Lessons Learned- 4 Certs in 11 months

			
Pass	Pass	Pass	Fail x3

```
$>whoami
```

Hello there!
My name is Ray. Thanks for taking the time to read my blog. I imagine, if you've found yourself here you might be interested in ethical hacking, or trying to weed through the absolute mountain of information on which certifications are the best.

As the title alludes, I attempted 4 certifications in the last 11 months. I've succeeded, but also failed spectacularly. The following are my experiences and my opinions. As with everything, opinions will vary greatly, my goal is to provide my insights in the hope someone will find them

helpful. I encourage you to form your own opinions, and if you find it valuable, attempt all of these certifications.

"Every journey begins with a single step, all we need is the courage to try"- Some Smart Guy

The PNPT Cert #1

The Practical Network Penetration Tester certification is offered by TCM Security The course material for this certification includes 5 different courses of study.

1. Practical Ethical Hacking
2. The External Pent Test Playbook
3. Linux Privilege Escalation
4. Windows Privilege Escalation
5. Open Source Intelligence

This exam should be considered an Intermediate exam. And unless you are very comfortable with Linux and all the various tools used to attack networked machines I would suggest you attempt the PJPT Certification first. This was just my path.

Some notable differences between the PNPT and other certifications. **"The Hacker Mindset"**,**OSINT** or Open Source Intelligence, and the **Client Debrief**.

The Course Material

The courses at TCM are very well done. Heath Adams has a style of instruction that is very easy to follow and honestly feels more like conversation than someone dictating "just do this". Heath explains the why behind what he is sharing.

To maximize your success with the course join the TCM discord. The support staff are world class and very responsive. Be sure you read all the pinned messages and follow course suggestions. If you do these simple things I promise you'll get the most out of those courses.

The Exam

What to expect

The cool thing about the exams from TCM, they are "On Demand" meaning there isn't any need to schedule the exam. Purchase your voucher, navigate to the exam website and begin. Additionally, the exams are not "Proctored" meaning there isn't someone watching you.

The PNPT is a lot of things, one thing it is not; a CTF. The structure of the exam mimics a real life engagement, with a scope and rules of engagement.

There aren't any flags to capture. Achieve Domain Administrator and report your findings with a remediation plan. If your report meets the standards, its on to the final Debrief. This for me was the most nerve racking part of the exam. A member of TCM staff assumes the role of the client, and its up to you to explain how you were able to gain access and how to better secure the network to prevent further breaches.

Overall I had the most fun with this course and exam. This experience lit a fire in me to learn more, and set me on a path to soak up as much as I can.

The PJPT Cert #2

The Practical Junior Network Penetration Tester exam is the PNPT's baby brother. While the PNPT covers 5 courses of study, this exam only covers the Practical Ethical Hacking course. **EVERYTHING** you need to be successful at this exam is in the PEH course material.

I know what you are thinking. You got the PNPT then the PJPT? Yes. Why? Because it was fun. I actually completed both exams in the same week.

I'm not sure how to explain it, but after completing the PNPT I missed not having something to work on. So I

pulled the trigger on the PJPT. And coming off the PNPT the PJPT lasted an entire hour and I was back to writing a report. No debrief needed for the PJPT so I had my passing result in less than 10 minutes. Again, the support staff is world class.

Don't discount this exam/certification! Yes its a beginner certification. I was still able to take away some lessons from this exam.

The Exam

What to expect

Same as the PNPT

DISCLAMER

Before I continue,

The following is by no means, intended or otherwise, meant to dissuade anyone from attempting this certification. These are my thoughts, not yours.

The OSCP Cert #3

The Offensive Security Certified Professional. By far this is the most referenced penetration testing certification

on job listings. Well known to be a difficult exam, but not for the reasons you may think.

The Course Material

The PEN-200 course offered by OFFSEC covers all phases of penetration testing. From Recon to Root. And here is where my issues with this course start.

The PEN-200 course is divided into learning modules and lab modules. Unless you are independently wealthy most students opt for the 90 day access of the learning modules and the labs for 1600.00 US dollars. That is about 18 dollars a day. As someone trying to work a full time job, deal with everyday problems and sleep, I think maybe I got to dedicate a maximum of 2 hours a day during the week, to the PEN-200.

To compound the pain the learning modules were packed with tasks that often had very little to do with the material taught in them. If i were to teach you that 2+2=4. Then quizzed you on the half life of uranium 235. Most would fail.

The labs were pretty straight forward however for the price of access I expected more. An example of this, the labs included 3 OSCP exam like groups of machines. An

Active directory set and 3 standalone machines. All of the practice exam AD sets had the same Domain Administrator password.

The Exam

What to expect

Unlike the PNPT/PJPT you must schedule your exam in advance. As I'm sure you can imagine weekend slots for the exam go quick. If you work a full time job like me, schedule way in advance. Also this exam is Proctored by Offsec staff. I have a dedicated Kali laptop. Personally I prefer to use Plasma KDE. Spoiler alert. The ssdm display driver does not play well with Offsec's proctoring software. Use gdm to avoid having to troubleshoot during your exam like I did.

Offsec will have you log into the proctoring software 15 minutes before the start of your exam. The proctor will check your legal identification, and ask to view your surroundings where you will be taking the exam.

As much frustration as I had with the course material, I had the same with the exam. I never felt, during the exam, that I was faced with technology or configurations that were new to me. My frustrations stemmed from

trying an attack and having it fail time after time. After hours, sure I had tried everything, I would revert the machine and have the same attack work. Again for the price I expected better.

With all that said I will continue to attempt the exam until I complete it, because I don't give up. 4th time is the charm.

The Certified Penetration Testing Specialist Cert #4

Hack The Box's Certified Penetration Testing Specialist job role path and certification was simply amazing. This was everything I had hoped the PEN-200 would be. However it may not be for everyone. Here's why.

The Course Material

Before attempting this Certification the student has to gain 100% completion of the Penetration Tester job role path from the Hack The Box Academy
The course of instruction has 28 modules, over 480 sections of content. Much like the PEN-200, the material covers recon to root. Multiple tools, TTPs (Tactics,Techniques,Procedures), attacking common services etc.

The entire course is text based. No video's like the PEN-200 or the PEH. I believe HTB estimates it takes 42 days to complete the course material. I managed to complete the course in 6 months. While it may seem like this is a beginner course, it is not. Can someone just starting out without any prior training complete the course and achieve the cert? Maybe, for me not having the prior experience of the PNPT and the ability to put the material into context it would have been tough.

The Exam

What to expect

Like the PNPT the exam is On Demand and not proctored. Prepare yourself, as the difficulty level is elevated a good amount. While the PNPT mimics a small to medium sized business, the CPTS is about attacking an Enterprise level network.

The exam is tough. But not impossible. There were periods where I was stuck for hours and days and periods where I advanced through the exam really quickly. Overall, this was the course/certification I learned the most from.

Lessons Learned

PNPT-

1. Mindset is incredibly important. Self belief is a real thing and its powerful. Cultivate a mindset that not only is compatible with the "Hacker Mindset", but also a mindset where you believe you can succeed
2. Breaks are important, your mind needs rest.
3. Don't discount information. However trivial it appears to be, it could very well make all the difference

PJPT-

1. Post exploitation of a target is essential. Check everything.

OSCP-

1. Nothing is ever perfect. You can complain or overcome.
2. Failure is not who you are as a person. Learn from it, improve, and move on.
3. Enumeration scripts like Linpeas and Winpeas are nice but sometimes you just need to look for yourself

4. Check the easiest path first. Just because in you think that would be too easy doesn't mean you should rule it out.
5. Don't rely on automated tools. Yes they make life easy but they shouldn't be your only tool.
6. Have a plan. but be flexible.

CPTS-

1. Having a solid, repeatable methodology is what carries you through a tough exam
2. Detailed notes are life. Arrange them logically. Being able to reference them in a manner that is logical will save your bacon
3. Report as you go. Trying to complete a professional report over 80 pages in 6 hours is a fools errand.
4. Be comfortable with being uncomfortable. You will not know everything. Take a breath and research. The answers are available
5. Time is relative. Be aware of the clock but don't panic. You could be seconds away from success.
6. Double check your report. Encrypted reports don't get reviewed.

In Closing

What would I do differently if tomorrow I had to start over?

I think the one thing I would adjust is completing the HTB job role path before attempting the OSCP. My frustrations with the PEN-200 course Left me lost and questioning my commitment to pursue this line of work. To fail 3 different OSCP attempts was a gut punch. A hit to my ego, I let doubt creep in. The CPTS was just what I needed to reaffirm that yes I can do this.

I would suggest if this field is something you are committed to, find a group of people on discord or a community where people share ideas and support each other. Surround yourself with people who more experienced, have accomplished something you are working towards. Ask questions, contribute, branch out of your comfort zone as that is the only true way to grow.

Dare to be exceptional, be humble, try to learn something from every new person you meet and in return share something. I believe this how we become better professionals.

Well, that is it for now. Thanks for stopping by.

Connect with me.

Github Linkedin medium