[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 2488 **L**

Unique Paper Code : 2343010018

Name of the Paper : Ethical Hacking

Name of the Course : **DSE**

Semester : VI / VIII

Duration : 3 Hours Maximum Marks : 90

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. Question No. **1 (Section A)** is compulsory.
3. Attempt any **4 (four)** questions from **Section B**.
4. Parts of a question should be attempted together.

Section A

Q1	(a)	Define Denial of Services attack, and how does it differ from DDoS attack?	3
	(b)	What is TCP connect Scan? Write the correct nmap options used to perform this scan and explain it.	3
	(c)	What is the role of the ICMP packet in the ping command? Explain with a suitable example.	3
	(d)	What is port scanning? List any four of the common port numbers and their corresponding services.	3

(e) What is password cracking? Name any two local password cracking tools. 3

(f) What is the relevance of domain / ICT Infrastructure to information security in threat and vulnerability management? 3

(g) What is SET? How is it used in gaining access to an organization? 3

(h) Differentiate between Black box and White box penetration testing with an example. 3

(i) How Social media platforms are used to conduct targeted attacks. 3

(j) Define Bind and reverse payload why they are used. 3

Section B

Q2 (a) A mid-sized organization recently noticed unusual activity in its network. Several employees reported that their systems were running slowly. Upon investigation, the IT team discovered that the systems were running outdated software, and sensitive company data appeared to have been accessed without authorization. An attacker had used a specific technique to take advantage of these weaknesses and gain unauthorized access to the network. 6

1) Identify and explain the type of cybersecurity issue faced by the organization.

2) Suggest any three measures the organization should implement to prevent such incidents in the future.

(b) Explain five malicious codes that can harm the computer system. 5

(c) What is the use of cross-site scripting? How can it help users to access trusted websites? 4

Q3 (a) How does scanning an enumeration help to gather information for any system? Explain its four distinct phases. 5

(b) Differentiate between adversarial and non-adversarial threats. Explain any two non-adversarial threat sources. 5

(c) Write any five elements of vulnerability Management Guidelines? 5

Q4 (a) List four web discovery tools. How do they work in finding the vulnerability of web discovery, explain through any one tool? 5

(b) List the stages of penetration testing, and explain it in reference to any startup company. 5

(c) What are the capabilities of MEDUSA? Explain the following commands. 5

```
medusa -h target_ip -u username -P
  path_to_password_dictionary -M
 authentication_service_to_attack
```

Q5 (a) How does Metasploit act as a powerful exploit tool to ethical hackers? 5

(b) Write short notes on the following: 10

1. Three-Way handshaking
2. ifconfig command
3. OWASP
4. Intrusion Prevention System
5. FISM Act

Q6 (a) Explain any five major elements of information security. 5

(b) What is an SQL Injection attack? Explain with an example. 5

(c) A tester performs an Xmas tree scan on two systems: Linux operating system and Windows operating system. The scan works effectively on Linux, but it fails on Windows. 5

1) Why does the scan work on Linux systems?

2) Why is it ineffective on Windows systems?

Q7 (a) What is a malicious hacker? Explain any four sub-categories of malicious hackers adapted from NIST. 5

(b) What are Google directives? Enlist six Google directives that help ethical hackers. 4

(c) Draft a sample executive summary for a Risk assessment of information security for hospital management. 6