

CYBER SECURITY INTERNSHIP – TASK 1

Understanding Cybersecurity Basics & Attack Surface

INTRODUCTION

Cybersecurity refers to the practice of protecting systems, networks, and data from cyber threats such as hacking, malware, and unauthorized access. With increasing digital usage, cybersecurity has become essential to safeguard personal and organizational information.

1. CIA TRIAD

The CIA triad is the foundation of cybersecurity.

Confidentiality:

Ensures that sensitive information is accessed only by authorized users.

Example:

- Banking apps protect your account using passwords, OTP, and biometrics.
- Social media apps use encryption to secure private chats.

Integrity:

Ensures data remains accurate and unaltered.

Example:

- Online transactions should not change the transferred amount.
- College portals must maintain correct marks.

Availability:

Ensures systems and data are accessible when required.

Example:

- UPI services should work 24/7.
- Social media platforms must stay online without downtime.

2. TYPES OF ATTACKERS

Script Kiddies:

Use ready-made hacking tools without technical knowledge.

Motivation: Fun, fame.

Example: Running DDoS tools on gaming servers.

Insiders:

Employees or contractors misusing internal access.

Motivation: Revenge, money.

Example: Stealing company data.

Hacktivists:

Hack for social or political causes.

Example: Defacing government websites.

Nation-State Actors:

Government-sponsored hackers.

Motivation: Cyber warfare, spying.

Example: Attacking power grids.

3. ATTACK SURFACES

Web Applications:

Login pages, forms, admin panels.

Threats: SQL injection, XSS.

Mobile Applications:

APK reverse engineering, insecure storage.

Threats: Fake apps, malware.

APIs:

Backend endpoints.

Threats: IDOR, broken authentication.

Networks:

WiFi, routers.

Threats: MITM, sniffing.

Cloud Infrastructure:

AWS, Azure.

Threats: Misconfigured storage, leaked keys.

4. OWASP TOP 10

OWASP Top 10 lists the most critical web vulnerabilities:

- Broken access control
- Injection
- Weak authentication
- Security misconfiguration
- Vulnerable components

These vulnerabilities cause:

- Data breaches
- Account takeover
- System compromise

5. DAILY APPLICATION MAPPING

Email:

Attack surfaces: phishing links, fake attachments.

WhatsApp:

Attack surfaces: malicious media, fake apps.

Banking Apps:

Attack surfaces: API abuse, fake apps, screen overlay malware.

6. DATA FLOW

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

Steps:

1. User enters data.
2. App sends encrypted data.
3. Server processes request.
4. Database stores/retrieves data.
5. Response sent back to user.

7. ATTACK POINTS

User:

Phishing, keylogging.

Application:

XSS, reverse engineering.

Network:

MITM attacks.

Server:

SQL injection.

Database:

Data breach.

8. SUMMARY

Cybersecurity is a continuous process of protecting data, understanding attackers, securing attack surfaces, and monitoring data flow. Security must be applied at every layer to prevent breaches.

CONCLUSION

This task helped me build a strong foundation in cybersecurity concepts and real-world threats.