Understanding Cyber Security Basics & Attack Surface

1. Introduction to Cyber Security

Cyber security is the practice of protecting computers, networks, applications, and data from unauthorized access, attacks, damage, or theft. It ensures that digital information remains safe from cyber threats such as hacking, malware, phishing, and data breaches.

In today's digital world, cyber security is essential because we use online banking, social media, email services, and cloud platforms daily. A single security failure can lead to financial loss, data leakage, or service disruption.

2. CIA Triad

The CIA Triad represents the three core principles of cyber security: **Confidentiality, Integrity, and Availability**.

Confidentiality

Confidentiality ensures that information is accessible only to authorized users.

Examples:

- Login passwords for email and banking apps
- OTP verification during transactions
- End-to-end encryption in WhatsApp

If confidentiality is compromised, attackers may steal sensitive data.

Integrity

Integrity ensures that data remains accurate and is not altered without authorization.

Examples:

- Bank account balance should change only after valid transactions
- Exam results stored in databases

If integrity is compromised, attackers can manipulate or modify data.

Availability

Availability ensures that systems and data are accessible when needed.

Examples:

- Banking apps during payments
- Websites during peak usage

If availability is compromised, services may go offline due to DoS or DDoS attacks.

3. Types of Cyber Attackers

Script Kiddies

- Beginners using pre-built tools
- Limited technical knowledge
- Aim for fun or recognition

Insiders

- Employees or trusted users
- Misuse access intentionally or accidentally
- High risk because they already have system access

Hacktivists

- Attack for political or social reasons
- Target organizations or governments
- Often perform website defacement or data leaks

Nation-State Attackers

- Government-sponsored hackers
- Highly skilled and well funded
- Perform cyber espionage and infrastructure attacks

---

4. Attack Surface

An attack surface refers to all possible points where an attacker can attempt to exploit a system.

Common Attack Surfaces

- Web applications
- Mobile applications
- APIs
- Networks (Wi-Fi, routers)
- Cloud infrastructure
- Databases

The larger the attack surface, the higher the risk.

---

5. OWASP Top 10

OWASP Top 10 is a list of the most critical web application security vulnerabilities.

Some common vulnerabilities include:

- SQL Injection
- Broken Authentication
- Security Misconfiguration
- Cross-Site Scripting (XSS)

Importance of OWASP Top 10

- Industry standard
- Helps developers build secure applications
- Helps security professionals identify vulnerabilities

---

6. Mapping Daily-Used Applications to Attack Surfaces

Application	Possible Attack Surface
Email	Phishing, credential theft
WhatsApp	Malicious links, account takeover
Banking Apps	Insecure APIs, weak authentication
Social Media	XSS, data leakage

---

7. Application Data Flow

User → Application → Server → Database

Possible Attack Points

- User level: phishing, malware
- Application level: XSS, SQL injection
- Server level: misconfiguration, RCE
- Database level: data breaches

8. Vulnerability vs Threat vs Risk

- **Vulnerability:** Weakness in a system (e.g., outdated software)
- **Threat:** Potential danger exploiting the vulnerability
- **Risk:** Probability and impact of the threat occurring

---

9. Summary

Cyber security focuses on protecting digital systems using the CIA triad. Different attackers exploit various attack surfaces such as web apps, APIs, and networks. Understanding OWASP Top 10 and application data flow helps identify and prevent real-world cyber attacks.

Final Outcome

This task helped build a strong foundation in cyber security fundamentals, attacker awareness, and attack surface understanding.