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 for Cyber Security Foundation Lab

S. No.	Activity 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 captured packets to identify different protocols and data types.
4	Implementing 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	● Set 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.