SYLLABUS

CYBER SECURITY · COURSE HANDOUT 2026

NETWORK SECURITY

FIREWALLS . VPN . SEGMENTATION . IDS . IPS . MONITORING . CLOUDENING . ZERO TRUST . RES

DURATION	LEVEL	MODULES	MODE
50 Hours	**Intermediate**	**8**	**Classroom · Online · Hybrid**

01 COURSE OVERVIEW

A defensive networking course on designing, hardening and monitoring a secure network. The course covers protocol-level weaknesses and the controls that answer them: segmentation, firewall policy, VPN design, intrusion detection, logging and access control, with configuration practice on pfSense and open-source tooling.

Learners design and defend a segmented network for a sample organisation.

WHO IT IS FOR

- Network and system administrators
- Security operations staff
- IT support engineers moving into security
- Infrastructure teams

PREREQUISITES

TCP/IP networking fundamentals and basic Linux.

02 LEARNING OUTCOMES

01 Explain protocol weaknesses at each network layer.

02 Design segmented networks with defined trust zones.

03 Write and audit firewall rule sets.

04 Deploy site-to-site and remote-access VPNs.

05 Detect intrusions with Snort or Suricata.

06 Harden switches, routers and endpoints.

07 Respond to and document a network incident.

03 MODULE STRUCTURE

8 MODULES

01 NETWORK THREAT MODEL

- OSI and TCP/IP review
- Threat actors
- Zero trust principles
- Common attacks per layer
- Defence in depth

02 SEGMENTATION AND DESIGN

- VLANs
- DMZ design
- East-west traffic
- Subnetting for security
- Micro-segmentation

03 FIREWALLS

- Stateful inspection
- NAT
- Policy review
- Rule design
- Application layer filtering
- Change control

LAB

PFSENSE POLICY BUILD

04 VPN AND ENCRYPTION

- IPSec
- WireGuard
- Key management
- SSL/TLS
- Certificate basics
- Remote access design

LAB

SITE-TO-SITE TUNNEL

05 INTRUSION DETECTION

- Signature vs anomaly
- Rule writing
- Network taps
- Snort and Suricata
- Tuning false positives

LAB

IDS DEPLOYMENT

06 MONITORING AND LOGGING

Flow data	Syslog
SIEM basics	Alert design
Retention	Baselines

TOOLS

WIRESHARK · ELK STACK

07 DEVICE HARDENING

Secure configuration	Management planes
Port security	802.1X
Patch discipline	Backups

08 INCIDENT RESPONSE

Detection to containment	Evidence capture
Eradication	Recovery
Post-incident review	

PROJECT

SECURE NETWORK DESIGN AND DEFENCE REPORT

04 ASSESSMENT & CERTIFICATION

Module assignments and labs	**25%**
Mini projects	**20%**
Internal assessments	**15%**
Final project and review	**40%**

CERTIFICATION

Learners who complete all modules, submit the final project and clear the review receive a course completion certificate from Kaizen Infinities Private Limited. Project work is documented for the learner's portfolio, and interview preparation is included in the closing sessions.

05 CAREER OUTCOMES

ROLES THIS PROGRAMME PREPARES FOR

NETWORK SECURITY ENGINEER · SECURITY ADMINISTRATOR · SOC ANALYST · INFRASTRUCTURE ENGINEER · FIREWALL ADMINISTRATOR

CALL US
+91 73051 33996

EMAIL US
apply@kaizeninfinities.com

VISIT OUR WEBSITE
www.kaizeninfinities.com