ICSI
INTERNATIONAL CYBERSECURITY INSTITUTE

Course Outline: Network Infrastructure Penetration Testing and Ethical Hacking

Certification: ICSI | CPT Certified Penetration Tester

Required Courses and Exams:

Course	Exam
a) Network Infrastructure Penetration Testing and Ethical Hacking (5 Days)	**CPT-INF**
b) Web Application Penetration Testing and Ethical Hacking (3 Days)	CPT-WEB

Note: You need to pass both exams to become an ICSI | CPT Certified Penetration Tester.

Accreditation: CREST Accredited Training Course (CRT) - University of Central Lancashire (MSc Cybersecurity Credits: 20)

Duration: 5 Days

Candidate Prerequisites:

Basic Familiarity with Networking and Linux Operating System.

Overview:

This course teaches 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.

Who Should Attend:

This course will provide students with basic to intermediate knowledge in Ethical Hacking and Penetration Testing, significantly benefiting any professional who is involved in the area of Information Security as well as new individuals wanting to begin a career in IT Security.

What is Included:

- eBook
- Lab Guide
- 6 months 24x7 remote access to a virtual lab
- 1 exam voucher - Online Exam Proctoring
- Certificate of Attendance (Digital)

Module 1: Introduction to Kali Linux

- Installing, configuring and updating Kali Linux
- Configuring Network Services

Module 2: Introduction to Pen Testing

- The need for Pen Testing
- Types of Pen Testing
- Methodology of Pen Testing
- Ethics and Compliance to Legal Systems

Module 3: Refreshing Network concepts

- TCP/IP and DNS Basics
- Netcat – TCP/IP Swiss Army Knife
- Sniffing Network Packets with Wireshark

Module 4: Information Gathering

- Discovering lives hosts over the network
- Discovering ports over the network
- OS Fingerprinting
- Service fingerprinting and enumeration

- User Enumeration
- Open-source information gathering

Module 5: Vulnerability Mapping

- Vulnerability assessment with OpenVAS Framework
- Using Nmap Scripting Engine (NSE)

Module 6: System and Password Exploitation on Windows

- Brute Force Attack (Hydra)
- Cracking Password Hashes
- Metasploit Framework – Auxiliary Modules, Exploits
- Client Side Exploits
- Social Engineering – SET Toolkit
- Exploiting vulnerable services (Unix/Linux)
- Exploiting vulnerable services (Windows)
- ARP Poisoning – MiTM

Module 7: Privilege Escalation and Maintaining Access

- Metasploit Meterpeter
- Building your own MSF Payload – backdoor
- Compromise Active Directory

Module 8: Pivoting

- Port Forwarding
- Pivoting with Meterpreter

Module 9: Covering Tracks

- Clearing tracks using find
- Clearev

Module 10: Documentation & Reporting

- Writing Pen Testing Reports

Module 11: Capture the Flag workshop

In this workshop you will apply skills acquired during the course to conduct a full penetration test in an isolated environment.

Exam:
The CPT-INF practical certification exam covers Hands-On material from all 10 modules. The exam duration is 2.5 hours. Passing Grade = 70%.