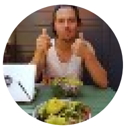

Luke Stephens (@lodestarluke)
Pentester | Hubby | Musician | On a mission to free my thoughts and actions from the limits which are imposed on them by society.
Feb 14 · 5 min read

Luke's Ultimate OSCP Guide: Part 1—Is OSCP for you? Some things you should know before you start

If you've landed here, you're probably thinking about taking the Offensive Security PWK course to become an OSCP, but you're not sure if you're quite ready to take the plunge. Well! You've found the right place, my soon-to-be hacker comrade. This is a list of questions that I get asked regularly from people thinking of signing up to the OSCP. I am not being paid to promote this course, just my opinion.

This document is a work in progress! If you have any ideas or questions you would like answered, get in touch!

Would you recommend it?

Yes. If you're hoping to work in the infosec field, or even if you're just interested, the course and the labs are fun and super educational. While having this certification is not as valuable as having experience in the field, it looks great on your CV, and shows that you have at least a basic understanding of common hacking tools and techniques.

How much time do I need?

The #1 misery-generator while sitting your OSCP is not having enough time. Make sure you have at least a few hours every day to focus on learning without distraction. Not only will you have a better chance of passing first go, you will also learn the content more deeply. The more you put into this course, the more you will get out of it.

How much lab time should I purchase?

A rule of thumb for choosing how much lab time you need:

- If you already a seasoned penetration tester, and you are just getting your OSCP to lengthen your CV and brag to your mum, go with 30 days. Unless you are a super master hacker who doesn't sleep, this probably won't be enough time to own everything in the labs, but you don't need to—you only need to pass the exam.
- If you have a fairly solid foundation in hacking and you have success with other hacking challenges such as hackthebox.eu or vulnhub, go with 60 days.
- If you aren't all that experienced with hacking, or you want to scrape every last drop of information out of the course, go with 90 days.

If it makes you feel any better, your decision is not final—you can always purchase a lab extention after the inital purchase. Also—if you fail your exam, you can resit it for $60 USD.

How is the PWK / OSCP structured?

Basically, the course is split into 3 sections:

1. Coursework

When your lab time starts, you are also sent a PDF textbook, and a series of tutorial videos to match. These materials teach a tonne of common hacking methods, and contain some tricks that you will be able to try in the labs. At the end of each section are some hands-on exercises to try out. If you document these exercises (with the exception of a few, as noted in the manual), and also provide a detailed report of how you owned 10 machines in the labs, you will receive an extra 5 points on your final exam—this can come in handy! It took me roughly 2 weeks to complete the coursework. While it is not compulsory, I chose to document all of the lab exercises in an effort to gain an extra 5 points in the exam. It was also a good way to hone my documentation skills.

2. The Labs

When your lab access starts, you will be granted access to the Offensive Security PWK labs. They consist of a few subnets, and many vulnerable machines. It's your job to own them. Go nuts, try things, experiment and learn.

3. The Exam

I'm not sure how much information I'm allowed to give here so I'm going to keep it fairly vague. The exam lasts 23 hours and 45 minutes. During this time you will connect to the exam network where you are provided with a series of vulnerable boxes, similar to the labs, only smaller. It is your job to break into these boxes and document your process.

Once you've completed your exam, you follow the submission guidelines *very carefully* and wait for the (hopefully) good news!

What's the difference between PWK and OSCP?

PWK stands for "Penetration Testing With Kali Linux", it is the name of the course you take in order to become an OSCP (Offensive Security Certified Professional).

How do the hackthebox/vulnhub boxes compare to the OSCP labs?

In my experience, challenge sites tend to have a lot of CTF style boxes which are self contained. The vulnerabilities in these boxes could be something you are highly unlikely to find in a real-world pentest, such as a file hidden inside an image, or plaintext passwords in HTML comments. OSCP labs are (mostly) focused more on real world applications. The labs even include client-side exploits, lateral movement and pivoting.

My thoughts about the "try harder" mentality

During your time in the labs, you will hear the offsec training slogan "try harder" being thrown around a lot. I get it. Good hackers have an unwavering thirst for knowledge. When you think a box is unbreakable, you need to enumerate again—harder, learn more, explore new avenues and not give up. I assume this is what the offsec staff mean by "try harder". The problem is, students can often misinterpret the message. Do not take the message to mean "don't take breaks", "don't go outside", "don't learn from others", "don't ask for help" or "belittle others". Different people learn in different ways, and I happen to learn well socially. Chatting with other students was one of my most valuable learning resources, but you have to talk in the right way. Spoilers will not help you learn, topics will, which brings us to our next point.

How to ask good questions

"Ask topics, not boxes." That pretty much sums it up. Let's say you're attacking a machine called "foo" which is running SMB. Don't ask "How did you hack foo?", instead, ask "What are your favourite techniques for enumerating SMB?". That way, instead of learning how to hack one machine, you have learned the skills to enumerate any SMB service you come accross in future.

Tips for the exam

- Read every word in this document multiple times: OSCP Exam Guide
- Take regular breaks
- Plan your time before the exam begins
- Document as you go
- Back up your notes regularly to avoid data loss
- If it seems too complicated, it's probably not the right path
- Believe in yourself, it's easy to get overwhelmed

Official Support

- Exam guide: https://support.offensive-security.com/#!oscp-exam-guide.md
- Support info and FAQs: https://support.offensive-security.com/#!pwk-support.md
- Chat live with the offsec staff: https://support.offensive-security.com/chat.php

Where are the other parts of this guide?

If you’re not finished reading just yet the other parts of this guide are below:

Luke’s Ultimate OSCP Guide: Part 2—Workflow and documentation tips

Luke’s Ultimate OSCP Guide: Part 3—Practical hacking tips and tricks