



Certified Practical Ethical Hacker (CPEH) Training Syllabus and Exam Overview

*Date: May 1st, 2021
Version 1.0*

Exam Overview

The CPEH exam is a one-of-a-kind ethical hacking certification exam that assesses a student's ability to perform an external and internal network penetration test at a professional level. Students will have **five (5) full days** to complete the assessment and an **additional two (2) days** to write a professional report.

To receive the certification, a student must:

- Perform Open-Source Intelligence (OSINT) to gather intel on how to properly attack the network
- Leverage their Active Directory exploitation skillsets to perform A/V and egress bypassing, lateral and vertical network movements, and ultimately compromise the exam Domain Controller
- Provide a detailed, professionally written report
- Perform a live 15-minute report debrief in front of our assessors, comprised of all senior penetration testers

Training Overview

The CPEH Training consists of five (5) full-length video courses designed to take a student with little to no background in ethical hacking to being able to pass the exam and earn the certification. Upon purchase, the student will automatically be enrolled in the TCM Academy (<https://academy.tcm-sec.com>) and be provided access to the following courses (please click on any link below to read further information about the courses):

- [Practical Ethical Hacking](#) (25 hours)
- [Open-Source Intelligence \(OSINT\) Fundamentals](#) (9 hours)
- [External Pentest Playbook](#) (3.5 hours)
- [Linux Privilege Escalation for Beginners](#) (6.5 hours)
- [Windows Privilege Escalation for Beginners](#) (7 hours)

In total, the student will receive over 50+ hours of video training. We strongly recommend that the courses be taken in the order listed above.

In addition to the course videos, students will have access to the course Discord, which provides a place to ask course related questions, receive assistance/troubleshooting, and network with other students and cybersecurity professionals. At the time of this writing, the Discord has over 25,000 active members and the training courses have over 200,000 enrollments.

Starting on the next page, you can review the Table of Contents, which includes the topics and sub-topics for each course provided with the CPEH training option.

Table of Contents

Table of Contents	3
Practical Ethical Hacking – 25 Hours	16
Introduction	17
Course Introduction.....	17
Course Discord	17
FAQ - Important.....	17
A Day in the Life of an Ethical Hacker.....	17
Notekeeping.....	17
Part 1 – Effective Notekeeping	17
Part 2 – Important Tools.....	17
Networking Refresher.....	17
Introduction	17
IP Addresses	17
MAC Addresses.....	17
TCP, UDP, and the Three-Way Handshake	17
Common Ports and Protocols.....	17
The OSI Model	17
Subnetting Part 1	17
Subnetting Part 2	17
Setting Up Our Lab.....	17
Installing VMWare / VirtualBox.....	17
Installing Kali Linux	17
Introduction to Linux.....	17
Exploring Kali Linux.....	17
Sudo Overview	17
Navigating the File System	17
Users and Privileges.....	17
Common Network Commands	17
Network Commands Update	17
Installing and Updating Tools	17
Installing gedit.....	17
Viewing, Creating, and Editing Files	17
Scripting with Bash	17
Introduction to Python	18
Introduction	18
Strings.....	18
Math.....	18
Variables and Methods	18

Functions	18
Boolean Expressions.....	18
Rational and Boolean Operators.....	18
Conditional Statements	18
Lists.....	18
Tuples.....	18
Looping	18
Important Modules.....	18
Advanced Strings.....	18
Dictionaries.....	18
Sockets	18
Building a Port Scanner	18
The Ethical Hacker Methodology.....	18
The Five Stages of Ethical Hacking.....	18
Information Gathering (Reconnaissance).....	18
Passive Reconnaissance Overview	18
Identifying Our Target.....	18
Email Gathering with Hunter.io	18
Gathering Breached Credentials with Breach-Parse.....	18
Using theharvester	18
Hunting Subdomains Part 1	18
Hunting Subdomains Part 2	18
Identifying Website Technologies.....	18
Information Gathering with Burp Suite	18
Google Fu.....	18
Utilizing Social Media	18
Scanning & Enumeration	18
Installing Kioptrix.....	18
Scanning with Nmap	18
Enumerating HTTP and HTTPS Part 1.....	18
Enumerating HTTP and HTTPS Part 2.....	18
Enumerating SMB	18
Enumerating SSH	18
Researching Potential Vulnerabilities	18
Our Notes So Far	18
Additional Scanning Tools.....	19
Scanning with Masscan	19
Scanning with Metasploit	19
Scanning with Nessus Part 1.....	19
Scanning with Nessus Part 2.....	19

Exploitation Basics	19
Reverse Shells vs Bind Shells	19
Staged vs Non-Staged Payloads.....	19
Gaining Root with Metasploit	19
Manual Exploitation	19
Brute Force Attacks.....	19
Credential Spraying and Password Stuffing	19
Our Notes, Revisited	19
Mid-Course Capstone	19
Introduction	19
Walkthrough - Legacy.....	19
Walkthrough - Lame.....	19
Walkthrough - Blue.....	19
Walkthrough - Devel.....	19
Walkthrough - Jerry.....	19
Walkthrough - Nibbles.....	19
Walkthrough - Optimum.....	19
Walkthrough - Bashed.....	19
Walkthrough - Grandpa.....	19
Walkthrough - Netmon.....	19
Introduction to Exploit Development (Buffer Overflows).....	19
Required Installations.....	19
Buffer Overflows Explained.....	19
Spiking	19
Fuzzing.....	19
Finding the Offset.....	19
Overwriting the EIP	19
Finding Bad Characters	19
Finding the Right Module.....	19
Generating Shellcode and Gaining Root.....	19
Exploit Development Using Python3 and Mona	19
Active Directory Overview	20
Active Directory Overview.....	20
Physical Active Directory Components.....	20
Logical Active Directory Components.....	20
Active Directory Lab Build	20
Lab Overview and Requirements	20
Downloading Necessary ISOs.....	20
Setting Up the Domain Controllers.....	20
Setting Up the User Machines.....	20

Setting Up Users, Groups, and Policies	20
Joining Our Machines to the Domain	20
Attacking Active Directory: Initial Attack Vectors	20
Introduction	20
LLMNR Poisoning Overview	20
Capturing NTLMv2 Hashes with Responder	20
Password Cracking with Hashcat	20
LLMNR Poisoning Defenses	20
SMB Relay Attacks Overview	20
Quick Lab Update	20
Discovering Hosts with SMB Signing Disabled	20
SMB Relay Attack Demonstration Part 1	20
SMB Relay Attack Demonstration Part 2	20
SMB Relay Attack Defenses	20
Gaining Shell Access	20
IPv6 Attacks Overview	20
Installing mitm6	20
Setting Up LDAPS	20
IPv6 DNS Takeover via mitm6	20
IPv6 Attack Defenses	20
Other Attack Vectors and Strategies	20
Credential Spraying and Password Stuffing	20
Our Notes, Revisited	20
Attacking Active Directory: Post-Compromise Enumeration	20
Introduction	20
PowerView Overview	20
Domain Enumeration with PowerView	20
Bloodhound Overview and Setup	20
Grabbing Data with Invoke-Bloodhound	20
Enumerating Domain Data with Bloodhound	20
Attacking Active Directory: Post-Compromise Attacks	21
Introduction	21
Pass the Hash / Password Overview	21
Installing crackmapexec	21
Pass the Password Attacks	21
Dumping Hashes with secretsdump.py	21
Cracking NTLM Hashes with Hashcat	21
Pass the Hash Attacks	21
Pass Attack Mitigations	21
Token Impersonation Overview	21
Token Impersonation with Incognito	21

Token Impersonation Mitigation	21
Kerberoasting Overview	21
Kerberoasting Walkthrough.....	21
Kerberoasting Mitigation	21
GPP / cPassword Attacks Overview	21
Abusing GPP: Part 1	21
Abusing GPP: Part 2	21
Mimikatz Overview	21
Credential Dumping with Mimikatz.....	21
Golden Ticket Attacks	21
Conclusion and Additional Resources	21
Post Exploitation	21
Introduction	21
File Transfers Review	21
Maintaining Access Overview	21
Pivoting Lab Setup	21
Pivoting Walkthrough	21
Cleaning Up.....	21
Web Application Enumeration, Revisited.....	21
Introduction	21
Installing Go.....	21
Finding Subdomains with Assetfinder	21
Finding Subdomains with Amass	21
Finding Alive Domains with Httprobe.....	21
Screenshotting Websites with GoWitness.....	21
Automating the Enumeration Process	21
Testing the Top 10 Web Application Vulnerabilities.....	22
Introduction	22
The OWASP Top 10 and OWASP Testing Checklist.....	22
Installing OWASP Juice Shop.....	22
Installing Foxy Proxy	22
Exploring Burp Suite.....	22
Introducing the Score Board.....	22
SQL Injection Attacks Overview	22
SQL Injection Walkthrough	22
SQL Injection Defenses.....	22
Broken Authentication Overview and Defenses.....	22
Testing for Broken Authentication.....	22
Sensitive Data Exposure Overview and Defenses.....	22
Testing for Sensitive Data Exposure	22
XML External Entities (XXE) Overview	22

XXE Attack and Defense	22
Broken Access Control Overview	22
Broken Access Control Walkthrough.....	22
Security Misconfiguration Attacks and Defenses	22
Cross-Site Scripting (XSS) Overview	22
Reflected XSS Walkthrough.....	22
Stored XSS Walkthrough.....	22
Preventing XSS	22
Insecure Deserialization	22
Using Components with Known Vulnerabilities.....	22
Insufficient Logging and Monitoring.....	22
Wireless Penetration Testing	22
Wireless Penetration Testing Overview.....	22
WPA PSK Exploit Walkthrough.....	22
Legal Documents and Report Writing	22
Common Legal Documents	22
Pentest Report Writing.....	22
Reviewing a Real Pentest Report.....	22
Career Advice	22
Career Advice.....	22
Open-Source Intelligence (OSINT) Fundamentals – 9 Hours	23
Introduction.....	23
Course Introduction.....	23
Course Discord	23
Important Disclaimer	23
OSINT Overview.....	23
What is OSINT?.....	23
Note Keeping	23
Taking Effective Notes	23
Sock Puppets	23
Introduction to Sock Puppets	23
Creating Sock Puppets.....	23
Search Engine OSINT	23
Search Engine Operators.....	23
Image OSINT	23
Reverse Image Searching.....	23
Viewing EXIF Data.....	23
Physical Location OSINT	23
Identifying Geographical Locations.....	23

Where in the World...Part 1	23
Where in the World...Part 2	23
Email OSINT	23
Discovering Email Addresses	23
Password OSINT.....	23
Introduction to Password OSINT.....	23
Hunting Breached Password Part 1.....	23
Hunting Breached Passwords Part 2	23
Username OSINT	24
Hunting Usernames and Accounts.....	24
People OSINT	24
Searching for People.....	24
Voter Records	24
Hunting Phone Numbers	24
Discovering Birthdates.....	24
Searching for Resumes.....	24
Social Media OSINT	24
Twitter OSINT Part 1.....	24
Twitter OSINT Part 2.....	24
Twitter OSINT Part 3.....	24
Facebook OSINT	24
Instagram OSINT	24
Snapchat OSINT	24
Reddit OSINT	24
LinkedIn OSINT	24
TikTok OSINT	24
Website OSINT	24
Website OSINT Part 1.....	24
Website OSINT Part 2.....	24
Website OSINT Part 3.....	24
Business OSINT	24
Hunting Business Information.....	24
Wireless OSINT	24
Wireless OSINT	24
Building an OSINT Lab.....	24
Building an OSINT Lab Part 1	24
Building an OSINT Lab Part 2	24
Building an OSINT Lab Part 3	24
Working with OSINT Tools	25

Introduction	25
Image and Location OSINT	25
Hunting Emails and Breached Data.....	25
Username and Account OSINT	25
Phone Number OSINT	25
Social Media OSINT.....	25
Website OSINT.....	25
Exploring OSINT Frameworks	25
Other Tools.....	25
OSINT Automation Foundations	25
Automating Website OSINT.....	25
Course Challenge.....	25
Course Challenge Overview	25
Course Challenge	25
Course Challenge Walkthrough.....	25
OSINT Report Writing.....	25
Writing an OSINT Report	25
Conclusion & Additional Resources	25
Conclusion & Additional Resources	25
External Pentest Playbook – 3.5 Hours	26
Introduction.....	26
Course Introduction.....	26
Course Discord	26
Before We Start	26
Objectives of an External Pentest	26
Checklists, FTW	26
Rules of Engagement.....	26
Verifying Scope	26
Client Communications.....	26
Kicking Off.....	26
Attack Strategy	26
Vulnerability Scanning	26
Reviewing & Extracting Information	26
Information Gathering / OSINT	26
Overview.....	26
Hunting Breached Credentials	26
Identifying Employees & Emails	26
Enumerating Valid Accounts (Pre-Attack)	26
Other Useful Information	26
Attacking Login Portals.....	26

Overview & Strategy	26
Attacking O365.....	26
Attacking OWA	26
Attacking Other Portals	26
Bypassing MFA	26
Escalating Access	26
Strategy & Walkthrough.....	26
Report Writing.....	26
Report Writing.....	26
Common Pentest Findings.....	27
Overview.....	27
Insufficient Authentication Controls.....	27
Weak Password Policy	27
Insufficient Patching	27
Default Credentials	27
Insufficient Encryption	27
Information Disclosure.....	27
Username Enumeration.....	27
Default Web Pages.....	27
Open Mail Relays.....	27
IKE Aggressive Mode.....	27
Unexpected Perimeter Services	27
Insufficient Traffic Blocking	27
Undetected Malicious Activity.....	27
Historical Account Compromises	27
Wrapping Up.....	27
Client Debriefs.....	27
Attestation Letters.....	27
Client Retests	27
Conclusion.....	27
Course Conclusion	27
Linux Privilege Escalation for Beginners – 6.5 Hours	28
Introduction.....	28
Course Introduction.....	28
Course Discord	28
Course Tips & Resources.....	28
Lab Overview & Initial Access	28
Lab Overview & Initial Access.....	28
Initial Enumeration	28
System Enumeration.....	28

User Enumeration	28
Network Enumeration	28
Password Hunting	28
Exploring Automated Tools	28
Introduction	28
Exploring Automated Tools	28
Escalation Path: Kernel Exploits	28
Kernel Exploits Overview	28
Escalation via Kernel Exploit	28
Escalation Path: Passwords & File Permissions	28
Overview	28
Escalation via Stored Passwords	28
Escalation via Weak File Permissions	28
Escalation via SSH Keys	28
Escalation Path: Sudo	28
Sudo Overview	28
Escalation via Sudo Shell Escaping	28
Escalation via Intended Functionality	28
Escalation via LD_PRELOAD	28
Challenge Overview	28
Challenge Walkthrough	28
CVE-2019-14287 Overview	29
Escalation via CVE-2019-14287	29
Overview and Escalation via CVE-2019-18634	29
Escalation Path: SUID	29
SUID Overview	29
Gaining a Foothold	29
Escalation via SUID	29
Escalation Path: Other SUID Escalation	29
Escalation via Shared Object Injection	29
Escalation via Binary Symlinks	29
Escalation via Environmental Variables	29
Escalation Path: Capabilities	29
Capabilities Overview	29
Escalation via Capabilities	29
Escalation Path: Scheduled Tasks	29
Cron & Timers Overview	29
Escalation via Cron Paths	29
Escalation via Cron Wildcards	29
Escalation via Cron File Overwrites	29

Challenge Overview	29
Challenge Walkthrough.....	29
Escalation Path: NFS Root Squashing	29
Overview & Escalation via NFS Root Squashing	29
Escalation Path: Docker	29
Overview.....	29
Gaining a Foothold	29
Escalation via Docker.....	29
Capstone Challenge	30
Capstone Overview.....	30
Capstone Walkthrough #1.....	30
Capstone Walkthrough #2.....	30
Capstone Walkthrough #3.....	30
Capstone Walkthrough #4.....	30
Capstone Walkthrough #5.....	30
Wrapping Up.....	30
Conclusion	30
Windows Privilege Escalation for Beginners – 7 Hours	31
Introduction.....	31
Course Introduction.....	31
Course Discord	31
Resources & Tips for Success.....	31
Gaining a Foothold	31
Introduction	31
Gaining a Foothold (Box 1)	31
Initial Enumeration	31
System Enumeration.....	31
User Enumeration	31
Network Enumeration	31
Password Hunting	31
AV Enumeration.....	31
Exploring Automated Tools	31
Automated Tools Overview	31
Exploring Automated Tools	31
Escalation Path: Kernel Exploits.....	31
Kernel Exploits Overview.....	31
Escalation with Metasploit.....	31
Manual Kernel Exploitation	31
Escalation Path: Passwords and Port Forwarding.....	31

Overview.....	31
Gaining a Foothold (Box 2)	31
Escalation via Stored Passwords	31
Escalation Path: Windows Subsystem for Linux.....	31
Overview.....	31
Gaining a Foothold (Box 3)	31
Escalation via WSL.....	31
Impersonation and Potato Attacks.....	32
Token Impersonation Overview	32
Impersonation Privileges Overview	32
Potato Attacks Overview	32
Gaining a Foothold (Box 4)	32
Escalation via Potato Attack.....	32
Alternate Data Streams	32
Escalation Path: getsystem.....	32
getsystem Overview	32
Escalation Path: RunAs	32
Overview of RunAs.....	32
Gaining a Foothold (Box 5)	32
Escalation via RunAs.....	32
Additional Labs	32
Overview of TryHackMe Labs	32
Escalation Path: Registry	32
Overview of Autoruns	32
Escalation via Autorun	32
AlwaysInstallElevated Overview and Escalation.....	32
Overview of regsvc ACL.....	32
regsvc Escalation	32
Escalation Path: Executable Files.....	32
Executable Files Overview	32
Escalation via Executable Files	32
Escalation Path: Startup Applications.....	32
Startup Applications Overview.....	32
Escalation via Startup Applications.....	32
Escalation Path: DLL Hijacking.....	32
Overview and Escalation via DLL Hijacking.....	32
Escalation Path: Service Permissions (Paths)	33
Escalation via Binary Paths	33
Escalation via Unquoted Service Paths	33

Challenge Overview	33
Gaining a Foothold	33
Escalation via Unquoted Service Path – Metasploit	33
Manual Challenge Walkthrough	33
Escalation Path: CVE-2019-1388.....	33
Overview of CVE-2019-1388	33
Gaining a Foothold	33
Escalation via CVE-2019-1388	33
Capstone Challenge	33
Capstone Overview.....	33
Capstone Walkthrough 1	33
Capstone Walkthrough 2	33
Capstone Walkthrough 3	33
Capstone Walkthrough 4	33
Capstone Walkthrough 5	33
Conclusion.....	33
Conclusion	33



Last Page