Roadmap to OSCP 2023

By: Usman Shah

@viehgroup

Note: This document is not created by a professional content writer so any mistake and error is a part of great design

Disclaimer

This document is generated by VIEH Group and if there is any contribution or or credit, it's mentioned on the first page. The information provided herein is for educational purposes only and does not constitute legal or professional advice. While we have made every effort to ensure the accuracy and reliability of the information presented, VIEH Group disclaims any warranties or representations, express or implied, regarding the completeness, accuracy, or usefulness of this document. Any reliance you place on the information contained in this document is strictly at your own risk. VIEH Group shall not be liable for any damages arising from the use of or reliance on this document. also we highly appreciate the source person for this document.

Happy reading !

Content Credit: Usman Shah

@viehgroup

Introduction

Crack OSCP in 6 months, starting from scratch.

Hello again,

I have received a lot of DMs asking me about how to prepare for OSCP, what all things to learn, where to learn from etc. So, lets pave a roadmap for the guys just starting out in OSCP looking to clear it in their first try.

OSCP is indeed one of the most prestigious certification in cybersecurity — no matter what any other certification body tells you, OSCP still tops the charts.

- They have quality material and their labs are amazingly good.
- Discussion forums are well built, support is 24x7.
- Teaches you how to manage time and stress to bring out the best in you. Enforcing the 'Try Harder' Mentality.
- Its one of those exams where you wont find any leaks/dumps for — if you do find, believe me they are just fake. OSCP has different set of labs and objectives for every single examination.
- It is expensive, but it has the potential to bring back your money 10X once you qualify and then market yourself properly.

Basics:

First get your foundations clear and strong.

- Start with Networking. Topics like IP, TCP, UDP, HTTP, HTTPS, DNS, DHCP and ARP.
- One of the best books that i have come across to make my foundations solid is: TCP/IP by behrouz A.Forouzan, you can find the book here: https://amzn.to/3XrUKro
- Another very useful resource for learning DNS is: https://slashroot.in/how-dns-works and you can also visit my

@viehgroup

own website for a generic understanding of how DNS works https://hackershares.com/dns

- You can visit https://www.practicalnetworking.net/series/arp/address-resolution-protocol/ for understanding ARP
- Rest of the basic topics should be covered in the book that i recommended above.
- Once you have your basics cleared, move on to TryHackMe, get yourself a monthly subscription and complete the following paths: Introduction to Cybersecurity, Complete Beginner, Web Fundamentals, Pre Security and Cyber Defence.
- For Linux — the best practical resource out there is https://overthewire.org/ — Complete at least 20 levels there. For linux theory, you can take the Linux 101 course on TCM Academy https://academy.tcm-sec.com/p/linux-101 and Linux fundamentals 1, 2 and 3 from TryHackMe [https://tryhackme.com/room/linuxfundamentalspart1 , https://tryhackme.com/room/linuxfundamentalspart2 , https://tryhackme.com/room/linuxfundamentalspart3] — where you'll also learn about the bash language, which is very helpful for a pentester.

@viehgroup

- For Windows — the essentials to learn are registry hives, directory structures, difference between x32 and x64 bit systems, command prompt and powershell. Complete these rooms on TryHackMe for these https://tryhackme.com/room/windowsfundamentals1xbx , https://tryhackme.com/room/windowsfundamentals2x0x , https://tryhackme.com/room/windowsfundamentals3xzx and https://tryhackme.com/room/powershell .
- It is essential for a pentester to have some sort knowledge on reading, debugging, writing and scripting code for automating purposes. Basic languages to know are Python and Rust. The best out there is yet again from TCM Academy [i just love the quality material they have], take up the Python101 and Rust101 courses from there [I myself am currently doing Rust101].
- Once you have covered networking, the tryhackme essential paths, Operating system fundamentals and basics on languages like powershell, bash, python and rust.
- Then you'll have to also learn some basics on languages which help build a website. Since, alot of web app pentesting revolves around understanding and exploiting the website front-end or backend code to get the initial foothold, and alot of juicy

@viehgroup

information can be found from these. Languages like HTML, CSS, JS and SQL. One of the best all-in-one resources to learn these are https://www.freecodecamp.org/ and https://portswigger.net/web-security/learning-path

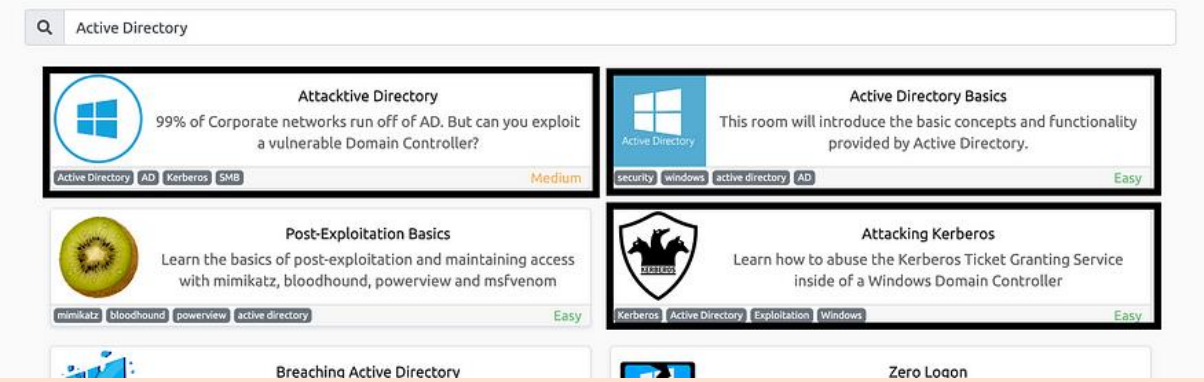
Great, now you have covered the basics on Networking, Operating Systems, Web fundamentals and essential scripting languages.

All the above mentioned basics should be covered easily in a span of one month.

Intermediate:

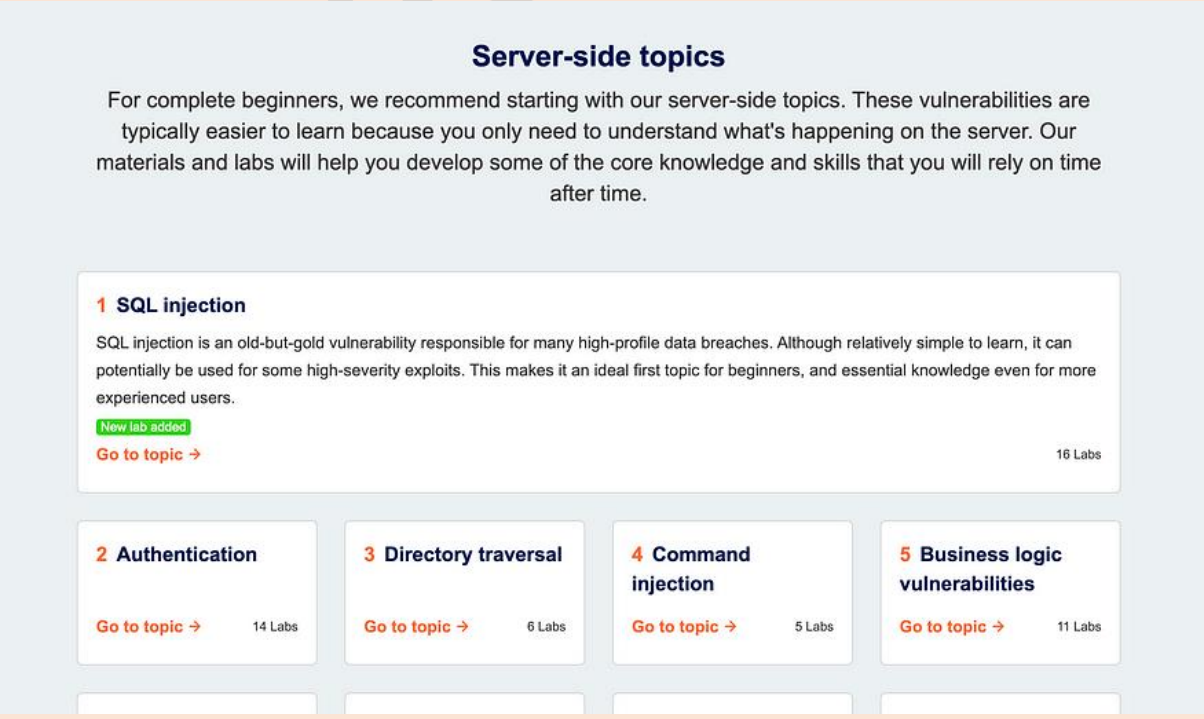
Now, lets focus on some stronger technologies and tools which will help you upskill yourself.

- **Active Directory**: Learn Active Directory [I cannot stress this enough] — not just for the exam, but AD will help you in real-life corporate jobs as well, its a great great skill to have. TryHackMe has great paths on AD https://tryhackme.com/room/winadbasics. Learn few basic AD Attacks like https://tryhackme.com/room/attackingkerberos and https://tryhackme.com/room/attacktivedirectory, https://tryhackme.com/room/windowsinternals.



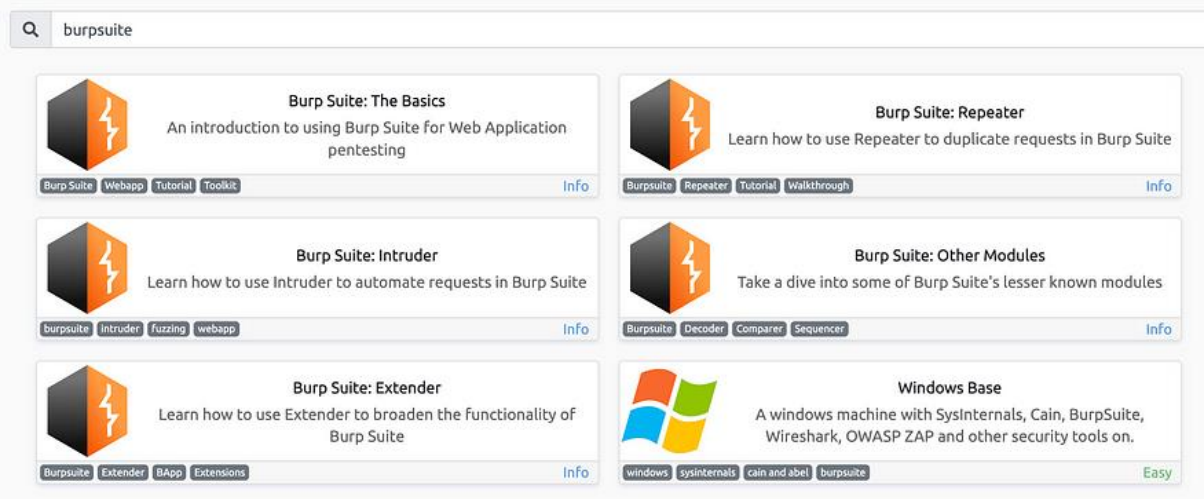
https://tryhackme.com/hacktivities?tab=search&page=1&free=all&order=most-popular&difficulty=all&type=all&searchTxt=Active+Directory

- **PortSwigger**: Hands-down the best theory and practical workplace to learn about web application penetration testing. It is free of cost. Complete all their rooms [or most of them] — you'll get a solid understanding on web application attacks, what are they and how to exploit them. They also provide free practice labs for each one of them.



https://portswigger.net/web-security/learning-path

- **BurpSuite**: An Amazing tool to intercept browser requests and play around with them. The TryHackMe burpsuite modules helps clear all the basics
- https://tryhackme.com/room/burpsuitebasics ,
- https://tryhackme.com/room/burpsuiteintruder ,
- https://tryhackme.com/room/burpsuiteextender ,
- https://tryhackme.com/room/burpsuiterepeater
- https://tryhackme.com/room/burpsuiteom

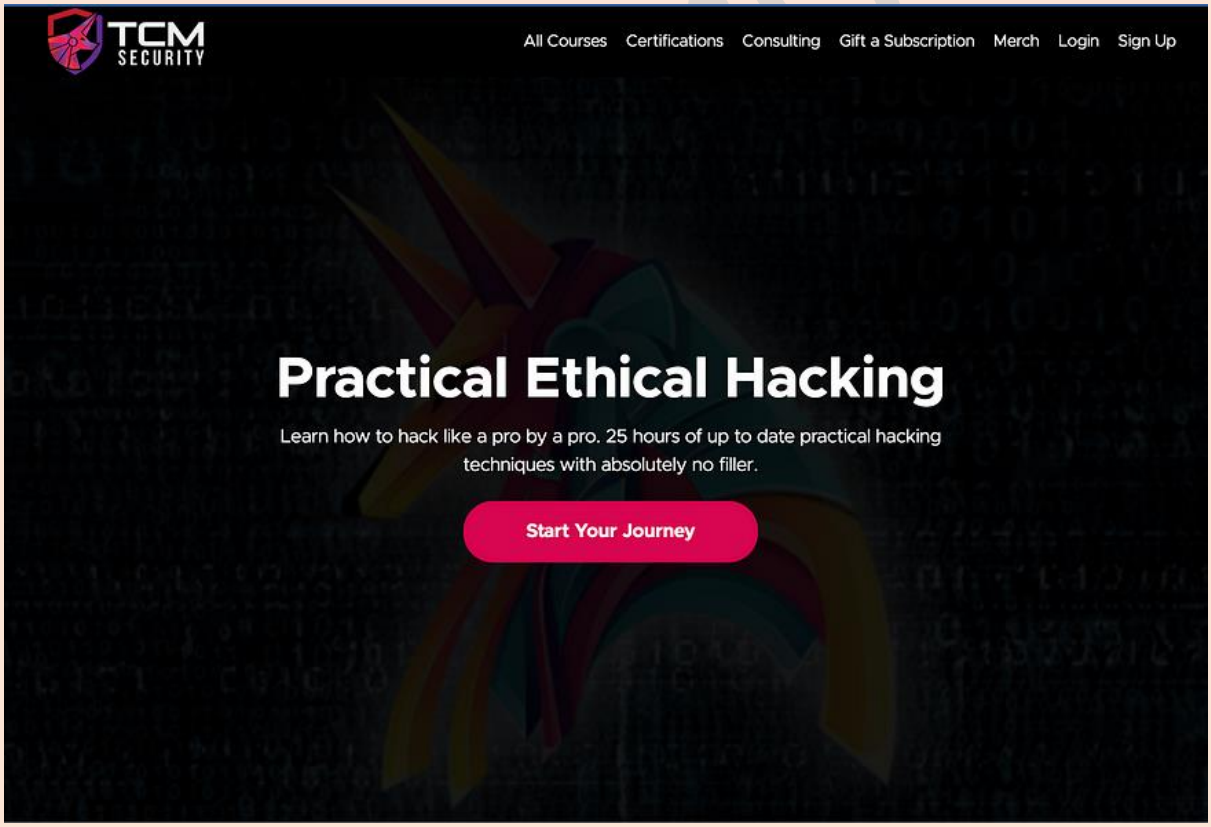


https://tryhackme.com/hacktivities?tab=search&page=1&free=all&order=most-popular&difficulty=all&type=all&searchTxt=burpsuite

- **TCM-PEH Course**: The **MUST-HAVE**.The practical ethical hacking course from TCM Academy covers everything that you'll

need to understand in penetration testing and successfully be able to showcase it too.Enroll in this course https://academy.tcm-sec.com/p/practical-ethical-hacking-the-complete-course and you will see yourself level up very fast.The course also covers creating your own vulnerable lab along with in-depth Active Directory practicals.

[**Pro-Tip:** The AD covered here is more than enough to ace the OSCP AD portion of the exam]

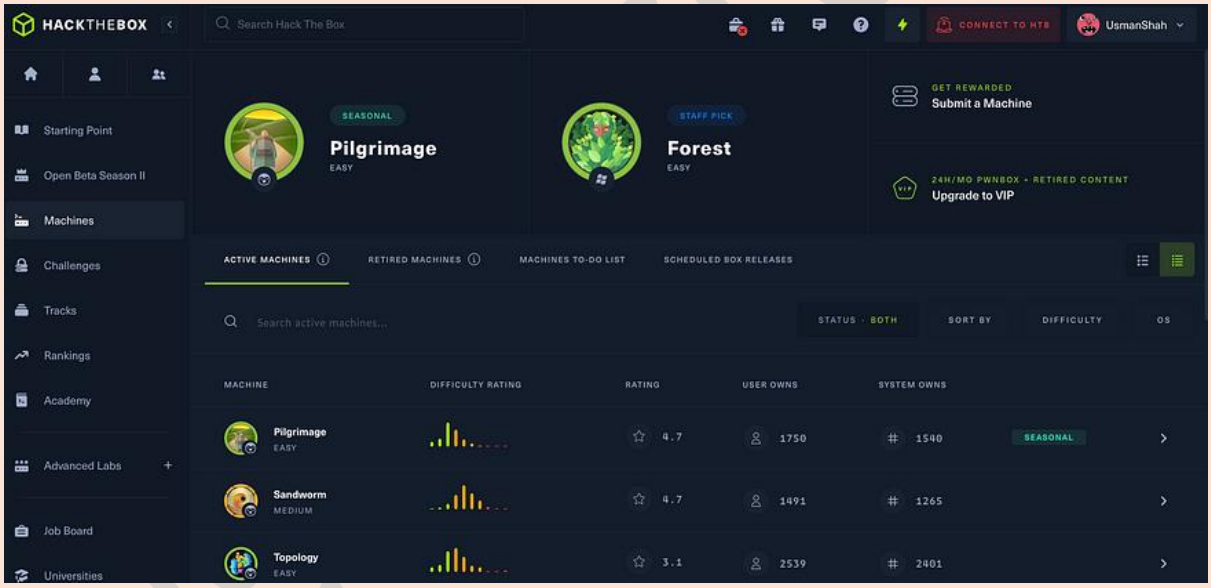


https://academy.tcm-sec.com/p/practical-ethical-hacking-the-complete-course

- **TryHackMe**: Apart from going through the learning rooms. Also involve yourself in individual boxes, where you'll be able to explore different scenarios, understand security concepts and even hack the machines. Few of the most interesting boxes are: livingofftheland [https://tryhackme.com/room/livingofftheland] , log4j [https://tryhackme.com/room/solar] , carnage [https://tryhackme.com/room/c2carnage] , JTR [https://tryhackme.com/room/johntheripper0] , DNS [https://tryhackme.com/room/dnsindetail] , Zerologon [https://tryhackme.com/room/zer0logon] , NMAP [https://tryhackme.com/room/furthernmap] , Overpass [https://tryhackme.com/room/overpass2hacked] , relevant [https://tryhackme.com/room/relevant] , kenobi [https://tryhackme.com/room/kenobi] , hackpark [https://tryhackme.com/room/hackpark] , picklerick [https://tryhackme.com/room/picklerick] etc and there are many more. You can go through them yourselves, pick any easy to medium ones and give it a try.
- **HackTheBox**: Now comes the real game, enrol yourself on HackTheBox — and start playing around with easy machines first. Don't worry, if you don't find your way in the machine or are not

@viehgroup

able to hack it fully, always look up the walkthroughs on the machines [**Pro-Tip**: Always lookup the write-ups when you have fully tried everything and exhausted your knowledge. Basically, ensure whenever you lookup the write-ups you learn something new, not something like ‘Oh shit, i knew that, i should have tried that’ , you should be like ‘Oh thats new, great to learn this new skill, lets add it up in my arsenal of skills’.- this will eventually build up your skills and you’ll learn many new ones. [Do approximately **50+** machines ony from HTB.]



https://app.hackthebox.com/machines

The intermediate level should take you almost 2 to 2.5 months to complete. Rest assured, once you do all these things — you already have completed more than 60% of OSCP.

Advanced:

- **Enrol** in for the OSCP Exam and finish all your topic exercises first — this will give you additional 10 points [which comes in very handy, if you get stuck at the 60 point mark in the exam, these 10 points will help you pass the exam]. **Pro-Tip:** Brisk through topics like AV Evasion and exploit development (90% of the time these topics are not tested in the new OSCP Pen-200 exam, these are more focused on the Pen-300 exam).
- Start doing '**Hard**' rooms in **TryHackMe**. Don't hesitate to lookup the walkthroughs, just keep in mind the pro-tip i gave on this above.
- Get the **TJ-Nulls List** [https://docs.google.com/spreadsheets/u/1/d/1dwSMIAPIam0PuRBkCiDI88pU3yzrqqHkDtBngUHNCw8/htmlview] of OSCP-Like machines, which he has collected from platforms like HTB, Vulnhub, Proving Grounds play and practice and start doing those machines.
- **Proving Grounds:** These machines are sooo similar to the machines that you see in your exam. The mentality and the approach used in the PG machines are the ones that you can

expect in your OSCP exam. Complete almost 50+ PG machines [Play+Practice].

- **Ippsec**: Watch and learn from ippsec as much as you can. He is popular for providing video walkthroughs of most of the HTB Machines — which is very helpful. Youtube: https://www.youtube.com/channel/UCa6eh7gCkpPo5XXUDfygQQA and website: https://ippsec.rocks/?# [helps in finding relevant commands for an attack type you might be looking for].
- **Practice**: Practice , Practice and Practice — thats whats going to make you perfect.

Extras:

- **Linux**: Play around with your own linux VM [that you'll be using for the exam], properly structure everything in specific folders, collect all linux tools, windows tools, public exploits, get some of the famous exploits compiled for both 64 and 32 bit windows versions (exploits like the potato ones) and structure everything for ease of access and navigation during your exam. Trust me, having a properly structured linux OS saves you a lot of time. Learn some quick linux shortcuts to get your work done in seconds to increase your efficiency and save you time. Learn

the directory structure, know what types of files are stored under which directory etc.

- **Powershell**: Strengthen your powershell skills. learn to create one-liner powershell reverse shells, enumeration commands on powershell, commands like finding hidden directories, looking up permissions, play around with attacks like DLL hijacking and unquoted service paths etc.
- **Bash**: Get expert in bash scripting. Learn to form loops and write simple scripts in bash. Learn bash one-liners for reverse shell, for loop, while loop, stabilising shells with TTY etc.
- **Enumeration and Reconnaissance:** Strengthen your recon skills. Master tools like NMAP, Dirbuster, Gobuster, Nikto, Dirb, Wpscan, Crackmapexec, Smbmap, enum4linux-ng, winpeas, linpeas, wes-ng, les, powershell nishang and empire tools, tools from impacket toolkit, learn to create virtualised environments quickly using pip and venv.
- **Know your tools**: Know your tools and their dependencies, know what type of tools require python 2.x, what type of tools require python 3.x and have a separate working environment for those type of tools. A lot of the misconfigurations in the linux OS are due to improper pip or apt installs, without knowing the

@viehgroup

dependencies and the affect it can have in your environment puts you in a lot trouble when you are stuck in a certain phase of a pentest and you just cant get the task done, because you have some improper set of dependencies or have some missing dependencies. Keeping this intact will save you alot of time.

- **Note-Making:** Note making is very essential and helps you save you a lot of time. If you need to look up on some concept or command, and you are finding it hard to recollect during your exam, instead of just randomly googling around, you can just go to your notes and take it up from there. The best tool for note making and the tool which i personally also use is **Obsidian**.

The advanced and extras portion should take you around 2–2.5 months more. Trust me, if you do all this , i can confidently say that you are very much ready for the exam.

Pro-Tips:

1. HTB machines are way harder than OSCP machines. If you find yourselves doing HTB [Medium level] machines easily without any walkthroughs — you are ready for the OSCP exam.
2. Complete the Full AD machines' path of HTB — Nothing in OSCP in the AD set will come outside of this.

@viehgroup

[https://app.hackthebox.com/tracks/Active-Directory-101]. If not the full path, at least do machines like Forest, Active, Sauna, Resolute and Cascade.

3. Don’t go for the exam before you complete the full TCM-PEH course by TCM Academy. In my experience, the things you’ll learn there will benefit you in your exam 10 folds, specially the AD Part.
4. Complete a total minimum of 100 Boxes from platforms like HTB, THM, PG-Play and PG-Practice.

Hope you had a good read.

Thank you.

@viehgroup

Thanks for reading

@viehgroup