



## Certified Professional Ethical Hacker

Duration: 5 Days

Language: English

Course Delivery: Classroom

### COURSE BENEFITS

The **Certified Professional Ethical Hacker** vendor neutral certification course is the foundational training to mile2's line of penetration testing courses.

The **CPEH** certification training enables students to understand the importance of vulnerability assessments by providing industry knowledge and skills in Vulnerability Assessments. In doing so, the CPEH student is able to understand how malware and destructive viruses function. In addition, the CPEH course helps students learn how to implement counter response and preventative measures when it comes to a network hack.

The **CPEH** course provides in-depth labs that focus on both open source and commercial based tools with industry best practices. These hands on labs emulate real world hacking scenarios and equip the candidate to assess your company's security posture, help implement controls to better secure your company's network infrastructure and how to combat against hackers and/or viruses, etc.

### Examination

The **Certified Professional Ethical Hacker** exam is taken online through Mile2's Assessment and Certification System ("MACS"), which is accessible on your mile2.com account. The exam will take 2 hours and consist of 100 multiple-choice questions.

### Course Outline

#### Module 1 - Security Fundamentals

Overview

The Growth of

Environments and Security

Our Motivation...

The Goal: Protecting Information!

CIA Triad in Detail

Approach Security Holistically

Security Definitions

Definitions Relationships

Method: Ping

The TCP/IP Stack

Which Services Use Which Ports?

TCP 3-Way Handshake

TCP Flags

Malware

Types of Malware

Types of Malware Cont...

Types of Viruses

More Malware: Spyware



Trojan Horses  
Back Doors  
DoS  
DDoS  
Packet Sniffers  
Passive Sniffing  
Active Sniffing  
Firewalls, IDS and IPS  
Firewall - First  
Line of Defense  
IDS - Second Line of Defense  
IPS - Last Line of Defense?  
Firewalls  
Firewall Types:  
(1) Packet Filtering  
Firewall Types:  
(2) Proxy Firewalls  
Firewall Types -  
Circuit-Level Proxy Firewall  
Type of Circuit-  
Level Proxy - SOCKS  
Firewall Types -  
Application-Layer Proxy  
Firewall Types: (3) Stateful  
Firewall Types:  
(4) Dynamic Packet-Filtering  
Firewall Types:  
(5) Kernel Proxies  
Firewall Placement  
Firewall Architecture  
Types - Screened Host  
Multi- or Dual-Homed  
Screened Subnet  
Wi-Fi Network Types  
Wi-Fi Network Types  
Widely Deployed Standards  
Standards Comparison  
802.11n - MIMO  
Overview of Database Server  
Review

## **Module 2 - Access Controls**

Overview  
Role of Access Control  
Definitions  
More Definitions  
Categories of Access Controls  
Physical Controls  
Logical Controls  
"Soft" Controls  
Security Roles  
Steps to Granting Access  
Access Criteria



Physical Access  
Control Mechanisms  
Biometric System Types  
Synchronous Token  
Asynchronous Token Device  
Memory Cards  
Smart Card  
Cryptographic Keys  
Logical Access Controls  
OS Access Controls  
Linux Access Controls  
Accounts and Groups  
Password &  
Shadow File Formats  
Accounts and Groups  
Linux and UNIX Permissions  
Set UID Programs  
Trust Relationships  
Review

### **Module 3 - Protocols**

Protocols Overview  
OSI - Application Layer  
OSI - Presentation Layer  
OSI - Session Layer  
Transport Layer  
OSI - Network Layer  
OSI - Data Link  
OSI - Physical Layer  
Protocols at  
Each OSI Model Layer  
TCP/IP Suite  
Port and Protocol Relationship  
Conceptual Use of Ports  
UDP versus TCP  
Protocols - ARP  
Protocols - ICMP  
Network Service - DNS  
SSH Security Protocol  
SSH  
Protocols - SNMP  
Protocols - SMTP  
Packet Sniffers  
Example Packet Sniffers  
Review

### **Module 4 -Cryptography**

Overview  
Introduction  
Encryption  
Cryptographic Definitions  
Encryption Algorithm  
Implementation



Symmetric Encryption  
Symmetric Downfalls  
Symmetric Algorithms  
Crack Times  
Asymmetric Encryption  
Public Key  
Cryptography Advantages  
Asymmetric  
Algorithm Disadvantages  
Asymmetric  
Algorithm Examples  
Key Exchange  
Symmetric versus Asymmetric  
Using the  
Algorithm Types Together  
Instructor Demonstration  
Hashing  
Common Hash Algorithms  
Birthday Attack  
Example of a Birthday Attack  
Generic Hash Demo  
Instructor Demonstration  
Security Issues in Hashing  
Hash Collisions  
MD5 Collision Creates  
Rogue Certificate Authority  
Hybrid Encryption  
Digital Signatures  
SSL/TLS  
SSL Connection Setup  
SSL Hybrid Encryption  
SSH  
IPSec - Network Layer Protection  
IPSec  
IPSec  
Public Key Infrastructure  
Quantum Cryptography  
Attack Vectors  
Network Attacks  
More Attacks (Cryptanalysis)  
Review

## **Module 5 - Why Vulnerability Assessments**

Overview  
What is a  
Vulnerability Assessment?  
Vulnerability Assessment  
Benefits of a  
Vulnerability Assessment  
What are Vulnerabilities?  
Security Vulnerability Life Cycle  
Compliance and Project Scoping



The Project  
Overview Statement  
Project Overview Statement  
Assessing Current  
Network Concerns  
Vulnerabilities in Networks  
More Concerns  
Network Vulnerability  
Assessment Methodology  
Network Vulnerability  
Assessment Methodology  
Phase I: Data Collection  
Phase II: Interviews, Information Reviews, and Hands-On Investigation  
Phase III: Analysis  
Analysis cont.  
Risk Management  
Why Is Risk  
Management Difficult?  
Risk Analysis Objectives  
Putting Together  
the Team and Components  
What Is the Value of an Asset?  
Examples of Some Vulnerabilities that Are Not Always Obvious  
Categorizing Risks  
Some Examples  
of Types of Losses  
Different Approaches  
to Analysis  
Who Uses What?  
Qualitative Analysis Steps  
Quantitative Analysis  
ALE Values Uses  
ALE Example  
ARO Values and Their Meaning  
ALE Calculation  
Can a Purely Quantitative Analysis Be Accomplished?  
Comparing Cost and Benefit  
Countermeasure Criteria  
Calculating Cost/Benefit  
Cost of a Countermeasure  
Can You Get Rid of All Risk?  
Management's Response to Identified Risks  
Liability of Actions  
Policy Review  
(Top-Down) Methodology  
Definitions  
Policy Types  
Policies with Different Goals  
Industry Best  
Practice Standards  
Components that Support the Security Policy  
Policy Contents  
When Critiquing a Policy



Technical (Bottom-Up)  
Methodology  
Review

## **Module 6 - Vulnerability Tools of the Trade**

### **Overview**

Vulnerability Scanners

Nessus

SAINT - Sample Report

Tool: Retina

Qualys Guard

<http://www.qualys.com/products/overview/>

Tool: LANguard

Microsoft Baseline Analyzer

MBSA Scan Report

Dealing with Assessment Results

Patch Management Options

Review

## **Module 7 - Output Analysis and Reports**

Overview

Staying Abreast: Security Alerts

Vulnerability Research Sites

Nessus

SAINT

SAINT Reports

GFI Languard

GFI Reports

MBSA

MBSA Reports

Review

## **Module 8 - Reconnaissance, Enumeration and Scanning**

Reconnaissance Overview

Step One in the

Hacking "Life-Cycle"

What Information is

Gathered by the Hacker?

Passive vs. Active Reconnaissance

Footprinting Defined

Social Access

Social Engineering Techniques

Social Networking Sites

People Search Engines

Internet Archive:

The WayBack Machine

Footprinting Tools Overview

Maltego GUI

Johnny.Ihackstuff.com

Google (cont.)

Domain Name Registration

WHOIS Output



DNS Databases  
Using Nslookup  
Traceroute Operation  
Web Server Info Tool: Netcraft  
Introduction to Port Scanning  
Which Services  
use Which Ports?  
Port Scan Tips  
Port Scans Should Reveal...  
Popular Port Scanning Tools  
Ping (Is the host online?)  
Stealth Online Ping  
TCP 3-Way Handshake  
TCP Flags  
TCP Connect Port Scan  
Half-open Scan (SynScan)  
Firewalled Ports  
NMAP TCP Connect Scan  
Enumeration Overview  
Web Server Banners  
HTTPrint  
DNS Enumeration  
SNMP Insecurity  
SNMP Enumeration Tools  
SNMP Enumeration Countermeasures  
Active Directory Enumeration  
LDAPMiner  
AD Enumeration Countermeasures  
Null Sessions  
Viewing Shares  
Tool: DumpSec  
Tool: Enumeration  
with Cain and Abel  
Null Session  
Countermeasures (cont.)  
Review

## **Module 9 - Gaining Access**

Overview  
How Do Exploits Work?  
Physical Access Attacks  
Lock Picking  
Tool Kit: Torque Wrench  
Tool Kit: Picks  
Tool Kit: Snap Gun  
Tool Kit: Electric Pick  
Internal Mechanism  
Pin Tumblers  
Pin Tumblers  
Picking  
Binding Pin  
Binding  
Binding



Binding Order  
Raking  
Raking  
Bumping  
Bump Keying  
Shimming Door Locks  
Padlocks  
Bypassing  
Padlock Shims  
Shock Energy  
Lock Picking Countermeasures  
The Metasploit Project  
Defense in Depth  
Instructor Demonstration  
SaintExploit at a Glance  
SaintExploit Interface  
Core Impact Overview  
Core Impact  
Review

#### **Module 10 - Maintaining Access**

Overview  
Back Doors  
Backdoor via Rootkits  
Linux Backdoor via Rootkits  
Linux Backdoor via Rootkits  
Windows RootKit Countermeasures  
Tool: Netcat  
Netcat Switches  
Netcat as a Listener  
Meterpreter  
Review

#### **Module 11 - Covering Tracks**

Overview  
Covering Tracks Overview  
Disabling Auditing  
Clearing and Event Log  
Hiding Files with  
NTFS Alternate Data Stream  
NTFS Streams  
Countermeasures  
Stream Explorer  
What is Steganography?  
Steganography Tools  
Shedding Files Left Behind  
Leaving No Local Trace  
More Anonymous Software  
StealthSurfer II Privacy Stick  
Tor: Anonymous Internet Access  
Encrypted Tunnel Notes  
Review





## Module 12 - Malware

Overview  
Distributing Malware  
Malware Capabilities  
Countermeasure: Monitoring Autostart Methods  
Tool: Netcat  
Netcat Switches  
Netcat as a Listener  
Executable Wrappers  
Benign EXE's Historically Wrapped with Trojans  
Tool: Restorator  
Tool: Exe Icon  
The Infectious CD-Rom Technique  
Trojan: Backdoor.Zombam.B  
Trojan: JPEG GDI+ All in One Remote Exploit  
Advanced Trojans: Avoiding Detection  
BPMTK  
Malware Countermeasures  
Gargoyle Investigator  
Spy Sweeper Enterprise  
CM Tool: Port Monitoring Software  
CM Tools: File Protection Software  
CM Tool: Windows File Protection  
CM Tool: Windows Software Restriction Policies  
CM Tool: Hardware Malware Detectors  
Countermeasure: User Education  
Review

## Module 13 - Buffer Overflows

Overview  
Buffer Overflow Definition  
Overflow Illustration  
Buffer Overflows  
Memory Organization  
How Buffers and Stacks  
Are Supposed to Work  
Stack Function  
How a Buffer Overflow Works  
Buffer Overflows  
Secure Code Review  
Prevention  
Review

## Module 14 - Password Cracking

Overview  
Attack Vectors  
Unix Passwords and Encryption  
Password Cracking Tools  
NAT Dictionary Attack Tool  
THC-Hydra  
Password Guessing  
Password Cracking  
LM/NTLM Hashes



LM Hash Encryption  
NT Hash Generation  
Windows Syskey Encryption  
Creating Rainbow Tables  
Free Rainbow Tables  
NTPASSWD:Hash Insertion Attack  
Password Sniffing  
Sniffing Remote Passwords  
Tool: Cain and Abel  
Review

## **Appendix 1 - Economics and Law**

Overview  
Attack Vectors  
Unix Passwords and Encryption  
Password Cracking Tools  
NT Dictionary Attack Tool  
THC-Hydra  
Password Guessing  
Password Cracking  
LM/NTLM Hashes  
LM Hash Encryption  
NT Hash Generation  
Windows Syskey Encryption  
Creating Rainbow Tables  
Free Rainbow Tables  
NTPASSWD:Hash Insertion Attack  
Password Sniffing  
Sniffing Remote Passwords  
Tool: Cain and Abel  
Review

## **Appendix 2 - Vulnerability Types**

Overview  
Critical Vulnerabilities  
Critical Vulnerability Types  
Buffer Overflows  
URL Mappings  
to Web Applications  
IIS Directory Traversal  
Format String Attacks  
Default Passwords  
Misconfigurations  
Known Backdoors  
Information Leaks  
Memory Disclosure  
Network Information  
Version Information  
Path Disclosure  
User Enumeration  
Denial of Service  
Best Practices  
Review



Lab

### **Appendix 3 - Assessing Web Servers**

Web Servers

Fingerprinting

Accessible Web Servers

Identifying and Assessing

Reverse Proxy Mechanisms

Proxy Mechanisms

Identifying Subsystems

and Enabled Components

Basic Web Server Crawling

Web Application

Technologies Overview

Web Application Profiling

HTML Sifting and Analysis

Active Backend

Database Technology Assessment

Why SQL "Injection"?

Web Application

Attack Strategies

Web Application Vulnerabilities

Authentication Issues

Parameter Modification

SQL Injection: Enumeration

SQL Extended Stored Procedures

Shutting Down SQL Server

Direct Attacks

SQL Connection Properties

Attacking Database Servers

Obtaining Sensitive Information

URL Mappings

to Web Applications

Query String

Changing URL Login Parameters

URL Login Parameters Cont.

IIS Directory Traversal

Cross-Site Scripting (XSS)

Web Security Checklist

Review

### **Appendix 4 - Assessing Remote & VPN Services**

Assessing Remote & VPN Services

Remote Information Services

Retrieving DNS

Service Version Information

DNS Zone Transfers

Forward DNS Grinding

Finger

Auth

NTP

SNMP

Default Community Strings



LDAP  
rwho  
RPC rusers  
Remote Maintenance Services

FTP  
SSH  
Telnet  
X Windows  
Citrix  
Microsoft Remote  
Desktop Protocol  
VNC  
Assessing IP VPN Services  
Microsoft PPTP  
SSL VPNs  
Review

## **Appendix 5 - Denial of Service**

Overview  
DDoS Issues  
DDoS  
Zombie Definition  
DDoS Attack Types  
Wifi Denial of Service (DoS)  
Evading The Firewall and IDS  
Evasive Techniques  
Firewall - Normal Operation  
Evasive Technique -Example  
Evading With Encrypted Tunnels  
Man-in-the-middle Attacks  
ARP Cache Poisoning  
ARP Normal Operation  
ARP Cache Poisoning  
ARP Cache Poisoning (Linux)  
Tool: Cain and Abel  
Ettercap  
Countermeasures  
What is DNS spoofing?  
Tools: DNS Spoofing  
Breaking SSL Traffic  
Tool: Breaking SSL Traffic  
Tool: Cain and Abel  
Voice over IP (VoIP)  
Intercepting VoIP  
Session Hijacking  
Review