NOTES

1. Cybersecurity Basics

The foundation of information security rests on three core principles, threats are the dangers you face, and attack vectors are the paths they take.

Understand the CIA Triad: Confidentiality, Integrity, Availability

The **CIA Triad** is a foundational security model that guides organizational security policies.

- **Confidentiality:** Ensures that data is kept **secret** and private. Only authorized users can access sensitive information.
    - *Controls:* Encryption, Access Control Lists (ACLs), Multi-Factor Authentication (MFA).
- **Integrity:** Guarantees that data is **accurate** and complete, and hasn't been tampered with or corrupted.
    - *Controls:* Hashing (like SHA-256), Digital Signatures, Version control, Access permissions.
- **Availability:** Confirms that systems and data are **accessible** to authorized users when needed.
    - *Controls:* Redundancy (backups, clustering), Load balancing, Disaster Recovery Plans, Hardware maintenance.

Explore Threat Types

Threats are potential dangers that can exploit vulnerabilities.

- **Phishing:** A social engineering attack where an attacker attempts to trick a user into revealing sensitive information, often through fraudulent emails impersonating a trusted entity.
- **Malware: Mal**icious soft**ware** designed to cause damage, gain unauthorized access, or steal data. Includes viruses, worms, and Trojans.
- **DDoS (Distributed Denial of Service):** An attack that overwhelms a target server or network with a flood of traffic from multiple compromised computer systems, preventing legitimate users from accessing the service.
- **SQL Injection (SQLi):** An injection vulnerability that occurs when an attacker can interfere with the queries an application makes to its database, allowing them to view, modify, or delete data.

- **Brute Force:** A method of trying many passwords or phrases with the hope of eventually guessing correctly, typically using automated tools.
- **Ransomware:** A type of malware that encrypts a victim's files or systems, demanding a **ransom** payment for the decryption key.

Study Attack Vectors

Attack vectors are the paths or methods an attacker uses to gain unauthorized access to a system or network.

- **Social Engineering:** Exploiting human psychology to manipulate people into performing actions or divulging confidential information (e.g., phishing, pretexting).
- **Wireless Attacks:** Targeting vulnerabilities in Wi-Fi networks and protocols (e.g., WEP/WPA cracking, rogue access points, Evil Twin attacks).
- **Insider Threats:** Security risks that originate from within the target organization, often involving current or former employees, contractors, or business associates who have authorized access to data. These can be **malicious** or **accidental**.

---

2. Linux Fundamentals

Essential commands for navigating and managing the Linux operating system, which is key for most cybersecurity tools.

- ### File System Navigation:
    - **cd (Change Directory):** Moves you between directories. E.g., cd /var/www to go to the web root directory.
    - **ls (List):** Lists files and directories in the current directory. Often used with options like -l (long format) and -a (all, including hidden files).
    - **pwd (Print Working Directory):** Displays the full path of your current directory.
- ### File & Directory Permissions:
    - **chmod (Change Mode):** Changes the permissions of a file or directory. Permissions are set for the **User (u)**, **Group (g)**, and **Others (o)**, and are represented numerically (e.g., **7** for read/write/execute, **6** for read/write). E.g., chmod 755 file.txt.

    - **chown (Change Owner):** Changes the owner and/or group of a file or directory. E.g., chown user:group file.txt.

- **Package Management:**
    - **apt (Advanced Package Tool):** The main command for managing software packages on Debian-based systems like Kali Linux. Used to install, remove, and update software. E.g., sudo apt update (to update lists) or sudo apt install nmap.
    - **dpkg (Debian Package):** A lower-level tool to install, remove, and manage .deb package files.
- **Networking Commands:**
    - **ifconfig / ip a (Interface Configuration / IP Address):** Displays network interface information, including the IP address, netmask, and MAC address.
    - **ping:** Tests network connectivity to another host by sending **ICMP** (Internet Control Message Protocol) echo requests.
    - **netstat / ss (Network Statistics / Socket Statistics):** Shows active network connections, routing tables, and interface statistics. Used to identify open ports and active services.
    - **traceroute / tracert:** Displays the route (path) that packets take to reach a network destination.

---

3. Networking Basics

Understanding how networks operate is critical, as all cyberattacks occur over a network.

OSI Model Layers & Functions

The **Open Systems Interconnection (OSI)** Model is a conceptual framework used to understand and standardize network communication by dividing it into seven abstract layers.

The 7 Layers of the OSI Model

1. Physical Layer – The Hardware Highway

This is the literal foundation. It deals with the physical connection between devices—cables, switches, Wi-Fi signals, electrical pulses, and even fiber optics. If your

Ethernet cable is unplugged or your Wi-Fi signal is weak, the problem is here. It's all about transmitting raw bits (0s and 1s) across a medium.

2. Data Link Layer – The Traffic Cop

Once the bits are moving, this layer organizes them into frames and handles error detection and correction. It also manages MAC addresses, which are unique identifiers for network interfaces. Think of it as the layer that ensures your device can talk to the switch or router directly.

3. Network Layer – The GPS of the Internet

This layer is responsible for routing data between devices across different networks. It uses IP addresses to figure out where data should go. Routers operate at this layer, making decisions about the best path for data to travel.

4. Transport Layer – The Delivery Service

Here's where things get reliable. The transport layer ensures that data arrives intact and in the right order. It uses protocols like TCP (which checks every packet) and UDP (which just sends it fast). If you're streaming Netflix, UDP is likely in play. If you're logging into your bank, TCP ensures nothing gets lost.

5. Session Layer – The Conversation Manager

This layer sets up, manages, and tears down sessions between applications. It's like a host at a networking event, making sure conversations start and end properly. It's less visible in day-to-day troubleshooting but important for maintaining persistent connections.

6. Presentation Layer – The Translator

Now we're getting closer to the user. This layer formats and encrypts data so it's readable and secure. It handles things like character encoding (ASCII, Unicode), data compression, and encryption (SSL/TLS). If you're sending a secure email or accessing a website via HTTPS, this layer is working behind the scenes.

7. Application Layer – The User's Gateway

This is the layer you interact with directly—your browser, email client, or messaging app. It's where protocols like HTTP, FTP, and SMTP live. When you type a URL into Chrome or send a message on WhatsApp, the application layer kicks off the entire OSI process.

TCP/IP Protocol Suite

The **TCP/IP** (Transmission Control Protocol/Internet Protocol) model is a four-layer model used in real-world internet communication. It essentially maps to the OSI model.

1. Application Layer – Where Users Interact

This is the topmost layer, where applications like web browsers, email clients, and file transfer tools operate. It includes protocols such as:

- HTTP/HTTPS: For web browsing.
- FTP: For file transfers.
- SMTP/IMAP/POP3: For email.
- DNS: Resolves domain names to IP addresses.

Imagine you type "www.example.com" into your browser. The application layer kicks off the request using HTTP, and DNS translates the domain into an IP address.

2. Transport Layer – Ensuring Reliable Delivery

This layer handles the actual transmission of data between devices. It breaks data into segments and ensures it arrives correctly and in order.

- TCP (Transmission Control Protocol): Reliable, connection-oriented. Think of it like sending a registered parcel with tracking.
- UDP (User Datagram Protocol): Fast, connectionless. Used for streaming and gaming where speed matters more than reliability.

TCP ensures that if you're downloading a file or logging into a secure site, every packet arrives intact. UDP is used when a few lost packets won't ruin the experience—like watching a video.

3. Internet Layer – The Routing Engine

Here, data is packaged into packets and assigned source and destination IP addresses. This layer decides how packets travel across networks.

- IP (Internet Protocol): Handles addressing and routing.
- ICMP (Internet Control Message Protocol): Used for diagnostics like .
- ARP (Address Resolution Protocol): Maps IP addresses to MAC addresses.

If your data needs to travel from Hyderabad to New York, the internet layer figures out the best route—like a GPS for your packets.

4. Network Access Layer – The Physical Connection

This bottom layer deals with how data is physically sent over the network—via cables, Wi-Fi, or fiber optics. It includes:

- Ethernet: Common wired LAN protocol.
- Wi-Fi protocols: For wireless transmission.
- Frame formatting and MAC addressing.

It's like the delivery truck that physically moves your parcel from one location to another. Without this layer, nothing gets off the ground.

DNS & HTTP/HTTPS Deep Dive

- **DNS (Domain Name System):** The **"phonebook of the Internet."** It translates human-readable **Domain Names** (e.g., google.com) into computer-readable **IP Addresses** (e.g., 142.250.72.78).
- **HTTP (Hypertext Transfer Protocol):** The primary protocol for transferring web pages and data over the internet. It is **unencrypted** and uses **Port 80**.
- **HTTPS (HTTP Secure):** The secure version of HTTP. It uses **SSL/TLS encryption** to secure the communication channel between the web browser and server, protecting data from eavesdropping. It uses **Port 443**.

IP Addressing, Subnetting, and NAT

- **IP Addressing:** A **32-bit (IPv4)** or **128-bit (IPv6)** numerical label assigned to a device participating in a computer network. The address is split into a **Network ID** and a **Host ID**.
- **Subnetting:** The process of dividing a large network into smaller, more efficient, and manageable subnetworks (subnets). A **Subnet Mask** (e.g.,

255.255.255.0 or /24) determines which part of the IP address is the Network ID and which is the Host ID.

- **NAT (Network Address Translation):** A method used to remap one IP address space into another by modifying the IP address information in the IP header of packets while they are in transit across a traffic routing device. This is commonly used to allow multiple devices with **private IP addresses** (e.g., 192.168.x.x) to share a single **public IP address** for external internet access.

---

4. Cryptography Basics

Cryptography secures data by making it unintelligible to unauthorized parties.

Symmetric vs Asymmetric Encryption

Feature	Symmetric Encryption (e.g., AES)	Asymmetric Encryption (e.g., RSA, ECC)
Key Type	Single **shared secret key**	Pair of keys: **Public Key** and **Private Key**
Speed	Very **fast**	Relatively **slow**
Usage	Encrypting large amounts of data (data at rest/in transit)	Securely exchanging the symmetric key, Digital Signatures

Hashing (MD5, SHA256)

- **Hashing:** A one-way function that takes an input (data of any size) and produces a fixed-size, unique string of characters called a **hash value** or **digest**.
    - **One-way:** You cannot reverse the hash to get the original data.
    - **Collision-resistant:** It should be computationally infeasible to find two different inputs that produce the same hash.
- **MD5 (Message Digest 5):** Produces a 128-bit hash. It is **cryptographically broken** (collision found) and should only be used for non-security purposes like file checksums.
- **SHA-256 (Secure Hash Algorithm 256):** Part of the SHA-2 family. Produces a **256-bit** hash. It is the current industry standard for digital signatures and data integrity checks (e.g., in Bitcoin).

Digital Certificates & SSL/TLS

- **SSL/TLS (Secure Sockets Layer/Transport Layer Security):** A protocol that provides a secure, encrypted communication channel between a client (like a web browser) and a server. TLS is the modern successor to SSL.
- **Digital Certificate (SSL/TLS Certificate):** A digital file that verifies the identity of a website or server. It contains the server's **Public Key** and is signed by a trusted **Certificate Authority (CA)**, ensuring the website is who it claims to be. This enables the secure **TLS Handshake** which uses asymmetric encryption to establish a shared symmetric key for the rest of the secure session.

Hands-on: Encrypt and Decrypt messages using OpenSSL

OpenSSL is a command-line tool and library for cryptographic functions.

- **Symmetric Encryption/Decryption with a Password:**
  - *Encrypt:* openssl enc -aes-256-cbc -salt -in plaintext.txt -out cipher.enc -k your_secret_password
  - *Decrypt:* openssl enc -d -aes-256-cbc -in cipher.enc -out decrypted.txt -k your_secret_password.

---

5. Tool Familiarization

These are essential tools in a cybersecurity professional's toolkit.

- **Wireshark (packet capture):** A powerful **network protocol analyzer** that captures network traffic in real-time. It allows you to examine the data (packets/frames) at a granular level, helping to understand network communication, troubleshoot issues, and analyze malicious activity.
- **Nmap (network scanning):** A popular **network discovery and security auditing tool**. It's used to scan a target network or host to find open ports, identify running services, and determine the operating system (OS fingerprinting).
- **Burp Suite (web proxy):** The leading software for web application security testing. It works as an **interception proxy**, sitting between your browser and a web application, allowing you to intercept, inspect, modify, and replay HTTP/HTTPS requests and responses.

- **Netcat (network debugging):** Often referred to as the "TCP/IP Swiss Army Knife." It's a versatile utility that reads and writes data across network connections using TCP or UDP. Used for port scanning, banner grabbing, and establishing simple backdoors/reverse shells in a lab environment.