Offensive Security Professional Overview Survival

Joas Antonio

Details

- This PDF is exclusive to put all types of content for you to prepare for OSCP, basically to consult the content links, the goal is to bring everything together in one place.

- My LinkedIn: https://www.linkedin.com/in/joas-antonio-dos-santos

OSCP Introduction

- https://www.offensive-security.com/pwk-oscp/
- https://en.wikipedia.org/wiki/Offensive_Security_Certified_Professional
- https://www.youtube.com/watch?v=78J6A8irz3M&ab_channel=I.T.CareerQuestions
- https://alpinesecurity.com/blog/oscp-vs-lpt-master-a-comparison-made-by-a-cybersecurity-professional-with-both-certifications/
- https://startacybercareer.com/oscp-vs-ceh-which-should-you-choose/

OSCP Mindmaps

- https://cd6629.gitbook.io/ctfwriteups/oscp-cheatsheet-unfinished
- https://emaragkos.gr/infosec-adventures/useful-oscp-mindmaps/
- https://medium.com/@peregerinebunny/my-oscp-journey-d3addc26f07b
- https://githubmemory.com/repo/corneacristian/OSCP-MindMap
- https://rafalharazinski.gitbook.io/security/penetration-testing-with-kali
- https://firebitsbr.wordpress.com/2015/04/04/mind-map-penetration-testing-with-kali-linux-pwk-2015-unofficial/
- https://github.com/umuttosun/OSCP-MindMap
- https://github.com/5bhuv4n35h/pentestmindmap
- https://www.linkedin.com/feed/update/urn:li:activity:6754329534872522753/

OSCP Labs

- https://www.mindmeister.com/pt/1781013629/the-best-labs-and-ctf-red-team-and-pentest
- https://www.offensive-security.com/labs/
- https://www.hackthebox.eu/
- https://tryhackme.com/
- https://www.youtube.com/watch?v=Zoiq69_7Dr0&ab_channel=MubasherSadeeque
- https://github.com/rkhal101/Hack-the-Box-OSCP-Preparation

OSCP Vuln Machines – Windows

OSCP Vuln Machines: Forest HTB

- https://www.youtube.com/watch?v=hWwvWwZEVLU&ab_channel=I.TSecurityLabs
- https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/windows-boxes/forest-writeup-w-o-metasploit

OSCP Vuln Machines: Legacy HTB

- https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/windows-boxes/legacy-writeup-w-o-metasploit
- https://www.youtube.com/watch?v=ZXsbEXhbFOI

OSCP Vuln Machines: Jerry HTB

- https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/windows-boxes/jerry-writeup-w-o-metasploit
- https://www.youtube.com/watch?v=PJeBIey8gc4&ab_channel=IppSec

OSCP Vuln Machines: Devel HTB

- https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/windows-boxes/devel-writeup-w-o-metasploit
- https://www.youtube.com/watch?v=pZXjvOzUago&ab_channel=I.TSecurityLabs

OSCP Vuln Machines – Linux

OSCP Vuln Machines: Lame HTB

- https://www.youtube.com/watch?v=r7GoQ-gAg_4&ab_channel=I.TSecurityLabs
- https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/linux-boxes/lame-writeup-w-o-metasploit

OSCP Vuln Machines: Brainfuck HTB

- https://www.youtube.com/watch?v=o5x1yg3JnYI&ab_channel=IppSec
- https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/linux-boxes/brainfuck-writeup-w-o-metasploit

OSCP Vuln Machines: Shocker HTB

- https://www.youtube.com/watch?v=GVjNI-cPG6M&t=2267s&ab_channel=s4vitar
- https://www.youtube.com/watch?v=6Zv2xG8xFYg&ab_channel=I.TSecurityLabs
- https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/linux-boxes/shocker-writeup-w-o-metasploit

OSCP Vuln Machines: Jarvis HTB

- https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/linux-boxes/jarvis-writeup-w-o-metasploit
- https://www.youtube.com/watch?v=9MBTlCCezVA&ab_channel=I.TSecurityLabs
- https://www.youtube.com/watch?v=YvFArFnaibg&ab_channel=s4vitar

OSCP Writeup HTB Preparation

https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/linux-boxes

OSCP Journey and Preparation

https://ranakhalil101.medium.com/my-oscp-journey-a-review-fa779b4339d9
https://medium.com/@akashgupta1496/my-oscp-journey-june-2020-d4512155d289
https://diesec.home.blog/2020/10/11/oscp-journey/
https://www.noobsec.net/oscp-journey/
https://alex-labs.com/my-oscp-journey/
https://github.com/strongcourage/oscp
https://www.linkedin.com/pulse/concluding-my-oscp-journey-dennis-perto/?trk=read_related_article-card_title
https://scriptkidd1e.wordpress.com/oscp-journey/
https://www.tripwire.com/state-of-security/security-awareness/oscp-journey/
https://esseum.com/the-oscp-journey-my-personal-experience-of-passing-the-exam/
https://pt.slideshare.net/VandanaVerma24/oscp-journey
https://www.daniel-pinto.dev/my-journey-to-oscp/
https://community.infosecinstitute.com/discussion/125665/beginning-my-oscp-journey

OSCP Journey and Preparation

https://bohansec.com/2020/08/08/My-Journey-to-OSCP/
https://omarm.ca/blog/my-oscp-journey
http://www.minuszeros.com/my-oscp-journey/
https://bksecurity.org/my-oscp-journey/
https://www.youtube.com/watch?v=fkNozXlrB6I&ab_channel=CryptoKnight
https://www.youtube.com/watch?v=7Sbx1QPy1mw&ab_channel=JSONSEC
https://www.youtube.com/watch?v=y8nqTtQawAk&ab_channel=JSONSEC
https://www.youtube.com/watch?v=DMwkLGbB_ac&ab_channel=cwinfosec
https://www.youtube.com/watch?v=L6vMBEla2Uk&t=98s&ab_channel=hyd3sec
https://www.youtube.com/watch?v=waUdifAzblE&ab_channel=BusraDemir
https://www.offensive-security.com/offsec/my-philosophical-approach-to-oscp/
https://sock-raw.org/blog/oscp-review/
https://royaljay.com/security/how-i-became-an-offensive-security-certified-professional/
https://www.helviojunior.com.br/it/security/minha-experiencia-no-oscp/

OSCP Journey and Preparation

https://steflan-security.com/my-oscp-journey/
https://johnjhacking.com/blog/the-oscp-preperation-guide-2020/
https://www.netsecfocus.com/oscp/2019/03/29/The_Journey_to_Try_Harder-_TJNulls_Preparation_Guide_for_PWK_OSCP.html
https://cybersecurity.att.com/blogs/security-essentials/how-to-prepare-to-take-the-oscp
https://medium.com/@shubhamkhichi5/how-to-practice-and-pass-oscp-from-scratch-a06ef4b5d28a
https://github.com/0x4D31/awesome-oscp
https://github.com/RustyShackleford221/OSCP-Prep
https://rana-khalil.gitbook.io/hack-the-box-oscp-preparation/my-oscp-journey-a-review
https://hackersinterview.com/oscp/pre-enrollment-oscp-preparation/
https://www.cbtnuggets.com/blog/career/career-progression/how-to-prepare-for-the-oscp

OSCP Repositores

https://github.com/cpardue/OSCP-PWK-Notes-Public
https://github.com/gh0x0st/OSCP-A-Step-Forward
https://github.com/noraj/OSCP-Exam-Report-Template-Markdown
https://github.com/wwong99/pentest-notes/blob/master/oscp_resources/OSCP-Survival-Guide.md
https://github.com/omurugur/OSCP
https://gist.github.com/natesubra/5117959c660296e12d3ac5df491da395
https://github.com/0x4D31/awesome-oscp
https://github.com/whoisflynn/OSCP-Exam-Report-Template
https://github.com/strongcourage/oscp
https://github.com/CyDefUnicorn/OSCP-Archives
https://github.com/DriftSec/AutoRecon-OSCP
https://gist.github.com/unfo/5ddc85671dcf39f877aaf5dce105fac3
https://github.com/six2dez/OSCP-Human-Guide

OSCP Repositores

https://github.com/tagnullde/OSCP
https://github.com/superhero1/OSCP-Prep
https://github.com/The-Lynx-Team/OSCP
https://github.com/chvancooten/OSCP-MarkdownReportingTemplates
https://github.com/ssstonebraker/oscp-scripts
https://github.com/CaptBoykin/oscp
https://github.com/burntmybagel/OSCP-Prep
https://github.com/alexiasa/oscp-omnibus
https://github.com/JoaoPauloF/OSCP

Support content

I made other PDF's that talk about advanced attacks on web applications, exploit development and privilege escalation, so I add this PDF as a complement.

https://drive.google.com/drive/u/0/folders/12Mvq6kE2HJDwN2CZhEGWizyWt87YunkU

Buffer Overflow to OSCP 25 Points

https://medium.com/techloop/understanding-buffer-overflow-vulnerability-85ac22ec8cd3
https://www.youtube.com/watch?v=qSnPayW6F7U&ab_channel=TheCyberMentor
https://www.youtube.com/watch?v=oS2O75H57qU&ab_channel=LiveOverflow
https://www.youtube.com/watch?v=d1U-czwATiM&ab_channel=DuckademyITcourses
https://bufferoverflows.net/for-beginners-linux-buffer-overflow-challenge/
https://www.sans.org/reading-room/whitepapers/threats/paper/481
https://github.com/CyberSecurityUP/Buffer-Overflow-Labs
https://github.com/V1n1v131r4/OSCP-Buffer-Overflow
https://github.com/rdoix/Buffer-Overflow-Cheat-Sheet
https://sec4us.com.br/cheatsheet/bufferoverflow-seh
https://oscp.securable.nl/buffer-overflow
https://www.youtube.com/watch?v=4rUN1F6_Mhk&ab_channel=NakerahNetwork
https://www.youtube.com/watch?v=yAsO25Fezdk&ab_channel=NakerahNetwork
https://www.youtube.com/watch?v=RmpNQQwhDms&ab_channel=IronHackers

Buffer Overflow to OSCP 25 Points

https://www.youtube.com/watch?v=_EYoYiSInSA&ab_channel=InfoCk
https://thelistsec.com/2020/06/23/oscp-like-buffer-overflow-walkthrough/
https://www.trenchesofit.com/2020/09/12/oscp-buffer-overflow-write-up/
https://github.com/justinsteven/dostackbufferoverflowgood
https://www.youtube.com/watch?v=UcR_tw4J0CM&ab_channel=NikhilSahoo
https://reigadaopsec.com/buffer-overflow-oscp-preparation-dostackbufferoverflowgood/
https://www.youtube.com/watch?v=VX27nq6EcjI&ab_channel=Vin%C3%ADciusVieira
https://www.youtube.com/watch?v=8So2XCateS8&t=144s&ab_channel=JoasAntonio

Z3r0 to H3R0

https://www.linkedin.com/pulse/certifica%C3%A7%C3%A3o-oscp-do-zero-ao-h3r0-pt1-joas-antonio/?trk=read_related_article-card_title
https://kentosec.com/2018/06/24/oscp-zero-to-hero-episode-0-new-beginnings/
https://noobshelly.com/home/another-oscp-blog/
https://medium.com/@igor.lrgomes/minha-jornada-na-oscp-d5b5297bcb2d
https://medium.com/@1chidan/zero-to-oscp-concise-edition-b5ecd4a781c3

Speaks and Playlist

https://www.youtube.com/watch?v=tUda04a3hfI&ab_channel=Vin%C3%ADciusVieira
https://www.youtube.com/watch?v=s2wXhgrwSkc&ab_channel=PapoBin%C3%A1rio
https://www.youtube.com/watch?v=pvhtg3JmCcU&ab_channel=RicardoLongatto
https://www.youtube.com/watch?v=5NvBujK_0dQ&list=PL0-qC9zS1xpmd5sANeqFhou7UrrZJknJB&ab_channel=Wraiith75
https://www.youtube.com/watch?v=exnd5kXh_FM&list=PLZ59RPGKmV91BQH5bTXOG-0IkuXvvD1CM&ab_channel=InfoSecAddicts
https://www.youtube.com/watch?v=Klmy6xeKW7o&ab_channel=BhargavTandel
https://www.youtube.com/watch?v=GbppskJ5FU4&list=PLqSNTTjCEmZG50-vtmdAHWGFbDLUMhPeN&ab_channel=RaDarth
https://www.youtube.com/watch?v=I1rUhUMSOCM&ab_channel=Ray%5BREDACTED%5D
https://www.youtube.com/watch?v=pwUZCiVB4Pk&ab_channel=JanWikholm
https://www.youtube.com/watch?v=2DqdPcbYcy8&list=PLidcsTyj9JXK-fnabFLVEvHinQ14Jy5tf&ab_channel=IppSec
https://www.youtube.com/watch?v=Nh8doFZcBJI&list=PLwDy-UjR-HbvP4l7IVr2B9UcKxQI6VB3b&ab_channel=V%C3%ADctorGarc%C3%ADa

Conclusion

The OSCP certification is one of the most coveted and feared at the same time, I am on my journey in search of it and I saw that many colleagues are lost in relation to content, so I created this framework that I hope will be useful.

But in summary, practice a lot in the laboratories and study the material well, develop reports also to have the habit of writing something that pleases the examiners, today it is much easier to conquer it, because there is plenty of content on the internet, so I did this favor to help catalog this content.