Surfaces

Gmail – Login page, attachments	
WhatsApp – Messages, links, media files	
Banking App – Payment gateway, user login	
E-commerce site – Checkout page, user data	

5. OWASP Top 10

What is OWASP?

OWASP (Open Web Application Security Project) is a globally recognized organization that identifies the most critical security risks to web applications.

Why OWASP Top 10 is Important?

- Helps developers understand common vulnerabilities
- Guides organizations to secure applications
- Reduces cyber attacks

Common OWASP Vulnerabilities

1. Injection Attacks
2. Broken Authentication
3. Sensitive Data Exposure
4. Security Misconfiguration
5. Cross-Site Scripting (XSS)

6. Data Flow in an Application

Typical data flow:
User → Application → Server → Database

Where Attacks Can Happen

User Input – SQL Injection
Application – Malware or XSS
Server – Unauthorized access
Database – Data theft or leakage

7. Difference Between Vulnerability, Threat, and Risk

Vulnerability – A weakness in a system
Threat – Anything that can exploit a vulnerability
Risk – Possibility of damage from a threat

Examples:

- Weak password = Vulnerability
- Hacker trying to log in = Threat
- Account getting hacked = Risk

Final Outcome

After completing this task, I have gained:

- Basic knowledge of cyber security
- Understanding of CIA triad
- Awareness of attackers and attack surfaces
- Importance of OWASP Top 10
- How real-world applications can be attacked

This task helped me build a strong foundation in cyber security concepts and threat awareness.

Interview Questions (Answers)

1. What is CIA Triad?

It stands for Confidentiality, Integrity, and Availability – the three core principles of cyber security.

2. What is an attack surface?
All possible entry points where a hacker can attack a system.

3. Difference between vulnerability, threat, and risk?
Vulnerability = weakness
Threat = potential danger
Risk = impact of threat exploiting vulnerability

4. What are common cyber attackers?
Script kiddies, insiders, hacktivists, nation-state attackers.

5. Why is OWASP Top 10 important?
It helps identify and prevent the most common web security risks.

Prepared By:
Deepika Ghanasyam Harikantra
Cyber Security Intern