**Corporate Training Solution:**

**CompTIA Pentest+ PT0-003 Course Content**

1. **Overview**

**Why Choose This Course?**

1. On-demand access: Learn at your own pace, anytime, anywhere.
2. Hands-on labs: Practice real-world penetration testing techniques.
3. Expert instruction: Learn from industry-leading cybersecurity professionals.
4. Career advancement: Boost your resume with a globally recognized certification.

Enroll Now and start your journey to becoming a certified penetration tester with the CompTIA Pentest+ Course (PTO-003). Don’t miss this opportunity to advance your cybersecurity career!

**Who Should Enroll?**

1. Aspiring **penetration testers** and **ethical hackers**.
2. IT professionals looking to specialize in **cybersecurity**.
3. Anyone preparing for the **CompTIA Pentest+ certification exam**.
4. **Durations: 5 days ( 6 modules - 90 lessons - 40 hours on-demand)**

* 6 Modules, 90 lessons, 4 downloadable resources
* Access on mobile, Desktop
* Full lifetime access
* Certificate of completion

1. **Audience**
2. You want to transition from IT Basic to Deployment standard requiment ISO 27001/27002.
3. You want to learn how to apply security and logic in IT infrastucture have standard COSO.
4. You want to reduce the stress of moving from traditional IT knowledge to internal IT auditing, need to survey, analyze to understand and manage operational monitoring and upgrade patching of business system software and learn an alternative way to clean up, transform and visualize the organization's software.
5. **Prerequisites**

You should have the following understanding or knowledge:

1. Understanding of concepts presented in the E-Learning LMS, self-learn and Self excutive Labs online.
2. Knowledge of basic Computing, Network, Storage, IT workflows and Security concepts.
3. Experience using CEH and or CompTIA Security (if you have).
4. **Objectives**
5. IT Executive or IT Admin.
6. Business Analytics & Bussiness Intelligent.
7. Line of Business for Internal Audit
8. KNIME for Excel User in Internal Audit.
9. This course by offering your educational services to help your accomplishing their goals and becoming the best in their profession or explore a new career path.
10. **Requirements**
11. I would encourage you to take my Awareness Cyber Security crashcourse for beginners first.
12. Laptop/Desktop with Wi-Fi/LAN can be access Internet for free.
13. Web browser to access Labs Online of Teacher ready (not can be download).
14. **Course outline**

**Module 1 - Engagement Management**

***1.1 Pre Engagement Activities***

***1.2 Collaboration and Communication Activities***

***1.3 Testing Frameworks and Methodologies***

*1.3.1 Examining MITRE ATT&CK*

***1.4 Engagement Management Review***

**Module 2 - Reconnaissance and Enumeration**

***2.1 Passive Reconnaissance***

*2.1.1 Google Hacking*

***2.2 Active Reconnaissance***

*2.2.1 Port Scanning and Fingerprinting*

*2.2.2 Tracing a Network Path with Traceroute*

*2.2.3 Intercepting Data with Wireshark*

*2.2.4 Web Scraping*

***2.3 Enumeration Techniques***

*2.3.1 Directory Enumeration*

*2.3.2 Email Enumeration*

***2.4 Reconnaissance and Enumeration Scripts***

*2.4.1 Using Scripts*

***2.5 Reconnaissance and Enumeration Tools***

*2.5.1 Perform OSINT with Recon ng*

*2.5.2 Adding an API Key to Recon ng*

*2.5.3 Discovering IoT with Shodan*

*2.5.4 Performing WHOIS Lookups*

*2.5.5 Performing DNS Lookups*

*2.5.6 Using NMAP Scripts*

*2.5.7 Performing OSINT with theHarvester*

***2.6 Reconnaissance and Enumeration Review***

**Module 3 - Vulnerability Discovery and Analysis**

***3.1 Vulnerability Discovery***

*3.1.1 Performing a Vulnerability Scan with OpenVAS*

*3.1.2 Performing Static Code Analysis*

***3.2 Reconnaissance, Scanning and Enumeration Output Analysis***

***3.3 Physical Security***

*3.3.1 Cloning an RFID Badge*

*3.3.2 Cloning NFC with Flipper Zero*

***3.4 Vulnerability Discover and Analysis Review***

**Module 4 - Attacks and Exploits**

***4.1 Prioritize and Prepare Attacks***

***4.2 Network Attacks***

*4.2.1 Performing an On Path Attack*

*4.2.2 Executing a Network Attack with Metasploit*

*4.2.3 Migrating Meterpreter to Another Process*

*4.2.4 Creating a Malware Dropper with Msfvenom*

*4.2.5 Using Netcat*

*4.2.6 Capturing Files with Wireshark*

***4.3 Authentication Attacks***

*4.3.1 Brute Forcing with Medusa*

*4.3.2 Pass the Hash*

*4.3.3 Password Spraying with Hydra*

*4.3.4 Pass the Token Attack*

*4.3.5 Spoofing Authentication with Responder*

*4.3.6 Cracking Linux Passwords with John the Ripper*

*4.3.7 Hashcat Password Cracking*

***4.4 Host Based Attacks***

*4.4.1 Privilege Escalation with Eternal Blue*

*4.4.2 Log Tampering*

*4.4.3 Pwn a Linux Target from Start to Finish*

***4.5 Web Application Attacks***

*4.5.1 Performing Directory Traversal*

*4.5.2 Grabbing Passwords with SQL Injection*

*4.5.3 SQLi on a Live Website Part 1*

*4.5.4 SQLi on a Live Website Part 2*

*4.5.5 Command Injection*

*4.5.6 Injecting an iFrame with Stored XSS*

*4.5.7 Busting the DOM*

*4.5.8 IDOR Abuse with Burp Suite*

*4.5.9 Web Session Hijacking*

*4.5.10 Parameter Tampering with Burp Suite*

***4.6 Cloud Based Attacks***

*4.6.1 Hacking S3 Buckets*

***4.7 Wireless Attacks***

*4.7.1 WiFi Pumpkin Evil Twin*

*4.7.2 WPA2 Crack Attack*

*4.8 Social Engineering Attacks*

*4.8.1 Phishing for Credentials*

*4.8.2 OMG Cable Baiting*

***4.9 Specialized System Attacks***

*4.9.1 Pwn a Mobile Device*

*4.10 Automated Script Attacks*

*4.11 Attacks and Exploits Review*

**Module 5 - Post-exploitation and Lateral Movement**

***5.1 Establishing and Maintaining Persistence***

*5.1.1 Creating a Persistent Netcat Back Door*

*5.1.2 Exfiltrating Data with a Scheduled Task*

***5.2 Lateral Movement***

*5.2.1 Preparing to Pivot*

*5.2.2 Lateral Movement through Pivoting*

***5.3 Staging and Exfiltration***

*5.3.1 Hiding Data with Steganography*

*5.3.2 Automatically Exfiltrating Data*

***5.4 Cleanup and Restoration***

*5.5 Post-Exploitation and Lateral Movement Review*

**Module 6 - Diliverables**

***6.1 Penetration Test Report Components***

***6.2 Report Findings and Recommendations***

***6.2.1 Examining Pentest Reports***

***6.3 Deliverables Review***

***6.4 Course Conclusion***

1. **Learning Path:**

**1. Pentest Survey Analytics (You are Here) > 2. Security Foundation > 3. Attache Simulation Environment Training > 4. CySA+ (AI/ML protection) > 5. CASP+**