Practical Ethical Hacking

Learn how to hack like a pro by a pro. 20 hours of up to date practical hacking techniques with absolutely no filler.

Course Overview

Welcome to this course on **Practical Ethical Hacking**. To enjoy this course, you need nothing but a positive attitude and a desire to learn. **No prior hacking knowledge is required.**

In this course, you will learn the practical side of ethical hacking. Too many courses teach

students tools and concepts that are never used in the real world. In this course, we will focus only on tools and topics that will make you successful as an ethical hacker. The course is incredibly **hands on** and will cover many foundational topics.

System Requirements:

- Basic IT, Linux, and Programming knowledge
- For Mid-Course Capstone: A minimum of 12GB of RAM is suggested.
- For Wireless Hacking: A wireless adapter that supports monitor mode (links provided in course).
- For Active Directory Lab Build: A minimum of 16GB of RAM is suggested. Students can still participate in the course, but may experience slow lab environments.

Practical Ethical Hacking Course Objectives

In this course, we will cover:

- **A Day in the Life of an Ethical Hacker**. What does an ethical hacker do on a day to day basis? How much can he or she make? What type of assessments might an ethical hacker perform? These questions and more will be answered.

- **Effective Notekeeping.** An ethical hacker is only as good as the notes he or she keeps. We will discuss the important tools you can use to keep notes and be successful in the course and in the field.

- **Networking Refresher.** This section focuses on the concepts of computer networking. We will discuss common ports and protocols, the OSI model, subnetting, and even walk through a network build with using Cisco CLI.

- **Hacking Methodology.** This section overviews the five stages of hacking, which we will dive deeper into as the course progresses.

- **Reconnaissance and Information Gathering.** You'll learn how to dig up information on a client using open source intelligence. Better yet, you'll learn how to extract

breached credentials from databases to perform credential stuffing attacks, hunt down subdomains during client engagements, and gather information with Burp Suite.

- **Scanning and Enumeration.** One of the most important topics in ethical hacking is the art of enumeration. You'll learn how to hunt down open ports, research for potential vulnerabilities, and learn an assortment of tools needed to perform quality enumeration.

- **Exploitation Basics.** Here, you'll exploit your first machine! We'll learn how to use Metasploit to gain access to machines, how to perform manual exploitation using coding, perform brute force and password spraying attacks, and much more.

- **Mid-Course Capstone.** This section takes everything you have learned so far and challenges you with 10 vulnerable boxes that order in increasing difficulty. You'll learn how an attacker thinks and learn new tools and thought processes along the way. Do you have what it takes?

- **Active Directory.** Did you know that 95% of the Fortune 1000 companies run Active Directory in their environments? Due to this, Active Directory penetration testing is one of the most important topics you should learn and one of the least taught. The Active Directory portion of the course focuses on several topics. You will build out your own Active Directory lab and learn how to exploit it. Attacks include, but are not limited to: **LLMNR poisoning, SMB relays, IPv6 DNS takeovers, pass-the-hash/pass-the-password, token impersonation, kerberoasting, GPP attacks, golden ticket attacks,** and **much more.** You'll also learn important tools like **mimikatz, Bloodhound,** and **PowerView.** This is not a section to miss!

- **Post Exploitation.** The fourth and fifth stages of ethical hacking are covered here. What do we do once we have exploited a machine? How do we transfer files? How do we pivot? What are the best practices for maintaining access and cleaning up?

- **Web Application Penetration Testing.** In this section, we revisit the art of enumeration and are introduced to several new tools that will make the process easier. You will also learn how to automate these tools utilize Bash scripting. After the enumeration section, the course dives into the OWASP Top 10. We will discuss attacks and defenses for each of the top 10 and perform walkthroughs using

vulnerable web applications. Topics include: **SQL Injection, Broken Authentication, Sensitive Data Exposure, XML External Entities (XXE), Broken Access Control, Security Misconfigurations, Cross-Site Scripting (XSS), Insecure Deserialization, Using Components with Known Vulnerabilities,** and **Insufficient Logging and Monitoring**

- **Wireless Attacks.** Here, you will learn how to perform wireless attacks against WPA2 and compromise a wireless network in under 5 minutes.

- **Legal Documentation and Report Writing.** A topic that is hardly ever covered, we will dive into the legal documents you may encounter as a penetration tester, including Statements of Work, Rules of Engagement, Non-Disclosure Agreements, and Master Service Agreements. We will also discuss report writing. You will be provided a sample report as well as walked through a report from an actual client assessment.

- **Career Advice.** The course wraps up with career advice and tips for finding a job in the field.

At the end of this course, you will have a deep understanding of **external and internal network penetration testing, wireless penetration testing,** and **web application penetration testing.** All lessons taught are from a real-world experience and what has been encountered on actual engagements in the field.

Note: This course has been created for educational purposes only. All attacks shown were done so with given permission. Please do not attack a host unless you have permission to do so.

Questions & Answers Team Availability and Rules

The Q&A team responds to most questions within 2 business days. Specific Q&A rules are as follows:

1. Please encourage each other and help each other out. The support team is here to help, but are not staffed 24/7.

2. Support assistance will only be provided for course related material only. If you are using a tool or method in your labs that is not taught in the course, it is better asked in Discord on an appropriate channel outside of #course-chat.

3. Avoid spoilers for the mid-course capstone. If you are assisting another user or asking a question related to this section, please try to not provide direct answers/ solutions.

4. Be kind to others and be patient. This field consists of patience, self-motivation, self-determination, and lots of Googling. Do not demand help or expect answers. That mindset will not take you far in your career. <3

What Our Students Say

Ty Atkin

"Most outstanding. There is no better course on this topic. After completing this course I crushed 3 different Red Team interviews and received two offers. Heath is the BEST mentor and teacher. So grateful he took the time to put this together. It unlocked an entirely new world in my career. Thanks Heath!"

Azeer Esmail

"It was such a pleasure learning from Heath, he has the skill, experience and right attitude to teach. I've been looking around for some time for such a comprehensive Pen-testing course, and I'm very happy I landed on this one. Thanks Heath! Keep giving from the heart!"

Mike Roberts

"Even as a veteran and IT business owner this was the most helpful and well polished course I've ever taken to further advance my security knowledge. Thank you Heath for putting so much time and passion into this."

Practical Ethical Hacking Course Curriculum - 20+ Hours

Before We Begin

- Special Thanks & Credits
- PNPT Certification Path Progression(2:32)
- Section Quiz

Introduction

- Course Introduction(7:24)

Course Discord (Important)(2:45)

A Day in the Life of an Ethical Hacker(20:55)

Why You Shouldn't Be An Ethical Hacker

Section Quiz

Notekeeping

Effective Notekeeping(7:39)

Screenshots for the Win(4:16)

Section Quiz

Networking Refresher

Introduction(1:11)

IP Addresses(13:06)

MAC Addresses(3:13)

TCP, UDP, and the Three-Way Handshake(5:12)

Common Ports and Protocols(6:09)

The OSI Model(5:30)

Subnetting Part 1(26:59)

Subnetting Part 2(4:13)

Section Quiz

Setting Up Our Lab

Installing VMWare / VirtualBox(6:15)

Configuring VirtualBox(3:16)

Installing Kali Linux(5:32)

Section Quiz

Help! Linux and Python Are Missing!

Read Me

The Ethical Hacker Methodology

The Five Stages of Ethical Hacking(5:16)

Section Quiz

Information Gathering (Reconnaissance)

Passive Reconnaissance Overview(7:32)

Identifying Our Target(3:33)

Discovering Email Addresses(15:48)

Gathering Breached Credentials with Breach-Parse(7:17)

Hunting Breached Credentials with DeHashed(11:55)

Hunting Subdomains Part 1(5:31)

Hunting Subdomains Part 2(4:48)

Identifying Website Technologies(7:06)

Information Gathering with Burp Suite(8:48)

Google Fu(5:31)

Utilizing Social Media(5:37)

Additional Learning (OSINT Fundamentals)(0:48)

Section Quiz

Scanning & Enumeration

- Installing Kioptrix(6:17)
- Scanning with Nmap(19:46)
- Enumerating HTTP and HTTPS Part 1(15:01)
- Enumerating HTTP and HTTPS Part 2(15:08)
- Enumerating SMB(14:19)
- Enumerating SSH(4:09)
- Researching Potential Vulnerabilities(14:49)
- Our Notes So Far(3:06)
- Section Quiz

Vulnerability Scanning with Nessus

- Scanning with Nessus Part 1(10:34)
- Scanning with Nessus Part 2(6:09)
- Section Quiz

Exploitation Basics

- Reverse Shells vs Bind Shells(7:00)
- Staged vs Non-Staged Payloads(3:21)
- Gaining Root with Metasploit(7:40)
- Manual Exploitation(12:40)
- Brute Force Attacks(7:49)
- Credential Stuffing and Password Spraying(14:02)

Our Notes, Revisited(3:03)

Section Quiz

New Capstone

Introduction(5:42)

Set Up - Blue(3:56)

Walkthrough - Blue(17:00)

Set Up - Academy(2:25)

Walkthrough - Academy(44:19)

Walkthrough - Dev(25:20)

Walkthrough - Butler(36:18)

Walkthrough - Blackpearl(23:30)

Active Directory Overview

Active Directory Overview(5:39)

Physical Active Directory Components(2:37)

Logical Active Directory Components(7:13)

Section Quiz

Active Directory Lab Build

Lab Overview and Requirements(3:03)

Lab Build - (Cloud Alternative)(2:04)

Downloading Necessary ISOs(3:59)

Setting Up the Domain Controller(16:25)

Setting Up the User Machines(11:01)

Setting Up Users, Groups, and Policies(17:02)

Joining Our Machines to the Domain(12:06)

Attacking Active Directory: Initial Attack Vectors

Introduction(2:14)

LLMNR Poisoning Overview(4:56)

Capturing Hashes with Responder(5:59)

Cracking Our Captured Hashes(11:04)

LLMNR Poisoning Mitigation(2:22)

SMB Relay Attacks Overview(5:28)

SMB Relay Attacks Lab(10:59)

SMB Relay Attack Defenses(3:45)

Gaining Shell Access(13:42)

IPv6 Attacks Overview(4:00)

IPv6 DNS Takeover via mitm6(10:57)

IPv6 Attack Defenses(2:50)

Passback Attacks(5:16)

Initial Internal Attack Strategy(3:56)

Section Quiz

Attacking Active Directory: Post-Compromise Enumeration

Introduction(2:10)

Domain Enumeration with ldapdomaindump(4:24)

Domain Enumeration with Bloodhound(12:28)

Domain Enumeration with Plumhound(6:42)

Domain Enumeration with PingCastle(6:16)

Section Quiz

Attacking Active Directory: Post-Compromise Attacks

Introduction(0:49)

Pass Attacks Overview(5:56)

Pass Attacks(13:37)

Dumping and Cracking Hashes(10:59)

Pass Attack Mitigations(1:53)

Kerberoasting Overview(3:47)

Kerberoasting Walkthrough(3:34)

Kerberoasting Mitigation(0:53)

Token Impersonation Overview(4:51)

Token Impersonation Walkthrough(9:26)

Token Impersonation Mitigation(1:19)

LNK File Attacks(8:00)

GPP / cPassword Attacks and Mitigations(4:20)

Mimikatz Overview(2:02)

Credential Dumping with Mimikatz(8:59)

Post-Compromise Attack Strategy(3:40)

Section Quiz

We've Compromised the Domain - Now What?

Post-Domain Compromise Attack Strategy(4:16)

Dumping the NTDS.dit(9:43)

Golden Ticket Attacks Overview(2:41)

Golden Ticket Attacks(7:18)

Additional Active Directory Attacks

Section Overview(2:53)

Abusing ZeroLogon(9:03)

PrintNightmare (CVE-2021-1675) Walkthrough(12:06)

Section Quiz

Active Directory Case Studies

AD Case Study #1(7:41)

AD Case Study #2(7:19)

AD Case Study #3(7:52)

Post Exploitation

Introduction(1:49)

File Transfers Review(2:32)

Maintaining Access Overview(3:33)

Pivoting Overview(4:00)

Pivoting Walkthrough(8:07)

Cleaning Up(2:48)

Section Quiz

Web Application Enumeration, Revisited

Introduction(1:49)

Installing Go(1:19)

Finding Subdomains with Assetfinder(7:43)

Finding Subdomains with Amass(5:27)

Finding Alive Domains with Httprobe(7:15)

Screenshotting Websites with GoWitness(4:10)

Automating the Enumeration Process(5:46)

Additional Resources(2:18)

Section Quiz

Find & Exploit Common Web Vulnerabilities

Introduction(0:58)

Lab Setup (full text instructions included in course notes)(8:35)

SQL Injection - Introduction(4:03)

SQL Injection - UNION(9:38)

SQL Injection - Blind Part 1(9:52)

SQL Injection - Blind Part 2(12:53)

SQL Injection - Challenge Waklthrough(5:36)

XSS - Introduction(4:50)

XSS - DOM Lab(3:25)

XSS - Stored Lab(7:38)

XSS - Challenge Walkthrough(3:24)

Command Injection - Introduction(2:24)

Command Injection - Basics(7:54)

Command Injection - Blind / Out-of-Band(8:49)

Command Injection - Challenge Walkthrough(4:04)

Insecure File Upload - Introduction(0:31)

Insecure File Upload - Basic Bypass(8:48)

Insecure File Upload - Magic Bytes(9:13)

Insecure File Upload - Challenge Walkthrough(3:29)

Attacking Authentication - Intro(1:14)

Attacking Authentication - Brute Force(7:00)

Attacking Authentication - MFA(6:20)

Attacking Authentication - Challenge Walkthrough(10:30)

XXE - External Entities Injection(6:04)

IDOR - Insecure Direct Object Reference(4:38)

Capstone - Introduction(0:57)

Capstone - Solution(17:07)

Section Quiz

Wireless Penetration Testing

Wireless Penetration Testing Overview(10:26)

WPA PS2 Exploit Walkthrough(13:12)

Section Quiz

Legal Documents and Report Writing

Common Legal Documents(7:18)

Pentest Report Writing(11:17)

Reviewing a Real Pentest Report(19:34)

Section Quiz

Career Advice

Career Advice(11:10)

Next Steps: Try a Certification!

About the Instructor: Heath Adams

Hi everyone! My name is Heath Adams, but I also go by "The Cyber Mentor" on social media. I am the founder and CEO of TCM Security, an ethical hacking and cybersecurity consulting company. While I am an ethical hacker by trade, I love to teach! I have taught courses to over 170,000 students on multiple platforms, including Udemy, YouTube, Twitch, and INE.

I am currently OSCP, OSWP, eCPPTX, eWPT, CEH, Pentest+, CCNA, Linux+, Security+, Network+, and A+ certified.

I'm also a husband, animal dad, tinkerer, and military veteran. I hope you enjoy my courses.

Follow Heath on Social Media:

LinkedIn - https://linkedin.com/in/heathadams

Twitter - https://twitter.com/thecybermentor

YouTube - https://youtube.com/c/thecybermentor

Twitch - https://twitch.tv/thecybermentor