The External Pentest Playbook

Learn to conduct an external network penetration test from start to finish.

Course Overview

This course focuses on external penetration testing tactics and techniques designed to help you improve your pentest game. Students should take this course if they are interested in:

- Gaining a better understanding of the external pentest attack methodology and mindset

- Improving overall penetration testing skillset and client relations
- Crushing their next penetration testing job interview

Prerequisites & System Requirements

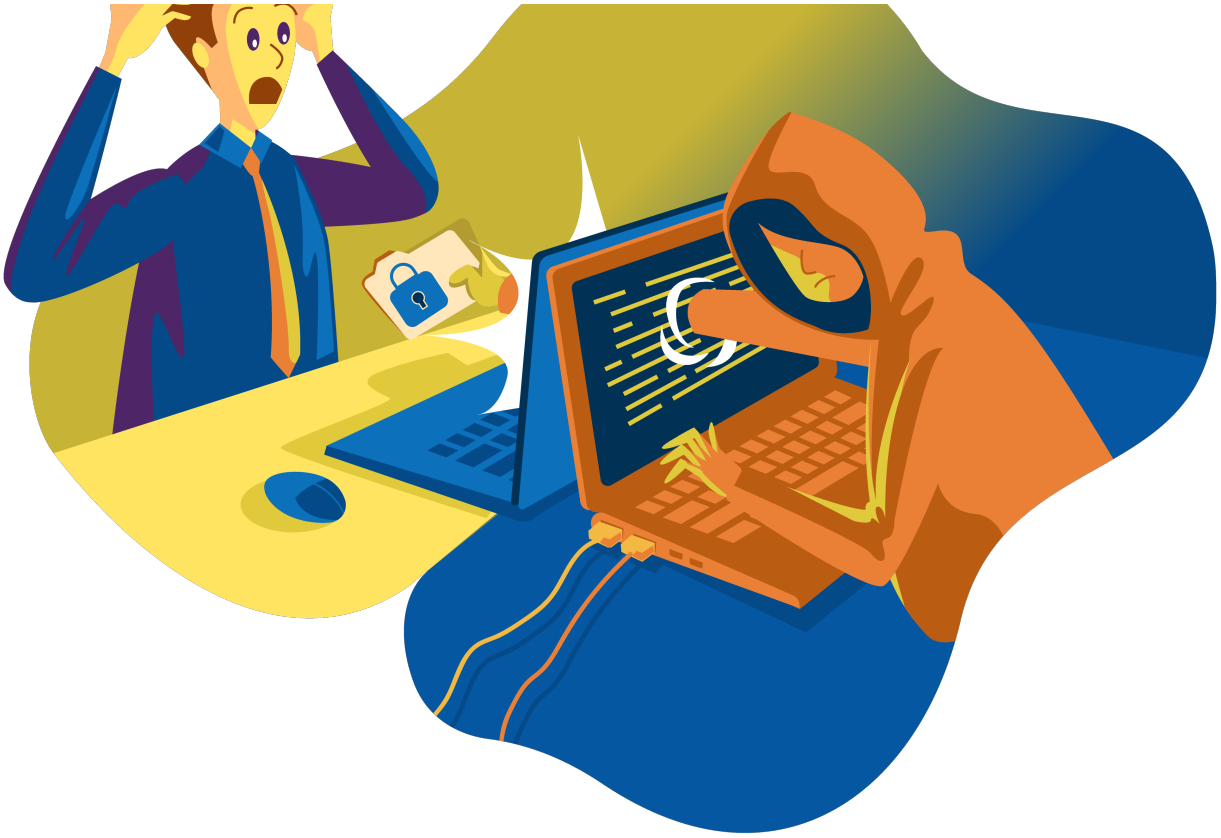
- Previous beginner pentest knowledge strongly preferred
- Prior basic security knowledge strongly preferred
- Desire to learn is required :)

External Pentest Playbook Course Objectives

What will I learn?

The following concepts will be taught in this course:

- Objectives of an External Pentest
- Important Documents and Procedures
- Scope Verification and Client Communication
- Attack Strategies
- Vulnerability Scanning
- Common OSINT and Information Gathering Techniques
- Attacking O365/OWA
- Attacking Login Portals
- Bypassing MFA and Escalating Access
- Report Writing
- Identifying Common Pentest Findings
- Client Debriefs, Retests, and Attestations



External Pentest Playbook Curriculum - 3.5 Hours

Introduction

- Introduction(8:18)
- Course Discord(2:45)

Before We Start

- Objectives of an External Pentest(3:11)
- Checklists, FTW(6:41)
- Rules of Engagement(9:20)
- Verifying Scope(3:38)

Client Communication(4:28)

Kicking Off

Attack Strategy(6:20)

Vulnerability Scanning(6:56)

Reviewing & Extracting Information(5:04)

Information Gathering / OSINT

Overview(1:55)

Hunting Breached Credentials(14:21)

Identifying Employees & Emails(6:27)

Enumerating Valid Accounts (Pre-Attack)(5:55)

Other Useful Information(5:43)

Attacking Login Portals

Overview & Strategy(6:41)

Attacking O365(15:31)

Attacking OWA(7:10)

Attacking Other Portals(9:51)

Bypassing MFA(7:09)

Escalating Access

Strategy & Walkthrough(12:30)

Report Writing

Report Writing(16:04)

Common Pentest Findings

- Overview(0:52)
- Insufficient Authentication Controls(4:16)
- Weak Password Policy(4:17)
- Insufficient Patching(3:13)
- Default Credentials(3:37)
- Insufficient Encryption(3:06)
- Information Disclosure(4:02)
- Username Enumeration(2:37)
- Default Web Pages(1:47)
- Open Mail Relays(2:00)
- IKE Aggressive Mode(1:43)
- Unexpected Perimeter Services(1:39)
- Insufficient Traffic Blocking(2:14)
- Undetected Malicious Activity(1:55)
- Historical Account Compromises(1:46)

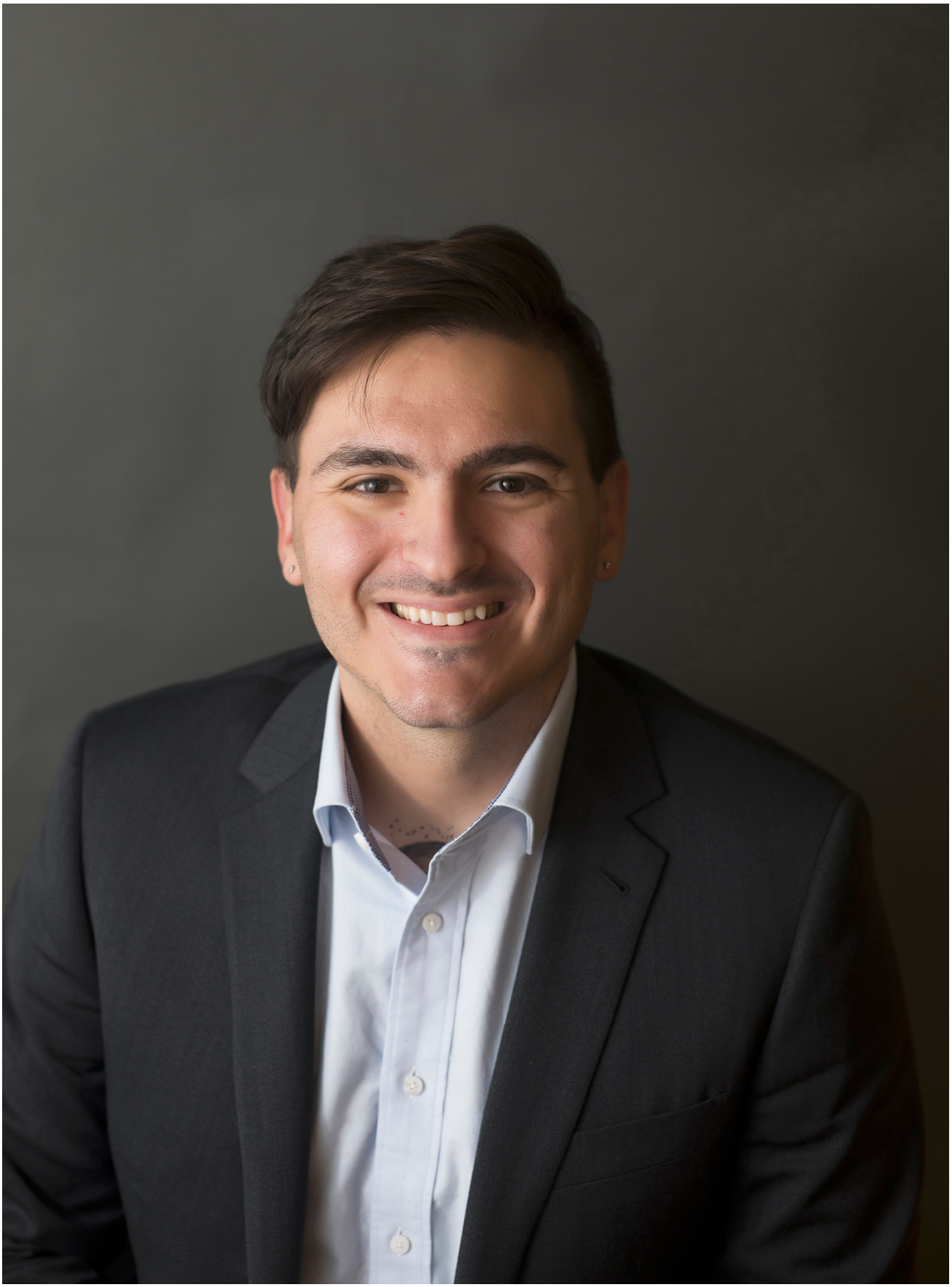
Wrapping Up

- Client Debriefs(5:36)
- Attestation Letters(2:02)
- Client Retests(2:13)

Next Steps: The Practical Network Penetration Tester (PNPT) Certification

Conclusion

Course Conclusion(2:37)



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