CYBERSECURITY INTERNSHIP – TASK 1 REPORT

1. Introduction to Cyber Security

Cyber security is the practice of protecting systems, networks, applications, and data from unauthorized access, misuse, attacks, or damage. With the increasing dependence on digital platforms such as banking systems, social media applications, cloud services, and mobile apps, cyber security has become a critical requirement for individuals and organizations.

Cyber security focuses on prevention, detection, response, and recovery from cyber threats. The foundation of cyber security is built on three core principles known as the CIA Triad.

2. CIA Triad – Core Security Principles

The CIA Triad represents the three fundamental goals of cyber security: Confidentiality, Integrity, and Availability. Every secure system must maintain all three to ensure effective protection.

2.1 Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized individuals and protected from unauthorized disclosure.

Confidentiality is achieved using authentication, authorization, encryption, and secure network controls.

Example: In banking applications, only the account holder can view balances and transaction history.

If confidentiality is compromised, it may result in identity theft, financial fraud, and loss of trust.

2.2 Integrity

Integrity ensures that data remains accurate, complete, and unaltered unless modified by authorized users.

Integrity is maintained using hashing, digital signatures, access controls, and audit logs.

Example: Online transaction amounts should not change during processing.

Violation of integrity can lead to incorrect decisions and financial losses.

2.3 Availability

Availability ensures that systems and data are accessible to authorized users whenever required.

Availability is maintained using backups, redundancy, load balancing, and protection against denial-of-service attacks.

Example: Payment applications must remain available during peak usage hours.

Failure of availability results in service disruption and business loss.

3. Types of Cyber Attackers

Understanding different types of attackers helps in designing appropriate defense mechanisms.

3.1 Script Kiddies

Script kiddies are inexperienced attackers who use ready-made tools and scripts without understanding the underlying technology.

They usually attack systems for curiosity or fun but can still cause serious damage.

3.2 Insider Threats

Insiders are individuals with legitimate system access who misuse it intentionally or accidentally.

They are dangerous because they are trusted and have internal system knowledge.

3.3 Hacktivists

Hacktivists perform cyber attacks to promote political or social causes.

Common activities include website defacement, data leaks, and denial-of-service attacks.

3.4 Nation-State Actors

Nation-state actors are government-sponsored attackers with advanced skills and resources.

They target critical infrastructure such as defense systems, power grids, and financial institutions.

4. OWASP Top 10 Web Application Security Risks

The OWASP Top 10 is a globally recognized list of the most critical web application security risks.

These vulnerabilities are commonly exploited in real-world cyber attacks.

- Broken Access Control – Unauthorized access to resources.
- Cryptographic Failures – Exposure of sensitive data.
- Injection – Execution of malicious commands.
- Insecure Design – Weak application architecture.
- Security Misconfiguration – Unsafe default settings.

- Vulnerable and Outdated Components – Use of insecure libraries.
- Identification and Authentication Failures – Account takeover risks.
- Software and Data Integrity Failures – Supply chain attacks.
- Security Logging and Monitoring Failures – Undetected breaches.
- Server-Side Request Forgery (SSRF) – Internal system access.

5. Mapping Daily Applications to Attack Surfaces

Daily-used applications such as email, messaging apps, banking apps, and shopping platforms have multiple attack surfaces.

Attackers exploit user inputs, insecure networks, and application vulnerabilities.

6. Data Flow in Applications

A typical data flow follows the sequence: User → Application → Server → Database → Response.

Understanding data flow helps identify where attacks can occur.

7. Attack Points in Data Flow

Attacks can occur at multiple stages including phishing at the user level, injection at the application level, unauthorized access at the server level, and data theft at the database level.

8. Conclusion

This report provides a strong foundation in cyber security concepts including the CIA triad, attacker types, attack surfaces, OWASP Top 10 vulnerabilities, and data flow analysis.

Understanding these fundamentals is essential for advanced cyber security learning and practical implementation.