Description:

,663,6629



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 set up dynamic defenses to prevent intrusion.

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

Icon

Description automatically generated

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

Hands-On Labs

**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

Key Course Information

Modules/Lessons

**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

Exam Information

Upon Completion

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.

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.

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

• IS Security Owners

• Security Officers

• Ethical Hackers

• Information Owners

• Penetration Testers

• System Owners and

Managers

• Cyber Security Engineers

**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](http://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 FAQ’s

Who Should Attend

Re-Certification Requirements

Accreditations



Logo

Description automatically generated





Course and Certification Learning Options

Graphical user interface, application

Description automatically generated





Detailed Outline:

**Course Introduction**

**Module 1 – Introduction to Ethical Hacking**

1. What and Why?
2. Differences
3. Security Definitions
4. Risk Management
5. Methodologies

**Module 2 – Linux Fundamentals**

1. Core Concepts
2. The shell and other items you need to know
3. Managing users
4. Basic Commands

**Module 3 – Protocols**

1. Network Models
2. Protocols & Services

**Module 4 – Cryptography**

1. Understanding Cryptography
2. Symmetric Encryption
3. Asymmetric Encryption
4. Hashing
5. Cryptography in Use
6. Crypto Attacks

**Module 5 – Password Cracking**

1. What and Why
2. Attacks and Tools of the Trade
3. Countermeasures

**Module 6 – Malware**

1. DOS & DDOS
2. Viruses & Backdoors
3. Trojans and Backdoors
4. Ransomeware

**Module 7 – Security Devices**

1. Basic Security Elements
2. Security Appliances

**Module 8 – Information Gathering**

1. What are we looking for?
2. Where/How do we find this information?
3. Are there tools to help?

**Module 9 – Social Engineering**

1. Social Engineering Types
2. Phishing Scams

**Module 10 – Reconnaissance**

1. What are we looking for?
2. Port Scanning
3. Are there tools to help?
4. Banner Grabbing
5. Enumeration

**Module 11 – Vulnerability Assessment**

1. What is a Vulnerability Assessment
2. Tools of the Trade
3. Testing Internal and External Systems

**Module 12 - Network Attacks**

1. Sniffing Techniques
2. Hijacking

**Module 13 – Hacking Servers**

1. Servers, What are they good for?
2. What is an Exploit?
3. Tools of the Trade

**Module 14 – Hacking Web Technologies**

1. OWASP Top 10
2. SQL Injection
3. XSS

**Module 15 – Hacking Wireless Networks**

1. Wireless Technologies
2. Mobile and IoT Technologies
3. Various Tools Used
4. Hacking Techniques
5. Countermeasures

**Module 16 – Maintaining Access and Covering Tracks**

1. Maintaining Access
2. Covering Tracks

Detailed Labs Outline:

**Lab 1 – Intro to C)PEH Setup**

1. Recording Ips and Logging into VMs
2. Joining the Domain

**Lab 2 - Linux Fundamentals**

1. Command Line Tips and Tricks
2. Linux Networking for Beginners
3. Using FTP during a Pentest

**Lab 3 – Understanding Protocols**

1. Analyze http session

**Lab 4 - Cryptography Lab**

1. Hashing Data of all Sorts
2. The Basics of Cryptographic Algorithms

**Lab 5 – Password Cracking**

**Lab 6 - Malware**

1. Creating a virus
2. Beast Trojan

**Lab 7 – Information Gathering**

1. Google Queries
2. Searching Pastebin
3. Maltego
4. People Search Using the Spokeo Online Tool
5. Recon with Chrome
6. Nslookup

**Lab 8 – Information Gathering – Active Reconnaissance**

1. Scanning with Nmap
2. Scanning with Hping
3. Banner Grabbing
4. Enumerating a local System with Hyena
5. SMTP Enumeration
6. Ad Enumeration

**Lab 9 – Vulnerability Assessment**

1. Vulnerability Assessment with Nessus
2. Vulnerability Assessment with Saint

**Lab 10 – Network Sniffing/IDS**

1. Sniffing Passwords with Wireshark
2. Performing MtM with Cain
3. Performing MtM with sslstrip

**Lab 11  - Windows Hacking**

1. Attack Windows 7 with Client-Side Exploit
2. Windows 2012 Reverse TCP Exploit
3. Cracking with John the Ripper

**Lab 12 – Attacking Databases**

1. Attacking MySQL Database
2. Manual SQL Injection

**Lab 13 – Attacking Web Applications**

1. Attacking with XSS
2. Attacking with CSRF

**Lab 13 - Backdoors**

1. Setting up a Backdoor