SOC MANAGEMENT

Defend Your Organization Against Cyber Threats

Build an adaptive SIEM architecture solutions

NETWORK PENETRATION TEST

Defend Your Organization Against Cyber Threats

Validate the network like a real hacker

DDOS PROTECTION

Defend Your Organization Against Cyber Threats

Onboard applications under DDoS protections

APPLICATION PENETRATION TEST

Defend Your Organization Against Cyber Threats

Validate the network like a real hacker

Cyber Security & IT Risk Management

DEFEND YOUR ORGANIZATION AGAINST CYBER THREATS

Building Your IT Career

Penetration Testing and OC Engineering

This learning path will teach you to execute adversary attack emulations as a Penetration Tester and a SOC Team Engineer

Course Curriculum

Penetration Testing and SOC Engineering

Training Methodology

- Digital Point is a global classroom. All classes are featured online (No recorded version). Students around the world can join this online live class.
- Each class is instructor oriented live class and will be recorded, and students will get access to watch video for practice.
- Real-world scenario labs.
- Class Notes and Labs for each class

Contact Us

Phone: 1-703-652-9640 | 226-972-1877
Web: https://training.digitalpoint.tech
Email: admin@digitalpoint.tech

Cyber Security Market Scope:

Cybersecurity jobs are in high demand. According to the Bureau of Labor Statistics, the job outlook in information security is projected at 33% (2023-33), much faster than the average for all other occupations. The number of Cybersecurity jobs in 2023 was. 180,770. Obtaining work in this industry can mean a great income, job security, and advancement potential.

The Highest-Paid Cybersecurity Jobs:

- Application Security Engineer: Average salary range is between $100,000 and $210,000
- Cybersecurity Specialist/Analyst: The annual average is between $90,000 and $185,000.
- Penetration Tester: The Penetration Tester's average salary is between $80,000 and $130,000.
- Red Team Engineer: The Red Team Engineer role nets an average salary between $120,000 and $180,000.
- SOC Specialist: An average salary range for a SOC Specialist/Analyst is $120,000 to $220,000.

Penetration and SOC Engineer

Benefits of the Course:

- Better Job Opportunities: If you are looking for a new job completing this course, you can apply as a Cyber Security Specialist/Engineer/ IS Security Engineer/Security Analyst.

- Improved Skills & Knowledge: If you are already a QA/IT professional, completion of this course will improve your skills to latest technologies.

- Increased Salary: Cyber Security professionals are the highest paid IT industry.

Prerequisites:

- A bachelor's degree in any background
- You must have good presentation skills

Course Duration: (60 Hours)

Penetration and SOC Engineer

Training Methodology:

- Real-world scenario labs.
- Class Notes and Labs for each class
- Each class is instructor oriented live class and will be recorded, and students will get access to watch video for practice.

Why choose us?

- Digital Point is a global classroom. All classes are featured online (No recorded version). Students around the world can join this online live class.
- The course is very interactive and has lots of lab practice.
- We help you with Resume preparation, Interview preparation, and before and after job support
- Students can repeat the same program once with no extra cost.

https://training.digitalpoint.tech

Course Curriculum

https://training.digitalpoint.tech

Phase 1: Foundation Training

Module 1 Overview of Enterprise Applications and N-Tier Infrastructure
Module 2 Operating System – Windows Server and Unix/Linux
Module 3 Networking Fundamentals, Active Directory and DNS
Module 4 Power Shell Scripting, Batch and Shell Scripting
Module 5 Incident, Problem and Change Management Process

Module 6 Infrastructure Lab setup

- Lab setup on Laptop/desktop
  - Installation of Virtual Machine
  - Build Active Directory and Kali Linux
- Lab setup on AWS
- Lab setup on Azure

Module 7 Cybersecurity Framework and Standards

- NIST Cybersecurity Framework (CSF)
- ISO/IEC 27001
- CIS Critical Security Controls (CIS Controls)
- COBIT (Control Objectives for Information and Related Technologies)
- PCI-DSS (Payment Card Industry Data Security Standard)
- HIPAA (Health Insurance Portability and Accountability Act)
- MITRE ATT&CK Framework

Phase 2: Network Penetration Testing

Module 8: Discovery and Reconnaissance

- Passive Reconnaissance
- Active Reconnaissance
- Vulnerability Scanning - Nmap, Metasploit, Wireshark, Burp Suite, recon-ng, shodan, maltego

Module 9: Active Directory

- Set up Active Directory lab environment
- Information gathering using PowerShell
- Active Directory Enumeration
- Active Directory Authentication - NTLM Authentication, Kerberos Authentication
- Cached Credential Storage and Retrieval
- Service Account Attacks
- Active Directory Lateral Movement
- Kerberoasting

Module 10: Network and Infrastructure Penetration Test

- Properly plan and prepare for an enterprise penetration test
- Scan in-scope environments using best-of-breed tools to identify systems and targets
- Understand the environment via efficient methods of gaining situation awareness to identify additional targets and attack paths
- Use privilege escalation techniques to elevate access on Windows or Linux systems
- Crack passwords using modern tools and techniques to extend or escalate access
- Use Command and Control (C2, C&C) frameworks to manage compromised hosts remotely
- Develop and deliver high-quality reports that communicate the accurate business risk stemming from the discovered flaws and misconfiguration

Phase 2: Network Penetration Testing

Module 11: Network Exploits

- FTP Exploits
- SMB Exploits
- Man-in-the-middle exploits
- Password cracking
- Code Vulnerabilities
- Local Host Vulnerabilities
- Privileged Escalation (Unix)
- privileged Escalation (Windows)

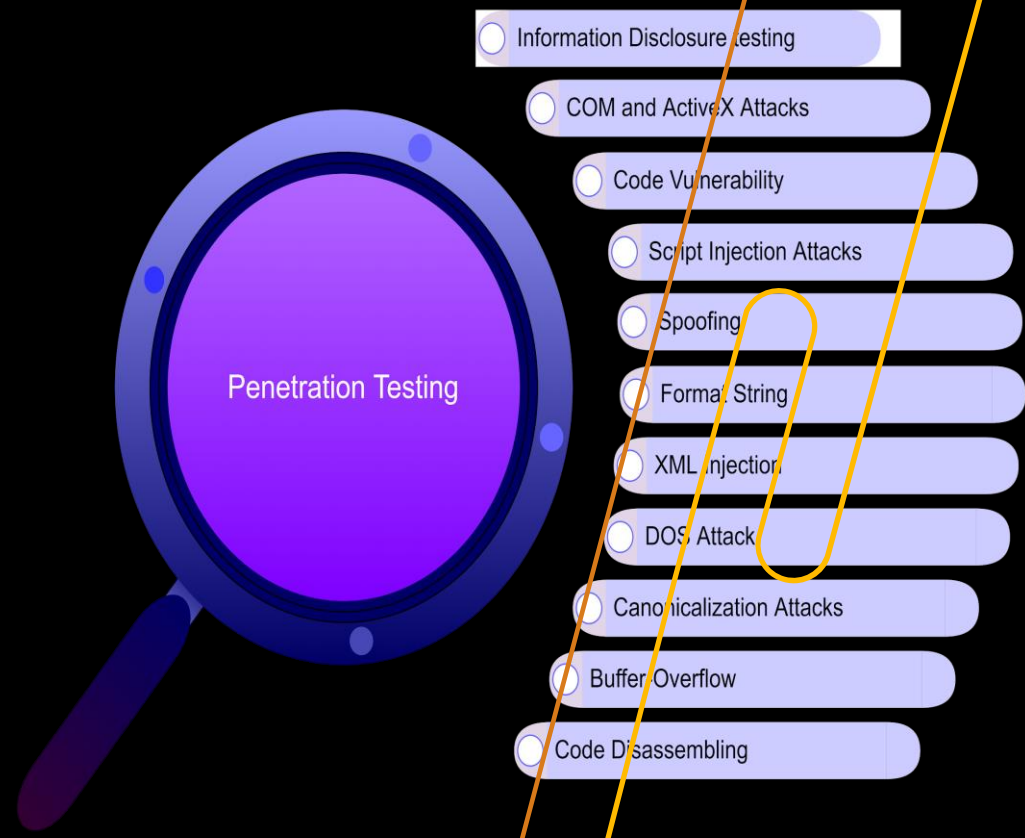
Module 12: Top Network Penetration Test Exploits

- NetBIOS Name Service (NBNS) Spoofing
- Link-Local Multicast Name Resolution (LLMNR) Spoofing
- IPV6 DNS Spoofing
- Accounts are vulnerable to Kerberos attacks
- IPMI Authentication Bypass
- Multicast DNS (mDNS) Spoofing
- Microsoft Windows RCE (EternalBlue and BlueKeep)
- SSL/TLS Configuration and Certificate Weakness
- Administrative/Unnecessary Services Exposed
- Insufficient Brute Force Protection
- Insecure Protocols on IoT devices
- Week password policy
- End of life (EOD) servers and applications
- Default password on network devices
- Cloud Storage Accounts

Phase 3: Application Penetration Testing

Module 13: Application Penetration Test

- Secure SLDC and DevSecOps
  - Threat Modelling
  - SAST
  - DAST
  - SCA
- OWASP top 10
- Burp Suite installation and configuration
- Cross-Site Scripting (XSS) – stored and reflected
- Cross-Site Request Forgery (CSRF)
- CORS misconfiguration
- Insecure Direct Object References (IDOR)
- File upload vulnerabilities
- Open Redirect
- JWT vulnerabilities
- JSON Web Tokens (JWT)
- Components with known vulnerabilities
- Insecure storage of session tokens
- SQL injection (SQLi)



Phase 4: Red Teaming

Module 14: Red Teaming

- SMB Relay Attacks
- Discovering Hosts with SMB Signing
- SMB Relay Attack Demonstration
- SMB Relay Attack Defenses
- Gaining Shell Access
- Post-Compromise Enumeration
  - Advanced Web Attacks
  - Domain Enumeration with Powerview
  - Bloodhound Overview and Setup
  - Grabbing Data with Invoke-Bloodhound
  - Enumerating Domain Data with Bloodhound
  - Windows Privilege Escalation
  - Windows Local Persistence
  - Lateral Movement and Pivoting
  - Data Exfiltration
  - MITRE ATT&CK Red Teaming
  - AWS Pen testing
  - Azure Pen testing
  - Advanced Web Attacks

Phase 5: SOC Engineering

Module 15: Introduction to Cyber Security and SOC Operations

- Understanding the Role of a SOC Analyst and Responsibilities
- Overview of SOC structure and operations
- Incident Response Process and Lifecycle

Module 16: Threat Intelligence and Research

- Cyber Threat Landscape
- Cyber Kill Chain and MITRE Framework
- Threat Actors and Their Motives
- Open-source intelligence (OSINT)
- Threat Feeds and Indicators of Compromise (IOC)

Module 17: Security Information and Event Management (SIEM)

- SIEM architecture and components
- Log collection and correlation
- Rule creation and customization
- Incident Investigation using different SIEM Tools
- Reporting, alerting, and root cause analysis

Module 18: Practical Labs and Hands-on Experience

- Real-world scenarios and simulations
- Hands-on Experience with Security Tools and Technologies
- Creating and Analyzing Incident Cases
- Building and configuring security systems

Phase 6: Reporting and Remediation

Module 19: Penetration Test Reports

- Network Penetration Test Report
- Application Penetration Test Report

Module 20: Remediation of Penetration Test Findings

- Design a remediation strategy
- Remediation exception and exemption process

Phase 7: Cybersecurity and Risk Management

Module 21: Network and Communication Security

- Assess and implement secure design principles in network architectures
- Secure network components
- Wireless Network Security
- Remote Access Network Security

Module 22: Identity and Access Management

- Control physical and logical access to assets
- Manage identification and authentication of people, devices, and services
- Federated identity with a third-party service

Module 23: Encryption and Cryptography Management

- Principles of encryption
- Data encryption at rest and in transit conditions

Phase 8: Real-World project

Module 24: Boot Camp

- Boot Camp with real-world project - Each student will be required to complete a real-time project lab that covers the entire course curriculum.

Phase 9: Real-World project

Module 25: Real-world Job Interview Preparation

- Professional real-world Resume Writing
- Interview Preparation
- Mock Interview

Thank you

Phone: 1-703-652-9640 | 226-972-1877

Web: https://training.digitalpoint.tech

Email: admin@digitalpoint.tech