Cybersecurity & Ethical Hacking - Expanded Notes

Task 1: Foundations of Cybersecurity (Days 1–12)

1. Linux Basics

File System Navigation
- **cd** – change directory (e.g., cd /home/user)
- **ls** – list files/folders (e.g., ls -l)
- **pwd** – print working directory

File & Directory Permissions
- **chmod** – change permissions (e.g., chmod 755 file.sh)
- **chown** – change ownership (e.g., chown user:group file.txt)

Permissions: r = read, w = write, x = execute

Package Management
- apt-get install
- dpkg -i
- apt update && apt upgrade

Networking Commands
- ifconfig – check IP addresses
- ping – test connectivity
- netstat -tulnp – list listening ports
- traceroute – trace packet path

2. Networking Basics

OSI Model Layers & Functions

Layer	Function	Example Protocols
7. Application	User interaction	HTTP, FTP, SMTP
6. Presentation	Data translation/encryption	SSL, TLS
5. Session	Communication management	NetBIOS, PPTP
4. Transport	Reliable delivery	TCP, UDP
3. Network	Routing & addressing	IP, ICMP
2. Data Link	Error detection, frames	Ethernet, PPP
1. Physical	Transmission medium	Cables, Hubs

TCP/IP Protocol Suite
- Application (HTTP, FTP, DNS, SMTP)
- Transport (TCP/UDP)
- Internet (IP, ICMP)
- Network Access (Ethernet, Wi-Fi)

DNS & HTTP/HTTPS
- DNS = Domain to IP mapping
- HTTP = unencrypted web traffic

- HTTPS = encrypted with SSL/TLS

IP Addressing, Subnetting, NAT

- IPv4 = 32-bit (192.168.1.1)
- IPv6 = 128-bit
- Subnetting divides large networks
- NAT maps private IPs to public IPs

3. Cryptography Basics

- **Symmetric Encryption**: Same key for encryption & decryption (AES, DES). Fast but key sharing is risky.
- **Asymmetric Encryption**: Uses public & private keys (RSA, ECC). More secure, used in SSL/TLS.
- **Hashing**: One-way, ensures integrity.

– MD5 (128-bit, weak)
– SHA-256 (secure, widely used)

4. Tools Familiarization

- **Wireshark**: Captures & analyzes packets.
- **Nmap**: Network scanning (ports, services, OS detection).
- **Burp Suite**: Web proxy, used for testing SQLi, XSS, CSRF.
- **Netcat**: Debugging, backdoors (e.g., nc -lvp 4444).
- **Digital Certificates & SSL/TLS**: Authenticate servers, encrypt communication.
- **OpenSSL Hands-on**:

`openssl enc -aes-256-cbc -in file.txt -out file.enc` (encrypt)
`openssl enc -d -aes-256-cbc -in file.enc -out file.txt` (decrypt)