**🔐 Cybersecurity Notes**

1. **Basics of Cybersecurity**

Definition: Protecting systems, networks, and data from digital attacks.

**CIA Triad**:

Confidentiality – Data sirf authorized users ko mile. (Encryption, Passwords)

Integrity – Data alter na ho bina permission ke. (Hashing, Digital Signatures)

Availability – Service hamesha accessible ho. (Backups, Redundancy, DoS protection)

2. **Common Threats**

* Malware → Virus, Worm, Trojan, Ransomware.
* Phishing → Fake emails/links se login details lena.
* SQL Injection → Database me malicious queries inject karna.
* XSS (Cross Site Scripting) → Website ke input box se malicious script chalana.
* MITM (Man-in-the-Middle) → Data sniff karna between 2 users.
* DoS/DDoS → Server overload karke service band karna.

3. **Security Mechanisms**

Authentication: Verify user identity (Password, OTP, Biometrics).

Authorization: Access control (Admin vs User rights).

Encryption: Convert data into unreadable form. (AES, RSA).

Hashing: One-way data conversion (SHA-256, MD5).

Firewall: Block unwanted traffic.

IDS/IPS: Detect aur prevent intrusion.

4. **Password Security**

Strong password: ≥12 chars, mix of upper/lowercase, numbers, symbols.

Avoid dictionary words & reuse.

Use Password Managers (Bitwarden, KeePass).

Enable 2FA (OTP/Authenticator App).

5. **Network Security**

* VPN: Encrypt traffic, hide IP.
* HTTPS: Secure website connection.
* WPA3: Secure Wi-Fi protocol.
* Port Scanning (Nmap) se open ports check karna.

6. **Ethical Hacking Phases**

1. Reconnaissance – Information gathering (OSINT, WHOIS).

2. Scanning – Network scanning, vulnerability check.

3. Exploitation – Exploit vulnerability (SQLi, XSS).

4. Maintaining Access – Backdoors, Trojans.

5. Covering Tracks – Logs clear karna.

7. **Security Best Practices**

Regular updates & patches.

Strong access control policies.

Take backups (3-2-1 rule).

Awareness training (phishing mails detect karna).

Incident Response Plan ready hona chahiye.

8. **Important Tools**

* Nmap – Port scanning.
* Wireshark – Packet sniffing.
* Burp Suite – Web vulnerability testing.
* Metasploit – Exploitation framework.
* John the Ripper / Hashcat – Password cracking.