Course Title:

EHPT-C

Duration:

6-8 sessions
(100% Practical)
No Theoretical Part

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:

Vulnerability-Assessment Workshop.
Ethical Hacking Workshop.

Certification Exam:

- Mile2 CPEH
- Mile2 CPTE
- Mile2 CPTC
- SANS SEC542: Web App Penetration Testing and Ethical Hacking

Course Overview

The Ethical Hacking & Penetration Testing Consultant workshop 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 15+ 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 (Cardholder Data Environment).

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.
- Ready to attend advanced Penetration Testing Workshop.

EHPT-C Content | Labs

- **Module 1:** Penetration Testing Phases.
- **Module 2:** Directory Encryption LAB.
- **Module 3:** Proxy chains LAB.
- **Module 4:** Random Tools LAB.
- **Module 5:** Joomla Exploitation Techniques LAB.
- **Module 6:** Wordpress Exploitation Techniques LAB.
- **Module 7:** Web Application PT | Advanced Testing LAB.
- **Module 8:** Password Attacks LAB.
- **Module 9:** Web Application PT | Advanced Testing LAB.
- **Module 10:** Wireless Attack LAB.
- **Module 11:** OWASP TOP 10.
- **Module 12:** Exploit DataBase LAB.