And I did OSCP!

Praveen Nair Follow
Oct 16, 2017 · 12 min read

I have never been a blogger of such, so be cautious!
Off that said, This July I became an **Offensive Security Certified Professional, HELL YEAH!**

0x00—The Course

I don't think the infamous PWK course for OSCP needs an introduction at this point of time. But for the sake of this blog post let me drop some key points of it.

COURSE

- Only one truly practical examination for an Intermediate level InfoSec Certification.(***That I came across***)
- You will learn more than it actually teaches you .
- A must take challenge if you are in Information Security domain.
- You will get the hang of ***TRY****ing* ***HARDER!!***

CONTENTS

- Given a 300+ pages PDF content. (***Read it first***)(***Syllabus***)
- 8hrs long video content.
- Complete the hands on exercises after each section.(***Preferably must be done and documented***)

LAB

- You can choose you Lab time from 30 to 60 to 90 days(***60 days recommended***)
- 50+ machine in private environment.

- Given access to one of the subnet, PWN the rest (***or at-least as many as possible***).
- Find ***network_secret.txt*** to unlock new subnet access.
- **End Goal -** Find your way into Admin network
- PWN ’em all to Learn ’em all. (***Keep everything documented***)
- Push yourself to the limits. (***If you believe you have got to the limits, take a step more***)

EXAM

- 23hr 45min Exam (***Keep everything noted down***).
- Will be given access to exam’s private network via a VPN connection.
- Several victim machines to be hacked. (***Hack ’em all! if at all possible***)
- Own user to get ***user*** flag and Own system to get ***root*** flag.
- 24hrs more to make report.
- Read the exam ***Instructions*** **carefully.**

- ***Thinks Smarter*** rather than ***Try***ing **Harder**.

If you still need to know about it, do take a look at Offensive Security's website.

0x01 — My Start

I was a small town bug bounty participant when I first heard about Offensive Security certifications, at that very moment I knew I had to do it. Let's not kid myself, I almost finished my high school and was planing for my college and also I didn't had a job, so technically I didn't had the money in my pocket that I could afford it at that point in time. But I had it in my mind that I'll do it one day for sure. I couldn't have asked more from Offensive Security, they have high quality content with great precision on each topic.

So, Finally I completed my college and got a job as "***Mobile App Pentester*** *and* ***Jr. Malware Analyst***" soon enough. Now I had my problems been dealt with at this point and I was all ready for some fun (***Pain and Sufferance mostly***). Don't take it as a joke when I say OSCP stands to it reputation of pushing your limits, not once, not twice but every single time.

So I signed up for the course on Feb 8th, and I choose 90 days of lab and scheduled 6hrs after my work for the labs. I know, it was too much for the day and I had like 90 days lab access but I use to take some long breaks in my lab so it all fitted for me.

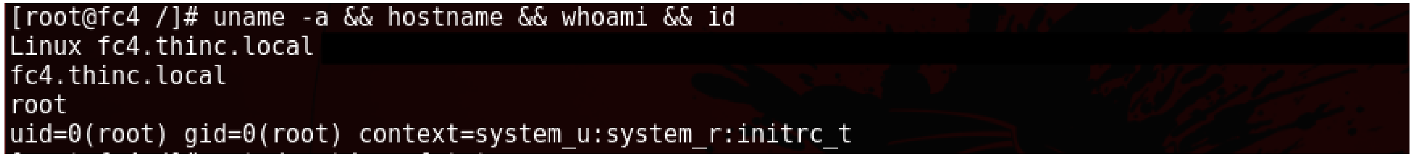
0x02—Vulnhub, Exploit-Exercises, and HTB

I did actually started doing random boxes from ***VulnHub*** way before I signed up for OSCP and I had quite some previous experience with VulnHub Boot2Root challenges so, it wasn't much of a game changer. But on my way of finding new challenges other than that on VulnHub, I ended up on ***Nebula*** at ***Exploit-Exercises*** and it's one of the best box to learn basic Linux Privilege Escalation and it is very precise ***(A highly recommended box).*** As soon as I finish nebula, I again started my search for finding relative challenges and ***OH GOOD LORD!*** I found ***Hack The Box (HTB).*** *BTW,* I found it after my labs got started and yeah! It's pretty much similar to that of OSCP lab environment but here all the boxes are standalone and you will not see pivoting concepts, There are also boxes which are off-limit's if you consider the course syllabus relatives. But I highly recommend joining the community and start pwning. These three places really really helped me a lot preparing for my exam.

0x03—The Course and LAB

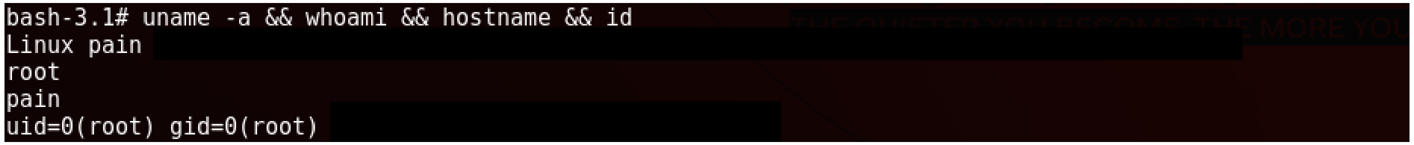
On Feb 19th I got my course bundle and my VPN connection details for the LAB as per schedule ***AND IT WAS TIME***. I started with my VPN connection test and had a look around the control panel, made a list of the machine I got from the first subnet and I was all set to start. I took first couple of weeks to complete all of my course materials (PDF + Videos + Exercises) and also by the time I did the whole network scan and made a rough outline of the boxes I should get started with. As recommended I started with the low hanging fruits and I got like 6–8 machine in 2 days and I felt it to be too easy start, but I knew that there were devils waiting for me. After a couple of weeks more I did got upto like 20–22 boxes down and my confidence just busted out. Now I had my eyes on the most notorious and infamous boxes ***“gh0st, fc4, pain, humble*** *and* ***sufferance”***. It was time to prove I was able enough. So I started with ***gh0st***, and It took like 3–4hr to totally own the box and I was happy to have owned it faster than that of I actually estimated.

I took a few days off the labs at this point of time. I came back and now off to popping "***fc4",*** this one was fairly easier than that of ***gh0st***. I found it rather quit straight forward to be frank.



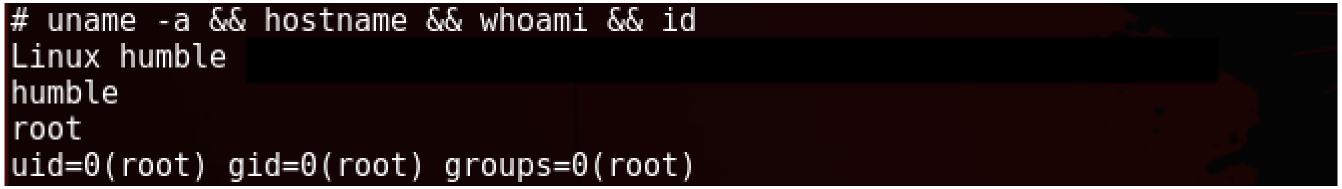
```
[root@fc4 /]# uname -a && hostname && whoami && id
Linux fc4.thinc.local [redacted]
fc4.thinc.local
root
uid=0(root) gid=0(root) context=system_u:system_r:initrc_t
```

2 down and 3 more to go. Onto "***pain"***, now this is the place where things got to heat up, This is where you realise how savage the OSCP lab creators are. I wasted 5hr of mine doing things that it pretends to be but which it is not. This is the place which made me feel stupid and made me slap my face when I finally figured it out. Darn good guys, you got me on this one and no kidding It was quite unexpected, but popped it in less that an hour after I got to know of the way.



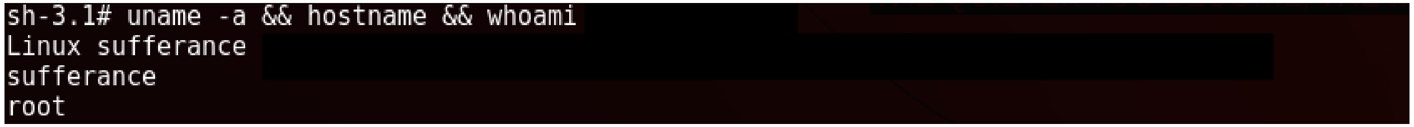
```
bash-3.1# uname -a && whoami && hostname && id
Linux pain [redacted]
root
pain
uid=0(root) gid=0(root) [redacted]
```

As I have done pain at this point, I knew what to expect and what not to and also to do the unexpected. So, I started with ***"humble"*** and ***Good Lord!*** I found the way quit easily with a bit of googling. Now the thing about humble is that you know the service well enough but you still need to work on the info you get via your ***"Google-Fu".*** It took me some time debugging and analysing as I didn't had much of the hands-on to the service prior to this. So, finally I had a shell and I left it there for few days again, as PE on this machine was not what actually I thought how it is. I popped some other box when I returned and then I started again and finally after a whole day of struggle I popped this box and I was so happy about it when I realised it actually taught me ***How to be HUMBLE!.***



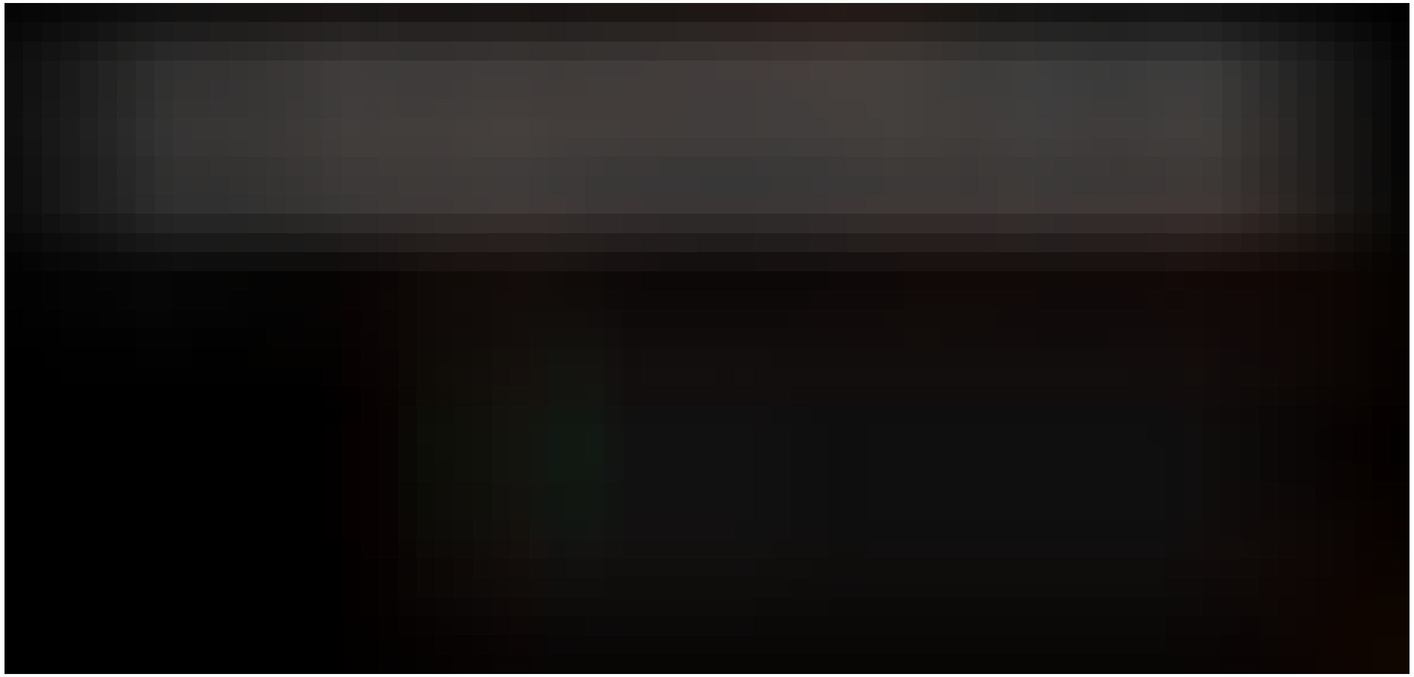
```
# uname -a && hostname && whoami && id
Linux humble [redacted]
humble
root
uid=0(root) gid=0(root) groups=0(root)
```

With this all done It was time for the ultimate ***Sufferance!!!*** This box made me feel so dumb that I actually had to left the box for good and didn't came close to it for days. But with the lesson learned from ***humble*** I started again and did a thorough recon of all the services running on the box for a whole day. This time I had something that I could actually use and I did. but It actually didn’t work. After some google I realised what was going wrong, so fixed it and I had a shell. Now the thing about sufferance is that the way is right facing you all the time and you always do miss it. I did suffer for sometime and when I realised how it is to be done my mind was blown. After days of ***sufferance*** I did popped it.



```
sh-3.1# uname -a && hostname && whoami
Linux sufferance [redacted]
sufferance
root
```

At this point I had pwned all the notorious boxes in the lab, by my 58th day in the lab I had unlocked all the Subnet and I had pwned every single box in the lab environment. I felt really confident enough to get my exam. After all this was done, I realised that there are several other underrated boxes in the OSCP lab that no one really talks about to name a few “**Sherlock, Master, Slave, Mario**”. These boxes felt to be very much competitive when trying to Pwn. I don’t know how other people think of these boxes but for me it did taught me quite a few things. The lab was just superb! and kudos to the OSCP Lab creators. They did and amazing job at making it too close to the live environment.



0x04—Sharpening my AXE

Now that I had another 30 days more in my lab so,I played it with ease on finding multiple ways on pwning the boxes and I found quite a few tricks to do so and no kidding It did help me in my exam. It was second week of MAY already and my lab time was to end in like next 5–6 days So, I scheduled my exam time to 11AM on 1st of July. Well, I was having quite some work pressure which had to be dealt with immediately at that point. So took one month(June) before my exam and started giving my spare time to

HackTheBox machines and also started writing python tools for automating my recon steps for the sake of saving time. I would test them with machines on HTB to be sure of, and this is one of the reason I always recommend HTB to anyone doing OSCP and OSCE. It just great! I have kept my notes organised with my bitbucket repo, So I can use it as reference in my exam. My scripts kept the results organised so I don’t have to bother searching for it.

0x04—The Exam

This section was edited because of critical exam information been disclosed previously

It was time, I got the email with the VPN access on sharp 11AM. I connected to the VPN tested with simple SYN scans to confirm everything was proper. I read through the instruction and the targets list. Now it was time to run through my arsenal, I had written a single script which will execute all the basic scans and invoke relative tools according to the resultant. I took my time completing the box I know what is to be done in a specific way.

- In next 3hr I was done with my first box.

I checked on my terminal for the scan result and it showed me nothing, It was running into a infinite loop of uselessness. Thats when I realised my script was broken and I have already wasted my 3hrs on it. This was not the time to fix the script as I remembered that I did try adding another functionality to the script and I didn't actually tested it properly. So I finally ending up running scans manually for all the targets, and I was so dumb that I used several terminator consoles running, that every time I would bump into the wrong one, messing up one box's resultant with another. At this point I had wasted almost 8hr+ of my time doing nothing but scanning the target. Yes, I did had a schedule for the things to be done but with my recon script failing really really bad, I didn't had a ***Plan B***. One thing that my script did that really helped was, it did saved the various nmap resultants of specific boxes in its workspace. So, I took a 5 min break, just looked at my laptop screen, took deep breathe and started doing one box at a time.
And tell you no more, it really helped adding few more points to my pocket

With ***18hrs*** past and I haven't slept yet. So, I took a 20 mins sleep and started again.

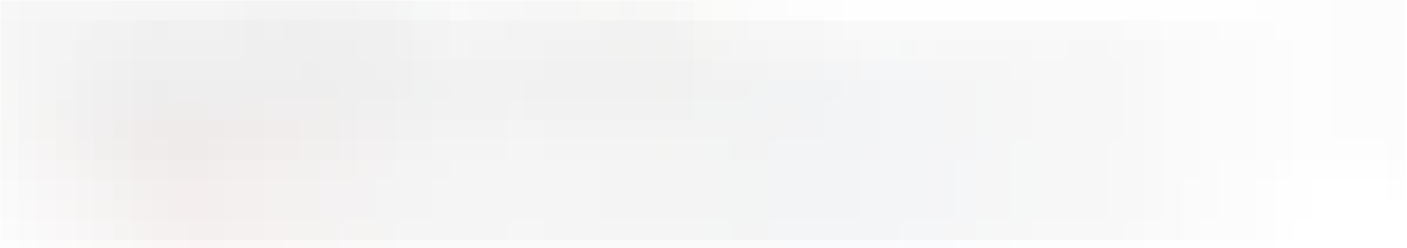
21hrs+ past I had enough points, and I knew I had enough points to pass the examination, but the last box was so competitive it kept me going further.

- Another 1hr and I had a Low Privilege shell on the last box.

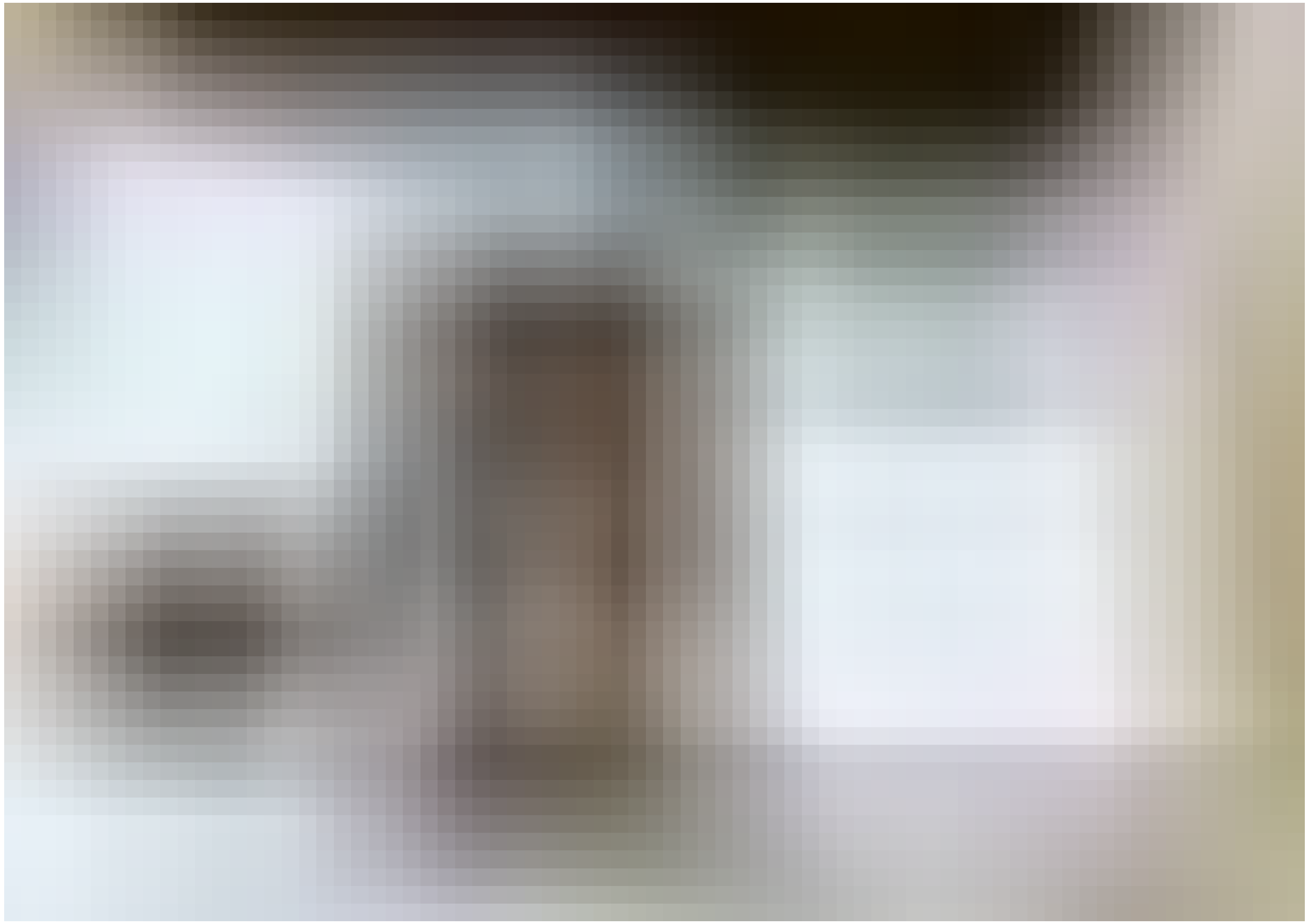
I didn’t stop there. I kept struggling till my exam VPN got disconnected. But I couldn’t escalate the last box in time. I knew I had passed, and I kept all the screenshots, scan logs and brief notes on each box.

I didn’t waste anytime of mine and started making the report. As soon as I finished it, I read it multiple times word by word, because I was already feeling really sleepy. I submitted the my report in next 13hrs and went home and just fall asleep.

Almost 36hrs later I got an email which basically said I became an OSCP and it was the happiest moment of my life till now.



And in August I got the Certificate that says ***I TRIED HARDER!***



0x05— Conclusion and Last Thoughts

I was so exited about this course, one of the reason is because its my first certification in Information Security domain and obviously OSCP is fun.(***Well mostly in pain, but like good pain)*.**

Offensive Security does a great job not only in teaching you stuff but also teaching you how to learn and grow outta you mistakes and thats the only reason for me (personally) to have opted to take their certification out running any other. They have a well maintained environment and a great support team and student admins.

There are a ton of certification in this domain but Offensive Security certifications are the ones that will really make you realise that you have actually earned it, rather than just crossed your fingers and did a MCQ exam. I'm too glad that I was able get this one done with and I'm totally looking forward to OSCE now.

If you are going to take OSCP and you reached at this point of my blog, here are few things you should keep in mind.

- Read the PDF throughly and do the exercises you will have most of the needed basics.
- Don’t stop at PDF and video content, google for more similar challenges.
- Take your favorite scripting language and make a single script to automate your solution for the box you owned, If you need to do tiny automation in exam this will help.
- Stop reading review and read the resources and google.
- Enumerate, Enumerate and Enumerate, and some times it right facing you so be smart enough not to ignore.
- Don’t focus too much in automation and always keep a ***Plan B***.
- Keep a fresh VM image with respective tools you might need as your backup.
- Prepare a schedule and if that start to fails, don’t give up easily and ***TRY Smarter***.
- Don’t use “*Dirty Cow*”, thats not the intended way in any of the boxes and when you realise it you already might have lost the first attempt in exam. (***Hard truth, a couple of friend didn’t understood, Now don’t be them***)

- Avoid Metasploit for good.

0x06 — Resources

All in one References

- http://pwnwiki.io/#!index.md
- https://jivoi.github.io/2015/07/01/pentest-tips-and-tricks/

Great Reviews

- http://www.abatchy.com/2017/03/how-to-prepare-for-pwkoscp-noob.html
- https://www.securitysift.com/offsec-pwb-oscp/

Enumeration Cheatsheet

- https://highon.coffee/blog/nmap-cheat-sheet/
- https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/
- http://www.0daysecurity.com/penetration-testing/enumeration.html

Privilege Escalation Cheatsheet

- https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
- https://github.com/rebootuser/LinEnum
- https://www.securitysift.com/download/linuxprivchecker.py
- https://github.com/PenturaLabs/Linux_Exploit_Suggester
- https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/
- https://www.youtube.com/watch?v=kMG8IsCohHA
- http://www.fuzzysecurity.com/tutorials/16.html
- https://toshellandback.com/2015/11/24/ms-priv-esc/
- https://github.com/51x/WHP
- https://isc.sans.edu/diary/Windows+Command-Line+Kung+Fu+with+WMIC/1229

Reverse Shell Cheatsheet

- https://www.phillips321.co.uk/2012/02/05/reverse-shell-cheat-sheet/

- https://highon.coffee/blog/reverse-shell-cheat-sheet/
- http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

Get TTY shell

- https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/
- https://netsec.ws/?p=337

Buffer Overflow

- https://www.corelan.be/index.php/2009/07/19/exploit-writing-tutorial-part-1-stack-based-overflows/
- http://netsec.ws/?p=180

Msfvenom Cheatsheet

- http://security-geek.in/2016/09/07/msfvenom-cheat-sheet/

Porting Metasploit Exploits

- https://netsec.ws/?p=262

Port forwarding & Pivoting

- https://artkond.com/2017/03/23/pivoting-guide/
- http://atropineal.com/2016/11/18/pivoting-with-ssh-and-proxychains/
- http://netsec.ws/?p=278

Client-Side Attacks

- https://www.offensive-security.com/metasploit-unleashed/client-side-exploits/

Practice Points

- https://www.hackthebox.eu/
- https://www.vulnhub.com/
- https://exploit-exercises.com/
- https://shellterlabs.com/en/

. . .

Find me here:

m4lv0id:: Member Profile

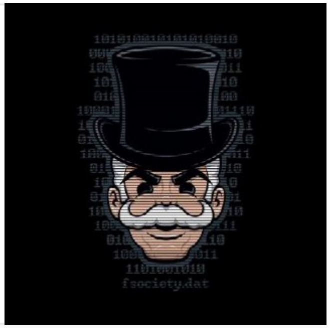
An online platform to test and advance your skills in penetration testing and cyber security.

www.hackthebox.eu

m4lv0id (Praveen Nair)

m4lv0id has 6 repositories available. Follow their code on GitHub.

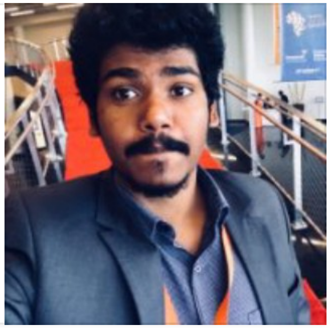
github.com



Praveen Nair | Professional Profile | LinkedIn

View Praveen Nair's professional profile on LinkedIn. LinkedIn is the world's largest business network, helping...

www.linkedin.com



Thanks to Nilesh Deokar.

Hacking Oscp Offensive Pentesting Review

741 claps

8

Praveen Nair

Follow

Security Researcher (OSCP) | Malware Enthusiast @KeralaCyberSquad. Find me @ https://www.linkedin.com/in/praveennair0x00/ https://www.hackthebox.eu/profile/389

Responses

Write a response…

Conversation between Muhammad Khizer Javed and Praveen Nair.

Muhammad Khizer Javed
Oct 20, 2017

Congratulations For OSCP :) And Thanks for sharing this :D from today i'm going to TRY HARDER :D to prepair For OSCP ;)

1

1 response

Praveen Nair
Oct 27, 2017

Thanks and hope this will help you in the journey of Trying Harder!

1

Conversation between Anugrah Sr Hadwads and Praveen Nair.

Anugrah Sr Hadwads
Dec 15, 2017

congrats bro…
pwolik bro

1

1 response

Praveen Nair
May 25, 2018

Thanks man, Hope it did help you :)

Conversation between Rahul R and Praveen Nair.

Rahul R

Apr 22, 2018

Awesome Writeup

1

1 response

Praveen Nair

May 25, 2018

Thanks man, Hope it did help you :)

Conversation between Ons A. and Praveen Nair.

Ons A.

Oct 20, 2017

Congrats on your OSCP, and thanks for the detailed write-up!

1

1 response

Praveen Nair
Oct 27, 2017

Thanks and glad to know you liked it :)

1

Conversation between Gamliel Seqwerty and Praveen Nair.

Gamliel Seqwerty
Nov 1, 2017

Thank you for sharing your experience, congratulations for your OSCP Cert and thanks for sharing amazing resources.

1 — 1 response

Praveen Nair
Nov 8, 2017

Thanks and hope it did help you.. (:

1

Conversation with Praveen Nair.

Biman Roy
May 27, 2018

Hi Praveen,

I have signed up for PWK/OSCP 90-day course. This is my 2nd week. I am finished about 180 pages of the 380 page pdf doc, and practising the exercises (e.g., the buffer overflow ones). When will I get those exercises of finding the vulnerability? Just want to make sure I have not losing out anything.

1 response

Praveen Nair
Jun 23, 2018

I believe you have gone through a quick read on the course content because it have it all. And about the vulnerability, I’m pretty sure the OSCP lab is the best way to figure it out. :)

Conversation with Praveen Nair.

Arbaz Hussain
Oct 16, 2017

Congrats for OSCP & Thanks for Awesome Resources .

1

1 response

Praveen Nair

Oct 17, 2017

> Congrats for OSCP & Thanks for Awesome Resources .

Thanks and hope it will help you.

1

Conversation between Praveen Nair and sang darkside.

sang darkside

Jun 3, 2018

hello bro,

Does OSCP exam has buffer overflow for linux ?

1

1 response

Praveen Nair

Praveen Nair
Jun 23, 2018

Sorry mate, I cannot disclose anything about the exam.

Please do avoid asking questions specific to the exam.

1 response

sang darkside
Jun 25, 2018

I passed the exam last 2 weeks. Thank bro.

1

1 response

Praveen Nair
Jun 27, 2018

Great, Congrats :)