CTR-901 Cyber Security Penetration Testing Professional

About this course

This is a 24-hour course that teaches the most practical and thorough education on penetration testing, as the Penetration Testing Professional (PTP) course is a self-paced program designed to develop educated IT security experts. This course provides theoretical aspects reinforced with practical exercises held in the most advanced virtual lab setting in the world, and creates solid foundations.

Audience profile

This CPTP course is advantageous for people who want to advance their careers as professional penetration testers or IT security specialists, whose positions need them to be able to defend their organizations.

At course completion

After completing this course, students will be able to:

- Students will be tested in a real-world setting at the conclusion of the course and required to create a commercial-grade penetration testing report that accurately pinpoints the flaws in this "interaction".

Course details:

Module 1: System Security

This module will teach students about the system security section and will provide them with a thorough understanding of x86 architecture and its weaknesses. They will be taught about architecture Fundamentals, assembler debuggers and tool arsenal, buffer overflow, shellcode, cryptography, and password cracking, and malware.

Module 2: Network Security

This module will cover security testing methodology, techniques, and tools for networked PC and devices. Topics like information gathering, scanning, enumeration, sniffing and MITM attacks, vulnerability assessment & exploitation, post-exploitation, anonymity, and social engineering.

Module 3: Performing a Penetration Test

This module will teach students about the three phases of the pretest, penetration testing tools and techniques as well as other penetration test steps.

Module 4: Ethical Hacking

Here, you will learn about the role of security and penetration testers, ethical hacking litigations, attacks and ethical hacking commandments, and cracking hackers' mindsets

Module 5: PowerShell for Pentesters Section

This module educates students on PowerShell is a powerful built-in shell and scripting environment we can utilize as penetration testers considering its wide-spread

availability on all modern Windows-based systems. The use of PowerShell allows us to take advantage of the "living off the land" concept, where using tools that are built-in to the Operating System works to our advantage once we've obtained access to a system. While studying how to Pentesters enables you to conduct targeted tests on specific portions of your organization, with results that are extremely useful for identifying system flaws – some of which can only be identified through testing – and highlighting the necessary steps to address them.

Module 6: Linux Exploitation Section
This module teaches you about Linux and other variants of UNIX that make up a very large segment of the overall internet infrastructure (including Critical Infrastructure), not to mention the exponentially expanding "Internet of Things" ecosystem of whose devices are mostly dependent on some form of *NIX or another. Those facts make Linux an increasingly popular target.

Module 7: Web Application Security
Today's penetration testers must master web application attack techniques; this lab-intensive section will teach the student how to conduct a thorough Penetration test against web applications. Here, you will learn how to gather information, also about cross-site scripting, SQL injection, and other web attacks.

Module 8: Wi-fi Security Section
The Wi-Fi Security section is an extremely in-depth section covering the most important attack techniques used against Wi-Fi networks. The student will learn the security mechanisms implemented in Wi-Fi architectures as well as their weaknesses and how to exploit them.

Module 9: Ruby for Pentesters and Metasploit Section
The Ruby for Pentesters and Metasploit section covers Ruby programming from the very basics to advanced techniques, in addition to penetration testing topics. This section also covers topics such as exploiting vulnerable applications with Ruby, as well as creating and editing Metasploit modules. They will learn how Pentesters help organizations identify and resolve security vulnerabilities affecting their digital assets and computer networks.

Module 10: Mastering Kali Linux for Advanced Penetration Testing
The 'Kill Chain' approach to penetration testing will be taught in this module as well as starting Kali Linux, identifying the target (passive reconnaissance), active reconnaissance and vulnerability scanning. Also, students will learn of its exploits, post exploit stages in both its action of objective and persistence.

Prerequisites:

- Entry Level exam (American test)
- No programming skills are required. However, a basic understanding of networks, internet protocols, IT security issues, and penetration testing

concepts, as well as the ability to read and understand code will greatly reduce the learning curve of a student.