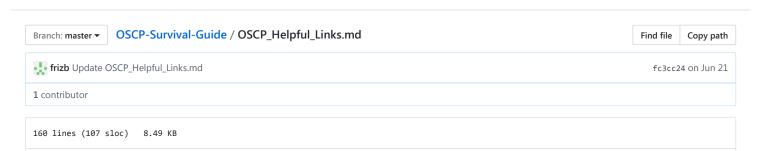
Frizb / OSCP-Survival-Guide



OSCP Course Review

- Offensive Security's PWB and OSCP My Experience http://www.securitysift.com/offsec-pwb-oscp/
- OSCP Journey https://scriptkidd1e.wordpress.com/oscp-journey/
- Down with OSCP
 http://ch3rn0byl.com/down-with-oscp-yea-you-know-me/
- Jolly Frogs Tech Exams (Very thorough)

http://www.techexams.net/forums/security-certifications/110760-oscp-jollyfrogs-tale.html

OSCP Inspired VMs and Walkthroughs

- https://www.vulnhub.com/ https://www.root-me.org/
- Walk through of TrOll-1 Inspired by on the Trolling found in the OSCP exam https://highon.coffee/blog/trOll-1-walkthrough/

Another walk through for Tr0ll-1

https://null-byte.wonderhowto.com/how-to/use-nmap-7-discover-vulnerabilities-launch-dos-attacks-and-more-0168788/

Taming the troll - walkthrough

https://leonjza.github.io/blog/2014/08/15/taming-the-troll/

Troll download on Vuln Hub

https://www.vulnhub.com/entry/tr0ll-1,100/

• Sickos - Walkthrough:

https://highon.coffee/blog/sickos-1-walkthrough/

Sickos - Inspired by Labs in OSCP

https://www.vulnhub.com/series/sickos,70/

• Lord of the Root Walk Through

https://highon.coffee/blog/lord-of-the-root-walkthrough/

Lord Of The Root: 1.0.1 - Inspired by OSCP

https://www.vulnhub.com/series/lord-of-the-root,67/

• Tr0ll-2 Walk Through

https://leonjza.github.io/blog/2014/10/10/another-troll-tamed-solving-troll-2/

Tr0II-2

https://www.vulnhub.com/entry/tr0ll-2,107/

Cheat Sheets

Penetration Tools Cheat Sheet
 https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/

• Pen Testing Bookmarks https://github.com/kurobeats/pentest-bookmarks/blob/master/BookmarksList.md

OSCP Cheatsheets
 https://qithub.com/slyth11907/Cheatsheets

CEH Cheatsheet

https://scadahacker.com/library/Documents/Cheat_Sheets/Hacking%20-%20CEH%20Cheat%20Sheet%20Exercises.pdf

Net Bios Scan Cheat Sheet
 https://highon.coffee/blog/nbtscan-cheat-sheet/

• Reverse Shell Cheat Sheet https://highon.coffee/blog/reverse-shell-cheat-sheet/

• NMap Cheat Sheet https://highon.coffee/blog/nmap-cheat-sheet/

Linux Commands Cheat Sheet
 https://highon.coffee/blog/linux-commands-cheat-sheet/

Security Hardening CentO 7
 https://highon.coffee/blog/security-harden-centos-7/

MetaSploit Cheatsheet
 https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

Google Hacking Database:
 https://www.exploit-db.com/google-hacking-database/

 Windows Assembly Language Mega Primer http://www.securitytube.net/groups?operation=view&groupId=6

• Linux Assembly Language Mega Primer http://www.securitytube.net/groups?operation=view&groupId=5

Metasploit Cheat Sheet
 https://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf

• A bit dated but most is still relevant

http://hackingandsecurity.blogspot.com/2016/04/oscp-related-notes.html

- NetCat
- http://www.sans.org/security-resources/sec560/netcat_cheat_sheet_v1.pdf
- http://www.secguru.com/files/cheatsheet/nessusNMAPcheatSheet.pdf
- http://sbdtools.googlecode.com/files/hping3_cheatsheet_v1.0-ENG.pdf
- http://sbdtools.googlecode.com/files/Nmap5%20cheatsheet%20eng%20v1.pdf
- http://www.sans.org/security-resources/sec560/misc_tools_sheet_v1.pdf
- http://rmccurdy.com/scripts/Metasploit%20meterpreter%20cheat%20sheet%20reference.html
- http://h.ackack.net/cheat-sheets/netcat

Essentials

- Exploit-db
 https://www.exploit-db.com/
- SecurityFocus Vulnerability database http://www.securityfocus.com/
- Vuln Hub Vulnerable by design https://www.vulnhub.com/
- Exploit Exercises https://exploit-exercises.com/
- SecLists collection of multiple types of lists used during security assessments. List types include usernames, passwords, URLs, sensitive data grep strings, fuzzing payloads https://github.com/danielmiessler/SecLists
- Security Tube http://www.securitytube.net/
- Metasploit Unleashed free course on how to use Metasploit https://www.offensive-security.com/metasploit-unleashed/
- ODay Security Enumeration Guide http://www.0daysecurity.com/penetration-testing/enumeration.html
- Github IO Book Pen Testing Methodology
 https://monkeysm8.gitbooks.io/pentesting-methodology/

Windows Privledge Escalation

- Fuzzy Security http://www.fuzzysecurity.com/tutorials/16.html
- accesschk.exe https://technet.microsoft.com/en-us/sysinternals/bb664922
- Windows Priv Escalation For Pen Testers https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/
- Elevating Privileges to Admin and Further https://hackmag.com/security/elevating-privileges-to-administrative-and-further/