CHAROTAR UNIVERSITY OF SCIENCE AND TECHNOLOGY
FACULTY OF TECHNOLOGY AND ENGINEERING
DEVANG PATEL INSTITUTE OF ADVANCE TECHNOLOGY AND RESEARCH
CSE312/IT348 - CRYPTOGRAPHY AND NETWORK SECURITY

PRACTICAL LIST – AY: 2025- 26

Practical Number		CO/PO
0	**Problem Definition** A security training institute plans to establish an advanced ethical hacking laboratory for beginner and intermediate learners. The institute must strategically select the most suitable penetration testing operating system between Kali Linux and Parrot Security OS by evaluating installation complexity, hardware resource consumption, tool ecosystem, update stability, and real-world usability. Students must perform a comparative technical assessment and justify the final OS selection for enterprise-scale cyber training deployment. **Key Questions / Analysis / Interpretation to be evaluated during/after Implementation** 1. Which operating system provides a smaller attack surface for a cybersecurity training lab, and why? 2. How would enterprise performance, compliance, and scalability requirements influence the final OS selection decision? **Supplementary Problems -** 1. Evaluate the effect of kernel hardening on penetration testing tool compatibility. **Key Skills to be addressed** – 1. Strategic OS evaluation 2. Performance vs Security Analysis **Applications -** 1. Cybersecurity training labs 2. Penetration testing **Learning Outcome -** Students will be able to evaluate and justify the selection of a penetration testing operating system for enterprise use. **Tools / Technology To Be Used -** • Kali Linux • Parrot OS • VirtualBox / VMware **Total Hours of Engagement**: 3 Hours **Post Laboratory Work Description -** Prepare comparative evaluation report.	CO1

	Reference - https://www.kali.org/ https://parrotlinux.org/	
1	The **CSE Department of DEPSTAR** has introduced a secure communication policy for internal messaging between **faculty coordinators and student volunteers** during spoural. Recently, an incident occurred where an external person tried to access internal communication messages on an unsecured Wi-Fi network. To avoid such issues, the department decided to use **classical encryption techniques** (Substitution and Transposition ciphers) for training students before moving to modern cryptography. As a security student, you have to: • Encrypt **a message** using 1. Substitution Cipher (Caesar OR Monoalphabetic) 2. Transposition Cipher (Columnar / Rail Fence) • Decrypt the received message at the faculty side. • Compare the security and analyse which technique provides better resistance to eavesdropping. **Key Questions / Analysis / Interpretation to be evaluated during/after Implementation** 1. How does key length and complexity impact the strength of the chosen cipher? 2. What are the limitations of classical cryptography in modern communication systems? **Supplementary Problems:** 1. Implement **double encryption**: Substitution → Transposition. Analyze if security improves. **Key Skills to be addressed –** 1. Understanding classical encryption techniques 2. Hands-on implementation of ciphers 3. Secure communication concepts 4. Cryptanalysis fundamentals 5. Problem-solving & logical reasoning **Applications -** 1. Secure messaging 2. Training in cryptography **Learning Outcome -** Students will understand and implement classical encryption techniques. **Tools / Technology To Be Used -** Python / C / Java	CO1

	Total Hours of Engagement: 3 Hours **Post Laboratory Work Description -** Prepare comparison report of ciphers. **Reference -** https://www.geeksforgeeks.org/classical-encryption-techniques/	
2	**Problem Definition** Secure covert communication is a growing concern in cyber defense and espionage domains. You are required to design, implement, and evaluate a steganographic communication system using images, audio, or video files. The objective is to critically analyze how hidden data transmission can be optimized for secrecy while minimizing forensic detectability, and to assess the potential for misuse in data exfiltration attacks. **Key Questions / Analysis / Interpretation to be evaluated during/after Implementation** 1. How does the choice of cover medium (image, audio, video) influence the detectability of hidden information? 2. What trade-offs exist between payload capacity and invisibility in steganographic systems? 3. How can attackers exploit steganography for covert data exfiltration and command transmission? **Supplementary Problems -** 1. Perform steganalysis using visual, histogram, and frequency-domain techniques. 2. Compare spatial-domain and transform-domain steganography under forensic attack conditions. **Key Skills to be addressed -** 1. Covert data hiding 2. Forensic analysis **Applications -** 1. Digital watermarking 2. Cyber forensics **Learning Outcome -** Students will be able to analyze secure steganographic communication. **Tools / Technology To Be Used -** • Steghide • Xiao Steganography **Total Hours of Engagement:** 2 Hours **Post Laboratory Work Description -** Prepare steganalysis report.	CO1

	Reference - https://www.youtube.com/watch?v=xepNoHgNj0w	
3	**Problem Definition** A medium-sized software enterprise, is exposed to increasing cyber threats originating from publicly available digital footprints. Students must act as cyber threat intelligence analysts and perform structured OSINT-based footprinting to extract, correlate, and evaluate publicly accessible organizational data. The goal is to assess how adversaries exploit digital exposure and to design strategic mitigation controls to reduce OSINT-based attack surfaces. **Key Questions / Analysis / Interpretation to be evaluated during/after Implementation** 1. How can multiple OSINT data sources be correlated to predict targeted cyberattacks on an organization? 2. Which categories of publicly available information pose the highest operational and reputational risk? 3. How can digital footprint minimization strategies reduce an organization's cyber exposure? **Supplementary Problems -** 1. Build a cyber threat actor profile. 2. Design an OSINT policy. **Key Skills to be addressed -** 1. Threat intelligence 2. Data correlation **Applications -** 1. Cyber intelligence units 2. Law enforcement **Learning Outcome -** Students will be able to evaluate cyber exposure using OSINT. **Total Hours of Engagement:** 4 Hours **Post Laboratory Work Description -** Prepare OSINT exposure assessment report. **Reference -** https://osintframework.com/	CO2
4	**Problem Definition** A corporate organization suspects internal network compromise and requires a complete adversarial security reconnaissance. Students must perform intelligent network scanning using Nmap to discover active hosts, services, OS fingerprints, and vulnerabilities. The task involves correlating scan results to predict possible attack chains and prioritizing devices based on breach impact and lateral movement potential.	CO2

	Key Questions / Analysis / Interpretation to be evaluated during/after Implementation 1. Which ports enable lateral movement? 2. How do misconfigurations escalate attacks? **Supplementary Problems -** 1. Map complete attack paths using the MITRE ATT&CK framework based on scan result. **Key Skills to be addressed -** 1. Network scanning 2. Threat analysis **Applications –** 1. Penetration testing 2. SOC monitoring **Learning Outcome -** Students will be able to analyze internal network vulnerabilities. **Tools / Technology To Be Used -** 1. Nmap 2. Kali Linux **Total Hours of Engagement**: 3 Hours **Post Laboratory Work Description -** Prepare scan interpretation report. **Reference -** https://nmap.org/	
5	**Problem Definition** A banking system using RSA encryption for customer data transmission is compromised due to weak cryptographic parameter selection. Students must mathematically analyze and implement both encryption and cryptanalytic decryption of intercepted ciphertext. The objective is to demonstrate how improper RSA configuration leads to complete security failure and to propose industry-grade cryptographic hardening strategies. **Key Questions / Analysis / Interpretation to be evaluated during/after Implementation** 1. Why does the selection of small RSA modulus values critically weaken cryptographic security? 2. How do mathematical attacks and brute-force attacks on RSA differ in practicality and efficiency? 3. Which padding and key-generation techniques strengthen RSA against modern cryptanalytic attacks?	CO3

	Supplementary Problems- Explore timing-based attacks on RSA decryption operations. **Key Skills to be addressed -** 1. Public-key cryptanalysis 2. Security hardening **Applications -** 1. Banking security 2. PKI **Learning Outcome -** Students will be able to analyze RSA vulnerabilities and mitigation. **Tools / Technology To Be Used -** 1. Python 2. RSA library **Total Hours of Engagement:** 3 Hours **Post Laboratory Work Description -** Prepare RSA attack analysis report. **Reference -** https://www.youtube.com/watch?v=VF3AHG0T9ec	
6	**Problem Definition** A digital forensics team is required to recover encrypted passwords from archived files and secured documents during a cybercrime investigation. Students must evaluate multiple forensic password recovery tools and analyze attack feasibility based on encryption strength, computational cost, time-to-crack, and legal boundaries. The exercise emphasizes ethical, technical, and forensic recovery decision-making. **Key Questions / Analysis / Interpretation to be evaluated during/after Implementation** 1. Which vulnerabilities identified by OpenVAS represent the highest risk for ransomware and remote exploitation? 2. How should vulnerability prioritization change when business impact is considered along with CVSS scores? 3. Which mitigation strategies provide the maximum reduction in exploitability with minimal operational disruption? **Supplementary Problems-** Correlate OpenVAS vulnerability findings with Exploit-DB and CVE databases. **Key Skills to be addressed -** 1. Risk assessment 2. Cyber governance **Applications -**	CO4

	1. Enterprise audits **Learning Outcome -** Students will be able to perform vulnerability assessment and mitigation planning. **Tools / Technology To Be Used -** 1. OpenVAS **Total Hours of Engagement:** 4 Hours **Post Laboratory Work Description -** Prepare a vulnerability remediation report by validating critical OpenVAS findings through controlled attack analysis such as remote exploitation, privilege escalation, or DoS feasibility. **Reference -** https://www.openvas.org/	
7	**Problem Definition** You must conduct an in-depth experimental analysis of classical and modern cryptographic algorithms using CrypTool. The objective is to evaluate algorithm strength, key entropy, susceptibility to cryptanalysis, and future resilience against emerging quantum threats. You are required to compare algorithm security under real-world adversarial conditions. **Key Questions / Analysis / Interpretation to be evaluated during/after Implementation** 1. How does encryption strength affect recovery? 2. What are legal constraints? **Supplementary Problem-** Design hybrid encryption system. **Key Skills to be addressed -** 1. Cipher evaluation 2. Entropy analysis **Applications -** 1. Crypto R&D 2. Security products **Learning Outcome -** Students will be able to evaluate cryptographic algorithms. **Tools / Technology To Be Used -** 1. CrypTool **Total Hours of Engagement:** 3 Hours	CO5

	Post Laboratory Work Description - Prepare algorithm comparison report. **Reference -** https://www.cryptool.org/en/	
8	**Problem Definition** An enterprise plans to deploy a next-generation firewall to protect sensitive network resources. Students must experimentally analyze and compare multiple firewall software solutions based on rule filtering efficiency, attack resistance, throughput performance, and policy misconfiguration risks. The goal is to design a robust enterprise-grade firewall policy architecture. Key Questions / Analysis / Interpretation to be evaluated during/after Implementation 1. How do firewall rule misconfigurations and rule-ordering errors enable unauthorized traffic bypass? 2. Which firewall architectures provide better resilience against zero-day network attacks? 3. How should performance, usability, and security be balanced while designing enterprise firewall policies? **Supplementary Problems-** Simulate classical cryptanalysis attacks on selected modern cryptographic algorithms. **Key Skills to be addressed –** 1. Policy design 2. Zero trust **Applications –** 1. Enterprise security 2. Cloud firewall **Learning Outcome –** Students will be able to be able to design secure firewall policies **Tools / Technology To Be Used –** Windows Defender Firewall **Total Hours of Engagement:** 2 Hours **Post Laboratory Work Description** Prepare firewall evaluation report. **Reference –** https://www.youtube.com/watch?v=pP7_nFBNR-M	CO5

9	**Problem Definition** Enterprise networks increasingly suffer from encrypted malware traffic, insider threats, and protocol abuse. You must use Wireshark to capture and deeply analyze live network traffic, identify anomalous communication patterns, detect suspicious handshakes, and reconstruct potential cyberattack scenarios through packet-level forensic inspection. **Key Questions / Analysis / Interpretation to be evaluated during/after Implementation** 1. Which packet-level behaviors indicate command-and-control (C2) communication by malware? 2. How can encrypted malicious traffic still be fingerprinted using traffic analysis techniques? 3. Which traffic anomalies are strong indicators of insider threat activity? **Supplementary Problems-** Simulate distributed denial-of-service (DDoS) attacks across tested firewall configurations. **Key Skills to be addressed –** 1. Packet analysis 2. Threat detection **Applications -** 1. SOC 2. Malware analysis **Learning Outcome -** Student will be able to analyze threats using packet inspection. **Tools / Technology To Be Used -** Wireshark **Total Hours of Engagement**: 2 Hours **Post Laboratory Work Description** - Prepare traffic forensic report. **Reference -** https://www.youtube.com/watch?v=yC0e0bSSleo	CO5
10	**Problem Definition** A secure web service “SecureDocs” relies on SSL/TLS for secure document transmission. Students must analyze the full SSL/TLS handshake process to verify certificate trust chains, encryption negotiation, and session key establishment. The objective is to identify cryptographic vulnerabilities such as downgrade attacks, fake certificates, replay risks, and to validate TLS security through forensic packet inspection.	CO5

Key Questions / Analysis / Interpretation to be evaluated during/after Implementation

1. How does manipulation of the certificate trust chain enable man-in-the-middle (MITM) attacks?
2. Which TLS downgrade attacks are still relevant in modern networks and why?
3. How does TLS 1.3 improve handshake security and privacy compared to earlier versions?

Supplementary Problems-

Reconstruct a complete ransomware infection timeline using captured network packets.

Key Skills to be addressed -

1. Trust verification
2. Protocol analysis

Applications -

1. HTTPS security
2. Secure APIs

Learning Outcome -

Students will be able to analyze SSL/TLS secure communication.

Tools / Technology To Be Used -

1. Wireshark
2. Browser Dev Tools

Total Hours of Engagement: 4 Hours

Post Laboratory Work Description -

Prepare TLS forensic verification report.

Reference -

https://www.ssl.com/article/ssl-tls-handshake-overview/

***