Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
End Semester Examination, Dec 2023

Course: Ethical Hacking & Penetration Testing **Semester: VII**
Program: B. Tech. CSE + CSF **Time 03 hrs.**
Course Code: CSSF4016P **Max. Marks: 100**

SECTION A

1. **Each Question will carry 5 Marks**
2. **Instruction: Complete the statement / Select the correct answer(s)**

S. No.	**Question**	**Marks**	**CO**
Q 1	________________ is the process of discovering systems on the network and taking a look at what open ports and applications may be running. a) scanning b) Cyber-printing c) OS fingerprinting d) OS penetration testing	5	**CO3**
Q2	______________ is the technique used in business organizations and firms to protect IT assets. a) Ethical hacking b) Unethical hacking c) Fixing bugs d) Internal data-breach	5	**CO1**
Q3	After performing _____________ the ethical hacker should never disclose client information to other parties. a) hacking b) cracking c) penetration testing d) exploiting	5	**CO1**
Q4	A penetration tester must identify and keep in mind the ____________ & ____________ requirements of a firm while evaluating the security postures. a) privacy and security b) rules and regulations c) hacking techniques d) ethics to talk to seniors	5	**CO4**

SECTION B

1. **Each question will carry 10 marks**
2. **Instruction: Write short / brief notes**

Q 7	Describe in detail the phases of ethical hacking. Provide a comprehensive overview of each phase, highlighting the key activities and their importance in ensuring the security of an organization's information systems. Additionally, explain how these phases contribute to the overall ethical hacking process.	10	**CO1**

Q 8	Explain the concept of wireless sniffing in detail, highlighting its significance and potential security risks for wireless networks. Describe the techniques used in wireless sniffing, emphasizing how attackers can intercept and analyze data packets.	10	**CO4**
Q 9	Following is a **CASE STUDY** given: A multinational corporation encountered a supply chain cyber attack that disrupted its manufacturing operations and compromised confidential business data. Assess the weaknesses in the supply chain that allowed the breach to occur and provide a strategic plan to strengthen the organization's supply chain security.	10	**CO2**
Q 10	Explain the terms Foot Printing and Reconnaissance. How to use it? Elaborate types of Foot Printing. OR Explain the phishing attack. How one can perform the phishing attack. Also, elaborate its mitigation steps.	10	**CO2**

Section C

1. **Each Question carries 20 Marks.**
2. **Instruction: Write long answer.**

Q12	What is SQL injection attack. Elaborate it with example. Explain the complete procedure to perform the SQL injection attack. Further, discuss the complete procedure to identify it and its mitigation steps.	20	**CO3**
Q13	Following is the **CASE STUDY** given: A multinational corporation's internal network was compromised by a targeted cyber attack, resulting in significant data loss. Investigate the spidering techniques employed by the ethical hacking team to assess the network's vulnerabilities, and propose an enhanced security protocol to prevent similar breaches in the future. Discuss the impact of the spidering findings on the corporation's data protection measures and overall cybersecurity strategy.	20	**CO5**