Linux Privilege Escalation for Beginners

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

Course Retirement!

The Linux 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 Windows Privilege Escalation course and **save $20**. Act fast this offer expires on May 7, 2025.

Course Overview

This course focuses on Linux 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
- Access to a Windows machine is preferred

Linux Privilege Escalation Course Objectives

What will I learn?

1) How to enumerate Linux systems manually and with tools

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

- Kernel Exploits
- Password Hunting
- File Permissions
- Sudo Attacks
- Shell Escaping
- Intended Functionality
- LD_PRELOAD
- CVE-2019-14287
- CVE-2019-18634
- SUID Attacks
- Shared Object Injection
- Binary Symlinks
- Environment Variables
- Capabilities Attacks
- Scheduled Tasks
- NFS
- Docker

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

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

What Our Students Are Saying

Deo Martinez

"Heath does a great job explaining the concepts of pen testing and follows it up with hands-on examples. Its easy to follow his methodology and he gives plenty of advice on some of the common tools to use based on the findings illustrated in his course. Great job, Heath!"

Jacob Surles

"This course is amazing. I have taken other privilege escalation courses and none of them were even close to as engaging and informative as this course. I highly recommend this course."

Florin Galaftion

"Excellent ! The Combo Windows/Linux privilege escalation courses was a great investment. Worth every penny and more! The CTFs were well chosen and included a full walk-thru of the techniques presented in lectures. Way to go Heath ! Looking for more coming from you in the near future !"

Linux Privilege Escalation Course

Curriculum - 6.5 Hours

Introduction

- Introduction(7:14)
- Course Discord (Important)(2:45)
- Course Tips & Resources(5:48)
- Course Repo

Lab Overview & Initial Access

- Lab Overview & Initial Access(7:17)

Initial Enumeration

- System Enumeration(6:08)
- User Enumeration(4:52)
- Network Enumeration(4:09)
- Password Hunting(5:51)

Exploring Automated Tools

- Introduction(4:41)
- Exploring Automated Tools(11:40)

Escalation Path: Kernel Exploits

- Kernel Exploits Overview(3:17)
- Escalation via Kernel Exploit(6:06)

Escalation Path: Passwords & File Permissions

Overview(0:34)

Escalation via Stored Passwords(8:31)

Escalation via Weak File Permissions(10:36)

Escalation via SSH Keys(5:39)

Escalation Path: Sudo

Sudo Overview(1:15)

Escalation via Sudo Shell Escaping(6:39)

Escalation via Intended Functionality(4:41)

Escalation via LD_PRELOAD(7:01)

Challenge Overview(1:18)

Challenge Walkthrough(12:44)

CVE-2019-14287 Overview(3:15)

Escalation via CVE-2019-14287(2:35)

Overview and Escalation via CVE-2019-18634(6:42)

Escalation Path: SUID

SUID Overview(8:21)

Gaining a Foothold(13:04)

Escalation via SUID(6:34)

Escalation Path: Other SUID Escalation

Escalation via Shared Object Injection(11:28)

Escalation via Binary Symlinks(9:29)

Escalation via Environmental Variables(11:13)

Escalation Path: Capabilities

Capabilities Overview(3:36)

Escalation via Capabilities(2:43)

Escalation Path: Scheduled Tasks

Cron & Timers Overview(4:59)

Escalation via Cron Paths(2:53)

Escalation via Cron Wildcards(5:24)

Escalation via Cron File Overwrites(3:48)

Challenge Overview(0:49)

Challenge Walkthrough(19:09)

Escalation Path: NFS Root Squashing

Overview & Escalation via NFS Root Squashing(6:00)

Escalation Path: Docker

Overview(1:26)

Gaining a Foothold(9:59)

Escalation via Docker(5:04)

Capstone Challenge

Capstone Overview(1:53)

Capstone Walkthrough #1(15:49)

Capstone Walkthrough #2(11:25)

Capstone Walkthrough #3(18:21)

Capstone Walkthrough #4(21:37)

Capstone Walkthrough #5(40:48)

Wrapping Up

Conclusion(1:57)

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