PEN-200 and the OSCP

Table of Contents

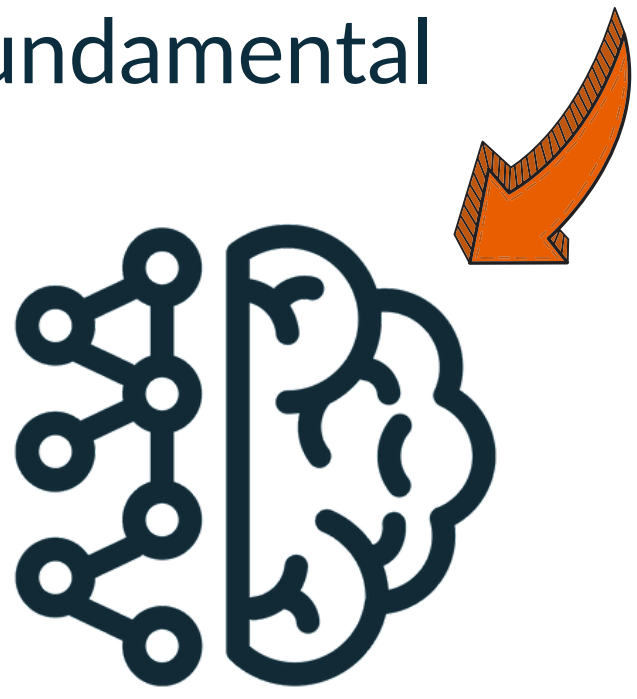
Start with Fundamentals

LEARN ONE SUBSCRIPTION

All prerequisites for PEN-200 can be found in **PEN-100.** 100-level courses are part of the Learn One annual subscription.

PEN-100 has beginner-level, fundamental content. Topics include:

- Linux Basics
- Network Scripting
- Troubleshooting
- Intro to Active Directory



Build Your Skills - Pt I

PROVING GROUNDS

PG Practice is a network for practicing your skills on real-world vectors.

A Learn subscription includes an entire year of unlimited access to PG.

EXPLOIT DATABASE

The Exploit Database is an **archive of public exploits** and corresponding vulnerable software, developed for use by penetration testers and vulnerability researchers.

VULNHUB

A **free training** resource that helps you gain hands-on experience in cybersecurity, computer software & network administration.

Build Your Skills - Pt II

Watch and learn from box walkthroughs:

offs.ec/youtube

twitch.tv/offsecofficial

Join the OffSec Community on Discord

discord.com/invite/offsec

The Importance of Community

From Jeremy Miller's Reflections on Failure, Part Two

"People in information security tend to have a strong sense of community, and indeed “community” is one of OffSec’s core values. But learning security can often feel lonely.

If I could ask one thing of the reader, it would be to please never hesitate to reach out to others in the space for practical and emotional support – there are plenty of infosec community members who are more than happy to help out."

The Adversarial Mindset

Mental Models of Hackers

Observations of the system and its components

[Ambiguity tolerance]

[Diagramming]

[Creativity]

Patterns of relationships among interrelated parts throughout the system

Recognized trends and patterns of operation

[Curiosity]

[Domain Expertise]

Assumptions, generalizations, and images influencing my understanding of the system and its functionality

Image adapted from Summers, Timothy. How Hackers Think: A Mixed Method Study of Mental Models and Cognitive Patterns of High-Tech Wizards. May 2015, etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=case1427809862.

How We Teach Hacking

On one hand, we're trying to teach technical information like what it means to attack web applications.
On the other, there is this whole concept of mindset, adversarial thinking, and how we're going about the process.

"...hackers express a desire and interest in solving problems that lack definition and appear not to have a solution."

Summers, Timothy. How Hackers Think: A Mixed Method Study of Mental Models and Cognitive Patterns of High-Tech Wizards. May 2015, etd.ohiolink.edu/apexprod/rws_etd/send_file/send?accession=case1427809862.

Learn from Failure

From Jeremy Miller's Reflections on Failure, Part Two

Set a timer for some arbitrary amount of time, say for three hours. Your goal is to attack a chosen machine and compromise it within the allotted time.

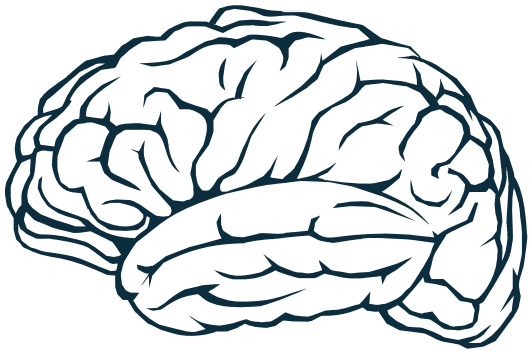
If you are able to compromise the target, then you have succeeded. Pick a more difficult machine or reduce the time period and try again. At some point, some combination of target and time period will inevitably cause you to fail.

When you do, write down what you have learned during the process, and particularly what your failed attempts might tell you about the machine.

Your failure contributes to your global progress and makes you a better cybersecurity professional.

Remember to Pause during Your Journey

and take a



Your brain is not designed to run non-stop.

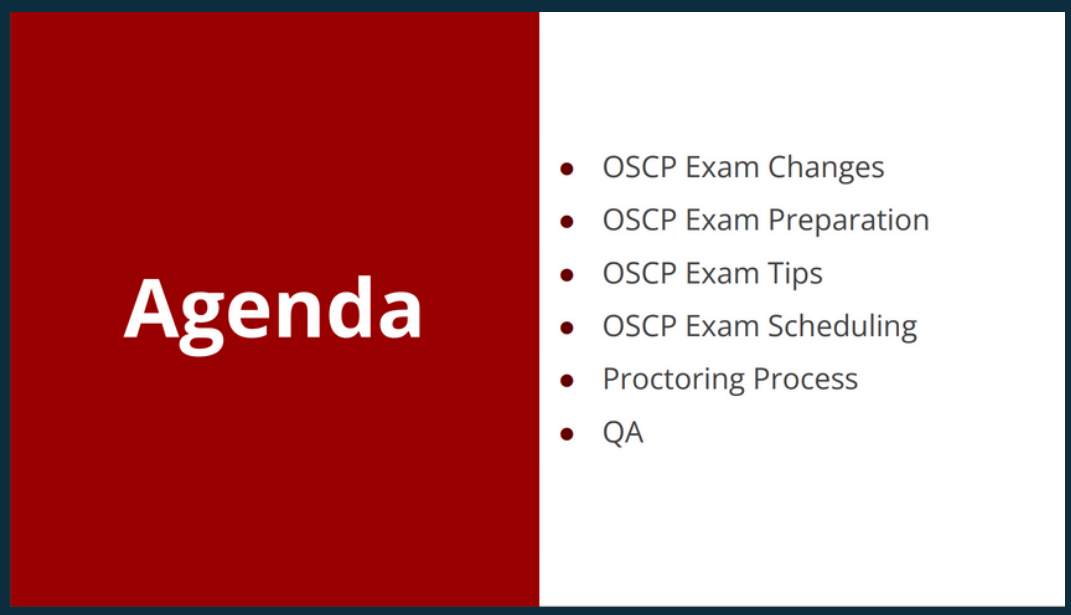
A 5-15 minute break every hour or so can:

- improve memory
- increase productivity
- reduce stress
- reignite your creativity

Exam Prep

A comprehensive overview of OSCP exam prep tips and best practices:

https://offs.ec/oscp-prep



OSCP Exam Prep Slides

Resources/FAQs

PEN-200 Onboarding

We selected 11 machines in the PEN-200 labs and provided the information needed to compromise them:

PEN-200 Labs Learning Path

How to manage documentation and reporting:

PEN-200 Reporting Requirements

Walkthrough of Alice, a PWK lab machine:

Alice with Siddicky (Student Mentor)

OSCP Exam Guide

OSCP Exam FAQ