CYBER SECURITY INTERNSHIP

TASK 1: Understanding Cyber Security Basics & Attack Surface

What is cyber security?

Cyber Security is the practice of protecting computers, networks, applications, and data from unauthorized access, using technologies, processes.
Cyber security is essential for protecting personal data, financial information, government systems, and business operations from cyber threats.

CIA Triad

The CIA Triad represents the three core principles of cyber security:

Confidentiality: *-Confidentiality ensure that sensitive information is accessible only to authorized Users.*

Real-world Examples:

- *Passwords and OTPs used in banking applications.*
- *Doctors keeping patient diagnoses secret.*
- *Government protecting classified national security document.*

Integrity: *-Ensures data is accurate, consistent, and trustworthy unaltered unless modified by authorized users.*

Real-world Examples:

- *Software updates verified using checksums.*
- *Alert on unauthorized file changes.*
- *Prevents lower-integrity data from corrupting higher-integrity data.*

Availability: -*Availability ensures that systems, applications, and data are accessible to authorized users whenever needed.*

Real-world Examples:

- *Online banking service available 24/7.*
- *Hospitals systems accessible during emergencies.*
- *Cloud services like Google Drive available without downtime.*

Types of Cyber Attackers

Cyber attackers are individuals or groups that attempt to gain unauthorized access to systems, networks, and data. Based on research from credible cybersecurity sources and security blogs.

1. *Script kiddies: Script kiddies are beginners with limited technical knowledge who use ready-made hacking tools or scripts created by others to carry out attacks.*
2. *Insiders: Insiders are individuals within an organization who misuse their authorized access to harm systems or steal data.*
3. *Hacktivists: Hacktivists conduct cyber-attack to promote political, social, or ideological causes rather than financial gain.*
4. *Nation-State Actors: Nation-State Actors are highly skilled cyber attackers sponsored by governments to conduct cyber espionage or cyber warfare.*

Security Blogs: -

- *Krebs on security*
- *OWASP Blog*
- *Cisco Talos Intelligence*
- *Palo Alto Networks Unit 42*
- *SANS Internet Strom Centre*

Common Attack Surfaces

An **attack surface** refers to all the possible points where an attacker can attempt to gain unauthorized access to a system.

1) *Web Applications: - Web applications are one of the most targeted attack surfaces because they are publicly accessible over the internet.*
2) *Mobile Applications: - Mobile apps stores and transmit sensitive user data, making them attractive targets for attackers.*
3) *APIs (Applications Programming Interfaces):- APIs enable communication between applications but can expose sensitive data if not properly secured.*
4) *Networks: - Networks connect systems and devices, making them critical attack surfaces.*
5) *Cloud Infrastructure: - Cloud platforms host applications, servers, and databases. Misconfigurations can lead to serious breaches.*

OWASP TOP 10 Vulnerabilities

1. ***Broken Access Control: -*** *Attackers can bypass authorization and perform actions or view data they shouldn't have access to.*

- ***Why its dangerous:*** *Enables unauthorized access to data, account takeover, privilege escalation with in applications.*

2. ***Security Misconfiguration: -*** *Apps or environment configure incorrectly such as default settings, exposed service, missing patches, improper cloud configuration.*

    - ***Why it's dangerous****: Misconfigurations are widespread and easy for attackers to exploit, often exposing sensitive endpoints or allowing privilege bypass.*

3. ***Software Supply Chain Failures****: - Vulnerabilities or compromises in external components, dependencies, CI/CD pipelines, and build/distribution systems.*

    - ***Why it's dangerous:*** *Attackers can infiltrate the software development lifecycle or dependencies and inject malicious code that affects every app using that component.*

4. ***Cryptographic Failures****: - Weak, improper, missing, or outdated cryptography for protecting data at rest or in transit.*

    - ***Why it's dangerous****: Exposes sensitive information like credentials and personal data to interception, tampering, or decryption by attackers.*

5. ***Injection****: - Flaws where untrusted input is interpreted as commands by interpreters (e.g., SQL, OS, LDAP).*

    - ***Why it's dangerous:*** *Can lead to data theft, data modification, command execution, and system compromise. Common types include SQL Injection, Command Injection, and others.*

6. ***Insecure Design: -*** *Inherent application design weaknesses — security not integrated into architecture or threat modelling.*

    - ***Why it's dangerous:*** *Even correct code can be fundamentally insecure, enabling logic abuse, privilege escalation, and bypass of protections.*

7. ***Authentication Failure: -*** *Weaknesses in authentication mechanisms — login, session management, token handling.*

    - ***Why it's dangerous:*** *Attackers can bypass authentication, hijack sessions, or impersonate other users, leading to account compromise.*

8. ***Software or Data Integrity Failure: -*** *Failures to ensure that software or data hasn't been tampered with or altered in unauthorized ways.*

    - ***Why it's dangerous:*** *Attackers can insert or modify code or data without detection, undermining trust in the application.*

9. ***Logging & Alerting Failure****: - Insufficient logging, monitoring, and alerting of security-relevant events.*

    - ***Why it's dangerous****: Incidents go unnoticed, preventing timely detection and response — attackers remain inside systems longer and do more damage.*

10. ***Mishandling of Exceptional Conditions: -*** *New category in 2025 focusing on poor error handling, logic flaws, and "fail-open" scenarios.*

    - ***Why it's dangerous:*** *Systems that don't handle errors or abnormal conditions securely can crash, leak information, open backdoors, or bypass security checks.*

Mapping Daily-Used Applications to Possible Attack Surfaces

1. **Email Applications (Gmail, Outlook, Yahoo):**
   Possible Attack Surfaces:
    - Phishing emails stealing credentials
    - Malicious attachments (malware, ransomware)
    - Account takeover via weak passwords
    - Man-in-the-Middle (if unsecured network)
2. **WhatsApp / Messaging Apps:**
   Possible Attack Surfaces:
    - Malicious links and scam messages
    - Spyware via infected media files
    - Account hijacking using OTP phishing
    - Data leakage from insecure backups
3. **Banking & Payment Apps (GPay, PhonePe, Paytm, Bank Apps):**
   Possible Attack Surfaces:
    - Phishing apps pretending to be bank apps
    - Man-in-the-Middle attacks on public Wi-Fi
    - Screen overlay attacks stealing PINs
    - Malware capturing OTPs
4. **Social Media Apps (Instagram, Facebook, X):**
   Possible Attack Surface
    - Account takeover
    - Fake profiles and impersonation

- Malicious links in DMs
- Data scraping and privacy abuse.

5. Web Browsers (Chrome, Firefox, Edge):

Possible Attack Surfaces:

- Malicious extensions
- Drive-by downloads
- Session hijacking
- Credential theft

Data flow & Vulnerability Mapping

To secure a system, we must understand how data moves from the user to the database and identify where it can be attacked.

The Flow Path*: User Device → Web Application → Web Server → Database*

User Device*: Compromised by malware or keyloggers*.

Application*: Exploited via Cross-Site Scripting (XSS)*.

Transit*: Data intercepted via Man-in-the-Middle (MitM) attacks*.

Database*: Data stolen via SQL Injection*.

The Attack Map: From User to Database

1. **The User Level (The Entry Point)**

Attacks here target the person or their hardware before data even enters the network.

- Phishing: Tricking the user into providing credentials on a fake login page.
- Keyloggers/Malware: Malicious software on the user's phone or laptop that records every keystroke.
- Social Engineering: Manipulating the user into revealing sensitive information via phone or chat.

2**. The Application Level (The Interface)**

Attacks here exploit flaws in how the web or mobile app was built.

- Cross-Site Scripting (XSS): Injecting malicious scripts into the web page to steal user session cookies.
- Broken Access Control: Exploiting a bug that lets a regular user access an "Admin" panel they shouldn't see.

- Session Hijacking: Stealing a user's active "token" to take over their account without a password.

3. **The Network/Transit Level (The Journey)**

Attacks here happen while the data is traveling through the air (Wi-Fi) or through internet cables.

- Man-in-the-Middle (MitM): An attacker sits between the user and the server (often on public Wi-Fi) to "sniff" or read the data being sent.
- Packet Sniffing: Using tools to capture unencrypted data packets.

4**. The Server Level (The Logic)**

Attacks here target the computer that hosts the website or application.

- DoS/DDoS: Overwhelming the server with so much fake traffic that it crashes and becomes "unavailable."
- Remote Code Execution (RCE): A critical flaw that allows an attacker to run their own commands directly on the server.

5**. The Database Level (The Prize)**

This is usually the ultimate goal for attackers, as it contains the "crown jewels" (passwords, credit cards, personal info).

- SQL Injection (SQLi): This is the most famous attack. The attacker inserts malicious SQL code into an input field (like a search bar) to trick the database into dumping all its records.

Summary of Understanding

Cybersecurity is the practice of defending the CIA triad: Confidentiality (keeping data private), Integrity (keeping data accurate), and Availability (keeping systems accessible). These three pillars are constantly under threat from diverse attackers, ranging from low-skilled script kiddies and vengeful insiders to highly sophisticated nation-state actors and motivated hacktivists.
The attack surface represents every potential entry point these attackers can exploit, including network vulnerabilities, software flaws (like those listed in the OWASP Top 10), and human errors. By mapping the data flow from the user’s device through the application and server to the database, we can identify specific high-risk zones where attacks like SQL injection or Man-in-the-Middle (MitM) interceptions are likely to occur.