Certified Penetration Tester

Stop the Critical Security Weaknesses & Vulnerabilities.
Start Analyze, Secure & Defend

Course Brochure and Outline

CODEC Networks Pvt Ltd
507, New Delhi House, Barakhamba Road, New Delhi 110001
trainings@codecnetworks.com
+91 11 43752299, 9971676124

Certified Penetration Tester

Training Program

Course Overview

Certified Penetration Tester course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

The design of the course is such that the instructor in the class will actually take you through the core concepts of conducting a penetration test based on penetration testing methodology and report writing process for this organisation.

Today this course & techniques are very demand in InfoSec consultants working for software companies, IT security firms, Government and Private Sectors etc.

This course brings an enhanced concentration on methodology for network, web application, database, wireless, and cloud pen testing by using penetration testing methodologies like suggested from ISO 27001, OSSTMM, OWASP and NIST Standards.

Who Should Attend

The training program is ideal for those working in positions such as, but not limited to -

Ethical Hackers, Penetration Testers, Network Server Administrators, Firewall Administrators, Security Testers, System Administrators and Risk Assessment Professionals.

Course Duration: 40 Hours.

Course Content / Outline

- **Introduction to Penetration Testing and Methodologies**
  - What is Penetration Testing?
  - Types of Penetration Testing
  - Penetration Testing Phases
  - Penetration Testing Methodology
  - Penetration Testing Strategies
  - Ethics of Penetration Tester

- **Penetration Testing Scoping and Engagement Methodology**
  - Security Concerns
  - Data security Measure
  - Risk Analysis
  - Risk Assessment Steps
  - Security Policies
  - Information Security Standards
  - Information Security Acts

- **Open Source Intelligence (OSINT) Methodology**

- **Packet Analysis**
  - Overview of TCP/IP Model
  - TCP/IP Protocol Stack
  - Analysis of TCP/UDP Services
  - Overview of IPv4 and IPv6

  Tools Covered:
  - Wireshark
  - CAPSA Network Analyser

- **Pre-penetration Testing Steps**
  - Send a Preliminary Information Request Document to the Client
  - Identify the Type of Testing: Black-box or White-box
  - List the Servers, Workstations, Desktops and Network Devices that Require Testing
  - Draft Contracts
  - Identify Who Will be Leading the Penetration Testing Project

- **Information Gathering Methodology**
  - What is Information Gathering
  - Find the Company's URL and Geographical Location
  - Search for Contact Information, Email Addresses, and Telephone Numbers about company and Employees
  - Gather Company's Infrastructure Details
  - Gather Competitive Intelligence

  Tools Covered:
  - Recon-ng
  - Dmitry
  - Wayback Machine
  - Technical Info
  - Whois
  - Cyber Forensic Email Tracker
  - Tools to Extract Sensitive Data
  - Domain Research Tool
  - DNS Integration Tools (Domain Dossier, NS Lookup)
  - Trace Route Tools (Visual Route, Path Analyser Pro)
  - Website Mirroring Tools (HTTTrack)

- **Vulnerability Analysis**
  - What is Vulnerability Assessment?
  - Why Assessment?
  - Vulnerability Classification
  - Types of Vulnerability Assessment
  - Vulnerability Management Life Cycle
  - Comparing Approaches to Vulnerability Assessment

Tools Covered:

  - Nessus Pro
  - Acunetix
  - Burp Suite
  - Metasploit
  - Nikto
  - SearchSploit
  - OpenVas
  - Other Host-Based Vulnerability Assessment Tools
  - Other Application-Layer Vulnerability Assessment Tools
  - Other Vulnerability Assessment Tools

- **External Network Penetration Testing Methodology**
  - External Intrusion Test and Analysis
  - Perform Information Gathering
  - Create Topological Map of the Network
  - Identify the Physical Location and OS of the Target Servers
  - Checking for Live Systems
  - Perform Port Scanning
  - Perform OS Fingerprint

Tools Covered:

  - Nessus
  - NSE Script
  - Nmap
  - Metasploit
  - Acunetix

- **Internal Network Penetration Testing Methodology**
  - Why Internal Network Penetration Testing?
  - Internal Network
  - Perform Information Gathering
  - Scan the Network
  - Perform Enumeration
  - Sniff the Network
  - Attempt Replay, ARP Poisoning, Mac Flooding, DNS Poisoning Attacks

Tools Covered:

  - Nessus
  - NSE Script
  - Nmap
  - Metasploit
  - Acunetix
  - Ettercap
  - Cain & Abel
  - Wireshark

- **Firewall Penetration Testing Methodology**
  - What is a Firewall?
  - What Does a Firewall Do?
  - Types of Firewalls
  - Firewall Policy
  - Build a Firewall Ruleset
  - Find the Information about Target
  - Locate the Firewall

Tools Covered:

  - Firewall Management and Testing Tools
  - Traceroute Tools

- **IDS Penetration Testing Methodology**
  - Introduction to Intrusion Detection System(IDS)
  - Types of IDS
  - Why IDS Penetration Testing?
  - Common Techniques Used to Evade IDS System
  - IDS Penetration Testing Steps
  - Test the IDS by Packet Flooding
  - Test the IDS for a Denial-of-Service(DoS) Attack

Tools Covered:

  - Snort
  - Packet Sniffing Tools
  - Network Traffic Generator tool
  - IDS Evasion Tools

- Intrusion Detection Tools

- **Web Application Penetration Testing Methodology (OWASP)**
  - Introduction to Web Application
  - Web App Pen Testing Phases
  - Perform Web Spidering
  - Perform Service Discovery
  - Examine Source of the Available Pages
  - Test for Proxy Functionality
  - Test for Database Connectivity

Tools Covered:

  - OWASP TOP 10 Manual Methodology
  - HTTP Analysis (Curl, Netcat)
  - Nessus
  - Acunetix
  - Metasploit
  - Burpsuite
  - NSE Script

- **SQL Penetration Testing Methodology**
  - An Overview to SQL Injection
  - Types of SQL Injection
  - SQL Penetration Testing
  - Manual SQL Injection Penetration Testing
  - Automated SQL Injection System
  - SQL Injection Penetration Methodology

Tools Covered:

  - SQL Map
  - SQL Injection Manual Methodologies

- **Database Penetration Testing Methodology**
  - Sniffing Database-Related Traffic
  - Retrieving the Database Information Through a Vulnerable Web Application
  - Google Hacks
  - Database Penetration Testing Steps
  - Penetrating Oracle Database
  - Scanning Default and Non-Default Ports

Tools Covered:

  - Database Password Hacking Tools
  - Database Vulnerability Assessment Tools
  - Database Penetration Testing Tools

- **Wireless Network Penetration Testing Methodology**
  - Wireless Penetration Testing
  - Wireless Security threats
  - Wireless Penetration Testing Tools
  - Wireless Penetration Testing Steps
  - Introduction to RFID Security

  Tools Covered:
  - Aircrack-ng
  - Airodump-ng
  - Aireplay-ng
  - Wireshark

- **Mobile Devices Penetration Testing Methodology**
  - Why Mobile Device Penetration Testing?
  - Requirements for Mobile Device Penetration Testing
  - Mobile Penetration Testing Methodology
  - Communication Channel Penetration Testing
  - Server-side Infrastructure Pen Testing
  - Application Penetration Testing

  Tools Covered:
  - Android Penetration Testing Tools
  - iPhone Penetration Testing Tools

- **Cloud Penetration Testing Methodology**
  - Cloud Computing Security and Concerns
  - Security Risk Involved in Cloud Computing
  - Scope of Cloud Pen Testing
  - Steps to Conduct Cloud Pen Testing

- **Report Writing and Post Test Actions**
  - Goal of the Penetration Testing Report
  - Examine Types of Pen Testing Reports
  - Analyse and Finalize the Report
  - Review and Finalise the Report
  - Sample Pen Testing Report Format