Yet Another OSCP Exam Blog Post

Hausec Infosec April 18, 2019 6 Minutes

I started my OSCP journey well over a year ago, almost two. It was a long time ago, but I remember still not knowing a lot and having anxiety because I'm not sure I'd do so well. When I finally decided to enroll, it was because someone told me that I didn't have enough experience and I'd fail. If there's one thing I am, it's competitive. When someone tells me I'll fail or there's a low chance of success, I'm going to do it. So I enrolled in Penetration Testing with Kali Linux (PWK), which is the actual name of the course you go through before you take the Offensive Security Certified Professional (OSCP) exam. I learned *a lot* comparing myself to almost two years ago, but there's certain things I've learned along the way that I think I should share with everyone because there's a lot of misinformation about the exam and course that I think I should clarify.

Let's start with the ugly truth: The OSCP exam does not make you ready to be a penetration tester. This goes against every blog I've read, but I'm being 100% honest here when I say there's a ton of stuff PWK/OSCP doesn't teach you. First and foremost, it has zip about Active Directory pentesting, which all pentesters will tell you is the number one thing that's going to be exploited in 95% of environments. To not have a module on AD in PWK was very disheartening. Second, the OSCP had a lot of CTF-like elements in it. If you've gone through the course, you know what I'm talking about, but if you haven't then just keep in mind that not everything you encounter is realistic.

With that being said, I'm not discrediting the OSCP at all, this is by far the hardest certification I've done and the course teaches you the mindset of a pentester, which is huge, but I don't want people to automatically assume since they're an OSCP they're ready for a job. I've written all about AD security, so I encourage you to go and read those posts. This goes for any certification though, the grind does not stop once you're certified. If anything, you need to push harder. Being in this field requires dedication, which means not clocking out at 5PM and not touching anything infosec related until the next morning. Always be doing research, always be improving yourself, always have a lab to practice in because it will show during an interview.

With that being said, here's the bit you've been reading for, some actual advice for PWK and OSCP.

1. Keep notes

It doesn't matter how, or what you use (I used KeepNote), but take notes and log everything you do. For the exercises, take plenty of screenshots and write out how you did them. That way, if you want those 5 extra bonus points for the OSCP exam, you can basically just copy+paste. In addition, keeping notes during the labs helps refresh your memory.

2. Get in the habit of screenshotting

Once you compromise a box, screenshot the output of if/ipconfig, whoami, and the flag. You have to do this on the exam to get points, so get in the habit of doing it in the labs.

3. Read up on Windows privilege escalation.

The course material does a real crappy job of teaching Windows PrivEsc. The one thing I recommend doing, if you pop a low-priv shell on a Windows box, is running two scripts

1. https://github.com/rasta-mouse/Sherlock/blob/master/Sherlock.ps1
2. https://github.com/PowerShellEmpire/PowerTools/blob/master/PowerUp/PowerUp.ps1

Sherlock will look at the installed patches and see if there's an exploit out there for missing MS patches.

PowerUp will look for almost everything else. It's *really* good at finding things like unquoted service paths, cached passwords, and much more.

These two scripts will escalate you to SYSTEM most of the time. Otherwise, the answer lies within enumeration.

Additionally, read these.

https://guif.re/windowseop

https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

4. Read up on Linux privilege escalation.

The course also does not teach you much about Linux privesc. I think the hardest thing here is just establishing what is 'normal' for a Linux machine. What I mean by

that, is when you run a script like LinEnum.sh and it finds all these services running, which one is the one that is meant to be exploited? Really, only experience helps here to recognize what is not normal on a Linux machine. Other than that, run these scripts

https://github.com/rebootuser/LinEnum/blob/master/LinEnum.sh

https://github.com/jondonas/linux-exploit-suggester-2

In my experience, these are the only two that you really need. In addition, read these blogs

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

https://blackwintersecurity.com/

https://guif.re/linuxeop

5. Don’t overthink it.

Believe it or not, this course is meant to be entry level. When I tell people that, they get all upset. Keep in mind, pentesting is not an entry level field. It’s meant to be at the top of the profession because you’re incorporating all the knowledge you have

as a system and network admin, and using it offensively. So PWK/OSCP is an entry level course into an expert level field. With that being said, a lot of the times the answer is right in front of you.

6. Do the buffer overflow exercise multiple times.

After my nearly two-year hiatus from PWK, I reupped for 15 days and in that time I only did the buffer overflow exercise. Why? Because if you can do it in the exercise, you can definitely do it on the exam, hint hint. My suggestion, and what I did, was build a template with the commands you'll run (e.g. offset.rb, !mona modules, etc.) and the required components to the buffer overflow (buffer size, JMP ESP location, etc.) that way you can just fill it out, plug it into your script, and done.

7. Try to avoid Metasploit

Metasploit makes things easy, but it takes away from some of the knowledge you learned. Some machines will intentionally not work with Metasploit but will work for another script. My recommendation is this: If you run searchsploit against something and find there's a Metasploit module and a Python script for the same exploit, run the Python script. On the exam, you get to use Metasploit once, against one target. I used it on a target and it failed, so it was a waste. I still passed without it.

8. Hackthebox.eu

I cannot recommend enough Hackthebox.eu. This wasn't as big as it was when I first started PWK, but now it's huge and the boxes there are very similar to what's in the course and exam. These are the machines most like the course.

https://forum.hackthebox.eu/discussion/612/oscp-practice

I recommend the VIP subscription as well, as it's cheap and you get much better access. If you get stuck, there's most likely a video from Ippsec on how to solve it. Seriously, his videos helped trememdously. Watch them all the way through and I guarantee you'll learn something.

9. Do the labs

This kinda goes without saying, but I'll read sometimes about people who do like 5-10 boxes in the labs then take the exam. Unless you've been doing CTFs for years, just do the labs. Again, there's a lot of unrealistic things in this course, so even if you've been pentesting for awhile, you need that CTF experience which is where the lab machines come in handy. I had 28 machines compromised before I took my exam.

10. Don't give up

I don’t like the phrase “try harder”. I think it’s implying people don’t try hard, which isn’t the case. Instead, don’t give up. There will be times where you fail to compromise a box, get a hint, and realize it’s dumb easy. Take it as a lesson and move on. There’s people who took the exam over five times, but it doesn’t matter because in the end the certificate is all the same. Keep trying, keep researching, take a break, then get back at it.

Hopefully this was helpful, I’m sure some of this is repeat as there’s a million other blogs out there talking about the OSCP, but just remember it’s really hard, but very rewarding. If you’re on the fence, do it, as there’s no better certification for the money.

Good luck, & have fun!

-OS-101-50323

Be the first to like this.

Published by Hausec

View all posts by Hausec

Published

April 18, 2019

‹ CypherDog Cheatsheet

Offensive Lateral Movement ›

2 thoughts on “Yet Another OSCP Exam Blog Post”

mzet

September 3, 2019 at 11:07 am

For identifying Linux priv escalation opportunities I'm also recommending: `https://github.com/mzet-/linux-exploit-suggester` and not only because I'm the author but because it has some additional tricks to reduce false positives (see here: `https://mzet-.github.io/2019/05/10/les-paper.html`) if interested.

Cheers

Anonymous
July 26, 2019 at 5:17 am

Nice blog. Thx for sharing. I have my exam today..

Leave a Reply

Enter your comment here...

Follow Me on Twitter

On Github