Notes

- Cybersecurity Basics

- CIA Triad

  1) Confidentiality

     •Meaning: Keeping data private and accessible only to authorized users.

     •Examples: Encryption (AES, SSL/TLS), Access control lists (ACLs), Passwords.

     •Violations: Data leaks, unauthorized access, eavesdropping.

  2) Integrity

     •Meaning: Ensuring data is accurate, unaltered, and trustworthy.

     •Examples: Hashing (SHA-256), Digital signatures, Checksums.

     •Violations: Tampering, unauthorized modification of files, man-in-the-middle attacks.

  3) Availability

     •Meaning: Ensuring systems and data are accessible when needed.

     •Examples: Redundant servers, Load balancing, Disaster recovery plans.

     •Violations: DDoS attacks, server crashes, ransomware locking access.

- Common Cyber Threat Types

  1) Phishing

     •Fake emails, websites, or messages trick users into revealing credentials or sensitive info.

     •Example: A fake banking email asking for login details.

  2) Malware (Malicious Software)

     •Software designed to harm or exploit systems.

     •Types: Viruses, Worms, Trojans, Spyware.

  3) DDoS (Distributed Denial of Service)

     •Overwhelming a server or network with traffic to make it unavailable.

     •Often performed using botnets.

  4) SQL Injection

     •Attacker inserts malicious SQL queries into input fields to access or alter databases.

     •Example: ' OR '1'='1 bypassing login forms.

  5) Brute Force Attack

     •Automated attempts to guess passwords by trying all possible combinations.

- Countermeasures: Strong passwords, account lockouts.

6) Ransomware

- Malware that encrypts files and demands payment (ransom) for decryption.
- Example: WannaCry ransomware attack.

- Attack Vectors

1) Social Engineering

- Manipulating people to reveal confidential information or perform actions.
- Techniques: Pretexting, Baiting, Tailgating, Phishing calls.

2) Wireless Attacks

- Exploiting weaknesses in Wi-Fi or Bluetooth.
- Examples: Evil twin hotspots, Wi-Fi sniffing, WPA cracking.

3) Insider Threats

- Attacks or leaks from employees, contractors, or trusted individuals.
- Can be intentional (malicious insider) or accidental (negligence).

➢ Steps to Set Up Lab

1) Install VirtualBox

2) Set Up Kali Linux

- Download the Kali Linux ISO from kali.org
- Create a new virtual machine in VirtualBox
- Allocate 2–4 GB RAM and 20 GB+ disk space.
- Install Kali Linux and create a user account.

3) Set Up Target Machines

- Metasploitable2: Download and import the pre-built VM from SourceForge
- Default login: msfadmin/msfadmin.

4) Configure Private Lab Network

- In VirtualBox: File → Host Network Manager → Create Host-Only Network.
- Set IP range (e.g., 192.168.0.1/24).
- Attach Host-Only Adapter to all VMs.

5) Test Connectivity

- Start Kali and target VMs.

- Open terminal in Kali and run:

  ifconfig # Check your IP

  ping <target IP>

- Successful replies confirm the lab is ready.

- Linux Fundamentals

1) File and Directory Management

cd – Change directory.

ls – List files and directories.

pwd – Print working directory.

touch – Create an empty file.

mkdir – Create a new directory.

rmdir – Remove an empty directory.

rm – Remove files or directories.

cp – Copy files or directories.

mv – Move or rename files/directories.

cat – View contents of a file.

more/less – View large files page by page.

head – View the first few lines of a file.

tail – View the last few lines of a file (use tail -f to follow logs).

find – Search for files and directories.

locate – Quickly find files by name.

2) User and Permission Management

whoami – Display current user.

id – Show user and group IDs.

groups – List groups a user belongs to.

adduser / useradd – Create a new user.

passwd – Change user password.

usermod – Modify user properties.

groupadd – Create a new group.

sudo – Execute a command with superuser privileges.

3) File Viewing and Editing

chmod – Change file permissions.

chown – Change file owner and group.

nano – Simple text editor.

vi / vim – Advanced text editor.

4) Package Management

apt – Advanced package tool for installing and managing software.

dpkg – Low-level package manager for Debian-based systems.

5) System Monitoring and Management

top / htop – Monitor running processes and resource usage.

ps – List running processes.

kill / killall – Terminate processes.

uptime – Show system running time.

df – Check disk space usage.

du – Show directory and file sizes.

free – Display memory usage.

6) Networking and Connectivity

ifconfig – View or configure network interfaces.

ping – Test network connectivity.

netstat – Display network connections and ports.

traceroute – Show the path packets take to a destination.

ip addr / ip link – Manage IP addresses and network interfaces (modern replacement for ifconfig).

curl – Transfer data from or to a server.

wget – Download files from the web.

ssh – Connect to another system securely.

scp – Securely copy files between systems.

ftp / sftp – File transfer protocols.

7) Archiving and Compression

tar – Archive files (tar -cvf, tar -xvf).

gzip / gunzip – Compress and decompress files.

zip / unzip – Create and extract ZIP archives.

8) System Information and Utilities

uname -a – Display system information.

hostname – Show or set the system hostname.

date – Display or set system date and time.

history – Show command history.

man – Show manual pages for commands.

- Networking Basics

1) OSI Model Layers & Functions

•Physical Layer – Deals with hardware, cables, and data transmission (bits).

•Data Link Layer – Handles MAC addressing, frames, and error detection (Ethernet, switches).

•Network Layer – Responsible for logical addressing and routing (IP, routers).

•Transport Layer – Provides reliable data delivery (TCP, UDP, ports).

•Session Layer – Manages sessions between applications.

•Presentation Layer – Translates, encrypts, and formats data.

•Application Layer – Interface for user applications (HTTP, FTP, DNS).

2) TCP/IP Protocol Suite

•Application Layer – Protocols like HTTP, DNS, SMTP.

•Transport Layer – TCP (reliable), UDP (fast, connectionless).

•Internet Layer – IP addressing, ICMP (ping).

•Network Access Layer – Handles physical data transmission.

3) DNS & HTTP/HTTPS

•DNS (Domain Name System) – Converts domain names to IP addresses.

•HTTP (HyperText Transfer Protocol) – Transfers web data in plain text.

•HTTPS (Secure HTTP) – Encrypted using SSL/TLS for confidentiality and integrity.

•How it works: Browser → DNS query → Server IP resolved → HTTP/HTTPS request sent → Server response.

4) IP Addressing, Subnetting, and NAT

•IP Addressing: IPv4 (32-bit), IPv6 (128-bit).

•Subnetting: Divides networks into smaller sub-networks to optimize IP usage and security.

•NAT (Network Address Translation): Maps private IPs to public IPs for internet access, hides internal network.

5) Networking devices

•Switch vs Router: Switch connects devices in a LAN; Router connects networks.

•Ports: Logical endpoints (e.g., 80 – HTTP, 443 – HTTPS).

•Firewall: Filters traffic based on rules.

- Cryptography Basics

1) Symmetric vs Asymmetric Encryption

- Symmetric Encryption: Same key for encryption and decryption (AES, DES).
- Asymmetric Encryption: Public key encrypts, private key decrypts (RSA, ECC).

2) Hashing (MD5, SHA-256)

- Purpose: Converts data into a fixed-size hash; one-way function.
- MD5: 128-bit, older, less secure.
- SHA-256: 256-bit, more secure and widely used.

3) Digital Certificates & SSL/TLS

- Digital Certificate: Proof of website identity issued by a Certificate Authority (CA).
- SSL/TLS: Protocols for encrypting data between client and server; ensures confidentiality, integrity, authentication.

4) Hands-On: Encrypt and Decrypt Using OpenSSL

- Encrypt a file:

```
openssl enc -aes-256-cbc -salt -in file.txt -out file.enc
```

- Decrypt a file:

```
openssl enc -aes-256-cbc -d -in file.enc -out file.txt
```

- Generate Hash:

```
openssl dgst -sha256 file.txt
```

➢ Tools

1) Wireshark (Packet Capture)

- Purpose: Network protocol analyzer used to capture and inspect packets in real time.

- Key Uses:

  - Analyze network traffic.
  - Troubleshoot connectivity issues.
  - Detect suspicious activity or attacks.
  - Example: Capture HTTP requests, DNS queries, or TCP handshakes.

2) Nmap (Network Scanning)

- Purpose: Network mapping and vulnerability scanning tool.

- Key Uses:

  - Discover devices on a network.
  - Identify open ports and services.
  - Detect OS and version information.
  - Example Command:

nmap -sV 192.168.1.1/24

(Scans the network for active hosts and service versions.)

3) Burp Suite (Web Proxy)

•Purpose: Web application security testing tool.

- Key Uses:

•Intercept and modify HTTP/HTTPS traffic.

•Perform vulnerability scanning on web apps.

•Test for SQL injection, XSS, and other flaws.

•Components: Proxy, Repeater, Intruder, Scanner.

4) Netcat (Network Debugging)

•Purpose: Versatile tool for reading and writing data across network connections.

- Key Uses:

•Create TCP/UDP connections.

•Test open ports.

•File transfers and simple chat servers.

•Example Command:

nc -l -p 1234

(Listens on port 1234 for incoming connections.)