Course Code	Course Name	Course Type	Cd	L	T	P	Marks		
							Sessional	Final Exam	Total
COM-412	Network Security Foundation Lab	PCC	2	0	0	4	50	-	50

Course Outcomes:

After completion of this course the student will be able to	
CO1	Identify and describe common enterprise network devices and protocols.
CO2	Configure IP addresses, subnetting, and DHCP on firewalls.
CO3	Analyze and capture network traffic using Wireshark.
CO4	Implement and understand encryption algorithms, key management, and PKI.
CO5	Configure and deploy NGFW features for a zero-trust environment.

List of Activities for Network Security Foundation Lab (CISCO Packet Tracer and NS2)

S. No.	Activities
1	Basic Network Configuration ● Learn to configure basic network settings on Cisco devices.
2	Configuring VLANs ● Implement VLANs to segment network traffic.
3	Inter-VLAN Routing ● Enable communication between VLANs using a router or Layer 3 switch.
4	Configuring Access Control Lists (ACLs) ● Use ACLs to control network traffic and restrict access.
5	Setting Up a DHCP Server. ● Configure a DHCP server to dynamically assign IP addresses to network devices.
6	Implementing Network Address Translation (NAT). ● Configure NAT to allow internal devices to access external networks.
7	Installation of NS2. ● Create a basic network with two nodes and simulate data transfer between them.
8	● Set up and simulate a basic network topology to understand the fundamental components of NS2.
9	● Simulate common network attacks like DoS (Denial of Service) in NS2.
10	● Simulate and analyze the performance of network security protocols, such as IPsec.
11	● Simulate and evaluate the effectiveness of an IDS in detecting network intrusions.
12	● Configure and evaluate network security with multiple security zones.

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

The PCNSE certification covers how to design, deploy, operate, manage, and troubleshoot Palo Alto Networks Next-Generation Firewalls.

Certification Objectives

Palo Alto Networks technology is highly integrated and automated. The Palo Alto Networks product portfolio comprises multiple separate technologies working in unison to prevent successful cyber-attacks. The Palo Alto Networks Certified Network Security Engineer (PCNSE) demonstrates that engineers can correctly deploy and configure Palo Alto Networks Next-Generation Firewalls while leveraging the rest of the platform.