CompTIA Penetration Testing (Pen Test+)

Online Course

ZETLAN TECHNOLOGIES

www.zetlantech.com

CompTIA Penetration Testing (Pen Test+)

Course Modules

1. The Pen Test Engagement

- PenTest Plus Introduction
- PenTest Engagement
- Threat Modelling
- Technical Constraints
- PenTest Engagement Review
- Examining PenTest Engagement Documents Act

2. Physical Security

- Physical Security
- Badge Cloning Act

CompTIA

3. Social Engineering

- Social Engineering
- Using Baited USB Stick Act
- Using Social Engineering to Assist Attacks
- Phishing Act

4. Cover Your Tracks

- Cover Your Tracks
- Cover Your Tracks - Timestamp Files Act
- Cover Your Tracks - Frame the Administrator Act
- Cover Your Tracks - Clear the Event Log Act

5. Passive Reconnaissance

- Passive Reconnaissance
- WHOIS Act
- Google Hacking Act
- DNS Querying Act
- Email Server Querying Act
- SSL-TLS Certificates
- Shodan Act
- The Havester
- The Harvester Act
- Recon-ng
- Recon-g Act
- Recon-ng-API-key Act
- Maltego
- Have I been Pwned
- Punked and Owned Pwned Act
- Fingerprinting Organization with Collected Archives
- FOCA Act
- Findings Analysis Weaponization
- Chp 2

6. Mobile Devices

- Mobile Devices
- Hacking Android Act
- Apple Exploits
- Specialized Systems

7. Active Reconnaissance

- Active Reconnaissance
- Discovery Scans Act
- Nmap
- Nmap Scans Types Act
- Nmap Options
- Nmap Options Act
- Stealth Scans
- Nmap Stealth Scans Act
- Full Scans
- Full Scans Act
- Packet Crafting
- Packet Crafting Act
- Network Mapping
- Metasploit
- Scanning with Metasploit Act
- Enumeration
- Banner Grabbing Act
- Windows Host Enumeration
- Windows Host Enumeration Act
- Linux Host Enumeration
- Linux Host Enumeration Act
- Service Enumeration
- Service Enumeration Act
- Network Shares
- SMB Share Enumeration Act

CompTIA Penetration Testing (Pen Test+)

- NFS Network Share Enumeration
- NFS Share Enumeration Ac
- Null Sessions
- Null Sessions Act
- Website Enumeration
- Website Enumeration Act
- Vulnerability Scans
- Compliance Scans Act
- Credentialed Non-credentialed Scans
- Using Credentials in Scans Act
- Server Service Vulnerability Scan
- Vulnerability Scanning Act
- Web Server Database Vulnerability Scan
- SQL Vulnerability Scanning Act
- Vulnerability Scan OpenVAS Act
- Web App Vulnerability Scan
- Web App Vulnerability Scanning Act
- Network Device Vulnerability Scan
- Network Device Vuln Scanning Act
- Nmap Scripts
- Using Nmap Scripts for Vuln Scanning Act
- Packet Crafting for Vulnerability Scans
- Firewall Vulnerability Scans
- Wireless Access Point Vulnerability
- Wireless AP Scans Act
- WAP Vulnerability Scans

8. Password Cracking

- Password Cracking
- Brute Force Attack Against Network Service Act
- Network Authentication Interception Attack
- Intercepting Network Authentication Act
- Pass the Hash Attacks
- Pass the Hash Act

9. Penetrating Wired Networks

- Penetrating Wired Network
- Sniffing Act
- Eavesdropping
- Eavesdropping Act
- ARP Poisoning
- ARP Poisoning Act
- Man in The Middle
- MITM Act
- TCP Session Hijacking
- Server Message Blocks SMB Exploits
- SMB Attack Act
- Web Server Attacks
- FTP Attacks
- Telnet Server Attacks
- SSH Server Attacks
- Simple Network Mgmt Protocol SNMP
- Simple Mail Transfer Protocol SMTP

10. Penetrating Wireless Networks

- Penetrating Wireless Networks
- Jamming Act
- Wireless Sniffing
- Replay Attacks
- WEP Cracking Act
- WPA-WPA2 Cracking
- WAP Cracking Act
- Evil Twin Attacks
- Evil Twin Attack Act
- Wi-Fi Protected Setup
- Bluetooth Attacks

11. Windows Exploits

- Windows Exploits
- Dumping Stored Passwords Act
- Dictionary Attacks
- Dictionary Attack Against Windows Act
- Rainbow Table Attacks
- Credential Brute Force Attacks
- Keylogging Attack Act
- Windows Kernel
- Kernel Attack Act
- Windows Components
- Memory Vulnerabilities
- Buffer Overflow Attack Act

12. Linux Exploits

- Linux Exploits
- Exploiting Common Linux Features Act
- Password Cracking in Linux
- Cracking Linux Passwords Act
- Vulnerability Linux
- Privilege Escalation Linux

13. Scripts

- Scripts
- Powershell
- Python
- Ruby
- Common Scripting Elements
- Ping Sweep
- Simple Port Scanner2
- Port Scanner with Nmap

14. Lateral Movement

- Lateral Movement
- Lateral Movement with Remote Mgmt Services
- Process Migration Act
- Passing Control Act
- Pivoting
- Tools the Enable Pivoting
- Lateral Movement Review

15. Application and Web Exploits Testing

- Application Testing
- Web App Exploits
- Webb App Exploits
- Injection Attacks
- HTML Injection
- SQL Hacking – SQL map Act
- Cross-Site Attacks
- Cross-Site Request Forgery
- Other Web-based Attacks
- File Inclusion Attacks
- Web Shells
- Web Shells Review

16. Persistence

- Persistence
- Breeding RATS Act
- Bind and Reverse Shells
- Bind Shells Act
- Reverse Shells
- Reverse Shells Act
- Netcat
- Netcat Act
- Scheduled Tasks
- Scheduled Tasks Act
- Services and Domains

6. Vulnerability Scan Analysis

- Vulnerability Scan Analysis
- Validating Vulnerability Scan Results Act

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