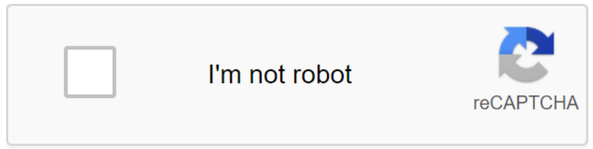

Continue

Offensive security certified professional study guide pdf

Throughout my career, I've always wanted it to focus on information security. I'm always looking for ways to improve my penetration testing skills. My hunger for knowledge and my strange craving for challenges that push me to the limit remained insatiable. Proof is something important to me, as is the creation of my InfoSec credentials. These are probably some of the main reasons why I took the OSCP certification exam. What is OSCP Certification Training? Offensive Security Certified Professional (OSCP) is a certification program that focuses on practical information security skills. It consists of two parts: a nearly 24-hour pen exam test, and the documentation report must be 24 hours after it. OSCP is a very hands-on exam. Before you pass the OSCP exam, you must take the Kali penetration test (PWK). Taking a course is a must for you to qualify to take OSCP. In addition to the knowledge you get from the course, it opens the door to several career opportunities in information security. Of course, those who pass get bragging rights too. How difficult is it to get OSCP certified? If you ask OSCP-takers about the difficulty level of the exam, you will get a variety of answers, but most people say it is the most difficult exam they have taken in their lives. That's why it's important to prepare well for it. The PWK course doesn't teach you everything, but there's enough material to get you started. I can't stress enough on the importance of pre-course training. Here's a list of things you have to learn to prepare for OSCP: Linux and Windows environment - you should be familiar with both. This will help you identify the keys to escalating privileges. I'm a Windows guy and during the lab, I learned Linux the hard way. Linux and Windows Commands - Knowing the Linux and Windows commands helps a lot. Brush on them! Basic Programming Skills - Expect to debug and rewrite feats, so know the Bash script. This will help you automate redundant tasks. Web Application Attacks (S'L, XSS, Local File Inclusion, Remote File Inclusion and Execution Commands) - Expect a lot of web application content in labs. It is also a practice of bypassing web security filters for injecting attacks. Metasploit Framework - Cleaning to create a payload with different formats, using multiple handlers, and using phased vs. invulnerable payloads. Knowing these things will save you some time during the exam. Nmap - Different scanning techniques and Nmap NSE scripts will help you a lot during your lab or exam. Netcat and Ncat - You'll use them a lot during OSCP. Wireshark and tcpdump - This is important because you will use Wireshark to debug your feat - tcpdump when machines don't have a graphical interface. Escalating privileges of Windows and Linux - Aside from using core exploits, brush up to refresh weak service/file permissions and NFS/Shares. Escaping from limited shells and spawning shells - you will encounter this a lot during OSCP. File Transfer - It's important that you know the different methods of transferring files to the target machine. Aside from these themes, these books also come in handy: Time to get your hands dirty! After reading and reviewing the topics above, you can apply what you've learned with this: I hope my suggestions will help you in your OSCP journey. If you want to learn more about my experience, you can check out my blog for cribs and methodology I'll be downloading it soon. If you have questions or need help, you can contact me via Twitter @blad3ism. I wanted to do this post detailing everything I did while studying for the OSCP exam. I made many mistakes along the way, and my path was far from the most effective and effective method to study to OSCP. However, I have learned something from every resource listed here, and I firmly believe that everything I have done has some value. With that in mind, there is always room for optimization, and in the interest of creating a resource to help people work towards OSCP as best I can, I've streamlined what I've done in a more targeted list. Keep in mind that this is designed for people who are brand new to penetration testing as I have been, so for those with more experience feel free to miss a few points below. My complete way to get OSCP, from scratch to hero style: In case you don't, complete all the beginner and advanced machines on the Virtual Hacking Labs platform before another exam attempt. I am confident that this path, combined with determination and the right attitude, will lead to success. This is without a doubt the way I would take it if I had to make the whole process more. For a full breakdown of everything I did in the run-up to the OSCP passage, read the rest of this post below. I've included links to relevant blog posts for further reading on specific platforms or resources, as well as some of my favorite tools that I've often used. My detailed experience with all the OSCP experience can be found in the accompanying post Pre PwK Preparation Before I even started in PwK coursework and laboratory environment, I put in a decent amount of research to make sure I'm not going to get too overwhelmed. Looking back, I think I have prepared too much, and not all of what is useful or relevant here. If you're a complete beginner, as I was, I recommend reading Penetration Testing - Hands on Hacking and Watching IppSec Videos Easier HackTheBox Machines. If you want to spend more time getting an eJPT certification can also be a useful thing. After that, just jump straight and give PwK a go. For More information my PwK Preparation, check out this CompTIA Security Security blog was my first security certification, so I included it here for the sake of completing. Not exactly relevant to OSCP, but useful to have for someone who is a complete beginner in security. Click here for a link to my blog where I discuss this certification further. Penetration Testing - Hands on the introduction to hacking Georgia Weidman's Incredible Book, this should be a read for beginners. It acts as an excellent segue in the pwK course as this technical guide walks readers through the basics of penetration testing. The Georgia accompanying video series on Cybrary, called Advanced Infiltration Testing is also helpful. I have written an in-depth review of this book for those interested in giving this a read. Hacker Playbook 2 Peter Kim is an interesting book that acts more as a reference guide, this book is useful to familiarize yourself with some of the tools and terms you may come across, but not particularly necessary in my opinion. I also wrote an in-depth review for this book that is available in another post. Kioptrix 1-4 on Vulnhub My First Vulnerable Machine, the Kioptrix series is well known in the community as a beginner friendly. There are also numerous step-by-step guides available that you can use to follow along with, including my own. IppSec video tutorials retired HackTheBox Machines I then watched the IppSec video collection, especially the ones it made for lighter machines. Having along with the video is extremely useful to help familiarize yourself with the commands and tools it uses. His channel can be found here Post PwK Lab Time I managed to get root or system access to 28.5 machines in the PwK lab environment, but wasn't sure I was good enough to pass the exam. I pushed the exam date a bit out of when my lab time was over and did some more research in between. Vulnerable machines on HackTheBox I almost exclusively used HackTheBox during this time, focusing on retired machines. I completed 25 OSCP-esque machines listed below, often using step-by-step guides or IppSec videos. Looking back, I think I would have learned a lot more at the moment if I had refrained from working alongside the video, but at the time my main concern was the impact of a wide range of services and attack vectors. I strongly recommend trying these machines without any help. Trying the exam #1 (failed with 65 points) I gave the OSCP exam a really good go, but in the end, I was just shy of passing on my first attempt - finishing with 65 points. I was so close to passing that even now I'm sorry I couldn't finish my exam for the first time. I feel like as soon as a little more I could passed, but it just wasn't meant to be. Details of this exam attempt and the reasons why I may not be in my post exam to write. Before the exam #2 (passed with 85 points) It was here that I made significant progress and learned the most. After a 3 month break to accommodate some big changes in my life, I jumped back into school. Deciding not to extend the lab time and check the waters with other external services, my focus was on web applications and the privileges of escalation. From what is listed below, Virtual Hacking Labs deserves special mention - it's absolutely incredible. PentesterLab I tried this platform as a colleague recommended it to me and it allowed for some targeted research on web application testing. Although interesting and well done, I personally didn't find it as valuable as racking up a more hands-on experience turned out to be. I've completed a web application basic icon that I discussed in some detail in another blog. Vulnerable machines on HackTheBox I went back to HackTheBox and completed 5 of the easiest active machines, taking my full tally on the platform to 30 machines. Active machines don't have step-by-step manuals available, as retired machines do, and are quite sophisticated (despite their easy ratings). In my opinion, the current generation of light active machines is noticeably more complex than what is in OSCP, so keep this in mind when completing these machines. eLearnSecurity Junior Pentest I then turned my attention to eJPT as I thought it would be a good overcoming certification as I continued to learn for OSCP. Although it is usually well thought out and executed, it was too easy for me at this point in my studies. I would recommend this for beginners as a precursor for admission to the PwK course. Virtual Hacking Labs I can't say enough good things about the virtual hacker lab platform. In my opinion, the utensils and the lab environment they provide are superior to what Offensive Security provides. I completed all 28 of the available 42 machines, and learned something new from each one. I believe that of all listed here, I got the most value from virtual hacker labs. For those who use this platform now or in the future, be sure to visit an unofficial channel of contention that is full of friendly and helpful members. Recommended tools and scripts, finally, I want to give a mention of some of the tools that I personally used while passing OSCP. These tools are not included in the default Kali Linux distribution, so I recommend downloading them and trying them for yourself. AutoRecon from Tib3rius - An incredible tool that makes listing much easier, this tool is basically a necessity for those trying the OSCP exam. Dirsearch by maurosoria - My go to listing tool, I personally believe this tool will be much faster faster more versatile than GoBuster or Dirb. pspy Dominic Breuker - Linux process monitoring tool, pspy is great for browsing running processes to detect cron jobs or other potentially exploited services. It came in handy a few times. Linux-smart-listing Diego Treitos - One of the best Linux privileges escalating tools out there, this has always been my first port of call when faced with a low privileged Linux shell. J.A.W.S by 411Hall - I've found that this script provides the most information needed to escalate Windows privileges, and it's worth working with a low-privilege Windows session. Session. offensive security certified professional study guide pdf