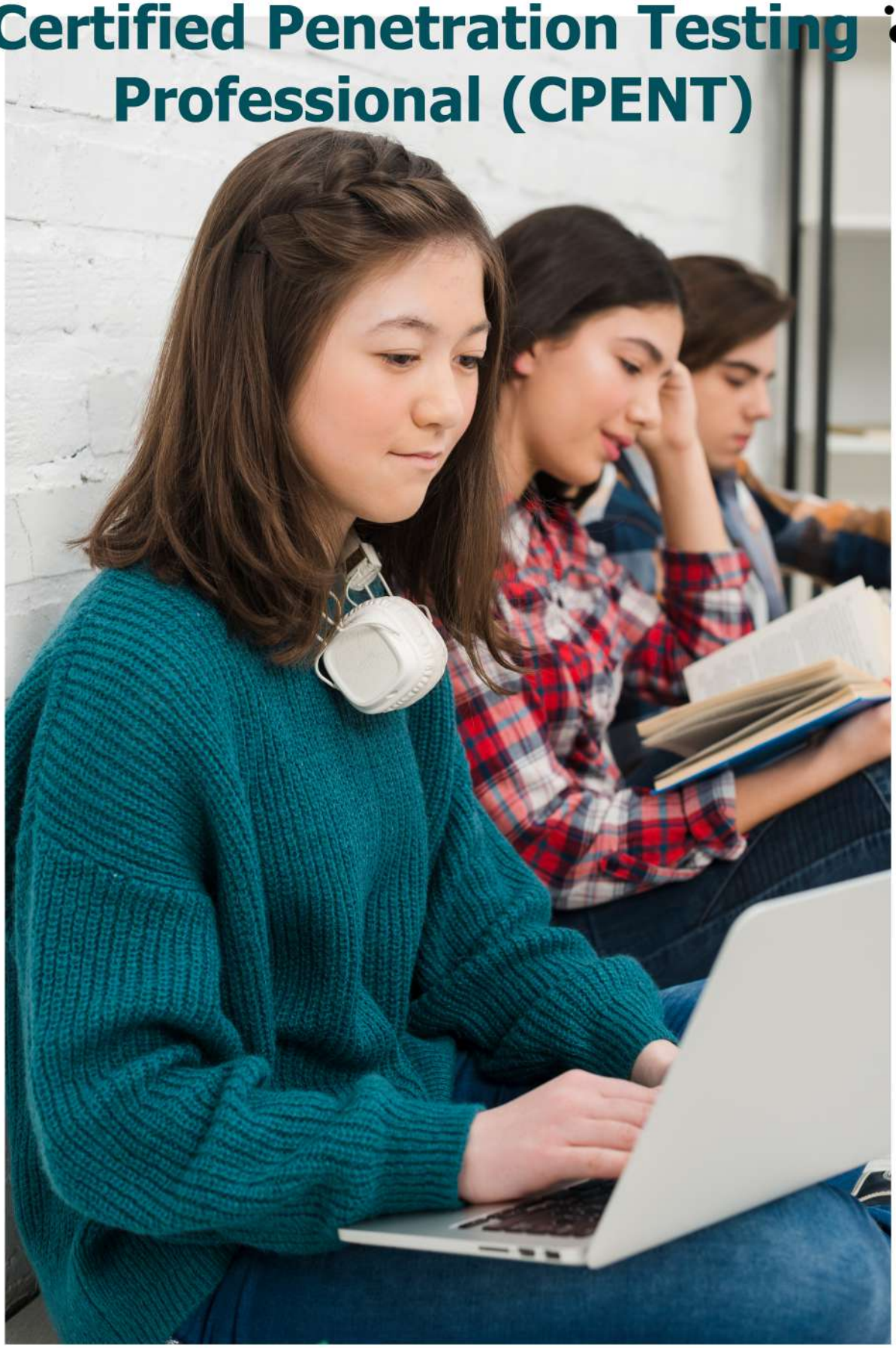
Certified Penetration Testing Professional (CPENT)

Zetlan Technologies



ZETLAN TECHNOLOGIES

www.zetlantech.com

Learn without Leaving Home..!

Online Course

Certified Penetration Testing Professional (CPENT)

Course Modules

1.Introduction to Penetration Testing

- Penetration Testing
- Penetration Testing Service Delivery Models
- ROI for Penetration Testing
- Types of Penetration Assessment
- Strategies of Penetration Testing
- Selection of Appropriate Testing Type
- Different methods of Penetration Testing
- Common Area of Penetration Testing
- Penetration Testing Process
- Penetration Testing Phases
- Penetration Testing Methodologies
- EC-Council LPT Methodology
- Qualities of a Licensed Penetration Tester
- Characteristics of Good Penetration test
- Ethics of a Penetration tester

Certified Penetration Testing Professional (CPENT)

2.Penetration Testing Scoping and Engagement

- Pre-engagement Activities
- Initiation of a Pen Testing Engagement Process
- Rules of Engagement
- Penetration Testing Schedule
- Identifying the Reporting Time Scales
- Deciding the time of day for the Test
- ROE Document
- Penetration Testing contract
- Penetration Testing Rules of Behaviour
- Confidentiality and Nondisclosure Agreement Clauses
- Identifying the Security Tools Required for the Penetration Test
- Preparing the Test Plan
- Penetration Testing Hardware/Software Requirements
- Mission Briefing
- Scope Creeping

3.Open-Source Intelligence (OSINT)

- OSINT through the WWW
- OSINT through website Analysis
- OSINT through DNS Interrogation
- Who is Lookups
- Reverse Lookups
- DNS Zone Transfer
- Traceroute Analysis
- Automatg the OSINT Process usg Tools / Frameworks / Scripts

4.Social Engineering Penetration Testing

- Social Engineering Penetration Testing
- Social Engineering Penetration Testing Modes
- Social Engineering Penetration Testing Process
- Social Engineering Using Email
- Phishing
- Spear Phishing
- Whaling
- Phone (Vishing)
- SmiShing (SMS Phishing)
- Social Engineering Using Physical Attack Vector
- Piggybacking / Tailgating
- Eavesdropping
- Dumpster Diving
- Reverse Social Engineering
- Social Engineering Using Motivation Techniques
- Social Engineering Countermeasures

5. Network Penetration Testing – External

- Network Penetration Testing
- External vs Internal Penetration Testing
- External network Penetration Testing
- Internal network Penetration Testing
- Network Penetration Testing Process
- Port Scanning
- Fingerprinting the OS
- Examining the Patches Applied to the Target OS
- Fingerprinting the Services
- External Vulnerability Assessment
- Searching & Mapping the Target with the Associated Security
- Find out the Security Vulnerability Exploits
- Running the Exploits against Identified Vulnerabilities

6.Network Penetration Testing – Internal

- Interna Network Penetration Testing
- Footprinting
- Network Scanning
- Scanning Analysis
- Scanning Methodology
- OS and Service Fingerprinting
- Identifying the OS
- SMB OS Discovery
- Manual Banner Grabbing
- Identifying the services
- Displaying services within Metasploit
- Map the internal network
- Enumeration
- Vulnerability assessment
- Internal Vulnerability Assessment Report
- Scan Analysis Process
- Windows Exploitation
- Unix / Linux Exploitation
- Attempt Repay Attacks
- Attempt ARP Poisoning
- Attempt Mac Flooding
- Conduct a Man-in-the-Middle Attack

Certified Penetration Testing Professional (CPENT)

- Attempt DNS Poisoning
- Automated Internal Network Penetration Testing
- Post Exploitation
- Pivoting
- Port Forwarding
- OS Discovery
- Proxychains
- Web Shells

Certified Penetration Testing Professional (CPENT)

7.Network Penetration Testing – Perimeter Devices

- Assessing Firewall Security Implementation
- Testing the Firewall from Both Sides
- Find Information about the Firewall
- Enumerate Firewall Access Control List Using Nmap
- Scan the firewall for Vulnerabilities
- Trying to Bypass the Firewall using various Techniques
- Assessing IDS Security Implementation
- Common Techniques used to Evade ISD System
- Test for Resource Exhaustion
- Test the IDS by using various Techniques
- Assessing security of Router Operating System and its cersion
- Identify Protocols Running
- Gain Access to the Router
- IP Spoofing
- Router Penetration Testing using secure Cisco Auditor (SCA)
- Assessing Security of Switches
- Test for Address of Cache Size
- Test for Data Integrity and Error Checking
- Test for Frame Error Filtering
- Test for VLAN Hopping
- Test for MAC table Flooding
- Testing for ARP Attack

Certified Penetration Testing Professional (CPENT)

9.Wireless Penetration Testing

- Wireless Penetration Testing
- Wireless Local Area network (WALN) Penetration Testing
- Discovering the Wireless Networks
- Detect Wireless Connections
- Use a Wireless Honeypot to Discovr Vulnerable wireless Clients
- Preforming a Denia-of-service Attack
- Attempt Rapid Traffic Generation
- Attempt Single-packet Decryption
- Perform an ARP Poisoning Attack
- Creak WPA-PSK Keys
- Creak WPA/WPA2 Enterprise Mode
- Check for MAC Filtering
- Spoof the MAC Address
- Create a Direct Connection to the Wireless Access Point
- Introduction to RFID Penetration Testing
- Perform Reverse Engineering
- Perform Power Analysis Attack
- Perform Eavesdropping
- Perform an MITM Attack
- Perform a DoS Attack
- Perform RFID Cloning / Spoofing

- Perform an RFID Replay attack
- Perform a Virus Attack
- Oscilloscopes
- RFID Antennas
- RFID Readers
- Introduction to NFC Penetration Testing
- Perform Data Corruption Attack
- Perform a MITM Attack

10. IoT Penetration Testing

- IoT
- Popular IoT Hacks
- IoT Challengers
- IoT Penetration Testing
- Abstract IoT testing Methodology
- Attack Surface Mapping
- IoT Architecture
- Typical IoT Vulnerabilities
- Steps to Analysing the IoT Hardware
- Firewall Attacks
- Attack Surface Map
- Sample Firewall Analysis Process
- Binwalk to Extract the File System
- Firmware Emulation

11. OT/SCADA Penetration Testing

- IT vs OT System Architecture
- ICS / SCADA Protocols
- Modbus
- ICS and SCADA Pen Testing
- Attack Monitoring
- Testing Environment
- Penetration Testing Actions
- Host Attack Types
- Network Attack Types
- Port of SCADA
- Attack Modification
- OT Testing Tools
- BACnet
- Commercial SCADA Fuzzing Tool
- Danger of Port Scanning
- Types of Vulnerability Scans
- Device Separation
- ICS Cyber test Impact

Certified Penetration Testing Professional (CPENT)

12. Cloud Penetration Testing

- Cloud Computing Security and Concerns
- Security Risk Involved in Cloud Computing
- Role of Penetration Testing in Cloud Computing
- Scope of Cloud Pen Testing
- Shared Responsibilities in Cloud
- Penetration Testing Process
- Identifying the Type of Cloud to be Tested
- Identifying Tools for Penetration Testing
- Perform a Detailed Vulnerability Assessment
- AWS Specific Penetration Testing
- Attempt to Identify S3 Buckets
- Azure Specific Penetration Testing
- Google Cloud Platform Specific Penetration Testing
- Google Cloud's Provision for Penetration Testing

13. Binary Analysis and Exploitation

- Binary Coding
- Machine Instructions
- Sample Stack Frame
- C Program Memory
- Analyzing Binaries
- Registers
- Important IA-32 Instructions for Pen Testing
- Executable and Linkable Format
- Advanced Binary Analysis
- Obfuscation Challenges
- Binary Instrumentation
- IA-64
- Binary Analysis Methodology
- Sample Program
- ASLR
- Return-to-libc vulnerability
- Defeating the No-execute Stack
- 64-bit Fundamentals
- Attack using ROP

14. Report Writing and Post Testing Actions

- Goal of the Penetration Testing Report
- Penetration Testing Deliverables
- Report Formats
- Types of Pen Test Reports
- Characteristics of a Good Pen Testing Report
- Phases of Report Development
- Sample Pen Testing Report Format
- Report Components
- Penetration Testing Report Analysis
- Section of the Penetration Testing Report
- Pen Test Team Meeting
- Research Analysis
- Prioritize Recommendations
- Delivering Penetration Testing Report
- Letter of Attestation
- Cleanup and Restoration
- Report Retention
- Sign-ff Document
- Post-Testing Actions for Organizations
- Develop an Action Plan
- Develop and Implement data Backup Plan
- Create a Process for Minimizing Misconfiguration Chances
- Updates and Patches

Zetlan Technologies

LEARN REMOTELY!!

The efficiency of online learning in terms of time management, flexibility, and the ability to access resources anytime, anywhere can be compelling.

ZETLAN TECHNOLOGIES

www.zetlantech.com

For contact: +91 8680961847
+91 9600579474