Cybersecurity Professional Program

Duration: 3 Months

Training Hours: 96 Hours (8 Hours/Week)

Prerequisites

- Basic Computer Knowledge
- Familiarity with Windows Operating System
- Basic Networking Concepts (Recommended)
- No Prior Cybersecurity Experience Required

MONTH 1 – Cybersecurity Foundations & Operating System Security

---

Week 1 – Cybersecurity Fundamentals (8 Hours)

Module 1: Cybersecurity Foundations

What You'll Learn

Build a strong foundation in cybersecurity by understanding security principles, cyber threats, attack methodologies, security controls, and the role of cybersecurity professionals.

Topics Covered

- Introduction to Cybersecurity
- Cybersecurity Domains
- Types of Cyber Attacks

- Threats vs Vulnerabilities vs Risks
- CIA Triad
- AAA (Authentication, Authorization & Accounting)
- Defense in Depth
- Security Controls
- Security Policies
- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001
- Cyber Kill Chain
- MITRE ATT&CK Framework
- Cybersecurity Lab Setup

Practical Labs

- Install VMware Workstation / VirtualBox
- Install Kali Linux
- Install Windows Virtual Machine
- Configure Virtual Network
- Install OWASP Juice Shop
- Explore Kali Linux Environment

Week 2 – Networking for Cybersecurity (8 Hours)

Module 2: Network Security Fundamentals

What You'll Learn

Understand how computer networks operate and learn how security professionals analyze, monitor, and secure enterprise network infrastructure.

Topics Covered

- OSI Model
- TCP/IP Model
- IPv4 Addressing
- Subnetting
- ARP
- DNS
- DHCP
- NAT

- Routing
- Switching
- VLAN
- HTTP & HTTPS
- FTP
- SSH
- SMTP
- POP3
- IMAP

Practical Labs

- Cisco Packet Tracer
- Wireshark Packet Capture
- TCP Three-Way Handshake Analysis
- DNS Traffic Analysis
- HTTP & HTTPS Traffic Analysis
- Nmap Host Discovery

Week 3 – Linux Security Essentials (8 Hours)

Module 3: Linux for Cybersecurity

What You'll Learn

Learn Linux administration, command-line operations, and security concepts essential for cybersecurity professionals.

Topics Covered

- Linux Architecture
- Linux File System
- File & Folder Permissions
- Users & Groups
- SSH
- Linux Services
- Networking Commands
- Cron Jobs
- Bash Scripting
- Linux Log Files
- Linux Hardening Techniques

Practical Labs

- User & Group Management
- Configure SSH
- Secure File Permissions
- Analyze Linux Logs
- Configure UFW Firewall
- Create Basic Bash Scripts

Week 4 – Windows Security Essentials (8 Hours)

Module 4: Windows Security

What You'll Learn

Understand Windows security architecture and implement essential security controls used in enterprise environments.

Topics Covered

- Windows Security Architecture
- User Accounts
- User Account Control (UAC)
- NTFS Permissions
- Windows Defender
- Windows Firewall
- Event Viewer
- Windows Logs
- Windows Services
- Task Scheduler
- Windows Registry
- Local Security Policies
- Introduction to PowerShell

Practical Labs

- Configure Windows Firewall
- Analyze Windows Event Logs
- Investigate Windows Services
- Secure User Accounts

- Registry Inspection
- PowerShell Basics

Skills Gained After Month 1

Students will be able to:

- Understand core cybersecurity concepts and frameworks.
- Analyze network traffic using Wireshark.
- Perform basic reconnaissance using Nmap.
- Secure Linux and Windows operating systems.
- Build and configure a cybersecurity virtual lab.

MONTH 2 – Ethical Hacking, Vulnerability Assessment & Web Application Security

---

Week 5 – Ethical Hacking Fundamentals (8 Hours)

Module 5: Ethical Hacking & Penetration Testing

What You'll Learn

Understand the complete penetration testing lifecycle, including reconnaissance, enumeration, vulnerability discovery, and reporting while following ethical hacking principles.

Topics Covered

- Ethical Hacking Fundamentals
- Reconnaissance
- Open Source Intelligence (OSINT)
- Scanning Techniques
- Enumeration
- Reporting
- Legal & Ethical Considerations

Practical Labs

- Google Dorking
- Whois Lookup
- DNS Enumeration
- Network Scanning using Nmap
- Gobuster
- Dirsearch

Week 6 – Vulnerability Assessment (8 Hours)

Module 6: Vulnerability Assessment & Management

What You'll Learn

Learn to identify, prioritize, and manage vulnerabilities using industry-standard assessment tools and reporting methodologies.

Topics Covered

- Common Vulnerabilities and Exposures (CVE)
- Common Vulnerability Scoring System (CVSS)
- Common Weakness Enumeration (CWE)
- Vulnerability Scanning
- Risk Assessment
- Patch Management
- Professional Reporting

Practical Labs

- Nessus Vulnerability Scanner
- OpenVAS
- Risk Assessment
- Vulnerability Assessment Report Preparation

Week 7 – Web Application Security (8 Hours)

Module 7: Web Application Security

What You'll Learn

Understand modern web application vulnerabilities based on the OWASP Top 10 and learn practical techniques for identifying and testing web security flaws.

Topics Covered

- HTTP & HTTPS
- Cookies
- Sessions
- Authentication
- Authorization
- SQL Injection (SQLi)
- Cross-Site Scripting (XSS)
- Cross-Site Request Forgery (CSRF)
- File Upload Vulnerabilities
- Security Misconfiguration

Practical Labs

- Burp Suite
- OWASP Juice Shop
- Damn Vulnerable Web Application (DVWA)
- PortSwigger Web Security Labs

Week 8 – API Security Fundamentals (8 Hours)

Module 8: API Security Testing

What You'll Learn

Understand REST API architecture, authentication mechanisms, and common API vulnerabilities based on the OWASP API Security Top 10.

Topics Covered

- REST APIs
- JSON
- JSON Web Token (JWT)
- OWASP API Security Top 10

- Broken Object Level Authorization (BOLA)
- Rate Limiting

Practical Labs

- API Testing using Postman
- API Testing using Burp Suite
- JWT Analysis

Skills Gained After Month 2

Students will be able to:

- Perform reconnaissance and information gathering.
- Conduct vulnerability assessments.
- Test web application security.
- Assess REST API security.
- Prepare professional penetration testing reports.

MONTH 3 – Security Operations, Incident Response & Digital Forensics

---

Week 9 – SOC Fundamentals (8 Hours)

Module 9: SOC Operations & Threat Monitoring

What You'll Learn

Learn how Security Operations Centers (SOC) monitor enterprise environments, detect threats, and investigate suspicious activities using SIEM platforms.

Topics Covered

- Security Operations Center (SOC)
- Security Information & Event Management (SIEM)

- Log Management
- Windows Logs
- Linux Logs
- Syslog
- Indicators of Compromise (IoCs)
- Threat Intelligence
- MITRE ATT&CK Framework

Practical Labs

- Install Wazuh SIEM
- Analyze Security Alerts
- Perform Threat Hunting

Week 10 – Incident Response & Digital Forensics (8 Hours)

Module 10: Incident Response & Digital Forensics

What You'll Learn

Learn how cybersecurity professionals investigate security incidents, preserve digital evidence, and perform forensic analysis.

Topics Covered

- Incident Response Lifecycle
- Malware Analysis
- Phishing Investigation
- Ransomware
- Chain of Custody
- Disk Forensics
- Memory Forensics
- Browser Forensics

Practical Labs

- Autopsy
- FTK Imager
- Volatility Framework
- Browser Forensics

Week 11 – Cloud Security Fundamentals (8 Hours)

Module 11: Cloud Security

What You'll Learn

Understand cloud security principles, identity management, and best practices for securing cloud infrastructure.

Topics Covered

- Shared Responsibility Model
- Identity & Access Management (IAM)
- Multi-Factor Authentication (MFA)
- Security Groups
- Cloud Storage Security
- Cloud Threats

Practical Labs

- Configure IAM
- Enable Multi-Factor Authentication
- Secure Cloud Virtual Machine

Week 12 – Enterprise Capstone Project & Career Readiness (8 Hours)

Module 12: Enterprise Security Assessment

What You'll Learn

Apply all cybersecurity concepts through a simulated enterprise security assessment while preparing for interviews and professional cybersecurity roles.

Capstone Project

Students will perform a complete enterprise security assessment including:

- Network Reconnaissance
- Vulnerability Assessment
- Web Application Security Testing
- API Security Testing
- Log Analysis
- Incident Investigation
- Security Hardening
- Risk Assessment

Practical Labs

- Enterprise Security Assessment
- Professional Security Assessment Report
- Resume Preparation
- Mock Technical Interview
- Capture The Flag (CTF) Challenge

Skills Gained After Month 3

Students will be able to:

- Monitor enterprise security events.
- Investigate cybersecurity incidents.
- Perform basic digital forensic investigations.
- Apply cloud security best practices.
- Conduct end-to-end enterprise security assessments.
- Prepare for entry-level cybersecurity roles and professional certifications.