Cyber Security

1. Threat Landscape

The **threat landscape** describes the **overall view of cyber risks and attacks** that organizations or individuals face at a given time.

- **Malware:** Viruses, worms, Trojans, ransomware, spyware.
- **Phishing & Social Engineering:** Tricking users into revealing sensitive info.
- **Network Attacks:** DoS/DDoS, Man-in-the-Middle (MITM), packet sniffing.
- **Insider Threats:** Employees or contractors misusing access.
- **Zero-Day Exploits:** Attacks that target unknown vulnerabilities.
- **Physical Threats:** Theft of devices, hardware tampering.
- **Supply Chain Attacks:** Compromising software/hardware from vendors.

2. Five Pillars of Security

(Also known as the **CIAAN Model**)

Pillar	Meaning	Example
Confidentiality	Only authorized users can access data.	Encrypting sensitive files
Integrity	Data is accurate and not altered.	File checksums, digital signatures
Availability	Data/services are accessible when needed.	Redundant servers, backups
Authentication	Verifying the identity of a user/device.	Passwords, biometrics
Non-Repudiation	Proof that an action happened and can't be denied.	Signed emails, transaction logs

3. Security & Hacking Terminology

What is Hacking?

Hacking is the **act of identifying and exploiting weaknesses** in computer systems, networks, or applications to gain unauthorized access, steal data, disrupt operations, or test security.

- **Ethical hacking** is performed legally to improve security.
- **Malicious hacking** is done for theft, damage, or personal gain.

Types of Hackers

- **White Hat:** Ethical hackers who test security legally.
- **Black Hat:** Malicious hackers breaking systems illegally.
- **Gray Hat:** Hackers in the middle — not fully legal, not fully malicious.
- **Script Kiddie:** Amateur hacker using pre-made tools.
- **Hacktivist:** Hacker motivated by political or social causes.

Common Terms

- **Exploit:** A method or code that takes advantage of a vulnerability.
- **Vulnerability:** Weakness in a system that can be exploited.
- **Payload:** The malicious code delivered during an exploit.
- **Backdoor:** Hidden entry point to a system.
- **Botnet:** Network of infected devices under attacker control.
- **Brute Force Attack:** Trying all possible password combinations.

- **Phishing:** Fraudulent attempt to get sensitive info via email, text, etc.
- **MITM (Man-in-the-Middle):** Attacker intercepts communication between two parties.
- **Zero-Day:** Vulnerability exploited before it is known/fixed.

4. Hacking Methodology (Based on the Cyber Kill Chain)

The **Cyber Kill Chain**, developed by Lockheed Martin, describes the stages of a cyberattack from planning to execution. Ethical hackers often follow similar steps during **penetration testing**.

1. Reconnaissance

- **Purpose:** Gather intelligence about the target's systems, networks, and personnel.

2. Weaponization

- **Purpose:** Create or prepare the malicious payload that will be delivered to the target.
- **Examples:**
    - Crafting a malicious document or exploit code.

3. Delivery

- **Purpose:** Send the malicious payload to the target.
- **Methods:**
    - Phishing emails

    - Malicious websites
    - USB drops

4. Exploitation

- **Purpose:** Execute the payload to exploit vulnerabilities and gain access.

5. Installation

- **Purpose:** Install malware or backdoors to maintain long-term access.

6. Command & Control (C2)

- **Purpose:** Establish a communication channel to remotely control the compromised system.

7. Actions on Objectives

- **Purpose:** Execute the attacker’s end goals.
- **Examples:**
    - Data theft
    - Disruption of services
    - Ransomware encryption
    - Espionage

5. Cryptography Fundamentals

Cryptography is the science of **securing information** by transforming it so only intended recipients can understand it.

1. Goals of Cryptography

Goal	Description
Confidentiality	Keep data secret from unauthorized users.
Integrity	Ensure data is not altered during transit.
Authentication	Verify the identity of the parties involved.
Non-repudiation	Prevent denial of sending or receiving data.

2. Basic Term

Term	Description
Plaintext	Original readable message or data.
Ciphertext	Encrypted, unreadable message.
Encryption	Process of converting plaintext to ciphertext.
Decryption	Converting ciphertext back to plaintext.
Key	Secret value used in encryption/decryption.

3. Types of Cryptography

a. Symmetric-Key Cryptography

- Uses the **same key** for encryption and decryption.
- Faster but key distribution is challenging.

b. Asymmetric-Key Cryptography (Public-Key)

- Uses **two keys**: public key (for encryption) and private key (for decryption).
- Solves key distribution problem but slower.

6. HTTPS and TLS Certificates

1. What is HTTPS?

- **HTTPS** stands for **HyperText Transfer Protocol Secure**.
- It is the secure version of **HTTP** used for communication between a web browser and a web server.
- HTTPS ensures that all data sent between the client and server is **encrypted**, protecting it from interception and tampering.

Main benefits of HTTPS:

- **Confidentiality**: Data is encrypted so that attackers cannot read it.
- **Integrity**: Ensures that the data has not been altered during transmission.
- **Authentication**: Confirms that the user is communicating with the intended website.

2. Role of TLS in HTTPS

- HTTPS uses **TLS** (Transport Layer Security) or its predecessor **SSL** (Secure Sockets Layer) to provide encryption.
- TLS works by establishing a **secure handshake** between the client and the server before any data is exchanged.

3. TLS Handshake Process (Simplified)

1. **Client Hello**:
   The browser sends supported encryption algorithms and a random number.
2. **Server Hello**:
   The server chooses an encryption method and sends its **TLS certificate**.
3. **Certificate Verification**:
   The browser checks if the certificate is valid, signed by a trusted authority, and matches the domain.

4. **Key Exchange**:
   A session key is generated (using asymmetric encryption initially).

5. **Secure Communication**:
   Both parties use the session key for **symmetric encryption** during the session.

4. TLS Certificates

A **TLS certificate** (often called an SSL certificate) is a digital file issued by a **Certificate Authority (CA)** that:

- Confirms the ownership of a domain.
- Contains the public key for encryption.
- Includes details like:
  - Domain name
  - Organization name
  - Expiration date