Shift – 1

MCQ Questions:

1. What does the term “white hat” refer to in ethical hacking?

A. A malicious hacker

B. A security expert who conducts ethical hacking

C. A hacker who steals sensitive information

D. A government surveillance expert

Answer: B

2. Which of the following is the first step in the ethical hacking process?

A. Maintaining Access

B. Gaining Access

C. Reconnaissance

D. Scanning

Answer: C

3. What is a vulnerability?

A. A feature that enhances a system's security

B. A flaw or weakness that can be exploited

C. A type of hacking tool

D. A legal framework for ethical hacking

Answer: B

4. What is the main tool used in a dictionary attack?

A. Wordlists

B. Malware

C. Backdoors

D. Keyloggers

Answer: A

5. Which of these is NOT a type of social engineering?

A. Phishing

B. Tailgating

C. Shoulder surfing

D. Port scanning

Answer: D

6. Which hacking technique involves sending fake emails to trick users into revealing sensitive information?

A. Denial of Service (DoS)

B. Social Engineering

C. Phishing

D. Keylogging

Answer: C

7. What does the term "Zero-Day" refer to in cybersecurity?

A. The number of days a system remains operational

B. A vulnerability that is discovered but not yet patched

C. A software release date

D. A full-system backup process

Answer: B

8. What is the purpose of the Nmap tool in ethical hacking?

A. To scan and map networks for vulnerabilities

B. To encrypt data for secure transmission

C. To test password strength

D. To detect malware on a system

Answer: A

9. Which of the following attacks relies on intercepting communication between two parties?

A. Cross-Site Scripting (XSS)

B. Man-in-the-Middle (MITM) Attack

C. SQL Injection

D. Denial of Service (DoS)

Answer: B

10. What is the goal of a denial-of-service (DoS) attack?

A. To gain administrative access to a system

B. To steal sensitive information

C. To overload a system, causing it to crash or become unavailable

D. To plant a Trojan horse

Answer: C

11. What is a honeypot in cybersecurity?

A. A type of encryption tool

B. A decoy system designed to attract attackers

C. A database of malware samples

D. A protocol for secure communication

Answer: B

12. What does the term “penetration testing” refer to?

A. Cracking passwords of users

B. Testing security by attempting to exploit vulnerabilities

C. Physically testing hardware for flaws

D. Installing antivirus software

Answer: B

13. Which Python library is commonly used for network scanning in ethical hacking?

A. NumPy

B. pandas

C. Scapy

D. matplotlib

Answer: C

14. Which Linux command is used to list all active network connections and listening ports?

A. `ls`

B. `netstat`

C. `ping`

D. `pwd`

Answer: B

15. In Bash scripting, what does the following command do?

```bash
echo "Hello World" > file.txt
```

A. Displays "Hello World" on the terminal

B. Deletes the file named "file.txt"

C. Writes "Hello World" into the file "file.txt"

D. Appends "Hello World" to the file "file.txt"

Answer: C

16. Which Python module is used to handle HTTP requests in ethical hacking scripts?

A. `http.client`

B. `requests`

C. `socket`

D. `urllib`

Answer: B

17. In ethical hacking, what does the following Python script perform?

```python
import socket
s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect(("example.com", 80))
```

A. Creates a web server

B. Opens a socket connection to "example.com" on port 80

C. Scans "example.com" for open ports

D. Downloads a file from "example.com"

Answer: B

18. Which of these tools is used to brute-force passwords and is commonly used in ethical hacking?

A. Wireshark

B. Hashcat

C. Nessus

D. OpenVAS

Answer: B

19. What does the following Python code snippet accomplish in ethical hacking?

A. Encrypts the string "password123"

B. Hashes the string "password123" using MD5

C. Decrypts the MD5 hash of "password123"

D. Finds vulnerabilities in passwords

Answer: B

20. Which platform is commonly used for penetration testing and ethical hacking, providing a wide range of pre-installed tools?

A. Windows 10

B. Ubuntu

C. Kali Linux

D. Fedora

Answer: C

21. Scenario: You are an ethical hacker tasked with testing the security of an e-commerce website. During your reconnaissance, you discover that the website is vulnerable to SQL Injection. What should be your next step?

A. Exploit the vulnerability and steal data to prove your point.

B. Report the vulnerability to the website's administrator without exploiting it.

C. Publicly disclose the vulnerability on social media.

D. Ignore the vulnerability as it is not your responsibility.

Answer: B

22. Scenario: A company hires you to perform penetration testing. During the test, you accidentally access sensitive customer data. What is the ethical response?

A. Save the data for later analysis.

B. Report the incident to the company immediately and document your findings.

C. Delete the data and proceed with testing.

D. Ignore it and focus on other vulnerabilities.

Answer: B

23. Scenario: You notice unusual traffic in a company's network, indicating a possible Man-in-the-Middle attack. What should you do first?

A. Shut down the network immediately.

B. Inform the network administrator and help analyze the traffic.

C. Wait to see if the attack causes any damage.

D. Block all external IPs without analysis.

Answer: B

24. Scenario: While scanning a system for vulnerabilities, you find a default password still being used on an administrative account. What should you recommend?

A. Leave it unchanged to avoid disrupting the system.

B. Change the password without informing anyone.

C. Recommend immediate password change and policy enforcement.

D. Use the password to demonstrate system access risks.

Answer: C

25. Scenario: During a penetration test, your tools flag a potential backdoor in the network. What is your next step?

A. Attempt to exploit the backdoor for more information.

B. Notify the organization and help them analyze the backdoor.

C. Ignore it if it is not part of your test scope.

D. Publicize the finding as a major vulnerability.

Answer: B