Certified Professional Ethical Hacker

Description:

To protect an information system you need to be able to see that system through the eyes of the attacker. The Certified Professional Ethical Hacker certification course is the foundational training to Mile2's line of penetration testing courses because it teaches you to think like a hacker. Therefore, you can

First, you will learn the value of vulnerability assessments. Then, you will discover how to use those assessments to make powerful changes in an information system's security. Additionally, you will learn how malware and destructive viruses function and how to implement counter response and preventative measures when it comes to a network hack.

Annual Salary Potential $80,077 AVG/year

Key Course Information

Live Class Duration: 5 Days
CEUs: 40
Language: English
Class Formats Available:

Instructor Led

Self-Study

Live Virtual Training

Suggested Prerequisites:
(any one of the following)

- Mile2's C)SP
- 12 months of IT Experience
- 12 Months of Networking Experience

Modules/Lessons

Module 1 -Introduction to Ethical Hacking
Module 2 -Linux Fundamentals
Module 3 -Protocols
Module 4 -Cryptography
Module 5 -Password Cracking
Module 6 -Malware
Module 7 -Security Devices
Module 8 -Information Gathering -Passive Reconnaissance
Module 9 -Social Engineering
Module 10 -Active Reconnaissance
Module 11 -Vulnerability Assessment
Module 12 -Network Attacks
Module 13 -Hacking Servers
Module 14 - Hacking Web Technologies
Module 15 – 16: See Detailed Outline Below

Hands-On Labs

Lab 1 – Intro to C)PEH Setup
Lab 2 - Linux Fundamentals
Lab 3 – Understanding Protocols
Lab 4 - Cryptography Lab
Lab 5 – Password Cracking
Lab 6 - Malware
Lab 7 – Information Gathering
Lab 8 – Information Gathering – Active Reconnaissance
Lab 9 – Vulnerability Assessment
Lab 10 – Network Sniffing/IDS
Lab 11 - Windows Hacking
Lab 12 – Attacking Databases
Lab 13 – Attacking Web Applications
Lab 14 - Backdoors

Upon Completion

Upon completion, the Certified Professional Ethical Hacker candidate will be able to competently take the C)PEH exam.

Who Should Attend

- IS Security Owners
- Security Officers
- Ethical Hackers
- Information Owners
- Penetration Testers
- System Owners and Managers
- Cyber Security Engineers

Accreditations

Exam Information

The Certified Professional Ethical Hacker exam is taken online through Mile2's Learning Management System and is accessible on you Mile2.com account. The exam will take approximately 2 hours and consist of 100 multiple choice questions.

A minimum grade of 70% is required for certification.

Re-Certification Requirements

All Mile2 certifications will be awarded a 3-year expiration date.

There are two requirements to maintain Mile2 certification:

1) Pass the most current version of the exam for your respective existing certification
2) Earn and submit 20 CEUs per year in your Mile2 account.

Course FAQ's

Question: Do I have to purchase a course to buy a certification exam?

Answer: No

Question: Do all Mile2 courses map to a role-based career path?

Answer: Yes. You can find the career path and other courses associated with it at www.mile2.com.

Question: Are all courses available as self-study courses?

Answer: Yes. There is however 1 exception. The Red Team vs Blue Team course is only available as a live class.

Question: Are Mile2 courses transferable/shareable?

Answer: No. The course materials, videos, and exams are not meant to be shared or transferred.

Course and Certification Learning Options

Detailed Outline:

Course Introduction

Module 1 – Introduction to Ethical Hacking

a. What and Why?
b. Differences
c. Security Definitions
d. Risk Management
e. Methodologies

Module 2 – Linux Fundamentals

a. Core Concepts
b. The shell and other items you need to know
c. Managing users
d. Basic Commands

Module 3 – Protocols

a. Network Models
b. Protocols & Services

Module 4 – Cryptography

a. Understanding Cryptography
b. Symmetric Encryption
c. Asymmetric Encryption
d. Hashing
e. Cryptography in Use
f. Crypto Attacks

Module 5 – Password Cracking

a. What and Why
b. Attacks and Tools of the Trade
c. Countermeasures

Module 6 – Malware

a. DOS & DDOS
b. Viruses & Backdoors

c. Trojans and Backdoors
d. Ransomeware

Module 7 – Security Devices

a. Basic Security Elements
b. Security Appliances

Module 8 – Information Gathering

a. What are we looking for?
b. Where/How do we find this information?
c. Are there tools to help?

Module 9 – Social Engineering

a. Social Engineering Types
b. Phishing Scams

Module 10 – Reconnaissance

a. What are we looking for?
b. Port Scanning
c. Are there tools to help?
d. Banner Grabbing
e. Enumeration

Module 11 – Vulnerability Assessment

a. What is a Vulnerability Assessment
b. Tools of the Trade
c. Testing Internal and External Systems

Module 12 - Network Attacks

a. Sniffing Techniques
b. Hijacking

Module 13 – Hacking Servers

a. Servers, What are they good for?
b. What is an Exploit?
c. Tools of the Trade

Module 14 – Hacking Web Technologies

a. OWASP Top 10
b. SQL Injection
c. XSS

Module 15 – Hacking Wireless Networks

a. Wireless Technologies
b. Mobile and IoT Technologies
c. Various Tools Used
d. Hacking Techniques
e. Countermeasures

Module 16 – Maintaining Access and Covering Tracks

a. Maintaining Access
b. Covering Tracks

Detailed Labs Outline:

Lab 1 – Intro to C)PEH Setup

a. Recording Ips and Logging into VMs
b. Joining the Domain

Lab 2 - Linux Fundamentals

a. Command Line Tips and Tricks
b. Linux Networking for Beginners
c. Using FTP during a Pentest

Lab 3 – Understanding Protocols

a. Analyze http session

Lab 4 - Cryptography Lab

a. Hashing Data of all Sorts
b. The Basics of Cryptographic Algorithms

Lab 5 – Password Cracking

Lab 6 - Malware

a. Creating a virus
b. Beast Trojan

Lab 7 – Information Gathering

a. Google Queries
b. Searching Pastebin
c. Maltego
d. People Search Using the Spokeo Online Tool
e. Recon with Chrome
f. Nslookup

Lab 8 – Information Gathering – Active Reconnaissance

a. Scanning with Nmap
b. Scanning with Hping
c. Banner Grabbing
d. Enumerating a local System with Hyena
e. SMTP Enumeration
f. Ad Enumeration

Lab 9 – Vulnerability Assessment

a. Vulnerability Assessment with Nessus
b. Vulnerability Assessment with Saint

Lab 10 – Network Sniffing/IDS

a. Sniffing Passwords with Wireshark
b. Performing MtM with Cain
c. Performing MtM with sslstrip

Lab 11 - Windows Hacking

a. Attack Windows 7 with Client-Side Exploit
b. Windows 2012 Reverse TCP Exploit
c. Cracking with John the Ripper

Lab 12 – Attacking Databases

a. Attacking MySQL Database
b. Manual SQL Injection

Lab 13 – Attacking Web Applications

a. Attacking with XSS
b. Attacking with CSRF

Lab 13 - Backdoors

a. Setting up a Backdoor