Course Title:

EHPT-C

Duration:

5 days,40 Hrs

Class Format Options:

Instructor-led classroom Live Training - Computer Based Training.

Who Should Attend:

- Cyber Security Professionals
- SOC Managers
- SOC Engineers
- IT Auditors
- System Administrators
- IS Managers

Prerequisites:

A minimum of 24 months experience in networking technologies

Network+, Security+

Provided Materials:

- Softcopy Materials.
- 20 GB hacking tools.

Certification Exam:

- Mile2 CPEH
- Mile2 CPTE
- Mile2 CPTC
- EC-Council CEH

Course Overview

The Ethical Hacking & Penetration Testing Consultant course is an advanced cyber security course aims to teach students on the proper technique to conduct penetration testing service and generate a professional report. It covers web application penetration testing as well; The **EHPT-C** is designed for those people who wish to become cyber security professionals, SOC engineers, SOC Managers, Information Security Assurance specialists or penetration testers including PT based on PCI – Data Security Standard.

Ethical hacking is the art of using these penetration testing techniques to identify and mitigate detected vulnerabilities in a system or a website, however the **EHPT-C** trains students on the 6 key elements of penetration testing from a practical way: information gathering Phase, Analysis Phase, Vulnerability Identification Phase, Exploiting Phase, Privilege Escalation Phase and Stress Testing Phase, At the completion of each module, students will be able to practice their knowledge with a specialized lab exercises that are specifically prepared for consultants.

Our certified trainers with more than 12 years experience in conducting penetration testing trainers keep abreast of their field by practicing what they teach along with experience resulted from conducting real penetration testing to high end clients.

Furthermore, This training course learn the students on how to comply with PCI-DSS penetration testing procedures and penetration testing report writing for PCI-DSS, EHPT-C presents detailed information related to the three primary parts of a penetration test: pre-engagement, engagement, and post-engagement as well as PCI DSS Requirement 11.3.4 that requires penetration testing to validate that segmentation controls and methods are operational, effective, and isolate all out-of-scope systems from systems in the CDE.

Upon Completion

Students will:

- Have the knowledge on proper using of penetration testing tools.
- Have the ability to plan, manage, and execute a penetration test projects.
- Have knowledge to properly report on a penetration test results.
- Conduct a full Penetration testing scenario.

EHPT-C Course Content

- **Module 0:** Course Overview.
- **Module 1:** Penetration Testing Phases.
- **Module 2:** Linux Fundamentals related to Penetration Testing.
- **Module 3:** Information Gathering Phase.
    - **Module 3-a:** Detecting Live Systems.
    - **Module 3-b:** Enumeration.
- **Module 4:** Vulnerability Assessments and tools training.
- **Module 8:** Windows Hacking
- **Module 9:** Advanced Exploitation Techniques.
- **Module 10:** Wireless Penetration Testing Tools.
- **Module 12:** Networks, Sniffing and IPS.
- **Module 13:** Injecting the Database.
- **Module 14:** Attacking Web Technologies.
- **Module 15:** – Penetration Testing depending on **PCI Data Security Standard.**
- **Module 16:** writing a Penetration Testing report.

EHPT-C Course Content

- **Lab 1:** Getting Set Up
- **Lab 2:** Linux Fundamentals
- **Lab 3:** Information Gathering
- **Lab 4:** Detecting Live Systems
- **Lab 5:** Reconnaissance
- **Lab 6:** Vulnerability Assessment
- **Lab 7:** Windows Hacking
- **Lab 8:** UNIX/Linux Hacking
- **Lab 9:** Advanced Vulnerability and Exploitation
- **Lab 10:** Attacking Wireless Networks
- **Lab 11:** Network Sniffing and IDS
- **Lab 12:** Database Hacking
- **Lab 13:** Hacking Web Applications
- **Lab 13:** Full Penetration Testing Scenario
- **Post Class Lab:** Armitage.
- **Post Class Lab:** Segmentation Checks.
- Separate testing environment.