digital Point IT Consulting Training IT Infrastructure Support Cloud Migration

http://training.digitalpoint.tech

CompTIA PenTest+ Certification

Course Overview:

The CompTIA PenTest+ (PT0-001) certification verifies that successful candidates have the knowledge and skills required to plan and scope an assessment, understand legal and compliance requirements, perform vulnerability scanning and penetration testing, analyze data, and effectively report and communicate results.

CompTIA PenTest+ is for cybersecurity professionals tasked with penetration testing and vulnerability management.

PenTest+ certification is globally recognized and industry supported.

About PenTest+ exam:

►CompTIA PenTest+ assesses the most up-to-date penetration testing, and vulnerability assessment and management skills necessary to determine the resiliency of the network against attacks.

►Successful candidates will have the intermediate skills required to customize assessment frameworks to effectively collaborate on and report findings.

►Candidates will also have the best practices to communicate recommended strategies to improve the overall state of IT security.

CompTIA PenTest+ meets the ISO 17024 standard. Regulators and government rely on ANSI accreditation because it provides confidence and trust in the outputs of an accredited program. Over 1.3 million CompTIA ISO/ANSI-accredited exams have been delivered since January 1, 2011.

The CompTIA Pentest+ (PT0-001) exam covers FIVE domains:

1. 15%: Planning and Scoping
2. 22%: Information Gathering and Vulnerability Identification
3. 30%: Attacks and Exploits
4. 17%: Penetration Testing Tools
5. 16%: Reporting and Communication

According to the Bureau of Labor Statistics of USA, Security Specialists, Administrators and Managers earn over $86,000 per year.

Who should attend?

► Anyone who wants to start Information Technology as a career
► Anyone who wants to upgrade the IT Skills
► Network Administrator
► Datacenter Architect
► IT Security Officer

Jobs that use CompTIA PenTest+

►Penetration Tester
►Vulnerability Tester
►Security Analyst (II)
►Vulnerability Assessment Analyst
►Network Security Operations
►Application Security Vulnerability

Course Duration: 80 Hours (10 Weeks)
Class: Mon and Wed (7:00 P.M -11:00 P.M EST)
Delivery Format: Virtual Classroom (Online live class)
Course Fee: **$1000**

What is next after PenTest+?

Your next level is to earn CSA+ CompTIA Cybersecurity Analyst (CSA+) or CompTIA Advanced Security Practitioner (CASP) or CISSP certification.

Course Description:

► Domain 1 - Planning and Scoping

- Planning and Scoping (Overview)
- Penetration Testing Methodology
- Planning a Penetration Test
- Rules of Engagement
- Legal Concepts
- Testing Strategies
- White Box Support Resources
- Types of Assessments
- Threat Actors
- Target Selection

► Domain 2 - Information Gathering and Vulnerability Identification

- Information Gathering and Vulnerability Identification
- Information Gathering
- Scanning and Enumeration
- Fingerprinting
- Scanning and Enumeration
- Cryptographic Inspection
- Eavesdropping
- Decompiling and Debugging
- Open Source Research
- Vulnerability Scanning

- Scanning Considerations
- Application and Container Scans
- Analyzing Vulnerability Scans
- Leverage Information for Exploit
- Common Attack Vectors
- Weaknesses in Specialized Systems

► Domain 3 - Attacks and Exploits

- Attacks and Exploits (Overview)
- Social Engineering
- Motivation Factors
- Physical Security Attacks
- Lock Picking (Demo)
- Network-based Vulnerabilities
- Wireless-based Vulnerabilities
- Wireless Network Attack
- Application-based Vulnerabilities
- Local Host Vulnerabilities
- Privilege Escalation (Linux)
- Privilege Escalation (Windows)
- Privilege Escalation
- Privilege Escalation
- Lateral Movement
- Persistence
- Covering Your Tracks
- Persistence and Covering Tracks

► Domain 4 - Penetration Testing Tools

- Penetration Testing Tools (Overview)
- Nmap Usage
- Use Cases for Tools
- Scanners

- Credential Testing Tools
- Password Cracking
- Debuggers
- Software Assurance
- OSINT
- Wireless
- Web Proxies
- Social Engineering Tools
- Remote Access Tools
- Networking Tools
- Mobile Tools
- Miscellaneous Tools
- Intro to Programming
- Programming Concepts
- BASH Script Example
- Python Script Example
- PowerShell Script Example
- Ruby Script Example

► Domain 5 - Reporting and Communication

- Reporting and Communication (Overview)
- Pentest Communications
- Report Writing
- Mitigation Strategies
- Post-Report Activities
- Pentest Report Example

CompTIA Certified PenTest+ professional exam

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

digital Point IT Consulting Training IT Infrastructure Support Cloud Migration

http://training.digitalpoint.tech

Instructor Profile:

Instructor: Nizam Mahmood, MCSE | MCDBA | OCP | SCSA | Web Sphere Admin

► Over 22 years of experience in Information Technology, Mr. Nizam is providing technology leadership to the global IT organization in the strategy, architecture, design, deployment, management and execution of IT infrastructure services including: network infrastructure, cloud computing, data center operations, disaster recovery, security and vendor management.

► Mr. Nizam is a subject matter expert of architecting, designing, and leading the implementation efforts of (a) cloud migration; (b) data center consolidation; (c) network convergence; (d) middle ware optimization.

► Experienced in planning and designing High Availability (HA) and Disaster Recovery (DR) processes for databases across multiple data center.

► As an Security Architect, Mr. Nizam is responsible to providing leadership, oversight and guidance of Network and Infrastructure Security, Application Security, Security Architecture and Governance Management.

►Mr. Nizam is a SME of designing and implementing DDoS technology that protects corporate data center and customer face application from any type of DDoS attacks.

To download the complete course catalog, please visit:

http://training.digitalpoint.tech

Email: admin@digitalpoint.tech