Cyber Security - Penetration Testing and Ethical Hacking

Training Methodology

- Digital Point is a global classroom. All classes are featured online (No recorded version).
- Students around the world can join online live classes.
- Each live class will be recorded, and students can watch videos for practice.
- Real-world scenario labs
- VPN access to digital Point's Lab that is accessible from anywhere 24/7
- Class Notes and Labs for each class

Contact Us

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

Web: http://training.digitalpoint.tech **Email:** admin@digitalpoint.tech

About This Course

News of large-scale cybersecurity threats and cyberattacks dominate the headlines all too often in today's Information Age: hackers exploiting vulnerabilities of a retail giant, foreign influence in elections, and new forms of ransomware underscore the importance of preparing for these types of emerging threats. As businesses, governments, financial institutions, and public sector organizations collect, store, and process vast amounts of sensitive and valuable data, those organizations become targets of groups seeking to wreak havoc on vulnerable systems and potentially disrupt everyday business functions. As a result, penetration tests and ethical hacking have become a fundamental component of business operations. Most businesses must conduct network and application penetration tests to identify the security gaps in the network infrastructure and remediate the applications to ensure the protection of data and networks.

Digital Point Technologies offers an online course on Penetration **Testing and Ethical Hacking Training** that equips students with a comprehensive understanding of conducting a successful penetration test. The course will help students assess and mitigate specific vulnerabilities within an organization's networks, systems, and data to provide the knowledge and skills to protect the integrity, security, and confidentiality of their digital assets.

Penetration Tester Market Scope

Cybersecurity jobs are in high demand. According to the US Bureau of Labor Statistics, the rate of growth for jobs in information security is projected at 37% from 2012–2022 that's much faster than the average for all other occupations. Obtaining work in this industry can mean a great income, job security, and advancement potential. There are many business opportunities, including company management positions, available for professional hackers in today's workforce.

The Highest-Paid Cybersecurity Jobs

- **Penetration Tester:** This role nets an average salary between $80,000 and $130,000
- **IS Security Engineer:** This role nets an average salary range of $90,000 to $150,000

Prerequisites:

- A bachelor's degree in any background (You don't need any IT background)
- You must have good presentation skills.

Why choose us?

- Real-world industry experienced instructor
- We help you with Resume preparation, Interview preparation, before and after job support
- Student can repeat the same program two times with no extra cost.

Benefit of the course

- Completion of this course, you can apply as a Penetration Test Engineer/ Red Team Tester
- Job Support – We will provide you with job support
- Interview Preparation
- Mock Interview
- Helping to write professional resume writing

Course Duration (40 Hours)

Class: Twice a week (3 hours each class)

Course Curriculum

Course Curriculum

Module 1 Overview of Enterprise Applications and N-Tier Infrastructure

Module 2 Operating System –Windows Server 2012/2016, UNIX

Module 3 Networking, Active Directory and DNS

Module 4 Power Shell Scripting, Batch Scripting

Module 5 Incident, Problem and Change Management Process

Module 6 Infrastructure setup

- Installation of Virtual Machine on Physical Server
- Installation of Virtual Machine on Cloud
- Configure VPN
- Connect Remote Windows Servers
- Connect Remote Unix Server

Module 7

- **Identifying Security Fundamentals**
  - Identify Information Security Concepts
  - Identify Security Controls
  - Identify Authentication and Authorization Concepts
  - Identify Cryptography Concepts

Module 8

- **Analyzing Risk**
  - Analyze Organizational Risk
  - Analyze the Business Impact of Risk

Module 9

- **Identifying Security Threats**
  - Identify Social Engineering Attacks
  - Identify Malware
  - Identify Software-Based Threats
  - Identify Network-Based Threats
  - Identify Wireless Threats
  - Identify Physical Threats

Module 10

- **Conducting Security Assessments**
  - Identify Vulnerabilities
  - Assess Vulnerabilities
  - Plan for remediation of findings

Module 11

- **IDS, Firewalls, and Honeypots**
  - IDS
  - Firewalls
  - Honeypots
  - Configuring IDS and Honeypots

Module 12

- **Cryptography**
  - Algorithm Cryptography
  - Algorithm and Hash Cryptography
  - Cryptography Tools
  - PKI, Disk Encryption, Email Encryption
  - Cryptography Lab

Module 13

- Vulnerability Scanning
  - Vulnerability Scanning Overview and Considerations 206
  - How Vulnerability Scanners Work
  - Manual vs. Automated Scanning
  - Internet scanning vs Internal Scanning
  - Authenticated vs Unauthenticated Scanning
  - Vulnerability Scanning with Nessus
  - Authenticated Scanning With Nessus
  - Vulnerability Scanning with Nmap

Module 14

- Web Application Attacks
  - Web Application Assessment Methodology
  - Web Application Enumeration
  - Inspecting URLs
  - Inspecting Page Content
  - Viewing Response Headers
  - Inspecting Sitemaps
  - Locating Administration Consoles
  - Web Application Assessment Tools

- DIRB
- Burp Suite
- Nikto
- Exploiting Web-based Vulnerabilities
- Exploiting Admin Consoles
- Cross-Site Scripting (XSS)
- Directory Traversal Vulnerabilities
- File Inclusion Vulnerabilities
- SQL Injection

Module 15

- Password Attacks
  - Wordlists
  - Standard Wordlists
  - Brute Force Wordlists
  - Common Network Service Attack Methods
  - HTTP htaccess Attack with Medusa
  - Remote Desktop Protocol Attack with Crowbar
  - SSH Attack with THC-Hydra
  - HTTP POST Attack with THC-Hydra
  - Leveraging Password Hashes
  - Retrieving Password Hashes
  - Passing the Hash in Windows
  - Password Cracking

Module 16

- Active Directory Attacks
  - Active Directory Theory
  - Active Directory Enumeration
  - Active Directory Authentication
  - NTLM Authentication
  - Kerberos Authentication
  - Cached Credential Storage and Retrieval
  - Service Account Attacks
  - Low and Slow Password Guessing
  - Active Directory Lateral Movement
  - Pass the Hash
  - Overpass the Hash
  - Pass the Ticket
  - Distributed Component Object Model
  - Active Directory Persistence
  - Golden Tickets
  - Domain Controller Synchronization

Module 17

- **Network Penetration Test**
  - Plan for Network Penetration Testing
  - External Network Penetration Testing
  - Internal Network Penetration Testing
  - Wireless Network Penetration Testing
  - Foot printing
  - Scanning and Enumeration

- System Hacking
- Malware
- Sniffing
- Social Engineering
- Denial of Service
- Session Hijacking

Module 18

- **Application Penetration Test**
  - Plan for application Penetration Testing
  - External Application Penetration Testing
  - Internal Application Penetration Testing
  - Web Servers and Apps
  - SQL Injection
  - OWASP top 10

Module 19

- **Network exploitation**
  - FTP Exploits
  - Man-in-the middle exploits
  - Wireless Exploits
  - Application Exploits
  - SQL Injection
  - Code Vulnerabilities
  - Local Host Vulnerabilities
  - Privileged Escalation (Unix)
  - privileged Escalation (Windows)

Module 20

- **Penetration Tet Reports**
  - Network Penetration Test Report
  - Application Penetration Test Report

Module 21

- **Remediation**
  - Design remediation strategy

Module 22

- **Boot Camp – PenTest+**
  - Preparation for CompTIA **PenTest+** exam

Module 23 Job Support

- Resume Writing
- Project Analysis
- Interview Preparation
- Mock Interview
- Job Support

CompTIA Certified professional exam

Exam#	Exam Name	Exam Duration	Passing Score
PT0-001	CompTIA PenTest+	90 Min	750 (out of 900)