


Name:			
Enrolment No:			
UNIVERSITY OF PETROLEUM AND ENERGY STUDIES End Semester Examination, May 2022			
Course: B.Tech (CSE+CSF) Program: Ethical Hacking & Penetration Testing Course Code: CSSF3010		Semester: VI Time : 03 hrs. Max. Marks: 100	
Instructions: All questions are compulsory (except Q9 & 11 of sections B & C respectively have an internal choice.)			
SECTION A (5Qx4M=20Marks)			
S. No.		Marks	CO
Q 1	a) If the TTL value is 128, what could be the target operating system? b) What is Banner Grabbing?	4	CO3
Q 2	Differentiate between Sniffing and Spoofing by taking an example. List at least 3 tools to perform sniffing.	4	CO1
Q 3	What is Man-in-the-middle (MITM) attack? Explain with the help of a diagram the various steps involved in performing the MITM attack.	4	CO4
Q 4	What is Active Reconnaissance? List at least 5 tools/methods for performing active reconnaissance.	4	CO1
Q 5	Explain TCP/IP 3-way Handshaking with the help of a diagram.	4	CO2
SECTION B (4Qx10M= 40 Marks)			
Q 6	What is 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	What is Vulnerability Assessment (VA)? How it is done? Write the different types of VA and the tools used. OR What is Penetration Testing? What are the different types of penetration testing? Explain the phases involved in penetration testing.	10	CO1
SECTION-C (2Qx20M=40 Marks)			

Q 10	<p>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.</p> <p>a) Explain your method of attack and operation within reasonable parameters of the law. [5 marks]</p> <p>b) Discuss specific malware, social engineering, or any other type of attacks you would deploy to achieve your desired goals. [5 marks]</p> <p>c) Assess the hurdles you expect and how you plan to overcome them. [5 marks]</p> <p>d) Determine how you would remain anonymous without blowing your cover. [5 marks]</p>	20	CO1
Q 11	<p>Write down OWASP Top 10 vulnerabilities in 2021. Also, explain them in short.</p> <p style="text-align: center;">OR</p> <p>What is Metasploit? For what purpose it is used? Write down the types of modules available in Metasploit. Write down the steps involved in attacking a machine whose IP address is 192.168.130.13</p>	20	CO4