OSCP Goldmine (not clickbait)

WEDNESDAY, MAY 09, 2018 - 3 MINS

OSCP PENTESTING CERTIFICATION

I ASKED HIM IF WE HAD A PROBLEM
HE SAID: "THE BUFFER IS TOO SMALL"
quickmeme.com

Introduction

Welcome to the OSCP resource gold mine. Compilation of resources I used/read/bookmarked in 2017 during the OSCP course…

Google-Fu anyone?

This was originally created on my GitBook but I decided to port it on my blog. This my way of giving back to the infosec community and I hope it can be useful to someone!

Backdoors/Web Shells

1. http://pentestmonkey.net/cheat-sheet/shells/reverse-shell-cheat-sheet
2. https://highon.coffee/blog/reverse-shell-cheat-sheet/
3. http://pentestmonkey.net/tools/web-shells/php-reverse-shell
4. http://pentestmonkey.net/tools/web-shells/perl-reverse-shell
5. https://github.com/bartblaze/PHP-backdoors
6. https://github.com/BlackArch/webshells
7. https://github.com/tennc/webshell/tree/master/php/b374k
8. https://github.com/tennc/webshell/tree/master/php/PHPshell/c99shell
9. http://www.acunetix.com/blog/articles/web-shells-101-using-php-introduction-web-shells-part-2/
10. http://securityweekly.com/2011/10/23/python-one-line-shell-code/

Buffer Overflows

1. http://www.primalsecurity.net/0x0-exploit-tutorial-buffer-overflow-vanilla-eip-overwrite-2/
2. http://proactivedefender.blogspot.ca/2013/05/understanding-buffer-overflows.html
3. http://justpentest.blogspot.ca/2015/07/minishare1.4.1-bufferoverflow.html
4. https://samsclass.info/127/proj/vuln-server.htm
5. http://www.bulbsecurity.com/finding-bad-characters-with-immunity-debugger-and-mona-py/

Information Gathering/Reconnaissance

1. LeeBaird Discover Script

2. Learning from the field - Intelligence Gathering

3. NetCraft - Information Gathering

4. The Basics Of Penetration Testing

5. Enumeration

6. Penetration Testing Framework

Cross-Compilation

1. https://arrayfire.com/cross-compile-to-windows-from-linux/

Local File Inclusion/Remote File Inclusion (LFI/RFI)

1. http://www.grobinson.me/single-line-php-script-to-gain-shell/
2. https://webshell.co/
3. https://www.insomniasec.com/downloads/publications/LFI%20With%20PHPInfo%20Assistance.pdf

4. https://osandamalith.com/2015/03/29/lfi-freak/
5. https://wiki.apache.org/httpd/DistrosDefaultLayout#Debian.2C_Ubuntu_.28Apache_httpd_2.x.29
6. https://roguecod3r.wordpress.com/2014/03/17/lfi-to-shell-exploiting-apache-access-log/
7. https://attackerkb.com/Windows/blind_files
8. https://digi.ninja/blog/when_all_you_can_do_is_read.php
9. https://updatedlinux.wordpress.com/2011/05/12/list-of-important-files-and-directories-in-linux-redhatcentosfedora/
10. https://www.idontplaydarts.com/2011/02/using-php-filter-for-local-file-inclusion/
11. https://github.com/tennc/fuzzdb/blob/master/dict/BURP-PayLoad/LFI/LFI_InterestingFiles-NullByteAdded.txt
12. http://www.r00tsec.com/2014/04/useful-list-file-for-local-file.html
13. https://www.gracefulsecurity.com/path-traversal-cheat-sheet-windows/
14. https://github.com/tennc/fuzzdb/blob/master/dict/BURP-PayLoad/LFI/LFI-FD-check.txt

File Transfer

1. https://insekurity.wordpress.com/2012/05/15/file-transfer/
2. https://www.cheatography.com/fred/cheat-sheets/file-transfers/
3. https://blog.ropnop.com/transferring-files-from-kali-to-windows/
4. https://linux.die.net/man/1/scp
5. https://www.freebsd.org/cgi/man.cgi?fetch(1)
6. https://curl.haxx.se/docs/manpage.html
7. https://linux.die.net/man/1/wget

**SCP, WGET, FTP, TFTP, CURL, NC, FETCH

Fuzzing Payloads

1. https://github.com/fuzzdb-project/fuzzdb
2. https://github.com/danielmiessler/SecLists

General Notes

1. https://bitvijays.github.io/LFC-VulnerableMachines.html
2. http://blog.knapsy.com/blog/2014/10/07/basic-shellshock-exploitation/
3. http://www.studfiles.ru/preview/2083097/page:7/
4. http://126kr.com/article/3vbt0k8fxwh
5. http://meyerweb.com/eric/tools/dencoder/
6. https://www.darkoperator.com/powershellbasics
7. https://wooly6bear.files.wordpress.com/2016/01/bwapp-tutorial.pdf
8. http://alexflor.es/security-blog/post/egress-ports/
9. https://www.exploit-db.com/papers/13017/
10. https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
11. http://explainshell.com/
12. https://pentestlab.blog/2012/11/29/bypassing-file-upload-restrictions/
13. https://github.com/g0tmi1k/mpc
14. https://www.reddit.com/r/netsecstudents/comments/5fwc1z/failed_the_oscp_any_tips_for_the_next_atter

15. https://security.stackexchange.com/questions/110673/how-to-find-windows-version-from-the-file-on-a-remote-system
16. https://www.veil-framework.com/veil-tutorial/ (AV Evasion)
17. https://blog.propriacausa.de/wp-content/uploads/2016/07/oscp_notes.html
18. https://jivoi.github.io/2015/07/01/pentest-tips-and-tricks/

Ignore SSL in python scripts : http://stackoverflow.com/questions/19268548/python-ignore-certicate-validation-urllib2

Jailed Shell Escape

1. http://netsec.ws/?p=337
2. https://pen-testing.sans.org/blog/2012/06/06/escaping-restricted-linux-shells
3. https://speakerdeck.com/knaps/escape-from-shellcatraz-breaking-out-of-restricted-unix-shells
4. http://airnesstheman.blogspot.ca/2011/05/breaking-out-of-jail-restricted-shell.html
5. http://securebean.blogspot.ca/2014/05/escaping-restricted-shell_3.html

Linux Post-Exploitation

1. https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List
2. https://github.com/huntergregal/mimipenguin
3. https://github.com/mubix/post-exploitation/wiki/Linux-Post-Exploitation-Command-List

Linux Privilege Escalation

1. https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/
2. https://www.kernel-exploits.com/
3. https://github.com/rebootuser/LinEnum
4. https://github.com/PenturaLabs/Linux_Exploit_Suggester
5. https://www.securitysift.com/download/linuxprivchecker.py
6. http://pentestmonkey.net/tools/audit/unix-privesc-check
7. https://github.com/mzet-/linux-exploit-suggester
8. http://www.darknet.org.uk/2015/06/unix-privesc-check-unixlinux-user-privilege-escalation-scanner/
9. https://www.youtube.com/watch?v=dk2wsyFiosg
10. http://resources.infosecinstitute.com/privilege-escalation-linux-live-examples/#gref
11. https://www.rebootuser.com/?p=1758

Metasploit

1. https://www.offensive-security.com/metasploit-unleashed/
2. http://www.securitytube.net/groups?operation=view&groupId=8

MSFVenom Payloads

1. http://netsec.ws/?p=331
2. https://www.offensive-security.com/metasploit-unleashed/msfvenom/
3. http://www.blackhillsinfosec.com/?p=4935

Port Scanning

1. https://highon.coffee/blog/nmap-cheat-sheet/
2. https://nmap.org/nsedoc/
3. https://github.com/superkojiman/onetwopunch
4. http://kalilinuxtutorials.com/unicornscan/

Password Cracking

1. https://uwnthesis.wordpress.com/2013/08/07/kali-how-to-crack-passwords-using-hashcat/
2. https://hashkiller.co.uk/
3. https://linuxconfig.org/password-cracking-with-john-the-ripper-on-linux
4. http://www.rarpasswordcracker.com/

Pivoting

1. https://www.offensive-security.com/metasploit-unleashed/portfwd/
2. https://www.offensive-security.com/metasploit-unleashed/proxytunnels/
3. https://github.com/rofl0r/proxychains-ng
4. https://www.sans.org/reading-room/whitepapers/testing/tunneling-pivoting-web-application-penetration-testing-36117
5. https://pentest.blog/explore-hidden-networks-with-double-pivoting/
6. https://blog.techorganic.com/2012/10/10/introduction-to-pivoting-part-2-proxychains/
7. https://www.cobaltstrike.com/help-socks-proxy-pivoting
8. https://sathisharthars.com/2014/07/07/evade-windows-firewall-by-ssh-tunneling-using-metasploit/
9. https://artkond.com/2017/03/23/pivoting-guide/

Remote Desktop Protocol (RDP)

1. https://serverfault.com/questions/148731/enabling-remote-desktop-with-command-prompt
2. https://serverfault.com/questions/200417/ideal-settings-for-rdesktop

Samba (SMB)

1. https://pen-testing.sans.org/blog/2013/07/24/plundering-windows-account-info-via-authenticated-smb-sessions
2. http://www.blackhillsinfosec.com/?p=4645

TTY Shell Spawning

1. http://netsec.ws/?p=337
2. https://github.com/infodox/python-pty-shells
3. https://blog.ropnop.com/upgrading-simple-shells-to-fully-interactive-ttys/

SQL Injection

1. http://www.sqlinjection.net/category/attacks/
2. http://sechow.com/bricks/docs/login-1.html
3. https://www.exploit-db.com/papers/12975/
4. https://websec.wordpress.com/2010/12/04/sqli-filter-evasion-cheat-sheet-mysql/
5. https://www.netsparker.com/blog/web-security/sql-injection-cheat-sheet/
6. https://github.com/cr0hn/nosqlinjection_wordlists
7. https://blog.scrt.ch/2013/03/24/mongodb-0-day-ssji-to-rce/
8. https://websec.ca/kb/sql_injection#MSSQL_Default_Databases

Vulnhub VMs

A few Vulnhub VMs. I recommend trying out a few before the exam or when your lab time expires.

Another good advice is to read/watch the walkthroughs of those machines. Try to root them yourself first!

1. Kioptrix: Level 1 (#1)
2. Kioptrix: Level 1.1 (#2)
3. Kioptrix: Level 1.2 (#3)
4. Kioptrix: Level 1.3 (#4)
5. FristiLeaks: 1.3
6. Stapler: 1
7. PwnLab: init
8. Tr0ll: 1
9. Tr0ll: 2
10. Kioptrix: 2014
11. Lord Of The Root: 1.0.1
12. Stapler: 1
13. Mr-Robot: 1
14. HackLAB: Vulnix
15. VulnOS: 2
16. SickOs: 1.2
17. pWnOS: 2.0

HackTheBox (HTB)

HTB is a penetration testing platform with many machines that feel like they belong in the OSCP labs. All you have to do is pass the registration challenge and only then, you will have your VPN access provided. I suggest doing a few as it is free and an excellent way to prepare for the exam without downloading a vulnerable VM.

Web Exploitation

1. http://www.studfiles.ru/preview/2083097/page:7/
2. http://126kr.com/article/3vbt0k8fxwh
3. http://meyerweb.com/eric/tools/dencoder/

Windows Post-Exploitation

1. https://github.com/gentilkiwi/mimikatz/releases/
2. https://github.com/gentilkiwi/mimikatz/wiki/module-~-sekurlsa
3. http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf
4. https://github.com/PowerShellMafia/PowerSploit
5. https://github.com/gentilkiwi/mimikatz/releases
6. http://www.handgrep.se/repository/cheatsheets/postexploitation/WindowsPost-Exploitation.pdf
7. https://github.com/mubix/post-exploitation/wiki/windows

Windows Privilege Escalation

1. http://www.fuzzysecurity.com/tutorials/16.html
2. https://toshellandback.com/2015/11/24/ms-priv-esc/
3. https://github.com/pentestmonkey/windows-privesc-check
4. https://blog.gdssecurity.com/labs/2014/7/11/introducing-windows-exploit-suggester.html
5. https://pentest.blog/windows-privilege-escalation-methods-for-pentesters/
6. https://github.com/foxglovesec/RottenPotato
7. http://www.exumbraops.com/penetration-testing-102-windows-privilege-escalation-cheatsheet/
8. https://www.youtube.com/watch?v=PC_iMqiuIRQ
9. https://www.youtube.com/watch?v=kMG8IsCohHA&feature=youtu.be
10. https://github.com/PowerShellMafia/PowerSploit
11. http://www.blackhillsinfosec.com/?p=5824
12. https://www.commonexploits.com/unquoted-service-paths/
13. https://github.com/abatchy17/WindowsExploits

« H1-212 CTF Write-up

0xc0ffee🇨🇦☕

Just a guy who enjoys coffee and breaking things

Tweet Share