


Name:			
Enrolment No:			
UPES End Semester Examination, May 2024			
Course: Ethical Hacking & Penetration Testing Program: B TECH(CSE+CSF-H/NH) Course Code: CSSF3010		Semester: VI Time : 03 hrs. Max. Marks: 100	
Instructions: All questions are COMPULSORY. Internal choice available in Q9 and Q11.			
SECTION A (5Qx4M=20Marks)			
S. No.		Marks	CO
Q 1	Exemplify the prioritization of vulnerabilities discovered during a penetration test?	4	CO1
Q 2	Write down the port numbers of the following protocols: a) SSH b) SMTP c) IMAPS d) POP3	4	CO2
Q 3	Differentiate between Sniffing and Spoofing?	4	CO2
Q 4	What is ARP Cache Poisoning? Explain with a diagram.	4	CO3
Q 5	List any four modules of Metasploit Framework.	4	CO4
SECTION B (4Qx10M= 40 Marks)			
Q 6	Explain the hacking process for WPA2 PSK. Also, explain at least 5 wireless hacking techniques.	10	CO4
Q 7	What is Session Hijacking? Explain the steps involved in Session Hijacking and discuss its prevention.	10	CO1
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	CO3

SECTION-C
(2Qx20M=40 Marks)

Q 10	<p>You are a senior cybersecurity consultant leading a team of ethical hackers and penetration testers assigned to assess the security posture of a multinational financial institution. The organization has recently experienced a series of cyberattacks targeting its online banking platform, resulting in significant financial losses and reputational damage.</p> <p>During the preliminary reconnaissance phase of the penetration test, your team uncovers evidence suggesting that the cyberattacks may be orchestrated by a sophisticated threat actor with access to advanced tools and techniques. Further investigation reveals indications of insider involvement, potentially compromising sensitive customer data and transaction records.</p> <p>Upon notifying the organization's executive management about the findings, you are tasked with conducting a thorough investigation to identify the root cause of the security breaches, assess the extent of the damage, and recommend immediate remediation measures to mitigate the ongoing risks.</p> <p>Question: a. Describe the steps you would take to investigate the security breaches within the financial institution's online banking platform, considering the potential involvement of both external threat actors and insider threats. (10 marks)</p> <p>b. Develop a comprehensive incident response plan outlining the roles, responsibilities, and actions to be taken by the cybersecurity team, IT personnel, and executive management in response to security breaches. Include measures to preserve evidence, contain the incident, and restore normal operations while minimizing further damage. (10 marks)</p>	20	CO5
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	CO2