Elevate Labs Cyber Security Internship – Task 1

Cyber Security Fundamentals: CIA Triad, Attack Types, and Attack Surfaces

1. CIA Triad with Real-World Examples -

The CIA Triad defines the three core objectives of cyber security. Every security control implemented in real-world systems is designed to protect one or more of these principles.

• **Confidentiality**: Ensures information is accessible only to authorized users.

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Examples:

• Banking applications encrypt customer credentials and transaction data.

• WhatsApp uses end-to-end encryption so only sender and receiver can read messages.

• Corporate systems enforce role-based access control to prevent employees from viewing sensitive data.

• **Integrity**: Ensures data is accurate and cannot be modified without authorization.

Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

Examples:

• Banking systems use transaction logs to prevent unauthorized balance changes.

• Software updates are digitally signed to prevent tampering.

• Databases use hashing and checksums to detect data modification.

• **Availability**: Ensures systems and data remain accessible when required.

Ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.

Examples:

• E-commerce platforms use load balancers to handle high traffic during sales.

• Cloud providers replicate data across multiple data centres.

• Organizations deploy DDoS protection to prevent service outages.

2. Types of Attackers –

Attackers differ in motivation, skill level, and resources. Understanding attacker types helps organizations design appropriate defences.

• **Script Kiddies**: Inexperienced attackers using ready-made tools without deep technical knowledge.

• **Cyber Criminals**: Financially motivated attackers conducting fraud, ransomware, and identity theft.

• **Insiders:** Employees or contractors abusing legitimate access, intentionally or accidentally.

• **Hacktivists:** Ideologically motivated attackers targeting governments or corporations.

• **Organized Crime Groups**: Well-funded groups running large-scale phishing, ransomware, and carding operations.

• **Nation-State Actors**: Government-backed attackers conducting espionage or cyber warfare.
• **Competitors:** Organizations attempting corporate espionage or IP theft.

3. Attack Surfaces –

An attack surface represents all possible points where an attacker can attempt to gain unauthorized access or extract data from a system. Some of them are:

• **Web Applications**: Login forms, input fields, file uploads, and session management.

• **Mobile Applications**: Insecure local storage, hardcoded secrets, and exposed APIs.

• **APIs**: Weak authentication, excessive permissions, and lack of rate limiting.

• **Networks**: Open ports, unencrypted traffic, and misconfigured firewalls.

• **Cloud Infrastructure**: Public storage buckets, overly permissive IAM roles.

• **Operating Systems**: Unpatched services, weak configurations, privilege escalation flaws.

• **Email Systems**: Phishing links, malicious attachments, spoofed senders.

• **Third-Party Services**: Supply chain vulnerabilities and insecure integrations.

• **IoT Devices**: Default credentials, outdated firmware, and exposed services.

Conclusion: Cyber security is built around protecting confidentiality, integrity, and availability. Different attacker types exploit various attack surfaces depending on their motivation and capability. A strong understanding of these fundamentals is essential for designing secure systems and defending against real-world cyber threats.

Name: JATINJAYASIMHA V N