

# Certified Professional Ethical Hacker



## KEY DATA

**Course Name:** CPEH

**Duration:** 5 days

**Language:** English

**Format:**

Instructor-led Course  
(Lecture and Lab)  
Live Virtual Training

**Prerequisites:**

- A minimum of 12 months experience in networking technologies
- Sound knowledge of TCP/IP
- Computer hardware knowledge
- Knowledge of Microsoft packages
- Network+, Microsoft Security+
- Knowledge of Linux would be beneficial but not essential

**Student Materials:**

- Student Workbook
- Student Reference Manual
- Software/Tools, 3xDVDs

**Certification Exam:**

CPTEngineer – Certified Penetration Testing Engineer

**Certification Track:**

CPEH  
CPTConsultant  
CDFE – Certified Digital Forensics Examiner™

## BENEFITS OF CPEH

As a result of this course, Certified Professional Ethical Hacker graduates will build real world security knowledge that will enable them to recognize vulnerabilities, expose system weaknesses and help safeguard clients against security threats. Graduates will learn the essentials of Ethical Hacking, along with the added professional edge of Penetration Testing.

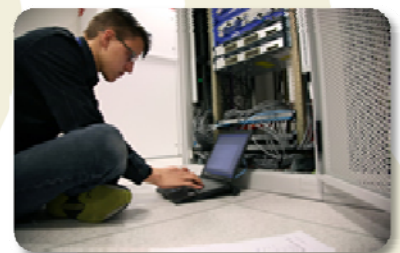
## COURSE OVERVIEW

CPEH is a custom designed course for certain partners in India and Europe. At its core are found time tested Penetration Testing techniques utilized by vulnerability consultants worldwide. As with other courses, mile2 trainers who teach CPEH keep abreast of their expertise by practicing what they teach. Our instructors believe that an equal emphasis should be placed on theoretical and real world experience for effective knowledge transfer to CPEH student.

The PEH training presents information on the latest security vulnerabilities and defenses. This class will also enhance the business skills needed by students to identify protection opportunities, justify testing activities and optimize security controls appropriate to the business needs in order to reduce business risk. As always, mile2 goes far beyond simply teaching you to “Hack” -- the norm with many other courses. Our courses are developed based on principles and methods used by malicious hackers; not by mere topic lists.

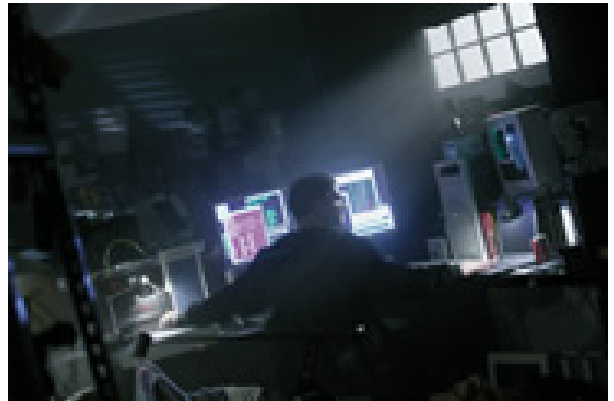
## UPON COMPLETION

Upon completion, CPEH students will be able to confidently undertake the Certified Professional Ethical Hacker exam. Students will enjoy an in-depth course that is continuously updated to maintain and incorporate the ever changing security environment. This course offers up-to-date proprietary laboratories that have been researched and developed by leading security professionals from around the world.



## CPEH COURSE MODULES

- Module 1:** Security Fundamentals
- Module 2:** Access Controls
- Module 3:** Protocols
- Module 4:** Network Attack and Defense
- Module 5:** Cryptography
- Module 6:** Economics and Law
- Module 7:** Reconnaissance
- Module 8:** Scanning and Enumeration
- Module 9:** Gaining Access/Exploitation
- Module 10:** Maintaining Access
- Module 11:** Covering Your Tracks
- Module 12:** Malware
- Module 13:** Buffer Overflows
- Module 14:** Password Cracking Attacks
- Module 15:** Denial of Service
- Module 16:** Attacking Web Technologies and Databases
- Module 17:** Attacking Wireless Devices



## OBJECTIVE OF CPEH LAB SCENARIOS

This is an intensive hands-on class; rather than spend too much time installing 300 tools, our focus will be on the Pen Testing model. The latest Pen Testing Tools and methods will be taught. Laboratories change weekly as new methods are found. Students will using many different tools from GUI to command line. As we work through structured attacks, we try and cover tools for both Windows and Linux systems.

**LIVE VIRTUAL TRAINING is a key training option for potential CPEH students. Join a live class from anywhere in the world!**

- \* Live Presentations offer powerful functionality by delivering delivers easy viewing of slides and other documents, web based collaboration, virtual whiteboard (in some classes), all through an easy-to-use browser based tools.
- \* Students will view live demonstrations, lectures, and participate in live discussions.
- \* Each remotely connecting student is given a dedicated high spec remote PC with full access as if you are sitting in-front of one of the PC's in the classroom lab.
- \* Instructors view each remote student's computer as they perform hands on labs. If necessary the instructor can access the remote students computer to demonstrate and give assistance in true mentor style learning.
- \* Public and private text chat allows for increased interactivity between students and instructor.

## DETAILED MODULE DESCRIPTION

### Module 1 – Security Fundamentals

The Growth of Environments and Security  
 Our Motivation  
 World Bank Hacked  
 UK Hospitals Shut Down  
 80% of Organizations Suffer Breaches  
 3<sup>rd</sup> Quarter of 2008 – What Happened!  
 IC3 2008 Report  
 The Evolving Threat  
 Security Vulnerability Life Cycle  
 Exploit Timeline  
 What to Expect in 2009!  
 The Goal: Protecting Information  
 AIC Triad in Detail

Approach Security Holistically  
 Security Definitions  
 Definitions Relationships  
 Potential Threats, Vulnerabilities and Risks  
 What is a Penetration Test?  
 Types of Penetration Testing  
 Vulnerability Assessment vs Pentest  
 Hacking Life Cycle – A Methodology  
 Methodology for Penetration Testing  
 Hacker vs Penetration Tester  
 Not Just Tools  
 Benefits of a Penetration Test  
 Penetration Testing Methodologies  
 Information Security Standards

Financial Regulations

**Module 2 – Access Controls**

Role of Access Control

Definitions

Categories of Access Controls

Physical Controls

Logical Controls

Administrative Controls

Security Roles

Steps to Granting Access

Access Criteria

Physical Access Control Mechanism

Biometric System Types

Synchronous Token

Asynchronous Token Device

Memory Devices

Smart Card

Cryptographic Keys

Logical Access Controls

OS Access Controls

Linux Access Controls

Accounts and Groups

Password and Shadow File Formats

Account and Groups Details

Linux and UNIX Permissions

Set UID Programs

Trust Relationships

**Module 3 - Protocols**

OSI – Application Layer

OSI – Presentation Layer

OSI – Session Layer

OSI – Transport Layer

OSI – Network Layer

OSI – Data Link

OSI – Physical Layer

Protocols at each OSI Layer

TCP/IP Suite

Port and Protocol Relationship

Conceptual Use of Ports

UDP vs TCP

Address Resolution Protocol

Internet Control Message Protocol

Domain Name Service

Secure Shell

Simple Network Management Protocol

Simple Mail Transfer Protocol

Packet Sniffers

Examples of Packet Sniffers

Wireshark

TCP Stream Re-Assembling

**Module 4 – Network Attack and Defense**

Vulnerabilities in Network Services

Vulnerabilities in Networks

Defense Options

Patch Management Tools

Networking Device – Bastion Host

Defense Against External Scanning

Firewall

Intrusion Detection System

Intrusion Prevention System

Firewall Types

Packet Filtering

Proxy FirewallsCircuit-Level Proxy Firewall

Application-Layer Proxy

Stateful Firewall  
Dynamic Packet Filtering  
Kernel Proxies  
Firewall Placement  
Screened Host  
Multi or Dual Homed  
Screened Subnet  
“New Age” Protection  
IPS Overview  
Spyware Prevention System  
Secure Surfing  
TOR  
Paros Proxy

**Module 5 - Cryptography**

Cryptographic Definitions  
The Science of Secret Communication  
Encryption  
Encryption Algorithm  
Symmetric Encryption  
Symmetric Algorithms  
Symmetric Downfalls  
Asymmetric Encryption  
Asymmetric Advantages  
Asymmetric Disadvantages  
Symmetric vs Asymmetric  
Asymmetric Algorithm Examples  
Diffie-Hellman Key Exchange  
Hybrid Encryption  
Hashing  
Common Hash Algorithms  
Security Issues in Hashing  
Hash Collisions

MD5 Collision Creates Rogue CA  
Birthday Attack  
Salting  
SSL/TLS  
SSL Connection Setup  
SSH  
IPSecPublic Key Infrastructure  
Attacks on Cryptosystems  
Cryptool

**Module 6 – Economics and Law**

Security Incentives and Motivations  
What is Your Weakest Link?  
What will it Cost You?  
What does a Hack Cost?  
What is the Value of an Asset?  
Non-Obvious Examples  
Categorizing Risks  
Examples of Types of Losses  
Approaches to Analyzing Risk  
Who Uses What Analysis Type?  
Qualitative Analysis  
Quantitative Analysis  
Can a Pure Quantitative Analysis be Accomplished?  
Comparing Cost and Benefit  
Cost of a Countermeasure  
Cyber Crime  
CSI Computer Crime Survey  
Classic Example  
Recent Example  
Computer Crime Websites  
Not Just Fun and Games

Examples of Computer Crimes  
Criminal Profiles  
Attack Types  
Telephone Fraud  
Identification Protection and Prosecution  
Privacy of Sensitive Data  
U.S. Laws and Examples  
EU Principles on Privacy  
Transborder Information Flow  
Employee Privacy Issue  
U.S. Law  
Civil Law  
Criminal Law  
Administrative Laws  
U.S. Federal Laws  
Intellectual Property Laws  
Software Licensing  
Digital Millennium Copyright Act  
Investigating  
Computer Crime and Its Barriers  
Countries Working Together  
Generally Accepted System Security Principles  
Violation Analysis  
Bringing in Law Enforcement  
Citizen vs Law Enforcement Investigation  
Investigation of Any Crime  
Role of Evidence in a Trial  
Evidence Requirements  
Chain of Custody  
Evidence Life Cycle  
Evidence Types  
Hearsay Rule Exemption

Incident Response  
Developing an Incident Response Team  
Incident Handling  
Collecting Evidence  
Computer Forensics  
Attempting to Trap the Bad Guy  
Companies Found Liable

**Module 7 - Reconnaissance**

Step One in the Hacking Life Cycle  
What Information does the Hacker want?  
Passive – Active Reconnaissance  
Footprinting Defined  
Methods of Obtaining Information  
Social Access  
Social Engineering Techniques  
Social Networking Sites  
People Search Engines  
WayBack Machine  
Digital Access  
Footprinting Tools Overview  
KartOO Website  
Maltego  
Google Hacking  
Johnny Long  
WHOIS  
Domain Name Registration  
WHOIS Output  
DNS Record Types  
Nslookup  
Dig  
Traceroute  
Netcraft

Blogs, Forums and Newsgroups  
EDGAR  
Companies House  
Domains by Proxy  
Footprinting Countermeasures

**Module 8 – Scanning and Enumeration**

Hacking Life Cycle – Step 2  
Introduction to Port Scanning  
Which Services use which Ports?  
Port Scanning Tips  
Port Scan Should Reveal  
Popular Port Scanning Tools  
Ping  
Stealth Online Ping  
Pinging with NMAP  
TCP 3-way Handshake  
TCP Flags  
TCP Connect Port Scan  
Half-Open Scan  
Firewalled Ports  
UDP Port Scan  
NMAP TCP Connect Scan  
NMAO Service Version Detection  
Look@LANSuperScan  
UnicornScan  
Autoscan  
Enumeration Overview  
Web Server Banners  
SMTP Server Banner  
DNS Enumeration  
SNMP Insecurity  
SNMP Enumeration Tools

SNMP Countermeasure  
Active Directory Enumeration  
LDAPMiner  
Active Directory Countermeasures  
Null Sessions  
Null Session Syntax  
Viewing Shares with Null Sessions  
DumpSec  
Cain and Able  
Null Session Countermeasures

**Module 9 – Gaining Access/Exploitation**

How do Exploits Work?  
Physical Access Attacks  
Lock Picking  
Torque Wrench  
Picks  
Snap Gun  
Electric Pick  
Lock Internal Mechanism  
Pin Tumblers  
Picking  
Binding Pin  
Binding  
Binding Order  
Raking  
Bumping  
Bump Key  
Shimming Door Locks  
Padlocks  
Bypassing Padlocks  
Padlock Shims  
Shock Energy

- Lock Picking Countermeasures
- The Metasploit Project
- SaintExploit
- Core Impact
- Products Compared

### **Module 10 – Maintaining Access**

- Backdoors
- Rootkits
- Linux Rootkits
- Windows Rootkits
- Netcat
- Netcat Switches
- Netcat as a Listener
- Meterpreter

### **Module 11 – Covering Your Tracks**

- Covering Tracks Overview
- Disabling Auditing
- Clearing Event Logs
- Alternate Data Streams
- ADS Countermeasures
- Stream Explorer
- Steganography
- Steganography Tools
- Shredding Files Left Behind
- Leaving No Local Trace
- More Anonymous Software
- StealthSurfer II Privacy Stick
- TOR
- Encrypted Tunnel Notes

### **Module 12 - Malware**

- Malware Types
- Worms, Logic Bomb and Trojan Horse

- Virus
- Types of Viruses
- Spyware
- Trojan Horse
- Rootkits
- Backdoors
- Distributing Malware
- Malware Capabilities
- Auto Starting Malware
- HijackThis Tool
- Executable Wrappers
- EXE's Historically wrapped with Trojans
- Restorator
- EXE Icon
- Infectious CD-ROM Technique
- Historical Trojans
- How Trojans Avoid Detection
- The Basic Manipulation Tool Kit
- Malware Countermeasures
- Gargoyle Investigator
- Spy Sweeper Enterprise
- Port Monitoring Software
- File Protection Software
- Windows Software Restriction Policies
- Hardware Based Malware Detectors
- User Education

### **Module 13 – Buffer Overflows**

- Buffer Overflow Definition
- Basic Example
- Buffer Overflows – Overview
- Memory Organization
- How Buffers and Stacks are suppose to work!

Stack Function

How a Buffer Overflow Works!

Secure Code Reviews

Secure Code Review Process

Know the Vulnerabilities

Know the Business Risks

When to Conduct the Code Review

Who Should Be Involved

What To Look For

Fixing the Issues

Automated Tools

Prevention

#### **Module 14 – Password Cracking Attacks**

Attack Vectors

Keystroke Loggers

Password Recovery Options

UNIX Passwords and Encryption

Linux/UNIX Password Cracking Tools

NAT Dictionary Attack Tool

THC-Hydra

Cracking Windows Passwords

Tsgrinder

Hashes in a Windows System

LM Hash

NT Hash

Syskey Encryption

Creating Rainbow Tables

Downloading Rainbow Tables

NTPASSWD

Password Sniffing

Kerbsniff and Kerbcrack

Cracking Passwords with Cain and Able

#### **Module 15 – Denial of Service**

DDoS issues

Stachledraht DDoS Attack

DDoS

Zombie Definition

DDoS Attack Types

WiFi DoS

Evading the Firewall and IDS

Evasive Techniques

Firewall – Normal Operation

Firewall – Evasive Technique

Evading with Encrypted Tunnel

Man-in-the-Middle Attacks

ARP Cache Poisoning

ARP Cache Poisoning with Linux

ARP Cache Poisoning with Windows

Ettercap

ARP Cache Poisoning Countermeasures

DNS Spoofing

DNS Spoofing Tools

Breaking SSL Traffic

Tools for Breaking SSL and SSH

VoIP Notes

Session Hijacking

#### **Module 16 – Attacking Web Technologies and Databases**

Web Server Market Share

Common Security Threats

OWASP Top 10

Anatomy of a Web App Attack

Components of a Generic Web App

URL Mappings

Older Web Attack Techniques  
Changing URL Login Parameters  
Cookies  
Cross-Site Scripting  
XSS Illustrated  
Reflected XSS Illustrated  
Business Impacts of XSS  
Finding and Fixing XSS  
Injection Flaws  
Unvalidated Input  
Unvalidated Input Illustrated  
Business Impacts of Unvalidated Input  
Finding and Fixing Unvalidated Input  
Attacks Against IIS  
IIS Directory Traversal  
Unicode Issues  
IIS Logs  
N-Stalker  
NTOSpider  
HTTrack Website Copier  
Wikto  
Paros Proxy  
Burp Proxy  
Brutus  
Dictionary Maker  
Query String  
Fuzzers  
Acunetix Web Scanner  
Eclipse  
OWASP WebScarab  
Samurai  
OWASP Assessment Template

Attacking Databases Overview  
Database Server Overview  
Types of Databases  
Vulnerabilities and Common Attacks  
SQL Injection  
Business Impacts of SQL Injection  
Why SQL Injection?  
Database Enumeration  
SQL Extended Stored Procedures  
Direct Attacks  
SQL Connection Properties  
Obtaining Sensitive Information  
SQL Ping2  
OSQL.EXE  
Query Analyzer  
SQLExec  
Pete Finnegan  
Metasploit Again?  
Finding and Fixing SQL

### **Module 17 – Attacking Wireless Devices**

WiFi Network Types  
Widely Deployed Standards  
Standards Comparison  
802.11n - MIMO  
SSID  
MAC Filtering  
WEP  
Weak IV Packets  
XOR - Basics  
WEP Weaknesses  
WPA Improvements on WEP  
TKIP

WPA MIC Vulnerability

802.11i – WPA2

WPA/WPA2 Mode Types

WPA-PSK Encryption

LEAP

LEAP Weaknesses

Hidden Node

Hidden Node Solutions

Near/Far Issue

Near/Far Solution

NetStumbler

KNSGEM

Vistumbler

Kismet

Omnipeek Personal

Eavesdropping

Aircrack-ng Suite

Airodump-ng

Aireplay-ng

DoS

Deauthentication/Disassociation Attack

Rogue Access Point

Aircrack-ng

Aircrack for Windows

Attacking WEP

Attacking WPA

coWPAtty

Exploiting Cisco LEAP

asleep

[www.wirelessdefence.org](http://www.wirelessdefence.org)

Typical Wireless Network

802.1X: EAP Types

EAP Advantages/Disadvantages

EAP/TLS Deployment

New Age Protection