UNIT 1

1. Introduction to Ethical Hacking

- **Hacking Evolution**: Hacking has shifted from curiosity-driven actions to a professional field focused on improving security.
- **What Is an Ethical Hacker?**: An ethical hacker is someone who tests and secures systems, with permission, by identifying vulnerabilities.
- **Ethical Hacking and Penetration Testing**: Both focus on finding and fixing security flaws. Penetration testing is a more specific, structured approach.
- **Hacking Methodologies**: Steps include gathering information, scanning for vulnerabilities, exploiting weaknesses, maintaining access, and covering tracks.

2. System Fundamentals

- **Computer Networks**: A system that connects devices to share data using protocols like TCP/IP.
- **TCP/IP Ports**: Channels for network communication; examples include 80 (HTTP) and 443 (HTTPS).
- **Network Devices**: Devices like routers, switches, and modems help manage and connect networks.
- **Proxies**: Servers acting as intermediaries between users and the internet, offering privacy and security.
- **Firewalls**: Security systems that filter incoming and outgoing traffic to protect devices.
- **Operating Systems**: Different OS types (Windows, Mac, Android, Linux) have unique security features and vulnerabilities.

3. Cryptography

- **History**: Cryptography has evolved from simple codes to complex algorithms used to secure communication.
- **Symmetric Cryptography**: Same key for encryption and decryption (e.g., AES).
- **Asymmetric Cryptography**: Uses a public key for encryption and a private key for decryption (e.g., RSA).
- **Hashing**: Converts data into a fixed-size string, useful for verifying data integrity (e.g., SHA-256).
- **Cryptography Issues**: Key management and the risk of weak algorithms.
- **Applications**: Cryptography is used in protocols like IPsec (for secure IP communication), PGP (for email encryption), and SSL (for securing internet connections).

Important MCQ

Introduction to Ethical Hacking

1. **What is the primary goal of ethical hacking?**
    - a) To exploit system vulnerabilities
    - **b) To test and secure systems**
    - c) To learn hacking techniques
    - d) To bypass security measures
2. **Which of the following is a key step in ethical hacking?**
    - a) Hiding traces
    - **b) Gaining unauthorized access**
    - c) Scanning for vulnerabilities
    - d) Attacking the system for fun
3. **What does "penetration testing" specifically focus on?**
    - a) Identifying malware
    - **b) Simulating attacks on systems**
    - c) Scanning networks
    - d) Creating firewalls
4. **Which of these is not a phase in common hacking methodologies?**
    - a) Reconnaissance
    - b) Gaining Access
    - **c) Copying data**
    - d) Covering Tracks
5. **Which of the following is a tool commonly used in ethical hacking for scanning vulnerabilities?**
    - a) Photoshop
    - **b) Nmap**
    - c) Excel
    - d) Microsoft Word

System Fundamentals

6. **Which device connects multiple devices within a local network?**
    - a) Router
    - **b) Switch**
    - c) Modem
    - d) Firewall
7. **What does TCP/IP stand for?**
    - **a) Transmission Control Protocol/Internet Protocol**
    - b) Total Control Protocol/Internet Protocol
    - c) Transmission Channel Protocol/Internet Pathway
    - d) None of the above
8. **What is the role of a proxy server?**
    - a) To encrypt network traffic
    - **b) To act as an intermediary between a user and the internet**
    - c) To block all incoming traffic
    - d) To store website data for faster loading
9. **Which of the following is responsible for filtering network traffic?**
    - a) Switch
    - b) Router
    - **c) Firewall**
    - d) Proxy
10. **Which operating system is known for being highly customizable and secure for servers?**
    - a) Windows
    - b) Android
    - **c) Linux**
    - d) MacOS

Cryptography

11. **What is the main difference between symmetric and asymmetric cryptography?**
    - **a) Symmetric uses one key, while asymmetric uses two keys**
    - b) Symmetric is slower than asymmetric
    - c) Asymmetric is only used for hashing
    - d) Symmetric is used for public key encryption
12. **Which of the following is a common symmetric encryption algorithm?**
    - a) RSA
    - **b) AES**
    - c) SHA-256
    - d) Diffie-Hellman
13. **Which cryptographic technique uses a public and a private key?**
    - a) Symmetric cryptography
    - **b) Asymmetric cryptography**
    - c) Hashing
    - d) Data obfuscation
14. **What is the primary use of hashing in cryptography?**
    - a) To secure communication
    - **b) To ensure data integrity**
    - c) To encrypt data
    - d) To manage keys
15. **What is a commonly used hashing algorithm?**
    - a) RSA
    - b) AES
    - **c) SHA-256**
    - d) IPsec
16. **Which of the following is a problem with cryptography?**
    - a) Encryption is always too fast
    - **b) Managing encryption keys can be challenging**
    - c) Hashing is never secure
    - d) Cryptography is not widely used

17. **Which cryptographic protocol is used to secure internet communication?**
    - a) PGP
    - **b) SSL**
    - c) RSA
    - d) AES
18. **PGP (Pretty Good Privacy) is primarily used for:**
    - a) File encryption
    - **b) Email encryption**
    - c) Video encryption
    - d) Server security
19. **Which protocol is used for securing IP communications?**
    - a) SSL
    - **b) IPsec**
    - c) TLS
    - d) SSH
20. **What does IPsec primarily protect?**
    - a) Data during storage
    - **b) Data during transmission over the internet**
    - c) User credentials
    - d) Files in a local machine

General Knowledge of Networking and Security

21. **Which of these is an example of a network device that directs traffic between different networks?**
    - a) Switch
    - **b) Router**
    - c) Modem
    - d) Firewall

22. **Which of the following ports is commonly used for HTTP traffic?**
    - a) 22
    - **b) 80**
    - c) 443
    - d) 21
23. **What does a firewall do in a network?**
    - a) Encrypts data
    - **b) Filters incoming and outgoing traffic**
    - c) Increases network speed
    - d) Connects different networks
24. **Which protocol is primarily used for secure web browsing?**
    - a) HTTP
    - b) FTP
    - **c) HTTPS**
    - d) TCP
25. **Which type of network device connects different networks and determines the best path for data?**
    - a) Switch
    - b) Modem
    - **c) Router**
    - d) Proxy

Ethical Hacking Tools and Techniques

26. **Which of the following tools is used for vulnerability scanning and network mapping?**
    - a) Burp Suite
    - **b) Nmap**
    - c) Kali Linux
    - d) Metasploit

27. **Which is the correct term for a simulated attack to test security?**
    - **a) Penetration test**
    - b) Phishing attack
    - c) Spoofing
    - d) Ransomware attack
28. **Which tool is commonly used for packet analysis in network security?**
    - a) Nmap
    - **b) Wireshark**
    - c) Kali Linux
    - d) Metasploit
29. **Which of the following is a type of denial-of-service (DoS) attack?**
    - a) Phishing
    - b) Man-in-the-middle
    - c) Buffer overflow
    - **d) Ping of death**
30. **What does a "man-in-the-middle" attack involve?**
    - a) Hacking into a database
    - **b) Intercepting and altering communication between two parties**
    - c) Stealing passwords from a server
    - d) Crashing a website