TechLabs

CYBER SECURITY

Program

Month 1: Cybersecurity Foundations

Week 1 – Introduction to Cybersecurity

- Cybersecurity Overview
- CIA Triad
- Threats, Risks & Vulnerabilities
- Common Cyber Attacks
- Cybersecurity Career Paths

Hands-On Lab

- VirtualBox Installation
- Kali Linux Setup
- Windows Lab Setup

Week 2 - Linux Fundamentals

- Linux Architecture
- File System Basics
- Users & Groups
- Permissions
- Essential Linux Commands

Hands-On Lab

- User Management
- File Operations
- SSH Configuration
- Basic Linux Administration

Week 3 – Networking Fundamentals

- OSI Model
- TCP/IP
- IP Addressing
- DNS
- DHCP
- HTTP & HTTPS
- Common Ports & Protocols

Hands-On Lab

- Network Traffic Analysis using Wireshark

Week 4 - Windows Security Fundamentals

- Windows Architecture
- User Accounts & Permissions
- Event Viewer
- Services & Processes
- Windows Security Features

Hands-On Lab

- Windows Log Analysis
- Event Investigation

Month 2: SOC Operations & Security Monitoring

Week 5 – Security Operations Center (SOC) Fundamentals

- What is a SOC?
- Roles and Responsibilities of a SOC Analyst
- IP Addressing
- Security Events vs Incidents
- Alert Lifecycle
- Incident Severity Classification

Week 6 – SIEM Fundamentals

- Introduction to SIEM
- Log Collection & Management
- Event Correlation
- Security Dashboards
- Common Detection Use Cases

Hands-On Lab

- Introduction to Splunk
- Basic Security Monitoring

Week 7 – Log Analysis & Investigation

- Windows Event Logs
- Linux Logs
- Authentication Events
- Failed Login Analysis
- Security Event Investigation

Hands-On Lab

- Log Investigation Exercises
- Alert Analysis Scenarios

Hands-On Lab

- Splunk Searches
- Dashboard Creation

Week 8 – Threat Intelligence & Incident Response

- Threat Intelligence Fundamentals
- Indicators of Compromise (IOCs)
- Introduction to MITRE ATT&CK
- Incident Response Lifecycle

Hands-On Lab

- IOC Investigation
- Incident Triage Exercises

Month 3: Basic Penetration Testing & Web Security

Week 9 – Reconnaissance & OSINT

- Information Gathering
- Footprinting
- Open-Source Intelligence (OSINT)
- WHOIS & DNS Enumeration

Hands-On Lab

- OSINT Investigation Exercises

Week 10 - Scanning & Enumeration

- Port Scanning
- Service Discovery
- Enumeration Techniques
- Banner Grabbing

Hands-On Lab

- Nmap
- Netcat
- Network Enumeration

Week 11 – Web Security Fundamentals

- How Web Applications Work
- HTTP Requests & Responses
- Cookies & Sessions
- Authentication & Authorization Basics

Hands-On Lab

- OWASP Juice Shop

Week 12 - OWASP Top 10 Overview

- SQL Injection
- Cross-Site Scripting (XSS)
- Broken Authentication
- Security Misconfigurations
- Access Control Issues

Hands-On Lab

- DVWA
- Burp Suite Community Edition

Month 4: Security Investigation & Career Readiness

Week 13 – Security Investigations

- Alert Analysis
- Log Correlation
- Investigation Workflow
- Security Case Studies

Hands-On Lab

- Real-World Security Investigation Scenarios

Week 14 - Threat Detection Fundamentals

- Detecting Suspicious Activity
- Brute Force Attack Indicators
- Phishing Indicators
- Malware Indicators

Hands-On Lab

- Detection Scenarios Using Security Logs

Week 15 – SOC Analyst Simulation

- Alert Triage
- Escalation Process
- Incident Documentation
- Reporting Best Practices

Hands-On Lab

- SOC Simulation Exercises
- Security Incident Handling

Week 16 - Career Preparation & Final Project

- Resume Building
- LinkedIn Profile Optimization
- Job Search Strategy
- Interview Preparation
- Mock Interviews

Hands-On Lab

- Final Project Presentation
- Technical Viva

Practical Assignments

Students will complete the following hands -on assignments throughout the program:

1. Linux Administration & User Management
2. Wireshark Network Traffic Analysis Report
3. Windows Log Investigation Assignment
4. Splunk Log Analysis Challenge
5. Threat Intelligence & IOC Investigation
6. Nmap-Based Network Assessment
7. OWASP Juice Shop Security Assessment
8. SOC Incident Investigation Report

Capstone Project

SOC Monitoring & Incident Investigation Lab
Students will build a small cybersecurity monitoring environment and perform a complete security investigation.

Project Components

- Windows Virtual Machine
- Kali Linux Virtual Machine
- Security Event Generation
- Log Collection & Analysis
- Alert Investigation
- Incident Documentation

Deliverables

- Lab Architecture Diagram
- Investigation Report
- Security Findings
- Incident Timeline
- Final Presentation

Tools & Technologies Covered Students will gain hands-on experience with:

- VirtualBox
- Kali Linux
- Wireshark
- Nmap
- TryHackme
- Splunk
- Burp Suite Community Edition
- OWASP Juice Shop
- DVWA
- Netcat

Expected Learning Outcomes
Upon successful completion of the program, students will be able to:

- Understand core cybersecurity concepts and security operations.
- Work effectively with Linux and Windows operating systems.
- Analyze network traffic using Wireshark.
- Investigate security events and alerts using SIEM tools.
- Perform basic incident response and alert triage activities.
- Conduct reconnaissance, scanning, and enumeration exercises.
- Identify common web application vulnerabilities.
- Create professional security investigation reports.
- Build and present a practical cybersecurity project.
- Demonstrate the foundational skills required for entry-level SOC and cybersecurity roles.

VTechLabs

alok@webmyne.com

+91 94276 02525

702, Ivory Terrace , Opp. Circuit House
R.C. Dutt Road, Vadodara-07
Gujarat - India.