OSCP Exam review "2019" + Notes & Gift inside!

21y4d March 15 edited March 24 in Off-topic

For the past couple of months, I have been away from HTB, as I have been working on the OSCP labs, as a preparation for my OSCP exam. I have just finished my OSCP exam and got my certification, and thought I would write this review, especially for HTB members, from an HTB member perspective.

PWK lab

First of, I would like to review the PWK labs.

Before starting on the lab machines, I took 5 days to finish the PWK course materials, as there are some useful things here and there.

The PWK lab in general is very well designed and well structured. This means that the lab can accommodate both beginners and advanced users, and that beginners will have plenty of machines to learn on before starting on advanced machines.

I have finished all of the lab networks, except for the Admin network, which I could not find the key to unlock it even though I literally owned all other machines. The support was of no help as well, as always.

Most of the machines in the PWK lab "80%" are designed for beginners, and are directly exploitable. This gives beginners a lot of space to learn and improve their skills before going for more advanced machines.

As for the advanced machines, the ones worth mentioning are:
-Humble "Shell"
-Sufferance "Shell"

-Alpha
-Joe
-Pain
-Ralph

The remaining machines were mostly directly exploitable with one exploit, and some times as a root/system user.

As for the other labs "IT & Dev", only a couple of machines were directly exploitable, and all of the rest needed credentials found on post exploitation on other machines "i.e. in txt file, repeated user pass, golden ticket stealing, etc". The useful thing from using these labs is having to learn pivoting properly, even though this is not required for the exam. I took this chance to write my personal instructions for pivoting using 5 different methods, in both port forwarding and dynamic forwarding.

You can find my pivoting notes here:
https://github.com/21y4d/Notes/blob/master/Pivoting.txt

My only negative take on the PWK lab machine is that they were getting outdated. This means dealing mostly with Windows XP, 2008, or REHL 5 machines, which meant too many unintended exploits, making it difficult to guess which one was actually the intended way. I think the PWK lab might need an overhaul in the near future, otherwise they might become irrelevant to the real world.

PWK lab vs HTB lab

As for the PWK lab from an HTB member perspective, I honestly thought the machines were relatively easy!

So you get an idea of my experience at HTB before I started my OSCP labs, my ranking at HTB was "elite hacker", I had 18/20 of the active machines, all of the retired machines, and the last machine I did was Sizzle, which was super fun.

The most difficult machines in the PWK lab were of a similar difficulty to a medium rated machine in HTB. The most challenging PWK machines "Sufferance, Gh0st, Observer", were of a similar difficulty to machines like Bastard, Mirai, SolidState, Shocker, Frolic, and other similar machines at HTB.

The PWK machines were almost exclusively exploitable using exploits, with the occasional system misconfiguration. Even in my exam, almost all of the machines were exploitable using a public exploit, with some modifications.

The main reason behind this is that OffSec wants to make the lab like a real pen testing, which in this case they did a very good job, as real pen testing is mostly dealing with exploits.

However, I wish they added more advanced techniques that dealt with system misconfigurations, to teach people how to look for those as well. In a real pen test, if a machine and all of its components is fully patched, that only gives 50% of the security, as the other 50% comes from looking for misconfigurations to get access.

Finally, I think any Pro Hacker in HTB is more than ready to take the OSCP exam. However, I would still suggest taking the PWK lab, as there are some things to learn, as I will mention next.

Proctored OSCP Exam

As for the my exam experience, here's how I did:

Owned machines: 5/5
Points collected: 100/100
Time taken: 10 hours
Report: 8 hours/50 pages
Exam attempts: 1

If you are comfortable enough with the level of machines I was explaining earlier, you should be able to take the OSCP exam. However, as I have stated before, there definitely are some skills that one needs to learn before taking the exam.

First off, the machines are definitely not the same level as the PWK lab, but more like the HTB machines I mentioned above, expect for the 10 points one which is very straightforward .

The exam has several things that make it more challenging, and not only the difficulty of the machines in it.

1. You have to really know how to handle your time properly. I

think this is the main challenge in the OSCP exam. Rooting 5 "medium difficulty" machines in just 24 hours is no easy task, as it takes a lot of skill to be able to enumerate, adjust, and exploit all of these targets in just 24 hours, while having to take some time to rest and cool off. Honestly, I think if the machines were more advanced, or if the exam time was just 12 hours instead, very few people would be able to pass the exam. Which is why I think the exam time/difficulty were very well matched.

2. Rabbit holes! If the PWK lab machines do not have many rabbit holes, the OSCP exam's definitely do! I think all of the machines I had to exploit had rabbit holes "except for the BOF of course". If you didn't know how to deal with rabbit holes, you will waste your precious time without any progress. This was one of the things I had to teach myself before taking the OSCP exam, so I started a habit of writing a summary of findings as I was doing any machine. I simply write the attack surface and chance of exploitation, then I start from the top, and if one does not work for a while I move to the other. This tip will make your life much easier during your OSCP exam. There's an excellent writeup by g0tmi1k for the Alpha machine in PWK forums, which teaches you how to do that.
3. Reporting. While some might think that having to write a report after getting the needed points from the exam is unnecessary, I would say otherwise. Personally, I work in this field, and I know that any pen tester who does not know how to write a good report will not be useful for anyone. The companies do not want you to tell them that their machines are vulnerable, they want to know how exactly, so that they can not only patch the vulnerability, but also fix their design and way of thinking. Having said that, the OSCP exam report prepares you for such real life pen testing reports, as it gives you a template you can build upon, and start learning the design of such reports.

As for the proctoring part of the exam, even though you would not have the freedom of doing the machines as if you were alone "i.e. like in the lab", since someone would be watching you all the time, I think this part was very necessary and well thought by OffSec. This

was just like when I took the PMP or CCNA exams, an online exam with someone proctoring you to prevent cheating. If you are not cheating, you have nothing to hide and should not have a problem with proctoring ”cheating means someone else doing your work for you". This will also give you credit for your efforts, and not have some people doubt that some OSCP holders might not have the skill.

The BOF machine was fairly similar to the example shown in the PWK course, which is basic Windows BOF, with nothing advanced "ASLR, DEP, x64..etc".

It is a simple buffer overflow, requiring you to know three basic thing:
1-Finding the length of the buffer
2-Finding bad characters
3-Finding a proper return address

You can find the python scripts I used with detailed instructions here:
Redacted

As for the use of Metasploit in the exam, I have always preferred not to use MSF unless it was necessary, as knowing how to manually exploit teaches you much much more. Even in the PWK lab, I didn't use MSF at all, except for post exploitation enumeration, so it would be faster. However, in my exam, I did use MSF, because I faced an exploit I knew that can only be done with MSF, as I have faced this exact vulnerability before here in one of the HTB boxes, and back then I tried everything without MSF "so did other people" and eventually I had to use MSF. This saved me a lot of time, since I already knew I have to use MSF here, and not waste my time trying to exploit it without it.

At the end, I think that the PWK lab does prepare you for a real pen test, and if you are OSCP certified, then you are definitely qualified to be a pen tester.

My Gift for HTB Members

I wish you liked my review of the OSCP exam, and I have a gift for you.

During my PWK lab time, I wanted to improve my bash scripting skills. So, I wanted to automate all of the process of recon/enumeration that I run every time, and instead focus my attention on real pen testing.

I created a tool I called "nmapAutomator", which is designed to run fully automatically with no interaction from your side whatsoever. If you choose the "All" option, and run the script for the target IP, I can assure you that you can leave the script running in the background, and if there's anything nmap can tell you, you will find it. I tried to make it as efficient as possible, so that it would give accurate results as fast as possible. I even added automatic recon/enumeration to be run after that "i.e. gobuster, nikto, smbmap..etc", based on the found ports.

I have tested this script on over 20 PWK lab machines, and I can say that 95% of the time if there's something recon would tell you, you will find it here. I have not yet tested this machine on HTB boxes, but I assume it would work just the same, as it should be universal.

Finally, I have used this script during my OSCP exam "which was the main reason I've written it", and I can honestly say that this was one of the reasons I was able to finish all machines in 10 hours. This is simply because before starting any machine, I run this script with the "All" option on another machine, and by the time I go to that other machine, I would have a full recon report ready for me, instead of wasting an hour or so waiting for that. I did not have to run any other recon tool during my exam, as everything was automatically laid out by this script.

I hope you like it, and please feel free to share it or improve it.

You can get it and read more about it from the following GitHub link: https://github.com/21y4d/nmapAutomator

Future Plans

Now that I have obtained my OSCP certification, I think I will directly go for OSCE, as I have been preparing for both together. For those who took it, how is it different from OSCP? What skills do I need before joining the CTP course and lab?

I also think I will take OSWE and OSEE after that, but we'll see about that later.

Thanks a lot for taking the time to read my review 🙂

Check out nmapAutomator:
[nmapAutomator](https://github.com/21y4d/nmapAutomator)

[![21y4d](https://www.hackthebox.eu/badge/image/36215)](https://www.hackthebox.eu/home/users/profile/36215)
OSCP | CCNA | PMP

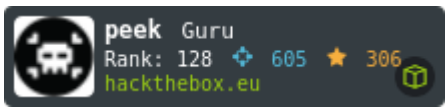
Oscp

Comments

« 1 2 »

peek March 15

very good review, point 2 will help a lot. and thanks so much for your tool.



Monty March 15

Exactly the review I needed as I'm considering taking the exam next couple of months.

achayan March 15

@21y4d that's an amazing write up ... really useful for people like me who prepare for such exams ... regarding the proctored part .... "what about breaks in b/w ? " .. and could we see the person watching us ? .. and were the machines were entirely new from previous machines in exam ? .. again thanks for such a useful write up 🙂

21y4d March 15

I'm glad you like it guys..

@achayan
Actually you forget about the proctor once you start focusing on the exam. You cannot see the the proctor, as this would probably distract students, and would give a feeling that someone is watching you..
You can take short/long breaks whenever you need, you just need inform the proctor before leaving and after returning, so that they make sure they can still see your screen and webcam before you start working again.

At the beginning of the exam you will need to show your ID and to give a webcam tour of the room you're in, and you should be alone in the room. Also, after a long break "several hours" you will have to scan the room again, which take around 30 seconds.

I guess I forgot to mention, but this was my only attempt at the exam. I'm pretty sure every attempt you would get different machines, as they have a big exam lab with so many machines you might get.

Check out nmapAutomator:
[nmapAutomator](https://github.com/21y4d/nmapAutomator)

[![21y4d](https://www.hackthebox.eu/badge/image/36215)](https://www.hackthebox.eu/home/users/profile/36215)
OSCP | CCNA | PMP

achayan March 15

@21y4d oh .. that's really informative .... thanks again for sharing your experience ...

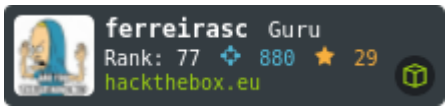
ferreirasc March 15

Fantastic! I will do my exam next month.

I will definitely consider your tool, mate! xD

I'll probably have some questions about the proctoring ... Could I ask you? 🙂

Big thank you @21y4d !



21y4d March 15

Type your comment> @ferreirasc said:

> *Fantastic! I will do my exam next month.*
>
> *I will definitely consider your tool, mate! xD*
>
> *I'll probably have some questions about the proctoring ... Could I ask you?* 🙂
>
> *Big thank you @21y4d !*

Sure.. PM me whenever you need 🙂

Check out nmapAutomator:
[nmapAutomator](https://github.com/21y4d/nmapAutomator)

[![21y4d](https://www.hackthebox.eu/badge/image/36215)](https://www.hackthebox.eu/home/users/profile/36215)
OSCP | CCNA | PMP

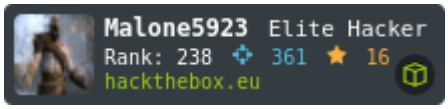
xd3m0n March 15

Golden material man. Thank you very much. Very useful.

meh

Malone5923 March 15

Really good review @21y4d . I like the fact you wrote from a pro HTB member perspective. Thank you for this. I will also appreciate a PM of your pivoting notes as I am taking the exam next month and this will be usefull to me.

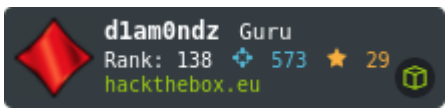


Patapinh0 March 16 edited March 16

Thanks a lot for this post, mate ! Really useful addition to the reviews already out there, should help a ton 🙂
Would it be possible to have your notes on pivoting via PM, too ?

d1am0ndz March 16

Thanks for contributing to the community! 🙂



B0rN2R00T March 16

Congrats @21y4d and thanks for sharing review and scripts 🙂

B0rN2R00T

21y4d March 16

I'm glad you find it useful 🙂

@Malone5923 @d1am0ndz
Check your PM 🙂

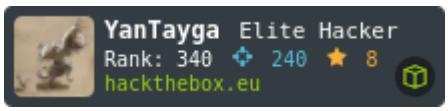
I've also added it above so anyone can access it now 🙂

Check out nmapAutomator:
[nmapAutomator](https://github.com/21y4d/nmapAutomator)

[![21y4d](https://www.hackthebox.eu/badge/image/36215)](https://www.hackthebox.eu/home/users/profile/36215)
OSCP | CCNA | PMP

YanTayga March 16

Thanx a lot for your report!
Is the exam BOF really so simple?



21y4d March 16

Type your comment> @YanTayga said:

> *Thanx a lot for your report!*
> *Is the exam BOF really so simple?*

It is just like the one in the PWK pdf course.

I have added above my BOF instructions and skeletal code, which goes into specific details of getting your exploit to work, making the process very easy and clear... Just follow it and you should be golden! 🙂

Check out nmapAutomator:
[nmapAutomator](https://github.com/21y4d/nmapAutomator)

[![21y4d](https://www.hackthebox.eu/badge/image/36215)](https://www.hackthebox.eu/home/users/profile/36215)
OSCP | CCNA | PMP

---

sysDom March 16

This is a great review, thanks! I'm about to start the OSCP lab, so I'm focusing on HTB until it starts. I'm really worried about the time contrainsts, more so because of the awkwark kali vm they make you use. It normally takes me a full night to get through just dirb; so maybe nmapAutomator will help with timing. I'm going to test it out on HTB and the OSCP labs, thanks so much for posting it.

21y4d March 17

If anyone has done OSCE or OSWE, I have some questions, and would appreciate a PM 🙂

Check out nmapAutomator:
[nmapAutomator](https://github.com/21y4d/nmapAutomator)

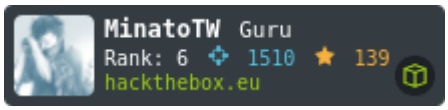
[![21y4d](https://www.hackthebox.eu/badge/image/36215)](https://www.hackthebox.eu/home/users/profile/36215)
OSCP | CCNA | PMP

sthmlflum March 17

The 'nmapAutomator' is simply 1337, thanks!

MinatoTW March 17

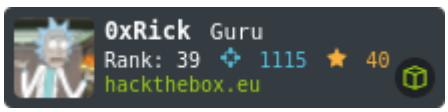
Well done and congrats 🙂



Don't let the box pwn you!!

Ahm3dH3sham March 17

Thanks for the review and the tool that's a great contribution.
Congrats !

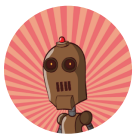


https://0xrick.github.io

Chuspi1k March 19

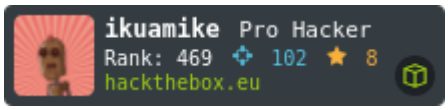
Thanks a lot @21y4d for your review, I'm right now training to pass the OSCP test and your information is amazing.
I hope that your tools and notes will be incredibles too.

Thank you so much mate.



ikuamike March 19

Thank you for this!!



CGonzalo March 19

Congrats!!!

And thank you very much @21y4d a valuable contribution!

xformer1337 March 20

regarding the proctoring thing.... does that mean we have to refrain from swearing even when we got stuck in the middle of oscp exam...? That can be a challenging thing to me... >"<

21y4d March 20

Type your comment> @xformer1337 said:

> *regarding the proctoring thing.... does that mean we have to refrain from swearing even when we got stuck in the middle of oscp exam...? That can be a challenging thing to me... >"<*

They can't hear you, if that's what you're asking..

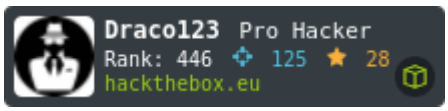
Check out nmapAutomator:
[nmapAutomator](https://github.com/21y4d/nmapAutomator)

[![21y4d](https://www.hackthebox.eu/badge/image/36215)](https://www.hackthebox.eu/home/users

/profile/36215)
OSCP | CCNA | PMP

Draco123 March 22 edited March 22

Congratulations !! This is Golden man. Thanks for the Super review about the exam and the tool. Very Informative and Helpful @21y4d .

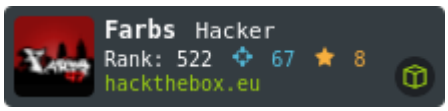


Farbs March 22

Type your comment> @21y4d said:

> *Type your comment> @xformer1337 said:*
>
> *show previous quotes*
>
> *They can't hear you, if that's what you're asking..*

This cracked me up lol.



bansheepk March 22

Congratilations on passing it the first time!!! I passed in the OSCP Exam on February 20th, but I failed multiples times, I started the PWK course having a very poor hacking knowledgement, and started learning everything during the course, and from there I met HTB. HTB really helped me to keep practicing to the exam after I pwned the whole offsec labs (except the PI box) and however I think the HTB machines intend to be more CTF-like boxes than offsec, the HTB boxes are much more difficult in general. I want to go for OSCE too

as soon as I feel prepared, but I started reading "The Shellcoders Handbook" as a preparation for OSCE, but I couldnt replicate most of the things the book teaches, I could never develop a shellcode to pop a calculator on windows, even after reading corelan guides, because of that I am feeling unconfident.

pingunrchable March 23

Hey man, congratulations on passing your OSCP.

I am looking to do OSCP soon but I feel that I am not ready to do so especially after doing some of the "easy" HTB boxes.

Should I:

- Do more HTB boxes before going on to OSCP or
- Do the OSCP course and exam then use HTB as a means of upkeeping my skill?

Let me know your opinion.

FYI: I am an experienced Network Engineer.

21y4d March 23

@bansheepk said:
> Congratilations on passing it the first time!!! I passed in the OSCP Exam on February 20th, but I failed multiples times, I started the PWK course having a very poor hacking knowledgement, and started learning everything during the course, and from there I met HTB. HTB really helped me to keep practicing to the exam after I pwned the whole offsec labs (except the PI box) and however I think the HTB machines intend to be more CTF-like boxes than offsec, the HTB boxes are much more difficult in general. I want to go for OSCE too as soon as I feel prepared, but I started reading "The Shellcoders Handbook" as a preparation for OSCE, but I couldnt replicate most of the things the book teaches, I could never develop a shellcode to pop a calculator on windows, even after reading corelan guides, because of that I am feeling unconfident.

I suggest you check Pentester Academy, they have some very useful courses that can help you a lot in learning shellcoding from scratch.

Check out nmapAutomator:
[nmapAutomator](https://github.com/21y4d/nmapAutomator)

[![21y4d](https://www.hackthebox.eu/badge/image/36215)](https://www.hackthebox.eu/home/users/profile/36215)
OSCP | CCNA | PMP

« 1 2 »

SIGN IN to comment.

Howdy, Stranger!

Click here to create an account.

SIGN IN

Categories
Recent Discussions
Activity

Categories

All Categories	1.7K
Support	238
Billing	23
VPN Connection	136
Website	71
Discussion	1K
Machines	511
Challenges	252
RastaLabs	11
Exploits	41
Programming	7
Off-topic	205
Tutorials	403
Writeups	242
Video Tutorials	48
Tools	58
Other	53
Links	8
News	8

In this Discussion

pingunrchable	March 24
bansheepk	March 22
Farbs	March 22
Draco123	March 22
xformer1337	March 20
CGonzalo	March 19
ikuamike	March 19
Chuspi1k	March 19
Ahm3dH3sham	March 17
MinatoTW	March 17

sthmlflum	March 17
sysDom	March 16
YanTayga	March 16
B0rN2R00T	March 16
d1am0ndz	March 16
Patapinh0	March 16
Malone5923	March 15
xd3m0n	March 15
ferreirasc	March 15
21y4d	March 23