ICSI CPT
CERTIFIED PENETRATION TESTER

Accreditations

uclan University of Central Lancashire

CREST ACCREDITED

CPT is accredited by CREST and helps you prepare for the CREST Registered Penetration Tester examination.

Course Outline: **Penetration Tester Course**

Certification: **ICSI|CPT Certified Penetration Tester**

Duration: **4 days**

Candidate Prerequisites: **Basic knowledge of Windows and Linux**

Overview:

This course teaches the fundamentals of penetration testing and will illustrate how to think like an attacker and use industry standard tools to perform penetration testing. The course is aligned with the CREST CRT technical syllabus.

Students will learn and perform the different phases of penetration testing assessments. The students will practice using Kali Linux and its tools to perform information gathering, target discovery and enumeration, vulnerability mapping, social engineering, system exploitation, privilege escalation, and maintaining access to compromised systems. The students will also learn to report the results of their assessments.

All exercises unless noted otherwise are performed in an isolated online hosted testing lab.

Who Should Attend:

This course will significantly benefit any professionals who are involved in the areas of Information Risk, IT audit, Information Security as well as new individuals wanting to begin a career in IT Security penetration testing.

Outline:

Module 1:
Penetration Testing Methodology

- What is a penetration test and why is it performed
- Types of penetration testing
- Penetration testing methodologies
- Ethics/ Legal and Compliance issues

Module 2:
Penetration Testing Engagement Lifecycle

- Client/Stakeholder requirements
- Scope of a penetration test
- Boundaries of the tests
- Project management of a test

Module 3:
The Basics

- Networking concepts (IP/OSI/DNS)
- Microsoft Windows
- Unix/Linux
- Cryptography
- Management and Networking Protocols
- Wi-Fi Security

Module 4:
Introduction to Kali Linux

- What is Kali Linux
- Some Kali Linux Basics
- Lab tour and configuring the virtual machines

IC SI CPT

CERTIFIED
PENETRATION TESTER

Module 5:
Information Gathering and Social Engineering

- Open source intelligence (OSINT)
- Domain registration information
- Obtaining DNS records and network routing information
- What is social engineering? Attack methods
- Social Engineering Toolkit (SET)

Module 6:
Target Discovery and Enumeration

- What is target discovery
- Identifying the target machine
- OS fingerprinting
- Port scanning the target
- SMB, SNMP enumeration

Module 7:
Vulnerabilities

- Types of vulnerabilities
- Windows / Linux common vulnerabilities
- Vulnerability taxonomy and analysis
- Windows/Linux vulnerabilities

Module 8:
Target Exploitation

- Vulnerability research
- Vulnerability and exploit repositories
- Exploitation toolkit
- Exploitation for Windows and Linux

Module 9:
Privilege Escalation

- Using a local exploit
- Password attack tools
- Network spoofing tools
- Escalation for Windows and Linux

Module 10:
Maintaining Access and Covering Tracks

- Why maintain access?
- Backdoors
- Tunnelling
- Covering Tracks

Module 11:
Documentation and Reporting

- Documentation and results verification
- Types of reports
- Remediating actions

Examination & Certification:

One-day penetration testing certification exam based on real word scenarios using our isolated online hosted testing lab.

Pass = 50 - 59%
Merit = 60 - 79%
Distinction = 80 - 100%

100% Final Assessment

40 Gracechurch Street,
London EC3V 0BT, UK.
t: +44(0)2035145523
f: +44(0)2035143985

www.icsi.co.uk

IC SI International CyberSecurity Institute™