1. Cybersecurity Basics — CIA Triad

Confidentiality

- Goal: ensure info is readable only by authorized parties.
- Controls: encryption (at-rest/in-transit), access control, least privilege.
- Example: encrypting sensitive files with AES or using HTTPS for web traffic.

Integrity

- Goal: ensure data is not altered unauthorizedly.
- Controls: hashing (SHA256), digital signatures, checksums, versioning.
- Example: using SHA256 hashes to verify file downloads.

Availability

- Goal: ensure legitimate users can access systems/data when needed.
- Controls: redundancy, backups, DDoS mitigation, failover.
- Example: load balancers and backups to survive outages.

2. Threat Types

Phishing —websites to steal creds.

- Mitigation: user training, email filtering, MFA.

Malware —spy (virus, worm, trojan).

- Mitigation: AV/EDR, patching, least privilege.

DDoS (Distributed Denial of Service) — overwhelm service with traffic.

- Mitigation: rate-limiting, CDN, traffic filtering.

SQL Injection — attacker injects SQL via input fields to manipulate DB.

- Mitigation: parameterized queries, input validation, WAF.

Brute Force — guessing passwords by trying many possibilities.

- Mitigation: account lockouts, rate limiting, strong passwords, MFA.

Ransomware — encrypts files and demands payment.

- Mitigation: backups, segmentation, patching, endpoint protections.

3. Attack Vectors

Social Engineering — manipulation of humans (phishing, vishing).
Wireless Attacks — rogue AP, WPA handshake cracking (aircrack-ng).
Insider Threats — authorized users misusing access.

4. Lab Environment Setup

1. Install virtualization: **VirtualBox** or **VMware Workstation Player**.

2. Download and install VMs:
    - **Kali Linux** (attacker).
    - **Metasploitable2** , **DVWA**
3. Create **Host-Only** network
4. Configure both VMs to include a Host-Only adapter
5. Boot VMs and verify IPs:
    - Kali: ip addr show
    - Target: ifconfig or ip addr

commands

ip addr show

ping -c 3 <target_ip>

5. Linux Fundamentals

File system & navigation

- ls -lah — list files
- cd /path/to/dir — change dir
- pwd — print working dir

Permissions

- chmod +x file — make executable
- chmod 644 file — rw-r--r--
- chown user:group file

Package management

- sudo apt update
- sudo apt install wireshark nmap netcat

Networking commands

- ip addr show or ifconfig
- ping -c 4 <ip>
- traceroute <host>

6. Networking Basics (concise)

OSI model (high-level) — 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, Application. Know which layer protocols live on (e.g., TCP = Transport, IP = Network, HTTP = Application).

TCP/IP Suite — Application, Transport (TCP/UDP), Internet (IP), Link.

DNS — name → IP mapping. Lookups: dig example.com / nslookup example.com.

IP addressing & subnetting (quick)

- Example CIDR: 192.168.56.0/24 → host range 192.168.56.1-254.
- NAT: translates private IPs to a public IP.

7. Cryptography Basics

Symmetric encryption — same key for encrypt/decrypt (AES). Fast, used for bulk data.
Asymmetric encryption — public/private keys (RSA, ECC). Used for key exchange and signatures.

Hashing — one-way digest (MD5, SHA256). Use for integrity checks (MD5 is insecure for collision-resistance; prefer SHA256).

Digital Certificates & SSL/TLS — certificates bind public keys to identities, signed by CAs. TLS secures HTTPS.

Hands-on OpenSSL examples

```
# Generate RSA private key (2048)

openssl genpkey -algorithm RSA -out private.key -pkeyopt rsa_keygen_bits:2048


# Generate public key

openssl rsa -in private.key -pubout -out public.pem


# Symmetric encryption (AES-256-CBC)

openssl enc -aes-256-cbc -salt -in secret.txt -out secret.txt.enc


# Decrypt

openssl enc -d -aes-256-cbc -in secret.txt.enc -out secret.txt


# SHA256 hash

sha256sum file.txt

# or

openssl dgst -sha256 file.txt
```

8. Tool Familiarization — quick usage & commands

Wireshark

- Purpose: packet capture & analysis.

- Start capture on the host-only adapter (e.g., vboxnet0) or on Kali with tcpdump then open pcap in Wireshark.
- Useful display filters: http, dns, tcp, ip.addr == 192.168.56.101 && ip.addr == 192.168.56.102

Nmap

- sudo nmap -sS -Pn -p- <target_ip> — TCP SYN scan, all ports.
- sudo nmap -sV -p80,443 <target_ip> — service/version.
- Save: -oN nmap_output.txt.

Burp Suite (web proxy)

- Intercept HTTP(S) by configuring browser proxy to 127.0.0.1:8080.
- Use for inspecting/rewriting requests to DVWA.

Netcat (nc)

- nc -lvp 4444 — open listener on port 4444.
- nc <ip> 4444 — connect to a listener. Useful for quick debugging and file transfers.