Useful OSCP Links

oscp_links.md Raw

24x7x365 SUPPORT

http://www.captiongenerator.com/320492/Offsec-Student-Admins

https://natesubra.com/go/oscp

OSCP Syllabus:

https://www.offensive-security.com/information-security-training/penetration-testing-training-kali-linux/

Windows Privilege Escalation:

http://www.fuzzysecurity.com/tutorials/16.html

https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/

http://it-ovid.blogspot.com/2012/02/windows-privilege-escalation.html

https://toshellandback.com/2015/11/24/ms-priv-esc/

Windows Post Exploitation:

http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf

Mubix: https://docs.google.com/document/d/1U10isynOpQtrIK6ChuReu-K1WHTJm4fgG3joiuz43rw/edit?hl=en_US

Linux Privilege Escalation:

https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/

https://speakerdeck.com/knaps/escape-from-shellcatraz-breaking-out-of-restricted-unix-shells

Linux Post Exploitation:

https://n0where.net/linux-post-exploitation/

Mubix: https://docs.google.com/document/d/1ObQB6hmVvRPCgPTRZM5NMH034VDM-1N-EWPRz2770K4/edit?hl=en_US#

Metasploit

https://www.offensive-security.com/metasploit-unleashed/

http://www.securitytube.net/groups?operation=view&groupId=8

Postex: https://docs.google.com/document/d/1ZrDJMQkrp_YbU_9Ni9wMNF2m3nIPEA_kekqqqA2Ywto/edit

Pivoting:

https://pentest.blog/explore-hidden-networks-with-double-pivoting/

http://nerderati.com/2011/03/17/simplify-your-life-with-an-ssh-config-file/

OSCP Reviews:

https://localhost.exposed/path-to-oscp/

http://www.en-lightn.com/?p=941

http://www.securitysift.com/offsec-pwb-oscp/

https://blog.g0tmi1k.com/2011/07/pentesting-with-backtrack-pwb/

http://www.jasonbernier.com/oscp-review/

https://n3ko1.github.io/certification/2015/05/27/oscp---offensive-security-certified-professional/

Precompiled Exploits:

https://github.com/offensive-security/exploit-database-bin-sploits

https://www.kernel-exploits.com/

MSFVenom:

http://netsec.ws/?p=331

http://www.securityunlocked.com/2016/01/02/network-security-pentesting/most-useful-msfvenom-payloads/

Shellcode:

http://www.primalsecurity.net/0x0-shellcoding-tutorial-introduction-to-asm/

https://paraschetal.in/writing-your-own-shellcode

http://althing.cs.dartmouth.edu/local/shellcode.html

https://www.exploit-db.com/docs/17065.pdf

Rev/Web Shells:

http://tools.kali.org/maintaining-access/webshells

http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet

https://github.com/stasinopoulos/commix/wiki/Upload-shells

https://highon.coffee/blog/reverse-shell-cheat-sheet/

https://github.com/JohnTroony/php-webshells

Spawn TTY Shell:

http://netsec.ws/?p=337

Tools

http://tools.kali.org/tools-listing

http://tools.kali.org/password-attacks/patator

http://tools.kali.org/web-applications/dirb

http://tools.kali.org/web-applications/dirbuster

http://tools.kali.org/web-applications/gobuster

http://tools.kali.org/web-applications/wpscan

http://tools.kali.org/web-applications/joomscan

http://tools.kali.org/vulnerability-analysis/sqlmap

http://tools.kali.org/exploitation-tools/commix

http://tools.kali.org/maintaining-access/weevely

http://tools.kali.org/password-attacks/ncrack

http://tools.kali.org/password-attacks/cewl

http://tools.kali.org/information-gathering/dotdotpwn

http://tools.kali.org/exploitation-tools/shellnoob

Wordlists

http://tools.kali.org/password-attacks/wordlists

https://github.com/danielmiessler/SecLists

https://github.com/govolution/betterdefaultpasslist

Pen Test Cheat Sheets:

https://github.com/Hack-with-Github/Awesome-Hacking

https://jivoi.github.io/2015/07/01/pentest-tips-and-tricks/

http://pwnwiki.io/

https://github.com/enaqx/awesome-pentest