Task 1

Understanding Cyber Security Basics & Attack Surface

1.What is Cyber Security?

Cyber security is the practice of protecting computers, networks, servers, applications, and data from digital attacks. It focuses on preventing unauthorized access, data theft, system damage, and service disruption. Cyber security helps ensure that information remains safe from hackers, malware, and other cyber threats in today's digital world.

CIA Triad in Cyber Security

The CIA Triad is a fundamental cyber security model that stands for Confidentiality, Integrity, and Availability. These three principles are used to design, implement, and evaluate secure systems**.**

Confidentiality:

Confidentiality ensures that sensitive information is accessible only to authorized users. It protects data from unauthorized access, disclosure, and misuse through security controls like passwords, encryption, and access permissions.

Banking Example:

Only the account holder can view their bank balance and transaction history after logging in with a password or OTP.

Social Media Example:

Only approved friends or the account owner can view private photos and messages on social media platforms.

Integrity:

Integrity ensures that data remains accurate, complete, and unaltered. It protects information from unauthorized modification, deletion, or tampering, whether accidental or malicious**.**

Banking:

Money transferred from one account to another must not be changed during the transaction process.

Social Media :

A user's profile details and posts should not be altered by anyone else without permission.

Availability:

Availability ensures that systems, services, and data are accessible to authorized users whenever needed. It protects against disruptions such as system failures, hardware issues, or denial-of-service attacks.

Banking

Customers should be able to access online banking services at any time to check balances or make payments.

Social

Users should be able to log in, send messages, and view content without unexpected downtime.

Conclusion :

The CIA triad forms the foundation of cyber security and helps organizations protect data from unauthorized access, manipulation, and service disruption

2.Types of Attackers in Cyber Security:

In cyber security, attackers are individuals or groups who try to gain unauthorized access to systems, networks, or data. Their skills, motivations, and targets are different. Some attack for fun, some for money, and some for political or national interests.

Script Kiddies

Script kiddies are beginners who do not have deep technical knowledge. They use ready-made tools and scripts downloaded from the internet to attack websites or systems.

- Motivation: Fun, curiosity, fame
- Method: Pre-built hacking tools
- Example: Using free tools to deface a website or launch a simple DDoS attack.

Insiders

Insiders are people who already have authorized access to an organization, such as employees, contractors, or partners. They may misuse their access intentionally or accidentally.

- Motivation: Revenge, money, carelessness
- Method: Misusing legitimate access
- Example: An employee stealing customer data or deleting important files.

Hacktivists:

Hacktivists are attackers who hack systems to promote political, social, or ideological messages. Their goal is usually to spread awareness, protest, or embarrass organizations.

- Motivation: Ideology, politics, activism
- Method: Website defacement, data leaks, DDoS
- Risk: Can damage reputation and trust
- Example: Defacing a government website to protest a policy.

3.Common Attack Surfaces in Cyber Security

An attack surface refers to all the possible points where an attacker can try to enter a system, steal data, or cause damage. Understanding attack surfaces helps organizations protect weak points and reduce security risks.

- ✓ **Web applications:**
  Web applications are websites and online systems that users access through browsers, such as login pages, online forms, e-commerce sites, and banking portals.

Why it is attacked:
Web applications are exposed to the internet and used by many people. Poor coding, weak authentication, and misconfigurations can allow attackers to steal data, inject malicious code, or take control of accounts.

- ✓ **Mobile Applications**
  Mobile applications are apps installed on smartphones and tablets, such as WhatsApp, banking apps, and shopping apps.

Why it is attacked:
Attackers target mobile apps to steal personal data, exploit insecure storage, inject malware, or create fake apps to trick users. Insecure permissions and outdated apps increase risk.

- ✓ **APIs (Application Programming Interfaces):**

What it is:
APIs act as a bridge between applications and servers, allowing apps to send and receive data, such as login requests, payments, and user information.

Why it is attacked:
If APIs are poorly protected, attackers can bypass apps, directly access servers, steal sensitive data, or perform unauthorized actions.

- ✓ **Networks**

Networks connect computers and servers through the internet or local connections. They transmit data between users, applications, and systems.

Why it is attacked:
Attackers target networks to intercept data, spread malware, perform man-in-the-middle attacks, or disrupt services using denial-of-service attacks.

- ✓ **Cloud Infrastructure**

Cloud infrastructure includes online servers, storage, and services provided by platforms like AWS, Google Cloud, and Microsoft Azure.

Why it is attacked:
Misconfigured cloud services, weak access control, and exposed storage can allow attackers to steal large amounts of data or take control of systems.

Conclusion :

Attack surfaces are the main entry points for cyber attacks, and securing them is critical to protecting modern digital systems.

4.OWASP Top 10 Web Application Vulnerabilities:

Vulnerability	Simple Meaning	Why Dangerous
A01: Broken Access Control	Users can access data or pages they shouldn't	Attackers can view, modify, or delete other users' data, and gain admin privileges
A02: Cryptographic Failures	Sensitive data is not properly encrypted	Passwords, credit card info, and personal data can be stolen
A03: Injection	Malicious code sent through input fields (SQL, commands, etc.)	Attackers can steal, change, or delete database information
A04: Insecure Design	Application design lacks proper security controls	Even well-coded apps can be exploited due to design flaws
A05: Security Misconfiguration	Weak or default security settings	Hackers can find open doors like admin panels, open ports, or default passwords
A06: Vulnerable & Outdated Components	Old libraries and software are used	Known vulnerabilities can be exploited easily
A07: Identification & Authentication Failures	Weak login systems or password handling	Attackers can take over user accounts
A08: Software & Data Integrity Failures	Software updates or data aren't verified	Attackers can insert malware or fake updates
A09: Security Logging & Monitoring Failures	Attacks are not logged or monitored	Breaches go unnoticed and attackers can stay longer
A10: Server-Side Request Forgery (SSRF)	Server is tricked into making malicious requests	Attackers can access internal systems and sensitive data

5.Mapping Daily-Used Applications to Attack Surfaces

This section shows how commonly used applications are connected to different attack surfaces and how attackers may target them.

1. Email (Gmail / Outlook)

- Web application → Phishing pages, cross-site scripting, fake login pages
- Mobile app → Malware-infected apps, insecure storage
- API → Unauthorized access to mail data, token abuse
- Network → Man-in-the-middle attacks, data interception
- Cloud → Data breaches, account takeover

2. WhatsApp

- Mobile app → Fake apps, malware, reverse engineering
- API → Message interception, unauthorized data access
- Network → Man-in-the-middle attacks, packet sniffing
- Cloud → Chat backup leaks, cloud data exposure
- User device → Phishing links, social engineering

3. Banking Application

- Mobile/Web app → Trojans, insecure login pages, fake banking apps
- API → Unauthorized transactions, data manipulation
- Network → Man-in-the-middle, session hijacking
- Cloud/Server → Database breaches, service compromise
- User side → OTP phishing, keyloggers

Conclusion :

Mapping daily-used applications to attack surfaces helps us understand how cyber attacks can target real systems and why multiple layers of security are required.

6.Identifying Where Attacks Can Happen in the Data Flow

Modern applications follow a basic data flow:

User → Application → Network → Server → Database

At each stage, different types of cyber attacks can occur.

1. User Level Attacks

(Where the attack starts)

- Phishing emails and fake websites
- Weak or reused passwords
- Social engineering
- Malicious downloads

Attackers trick users to steal credentials or install malware.

2. Application Level Attacks

- Malware-infected or fake apps
- Reverse engineering of apps
- Insecure storage of sensitive data
- Cross-site scripting or input abuse

Attackers exploit weaknesses in mobile or web applications.

3. Network Level Attacks

- Man-in-the-Middle (MITM)
- Packet sniffing
- Session hijacking
- Denial-of-Service attacks

Attackers intercept or disrupt data traveling over the network.

4. Server Level Attacks

- SQL injection
- Brute force login attempts
- Exploiting unpatched vulnerabilities
    - Remote code execution

Attackers target servers to gain control or access stored data.

5. Database Level Attacks

- Data breaches
- Unauthorized data access
- Data deletion or modification
- Ransomware attacks

Attackers steal, alter, or destroy sensitive information.

Conclusion :

By identifying attack points at each stage of the data flow, organizations can apply security controls to prevent, detect, and respond to cyber threats effectively.

7.Summary:

Cyber security is the practice of protecting computers, networks, applications, and data from unauthorized access, theft, or damage. The CIA Triad — Confidentiality, Integrity, and Availability — ensures that data remains private, accurate, and accessible when needed. Different attackers, such as script kiddies, insiders, hacktivists, and nation-state actors, target systems for various reasons. Attacks can happen at multiple points: the user (phishing, weak passwords), application (malware, insecure apps), network (MITM, sniffing), server (SQL injection, brute force), and database (data breaches). The OWASP Top 10 highlights common vulnerabilities like broken access control, injection, and misconfigurations that attackers exploit. Daily apps like email, WhatsApp, and banking apps are vulnerable if proper security measures are not followed.

Conclusion: This task helped me understand how cyber attacks happen and why protecting systems with strong security practices is essential.