Course: ICSI | CPT Certified Penetration Tester

This course is designed to teach how to perform penetration tests, how to think like an attacker and demonstrates the tools needed to perform penetration testing. The course is aligned with the CREST CRT technical syllabus.

Students will learn and perform information gathering, target discovery and enumeration, vulnerability mapping, system exploitation including Windows Domain attacks, and Azure AD (Active Directory), privilege escalation and maintaining access to compromised systems with over 40 detailed hands-on labs.

Audience Profile:

- Penetration Tester
- Ethical hackers
- Red Team members
- Vulnerability Tester
- Security Analyst
- Vulnerability Assessment Analyst
- Network Security Operations

Candidate Prerequisites:

Basic familiarity with networking and Linux operating system.

Accreditation:

CREST Approved Training
MSc Cybersecurity 20 Credits

Exam Details:

Exam Code: CPT
Type of Questions: Hands-On Multiple Choice
Duration: 3 Hours
Passing Score: 70%
Exam Voucher Included

Course Outline:

Module 1: Introduction to Kali Linux

Lessons:

- Kali Linux History
- Kali Linux Installation
- Kali Linux Configuration
- Basic Search Utilities

Labs:

- Finding Files
- Starting and Stopping Services

Module 2: Introduction to Penetration Testing

Lessons:

- What is Penetration testing
- Benefits of Penetration Testing
- Vulnerability Scans
- Methodologies
- Ethical Issues
- Legal Issues

Review Questions

Module 3: Standards

Lessons:

- Penetration Testing Execution Standard (PTES)
- PCI DSS
- NIST 800-115
- CREST UK
- OWASP Top 10
- ISO 27002

Review Questions

Module 4: Network Essentials

Lessons:

- TCP/IP
- IP Protocols
- Network Architectures
- Domain Name Server (DNS)
- Management Protocols
- Network Protocols
- Using Netcat

Labs

- Using Netcat

Module 5: Cryptography

Lessons:

- Basics of Cryptography
- History of Encryption
- Symmetric Encryption
- Asymmetric (Public Key) Encryption
- Digital Signatures
- Hashing
- MAC and HMAC
- Encoding
- Password Crackers
- Steganography
- Cryptanalysis

Review Questions

Module 6: Scripting

Lessons:

- Scripting
- Windows PowerShell (Command Line Interface)

- Linux Shell (Command Line Interface)

Labs:

- Writing a Simple Bash Script

Module 7: Information Gathering

Lessons:

- Passive Information Gathering
- Registration Records
- Google Searching
- Active Information Gathering
- DNS Enumeration
- Host Discovery
- Port and Operating System Discovery
- Fingerprinting and Enumeration

Labs:

- Using Shodan
- DNS Enumeration
- Host Discovery
- Port and operating System Discovery
- Fingerprinting and Enumeration
- Information Gathering

Module 8: Vulnerability Assessment

Lessons:

- Vulnerabilities
- Packet Capture
- Network Scanners
- Nmap NSE
- Metasploit Framework
- Web Application Scanners

Labs:

- Using Wireshark

- Using OpenVas
- Using Nmap Scripts
- Using Metasploit Framework
- Finding Vulnerabilities

Module 9: Reconnaissance and Exploitation of Windows Services

Lessons:

- Important Windows Files
- Windows Logs
- The Registry
- Active Directory Roles
- Active Directory Database
- Active Directory Reconnaissance
- User and System Enumeration
- Windows Vulnerabilities
- Windows Privilege Escalation
- Antivirus Evasion
- Harvesting Credentials
- Windows Password Cracking

Labs:

- Active Directory Reconnaissance
- User and System Enumeration
- Windows Vulnerabilities
- Windows Privilege Escalation
- Evading Windows Defender
- Responder
- Dumping Credentials from Memory
- Extract SAM File from Windows Registry
- Attacking SMB

Module 10: Reconnaissance and Exploitation of Linux/UNIX Services

Lessons:

- Linux Permissions Review
- User Enumeration
- Linux/Unix Service Enumeration
- Linux/Unix Vulnerabilities
- Linux Privilege Escalation
- Linux/Unix Passwords

Labs

- User Enumeration
- Service Enumeration
- Exploit ProFTP
- Linux Privilege Escalation
- Linux/Unix Vulnerabilities

Module 11: Reconnaissance and Exploitation of Web-Based Applications

Lessons:

- Web Protocols
- Web Servers
- Web Application Structure Discovery
- Cross-Site Scripting (XSS)
- SQL Injection
- Directory Traversal
- File Uploads
- Command Execution

Labs:

- XSS
- SQL Injection
- Directory Traversal
- File Uploads

- Command Execution

Module 12: Databases

Lessons

- Databases
- Microsoft SQL Server
- Oracle RDBMS
- MySQL

Labs

- Assessing Databases

Module 13: Lateral Movement

Lessons

- Discovery
- Windows Situational Awareness
- Linux Situational Awareness
- Lateral Movement

Labs

- Pass the Hash
- Port Forwarding

Module 14: Data Exfiltration

Lessons

- Data from Local System
- Data Exfiltration with Frameworks

Labs

- Data Exfiltration with Metasploit

Module 15: Maintaining Access and Covering Tracks

Lessons

- Persistence
- Windows Persistence
- Windows Persistence with Scheduled Tasks
- .bash Startup File Manipulation
- Local Job Scheduling
- Linux Persistence by Adding User Accounts
- Windows Persistence by Adding User Accounts

Labs

- Maintaining Access

Module 16: Pen Testing Cloud Services (Azure)

Lessons

- Introduction to Cloud Computing
- Cloud Security
- Threats and Attacks
- Azure
- Azure AD
- Access Control
- Attacking Azure with PowerZure

Labs

- Attacking Azure