[This question paper contains 4 printed pages.]

Your Roll No.....

Sr. No. of Question Paper : 273 **L**

Unique Paper Code : 2343010018

Name of the Paper : Ethical Hacking

Name of the Course : **DSE (NEP-UGCF2022)**

Semester : 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. The paper has **two** sections. **All** questions in **"Section A"** are compulsory.
3. Attempt any **four** questions from **"Section B"**.
4. Parts of a question must be answered together.

SECTION A

1. (a)	What is Hashing? How is it different from encryption?	(3)
(b)	Differentiate between footprinting and scanning.	(3)
(c)	What is Social Engineering? Explain any one technique.	(3)
(d)	Name any two password cracking techniques and explain any one of the techniques.	(3)
(e)	What do you mean by a three-way handshake?	(3)
(f)	What is Session Hijacking? Give a suitable example.	(3)
(g)	What is a loopback address? Differentiate between the `ipconfig` and `ifconfig` commands.	(3)
(h)	Give any three disadvantages of clearing logs.	(3)

(i) Write any three ways to gather intelligence for Threat and Vulnerability Management (TVM). (3)

(j) Describe the features of the Metasploit Framework. (3)

SECTION B

2. (a) What is Malware? Explain any two types of Malware. (5)

(b) An e-commerce company plans to test its web application's security ahead of a major sale event. The security team hires a penetration tester and provides only the website URL, without any internal details. During testing, the tester identifies vulnerabilities in the login page and the payment gateway. (5)

Based on the above case, answer the following:

a) Identify the type of penetration testing being performed.

b) Explain the approach used by the tester.

c) Mention two limitations of this testing method in this scenario.

(c) What is Information Security? Describe the CIA triad and its importance in security systems. (5)

3. (a) What are the three core functions of the NIST cybersecurity framework? Explain the role of NIST guidelines (SP 800-12) in information security. (5)

(b) What is black box hacking and white box hacking? Identify the type of hacking in the scenarios given below: (5)

i) A company is preparing to launch a web-based platform and hires a security analyst to review its functionality

ii) A person is trying to use the money that belongs to another unknown person's bank account on the Amazon website.

iii) A hacker finds the bug in an e-commerce company's website and reports it to the concerned company.

(c) Explain how the TCP packet is handled in Wireshark for network analysis and security. How is the network traffic sniffed using the Wireshark tool? (5)

4.(a) A university network administrator observes unusual activities on the campus network. In one instance, sensitive student data is being secretly monitored without being altered. In another instance, an attacker modifies students' grades in the database without authorization. Based on the above case, answer the following: (5)

i) Identify the type of attack in both scenarios.
ii) Differentiate between these two types of attacks.
iii) Suggest one preventive measure for each type of attack.

(b) What is SQL Injection? Give any two examples and how they can be prevented? (5)

(c) Explain the Ethical Hacking Lifecycle with a diagram. (5)

5.(a) What is Cross-Site Scripting (XSS)? Differentiate between stored and reflected XSS. (5)

(b) What is the function of the options in the following commands? (5)

i. `fping -a -g 192.17.44.1 192.17.44.254`

ii. `nmap -sT -p- -Pn 192.16.48.132`

(c) Differentiate between a DoS and a DDoS attack with the help of a real-time scenario. (5)

6.(a) What are the different stages of the Cyber Kill Chain Model? (5)

(b) What is a password dictionary? How does the John the Ripper (JtR) tool use a password dictionary to crack the password? Explain with an example. (5)

(c) Explain NetBIOS enumeration with real-world implications. (5)

7. (a) Define the following terms: (10)

(i) Intrusion Detection Systems

(ii) HTTrack

(iii) Trojan Horse

(iv) Bot-Network

(v) Advanced Persistent Threat

(b) What are the different phases of penetration testing? (5)