Windows Privilege Escalation for Beginners

Learn how to escalate privileges on Windows machines with absolutely no filler.

Course Retirement!

The Windows Privilege Escalation for Beginners course will be retired on **May 7, 2025**. This course will no longer be available as part of the All-Access Membership. However, it will still be available to students who have purchased individual lifetime access and to those who have purchased access through the PNPT certification. Please read our blog for more details.

For a limited time, you can purchase lifetime access to the course for just $60! Bundle it with the Linux Privilege Escalation course and **save $20**. Act fast this offer expires on May 7, 2025.

Course Overview

This course focuses on Windows Privilege Escalation tactics and techniques designed to help you improve your privilege escalation game. Students should take this course if they are interested in:

- Gaining a better understanding of privilege escalation techniques
- Improving Capture the Flag skillset
- Preparing for certifications such as the Practical Network Penetration Tester (PNPT).

Prerequisites & System Requirements

- Prior beginner hacking knowledge preferred
- Prior virtualization knowledge preferred
- A subscription to Hack the Box is required to complete the course.
- A subscription to TryHackMe is strongly recommended to complete the course.

Windows Privilege Escalation Course Objectives

What will I learn?

1) How to enumerate Windows systems manually and with tools

2) A **multitude** of privilege escalation techniques, including:

- Kernel Exploits
- Password Hunting
- Impersonation Attacks
- Registry Attacks
- Executable Files
- Schedule Tasks
- Startup Applications
- DLL Hijacking
- Service Permissions
- Windows Subsystem for Linux
- CVE-2019-1388

3) Tons of **hands-on** experience, including:

- 13 vulnerable machines total
- Capstone challenge
- Custom lab with no installation required

PLEASE NOTE

Due to the cost of Windows licensing, this course is designed around Hack The Box and TryHackMe platforms, **which are additional charges**, but offer an incredible variety of vulnerable machines at a fraction of the cost of one Windows license. I do not receive any financial incentive from either platform for utilizing them in the course.

What Our Students Are Saying

Kelly James

"This is my second course with Heath and he has once again exceeded my expectations. He is a natural at teaching and very knowledgeable about the course materials. I would definitely recommend that all new pentesters take this course and master the skills and methods provided."

Michael Marshall

"Fantastic course! I learned a ton and the way Heath presents the material is so conversational that it's like you're sitting next to a knowledgable friend as he shares cool tips. I can't say enough about the high-quality material and the easy way it's presented!"

Doug Kras

"If you are looking for an amazing course to learn Windows Privilege escalation I highly recommend this course! There's no better teacher than The Cyber Mentor. Highly recommend every one of the classes!!!"

Windows Privilege Escalation Course

Curriculum - 7 Hours

Introduction

- Course Introduction(5:39)
- Course Discord (Important)(2:45)
- Resources and Tips for Success(3:00)
- Course Repo

Gaining a Foothold

- Introduction(3:27)
- Gaining a Foothold (Box 1)(7:45)

Initial Enumeration

- System Enumeration(7:19)
- User Enumeration(4:02)
- Network Enumeration(4:46)
- Password Hunting(4:52)
- AV Enumeration(5:08)

Exploring Automated Tools

- Automated Tool Overview(11:20)
- Exploring Automated Tools(11:07)

Escalation Path: Kernel Exploits

- Kernel Exploits Overview(3:29)

Escalation with Metasploit(4:31)

Manual Kernel Exploitation(10:09)

Escalation Path: Passwords and Port Forwarding

Overview(1:53)

Gaining a Foothold (Box 2)(8:23)

Escalation via Stored Passwords(18:03)

Escalation Path: Windows Subsystem for Linux

Overview(1:54)

Gaining a Foothold (Box 3)(15:02)

Escalation via WSL(8:45)

Impersonation and Potato Attacks

Token Impersonation Overview(4:06)

Impersonation Privileges Overview(3:27)

Potato Attacks Overview(2:45)

Gaining a Foothold (Box 4)(11:26)

Escalation via Potato Attack(2:38)

Alternate Data Streams(2:08)

Escalation Path: getsystem

getsystem Overview(3:54)

Escalation Path: RunAs

Overview of RunAs(1:44)

Gaining a Foothold (Box 5)(7:53)

Escalation via RunAs(4:33)

Additional Labs

Overview of TryHackMe Labs(5:34)

Escalation Path: Registry

Overview of Autoruns(6:17)

Escalation via Autorun(4:35)

AlwaysInstallElevated Overview and Escalation(7:04)

Overview of regsvc ACL(2:41)

regsvc Escalation(8:09)

Escalation Path: Executable Files

Executable Files Overview(4:25)

Escalation via Executable Files(2:40)

Escalation Path: Startup Applications

Startup Applications Overview(3:13)

Escalation via Startup Applications(3:58)

Escalation Path: DLL Hijacking

Overview and Escalation via DLL Hijacking(9:40)

Escalation Path: Service Permissions (Paths)

Escalation via Binary Paths(6:28)

Escalation via Unquoted Service Paths(6:51)

Challenge Overview(2:36)

Gaining a Foothold(4:47)

Escalation via Unquoted Service Path Metasploit(8:07)

Manual Challenge Walkthrough(8:59)

Escalation Path: CVE-2019-1388

Overview of CVE-2019-1388(2:38)

Gaining a Foothold(8:41)

Escalation via CVE-2019-1388(5:35)

Capstone Challenge

Capstone Overview(1:58)

Challenge Walkthrough 1(15:59)

Challenge Walkthrough 2(18:27)

Challenge Walkthrough 3(14:44)

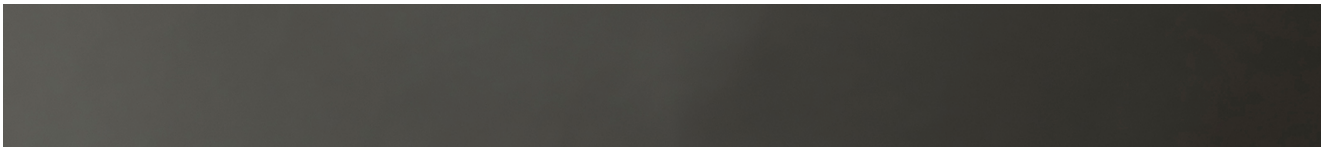
Challenge Walkthrough 4(27:54)

Challenge Walkthrough 5(24:37)

Conclusion

Conclusion(2:03)

Next Steps: The Practical Network Penetration Tester (PNPT) 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