Sardar Patel Institute of Technology
Bhavan's Campus, Munshi Nagar, Andheri (W), Mumbai : 400058, India
(Autonomous College of Affiliated to University of Mumbai)

End Semester Examination

May 2023

Maxi Marks : 100
Class : T.E./B.E. Semester :VI/VII
Course code: IT321
Name of the course : Ethical Hacking

Duration : 3 hours
Date:17/05/2023
Branch : IT/COMP

Note:
[1] Answer all questions.
[2] Assume suitable data if necessary stating it clearly.
[3] *Read the each question carefully and follow instructions given for each question if any.*
[4] *Keep your answers clear and concise, and state all of your assumptions carefully.*

Q No	Question	Marks	CO	BL
1 (a)	i. If you accidentally find someone's password and use it to get into a system, is this hacking? Explain. ii. Someone sends you a "game." When you run it, it logs you into critical server. Is this hacking? Explain. iii. Could you be prosecuted for doing this? iv. You have access to your home page on a server. By accident, you discover that if you hit a certain key, you can get into someone else's files. You spend just a few minutes looking around. Is this hacking? Explain.	10	1	3
1(b)	What makes system vulnerable?	5	1	3
1(c)	As you know telnet is insecure protocol. It is highly discouraged to use telnet service in enteprise network as per security policy. But you have a got preinstalled the system (OS or Manageable Switch) in which telnet is already running. i. How do you take care of insecure telnet service at operating system (OS) level? i. ii. How do you take care of insecure telnet service in case, system administrator forgot to stop the service?	5	1	3
2(a)	Why do you think DoS attackers use zombies to attack victims instead of sending attack packets directly to victims? Come up with two reasons.	10	2	3
2(b)	Develop a comprehensive plan for conducting a penetration test using the Penetration Testing Execution Standard (PTES) framework. Your plan should include all seven phases of the PTES framework, as well as specific tools and techniques that you would use in each phase. Additionally, describe any challenges or obstacles that you might encounter during the penetration testing process and how you would address them	10	4, 2	6

3(a)	VAPT-Vulnerability Assessment and Penetration Testing: Compare and contrast the key differences between Network VAPT and Web VAPT. In your answer, discuss the objectives, scope, methodology, tools, and techniques used in each type of VAPT. Provide specific examples to illustrate your points.	10	3	4
3(b)	Can you design a complex blended cyber attack against a large financial institution that could result in the theft of millions of dollars? Describe the various stages of the attack, including the tools and techniques used, the potential vulnerabilities exploited, and the potential impact on the organization. How would you defend against such an attack? What kind of proactive security measures should the financial institution have in place to prevent such an attack from happening?	10	4	5
4(a)	Can you analyze and evaluate the mindset of a hacker, comparing and contrasting ethical and malicious motivations, and provide examples of how each type of hacker approaches a security challenge? **OR** What are the potential vulnerabilities in a wireless network, and how can they be exploited by attackers? How would you go about conducting a wireless penetration testing engagement for a corporate network, and what tools and techniques would you use to identify and exploit vulnerabilities? How would you prioritize the vulnerabilities you discover based on their potential impact to the organization, and how would you communicate those findings to senior leadership and technical stakeholders?	10	1, 2	4
4(b)	Analyze the impact of viruses, computer worms, and malware on a system's security and identify ways to prevent or mitigate the effects of such attacks.	10	3	6
5(a)	Design a complex blended cyber attack that includes evasion techniques for intrusion detection systems (IDS). Describe the various stages of the attack, including the tools and techniques used, the potential vulnerabilities exploited, and the potential impact on the targeted organization.	10	3	4
5(b)	DevOps (Development and Operations) is a methodology that emphasizes collaboration and communication between software developers and IT operations teams. It aims to reduce the time between code development and its deployment, while ensuring quality and security. Evaluate the Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) **OR** As a security consultant, how would you go about designing and implementing a Security Operations Center (SOC) for a large multinational organization with complex and diverse network assets and operations? What factors would you need to consider when designing the SOC, such as the organization's risk profile, regulatory requirements, and business objectives? How would you identify the right mix of people, processes, and technology to effectively monitor, detect, and respond to security threats in real-time? What tools and technologies would you recommend for the SOC.	10	4	4