RAMAIAH Institute of Technology

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

M.Tech in Computer Network Engineering

II SEMESTER

Network Security Laboratory-MCNL28

I.A. Marks: 50 **Exam Hours: 03**

Credits: 0:0:1 **Exam Marks: 50**

SL. No.	QUESTIONS
1.	Imagine you are working as a cybersecurity analyst for a financial institution, you have been assigned the critical task of conducting a Nessus vulnerability analysis on a critical host system (windows, Linux) in the local network hosting sensitive customer data. Detail your step-step approach, including pre-scan preparations, specific Nessus configurations for maximum efficacy in an environment, scan the targets, prioritize and analyze the results and generate reports.
2.	As part of a penetration testing engagement for a client, you're tasked with evaluating the security internal network. You suspect that sensitive data might be leaking from one of their development due to a potential misconfiguration or a compromised machine within their network. To investigate you plan to intercept network traffic using Wireshark to identify any unauthorized data transfers.
3.	As a member of Blue team experts in Monitoring and Technical Support of a medium sized company, you have been asked to assess the security posture of the internal network. Use Nmap for network discovery, Port scanning, Service version detection and vulnerability detection. Then Document your findings, including the identified vulnerabilities, their severity levels.
4.	Design a C program to demonstrate Buffer overflow. And illustrate how it can be exploited by the attacker.
5.	Imagine you are a member of Red Team in a company, you have been assigned a penetration testing task to assess the security of a corporate network using Kali Linux and the Metasploit framework. Outline a step-by-step process for utilizing Metasploit to identify and exploit vulnerabilities within the network.
6.	Imagine a legal firm handling contracts for clients remotely. Let's say a client, Mr. John, needs to sign a contract for a property purchase. how could Cryptool be applied to digitally sign a contract document, authenticate its validity, and ensure the secure storage of both the digital signature and the original document? Demonstrate the use of digital signatures using cryptool by performing following things: a) Creation of signature b) Storing the signature c) Verifying the signature
7.	Design a python program to implement RSA Algorithm.
8.	Imagine you're a cybersecurity analyst tasked with assessing the security of a newly developed e-commerce website. You would utilize Burp suite and perform following activities to identify and mitigate security flaws in the web application. Start by describing the setup process for Burp Suite, including configuring proxy settings and initiating automated scans to detect common vulnerabilities like SQL Injection. i. Manual Testing of SQL Injection ii. Proxy Attack with Burp Suite.
9.	Imagine you're a cybersecurity analyst responsible for evaluating the security of a newly launched online education platform. You need to use Burp Suite to find and address any security issues

	within the application. Explain how you would set up Burp Suite, including configuring the proxy settings and running automated scans to uncover common vulnerabilities. a) XSS (Cross Site Scripting) b) CSRF (Cross Site Request Forgery)
10.	ABC Corp, a medium-sized company, is concerned about the security of its network and wants to ensure that its employees are using strong passwords. The IT security team has been tasked with conducting a password strength assessment to identify weak passwords that may pose a security risk. The IT security team decides to use a password cracking tool, to perform the password strength assessment. The plan to target the company's internal systems, including FTP, SSH. By using Hydra password cracking tool perform a password strength assessment, so that ABC Corp's IT security team was able to identify and address weaknesses in their network's authentication mechanisms.
11.	Imagine you are the network security administrator for a medium-sized e-commerce company that operates an online store handling sensitive customer information. Recently, there have been reports of intermittent service disruptions and slow response times on your company's website, resulting in customer complaints and loss of revenue. After conducting initial investigations, you suspect that the website may be experiencing denial-of-service (DoS) attacks, specifically SYN floods and Ping flood attacks. So, it is important for organizations to have response plans in place to mitigate the impact of DoS attacks on their operations. Use Hping3, kali Linux tool to perform SYN floods and ping flood attacks to launch DOS attack on the target machine and proactively monitor the networks for signs of attack.
12.	In a cybersecurity lab environment, a team is tasked with implementing and testing an Intrusion Prevention and Detection System (IDS) using Snort. The team's objectives include configuring Snort for optimal performance, conducting rigorous testing to ensure its effectiveness, and developing custom Snort rules tailored to specific security requirements. Additionally, the team aims to simulate real-world attack scenarios using Kali Linux to detect and mitigate potential threats effectively.

Marks Distribution:

	Write-Up	Execution	Viva/Demo	Change of Program	Total
Conduction and Result	**8**	**35**	**7**	**-10 Marks**	**50 Marks**

Reviewed by HoD, Dept. of CSE

RAMAIAH
Institute of Technology

Reviewed by

HoD, Dept. of CSE