Understanding Cyber Security Basics & Attack Surface

Cyber security is the practice of protecting computer systems, networks, applications, and data from unauthorized access, cyber attacks, and data breaches. It helps ensure that personal, financial, and organizational information remains safe from hackers and other threats.

CIA Triad

The foundation of cyber security is the **CIA Triad**, which includes Confidentiality, Integrity, and Availability.

- **Confidentiality** ensures that sensitive information is accessed only by authorized users. For example, online banking passwords and private social media messages must remain secret.
- **Integrity** ensures that data remains accurate and is not altered without permission. For example, bank balances or academic records should not be modified illegally.
- **Availability** ensures that systems and services are accessible whenever needed. For example, banking apps and email services should be available at all times.

Types of Attackers

Different types of attackers target systems for various reasons:

- **Script Kiddies:** Beginners who use pre-made hacking tools.
- **Insiders:** Employees or trusted users who misuse their access.
- **Hacktivists:** Attack systems to promote political or social causes.
- **Nation-State Actors:** Government-backed attackers targeting critical infrastructure.

Attack Surface

An attack surface refers to all the possible entry points where an attacker can try to access a system or steal data. A larger attack surface increases security risk.

Common Attack Surfaces

Common attack surfaces include web applications, mobile applications, APIs, networks (Wi-Fi, routers), and cloud infrastructure. Vulnerabilities in these areas can allow attackers to exploit systems.

OWASP Top 10

The OWASP Top 10 is a list of the most critical web application security risks, such as broken access control, injection attacks, security misconfiguration, and weak authentication. These

vulnerabilities are dangerous because they can lead to data theft or system compromise.

Data Flow and Attack Points

A typical data flow is:

User → Application → Server → Database → Application → User

Attacks can occur at each stage, such as phishing at the user level, vulnerabilities in applications, injection attacks on servers, and unauthorized access to databases.

Summary

Understanding cyber security basics, the CIA Triad, types of attackers, and attack surfaces helps build strong awareness of cyber threats. This knowledge is essential for protecting modern digital applications and systems.

Prepared by: MOHAMMED JAVEETH .M