Name:

Enrolment No:

UPES
UNIVERSITY WITH A PURPOSE

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES
Online End Semester Examination, May 2021

Course: Ethical Hacking & Penetration Testing **Semester: VI**
Program: B. Tech. CSE + CSF **Time 03 hrs.**
Course Code: CSSF 3010 **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**	**CO**
Q 1	In TCP Header, ____________ flag forces the delivery of data, without concern for any buffering whereas ______________ flag signifies an ordered close to communications.	**CO1**
Q2	Mention any 5 tools that can be used in Active Reconnaissance. ___________ , __________ , ______________ , _______________ , ______________ .	**CO1**
Q3	_______________ , ________________ and _____________ are the three tools that are used for performing ARP Poisoning.	**CO3**
Q4	Write down the port numbers of the following protocols / services: A) SMB = B) RDP = C) DNS = D) Telnet = E) SSH =	**CO4**
Q5	Which of the following options shows the protocols in order from strongest to weakest? A) WPA, WEP, WPA2, Open B) WEP, WPA2, WPA, Open C) Open, WPA, WPA2, WEP D) WPA2, WPA, WEP, Open	**CO5**
Q6	MAC spoofing applies a legitimate MAC address to an unauthenticated host, which allows the attacker to pose as a valid user. Based on your understanding of ARP, what would indicate a bogus client? A) The MAC address doesn't map to a manufacturer. B) The MAC address is two digits too long. C) A reverse ARP request maps to two hosts. D) The host is receiving its own traffic.	**CO3**

SECTION B

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

Q 7	Imagine for a moment that you are a hacker; an ethical one. What steps do you follow to hack	**CO1**

	the target? Explain the steps by taking an example and tools used.	
Q 8	What is session hijacking? Explain the steps involved and preventive measures for session hijacking?	**CO2**
Q 9	Differentiate between Vulnerability Assessment and Penetration Testing. Also, write down the types of penetration testing approaches.	**CO3**
Q 10	Explain Sniffing and Spoofing with an example? Name at least 3 tools used for sniffing and spoofing.	**CO3**
Q 11	Write down OWASP Top 10 Web Applications vulnerabilities. Also, explain about them in short. OR What are various Network related vulnerabilities? How Vulnerability Assessment is done through Nessus? Mention the steps involved.	**CO5**
Section C **1. Each Question carries 20 Marks.** **2. Instruction: Write long answer.**		
Q12	What is Metasploit? For what purpose it is used? Write down about the types of modules available in Metasploit. Write down the steps involved in attacking a machine whose IP address is 192.168.135.139 OR What is NMAP? For what purpose it is used? Write down the commands for running the different types of scans on target IP 192.168.135.139.	**CO4**