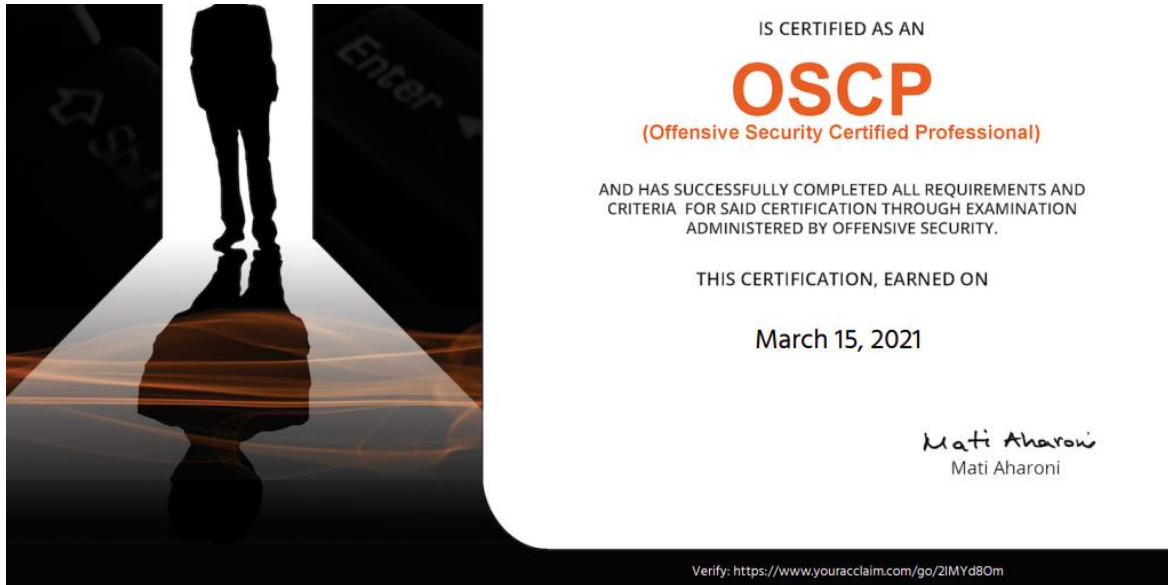


**Passing OSCP with 100
points in 12 hours in
first attempt with OSCP
Preparation Guide, 2021**





OSCP Digital Certificate

Here's my Webinar on The Ultimate OSCP Preparation Guide.
The Ultimate OSCP Preparation Guide 2021

I'm 21 years old and I decided to take OSCP two years ago when I was 19 years old. I had to wait for 1 and a half years until I won an OSCP voucher for free. Not just a normal 30 days lab voucher, but a sophisticated 90 days lab voucher that costs about 1349\$. Here's [How I cracked Secarmy's OSCP challenge and won the OSCP lab voucher for free.](#)



**DESTROY THE FEAR OF BUFFER
OVERFLOWS BY BECOMING AN EXPERT IN IT**



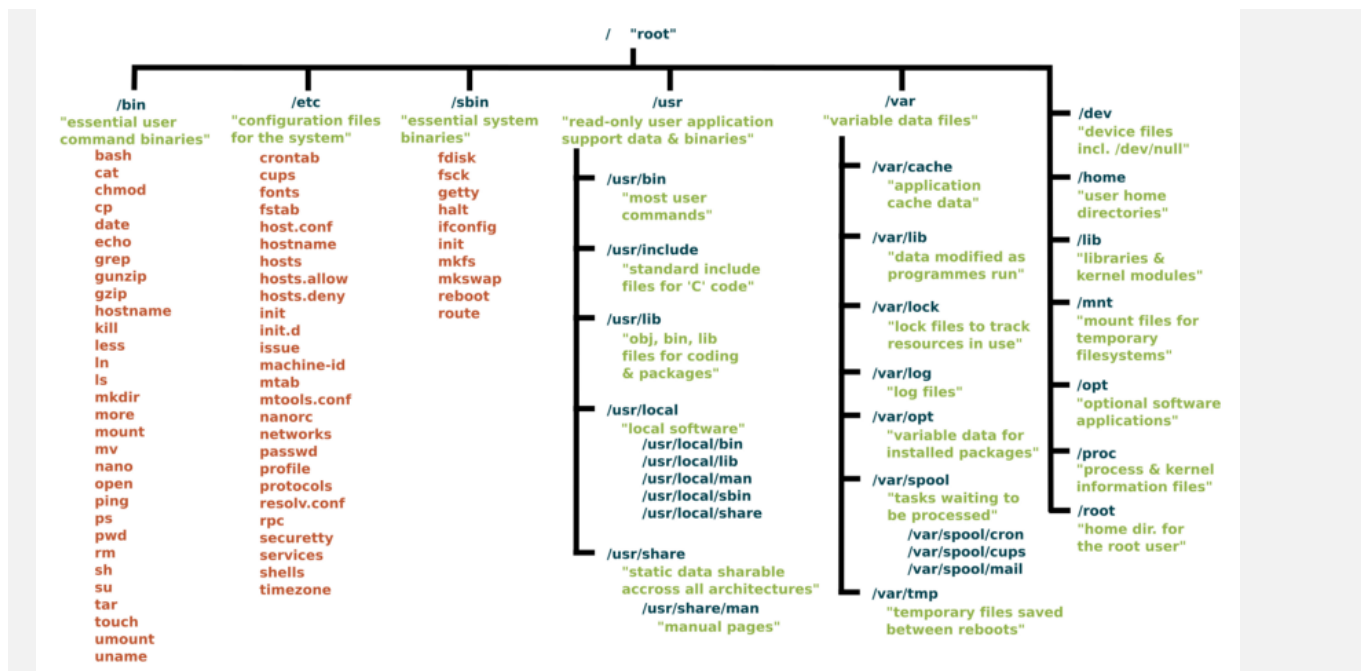
Even though I had no idea when I'll be taking OSCP, or even will I be able to afford it, I just started learning buffer overflows hoping that at one point in my life, I will be able to afford the exam cost. LOL... Crazy that, it all started with a belief.

Passive Preparation 1 year ago :

HackTheBox for the win. I started HackTheBox exactly one year ago (2020) after winning an HTB VIP subscription in Nova CTF 2019. I practiced OSCP like [VM list by TJNull](#). Because I had a few years of experience in application security from the bug bounty programs I participated in, I was able to get the initial foothold without struggle in HTB machines. But that's not the case of Privilege escalation.

So, I wanted to brush up on my Privilege escalation skills. You can find all the resources I used at the end of this post. Getting comfortable with Linux and Windows file systems is crucial for privilege escalation. This will help you find the odd scripts located at odd places. Spend hours looking at the output of privilege escalation enumeration scripts to know which are common files and which aren't.

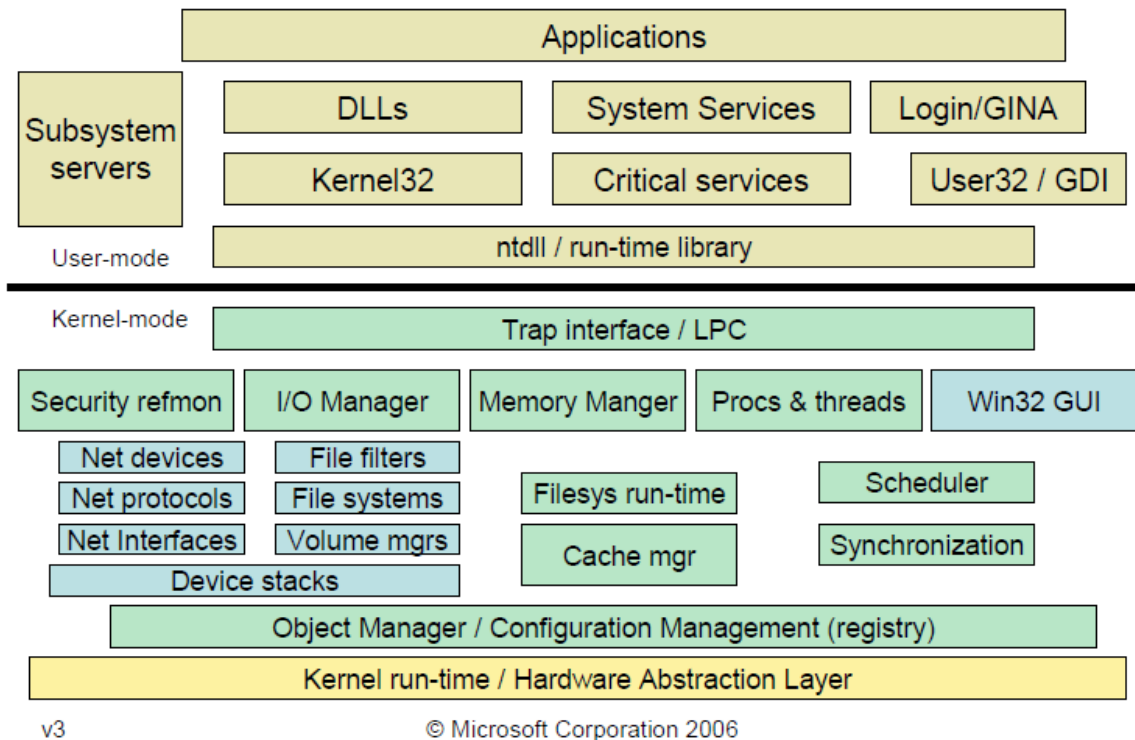




Linux Filesystem Architecture



Windows Architecture



Windows Architecture

Active Preparation 45 days :

My PWK lab was activated on Jan 10th, 2021. My lab experience was a disappointment. I felt like there was no new learning. I pwned just around 30 machines in the first 20 days I guess, but I felt like I'm repeating. So, I paused my lab and went back to TJ null's recent OSCP like VM list. Pwned 50-100 vulnhub machines. I sincerely apologize to Secarmy for wasting their 90 days lab 😞



Whenever I tackle new machines, I did it like an OSCP exam. I will always try to finish the machine in a maximum of 2 and half hours without using Metasploit. Of

course, when I started pwning machines a year ago, things weren't going exactly as I planned. It took me more than a day to solve an easy machine and I was stuck often. But I made notes of whatever I learn. So when I get stuck, I'll refer to my notes and if I had replicated everything in my notes and still couldn't pwn the machine, then I'll see the walkthrough without guilt :)

Feel free to make use of walkthroughs but make sure you learn something new every time you use them

I never felt guilty about solving a machine by using walkthroughs. New skills **can't** be acquired if you just keep on replicating your existing ones. Walkthroughs are meant to teach you. It's not like if you keep on trying harder, you'll eventually hack the machine. You aren't here to find zero days. Use walkthroughs, but make notes of them so that you won't have to refer to a walkthrough if you had to pwn the same machine a few days later.

In mid-February, after 30 days into the OSCP lab, I felt like I can do it. There's no clear indication of when you can take it. But I decided to schedule the exam after this.

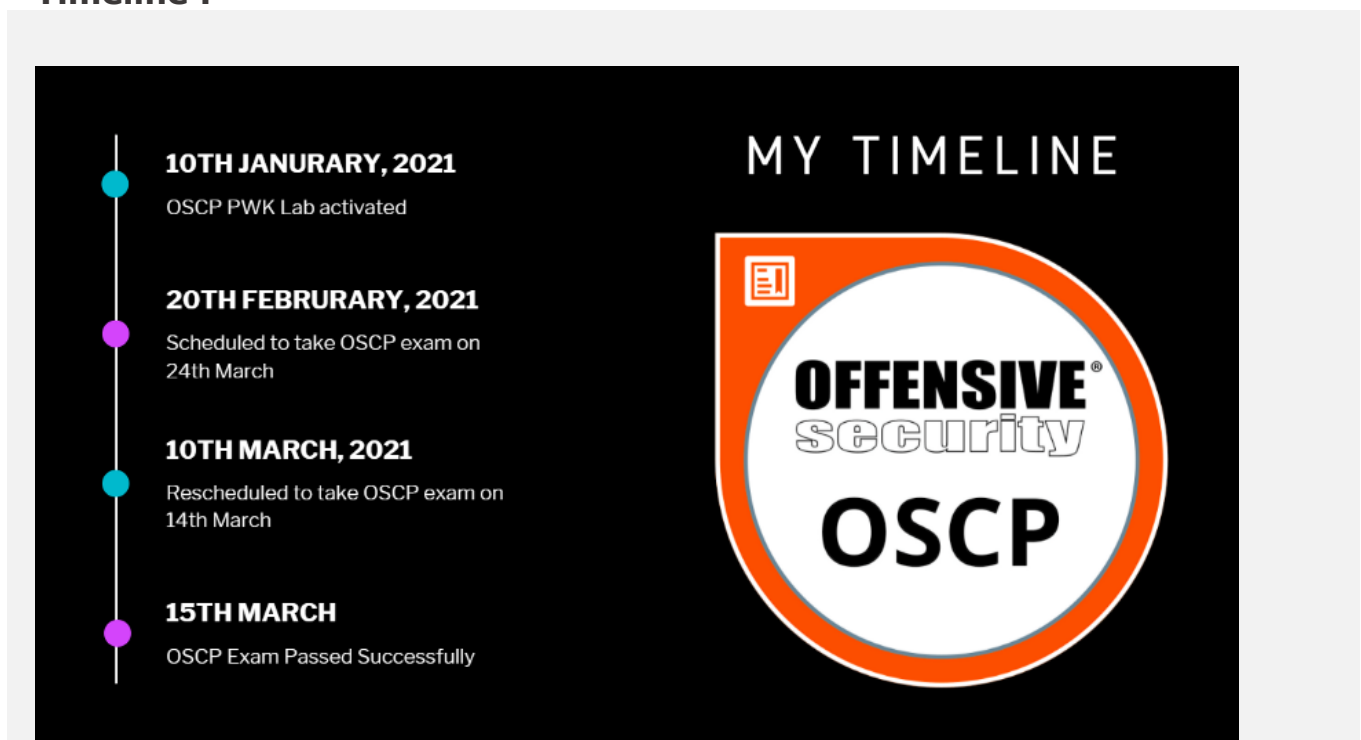
How did I know I was ready?

Whenever I start a machine, I always have this anxiety about whether I'll be able to solve the machine or not. After continuously pwning 100+ machines OSCP lab and vulnhub for straight 40 days without rest, at one point, my anxiety started to

fade and my mindset was like “***Chuck it, I learned so much in this process. It’s just an exam. It would be worth to retake even if I fail***”.

After reaching that point, I faced the next few machines without fear and was able to compromise them completely. On the 20th of February, I scheduled to take my exam on the 24th of March. After scheduling, my time started to run in slow motion. I didn’t feel like pwning any more machines as I have almost completed TJNull’s list. I was afraid that I would be out of practice so I rescheduled it to 14th March. From, 20th February to 14th March (22 days prior to exam day), I haven’t owned a single machine. I just kept watching videos, reading articles and if I come across a new technique that my notes don’t have, I’ll update my notes.

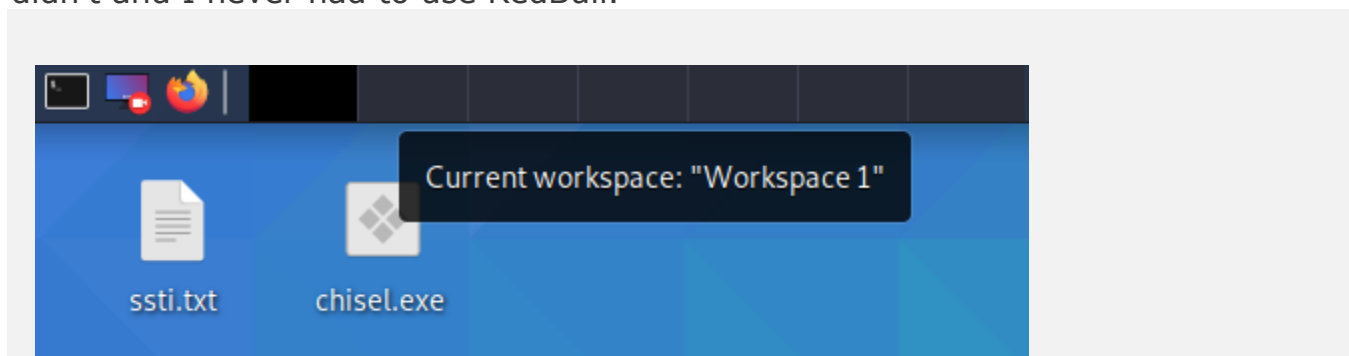
Timeline :



My timeline for passing OSCP

Exam Setup :

I had split 7 Workspaces between Kali Linux. 5 Desktop for each machine, one for misc, and the final one for VPN. Took a VM snapshot a night before the exam just in case if things go wrong, I can revert to the snapshot state. Created a recovery point in my host windows as well. I used OneNote for note-making as that syncs with the cloud in case if my host machine crashes. In short, I was prepared for all kinds of worst-case scenarios as I was expecting the worst to be honest. I even had RedBull as a backup in case if too-much coffee goes wrong 😊 Thank god it didn't and I never had to use RedBull.



Workspace for OSCP

Exam Experience :

I scheduled my exam to start at 5.30 A.M. Because I wanted to finish the exam in 24 hours without wasting time for sleep (although people say sleep is crucial, I wanted to finish it off in one run and sleep with peace). Sleep doesn't help you solve machines. It will just help you take a rest. But working for 24 hours is fine with me. That way, even if things go wrong, I just have to stay awake till maybe 2-3 a.m to know if I can pass or not, and not the whole night. If I had scheduled anytime during late morning or afternoon, then I might have to work all night and my mind will automatically make me feel like I'm overkilling it and ask me to take a nap. So, 5 a.m was perfect for me. Woke at 4, had a bath, and drank some coffee. Logged into proctoring portal at 5.15 and finished the identity verification.

Respect your proctors. Greet them. Get comfortable with them. BE sure to remember that they are humans, not bots lol. My Proctors were super friendly and coped with me even when I had few internet troubles and screen sharing issues. I had no trouble other than that and everything was super smooth.

My strategy to pass:

1. BOF
2. 25 pointer
3. 20 Pointer

Thankfully things worked as per my strategy and I was lucky.

Luck is directly proportional to the months of hard work you put

Created a targetst.txt file. Pasted the 4 IPs (excluding BOF) into targets.txt and started with

```
autorecon -t targets.txt — only-scans-dir
```

Buffer Overflow — 25 Points :

While that was running, I started with Buffer Overflow like a typical OSCP exam taker. I'm super comfortable with buffer overflows as I have almost 2 years of experience with it. I had to finish it in 30 minutes and hell yeah, I did it. Though there were few surprise elements there that I can't reveal, I didn't panic. Because

the writeups of OSCP experience from various people had always taught me one common thing

Pray for the Best, Prepare for the Worst and Expect the Unexpected

Took a break for 20 minutes right after submitting proof.txt for the Buffer Overflow machine.

Hard 25 Point machine :

3 hours to get an initial shell. Took two breaks in those 3 hours but something stopped me from moving on to the next machine. Breaks are helpful to stop you from staring at the screen when the enumeration scripts running. The only hurdle I faced in OSCP is the same issue that we face on HackTheBox. The VPN is slow, I can't keep my enumeration threads high because it breaks the tool often and I had to restart from the beginning. So, I had to run all the tools with reduced threads. So, the enumeration took 50x longer than what it takes on local vulnhub machines. But I never gave up on enumerating. Because, in one of the OSCP writeups, a wise man once told

I'm not crying, you are

Once I got the initial shell, then privilege escalation was KABOOM! The only thing you need is the experience to know which one is fishy and which one isn't. This experience comes with time, after pwning 100's of machines and spending countless hours starting at **linpeas/winpeas** output.

After 4 hours into the exam, I'm done with buffer overflow and the hardest 25 point machine, so I have 50 points in total. I'll pass if I pwn one 20 point machine. Didn't take a break and continued to the 20 point machine.

First — 20 point machine:

10 minutes to get the initial shell because all the enumeration scripts were already done and I had a clear path. Thank god, the very first path I choose was not a rabbit hole. It would have felt like a rabbit hole if I didn't have the enumeration results first on-hand. So, I highly suggest you enumerate all the services and then perform all the tests. Trust me, testing all your techniques may take 30 minutes hardly if you're well-versed but a full-scale enumeration in that slow VPN will take you hours.

Also, this machine taught me one thing. Sometimes, an abundance of information from autorecon can lead you to the rabbit hole. This is where manual enumeration comes in handy. I first saw the autorecon output and was like, "***Damn, testing all these services gonna cost me a day***". So, I discarded the autorecon output and did manual enumeration. It gave me a confined amount of information which was helpful for me in deciding which service to focus on and ignore.

So, after the initial shell, took a break for 20 minutes. Came back. Escalated privileges in 30 minutes. That moment, when I got root, I was laughing aloud and I felt the adrenaline rush that my dreams are coming true. 5 hours 53 minutes into the exam and I already have a passing score of 70 points. I took a 30 minutes break and had my breakfast. For these 6 hours, I had only been sipping my coffee and water.

Easy 10 Point machine:

DO NOT UNDERRATE THIS MACHINE! This is the trickiest machine I had ever seen. Partly because I had underrated this machine from the writeups I read. This cost me an hour to pwn. So, after 07:23 minutes into the exam, I have 80 points and I'm in the safe zone 😊 But I didn't take a break. I did all the manual enumeration required for the second 20 point machine and ran the required auto-enumeration scripts as well. Took a break for an hour.

Second — 20 point machine:

It took me 4 hours to get an initial foothold. Well yeah, you can't always be lucky to spot rabbit holes. I was tricked into a rabbit hole but again, deployed the wise man's **Enumerate harder** tip. Bruh, I got a shell in 10 minutes after enumerating properly 😊 I felt like I was trolled hard by the Offsec at this point.

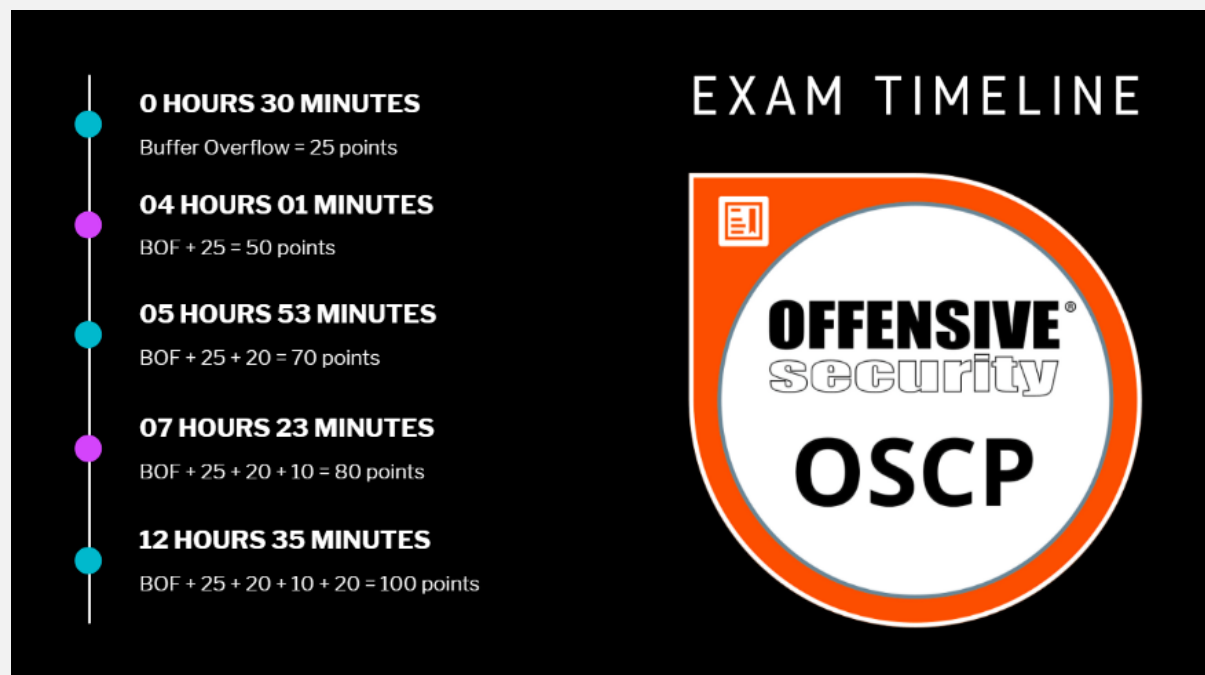
Privilege escalation is 17 minutes. Hehe. I can't believe my eyes I did it in 17 minutes that I had to recheck and rerun the exploit multiple times. I was so confused whether what I did was the intended way even after submitting proof.txt lol 😊

So yes, I pwned all the 5 machines and attained 100 points in **12 hours and 35 minutes (including all the 6 breaks which account for 2.5 — 3 hours)**. Though it seems like I completed the exam in **~9 hours and 30 minutes**, I can't neglect the break hours as the enumeration scripts have been constantly running during all the breaks. I took another hour to replicate all the exploits, retake screenshots, check if I have the necessary screenshots, and ended the exam. I made sure I have the output screenshot for each machine in this format.

Windows : type proof.txt && whoami && hostname && ipconfig

Linux : cat proof.txt && whoami && hostname && ip addr

Exam Timeline :



OSCP Exam Timeline

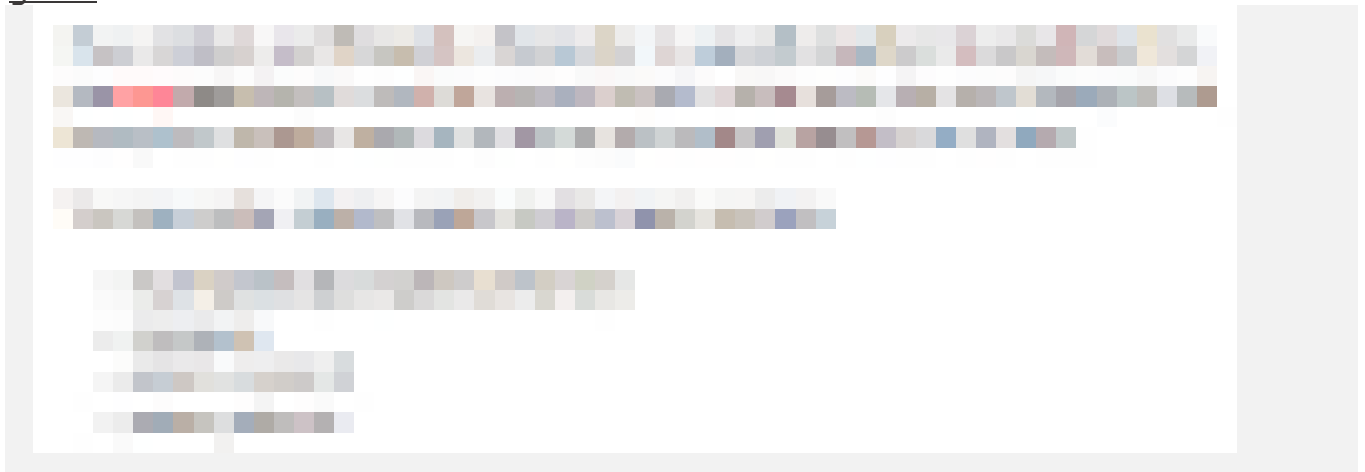
Metasploit :

I forgot that I had a tool called Metasploit installed even when I was extremely stuck because I never used that during my preparation. In fact, during my preparation, I was ignoring the rapid7 blog posts while searching for exploits LMAO!

Also, remember that you're allowed to use the following tools for infinite times.

- multi handler (aka exploit/multi/handler)
- msfvenom
- pattern_create.rb
- pattern_offset.rb

So, make use of msfvenom and multi handler whenever you feel like the normal reverse shell isn't working out and you need to use encoders. Refer to the [exam guide](#) for more details.



If you decide to use Metasploit or Meterpreter on a specific target and the attack fails, then you **may not** attempt to use it on a second target. In other words, the use of Metasploit and Meterpreter becomes locked in as soon as you decide to use either one of them.

You may use the following against all of the target machines:

- multi handler (aka exploit/multi/handler)
- msfvenom
- pattern_create.rb
- pattern_offset.rb

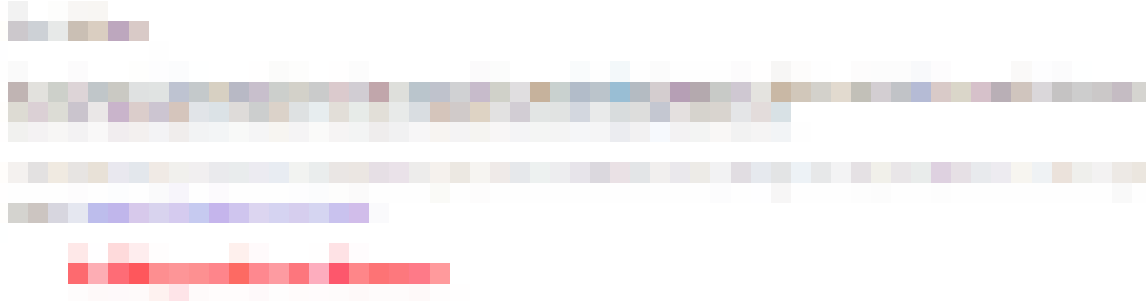
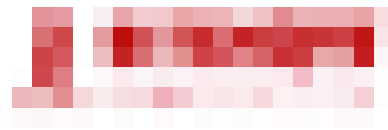
Offsec Exam guide about the use of Metasploit

Reporting :

I used the standard report template provided by offsec. Just made few changes and gave a detailed walkthrough of how I compromised all the machines. My report was 47 pages long. I wrote it as detailed as possible. I did some background research on the vulnerabilities I exploited, including the CVE numbers, the CVSS score, and the patches rolled out for the vulnerabilities. I even reference the git commits in which the vulnerability has raised and the patch has been deployed.

Result Day :

I had to wait 5 days for the results. This was probably the hardest part of OSCP for me. Though I had 100 points, I could not feel the satisfaction in that instance. I have seen writeups where people had failed because of mistakes they did in reports. I waited one and half years to get that OSCP voucher, but these 5 days felt even longer.



Dear Adithyan,

We are happy to inform you that you have successfully completed the Penetration Testing with Kali Linux certification exam and have obtained your Offensive Security Certified Professional (OSCP) certification.

Listed below is your name as it will appear on your printed certification. If any changes are required, please let us know right away at orders@offensive-security.com.

Adithyan Arun Kumar

Results received

View my **verified**

achievement here: https://www.youracclaim.com/badges/0dc859f6-3369-48f8-b78a-71895c3c6787/public_url

OSCP Preparation Plan :

This is my personal suggestion. Instead of buying 90 days OSCP lab subscription, buy 30 days lab voucher but prepare for 90 days. Here's how you can do it.

1. Practice OSCP like Vulnhub VMs for the first 30 days

2. Buy HackTheBox VIP & Offsec Proving Grounds subscription for one month and practice the next 30 days there. Recently, I hear a lot of people saying that proving grounds has more OSCP like VMs than any other source.

3. Finally, buy a 30 days lab voucher and pwn as many machines as possible.

HackTheBox VIP and Offsec PG will cost 15\$ and 20\$ respectively. OSCP 30 days lab is 1000\$. So, It will cost you **1035\$** in total. 90 days lab will cost you 1350\$. You can essentially save up to **300\$** following my preparation plan.

Preparation Tips :

- You'll run out of techniques before time runs out. So learn as many techniques as possible that you always have an alternate option if something fails to produce output.
- Try harder doesn't mean you have to try the same exploit with 200x thread count or with an angry face. Go, enumerate harder.

Exam Tips :

- Bruh you have unlimited breaks, use it. You aren't writing your semester exam.
- 24 reverts are plenty enough already. Go use it.
- Caffeine is a must.
- You're not gonna pentest a real-world machine. You're gonna try to hack into an intentionally vulnerable machine that is vulnerable to a specific exploit.

Exploiting it right in 24 hours is your only goal. So, OSCP is actually a lot easier than real-world machines where you don't know if the machine is vulnerable or not.

- ippsec.rocks is a good resource to use if you need help in exploiting a specific service

Tip for Enumeration :

Enumerate more means:

- Scan ports, scan all the ports, scan using different scanning techniques,
- brute force web dirs, brute force web dirs using different wordlist and tools
- check for file permissions, check for registry entries, check for writable folders, check for privileged processes and services, check for interesting files,
- look for a more suitable exploit using searchsploit, search google for valuable information, etc.
- webserver version, web app version, CMS version, plugin versions

Tip for Foothold :

- Password reuse
- The default password of the application / CMS
- Guess the file location incase of LFI with username
- username from any notes inside the machine might be useful for Bruteforce

- Try harder doesn't mean you have to try the same exploit with 200x thread count or with an angry face. Go, enumerate harder.

Credits :

I thank my **family** for supporting me. My parents are super excited, even though they don't know what OSCP is at first, they saw the enormous nights I have been awake and understood that it's a strenuous exam. I thank Secarmy(now dissolved into AXIAL), Umair Nehri, and Aravindha Hariharan. I'm forever grateful to all my **Infosec seniors** who gave me moral support and their wisdom whenever needed. Finally, I thank all the authors of the infosec blogs which I did and didn't refer to.

Social handles: LinkedIn, Instagram, Twitter, Github, Facebook

FAQ :

How many years of experience do you have?

4 years in Application and Network Security. Overall, I have been a passive learner in Infosec for 7+ years.

How many months did it take you to prepare for OSCP?

One year, to be accurate. Exactly a year ago (2020), I pwned my first machine in HTB. From then, I actively participated in CTFs.

What are you studying?

I completed my undergraduate program in Information Technology and will be pursuing my Masters in Information Security at Carnegie Mellon University this fall 2021.

The Ultimate OSCP Preparation Guide, 2021

An organized guide to highlight some of the smartest techniques and resources for your OSCP journey. Updated with new techniques and refined on: 2/2/2021

Published on Aug 17, 2020

Reading time: 32 minutes.

The Ultimate OSCP Preparation Guide, UPDATED: 2021

Update Notes

Due to popular demand, and some additional observations that have been brought to my attention, I have made the following revisions:

- Expanded on some of the instructional language [to reduce confusion]
- Added additional information to skill-based-tips
- Implemented a King of the Hill TryHackMe practice section
- Expanded the OSCP notetaking section to reflect my thought processes
- Removed unnecessary reliance upon Hacking books and instead made it optional [due to many complaints about dated material]

- Added information about TryHackMe lesson recommendations for beginners
- Fixed TryHackMe Offensive Security Path URL [Now known as Offensive Pentesting]
- Minor improvements to PWK enumeration considerations.
- Various improvements to p/much all sections within this guide

Note: To anyone who has this URL embedded somewhere, it will remain the same to avoid breaking these external references.

Understanding this guide

When I first began my hacking journey, I would bookmark guides and resources like a madman. If you've contemplated tackling the OSCP, you know what I'm talking about: You're browsing google, trying to figure out what the secret sauce is for starting the course, taking the exam, and quite frankly, passing the exam.

There are a ton of issues with the method of bookmarking everything. The most prominent issue is resource overload. I don't know about you, but, I've reviewed my bookmarks at one point and said to myself:

"Oh my God, where do I even start? Do I study commands? Do I learn to code? Do I use TryHackMe or HackTheBox?"

This was the most stressful part of the growing pains that come with the OSCP. I'm going to attempt to take the stress out of this effort for you. Instead of writing some redundant experience of what the exam was like for me, and sprinkling all of my tips throughout the text. I'm going to attempt a much different approach in this guide:

1. Create segmentation between where beginners should start vs. intermediate hackers.
2. Create separate tip sections for beginners and intermediate hackers.
3. Highlight pre-examination tips & tips for taking the exam.

Why would I take the time to create so much segmentation?

Accessibility. You're not here for me; you're here for you. Forgive me if I come off as a little philosophical. I believe that my exam attempt will not be like your exam attempt. I don't want anyone to get stressed out trying to scrape through a writeup to get tips or deduce anything that is untrue about the exam based off of my attempt. I would prefer to give you the tools to prepare for your own attempt. You can determine what type of experience I had with this guide.

For Beginners

First and foremost, if you're new to hacking, welcome to the insanity that is Penetration Testing! **(If you've been hacking for a while and are looking to get straight into OSCP tips, skip to "Intermediate Hackers")** You may have

stumbled upon this guide because you're new, but you have a mountain to climb. You want to obtain the OSCP...it seems impossible, but I promise you. It's not.

Hacking is fun! The rush of cracking into a system and getting a reverse shell is priceless. However, If this is you, we have some work to do:



The funniest part about this meme is the sheer amount of truth that it carries. When you've been hacking for a bit, you'll start to understand why this meme exists.

The prerequisites for starting your Penetration Testing journey:

1. A basic understanding of Networking: Everything taught in CompTIA's Network+ Course
2. Security Practices and Network/Host defense principles: Everything taught in CompTIA's Security+ Course.

If you were to buy some Udemy courses that go through all of the Network+ and Security+ materials, you would be in a far better place to start hacking. I consistently have been asked by beginners for hacking resources or mentoring. I began to notice a reoccurring theme when lecturing others: I would presume

that people who are interested in hacking have this essential skill set. Still, I've found that my presumptions were usually wrong.

Money seems to be a common issue. That's fine, there are workarounds. For example, here are free YouTube playlists offered by Professor Messer:

Free Network+ Video Series

<https://www.youtube.com/playlist?list=PLG49S3nxzAnmpdmX7RoTOyuNJQAb-r-gd>

Free Security+ Video Series

https://www.youtube.com/playlist?list=PLG49S3nxzAnnVhoAaL4B6aMFDQ8_gdxAy

Free != bad

I've personally watched both the Net+ and Sec+ playlists when I originally prepared for the examinations and I promise you, I learned a lot. I highly recommend watching these.

Review the following example:

I spent time mentoring someone who wanted to learn how to hack. I showed them how to set up Metasploitable, and we ran through some basic NMAP commands. They seemed to have the active scanning phase down. We were off to a great start, and I had projected that we were going to get through a lot of material quickly.

I asked my mentee to review the ports and services in front of them. They were stuck; I asked them what service was running on the FTP port. It was clear that they were unsure of what I meant by a "service".

Then I asked them what FTP did. Once again, they did not know. I repeated the same line of questioning with SSH, Telnet, IMAP, etc. The only port that they correctly identified was 80 and 443, and still, they did not see the difference between HTTP and HTTPS.

The point of this story isn't to rip on them [I spent time going back to the basics and teaching that instead] it's to let you know this: if these concepts seem foreign, accept it and start with the basics. Learning hacking commands and tooling will be pointless if a baseline knowledge level of Windows, Linux, Unix, Networking, Security, etc is not established.

I can't stress this enough: **Do not** start hacking until you understand the basic principles of Security and Networking. If this seems stupid to you, and you want to throw commands at a system until something works, by all means - be my guest. However, it will likely take you 3 to 4 times longer to get where you could have been if you did the legwork of learning the basics first. Trust me, save your time. It's valuable.

What to do after Security+ and Network+

Great! So you've taken my advice and, at a minimum, learned structured Security and Networking principles. Now you're ready to learn to hack, let's begin:

1. Watch Hackersploit's Ethical Hacking Playlist:

<https://www.youtube.com/playlist?list=PLBf0hzazHTGOEuhPQSnq-Ej8jRyXxfYvI>

Watch it start to finish. A few of the videos on the playlist aren't directly related to exploitation, and some of the skills are unnecessary for OSCP preparation. However, understanding a lot of the technical knowledge that goes behind hacking [even the anonymity portions of the playlist] will be essential, especially if you eventually move into the live-target phase of hacking and away from certification preparation.

2. Create a TryHackMe account and do, everything:

<https://tryhackme.com/>

Aspire to do the various courses such as Linux Fundamentals, Web Hacking Fundamentals, etc. In addition, there are learning paths. For a beginner, I would recommend doing the Complete Beginner and Web Fundamentals paths. Save the Offensive Pentesting path for pre-exam preparation. However - I will note, some of the content does cost money so work around it if you can't afford to pay for a subscription.

3. Read Hacking Books [Optional but highly recommended]. Previously I had recommended Penetration Testing: A Hands-On Introduction to Hacking & The Hacker Playbook. However, I've received quite a bit of negative feedback from my 2020 version of this guide. The complaints I received varied, but typically were related to the material being dated. **If you stumble upon dated material in a book that you are reading**, aspire to understand Linux well enough to adapt the recommended Penetration Testing tools to current-day Linux distributions. If you cannot adjust out-of-date tooling to a more current environment, I highly recommend learning how to do so. An efficient hacker maintains the ability to adjust. If you are unwilling to learn how to adapt, you will struggle to be an efficient hacker.

4. Join a hacking group. Google is a hell of a tool. Start looking for hacking discord groups, slack channels, etc. When I started, I found these groups within minutes. If you seriously can't find any (which would be concerning at this point), message some hackers and get the lowdown. I don't know a lot of lone-wolf hackers. You will miss out on a lot of resources if you attempt to fly solo.

5. Vulnhub is going to be your bread and butter. By this point, you've likely read and watched a lot of material on hacking. Start downloading beginner boxes and practicing. **If you get stuck, read some writeups** until you can progress. Rinse and repeat. Keep doing this until you get a robust methodology. Watch more hacking videos if you feel like your methods aren't quite there.

6. Once you've cracked open a bunch of Vulnhub boxes, pursue the creation of a HackTheBox account, start reaching out to people in the hacking group you joined in step (4), and look for collaboration on active boxes, proceed to the "**Intermediate Hacker**" section. Be sure to check out the "**Beginner Tips**" section first! Don't cheat yourself on the HackTheBox account creation. Hack your invite. You don't need help.

Beginner Tips

The following are tips that I think are valuable to a beginner, crafted for the convenience of not having to spend months struggling:

1. Download Joplin, or utilize Cherrytree to take notes.
2. Segment your notes. For instance, if you're attacking a single-target, create sub-notes for Enumeration, Interesting finds, Exploitation, Privilege Escalation, etc.
3. Read everything. Read writeups, read books, read resources about infrastructure, and new hacking methodology.
4. Don't listen to Gatekeepers. If you want to be a Penetration Tester, do it. Be realistic though, maintain a low-profile - not every person that you will meet is a Gatekeeper. Sometimes, the more seasoned Penetration Testers are busy with their own projects and do not have the time nor the willingness to answer hundreds of questions about hacking. Please realize that this is OK. If someone doesn't want to help you, there are plenty of other people in the world and thousands of free resources.
5. Do what you believe is correct, however, don't be stubborn. I cannot express how many times I've educated beginners and watched them ignore everything I was saying to search for an easier way and then realize my advice was the easiest all along. Be skeptical of ALL advice given. You do not need to spend hundreds of dollars on custom infrastructure and tooling to setup a hacking lab. VMware or Virtualbox with ISOs are a great way to setup a lab.
6. Time is valuable, don't attack a machine repeatedly using the same failed techniques. If you are certain it should be working, consult with someone, or troubleshoot.
7. Spend as much time building your network as you do hacking. The more hackers you meet, the more techniques and unique styles you'll observe. This will allow you to develop your own style. Also, don't worry about identifying a style - just hack. It will take some time, but you'll start to understand your strengths and weaknesses.

8. Save all of the cheatsheets you stumble across: Reverse shell cheatsheets, privilege escalation cheatsheets, payloads, everything! I consistently refer back to the cheatsheets I have saved.

9. Do **NOT** quit. I promise you, it gets easier. It does! Learning is difficult, and growth as a hacker will take time. Growth will result in growing pains. You may feel like a bad hacker that doesn't know anything, but I promise, it's not the case. The best thing you can do for yourself is to keep pushing and to hang in there, even during the low points.

For Intermediate Hackers

If you're reading this section, it means you've met the following pre-requisites:

1. Basic understanding of Networking and Security
2. Have actively participated and hacked several purposefully vulnerable systems
3. Are actively preparing to start the PWK course

Six months after starting the PWK I passed the OSCP, and you can too! [My total journey was closer to three years because of breaks that I had taken]

Methodology to prepare for the PWK

1. Spend two to three months working together with one or two people to root Active Boxes on HackTheBox. You can find people that are willing to work on boxes all over the place, including LinkedIn, Twitter, and the official HackTheBox discord channel: (<https://discord.com/invite/hRXnCFA>) again, have respect for other hackers. No one owes you their time, so please exercise a little kindness.

If you find that you're having difficulty locating people to work with, that's OK. I spent many hours within those HackTheBox practice months flying solo. When I would get stuck, I would look at the HackTheBox forums or hop on the discord. There's nothing wrong with getting a nudge, especially at this stage.

You should aim to completely root between 5 to 10 boxes in the two to three month defined period. If you can't completely hit it, that's okay, but if you do not at least root 3 boxes, I wouldn't recommend starting the PWK. The material is geared towards teaching someone new to Penetration Testing. Do not want to burn your lab time learning methodology you should have already known - you will mentally beat yourself up, especially if you're spending far too much time trying to understand basic concepts.

During the PWK

1. Before approaching the labs, I consumed the provided PWK PDF workbook. There are videos you can utilize, but I didn't watch any of them. Utilize the methodology that you're most comfortable with. Don't skip the videos because I did if the videos will be helpful.

2. Plan to read 'X' amount of pages in the PDF file every single day. The worst thing you can do to yourself is procrastinate, you're literally burning your own money. Even avid readers may linger and attempt to avoid crushing the PDF workbook. Adjust the pages read daily by scaling with your off days. For example, if you plan to read 40 pages on Thursday, aspire to read 80 or 120 on Saturday. If you have the ability to ingest information well this can be a useful time-saving technique. The important part is to ensure that you understand the content. Reading pages within itself is not useful if you can't work through the material and there's no shame in going back to re-read the more difficult concepts.

3. It depends on who you are, but I found the Buffer Overflow material in the PWK to be confusing. That was undoubtedly a technique I needed a better approach to learn, therefore I skipped it and saved it until the end of my lab time. Saving the overflow material until the end saved a lot of hardship. TCM's Buffer Overflow material is amazing, as we will discuss in a bit.

4. I didn't do the lab exercises. Personally, I felt like at least half of the exercises were geared towards a complete beginner. I had started the exercises and a quarter of the way through, I did a time analysis of lost time spent documenting and writing and decided to skip them. In a sense, I was overprepared and the PWK PDF material hardly taught me any new concepts. If this doesn't sound like you, I would recommend that you do the exercises. In fact, if I had done the exercises, I would have passed the exam the first time instead of the second. Nonetheless, if I could go back in time and do the exercises to lock-in in a pass, I wouldn't. The exercises were not my cup of tea, but they may teach you a lot.

5. If you choose to do the exercises have a plan. Commit to working through the material fast, and efficiently. Again, procrastination will destroy your ability to maximize time spent attacking systems.

6. When I started the labs, my approach was doing a full subnet scan, with a basic Nmap switch of -sS. This will help you quickly identify interesting services on the lab machines, and then you can go deeper into your scanning methodology, such as utilizing service scans -sV and testing nmap scripts against some of the services -sC. I recommend immediately utilizing nmapAutomator or Autorecon to get in the habit of scanning systems quickly, and avoiding the possibility of overlooking enumeration that you should be doing. Additionally, there's nothing better than having neat folders of the hosts to go back to. **Do not** utilize automation until you are confident that you know how to operate and understand all of the commands that the scripts execute. nmapAutomator provides a ridiculous amount of tool integration and scanning functionality, therefore let this be my warning not become too reliant on it.

7. Feel free to attack boxes for a few hours at a time, but don't spend too much time in a rabbit hole. If you've been on a box for more than two hours, and you have gotten nowhere, move on. There are plenty of machines to compromise, and you'll likely have new ideas when you return to the boxes you were stuck on

later. If you don't have new ideas, review some of the tooling taught in the PWK material. You may be overlooking something far more simple. Take everything **one port and service** at a time.

8. Do not get caught up with "The Big Four" or "Amount of systems compromised". You'll learn quickly that it's nothing more than bragging rights - and quick frankly, ridiculous to brag about. The number of systems you compromise or the machine difficulty is not indicative of your preparedness for the examination, in fact, it's not even a good indicator for the real world. A lot of the people that compromise all of the systems in the labs live on the forums, and solicit tips from others - don't be this person. I highly recommend using your lab time to organically compromise host machines. Exploiting one machine without any tips means far more than ten machines compromised because you were bumped in the right direction. Who's going to pull you out of Rabbit Holes on the exam?

9. When you're nearing the end of your lab time [the last week or so] consume as many tips as you can. Go back and try to get unstuck and exploit all of your remaining machines.

...You said no tips.

Yes, don't utilize tips until the end of your lab time. Since you gave up your hard-earned money for this lab time, you'll want to try and get as much done by any means necessary during that last week of your lab time. Doing so will help you potentially learn more exploitation and privilege escalation techniques.

10. Once you wrap up your labs, go back through the **notes you should have taken**, and compile some cheatsheets of techniques, things that worked, etc. Having a good runbook will help you on the exam and in your future endeavors. In the Information Security field, this is known as your, "Lessons Learned" writeup. You must be truthful while assessing your own skills and progression to get the most out of your study sessions.

Post-PWK

If you followed my advice word for word, you're in a fairly good position. Maybe you managed to compromise 25+ hosts, maybe you did not. Nonetheless it hardly matters and there isn't really a "standard". Don't focus on what you compromised unless you spent weeks in the lab and accomplished nothing. If you don't feel comfortable, study more and then extend your lab time. NOTE: You will never TRULY feel good about your skill set, try not to get inside of your own head.

Food for thought: Imagine being hired to do a Penetration Test for a client. Are you going to visit the [Insert client's company] Penetration Testing forums? No. That doesn't exist. You're going to have to utilize the methodology you built, there will be no tips given to you [unless they are coming from the client]. Trust me, it's stressful to root fewer boxes than others, but walkthrough methodology

only goes so far. That's why Offensive Security consistently tells you to Try Harder. You **need to try harder**.

Now that you've completed the labs, you're going to want more practice. If you only use the PWK Material + Labs and take the exam, you'll likely fail. Okay, Okay - you might pass, but I highly recommend following these steps to fill all of the gaps:

1. Purchase and Complete the Linux and Windows Privilege Escalation courses offered by TheCyberMentor. In my opinion, it's not optional. Take notes, and utilize them (because you will).

Windows Privilege Escalation

<https://www.udemy.com/course/windows-privilege-escalation-for-beginners/>

Linux Privilege Escalation

<https://www.udemy.com/course/linux-privilege-escalation-for-beginners/>

2. Next, get ready to learn Buffer Overflow, the RIGHT way. Go watch TCM's Buffer Overflow Series, use my Github reference guide for an easy recap of TCM's playlist and to clone the scripts that you'll need prior to the start:

TCM's Buffer Overflow Series

https://www.youtube.com/playlist?list=PLLKT_MCUeix3O0DPbmuaRuR_4Hxo4m3G

Buffer Overflow Guide

<https://github.com/johnjhacking/Buffer-Overflow-Guide>

3. By the time you complete the video series, you should have a good idea of Buffer Overflow attacks. You should now move onto TryHackMe. Pay for a one-month subscription and complete the Offensive Pentesting path:

<https://tryhackme.com/path/outline/pentesting>

The Offensive Pentesting path has practice lined up for Buffer Overflow attacks, which will be helpful.

4. After completing the Offensive Pentesting Path on THM, you're going to want to move onto TJ Null's Retired Box List on HackTheBox. Purchase a VIP HackTheBox subscription, and start working through these.

Hack The Box OSCP-like VMs

Linux Boxes:	Windows Boxes:	More challenging than OSCP, but good practice:
Lame	legacy	Jeeves [Windows]
brainfuck	Blue	Bart [Windows]
shocker	Devel	Tally [Windows]
bashed	Optimum	Active [Windows]
nibbles	Bastard	Jail [Linux]
beep	granny	falafel [Linux]
cronos	Arctic	Devops [Linux]
nineveh	grandpa	Hawk [Linux]
sense	silo	
solidstate	bounty	
kotarak	jerry	
node		
valentine		
poison		
sunday		
tartarsauce		

My methodology recommendation is simple; rotate between Linux and Windows boxes, you do not need to focus on any of the boxes in the red section, but doing so will not hurt. In fact, I would encourage the completion of these as well [**with specific exceptions: see below**] If you get stuck, read a writeup only to the point of being able to get unstuck, and keep pushing. Seriously, I mean it. Don't just read all of the walkthroughs and expect to pass the exam.

Do **NOT** complete these boxes, save them for the dry run!

Sense, Cronos, Chatterbox, Jeeves

Also I'm not exactly sure why I've gotten many questions pertaining to the dry run, it's simple: Don't complete Sense, Cronos, Chatterbox, Jeeves – instead, exploit them via the dry run instructions below...

5. The Dry Run is a step to test your mettle and preparedness for the exam (Thank you Rana for the suggestion). I highly recommend practicing a full exam. Schedule 24 hours where you can hack as if you were taking the OSCP. The night before your practice exam, do the following:

- Setup any Vulnhub buffer overflow machine, preferably something like Brainpan. Don't set up something overcomplicated, just a simple Stack Based Buffer Overflow Box.
- Use nmapAutomator or Autorecon to scan all of the non-bufferflow machines (4 HTB Retired Boxes total) the reason I'm telling you to do it prior and save the data is because you cannot have everything active at once. [HTB Limitations] I recommend against looking at any of the data prior, resist the temptation - you'll want it to as if you're seeing it for the first time.

Your Practice Environment:

Buffer Overflow Machine (25 Points)
 Jeeves (25 Points)
 Chatterbox (20 Points)

Cronos (20 Points)

Sense (10 Points)

Practice like you play. Take notes and screenshots, do not use writeups, make sure you take breaks, and act as if it was the real exam. If you can acquire 70 points, you're in a good place. If you don't hit 70 points it's okay. You can't possibly know everything, and the purpose of practicing is to get used to the real exam. Seriously though, please do not beat yourself up if the simulated "70 points" is missed. However, if you find that you cannot exploit any of these systems, it's indicative of a serious issue and I do not recommend moving forward with the exam. If you obtain the simulated 70 points, practice report writing with the OSCP report template if you can muster the willingness and courage to do so. A practice report will help you learn what aspects of note taking that you may need to improve. In addition, having a practice report template established will make the note integration quicker on the real examination. If you opt to take the practice report route, go as far as you can per Offensive Security's standards. Personally, when I was done with my report, I used 7zip with my OS-ID number a million times and practiced unzipping it because I was paranoid that I would furnish incorrect information. Follow their guidelines and be proficient as it will contribute towards saving valuable time.

You'll want to know that you can get that buffer overflow done in two hours or less.

6. The Dry Run should help identify if any gaps in your methodology exist, but you may be someone who finds comfort in practicing more.

More Practice:

One of the most difficult aspects of the exam is beating the pre-exam jitters. Don't worry about it. If you fail, it's not a loss - reschedule your exam and try again. Nevertheless, TryHackMe has a "King of The Hill" mode which allows you to compete against multiple players to attempt to exploit a system. The ultimate objective is to hack into the system, and prevent others from hacking it. Obviously that works against what you're trying to accomplish, therefore, make a private game and compete against the box yourself instead [that way no one can harden it]. Your objective will be to hack all of the systems in as many ways as you possibly can. Most of the systems have multiple vulnerabilities, here's a rough outline of the approach:

- Attempt to exploit the box in as many ways as you possibly can in the time limit.
- If the vulnerability allows you to obtain full privileges, take notes on your method of exploitation, and then drop the shell/log-out of the service.
- Rinse and repeat exploitation on any vector that you can until you obtain a shell or login-credentials for a user/service with no or low privileges.
- Attempt to escalate your privileges as that user or service, do not attempt other vectors of attack until you successfully pull off privilege escalation.
- Strive to: Exploit the box by abusing **two different** vectors of attack. Do not

stop until you've practiced privilege escalation with a low-level account. Since there are multiple avenues of exploitation, it shouldn't be difficult to obtain a user account.

-If you can, attempt to do this on every TryHackMe King of the Hill system. I realize this either may not be possible for some, either physically or financially. Try your best.

-Bonus Points: Do some public games and search for flags/harden the systems ;)

If you approach the King of the Hill Game with a "learning" mentality, you'll benefit greatly. Once again, document your exploits. Practice these boxes like you play. Don't use Metasploit or Automated Exploitation Tools like SQLmap. In addition, avoid bruteforcing. I promise you, each of these boxes can be exploited without bruteforce.

Note: If you are not a premium TryHackMe member you'll only have the option to start the game, but you will not be able to pick which box to practice on. If you don't have the means to purchase premium membership, consider documenting all of the ports and services to pickup where you left off if you get the same system. Don't use writeups to get unstuck. Treat this as the OSCP exam with a time crunch.

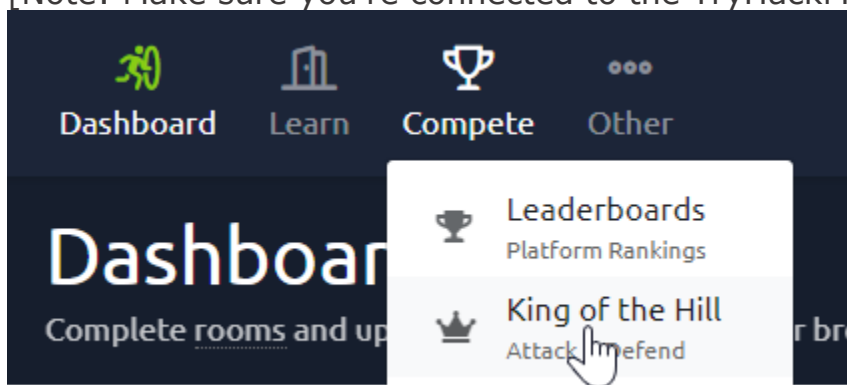
There are a decent rotation of boxes available, introducing plenty of practice opportunities pre-exam. Also, something about having a timer escalates the pressure of exploitation - which is fairly useful in preparation for the OSCP examination.

Systems:

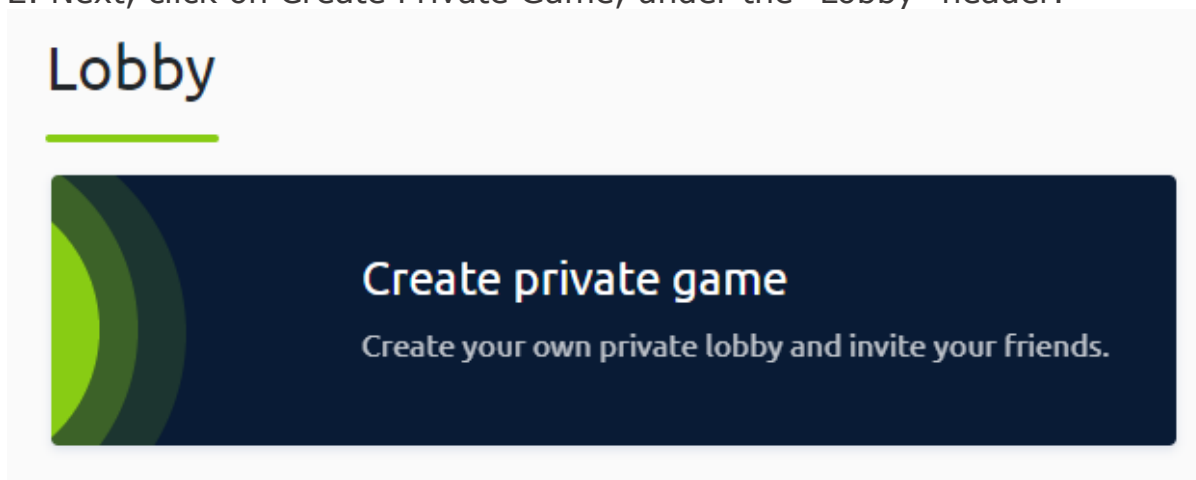
Machine Pool	
Name	OS
Hogwarts	 Linux
Carnage	 Linux
Lion	 Linux
Hackers	 Linux
Fortune	 Linux
Offline	 Windows
Panda	 Linux
Space Jam	 Linux
Food	 Linux
Production	 Linux

Getting started:

1. Go to TryHackMe and login, then click on Compete -> King of the hill
[Note: Make sure you're connected to the TryHackMe VPN]



2. Next, click on Create Private Game, under the "Lobby" header.



3. You'll see an interface that pops up. Normally, this interface is what you would use to select the box you want to attempt [if you have a premium THM account]. Set the time to start to 5 minutes, which is the lowest. Get all of your tooling ready.

Private games are invite-only. If you want to play with random users, close this modal and join a public game.

Start In

In 5 minutes

When do you want to start?

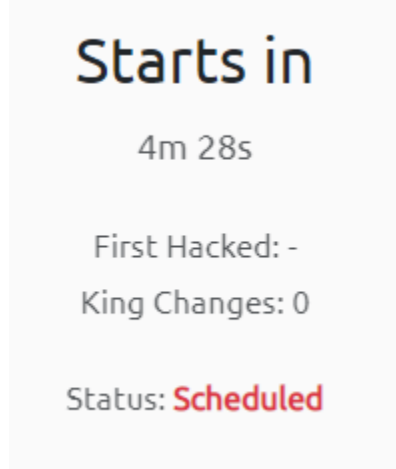
Machine to play (Subscriber-Only)

Random

What KoTH machine do you want to play?

Create

4. The countdown will begin. Once the game is close to starting, you will see an IP address populate. This will be the system that you are attempting to exploit. Don't worry about submitting flags, it's unnecessary for the exercise.



Once more, TAKE NOTES. There's no point in practicing these systems if you're not applying the methodology that you will use on the exam.

Tips for Intermediate Hackers

1. Take extensive notes on everything. That means everything: important parts of the PWK, the lab, the dry run, TryHackMe king of the hill [if you choose to do it] and your overall journey. You will not remember everything learned, especially without notes.
2. You'll start to identify what you struggle with throughout your journey. Document this, and be sure to read guides, watch videos, and read writeups pertaining to the methodology that you may be weak in.
3. Don't worry about learning the Buffer Overflow in the PWK material. Seriously, I cannot recommend TCM's YouTube video series enough.
4. Once you complete all of the above steps, don't be afraid to schedule your exam. It's just an exam, just take it. If you fail, you fail, it hardly matters. The OSCP Certification looks the same to everyone, even if it took five times to achieve vs. someone else who obtained it on the first try.
5. Practice on everything. There's no such thing as categories of hacking that are "off-limits" – Reverse Engineering, Web Application Hacking, Network Hacking, IoT Hacking, etc, all have unique skills that can assist in honing your preparedness for the examination. For example, Local File Inclusion is considered a Web Application Attack, yet can potentially lead to Server Exploitation and access to the Network. Don't worry about how you hack, just hack.

The OSCP Exam

It's time. All of your preparation will have paid off at this point, whether you pass or fail. If you've made it to the point of feeling confident enough to take the exam, I'm proud of you. It's a difficult journey attempting to obtain the OSCP, it hurts, but this is what you prepared for. When you progress beyond the OSCP, you'll learn that there's much more to hacking than a certification. Hacking is about the curiosity and willingness to learn. It's a journey that extends far beyond a certification. Enjoy every step that you walk along your path.

What to do/Expect:

1. Make sure you get a good night of rest before the exam. You're going to need it. If you have trouble sleeping, don't fret. You'll be fine.

2. The night before the exam, make sure you review the exam guide and all of the provided report submission guidelines and requirements. In addition to that, set up your note-taking space. Personally, I created notebooks with sub-sections in my Joplin note-taking software for enumeration, exploitation, etc. In addition, every time I found or did something interesting, I would make a sub-note underneath that specific section for tool results, credentials, exploitation methodology – you get the point:

Target 1 - X.X.X.X (25 Points)

Enumeration

- nmapAutomator results basic
- nmapAutomator results full
- Possible LFI parameter
- Successful LFI payloads
- Interesting Files found, Port 80
- example.txt
- example2.txt

Exploitation

- LFI to RCE steps/proof
- Fixing TTY on Shell

Privilege Escalation

- linpeas.sh results
- SUIDs on 'x' commands
- Strange non-default scripts
- Random credentials for 'x' service
- Escalation
- Abusing 'x' SUID steps/proof

Local

- Steps to get there
- Screenshot

Proof

- Steps to get there
- Screenshot

Target 2 - X.X.X.X (25 Points)

Enumeration

Exploitation

Privilege Escalation

Local

Proof

Creating target placeholders for notes in Joplin will help you quickly dump screenshots or relevant material directly into the correct sections. This will prevent you from stressing out. Go into the exam prepared. Remember that the guidelines presented on your examination will indicate which boxes have local.txt files, or both a local and a proof. **Do not forget** to submit these in the control panel and take screenshots for your report.

3. I cannot stress this point enough: turn off your firewall if you're on Windows! I spent two hours troubleshooting on my first OSCP attempt because I had no idea that Windows was dropping my traffic to the proctor. Save yourself the trouble and disable your pesky firewall.

4. You'll start the exam. Here's what I recommend:

- Read everything carefully.

- Immediately use nmapAutomator or Autorecon to start scanning the 4 targets you will not be attacking [non-buffer overflow machines]

- Start the buffer overflow machine, by the time you're finished, all of your scans will be done [unless you're a mad-person and finish Buff in less than 30 minutes]

- Attack the hosts in descending order, 25 points to 20 points to 20 points to 10 points.

- Profit, you're going to get the 70 points. Do not stress.

OSCP Exam Tips

1. Forced Time Management. Spend two hours on any given box, use a timer to keep yourself honest. If you manage to get a shell on a box in the two hour period, reset the timer and give yourself another two hours for privilege escalation. If you can't shell or perform Privilege Escalation in that two hour period, move on. No seriously. Move on. If you feel like you almost have a shell, or that you will have the box rooted close to the two hour period, try whatever you're going to try and then immediately move on if it doesn't work. "Try whatever you're going to try" **does not mean** to spend another two hours on it. Run through your exploit attempt and then stop if it doesn't work.

But...but..



No, don't lie to yourself. The most common pitfall I hear from people who fail is: "I spent way too much time trying xyz when I realized I could do xyz on another box". I'm nowhere near perfect, I did the exact same thing. You have to catch yourself abusing your timer. Move on, you'll thank me later. Hackers that fail will tell you that their biggest regret is not moving on.

2. No box bouncing. A lot of people will see a port or service on one box, try a bunch of enumeration or exploitation methodology and see another service on another box and keep hammering away from box-to-box until they've stressed themselves out and ended up with limited points. Stay methodical, you know how to perform Penetration Tests, stick to the timer, stick to the Penetration Testing framework:

Enumerate, Enumerate some more -> Exploit -> Perform Privilege Escalation

Consider the following example:

- You find credentials for a service, log in, but are stuck
- You quickly decide to instead attempt to exploit 'X' on another box, which doesn't work so you:
- Perform in-depth enumeration on another box and find nothing so you return to the first box you started with
- That's stressful and non-methodical. Don't do it. Use your time to thoroughly enumerate a system, look for an exploit, and abuse the system. If you can't do it in that two hour period, suck it up, perform the same in-depth enumeration on the next system. If you stick to this method, you will exploit the systems. You'll have to be dead-lucky to gather enough points by box-bouncing unless you're just that good [you're not, don't do it]

3. Forget about tracking your time spent on the exam, outside of the scope of the Time Management system you set for yourself. I love what [Rana Khalil](#) said on Twitter when she gave OSCP tips.

"You'll run out of ideas before you run out of time."

This is legitimately the most factual statement that was ever presented. I was nowhere NEAR close to running out of time before I started running out of ideas to exploit the last system I was working on. You can only know what you know.

After I published the first version of this guide, I was asked for clarification on this section. I don't know how I can clarify further: **24 hours is enough time to exploit the systems**

4. If there's a Metasploit module for it, a manual exploit exists. Instead of searching an exploit for MySQL version 5.x.x try typing in "github mysql version 5.x.x exploit" you'll be absolutely shook after you see the POCs and scripts that manifest in front of you. If you're worried about the third-party exploit permissions on the exam, a good rule of thumb is that the exploit shouldn't be too automated. For example, if you identify an exploit that will overwrite the password of a specific service, and then give you a shell, you're probably fine. What Offensive Security doesn't like are typically tools that will fuzz for vulnerabilities and automate the exploitation process. If there's manual work involved with the exploitation process, you should be good. However, ensure that you're following Offensive Security's guidelines – I am not responsible for any exploits that you may use towards compromising systems, follow the Offensive Security guidelines.

5. Brute Force? Yeah, no. Save that for a hail-mary last ditch attempt to exploit a system. I don't know what all of the OSCP machines look like, but I'm fairly positive that Brute Forcing is the loudest and most disruptive exploitation methodology and probably not [I say probably not because I don't know all of their systems] the route of exploitation that you'll want to use.

6. Take notes and screenshots as you go along, I used Greenshot to offload screenshots to my Windows system outside of the Virtual Machine, and to take quick enumeration screenshots to copy and paste within my Joplin notes. I think this is the most stressful part for many people, but remember, your time is not limited. 24 hours is quite a bit of time. This was my approach:

- Started a box
- Dumped suspicious or relevant services identified from scans into my Joplin notes
- Took screenshots of suspicious services and dumped it into my Joplin notes
- Attempted exploitation, and if I got it, I would replicate, screenshot, and write about it
- Rinse and repeat for the Privilege Escalation process

You may not be the best note-taker, but you should have practiced good note-taking during your dry run exam. It was an amazing feeling to get the points I needed to pass the exam, and then throw a bunch of exploits and mess around with my final box because I did not have to go back and document anything [since I already documented everything]

7. Reset boxes. You're allowed to do so for a reason. If you're exploiting the Buffer Overflow system or another system and you know if your exploit should be working, reset the box and try again. If it doesn't work, it's possible that your exploit isn't as infallible as you may have previously thought. Believe it or not, I

wasted one full-hour on my OSCP because I had a box that was unresponsive. Once I reset the box, I managed to exploit it with the same exploit that I had been attempting to use. I still passed the exam, so try not to fret about time lost.

8. Do what works for you. I've heard people say they have slept for 'x' hours or didn't sleep at all. You know your body, and you know what you can handle. If I can recommend anything, it would be at a bare minimum, taking several breaks and stepping away from your computer for some fresh air. Don't aimlessly attack systems when you're stressed out. Come back and start attacking again once you reset your approach. I would even recommend starting with a different system than what you left off with after a break for a different perspective [unless you just need a pre-privesc break or something]

9. Keep track of your points. You need to know where you're at and what it's going to take to pass, but don't stress. It doesn't matter if 12 hours in you only have 45 points. You could easily root every system in the next couple of hours.

10. Realistically, there are so many great tips. The most important one you need to know is that you could fail the exam or you could pass, but don't waste any of your time anticipating or projecting the outcome. Just hack.

11. Ending on an odd number irritates people, but I had to throw this last bit in here. Save your Metasploit usage for your last-ditch effort. You won't need to utilize it if you've thoroughly prepared, but it could be a game-changer if you're 65 points deep and looking for an easy win. Seriously, I will say it one more time: Don't even think about touching Metasploit until your last 3-6 hours of the exam.

If you fail the exam, it means nothing. There are people who have failed the exam 5+ times, there are people who have passed on their first attempt. None of that really matters. Study, work hard, and take the exam.

If you fail your first attempt, don't quit. You've toiled for this, you've paid for the course. Refocus and study, you will get it next go around if you spend the downtime before you can reschedule studying instead of sulking. You will pass, but you need to be honest with yourself and your abilities and work on weak spots. I have friends who have taken it once and then quit. Don't do this to yourself, you're better than that.

I'm hoping this guide gave you some visibility and insight. If you like it, follow me on Twitter: @johnjhacking

Thank you for reading!

Resources :

- My personal notes: <https://blog.adithyanak.com/oscp-preparation-guide/enumeration>
- TJNull's list updated list 2021 : https://docs.google.com/spreadsheets/d/1dwSMIAP_Iam0PuRBkCiDI88pU3yzrqqHkDtBngUHNcw8/edit#gid=0

OSCP Journeys and Preparation guides:

- <https://medium.com/@parthdeshani/how-to-pass-oscp-like-boss-b269f2ea99d>
- https://www.netsecfocus.com/oscp/2019/03/29/The_Journey_to_Try_Harder-TJNulls_Preparation_Guide_for_PWK_OSCP.html
- <https://medium.com/@calmhavoc/oscp-the-pain-the-pleasure-a506962baad>
- <https://github.com/burntmybagel/OSCP-Prep>
- <https://medium.com/@m4lv0id/and-i-did-oscp-589babbfea19>
- <https://gr0sabi.github.io/security/oscp-insights-best-practices-resources/#note-taking>
- https://satiex.net/2019/04/10/offensive-security-certified-professional/amp/?_twitter_impression=true

- <https://hakin9.org/try-harder-my-penetration-testing-with-kali-linux-oscp-review-and-courselab-experience-my-oscp-review-by-jason-bernier/>
- <https://theslickgeek.com/oscp/>
- <http://dann.com.br/oscp-offensive-security-certification-pwk-course-review/>
- <https://h0mbre.github.io/OSCP/#>
- <https://prasannakumar.in/infosec/my-walk-towards-cracking-oscp/>
- <https://infosecuritygeek.com/my-oscp-journey/>
- <https://acknak.fr/en/articles/oscp-tools/>
- <https://r3dg33k.com/2018-10-09-oscp-exp/>
- <https://www.jimwilbur.com/oscp-links/>
- <https://www.linkedin.com/pulse/road-oscp-oluwaseun-oyelude-oscp>
- <https://scund00r.com/all/oscp/2018/02/25/passing-oscp.html>
- <https://blog.vonhewitt.com/2018/08/oscp-exam-cram-log-aug-sept-oct-2018/>
- <https://jhalon.github.io/OSCP-Review/>
- <https://www.alienvault.com/blogs/security-essentials/how-to-prepare-to-take-the-oscp>

- <https://niiconsulting.com/checkmate/2017/06/a-detail-guide-on-oscp-preparation-from-newbie-to-oscp/>
- https://thor-sec.com/review/oscp/oscp_review/

Cheatsheets :

- <https://github.com/P3t3rp4rk3r/OSCP-cheat-sheet-1?files=1>
- <https://github.com/crsftw/oscp?files=1>
- <https://github.com/crsftw>
- <https://h4ck.co/wp-content/uploads/2018/06/cheatsheet.txt>
- <https://sushant747.gitbooks.io/total-oscp-guide/reverse-shell.html>
- <https://jok3rsecurity.com/cheat-sheet/>
- <https://github.com/UserXGnu/OSCP-cheat-sheet-1?files=1>
- <https://archive.is/IZLjv>
- <https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/>
- <http://ramunix.blogspot.com/2016/10/oscp-cheat-sheet.html?m=1>

- <http://0xc0ffee.io/blog/OSCP-Goldmine>
- <https://hausec.com/pentesting-cheatsheet/>
- <https://jordanpotti.com/oscp/>
- <https://github.com/ucki/URP-T-v.01?files=1>
- https://blog.propriacausa.de/wp-content/uploads/2016/07/oscp_notes.html
- <https://zsahi.wordpress.com/oscp-notes-collection/>
- <https://github.com/weaknetlabs/Penetration-Testing-Grimoire?files=1>
- <https://github.com/OlivierLaflamme/Cheatsheet-God?files=1>
- <https://medium.com/@cymtrick/oscp-cheat-sheet-5b8aeae085ad>

Linux Privilege Escalation :

- <https://adithyanak.gitbook.io/oscp-2020/privilege-escalation>
- https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_linux.html
- <https://github.com/Ignitetechnologies/Privilege-Escalation>
- <https://gtfobins.github.io/>

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

Linux Privesc Tools :

- Linux Exploit Suggester (<https://github.com/mzet-/linux-exploit-suggester>)
- SUIDENUM (<https://github.com/Anon-Exploiter/SUID3NUM>)
- LinEnum.sh (<https://github.com/rebootuser/LinEnum>)
- linpeas.sh (<https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS>)
- Linprivchecker
(<https://github.com/sleventyeleven/linuxprivchecker>)
- pspy (<https://github.com/DominicBreuker/pspy>)
(crontabs)

Windows Privilege Escalation :

- <https://adithyanak.gitbook.io/oscp-2020/windows-privilege-escalation>
- https://sushant747.gitbooks.io/total-oscp-guide/privilege_escalation_windows.html

- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md>
- <https://www.absolomb.com/2018-01-26-Windows-Privilege-Escalation-Guide/>
- <http://www.fuzzysecurity.com/tutorials/16.html>
- <https://book.hacktricks.xyz/windows/checklist-windows-privilege-escalation> (Win PrivEsc Checklist)
- <https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/>