LABORATORY HANDOUT

CYBER SECURITY FOUNDATION LAB (COM-311)

CSE (Cyber Security) - 3RD SEMESTER

ACADEMIC YEAR (2023-24)

Mr. Arsalan Manzoor Zargar

Assistant Professor

Department of Computer Science and Engineering

Department of Computer Science and Engineering

Model Institute of Engineering & Technology (Autonomous)

Kot Bhalwal, Jammu - 181122

www.mietjmu.in

Course Code	Course Name	Course Type	Cd	L	T	P	Marks		
							Sessional	Final Exam	Total
COM-311	Cyber Security Foundation Lab	PCC	2	0	0	4	50	-	50

COURSE OUTCOMES

At the end of the course the student will be able to:	
CO1	Identify and analyze contemporary cyber threats and their business impact.
CO2	Configure network interfaces and manage security zones on an NGFW.
CO3	Recognize and mitigate malware, exploits, and advanced threats.
CO4	Implement and test authentication policies and access controls.
CO5	Secure computational environments and apply advanced security architectures.

LIST OF ACTIVITIES

S. No.	Title
1	Information Gathering using Google • Searching Techniques of Google Search Engine
2	Port Scanning and Information Gathering • Install Nmap on your system • Perform network scans to discover hosts and services, using different scan types (e.g., TCP SYN scan, UDP scan)
3	Packet Capturing and Analyzing • Install Wireshark on your system • Use Wireshark to capture network traffic on a specific network interface • Analyze the captures packets to identify different protocols and data types
4	**Implement a Basic Key Logger:** • **Tool:** C Programming • **Practical:** Writing a basic key logger in C to understand how key logging works, and discussing ethical implications and detection methods.
5	**Buffer Overflow Exploit:** • **Tool:** C Programming • **Practical:** Writing a C program with a buffer overflow vulnerability, exploiting the vulnerability, and discussing mitigation strategies
6	Detecting and mitigating phishing attacks: • **Tool:** Gophish • **Practical:** Setting up a phishing simulation, analyzing phishing emails, and learning

	mitigation techniques
7	Using Intrusion Detection Systems (IDS): • **Tool:** Snort Practical: Setting up and configuring Snort as an IDS, creating rules, and analyzing alerts
8	Brute Force and Dictionary Attacks: • **Tool:** Hydra • **Practical:** Performing brute force and dictionary attacks on a test server to understand password vulnerabilities
9	• Setting up a Next-Generation Firewall
10	• Using Wireshark and Cookies Editor to open any social media page • Use defensive approach to detect and prevent from the Cookies grabbing attack

***Note: Value Added Course (VAC**): The students must complete the Certification for Palo Alto Networks Certified Network Security Administrator.

The PCNSA certification validates the knowledge and skills required for network security administrators responsible for operating and managing Palo Alto Networks Next-Generation Firewall. PCNSA – certified individuals have demonstrated knowledge of the Palo Alto Networks firewall feature set.

LAB REPORT INSTRUCTIONS

- Provide specific title of the lab experiment.
- Theory: Provide a concise abstract (typically 100-200 words) that summarizes the purpose, methods, key findings, and significance of the experiment.
- Materials/ Equipment: List all materials, components, and equipment used in the experiment. Include specifications when applicable.
- Software/Simulation Tools:
- Experimental Procedure: Describe the step-by-step procedure for conducting the experiment. Be detailed and clear in your instructions. Include diagrams or schematics to illustrate the setup, connections, and component placement. Explain any variations or adjustments made to the standard procedure.
- Observation & Calculations/Analysis: Detail the data you collected during the experiment. Include descriptions of measurements and any calculations made. Use tables, charts, or graphs to present data clearly. Discuss any trends, patterns, or significant observations. Interpret the data in the context of the experiment's objectives. Ensure that all figures, tables, and equations are correctly labeled.
- Results: Summarize the key findings of the experiment. Present results in a clear and organized manner using tables and graphs. Include units of measurement and labels for data points.
- Conclusion: Provide a concise summary of the experiment's key points and outcomes.

GRADING AND ASSESSMENT

- **Continuous Evaluation**: 30 marks
- **Final Demo & Viva**: 10 marks
- **Attendance**: 10 marks
- **Lab Overall Marks**: 50 marks

COURSE POLICIES

- **Attendance**: Minimum 75% attendance is mandatory to appear in the final examination of the course.
- **Late Submissions**: Manuals and projects must be submitted by the specified timelines.

FACULTY INFORMATION

- **Office Hours**
  Monday (02:35 PM - 04:20 PM)
  Saturday (Full Day)

- **Contact Information**
  arsalan.cse@mietjammu.in | +91-7006416585

RUBRICS FOR LAB CONTINUOUS EVALUATION

Parameters	Performance			
	Low	**Medium**	**High**	**Marks**
Execution of the Experiment	Student was not able to setup and conduct the Experiment completely	Student was able to setup and conduct the experiment but measurement / results / observations were not correct	Students was able to set and conduct the experiment and the measurement / results / observations were correct	10
	0-2 Marks	3-6 Marks	7-10 Marks	
Record	Student was not able to describe the detailed procedure and could not record the measurement.	Student was able to describe the detailed procedure partially or with some inaccuracy.	Student was able to describe the detailed procedure accurately and record all measurements correctly.	10
	0-2 Marks	3-6 Marks	7-10 Marks	
Viva Voice	Students could not demonstrate sufficient knowledge of foundation, functional or applied aspects related to the experiment during viva.	Students demonstrated sufficient knowledge of foundation, functional or applied aspects related to the experiment during viva.	Students demonstrate strong knowledge of foundation, functional or applied aspects related to the experiment during viva	10
	0-2 Marks	**3-6 Marks**	**7-10 Marks**	
Total Marks				**30**