Term -4 Gt; Ech - Introduction To Ethical Hacking

1.CIA Triad – Confidentiality, Integrity, Availability; the foundation of cybersecurity ensuring data privacy, accuracy, and accessibility.

2.Firewall – A security device/software that filters incoming and outgoing traffic to block malicious activity.

3.VA vs. PT – Vulnerability Assessment (VA) identifies system weaknesses; Penetration Testing (PT) exploits them to measure security strength.

4.HIDS vs. NIDS – HIDS (Host-Based IDS) monitors a single device; NIDS (Network-Based IDS) monitors network traffic.

5.SSL Encryption – Secure Sockets Layer encrypts communication between web browsers and servers to prevent data interception.

6.Data Leakage – Unauthorized exposure of sensitive information due to weak security or insider threats.

7.Brute Force Attack – Guessing passwords by trial & error; prevent with strong passwords, multi-factor authentication (MFA), and account lockouts.

8.MITM Attack (Man-in-the-Middle) – Hacker intercepts communication between two parties; prevent using SSL/TLS, VPNs, and secure Wi-Fi.

9.XSS Attack (Cross-Site Scripting) – Injecting malicious scripts into websites; prevent with input validation and Content Security Policy (CSP).

10.Botnet – A network of infected devices controlled by hackers for DDoS attacks, spam, or data theft.

11.SSL vs. TLS – TLS (Transport Layer Security) is the improved version of SSL with better encryption and security.

12.Virus, Malware, Ransomware – Virus: Self-replicating malicious program; Malware: Any malicious software; Ransomware: Encrypts files, demanding ransom.

13.Phishing – Fraudulent emails or messages trick users into revealing sensitive data (e.g., fake banking emails asking for login details).

14.Encryption & Decryption – Encryption converts plaintext into unreadable format; Decryption converts it back to readable form.

15.DDoS Attack – Overloading a server with excessive traffic to make it unavailable; mitigated using CDN, rate limiting, and firewalls.

16.Zero-Day Vulnerability – A security flaw unknown to the vendor, exploited before a patch is available.

17.Network Sniffing – Capturing network traffic to steal credentials or sensitive data; prevented using encryption and secure connections.

18.SOC (Security Operations Center) – A team monitoring, detecting, and responding to cybersecurity threats 24/7.

19.Cyber Forensics – Investigates cybercrimes by analyzing digital evidence to track attackers and prevent future breaches.

20. Future Trends in Cybersecurity & Essential Skills
Future Trends:
AI & Machine Learning – Automating threat detection and response.

Zero Trust Architecture – "Never trust, always verify" security model.

Cloud Security – Growing need for multi-cloud protection.

Quantum Computing Threats – Potential to break current encryption methods.

IoT & OT Security – Protection for connected devices and industrial systems.
Ransomware Defense – Stronger backup and recovery strategies.

Regulatory Compliance – Stricter data protection laws (GDPR, CCPA, etc.).

Essential Skills for Cybersecurity Professionals:

Networking & System Security – Firewalls, IDS/IPS, VPNs.

Ethical Hacking & Penetration Testing – Offensive security techniques.

Incident Response & Forensics – Investigating and mitigating attacks.

Cloud Security – AWS, Azure, GCP protection strategies.

Cryptography & Secure Coding – Encryption, hashing, secure development.

SIEM & Threat Intelligence – Security event monitoring & analysis.

AI & Automation – Using machine learning for cybersecurity.

21. IDS vs. IPS

IDS (Intrusion Detection System) – Monitors traffic and alerts on suspicious activities.

IPS (Intrusion Prevention System) – Blocks or mitigates detected threats automatically