Windows Privilege Escalation - Overview

Joas Antonio

Details

- This book aims to show the techniques of Privilege Escalation in Windows;
- It is not a practical book, just an overview with references to help you in your research;
- https://www.linkedin.com/in/joas-antonio-dos-santos

Low Hanging Passwords

- https://medium.com/hackernoon/picking-the-low-hanging-passwords-b64684fe2c7
- https://vdalabs.com/2019/10/17/password-security/

Enumeration

- https://arnavtripathy98.medium.com/smb-enumeration-for-penetration-testing-e782a328bf1b
- https://medium.com/bugbountywriteup/automating-ad-enumeration-with-frameworks-f8c7449563be
- https://medium.com/@Shorty420/enumerating-ad-98e0821c4c78
- https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1
- https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet#domain-enumeration
- https://www.ired.team/offensive-security/enumeration-and-discovery

Interesting Files and Registrys

- https://medium.com/@hakluke/sensitive-files-to-grab-in-windows-4b8f0a655f40

Important Extensions: install, backup, .bak, .log, .bat, .cmd, .vbs, .conf, .cnf, .config, .ini, .xml, .txt, .gpg, .pgp, .p12, der, id_rsa, .ovpn

Command CMD: findstr /i ovpn

- Configuration files are critical, especially for collecting default passwords
- In addition to the registry keys that often contain passwords

Password Manager Abusing

- https://posts.specterops.io/operational-guidance-for-offensive-user-dpapi-abuse-1fb7fac8b107
- https://resources.infosecinstitute.com/topic/steal-windows-login-credentials-abusing-server-message-block-smb-protocol/
- https://dl.packetstormsecurity.net/papers/general/abusing-windowsdpapi.pdf

Services Exploitation

- https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html
- https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae
- https://www.youtube.com/watch?v=zdu3f2oZZLI&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=MGqypN2uSjM&ab_channel=raulcpop
- https://pentestlab.blog/2017/03/30/weak-service-permissions/
- https://www.noobsec.net/privesc-windows/
- https://www.ired.team/offensive-security/privilege-escalation/weak-service-permissions

Kernel Exploitation

- https://github.com/SecWiki/windows-kernel-exploits
- https://kakyouim.hatenablog.com/entry/2020/05/27/010807
- https://www.hackingarticles.in/windows-kernel-exploit-privilege-escalation/
- https://pentestlab.blog/2017/04/24/windows-kernel-exploits/
- https://blog.xpnsec.com/windows-warbird-privesc/
- https://www.offensive-security.com/metasploit-unleashed/privilege-escalation/

DLL Hijacking

- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/dll-hijacking
- https://medium.com/@dannyp4p/privilege-escalation-dll-hijacking-668d7235bc98
- https://ivanitlearning.wordpress.com/2019/03/26/windows-privilege-escalation-via-dll-hijacking/
- https://pentestlab.blog/2017/03/27/dll-hijacking/
- https://www.youtube.com/watch?v=9-HNMUo9urA&ab_channel=MotasemHamdan-CyberSecurityTrainer
- https://www.youtube.com/watch?v=zvQIi2Kfk-k&ab_channel=PentesterAcademyTV

DLL Hijacking 2

- https://www.youtube.com/watch?v=e_l5TCgw3wo&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=OON0LdwCi0Q&ab_channel=PentesterAcademyTV
- https://itm4n.github.io/windows-dll-hijacking-clarified/
- https://gracefulsecurity.com/privesc-dll-hijacking/

Exploitation Path

- https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae
- https://gracefulsecurity.com/privesc-unquoted-service-path/
- https://trustfoundry.net/practical-guide-to-exploiting-the-unquoted-service-path-vulnerability-in-windows/
- https://ivanitlearning.wordpress.com/2018/12/05/windows-privilege-escalation-by-unquoted-service-paths/
- https://packetstormsecurity.com/files/157263/Microsoft-Windows-Unquoted-Service-Path-Privilege-Escalation.html

Task Scheduled

- https://www.exploit-db.com/exploits/15589
- http://remoteawesomethoughts.blogspot.com/2019/05/windows-10-task-schedulerservice.html
- https://www.youtube.com/watch?v=Kgga91U3B4s&ab_channel=SagiShahar
- https://packetstormsecurity.com/files/153698/Microsoft-Windows-Task-Scheduler-Local-Privilege-Escalation.html
- https://www.youtube.com/watch?v=GSCPiOCWzes&ab_channel=TheHackerNews
- https://www.youtube.com/watch?v=c9vQJoeJDA8&ab_channel=0patchbyACROSSecurity
- https://www.youtube.com/watch?v=gd-F1dlWBAw&ab_channel=EricRomang

UACME

- https://github.com/hfiref0x/UACME
- https://medium.com/@lucideus/privilege-escalation-on-windows-7-8-10-lucideus-research-c8a24aa55679
- https://technologyredefine.blogspot.com/2018/01/privilege-escalation.html
- https://securityonline.info/uacme-defeating-windows-user-account-control/
- https://www.youtube.com/watch?v=3BQKpPNlTSo&ab_channel=ZeroDayInitiative
- https://www.youtube.com/watch?v=C9GfMfFjhYI&ab_channel=Hak5
- https://medium.com/@mattharr0ey/privilege-escalation-uac-bypass-in-changepk-c40b92818d1b
- https://null-byte.wonderhowto.com/how-to/bypass-uac-escalate-privileges-windows-using-metasploit-0196076/
- https://github.com/yanncam/LPE_AT-UAC

UACME & GETSYSTEM

- https://docs.rapid7.com/metasploit/meterpreter-getsystem/
- https://medium.com/@cmpbilge/privilege-escalation-with-meterpreter-3e3f999d9978
- https://54m4ri74n.medium.com/windows-7-privilege-escalation-using-uac-bypass-b08f5523b7de
- https://blog.xpnsec.com/becoming-system/
- https://ivanitlearning.wordpress.com/2018/12/02/privilege-escalation-on-win-7/
- https://kellgon.com/common-privilege-escalation-vectors-for-windows-and-linux/
- https://www.youtube.com/watch?v=gdMt5G6ajx0&ab_channel=DonDoes30Official

GETSYSTEM: Leaked Handle

- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/leaked-handle-exploitation
- https://www.youtube.com/watch?v=IzZ649EvWXI&ab_channel=MeetSektor7
- http://dronesec.pw/blog/2019/08/22/exploiting-leaked-process-and-thread-handles/
- https://masthoon.github.io/exploit/2019/03/29/cygeop.html

GETSYSTEM: Named Pipes

- https://www.ired.team/offensive-security/privilege-escalation/windows-namedpipes-privilege-escalation
- https://www.exploit-db.com/exploits/22882
- https://www.elastic.co/guide/en/security/current/privilege-escalation-via-named-pipe-impersonation.html
- https://www.securityfocus.com/bid/8128/exploit

Token Abusing

- https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-abusing-tokens
- https://www.ired.team/miscellaneous-reversing-forensics/windows-kernel-internals/how-kernel-exploits-abuse-tokens-for-privilege-escalation
- https://foxglovesecurity.com/2017/08/25/abusing-token-privileges-for-windows-local-privilege-escalation/
- https://www.exploit-db.com/exploits/42556
- https://stark0de.com/2019/08/05/abuse-privilege-access-token.html
- https://attack.mitre.org/techniques/T1134/

Privilege Escalation Courses

- https://www.udemy.com/course/windows-privilege-escalation/?src=sac&kw=windows+privilege
- https://www.udemy.com/course/windows-privilege-escalation-for-beginners/?src=sac&kw=windows+privilege
- https://institute.sektor7.net/rto-lpe-windows
- https://www.udemy.com/course/advanced-windows-privilege-escalation-with-hack-the-box/?src=sac&kw=windows%20privilege

Extras

- https://github.com/TCM-Course-Resources/Windows-Privilege-Escalation-Resources
- https://www.youtube.com/watch?v=WKmbIhH9Wv8&ab_channel=MotasemHamdan-CyberSecurityTrainer
- https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md
- https://github.com/rhodejo/OSCP-Prep/blob/master/Priv-Esc.md
- https://medium.com/bugbountywriteup/privilege-escalation-in-windows-380bee3a2842
- https://www.hackingdream.net/2020/03/windows-privilege-escalation-cheatsheet-for-oscp.html
- https://github.com/frizb/Windows-Privilege-Escalation

Extras 2

- https://github.com/togie6/Windows-Privesc
- https://github.com/netbiosX/Checklists/blob/master/Windows-Privilege-Escalation.md
- https://github.com/carlospolop/winPE
- https://github.com/sagishahar/lpeworkshop
- https://www.youtube.com/watch?v=Wc7NVl-wNXI