Bharatiya Vidya Bhavan's
Sardar Patel Institute of Technology
Munshinagar, Andheri(W), Mumbai-400058
Master of Computer Application Department
IT321: Ethical Hacking
T.Y. B.Tech Sem-VI
End Semester Examination (Makeup)

Date: 4/7/2023

Total:100 Marks
Duration: 180 Minutes

Note:
[1] *Answer all questions.*
[2] *Assume suitable data if necessary stating with 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	BL	CO
Q.1a)	Distinguish between Attack,Attacker, Asset, Vulnerability, Risk, Exploit and Access Control.	10	3	1,2
Q.1b)	Analyzing a network infrastructure, identify and classify the potential attack vectors that could be exploited by an external threat actor. Describe the characteristics and potential impact of each attack vector, and propose appropriate countermeasures to mitigate the risks.	10	4	1,2
Q.2a)	Analyse the following wireless network attacks and provide the appropriate countermeasures: i] Wardriving ii] Rouge Access Point iii] Bluesnarfing iv] Bluebugging	10	4	1,2
Q.2b)	You would be expected to compare and contrast the methodologies and tools used for malware testing with those used in traditional vulnerability assessments. This analysis should encompass the specific evasion techniques employed by advanced malware to bypass detection, as well as the countermeasures employed by security solutions to detect and mitigate malware attacks.	10	3	3
Q.3a)	Diferentiate between SQL injection attack and Cross-Site Scripting attack (XSS)	10	3	4
Q.3b)	Analyze the characteristics and potential impacts of viruses, computer worms, and malware as exploit mechanisms for computer systems. Compare and contrast their modes of operation, propagation methods, and the types of vulnerabilities they target.	10	4	3

	Evaluate the potential consequences of a successful infection by each type of malicious software on a networked system, including data loss, system downtime, and unauthorized access.			
Q.4a)	Cloud Computing is all the more important for small businesses than big ones given the fact that it reduces operational cost and brings speed, accuracy. There are a lot of innovative products that provide storage, software, and infrastructure through the cloud, businesses can minimize their IT expenses. You are conducting Vulnerability Assessment and Penetration Testing (VAPT). Draw a neat diagram of process in Cloud Application Penetration Testing (Cloud VAPT)	10	4	4
Q.4b)	Develop a comprehensive penetration testing plan for a mobile application, outlining the specific steps, tools, and methodologies to assess its security. **OR** Conduct a comprehensive analysis of the role and methodologies involved in firewall penetration testing for assessing the effectiveness of network security controls. Evaluate the challenges and considerations specific to firewall penetration testing, including different firewall types (e.g., packet-filtering, stateful inspection) and network architectures.	10	4	1,4
Q.5a)	From a technology perspective, any device connected to a network could be a potential entry point for hackers.When evaluating solutions for critical infrastructure locations. Define Critical Infrastructure. Analyse key factors should organizations look for to reduce the risk that they will not be the "weakest link" on the network?	10	4	3
Q5b)	Conduct a comprehensive analysis of the role and importance of DevOps penetration testing in ensuring the security of software development and deployment processes. Evaluate the specific challenges and considerations involved in conducting penetration testing within a DevOps environment, including continuous integration/continuous deployment (CI/CD) pipelines. Compare and contrast traditional penetration testing methodologies with those adapted for DevOps. **OR** Propose strategies to integrate penetration testing seamlessly into the DevOps workflow while ensuring minimal disruption to software delivery and maintaining a high level of security.	10	4	4