Name:

Enrolment No:

UNIVERSITY OF PETROLEUM AND ENERGY STUDIES

End Semester Examination, May 2022

Course: B. Tech (CSE H+NH) **Semester: VI**

Program: Ethical Hacking & Penetration Testing **Time : 03 hrs.**

Course Code: CSSF3010 **Max. Marks: 100**

Instructions: All questions are compulsory (except Q9 & 11 of sections B & C respectively have an internal choice.)

SECTION A
(5 Q x 4 Marks = 20 Marks)

S. No.		**Marks**	**CO**
Q 1	Explain Passive Reconnaissance? List at least 5 tools/methods for performing passive reconnaissance.	**4**	**CO1**
Q 2	Differentiate between Sniffing and Spoofing by taking an example. List at least 3 tools to perform sniffing.	**4**	**CO1**
Q 3	Explain TCP/IP 3-way Handshaking with the help of a diagram.	**4**	**CO2**
Q 4	a) If the TTL value is 128, what could be the target operating system? b) What is Banner Grabbing?	**4**	**CO3**
Q 5	Describe the Man-in-the-middle (MITM) attack? Explain with the help of a diagram the various steps involved in performing the MITM attack.	**4**	**CO4**

SECTION B
(4 Q x 10 Marks = 40 Marks)

Q 6	Enumerate Session Hijacking? Explain the steps involved in Session Hijacking and discuss its prevention.	**10**	**CO4**
Q 7	Explain the hacking process for WPA2 PSK. Also, explain at least 5 wireless hacking techniques.	**10**	**CO3**
Q 8	Differentiate between the following (2 marks each): a) Bind shell v/s Reverse Shell b) WEP v/s WPA v/s WPA2 c) Staged v/s Non-staged payload d) SQL Injection v/s CSRF e) Activity Profiling v/s Sequential Change-Point Detection	**10**	**CO2**

Q 9	Explain Vulnerability Assessment (VA)? How is it performed? Write the different types of VA and the tools used. OR Describe Penetration Testing? What are the different types of penetration testing? Explain the phases involved in penetration testing.	**10**	**CO1**
SECTION-C **(2 Q x 20 Marks = 40 Marks)**			
Q 10	Imagine for a moment that you are a hacker; an ethical one. You are called upon by law enforcement based on your expertise to hack into a network of a business known to be launching crimes against humanity as its primary mission for operation and capital gain. Assume you are not to be concerned with any politics of the job and your actions are legal and ethically justified. This nefarious business takes its own security seriously and therefore has implemented several forms of network security such as firewalls, Web proxies for its Web gateways, and VPNs for remote users. You also know that this business exists much like any normal corporation, renting several floors of office space to accommodate between 100-200 employees. Also, imagine that the business's entire network topology is located in that same location. Your goal is to infiltrate the security enough to find evidence included in the local MSQL database. You need to remain anonymous and operate within the reasonable parameters of the law. a) Explain your method of attack and operation within reasonable parameters of the law. [5 marks] b) Discuss specific malware, social engineering, or any other type of attacks you would deploy to achieve your desired goals. [5 marks] c) Assess the hurdles you expect and how you plan to overcome them. [5 marks] d) Determine how you would remain anonymous without blowing your cover. [5 marks]	**20**	**CO1**
Q 11	Explain OWASP Top 10 vulnerabilities in detail with diagrams and examples wherever possible. OR Enumerate the attack tool 'Metasploit'. What is the purpose and mention the types of modules available along with the steps involved in attacking a machine whose IP address is 192.168.130.13 on port 80 and 21.	**20**	**CO4**