⍰ Cybersecurity & Networking Notes

1. CIA Triad

Confidentiality

Confidentiality ensures that sensitive information is accessible only to authorized users. This prevents unauthorized access to data, protecting personal, corporate, or classified information. Methods to maintain confidentiality include encryption, strong passwords, and access controls.

Integrity

Integrity ensures that data remains accurate, consistent, and trustworthy. It protects against unauthorized modification or deletion of information. Techniques include hashing, digital signatures, and regular audits.

Availability

Availability ensures that information and systems are accessible to authorized users when needed. This involves maintaining uptime, preventing downtime, and ensuring resilience against attacks such as DDoS. Methods include redundancy, backups, and disaster recovery plans.

2. Common Threats

Phishing

Phishing is a cyberattack where attackers trick individuals into revealing sensitive information, such as passwords or credit card numbers, typically via emails, messages, or fake websites.

Malware

Malware is malicious software designed to damage, disrupt, or gain unauthorized access to computer systems. Types include viruses, worms, trojans, spyware, and adware.

DDoS (Distributed Denial of Service)

A DDoS attack overwhelms a system or network with excessive traffic, rendering it unavailable to legitimate users. It often uses botnets to flood the target.

SQL Injection

SQL Injection is an attack where malicious SQL queries are inserted into input fields, allowing attackers to manipulate databases and extract or modify data.

Brute Force

Brute force attacks involve systematically trying all possible combinations to crack passwords or encryption keys.

Ransomware

Ransomware is malware that encrypts a victim's files and demands a ransom for decryption. It can cause severe data loss and financial damage.

3. Attack Vectors

Social Engineering

Social engineering exploits human psychology to gain confidential information. Common techniques include pretexting, baiting, phishing, and tailgating.

Wireless

Wireless attack vectors involve exploiting vulnerabilities in Wi-Fi networks, Bluetooth, or other wireless communication methods to intercept data or gain unauthorized access.

Insider Threats

Insider threats originate from trusted employees or contractors who misuse their access to harm the organization, intentionally or unintentionally.

4. OSI Model & TCP/IP Basics

OSI Model

The OSI model is a conceptual framework that standardizes the functions of a telecommunication or computing system into seven layers: Application, Presentation, Session, Transport, Network, Data Link, and Physical. It helps understand and troubleshoot network interactions.

TCP/IP Model

The TCP/IP model is a simplified framework used in real-world networking. It consists of Application, Transport, Internet, and Network Access layers, mapping closely to OSI layers. TCP/IP governs internet communication using protocols like TCP, UDP, IP, and HTTP/HTTPS.

5. Networking Basics

DNS (Domain Name System)

DNS translates human-readable domain names (like www.example.com) into IP addresses that computers use to identify each other on the network. This system is crucial for web navigation.

HTTP/HTTPS

HTTP (Hypertext Transfer Protocol) is the foundation of web communication. HTTPS is the secure version using encryption (SSL/TLS) to protect data transmitted between the browser and server.

IP Addressing

IP addresses uniquely identify devices on a network. IPv4 uses 32-bit addresses, while IPv6 uses 128-bit addresses to accommodate more devices.

Subnetting

Subnetting divides a larger network into smaller, manageable sub-networks. It improves network performance, security, and efficient IP address utilization.