

PenTest in Windows Server and Active Directory - Overview

Joas Antonio

Details

- O objetivo do PDF é trazer os diferentes tipos de técnicas utilizadas para comprometer um servidor Windows e um ambiente de Active Directory;
- Esse PDF é mais teórico e não contém passo a passo nem nada prático, apenas materiais de referência para auxiliar você nessa jornada;
- Meu LinkedIn: <https://www.linkedin.com/in/joas-antonio-dos-santos>
- Outros ebooks: <https://bit.ly/3n8Ghgc>

Enumeration Win and AD 1

- <https://medium.com/bugbountywriteup/automating-ad-enumeration-with-frameworks-f8c7449563be>
- <https://medium.com/@Shorty420/enumerating-ad-98e0821c4c78>
- <https://www.exploit-db.com/docs/english/46990-active-directory-enumeration-with-powershell.pdf>
- <https://github.com/CroweCybersecurity/ad-ldap-enum>
- <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/active-directory-enumeration-with-powerview>
- https://owasp.org/www-pdf-archive/OWASP_FFM_41_OffensiveActiveDirectory_101_MichaelRitter.pdf
- <https://www.trustedsec.com/blog/targeted-active-directory-host-enumeration/>
- <https://www.attackdebris.com/?p=470>

Enumeration Win and AD 2

- https://www.youtube.com/watch?v=TKXc2n9Qucc&ab_channel=PwnDefend
- https://www.youtube.com/watch?v=gl6-8AXIfL4&ab_channel=YaksasCSC
- https://www.youtube.com/watch?v=DBx-AA9nOc0&ab_channel=PentesterAcademyTV
- <https://adsecurity.org/?p=3719>
- <https://0xdarkvortex.dev/index.php/2019/01/01/active-directory-penetration-dojo-ad-environment-enumeration-1/>
- <https://www.sakshamdixit.com/powershell-enum-of-active-directory-part-1/>
- <https://derkvanderwoude.medium.com/active-directory-enumeration-detected-by-microsoft-security-solutions-9f983ab3382a>

Enumeration Win and AD 3

- <https://arnavtripathy98.medium.com/smb-enumeration-for-penetration-testing-e782a328bf1b>
- <https://www.varonis.com/blog/powershell-for-pentesters/>
- <https://www.hackercoolmagazine.com/windows-powershell-enumeration-post-exploit/>
- <https://resources.infosecinstitute.com/topic/powershell-for-pentesters-part-1-introduction-to-powershell-and-cmdlets/>
- <http://www.lifeoverpentest.com/2018/02/enumeration-cheat-sheet-for-windows.html>

Enumeration Win and AD 4

- <https://blog.fox-it.com/2018/04/26/escalating-privileges-with-acls-in-active-directory/>
- <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-acls-aces>
- <https://book.hacktricks.xyz/windows/active-directory-methodology/acl-persistence-abuse>
- <https://www.sakshamdixit.com/domain-enumeration-part-3/>
- <https://pentesttools.net/adrecon-active-directory-reconnaissance/>
- <http://thewindowsupdate.com/2019/04/17/ldap-reconnaissance-the-foundation-of-active-directory-attacks/>

Enumeration Win and AD 5

- <https://attack.stealthbits.com/ldap-reconnaissance-active-directory>
- <https://techcommunity.microsoft.com/t5/microsoft-security-and/ldap-reconnaissance-the-foundation-of-active-directory-attacks/ba-p/462973>
- <https://minutodaseguranca.blog.br/overview-para-pen-test-no-active-directory/>
- <https://github.com/sense-of-security/ADRecon>
- https://www.youtube.com/watch?v=1sN8gqDdm3k&ab_channel=Motase+mHamdan-CyberSecurityTrainer
- <https://becomepentester.gitbook.io/pentesting/active-directory-enumeration-1/active-directory-enumeration-part-1>

Enumeration Win and AD 6

- <https://adsecurity.org/?p=1508>
- <https://pentestlab.blog/2018/06/04/spn-discovery/>
- <https://stealthbits.com/blog/extracting-service-account-passwords-with-kerberoasting/>
- <https://stealthbits.com/blog/20170501discovering-service-accounts-without-using-privileges/>
- <https://pentestlab.blog/2019/09/12/microsoft-exchange-acl/>

BloodHound 1

- <https://wald0.com/?p=112>
- <https://stealthbits.com/blog/attacking-active-directory-permissions-with-bloodhound/>
- <https://mcpmag.com/articles/2019/11/13/bloodhound-active-directory-domain-admin.aspx>
- <https://www.pentestpartners.com/security-blog/bloodhound-walkthrough-a-tool-for-many-tradecrafts/>
- https://www.youtube.com/watch?v=1OSdHTvF03Y&ab_channel=Semperis

BloodHound 2

- https://www.youtube.com/watch?v=RUbADHcBLKg&ab_channel=SpecterOps
- <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/abusing-active-directory-with-bloodhound-on-kali-linux>
- <https://blog.compass-security.com/2019/12/finding-active-directory-attack-paths-using-bloodhound/>
- <https://www.microsoft.com/security/blog/2020/08/27/stopping-active-directory-attacks-and-other-post-exploitation-behavior-with-amsi-and-machine-learning/>
- <https://datacellsolutions.com/2020/11/10/active-directory-domain-enumeration-and-exploitation-using-bloodhound/>

ZeroLogon

- https://www.trendmicro.com/en_us/what-is/zerologon.html
- https://www.youtube.com/watch?v=U_1RTCl63hc&ab_channel=DanielDonda
- https://www.youtube.com/watch?v=6xMGsdD-Arl&ab_channel=TheCyberMentor
- <https://www.kroll.com/en/insights/publications/cyber/cve-2020-1472-zerologon-exploit-detection-cheat-sheet>

DCSYNC

- <https://adsecurity.org/?p=1729>
- <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/dump-password-hashes-from-domain-controller-with-dcsync>
- <https://attack.stealthbits.com/privilege-escalation-using-mimikatz-dcsync>
- <https://www.exploit-db.com/docs/48298>
- [https://www.qomplx.com/kerberos dcsync attacks explained/](https://www.qomplx.com/kerberos-dcsync-attacks-explained/)
- <https://pentestlab.blog/tag/dcsync/>

Kerberos & Golden Ticket

- <https://attack.stealthbits.com/how-golden-ticket-attack-works>
- <https://www.varonis.com/blog/kerberos-how-to-stop-golden-tickets/>
- <https://adsecurity.org/?tag=goldenticket>
- <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/kerberos-golden-tickets>
- [https://owasp.org/www-pdf-archive/OWASP Frankfurt - 44 Kerberoasting.pdf](https://owasp.org/www-pdf-archive/OWASP_Frankfurt_-_44_Kerberoasting.pdf)

Kerberos

- <https://periciacomputacional.com/exploiting-smb-and-kerberos-to-obtain-administrator-access/>
- <https://m0chan.github.io/2019/07/31/How-To-Attack-Kerberos-101.html>
- <https://www.zdnet.com/article/proof-of-concept-exploit-code-published-for-new-kerberos-bronze-bit-attack/>
- https://www.youtube.com/watch?v=ErWhWBdDwTU&ab_channel=MotasemHamdan-CyberSecurityTrainer
- https://www.youtube.com/watch?v=JklA7eWeVoY&ab_channel=AnkitJoshi

PenTest AD

- <https://medium.com/@daniela.mh20/attaktive-directory-thm-walkthrough-9a7f0c7cc925>
- <https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection.pdf>
- <https://www.blackhat.com/docs/eu-17/materials/eu-17-Thompson-Red-Team-Techniques-For-Evading-Bypassing-And-Disabling-MS-Advanced-Threat-Protection-And-Advanced-Threat-Analytics.pdf>
- <https://i.blackhat.com/USA-20/Thursday/us-20-Bienstock-My-Cloud-Is-APTs-Cloud-Investigating-And-Defending-Office-365.pdf>
- <https://www.blackhat.com/docs/us-15/materials/us-15-Metcalf-Red-Vs-Blue-Modern-Active-Directory-Attacks-Detection-And-Protection-wp.pdf>
- <https://i.blackhat.com/eu-19/Wednesday/eu-19-Lagadec-Advanced-VBA-Macros-Attack-And-Defence-2.pdf>
- <https://www.blackhat.com/docs/webcast/05172018-BlackHat-Active-Directory-Delegation-Dissected.pdf>

PenTest AD 2

- <https://github.com/balaasif6789/AD-Pentesting>
- <https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet>
- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Active%20Directory%20Attack.md>
- [https://github.com/SofianeHamlaoui/Pentest-Notes/blob/master/Security cheatsheets/windows/active-directory.md](https://github.com/SofianeHamlaoui/Pentest-Notes/blob/master/Security%20cheatsheets/windows/active-directory.md)
- <https://github.com/initstring/pentest-methodology/blob/master/internal-ad.md>
- <https://github.com/browninfosecguy/ADLab>
- <https://github.com/R3dy/capsulecorp-pentest/blob/master/README.md>
- <https://github.com/Twi1ight/AD-Pentest-Script>

WSUS PenTest

- <https://www.gosecure.net/blog/2020/09/03/wsus-attacks-part-1-introducing-pywsus/>
- <https://pentestit.com/wsuxploit-weaponized-wsus-exploit-script/>
- <https://www.contextis.com/en/blog/securing-against-wsus-attacks>
- <https://github.com/AlsidOfficial/WSUSpendu>
- <https://resources.infosecinstitute.com/topic/targeting-wsus-server/>
- <https://medium.com/@bazyli.michal/more-than-a-penetration-test-cve-2019-1082-647ba2e59034>

Privilege Escalation

- <https://book.hacktricks.xyz/windows/windows-local-privilege-escalation>
- <https://medium.com/bugbountywriteup/privilege-escalation-in-windows-380bee3a2842>
- <https://medium.com/@SumitVerma101/windows-privilege-escalation-part-1-unquoted-service-path-c7a011a8d8ae#:~:text=When%20a%20service%20is%20created,of%20the%20time%20it%20is>
- https://medium.com/@orhan_yildirim/windows-privilege-escalation-unquoted-service-paths-61d19a9a1a6a

Privilege Escalation 2

- <https://www.ired.team/offensive-security/privilege-escalation/unquoted-service-paths>
- <https://pentestlab.blog/2017/03/09/unquoted-service-path/>
- <https://gracefulsecurity.com/privesc-insecure-service-permissions/>
- <https://medium.com/@shy327o/windows-privilege-escalation-insecure-service-1-ec4c428e4800>
- <https://itm4n.github.io/windows-registry-rpceptmapper-eop/>
- <https://labs.f-secure.com/assets/BlogFiles/mwri-windows-services-all-roads-lead-to-system-whitepaper.pdf>

Privilege Escalation 3

- <https://sec-consult.com/blog/detail/windows-privilege-escalation-an-approach-for-penetration-testers/>
- <https://medium.com/@anastasisvasileiadis/windows-privilege-escalation-alwaysinstallelevated-641e660b54bd>
- <https://www.hackingarticles.in/windows-privilege-escalation-alwaysinstallelevated/>
- <https://pentestlab.blog/2017/02/28/always-install-elevated/>
- https://www.rapid7.com/db/modules/exploit/windows/local/always_install_elevated/

Privilege Escalation 4

- <https://medium.com/techzap/dll-hijacking-part-1-basics-b6dfb8260cf1>
- <https://www.ibliss.com.br/dll-hijacking-exploracao/>
- <https://pentestlab.blog/2017/03/27/dll-hijacking/>
- <https://www.cyberark.com/resources/threat-research-blog/dllspy-tighten-your-defense-by-discovering-dll-hijacking-easily>
- <https://itm4n.github.io/windows-dll-hijacking-clarified/>
- <https://medium.com/@dannyp4p/privilege-escalation-dll-hijacking-668d7235bc98>
- <https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/dll-hijacking>

Privilege Escalation 5

- <https://ivanitlearning.wordpress.com/2019/03/26/windows-privilege-escalation-via-dll-hijacking/>
- <https://www.ired.team/offensive-security/privilege-escalation/t1038-dll-hijacking>
- https://www.youtube.com/watch?v=e_I5TCgw3wo&ab_channel=PentesterAcademyTV
- https://www.youtube.com/watch?v=9-HNMUo9urA&ab_channel=MotasemHamdan-CyberSecurityTrainer
- <https://www.ired.team/miscellaneous-reversing-forensics/windows-kernel-internals/how-kernel-exploits-abuse-tokens-for-privilege-escalation>
- <https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-abusing-tokens>
- <https://lifars.com/2018/10/privilege-escalation-on-windows-abusing-tokens/>

Privilege Escalation 6

- <https://medium.com/@shadowslayerqwerty/windows-token-based-privilege-escalation-8f282f722e03>
- <https://medium.com/palantir/windows-privilege-abuse-auditing-detection-and-defense-3078a403d74e>
- <https://www.cynet.com/network-attacks/privilege-escalation/>
- <https://www.ired.team/offensive-security/privilege-escalation/>
- <https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS>
- <https://lolbas-project.github.io/>
- <https://pentestlab.blog/2017/03/31/insecure-registry-permissions/>

Privilege Escalation 7

- <https://blueteamdope.gitbook.io/penetration-testing-playbook/privilege-escalation/windows-privilege-escalation>
- <https://github.com/frizb/Windows-Privilege-Escalation>
- <https://github.com/carlospolop/winPE>
- <https://github.com/togie6/Windows-Privesc>
- <https://github.com/netbiosX/Checklists/blob/master/Windows-Privilege-Escalation.md>
- <https://github.com/TCM-Course-Resources/Windows-Privilege-Escalation-Resources>
- <https://github.com/M4ximuss/Powerless>
- <https://github.com/antonioCoco/RogueWinRM>
- <https://cd6629.gitbook.io/oscp-notes/windows-privesc/windows-privesc-arena-wlk>
- <https://github.com/rhodejo/OSCP-Prep/blob/master/Priv-Esc.md>

Privilege Escalation 8

- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Windows%20-%20Privilege%20Escalation.md>
- <https://www.fuzzysecurity.com/tutorials/16.html>
- https://sushant747.gitbooks.io/total-oscp-guide/content/privilege_escalation_windows.html
- <https://sec-consult.com/blog/detail/windows-privilege-escalation-an-approach-for-penetration-testers/>

C2 and C3

- <https://howto.thec2matrix.com/>
- <https://akijosberryblog.wordpress.com/2018/03/17/active-directory-as-a-c2-command-control/>
- <https://www.harmj0y.net/blog/powershell/command-and-control-using-active-directory/>
- <https://www.hackingloops.com/c2/>
- <https://www.blackhillsinfosec.com/c2-c3-whatever-it-takes/>
- <https://securityonline.info/spray-ad-a-cobalt-strike-tool-to-audit-active-directory-user-accounts/>
- <https://blog.cobaltstrike.com/2015/09/30/advanced-threat-tactics-course-and-notes/>
- <https://medium.com/@ivecodoe/detecting-ldapfragger-a-newly-released-cobalt-strike-beacon-using-ldap-for-c2-communication-c274a7f00961>
- <https://www.ired.team/offensive-security/red-team-infrastructure/cobalt-strike-101-installation-and-interesting-commands>
- <https://github.com/FSecureLABS/C3>
- <https://0x1.gitlab.io/exploitation-tools/C3/>

C2 and C3 - 2

- <https://mohad.red/Integrating-C3-With-Cobalt-Strike/>
- <https://www.mdsec.co.uk/2019/02/external-c2-ie-com-objects-and-how-to-use-them-for-command-and-control/>
- <https://stealthbits.com/blog/next-gen-open-source-c2-frameworks/>
- <https://fatrodzianko.com/2019/08/14/getting-started-with-covenant-c2/>
- https://www.youtube.com/watch?v=gbX0A1mx6no&ab_channel=Defsecone

Lateral Movement

- <https://www.hackingarticles.in/lateral-movement-over-pass-the-hash/>
- <https://attack.mitre.org/techniques/T1550/002/>
- <https://www.varonis.com/blog/penetration-testing-explained-part-vi-passing-the-hash/>
- <https://logrhythm.com/blog/detecting-lateral-movement-from-pass-the-hash-attacks/>
- <https://dmcxblue.gitbook.io/red-team-notes/lateral-movement/pass-the-hash>
- <https://www.hackingarticles.in/lateral-movement-pass-the-ticket-attack/>

Lateral Movement 2

- <https://resources.infosecinstitute.com/topic/pass-hash-pass-ticket-no-pain/>
- <https://bouj33boy.com/lateral-movement-without-lsass/>
- <https://redcanary.com/blog/lateral-movement-and-cryptomining/>
- <https://hackmag.com/security/lateral-movement/>
- <https://medium.com/attivotechblogs/lateral-movement-using-smb-session-enumeration-f4b1b17b6ee8>
- <https://www.ired.team/offensive-security/lateral-movement/lateral-movement-with-psexec>
- <https://redcanary.com/blog/threat-hunting-psexec-lateral-movement/>
- <https://www.mindpointgroup.com/blog/lateral-movement-with-psexec/>

Lateral Movement 3

- <https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f>
- <https://logrhythm.com/blog/what-is-lateral-movement-and-how-to-detect-it/>
- <https://pentestlab.blog/2020/07/21/lateral-movement-services/>
- <https://medium.com/redteam-blueteam-series/lateral-movement-702e5b2a5177>
- <https://www.blackhat.com/docs/us-15/materials/us-15-Graeber-Abusing-Windows-Management-Instrumentation-WMI-To-Build-A-Persistent%20Asynchronous-And-Fileless-Backdoor-wp.pdf>

Lateral Movement 4

- <https://github.com/Mr-Un1k0d3r/SCShell>
- <https://github.com/JPCERTCC/DetectLM>
- <https://github.com/codewhitesec/LethalHTA>
- <https://github.com/0xthirteen/MoveKit>
- <https://github.com/CompassSecurity/Readinizer>
- https://github.com/rmusser01/Infosec_Reference/blob/master/Draft/ATT%26CK-Stuff/ATT%26CK/Lateral%20Movement.md
- <https://riccardoancarani.github.io/2019-10-04-lateral-movement-megaprimer/>

Powershell PenTest

- <https://www.optiv.com/explore-optiv-insights/blog/unmanaged-powershell-binaries-and-endpoint-protection>
- <https://github.com/leechristensen/UnmanagedPowerShell>
- <https://www.youtube.com/watch?v=7tvfb9poTKg>
- <https://periciacomputacional.com/pentesting-with-powershell-in-six-steps/>
- <https://book.hacktricks.xyz/windows/basic-powershell-for-pentesters>
- <https://www.varonis.com/blog/powershell-for-pentesters/>
- <https://resources.infosecinstitute.com/topic/powershell-for-pentesters-part-1-introduction-to-powershell-and-cmdlets/>
- <https://medium.com/@akash.sarode1234/pentesting-with-powershell-5918dfcd0eb4>

LLMNR POISONING

- <https://medium.com/coreshield/research-llmnr-e-nbt-ns-poisoning-attack-ad58c039b97e>
- <https://medium.com/@subhammisra45/llmnr-poisoning-and-relay-5477949b7bef>
- <https://attack.mitre.org/techniques/T1557/001/>
- <https://www.aprive.co.uk/blog/llmnr-nbt-ns-spoofing/>
- <https://www.sternsecurity.com/blog/local-network-attacks-llmnr-and-nbt-ns-poisoning/>
- <https://dmcxblue.gitbook.io/red-team-notes/untitled-1/llmnr-nbt-ns-poisoning-and-relay>

LDAP RELAY

- <https://www.youtube.com/watch?v=pKt9IJJOM3I>
- <https://dirkjanm.io/exploiting-CVE-2019-1040-relay-vulnerabilities-for-rce-and-domain-admin/>
- <https://www.praetorian.com/blog/obtaining-laps-passwords-through-ldap-relaying-attacks>

Persistence AD

- <https://bohops.com/2018/03/26/diskshadow-the-return-of-vss-evasion-persistence-and-active-directory-database-extraction/>
- <https://pentestlab.blog/2019/11/04/persistence-scheduled-tasks/>
- <https://www.ired.team/offensive-security/persistence/t1053-schtask>
- <https://isc.sans.edu/forums/diary/Adding+Persistence+Via+Schedule+Tasks/23633/>
- <https://attack.mitre.org/techniques/T1053/005/>
- <https://attack.mitre.org/techniques/T1053/>
- <https://adsecurity.org/?p=1929>

Persistence AD 2

- <https://adsecurity.org/?tag=ad-sneaky-persistence>
- <https://attack.stealthbits.com/adminsdholder-modification-ad-persistence>
- <https://www.ired.team/offensive-security-experiments/active-directory-kerberos-abuse/how-to-abuse-and-backdoor-adminsdholder-to-obtain-domain-admin-persistence>
- https://www.youtube.com/watch?v=9ZYsVI5Xmrg&ab_channel=RaphaelMudge
- <https://ijustwannared.team/2019/03/11/browser-pivot-for-chrome/>
- <https://lsdsecurity.com/2020/02/lateral-movement-in-active-directorywindows-some-simple-forgotten-yet-effective-ad-pivoting-techniques-part-1/>
- <https://attack.mitre.org/techniques/T1185/>

Persistence AD 3

- <https://bohops.com/2018/04/28/abusing-dcom-for-yet-another-lateral-movement-technique/>
- https://pt.slideshare.net/nikhil_mittal/race-minimal-rights-and-ace-for-active-directory-dominance
- <https://www.ired.team/offensive-security/lateral-movement/t1175-distributed-component-object-model>
- <https://adsecurity.org/?p=1785>
- <https://adsecurity.org/?tag=winrm>
- <https://pentestlab.blog/2018/05/15/lateral-movement-winrm/>
- <https://resources.infosecinstitute.com/topic/active-directory-walkthrough-series-golden-ticket/>
- <https://github.com/Hackplayers/evil-winrm>

Pivoting

- <https://ijustwannared.team/2019/11/07/c2-over-rdp-virtual-channels/>
- <https://github.com/shunf4/proxychains-windows>
- <https://blog.techorganic.com/2012/10/10/introduction-to-pivoting-part-2-proxychains/>
- <https://www.voidwarranties.tech/posts/pentesting-tuts/pivoting/proxychains/>
- <https://github.com/klsecservices/rpivot>
- <https://securityonline.info/rpivot-socks4-reverse-proxy/>

Pivoting 2

- <https://nagarrosecurity.com/blog/smb-named-pipe-pivoting-meterpreter>
- <https://medium.com/@petergombos/smb-named-pipe-pivoting-in-meterpreter-462580fd41c5>
- <https://blog.cobaltstrike.com/2015/10/07/named-pipe-pivoting/>
- <https://www.bordergate.co.uk/lateral-movement-with-named-pipes/>
- https://rhq.reconinfosec.com/tactics/lateral_movement/
- <https://github.com/mis-team/rsockspipe>
- <https://www.youtube.com/watch?v=lelRK-SDubc>
- <https://github.com/blackarrowsec/mssqlproxy>

LAB AD

- <https://medium.com/@browninfosecguy/active-directory-lab-for-penetration-testing-5d7ac393c0c4>
- <https://www.hebunilhanli.com/wonderland/ad-pentest/ad-pentest-lab-setup/>
- https://www.youtube.com/watch?v=xftEuVQ7kY0&ab_channel=TheCyberMentor
- <https://1337red.wordpress.com/building-and-attacking-an-active-directory-lab-with-powershell/>
- <https://forum.hackthebox.eu/discussion/2996/building-an-active-directory-pen-test-lab>

TTPs (Mitre)

- <https://attack.mitre.org/techniques/T1087/>
- <https://attack.mitre.org/techniques/T1482/>
- <https://attack.mitre.org/techniques/T1087/002/>
- <https://attack.mitre.org/techniques/T1018/>
- <https://redcanary.com/threat-detection-report/techniques/domain-trust-discovery/>
- <https://attack.mitre.org/techniques/T1574/001/>
- <https://attack.mitre.org/techniques/T1003/006/>
- <https://www.corelight.com/mitre-attack/c2/t1094-custom-command-and-control-protocol/>
- <https://attack.mitre.org/tactics/TA0011/>
- <https://attack.mitre.org/techniques/T1095/>
- <https://attack.mitre.org/techniques/T1550/003/>

Cheatsheet

- <https://github.com/Kitsun3Sec/Pentest-Cheat-Sheets>
- <https://github.com/S1ckB0y1337/Active-Directory-Exploitation-Cheat-Sheet>
- <https://www.ired.team/offensive-security-experiments/offensive-security-cheatsheets>
- <https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/>
- <https://pentest.tonyng.net/windows-privilege-escalation-a-cheatsheet/>
- <https://ceso.github.io/posts/2020/04/hacking/oscp-cheatsheet/>
- <https://github.com/Integration-IT/Active-Directory-Exploitation-Cheat-Sheet>
- <https://book.hacktricks.xyz/windows/active-directory-methodology>

PENTEST COM POWERSHELL – OVERVIEW

JOAS ANTONIO

SOBRE

- APRESENTAR MATERIAIS DE ESTUDOS PARA SE APROFUNDAR NO TEMA;
- CONCEITOS BÁSICOS DE POWERSHELL;
- AUXILIAR EM SEUS PENTESTS COM FOCO EM INFRAESTRUTURA WINDOWS;

AUTOR

- JOAS ANTONIO DOS SANTOS;
- ENTUSIASTA EM SEGURANÇA DA INFORMAÇÃO;
- [HTTPS://WWW.LINKEDIN.COM/IN/JOAS-ANTONIO-DOS-SANTOS/](https://www.linkedin.com/in/joas-antonio-dos-santos/)

CONCEITOS DE POWERSHELL

O QUE É POWERSHELL

- O POWERSHELL É UMA ESTRUTURA MULTIPLATAFORMA DE GERENCIAMENTO DE CONFIGURAÇÃO E DE AUTOMAÇÃO DE TAREFAS, QUE CONSISTE EM UM SHELL DE LINHA DE COMANDO E EM UMA LINGUAGEM DE SCRIPT. AO CONTRÁRIO DA MAIORIA DOS SHELLS, QUE ACEITAM E RETORNAM TEXTO, O POWERSHELL É CRIADO COM BASE NO CLR (COMMON LANGUAGE RUNTIME) DO .NET E ACEITA E RETORNA OBJETOS .NET. ESSA MUDANÇA FUNDAMENTAL TRAZ FERRAMENTAS E MÉTODOS TOTALMENTE NOVOS PARA A AUTOMAÇÃO.

O QUE É POWERSHELL

- AO CONTRÁRIO DE INTERFACES DE LINHA DE COMANDO TRADICIONAIS, OS CMDLETS DO POWERSHELL SÃO PROJETADOS PARA LIDAR COM OBJETOS. UM OBJETO REPRESENTA INFORMAÇÕES ESTRUTURADAS QUE VÃO ALÉM DA UMA CADEIA DE CARACTERES EXIBIDA NA TELA. A SAÍDA DO COMANDO SEMPRE ACOMPANHA INFORMAÇÕES EXTRAS QUE PODERÃO SER USADAS QUANDO NECESSÁRIO.
- SE VOCÊ JÁ USOU FERRAMENTAS DE PROCESSAMENTO DE TEXTO PARA PROCESSAR DADOS, PERCEBERÁ QUE ELAS SE COMPORTAM DE MANEIRA DIFERENTE QUANDO USADAS NO POWERSHELL. NA MAIORIA DOS CASOS, VOCÊ NÃO PRECISA DE FERRAMENTAS DE PROCESSAMENTO DE TEXTO PARA EXTRAIR INFORMAÇÕES ESPECÍFICAS. VOCÊ ACESSA DIRETAMENTE PARTES DOS DADOS USANDO A SINTAXE DE OBJETO PADRÃO DO POWERSHELL.

O QUE É POWERSHELL

- AO CONTRÁRIO DE INTERFACES DE LINHA DE COMANDO TRADICIONAIS, OS CMDLETS DO POWERSHELL SÃO PROJETADOS PARA LIDAR COM OBJETOS. UM OBJETO REPRESENTA INFORMAÇÕES ESTRUTURADAS QUE VÃO ALÉM DA UMA CADEIA DE CARACTERES EXIBIDA NA TELA. A SAÍDA DO COMANDO SEMPRE ACOMPANHA INFORMAÇÕES EXTRAS QUE PODERÃO SER USADAS QUANDO NECESSÁRIO.
- SE VOCÊ JÁ USOU FERRAMENTAS DE PROCESSAMENTO DE TEXTO PARA PROCESSAR DADOS, PERCEBERÁ QUE ELAS SE COMPORTAM DE MANEIRA DIFERENTE QUANDO USADAS NO POWERSHELL. NA MAIORIA DOS CASOS, VOCÊ NÃO PRECISA DE FERRAMENTAS DE PROCESSAMENTO DE TEXTO PARA EXTRAIR INFORMAÇÕES ESPECÍFICAS. VOCÊ ACESSA DIRETAMENTE PARTES DOS DADOS USANDO A SINTAXE DE OBJETO PADRÃO DO POWERSHELL.

O QUE É POWERSHELL

- INTERFACES COMO A DO CMD.EXE NÃO FORNECEM UMA FORMA DE ESTENDER DIRETAMENTE O CONJUNTO DE COMANDOS INTERNOS. VOCÊ PODE CRIAR FERRAMENTAS DE LINHA DE COMANDO EXTERNAS QUE SÃO EXECUTADAS NO CMD.EXE. MAS ESSAS FERRAMENTAS EXTERNAS NÃO TÊM SERVIÇOS, COMO A INTEGRAÇÃO COM A AJUDA. O CMD.EXE NÃO SABE AUTOMATICAMENTE QUE ESSAS FERRAMENTAS EXTERNAS SÃO COMANDOS VÁLIDOS.
- OS COMANDOS NO POWERSHELL SÃO CONHECIDOS COMO CMDLETS. VOCÊ PODE USAR CADA CMDLET SEPARADAMENTE, MAS O POTENCIAL DELES É ATINGIDO QUANDO VOCÊ OS COMBINA PARA EXECUTAR TAREFAS COMPLEXAS. COMO MUITOS SHELLS, O POWERSHELL FORNECE ACESSO AO SISTEMA DE ARQUIVOS NO COMPUTADOR. OS PROVEDORES DO POWERSHELL PERMITEM QUE VOCÊ ACESSE OUTROS ARMAZENAMENTOS DE DADOS, COMO O REGISTRO E OS REPOSITÓRIOS DE CERTIFICADOS, COM TANTA FACILIDADE QUANTO O SISTEMA DE ARQUIVOS.
- VOCÊ PODE CRIAR MÓDULOS DE CMDLET E DE FUNÇÃO USANDO CÓDIGO COMPILADO OU SCRIPTS. OS MÓDULOS PODEM ADICIONAR CMDLETS E PROVEDORES AO SHELL. O POWERSHELL TAMBÉM DÁ SUPORTE A SCRIPTS QUE SÃO ANÁLOGOS AOS SCRIPTS DE SHELL DO UNIX E AOS ARQUIVOS EM LOTES DO CMD.EXE.

O QUE É POWERSHELL

- QUANDO VOCÊ DIGITA UM COMANDO, O POWERSHELL SEMPRE PROCESSA A LINHA DE COMANDO DE ENTRADA DIRETAMENTE. O POWERSHELL TAMBÉM FORMATA A SAÍDA EXIBIDA NA TELA. ESSA DIFERENÇA É CONSIDERÁVEL PORQUE REDUZ O TRABALHO NECESSÁRIO EM CADA CMDLET. ISSO GARANTE QUE VOCÊ POSSA FAZER AS COISAS SEMPRE DA MESMA MANEIRA COM QUALQUER CMDLET. OS DESENVOLVEDORES DE CMDLET NÃO PRECISAM ESCREVER CÓDIGOS PARA ANALISAR OS ARGUMENTOS DE LINHA DE COMANDO OU FORMATAR A SAÍDA.
- FERRAMENTAS DE LINHA DE COMANDO TRADICIONAIS TÊM SEUS PRÓPRIOS ESQUEMAS PARA SOLICITAR E EXIBIR A AJUDA. ALGUMAS FERRAMENTAS DE LINHA DE COMANDO USAM /? PARA DISPARAR A EXIBIÇÃO DA AJUDA; OUTRAS USAM -?, /H OU ATÉ MESMO //. ALGUMAS DELAS EXIBEM A AJUDA EM UMA JANELA GUI EM VEZ DE NA EXIBIÇÃO DO CONSOLE. SE VOCÊ USAR O PARÂMETRO ERRADO, A FERRAMENTA PODERÁ IGNORAR O QUE VOCÊ DIGITOU E COMEÇAR A EXECUTAR UMA TAREFA AUTOMATICAMENTE. COMO O POWERSHELL ANALISA E PROCESSA A LINHA DE COMANDO AUTOMATICAMENTE, O PARÂMETRO -? SEMPRE SIGNIFICA "MOSTRE-ME A AJUDA PARA ESTE COMANDO". INTERFACES COMO A DO CMD.EXE NÃO FORNECEM UMA FORMA DE ESTENDER DIRETAMENTE O CONJUNTO DE COMANDOS INTERNOS. VOCÊ PODE CRIAR FERRAMENTAS DE LINHA DE COMANDO EXTERNAS QUE SÃO EXECUTADAS NO CMD.EXE. MAS ESSAS FERRAMENTAS EXTERNAS NÃO TÊM SERVIÇOS, COMO A INTEGRAÇÃO COM A AJUDA. O CMD.EXE NÃO SABE AUTOMATICAMENTE QUE ESSAS FERRAMENTAS EXTERNAS SÃO COMANDOS VÁLIDOS.
- OS COMANDOS NO POWERSHELL SÃO CONHECIDOS COMO CMDLETS. VOCÊ PODE USAR CADA CMDLET SEPARADAMENTE, MAS O POTENCIAL DELES É ATINGIDO QUANDO VOCÊ OS COMBINA PARA EXECUTAR TAREFAS COMPLEXAS. COMO MUITOS SHELLS, O POWERSHELL FORNECE ACESSO AO SISTEMA DE ARQUIVOS NO COMPUTADOR. OS PROVEDORES DO POWERSHELL PERMITEM QUE VOCÊ ACESSE OUTROS ARMAZENAMENTOS DE DADOS, COMO O REGISTRO E OS REPOSITÓRIOS DE CERTIFICADOS, COM TANTA FACILIDADE QUANTO O SISTEMA DE ARQUIVOS.
- VOCÊ PODE CRIAR MÓDULOS DE CMDLET E DE FUNÇÃO USANDO CÓDIGO COMPILADO OU SCRIPTS. OS MÓDULOS PODEM ADICIONAR CMDLETS E PROVEDORES AO SHELL. O POWERSHELL TAMBÉM DÁ SUPORTE A SCRIPTS QUE SÃO ANÁLOGOS AOS SCRIPTS DE SHELL DO UNIX E AOS ARQUIVOS EM LOTES DO CMD.EXE.

MATERIAIS INTRODUTÓRIOS

- [HTTPS://LEANPUB.COM/POWERSHELL101](https://leanpub.com/powershell101)
- [HTTPS://DOCS.MICROSOFT.COM/PT-BR/POWERSHELL/SCRIPTING/LEARN/PS101/01-GETTING-STARTED?VIEW=POWERSHELL-7](https://docs.microsoft.com/pt-br/powershell/scripting/learn/ps101/01-getting-started?view=powershell-7)
- [HTTPS://WWW.COMPARITECH.COM/NET-ADMIN/POWERSHELL-CHEAT-SHEET/](https://www.comparitech.com/net-admin/powershell-cheat-sheet/)
- [HTTP://RAMBLINGCOOKIEMONSTER.GITHUB.IO/IMAGES/CHEAT-SHEETS/POWERSHELL-BASIC-CHEAT-SHEET2.PDF](http://ramblingcookiemonster.github.io/images/cheat-sheets/powershell-basic-cheat-sheet2.pdf)
- [HTTPS://GIST.GITHUB.COM/PCGEEK86/336E08D1A09E3DD1A8F0A30A9FE61C8A](https://gist.github.com/PCGEEK86/336e08d1a09e3dd1a8f0a30a9fe61c8a)
- [HTTPS://GITHUB.COM/LAZYWINADMIN/POWERShell](https://github.com/LazyWinAdmin/PowerShell) (SCRIPTS)
- [HTTPS://GITHUB.COM/CLYMB3R/POWERShell](https://github.com/CLYMB3R/PowerShell)
- [HTTPS://DOCS.MICROSOFT.COM/PT-BR/POWERSHELL/SCRIPTING/SAMPLES/SAMPLE-SCRIPTS-FOR-ADMINISTRATION?VIEW=POWERSHELL-7](https://docs.microsoft.com/pt-br/powershell/scripting/samples/sample-scripts-for-administration?view=powershell-7)
- [HTTPS://WWW.UDEMY.COM/COURSE/APRENDA-POWERSHELL-DO-ZERO/](https://www.udemy.com/course/aprenda-powershell-do-zero/)
- [HTTPS://WWW.UDEMY.COM/COURSE/AUTOMATIZANDO-ADMINISTRACAO-COM-POWERSHELL-CURSO-10961/](https://www.udemy.com/course/automatizando-administracao-com-powershell-curso-10961/)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=XODfGoJFR9Q](https://www.youtube.com/watch?v=xOdfGoJFR9Q)

INTRODUÇÃO AO PENTEST COM POWERSHELL

PENTEST COM POWERSHELL

- A UTILIDADE DO POWERSHELL VAI ALÉM EM APENAS ADMINISTRAR UM SISTEMA OPERACIONAL, DEPENDENDO DO CASO, ELE PODE SER UTILIZADO PARA EXECUTAR GRANDES AÇÕES MALICIOSA;
- MUITOS ATAQUES QUE PARTEM DE AMEAÇAS AVANÇADAS, USAM TÉCNICAS DE COMPROMETIMENTO VIA POWERSHELL PARA ALCANÇAR UMA SHELL, ESCALAR PRIVILÉGIOS, REALIZAR UM PIVOTING, EXFILTRAR DADOS OU ATÉ MESMO PARA EXECUTAR MALWARES E FAZER DO SEU ALVO UMA BOTNET;

TÉCNICAS DE ENUMERAÇÃO, RECON E SCANNING

- [HTTPS://MEDIUM.COM/@NALLAMUTHU/POWERSHELL-PORT-SCAN-BF27FC754585](https://medium.com/@nallamuthu/powershell-port-scan-bf27fc754585)
- [HTTPS://SID-500.COM/2017/11/12/TEST-PORT-USE-POWERSHELL-AS-A-PORT-SCANNER/](https://sid-500.com/2017/11/12/test-port-use-powershell-as-a-port-scanner/)
- [HTTPS://TECHCOMMUNITY.MICROSOFT.COM/T5/ITOPS-TALK-BLOG/POWERSHELL-BASICS-HOW-TO-SCAN-OPEN-PORTS-WITHIN-A-NETWORK/BA-P/924149](https://techcommunity.microsoft.com/t5/itops-talk-blog/powershell-basics-how-to-scan-open-ports-within-a-network/ba-p/924149)
- [HTTPS://GITHUB.COM/BORNTOBEROOT/POWERSHELL_IPv4PORTSCANNER](https://github.com/BORNTOBEROOT/POWERSHELL_IPv4PORTSCANNER)
- [HTTP://5UBTOOLS.BLOGSPOT.COM/](http://5ubtools.blogspot.com/)
- [HTTPS://GITHUB.COM/Z3R0TH-13/ENUM](https://github.com/Z3R0TH-13/ENUM)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=QKZSiBeKAC0&AB_CHANNEL=TECHSNIPS](https://www.youtube.com/watch?v=QKZSiBeKAC0&ab_channel=TechSnips)
- [HTTPS://GITHUB.COM/PYROTEK3/POWERSHELL-AD-RECON](https://github.com/PyroTek3/POWERSHELL-AD-RECON)
- [HTTPS://BLOG.STEALTHBITS.COM/PERFORMING-DOMAIN-RECONNAISSANCE-USING-POWERSHELL/](https://blog.stealthbits.com/performing-domain-reconnaissance-using-powershell/)
- [HTTPS://MEDIUM.COM/@SMURF3R5/RECON-DOMAIN-SHARES-872914697980](https://medium.com/@smurf3r5/recon-domain-shares-872914697980)
- [HTTPS://WWW.TRUSTEDSEC.COM/BLOG/POWERSHELL-RECONNAISSANCE/](https://www.trustedsec.com/blog/powershell-reconnaissance/)
- [HTTPS://WWW.HEBUNILHANLI.COM/WONDERLAND/AD-PENTEST/RECON-WITH-POWERSHELL/](https://www.hebunilhanli.com/wonderland/ad-pentest/recon-with-powershell/)
- [HTTPS://PERICIACOMPUTACIONAL.COM/PENTESTING-WITH-POWERSHELL-IN-SIX-STEPS/](https://periciacomputacional.com/pentesting-with-powershell-in-six-steps/)
- [HTTPS://GITHUB.COM/ELITELOSER/PSNMAP](https://github.com/ELITELOSER/PSNMAP)

TÉCNICAS DE ENUMERAÇÃO, RECON E SCANNING

- [HTTPS://MEDIUM.COM/@DRAGON/SOME-USEFUL-INTERESTING-POWERSHELL-SCRIPTS-9B9490CEE0CD](https://medium.com/@dragon/some-useful-interesting-powershell-scripts-9b9490cee0cd)
- [HTTPS://ADSECURITY.ORG/?P=2535](https://adsecurity.org/?p=2535)
- [HTTPS://WWW.VARONIS.COM/BLOG/POWVIEW-FOR-PENETRATION-TESTING/](https://www.varonis.com/blog/powerview-for-penetration-testing/)
- [HTTPS://WWW.SANS.ORG/BLOG/PEN-TEST-POSTER-WHITE-BOARD-POWERSHELL-BUILT-IN-PORT-SCANNER/](https://www.sans.org/blog/pen-test-poster-white-board-powershell-built-in-port-scanner/)
- [HTTPS://GITHUB.COM/SCIPAG/POWERSHELLUTILITIES](https://github.com/scipag/powershellutilities)
- [HTTPS://WWW.ADAMCOUCH.CO.UK/CONDUCTING-POWERSHELL-PORT-SCAN/](https://www.adamcouch.co.uk/conducting-powershell-port-scan/)
- [HTTPS://WWW.INFOSECMATTER.COM/MINIMALISTIC-TCP-AND-UDP-PORT-SCANNER/](https://www.infosecmatter.com/minimalistic-tcp-and-udp-port-scanner/)
- [HTTPS://GITHUB.COM/XORRIOR/REMOTECON](https://github.com/xorrior/remoterecon)
- [HTTPS://GITHUB.COM/MATTIFESTATION/PSREFLECT](https://github.com/mattifestation/psreflect)

CHEATSHEETS PROJECTS

- [HTTPS://GITHUB.COM/HARMJOY/CHEATSHEETS/BLOB/MASTER/POWERUP.PDF](https://github.com/HarmJoy/Cheatsheets/blob/master/PowerUp.pdf)
- [HTTPS://GITHUB.COM/HARMJOY/CHEATSHEETS/BLOB/MASTER/POWERSPLOIT.PDF](https://github.com/HarmJoy/Cheatsheets/blob/master/PowerSploit.pdf)
- [HTTPS://GITHUB.COM/HARMJOY/CHEATSHEETS/BLOB/MASTER/EMPIRE.PDF](https://github.com/HarmJoy/Cheatsheets/blob/master/Empire.pdf)
- [HTTPS://GITHUB.COM/HARMJOY/CHEATSHEETS/BLOB/MASTER/POWERVIEW.PDF](https://github.com/HarmJoy/Cheatsheets/blob/master/PowerView.pdf)

POWERUP

- [HTTPS://GITHUB.COM/POWERSHELLMAFIA/POWERSPLOIT/BLOB/MASTER/PRIVESC/POWERUP.PS1](https://github.com/PowerShellMafia/PowerSploit/blob/master/Privesc/PowerUp.ps1)
- [HTTPS://WWW.HARMJ0Y.NET/BLOG/POWERSHELL/POWERUP-A-USAGE-GUIDE/](https://www.harmj0y.net/blog/powershell/powerup-a-usage-guide/)
- [HTTPS://RECIPEFORROOT.COM/ADVANCED-POWERUP-PS1-USAGE/](https://recipeforroot.com/advanced-powerup-ps1-usage/)
- [HTTPS://JANIKVONROTZ.GITHUB.IO/POWERSHELL-POWERUP/](https://janikvonrotz.github.io/powershell-powerup/)
- [HTTPS://MEDIUM.COM/BUGBOUNTYWRITEUP/PRIVILEGE-ESCALATION-IN-WINDOWS-380BEE3A2842](https://medium.com/bugbountywriteup/privilege-escalation-in-windows-380bee3a2842)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=DNWWTJFQW78&AB_CHANNEL=METASPLOITATION](https://www.youtube.com/watch?v=DNWWTJFQW78&ab_channel=Metasploitation)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=DLJyKGfkoKQ&AB_CHANNEL=SECURITYWEEKLY](https://www.youtube.com/watch?v=DLJyKGfkoKQ&ab_channel=SecurityWeekly)

POWERSPLOIT

- [HTTPS://GITHUB.COM/POWERSHELLMAFIA/POWERSPLOIT](https://github.com/PowerShellMafia/PowerSploit)
- [HTTPS://PENTESTLAB.BLOG/TAG/POWERSPLOIT/](https://pentestlab.blog/tag/powersploit/)
- [HTTPS://WWW.CYBERPUNK.RS/POWERSPLOIT-POWERSHELL-POST-EXPLOITATION-FRAMEWORK](https://www.cyberpunk.rs/powersploit-powershell-post-exploitation-framework)
- [HTTPS://WWW.DARKNET.ORG.UK/2015/12/POWERSPLOIT-POWERSHELL-POST-EXPLOITATION-FRAMEWORK/](https://www.darknet.org.uk/2015/12/powersploit-powershell-post-exploitation-framework/)
- [HTTPS://ATTACK.MITRE.ORG/SOFTWARE/S0194/](https://attack.mitre.org/software/S0194/)
- [HTTPS://ADSECURITY.ORG/?TAG=POWERSPLOIT](https://adsecurity.org/?tag=powersploit)
- [HTTPS://MEDIUM.COM/@BENOIT.SEVENS/POWERSHELL-AV-EVASION-4E4BB6A6A961](https://medium.com/@benoit.sevens/powershell-av-evasion-4e4bb6a6a961)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=OTPNWbEADA&AB_CHANNEL=CHIEFRIVER](https://www.youtube.com/watch?v=OTPNWbEADA&ab_channel=ChiefRiver)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=LEll6QA-REY&AB_CHANNEL=METASPLOITATION](https://www.youtube.com/watch?v=LEll6QA-REY&ab_channel=Metasploitation)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=B-XJnMFZ7Ls&AB_CHANNEL=%5BMISTER_BERT0ni%5D](https://www.youtube.com/watch?v=B-XJnMFZ7Ls&ab_channel=%5BMISTER_BERT0ni%5D)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=zBMOS_fNxNG&AB_CHANNEL=SECURITYNOTES](https://www.youtube.com/watch?v=zBMOS_fNxNG&ab_channel=SecurityNotes)

EMPIRE

- [HTTPS://DANIELDONDA.COM/2019/04/07/POWERSHELL-EMPIRE/](https://danielondona.com/2019/04/07/powershell-empire/)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=52xkWbDMUUM&AB_CHANNEL=HACKERSPLOIT](https://www.youtube.com/watch?v=52xkWbDMUUM&ab_channel=HACKERSPLOIT)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=0GHS3U9zMKI&AB_CHANNEL=GusKhawaja](https://www.youtube.com/watch?v=0GHS3U9zMKI&ab_channel=GusKhawaja)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=67EXQPHK2SE&AB_CHANNEL=SeckC](https://www.youtube.com/watch?v=67EXQPHK2SE&ab_channel=SeckC)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=9-kwVLJDXWs&AB_CHANNEL=ROOTSPLOIT](https://www.youtube.com/watch?v=9-kwVLJDXWs&ab_channel=ROOTSPLOIT)
- [HTTPS://WWW.POWERSHELLEMPIRE.COM/](https://www.powershell-empire.com/)
- [HTTPS://WWW.CYBERPUNK.RS/EMPIRE-POWERSHELL-POST-EXPLOITATION-FRAMEWORK](https://www.cyberpunk.rs/empire-powershell-post-exploitation-framework)
- [HTTPS://NULL-BYTE.WONDERHOWTO.COM/HOW-TO/USE-POWERSHELL-EMPIRE-GETTING-STARTED-WITH-POST-EXPLOITATION-WINDOWS-HOSTS-0178664/](https://null-byte.wonderhowto.com/how-to/use-powershell-empire-getting-started-with-post-exploitation-windows-hosts-0178664/)
- [HTTPS://WWW.HACKINGARTICLES.IN/HACKING-WITH-EMPIRE-POWERSHELL-POST-EXPLOITATION-AGENT/](https://www.hackingarticles.in/hacking-with-empire-powershell-post-exploitation-agent/)
- [HTTPS://MEDIUM.COM/@RATIROS01/TRYHACKME-PS-EMPIRE-BD96FBF822CC](https://medium.com/@ratiros01/tryhackme-ps-empire-bd96fbf822cc)
- [HTTPS://BLOG.STEALTHBITS.COM/NEXT-GEN-OPEN-SOURCE-C2-FRAMEWORKS/](https://blog.stealthbits.com/next-gen-open-source-c2-frameworks/)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

PAYLOAD AND EVASION – TÉCNICAS COM PS

- [HTTPS://GITHUB.COM/JAREDHAIGHT/INVOKE-METASPLOITPAYLOAD](https://github.com/JaredHaight/Invoke-MetasploitPayload)
- [HTTPS://MEDIUM.COM/SWLH/FUN-WITH-POWERSHELL-PAYLOAD-EXECUTION-AND-EVASION-F5051FD149B2](https://medium.com/swlh/fun-with-powershell-payload-execution-and-evasion-f5051fd149b2)
- [HTTPS://GITHUB.COM/TRUSTEDSEC/UNICORN](https://github.com/TrustedSec/Unicorn)
- [HTTPS://GITHUB.COM/LOADENMB/TVASION](https://github.com/loadenmb/tvasion)
- [HTTPS://THREAT.TEVORA.COM/DISSECTING-VEIL-EVASION-POWERSHELL-PAYLOADS-AND-CONVERTING-TO-A-BIND-SHELL/](https://threat.tevora.com/dissecting-veil-evasion-powershell-payloads-and-converting-to-a-bind-shell/)
- [HTTPS://HAKIN9.ORG/XENCRYPT-A-POWERSHELL-SCRIPT-ANTI-VIRUS-EVASION-TOOL/](https://hakin9.org/xencrypt-a-powershell-script-anti-virus-evasion-tool/)
- [HTTPS://ARNO0X0X.WORDPRESS.COM/2016/04/13/METERPRETER-AV-IDS-EVASION-POWERSHELL/](https://arno0x0x.wordpress.com/2016/04/13/meterpreter-av-ids-evasion-powershell/)
- [HTTPS://HACK-ED.NET/2016/04/04/VEIL-EVASION-PAYLOADS-MADE-EASY/](https://hack-ed.net/2016/04/04/veil-evasion-payloads-made-easy/)
- [HTTPS://KAIZENSECURITY.WORDPRESS.COM/2016/08/19/METASPLOIT-AV-EVASION-WITH-POWERSHELL/](https://kaizensecurity.wordpress.com/2016/08/19/metasploit-av-evasion-with-powershell/)
- [HTTPS://WWW.BLACKHAT.COM/DOCS/EU-17/MATERIALS/EU-17-THOMPSON-RED-TEAM-TECHNIQUES-FOR-EVADING-BYPASSING-AND-DISABLING-MS-ADVANCED-THREAT-PROTECTION-AND-ADVANCED-THREAT-ANALYTICS.PDF](https://www.blackhat.com/docs/eu-17/materials/eu-17-Thompson-Red-Team-Techniques-For-Evading-Bypassing-And-Disabling-MS-Advanced-Threat-Protection-And-Advanced-Threat-Analytics.pdf)
- [HTTPS://WWW.BLACKHAT.COM/DOCS/US-14/MATERIALS/US-14-KAZANCIYAN-INVESTIGATING-POWERSHELL-ATTACKS-WP.PDF](https://www.blackhat.com/docs/us-14/materials/us-14-Kazanciyan-Investigating-Powershell-Attacks-WP.pdf)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

REVERSE SHELL – TÉCNICAS COM PS

- [HTTPS://RESOURCES.INFOSECINSTITUTE.COM/POWERSHELL-FOR-PENTESTERS-PART-5-REMOTING-WITH-POWERSHELL/](https://resources.infosecinstitute.com/powershell-for-pentesters-part-5-remoting-with-powershell/)
- [HTTPS://PENTESTN00B.WORDPRESS.COM/2016/08/22/POWERSHELL-PSREMOTING-PWNAGE/](https://pentestn00b.wordpress.com/2016/08/22/powershell-psremoting-pwnage/)
- [HTTPS://KALILINUXTUTORIALS.COM/EVIL-WINRM-HACKING-PENTESTING/](https://kalilinuxtutorials.com/evil-winrm-hacking-pentesting/)
- [HTTPS://WWW.RAPID7.COM/DB/MODULES/EXPLOIT/WINDOWS/LOCAL/POWERSHELL_REMOTING](https://www.rapid7.com/db/modules/exploit/windows/local/powershell_remoting)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=TVGJ-9FJKxE&AB_CHANNEL=HAK5](https://www.youtube.com/watch?v=TVGJ-9FJKxE&ab_channel=HAK5)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

REVERSE SHELL – TÉCNICAS COM PS

- [HTTPS://GIST.GITHUB.COM/EGRE55/C058744A4240AF6515EB32B2D33FB3ED3](https://gist.github.com/EGRE55/c058744a4240af6515eb32b2d33fb3ed3)
- [HTTPS://GITHUB.COM/SWISSKYREPO/PAYLOADSALLTHETHINGS/BLOB/MASTER/METHODOLOGY%20AND%20RESOURCES/REVERSE%20SHELL%20CHEATSHEET.MD](https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Reverse%20Shell%20Cheatsheet.md)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=NJ5xBHrTWWA&AB_CHANNEL=CYBERSECURITYLEARNING](https://www.youtube.com/watch?v=NJ5xBHrTWWA&ab_channel=CyberSecurityLearning)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=KKFrJTLM5LI&AB_CHANNEL=INFOSECADDICTS](https://www.youtube.com/watch?v=KKFrJTLM5LI&ab_channel=InfoSecAddicts)
- [HTTPS://HACKERSINTERVIEW.COM/OSCP/REVERSE-SHELL-ONE-LINERS-OSCP-CHEATSHEET/](https://hackersinterview.com/oscp/reverse-shell-one-liners-oscp-cheatsheet/)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=KKFrJTLM5LI&AB_CHANNEL=INFOSECADDICTS](https://www.youtube.com/watch?v=KKFrJTLM5LI&ab_channel=InfoSecAddicts)
- [HTTPS://WWW.OFFENSIVE-SECURITY.COM/OFFSEC/KALI-LINUX-POWERSHELL-PENTESTING/](https://www.offensive-security.com/offsec/kali-linux-powershell-pentesting/)
- [HTTPS://SECURITYONLINE.INFO/REVERSE-POWERSHELL/](https://securityonline.info/reverse-powershell/)
- [HTTPS://BLOG.NETSPI.COM/POWERSHELL-REMOTING-CHEATSHEET/](https://blog.netSPI.com/powershell-remoting-cheatsheet/)
- [HTTPS://WWW.IRED.TEAM/MISCELLANEOUS-REVERSING-FORENSICS/GET-INJECTEDTHREAD](https://www.ired.team/miscellaneous-reversing-forensics/get-injectedthread)
- [HTTPS://MEDIUM.COM/@THREATPOINTER/PENTESTING-POWERSHELL-REMOTING-FA605EF325D4](https://medium.com/@threatpointer/pentesting-powershell-remoting-fa605ef325d4)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

REVERSE SHELL – TÉCNICAS COM PS + BADUSB

- [HTTPS://GITHUB.COM/JODYWEIJERS/BADUSB-DIGISPARK](https://github.com/JodyWeijers/BADUSB-DIGISPARK)
- [HTTPS://WWW.ZDNET.COM/ARTICLE/RARE-BADUSB-ATTACK-DETECTED-IN-THE-WILD-AGAINST-US-HOSPITALITY-PROVIDER/](https://www.zdnet.com/article/rare-badusb-attack-detected-in-the-wild-against-us-hospitality-provider/)
- [HTTPS://HACKADAY.COM/TAG/BADUSB/](https://hackaday.com/tag/badusb/)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=IAH5RUYO2VY&AB_CHANNEL=DIMUSTECH](https://www.youtube.com/watch?v=IAH5RUYO2VY&ab_channel=DIMUSTECH)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=M6BHx75RMs&AB_CHANNEL=HAK5](https://www.youtube.com/watch?v=M6BHx75RMs&ab_channel=HAK5)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=M0AWKEf0b8C&AB_CHANNEL=IMMUNETechnologyInstitute](https://www.youtube.com/watch?v=M0AWKEf0b8C&ab_channel=IMMUNETechnologyInstitute)
- [HTTPS://GITHUB.COM/SCREETSEC/BRUTAL](https://github.com/ScreeTSEC/BRUTAL)
- [HTTPS://ATTACK.MITRE.ORG/TECHNIQUES/T1059/001/](https://attack.mitre.org/techniques/T1059/001/)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

LATERAL MOVEMENT – TÉCNICAS COM PS

- [HTTPS://MEDIUM.COM/@SUBHAMMISRA45/LATERAL-MOVEMENT-POWERSHELL-REMOTING-89DA402A9885](https://medium.com/@subhammisra45/lateral-movement-powershell-remoting-89da402a9885)
- [HTTPS://POSTS.SPECTEROPS.IO/OFFENSIVE-LATERAL-MOVEMENT-1744AE62B14F](https://posts.specterops.io/offensive-lateral-movement-1744ae62b14f)
- [HTTPS://PT.SLIDESHARE.NET/KIERANJACOBSEN/LATERAL-MOVEMENT-WITH-POWER-SHELL-2](https://pt.slideshare.net/kieranjacobsen/lateral-movement-with-power-shell-2)
- [HTTPS://WWW.IRED.TEAM/OFFENSIVE-SECURITY/LATERAL-MOVEMENT/WMI+-POWERSHELL-DESIRED-STATE-CONFIGURATION-LATERAL-MOVEMENT](https://www.ired.team/offensive-security/lateral-movement/wmi+-powershell-desired-state-configuration-lateral-movement)
- [HTTPS://GENNAROMIGLIACCIO.COM/LATERAL-MOVEMENT-TACTICS-AND-TECHNIQUES](https://gennaromigliaccio.com/lateral-movement-tactics-and-techniques)
- [HTTPS://REDCANARY.COM/BLOG/LATERAL-MOVEMENT-WINRM-WMI/](https://redcanary.com/blog/lateral-movement-winrm-wmi/)
- [HTTPS://WWW.FORWARDDEFENSE.COM/PDFS/LATERAL-MOVEMENT-ANALYSIS.PDF](https://www.forwarddefense.com/pdfs/Lateral-Movement-Analysis.pdf)
- [HTTPS://WWW.SNAPLABS.IO/INSIGHTS/LATERAL-MOVEMENT-METHODS-AND-GOOD-PRACTICES](https://www.snaplabs.io/insights/lateral-movement-methods-and-good-practices)
- [HTTPS://GIST.GITHUB.COM/JAREDCATKINSON/C95FD1E4E76A4B9B966861F64782F5A9](https://gist.github.com/jaredcatkinson/c95fd1e4e76a4b9b966861f64782f5a9)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

LATERAL MOVEMENT – TÉCNICAS COM PSEXEC (BÔNUS)

- [HTTPS://ATTACK.MITRE.ORG/SOFTWARE/S0029/](https://ATTACK.MITRE.ORG/SOFTWARE/S0029/)
- [HTTPS://WWW.OFFENSIVE-SECURITY.COM/METASPLOIT-UNLEASHED/PSEXEC-PASS-HASH/](https://WWW.OFFENSIVE-SECURITY.COM/METASPLOIT-UNLEASHED/PSEXEC-PASS-HASH/)
- [HTTPS://WWW.CONTEXTIS.COM/DE/BLOG/LATERAL-MOVEMENT-A-DEEP-LOOK-INTO-PSEXEC](https://WWW.CONTEXTIS.COM/DE/BLOG/LATERAL-MOVEMENT-A-DEEP-LOOK-INTO-PSEXEC)
- [HTTPS://WWW.MINDPOINTGROUP.COM/BLOG/LATERAL-MOVEMENT-WITH-PSEXEC/](https://WWW.MINDPOINTGROUP.COM/BLOG/LATERAL-MOVEMENT-WITH-PSEXEC/)
- [HTTPS://REDCANARY.COM/BLOG/THREAT-HUNTING-PSEXEC-LATERAL-MOVEMENT/](https://REDCANARY.COM/BLOG/THREAT-HUNTING-PSEXEC-LATERAL-MOVEMENT/)
- [HTTPS://MEDIUM.COM/@UPADHYAY.VARUN/PASS-THE-HASH-ATTACK-B0F214B2884A](https://MEDIUM.COM/@UPADHYAY.VARUN/PASS-THE-HASH-ATTACK-B0F214B2884A)
- [HTTPS://PERICIACOMPUTACIONAL.COM/WINDOWS-ACCOUNT-HIJACKING-PSEXEC-E-SUAS-POSSIBILIDADES/](https://PERICIACOMPUTACIONAL.COM/WINDOWS-ACCOUNT-HIJACKING-PSEXEC-E-SUAS-POSSIBILIDADES/)
- [HTTPS://PENTESTLAB.BLOG/TAG/PSEXEC/](https://PENTESTLAB.BLOG/TAG/PSEXEC/)
- [HTTPS://WWW.TOSHELLANDBACK.COM/2017/02/11/PSEXEC/](https://WWW.TOSHELLANDBACK.COM/2017/02/11/PSEXEC/)
- [HTTPS://WWW.POFTUT.COM/USE-PSEXEC-TOOLS-RUN-COMMANDS-GET-SHELL-REMOTE-WINDOWS-SYSTEMS/](https://WWW.POFTUT.COM/USE-PSEXEC-TOOLS-RUN-COMMANDS-GET-SHELL-REMOTE-WINDOWS-SYSTEMS/)
- [HTTPS://WWW.IRED.TEAM/OFFENSIVE-SECURITY/LATERAL-MOVEMENT/LATERAL-MOVEMENT-WITH-PSEXEC](https://WWW.IRED.TEAM/OFFENSIVE-SECURITY/LATERAL-MOVEMENT/LATERAL-MOVEMENT-WITH-PSEXEC)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

PRIVILEGE ESCALATION – TÉCNICAS COM PS

- <https://www.varonis.com/blog/how-to-use-powershell-for-privilege-escalation-with-local-computer-accounts/>
- <https://github.com/frizb/windows-privilege-escalation>
- https://www.youtube.com/watch?v=-sBXN-CGUD0&ab_channel=PentesterAcademyTV
- <https://hakin9.org/privesccheck-privilege-escalation-enumeration-script-for-windows/>
- <https://githacktools.blogspot.com/2019/04/winroothelper-windows-privilege-escalation-powershell-script.html>
- <https://www.hackingarticles.in/window-privilege-escalation-via-automated-script/>
- https://www.youtube.com/watch?v=VLKPCSQW8QY&ab_channel=UbeerILabs
- https://www.youtube.com/watch?v=BAhOHAIaQ7U&ab_channel=SANSPenTestTraining
- https://www.youtube.com/watch?v=2VZoSUJ4nWU&ab_channel=CyberStorm-Warfareinthe5thDomain
- https://www.youtube.com/watch?v=v0zYorQ0EEY&ab_channel=PowerShellEmpireTutorials
- https://www.youtube.com/watch?v=dZJfIlw3kZE&ab_channel=Moss%20CyberSecurityInstitute
- https://www.youtube.com/watch?v=BPBQUU91-Q&ab_channel=BreakTheSecurity
- <https://github.com/rmusser01/infosec-reference/blob/master/draft/privescPostEx.md>

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

COMMAND AND CONTROL – TÉCNICAS COM PS

- [HTTPS://PENTESTLAB.BLOG/2017/08/19/COMMAND-AND-CONTROL-POWERSHELL/](https://pentestlab.blog/2017/08/19/command-and-control-powershell/)
- [HTTPS://ENIGMA0X3.NET/2014/01/17/COMMAND-AND-CONTROL-USING-POWERSHELL-AND-YOUR-FAVORITE-WEBSITE/](https://enigma0x3.net/2014/01/17/command-and-control-using-powershell-and-your-favorite-website/)
- [HTTPS://WWW.SNAPLABS.IO/INSIGHTS/COMMAND-AND-CONTROL-WITH-POWERSHELL-EMPIRE-PT1](https://www.snaplabs.io/insights/command-and-control-with-powershell-empire-pt1)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=WVHVDUVFQNM&AB_CHANNEL=DEMMSEC](https://www.youtube.com/watch?v=wVHvDUVFQNM&ab_channel=DEMMSEC)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=OH-LCN5K9K8&AB_CHANNEL=COVER6SOLUTIONS](https://www.youtube.com/watch?v=OH-LCN5K9K8&ab_channel=COVER6SOLUTIONS)
- [HTTPS://TRUNESKI.GITHUB.IO/BLOG/2017/03/03/DROPBOX-COMMAND-AND-CONTROL-OVER-POWERSHELL-WITH-INVOKE-DBC2/](https://truneski.github.io/blog/2017/03/03/dropbox-command-and-control-over-powershell-with-invoke-DBC2/)
- [HTTPS://WWW.COVER6SOLUTIONS.COM/WEBINAR-INTRO-TO-C2-WITH-POWERSHELL-EMPIRE/](https://www.cover6solutions.com/webinar-intro-to-c2-with-powershell-empire/)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

PERSISTENCE – TÉCNICAS COM PS

- [HTTPS://PENTESTLAB.BLOG/2019/11/05/PERSISTENCE-POWERSHELL-PROFILE/](https://pentestlab.blog/2019/11/05/persistence-powershell-profile/)
- [HTTPS://PENTESTLAB.BLOG/2019/11/04/PERSISTENCE-SCHEDULED-TASKS/](https://pentestlab.blog/2019/11/04/persistence-scheduled-tasks/)
- [HTTPS://GITHUB.COM/EMILYANNCR/WINDOWS-POST-EXPLOITATION](https://github.com/emilyanncr/windows-post-exploitation)
- [HTTPS://ADSECURITY.ORG/?P=429](https://adsecurity.org/?p=429)
- [HTTPS://BOOK.HACKTRICKS.XYZ/WINDOWS/BASIC-POWERSHELL-FOR-PENTESTERS](https://book.hacktricks.xyz/windows/basic-powershell-for-pentesters)
- [HTTPS://MEDIA.BLACKHAT.COM/EU-13/BRIEFINGS/MITTAL/BH-EU-13-POWERSHELL-FOR-PENETRATION-MITTAL-SLIDES.PDF](https://media.blackhat.com/EU-13/briefings/Mittal/BH-EU-13-powershell-for-penetration-mittal-slides.pdf)

TÉCNICAS DE EXPLORAÇÃO E PÓS EXPLORAÇÃO

EXFILTRATION – TÉCNICAS COM PS

- [HTTPS://WWW.IRED.TEAM/OFFENSIVE-SECURITY/EXFILTRATION](https://www.ired.team/offensive-security/exfiltration)
- [HTTPS://AZERIA-LABS.COM/DATA-EXFILTRATION/](https://azeria-labs.com/data-exfiltration/)
- [HTTPS://WWW.HACKINGARTICLES.IN/DATA-EXFILTRATION-USING-POWERSHELL-EMPIRE/](https://www.hackingarticles.in/data-exfiltration-using-powershell-empire/)
- [HTTPS://WWW.SANS.ORG/WEBCASTS/PEN-TESTING-POWERSHELL-DATA-EXFILTRATION-TECHNIQUES-108740](https://www.sans.org/webcasts/pen-testing-powershell-data-exfiltration-techniques-108740)
- [HTTPS://BLOG.STACKATTACK.NET/2019/03/14/QUICK-HIT-BASE64-POWERSHELL-EXFILTRATION/](https://blog.stackattack.net/2019/03/14/quick-hit-base64-powershell-exfiltration/)
- [HTTPS://NIICONCONSULTING.COM/CHECKMATE/2016/03/EXFILTRATION-USING-POWERSHELL-OUTLOOK/](https://niiconsulting.com/checkmate/2016/03/exfiltration-using-powershell-outlook/)
- [HTTPS://WWW.SEVENLAYERS.COM/INDEX.PHP/305-POWERSHELL-DATA-EXFIL](https://www.sevenlayers.com/index.php/305-powershell-data-exfil)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=8ZAREHY5HBW](https://www.youtube.com/watch?v=8ZAREHY5HBW)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=TBBT1C2ZJMS&AB_CHANNEL=HAK5](https://www.youtube.com/watch?v=TBBT1C2ZJMS&AB_CHANNEL=HAK5)
- [HTTPS://WWW.YOUTUBE.COM/WATCH?V=MIQVvx943FW&AB_CHANNEL=SANSPenTestTraining](https://www.youtube.com/watch?v=MIQVvx943FW&AB_CHANNEL=SANSPenTestTraining)

RECURSOS

- [HTTPS://GITHUB.COM/TOPICS/PENETRATION-TESTING?L=POWERSHELL](https://github.com/topics/penetration-testing?l=powershell)
- [HTTPS://WWW.FIREEYE.COM/CONTENT/DAM/FIREEYE-WWW/GLOBAL/EN/SOLUTIONS/PDFS/WP-LAZANCIYAN-INVESTIGATING-POWERSHELL-ATTACKS.PDF](https://www.fireeye.com/content/dam/fireeye-www/global/en/solutions/pdfs/wp-lazancian-investigating-powershell-attacks.pdf)
- [HTTPS://LIVE.SYSINTERNALS.COM/](https://live.sysinternals.com/)
- [HTTPS://GITHUB.COM/BLUSCREENOFJEFF/RED-TEAM-INFRASTRUCTURE-WIKI](https://github.com/bluscreenofjeff/red-team-infrastructure-wiki)
- [HTTPS://BLOG.HARMJ0Y.NET/](https://blog.harmj0y.net/)
- [HTTPS://ENIGMA0X3.NET/](https://enigma0x3.net/)
- [HTTPS://WALD0.COM/](https://wald0.com/)
- [HTTPS://POSTS.SPECTEROPS.IO/](https://posts.specterops.io/)
- [HTTP://WWW.EXPLOIT-MONDAY.COM/](http://www.exploit-monday.com/)
- [HTTPS://ADSECURITY.ORG/](https://adsecurity.org/)
- [HTTP://WWW.INVOKE-IR.COM/](http://www.invoke-ir.com/)
- [HTTPS://SPECTEROPS.IO/RESOURCES/RESEARCH-AND-DEVELOPMENT](https://specterops.io/resources/research-and-development)

RECURSOS

- [HTTPS://WWW.BLACKHAT.COM/US-16/TRAINING/ADVANCED-POWERSHELL-FOR-OFFENSIVE-OPERATIONS.HTML](https://www.blackhat.com/us-16/training/advanced-powershell-for-offensive-operations.html)
- DORKS:
 - POWERSHELL RED TEAM FILETYPE:PDF
 - POWERSHELL RED TEAM SITE:WWW.BLACKHAT.COM FILETYPE:PDF
 - POWERSHELL PENTEST SITE:WWW.BLACKHAT.COM FILETYPE:PDF
 - POWERSHELL PENTEST FILETYPE:PDF

CONCLUSÃO

- COM CERTEZA O POWERSHELL É UM DOS UTILITÁRIOS QUE ABRE BASTANTE POSSIBILIDADES EM UM PENTEST EM INFRAESTRUTURA WINDOWS, PRINCIPALMENTE PELO SEU PODER NA ADMINISTRAÇÃO DE SISTEMAS OPERACIONAIS COMO WINDOWS SERVER;
- POR ISSO, EU RECOMENDO QUE VOCÊ PESQUISE E SE APROFUNDE CADA VEZ MAIS, E MONTE SEMPRE SEUS LABORATÓRIOS, RECOMENDO SEMPRE O TRYHACKME, HACKTHEBOX E VULNHUB QUE CONTA COM ÓTIMAS MÁQUINAS PARA LABORATÓRIO;
- ESPERO QUE TENHA GOSTADO DESSE OVERVIEW!

Pentest in Office365 and Security

Joas Antonio

Details

- This pdf aims to bring techniques and tools for performing pentesting in Office365 environments

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

Introduction

- <https://docs.microsoft.com/pt-br/microsoft-365/?view=o365-worldwide>
- <https://docs.microsoft.com/pt-br/office/>
- [https://docs.axway.com/bundle/AMPLIFY Integration Builder allOS en/page/microsoft office 365 api documentation.html](https://docs.axway.com/bundle/AMPLIFY_Integration_Builder_allOS_en/page/microsoft_office_365_api_documentation.html)
- <https://system.suny.edu/userservices/office365-faq/>
- <https://github.com/MicrosoftDocs/microsoft-365-docs>
- <https://techdocs.blogs.brynmawr.edu/6634>
- <https://www.varonis.com/blog/microsoft-office-365-file-sharing/>
- <https://www.youtube.com/watch?v=01T6gSvR0xs>

Introduction

- <https://www.microsoft.com/pt-br/microsoft-365>
- <https://www.microsoft.com/pt-br/microsoft-365/microsoft-office>
- <https://www.microsoft.com/pt-br/microsoft-365/microsoft-365-for-existing-subscribers>
- <https://www.youtube.com/watch?v=HhgpVvqZhzA>
- <https://www.youtube.com/watch?v=zsBt85WjtIY>

PenTest in Office365

- <https://www.microsoft.com/en-us/msrc/pentest-rules-of-engagement>
- <https://www.agileit.com/news/pentesting-microsoft-office-365/>
- <https://bond-o.medium.com/microsoft-office-365-enumeration-58f9b5ba21c8>
- <https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/>
- <https://thecyphere.com/blog/office365-security-best-practices/>
- <https://www.imgsecurity.com/will-you-be-pwned-in-an-office-365-brute-force-attack-use-this-free-tool-for-testing/>
- <https://intercom.help/cobalt/en/articles/4641747-network-office-365-penetration-testing>
- <https://www.trustedsec.com/blog/owning-o365-through-better-brute-forcing/>
- <https://www.redscan.com/news/office-365-security-six-ways-to-safeguard-your-environment-against-cyber-attacks/>
- <https://www.kitploit.com/2019/07/o365-attack-toolkit-toolkit-to-attack.html?m=0>

PenTest in Office365

- <https://vapt.ee/offensive-security/penetration-testing/cloud-penetration-testing/office365-penetration-testing/>
- <https://www.blackhillsinfosec.com/tag/office365/>
- <https://github.com/0xZDH/o365spray>
- <https://github.com/S3cur3Th1sSh1t/Pentest-Tools>
- <https://github.com/mdsecresearch/LyncSniper>
- <https://github.com/byt3bl33d3r/SprayingToolkit>
- <https://github.com/sensepost/ruler>
- <https://pentestbook.six2dez.com/enumeration/cloud/azure>
- <https://www.blackhatethicalhacking.com/tools/o365-attack-toolkit/>
- <https://www.cryptron.ch/security-analysis-microsoft-office-365-advanced-threat-protection/>
- <https://securityonline.info/raindance/>
- <https://www.microsoft.com/pt-br/msrc/pentest-rules-of-engagement>

PenTest in Office365

- <https://www.agileit.com/news/pentesting-microsoft-office-365/>
- <https://www.mdsec.co.uk/2019/07/introducing-the-office-365-attack-toolkit/>
- <https://thecyphere.com/blog/office365-security-best-practices/>
- <https://www.linkedin.com/pulse/risk-assessment-penetration-testing-microsoft-azure-satinder/>
- <https://www.cryptron.ch/security-analysis-microsoft-office-365-advanced-threat-protection/>
- <https://i.blackhat.com/USA-20/Thursday/us-20-Bienstock-My-Cloud-Is-APTs-Cloud-Investigating-And-Defending-Office-365.pdf>
- <https://i.blackhat.com/USA-19/Wednesday/us-19-Metcalf-Attacking-And-Defending-The-Microsoft-Cloud.pdf>
- <https://www.blackhat.com/docs/us-17/wednesday/us-17-Dods-Infecting-The-Enterprise-Abusing-Office365-Powershell-For-Covert-C2.pdf>
- <https://github.com/Kyuu-Ji/Awesome-Azure-Pentest>
- <https://github.com/swisskyrepo/PayloadsAllTheThings/blob/master/Methodology%20and%20Resources/Cloud%20-%20Azure%20Pentest.md>
- <https://book.hacktricks.xyz/cloud-security/cloud-security-review>
- <https://www.blackhillsinfosec.com/exploiting-mfa-inconsistencies-on-microsoft-services/>
- <https://www.optiv.com/insights/source-zero/blog/go365-office-365-password-spraying-tool>

Phishing Office365

- <https://github.com/duocircle/Office365-Phishing-Rules>
- <https://github.com/AlteredSecurity/365-Stealer>
- <https://github.com/mdsecactivebreach/o365-attack-toolkit>
- <https://docs.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?redirectSourcePath=%252fen-us%252farticle%252fSet-up-multi-factor-authentication-for-Office-365-users-8f0454b2-f51a-4d9c-bcde-2c48e41621c6&view=o365-worldwide#enablemfaoffice365>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/set-up-anti-phishing-policies.md>
- <https://github.com/pentestgeek/phishing-frenzy-templates/tree/master/office365>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/campaigns/m365-campaigns-phishing-and-attacks.md>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/tuning-anti-phishing.md>
- <https://github.com/milo2012/phishing-scripts/blob/master/o365.py>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/recommended-settings-for-eop-and-office365.md>

Phishing Office365

- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/attack-simulation-training.md>
- <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/attack-simulator-need-a-real-phishing-template-library-to-be/m-p/1405895>
- <https://staaldraad.github.io/2017/08/02/o365-phishing-with-oauth/>
- <https://medium.com/sekoia-io-blog/analysis-and-detection-of-mitm-phishing-attacks-bypassing-2fa-o365-use-case-cf0ffdae9cae>
- <https://hooksecurity.co/phishing-examples/github-phishing-example>
- <https://otx.alienvault.io/pulse/5df9f836cfe26eacac1703ad>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/attack-simulator.md>
- https://github.com/MicrosoftLearning/MS-500-Microsoft-365-Security/blob/master/Instructions/Labs/MS500T00/LAB_AK_06_Lab1_Ex1_Phishing_attack.md
- https://github.com/MicrosoftLearning/MS-101T00-Microsoft-365-Mobility-and-Security/blob/master/Instructions/Labs/LAB_AK_03_Lab3_Ex1_AttackSim_Phishing_attack.md

Office 365 Security

- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/defender-for-office-365.md>
- <https://github.com/microsoft/Microsoft-365-Defender-Hunting-Queries/blob/master/Delivery/Open%20email%20link.txt>
- <https://github.com/MicrosoftDocs/microsoft-365-docs/blob/public/microsoft-365/security/office-365-security/security-recommendations-for-priority-accounts.md>
- <https://docs.microsoft.com/pt-br/microsoft-365/security/defender/overview-security-center?view=o365-worldwide#:~:text=O%20Microsoft%20365%20de%20seguran%C3%A7a,seguran%C3%A7a%20para%20o%20portal%20unificado.&text=As%20fun%C3%A7%C3%B5es%20j%C3%A1%20nos%20produtos,portal%20Microsoft%20365%20seguran%C3%A7a%2C%20automaticamente.>
- <https://www.microsoft.com/security/blog/office-365-security/>
- <https://www.cloudfastpath.com/office-365-migration/top-office-365-security-features-examples/>
- <https://docs.microsoft.com/pt-br/microsoft-365/security/office-365-security/security-dashboard?view=o365-worldwide>
- <https://www.youtube.com/watch?v=eBByRs1GsuA>
- <https://www.youtube.com/watch?v=hl4Kid-uzxY>
- <https://techcommunity.microsoft.com/t5/security-compliance-and-identity/announcing-microsoft-365-security-for-it-pros-2021-edition/m-p/1518661>
- <https://medium.com/falconforce/reducing-your-office365-attack-surface-1073a4d46a7b>
- https://www.beazley.com/documents/TMB/Insights/beazley-bbr-hardening_O365_best_practices_08312018.pdf
- https://www.cisecurity.org/benchmark/microsoft_office/
- <https://static1.squarespace.com/static/5bbb4a7301232c6e6c8757fa/t/603f6ea2dbc4a57691453b61/1614769826578/Office+365+Hardening.pdf>

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=raulcopp
- <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=zvQli2Kfk-k&ab_channel=PentesterAcademyTV

DLL Hijacking 2

- https://www.youtube.com/watch?v=e_I5TCgw3wo&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=0patchbyACROS Security
- https://www.youtube.com/watch?v=gd-F1dIWBAw&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=3BQKpPNITSo&ab_channel=ZeroDayInitiative
- https://www.youtube.com/watch?v=C9GfMfFjhYI&ab_channel=Hak5
- <https://medium.com/@mattharr0ey/privilege-escalation-uac-bypass-in-changeapk-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://mastroon.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

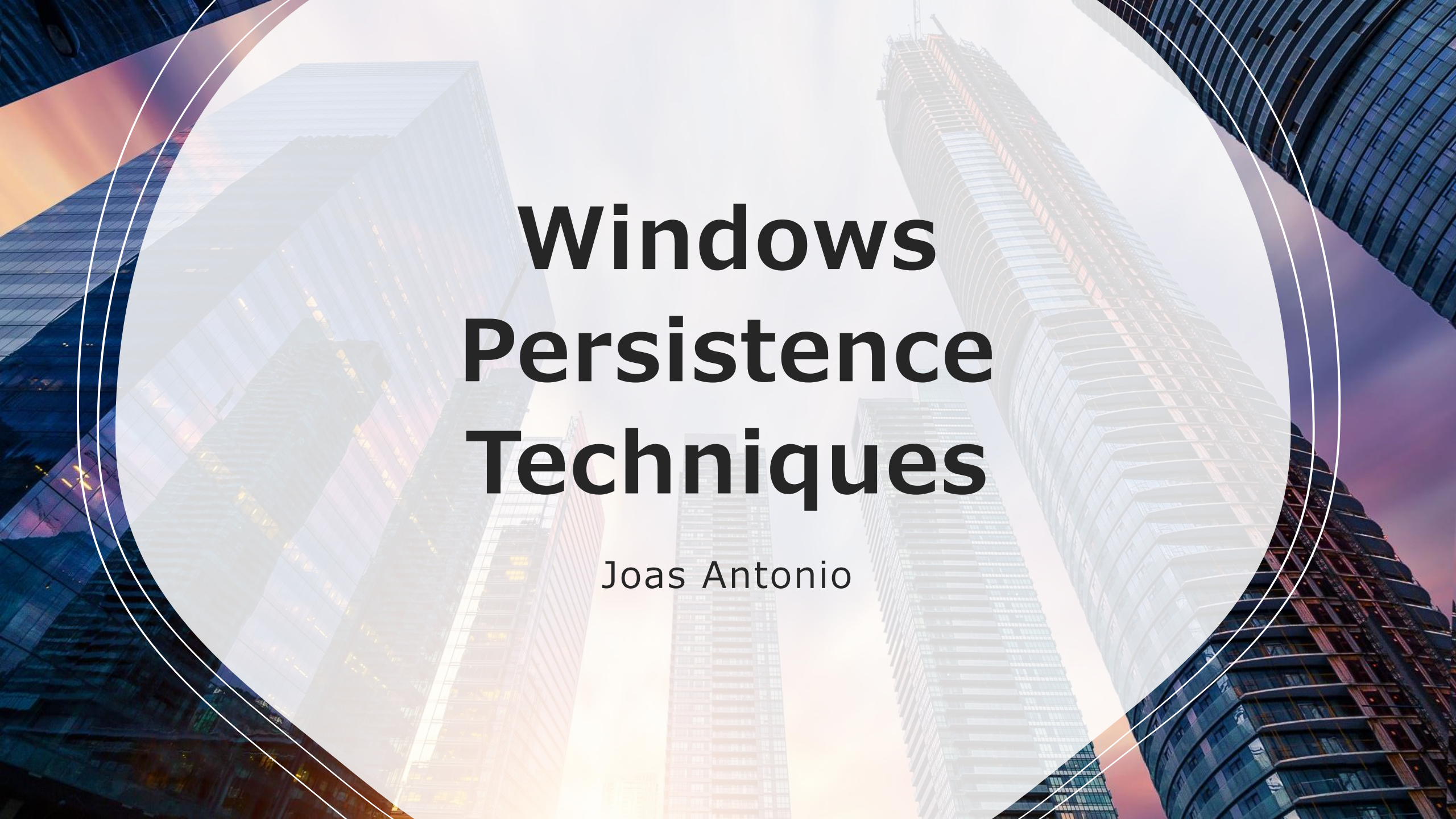
- <https://www.udemy.com/course/windows-privilege-escalation/?src=sac&kw=windows+privilege>
- <https://www.udemy.com/course/windows-privilege-escalation-for-beginners/?src=sac&kw=windows+privilege>
- <https://institute.sektor7.net/rto-lpe-windows>
- <https://www.udemy.com/course/advanced-windows-privilege-escalation-with-hack-the-box/?src=sac&kw=windows%20privil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

Extras

- <https://github.com/TCM-Course-Resources/Windows-Privilege-Escalation-Resources>
- https://www.youtube.com/watch?v=WKmbIhH9Wv8&ab_channel=MotasmHamdan-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=Wc7NVI-wNXI>



Windows Persistence Techniques

Joas Antonio

Details

Just an overview of some persistence techniques on windows operating systems

<https://www.linkedin.com/in/joas-antonio-dos-santos>

Introduction

<https://www.linkedin.com/in/joas-antonio-dos-santos>

Addendum

https://media.howard.com/CNET/USER_MANUAL/2E5177A4-159B-4A2E-9BD8-AAD90ACB0981.pdf

https://nimax-img.de/Produktdownloads/addendum_18877.pdf

https://www.eldoled.com/cms_file.php?fromDB=5567

<https://www.microsoft.com/en-us/licensing/product-licensing/products>

https://www.energytrust.org/wp-content/uploads/2016/10/HES_FM_WindowsAddendum.pdf

<https://github.com/Juanito99/Windows.Computer.DataOnDemand.Addendum>



PrivEsc Techniques

<https://www.linkedin.com/in/joas-antonio-dos-santos>

My ebook

https://drive.google.com/file/d/1Hjq_Hc8dQEF_ZhNFtGMrI2GELo_ryboyW/view?usp=sharing

Folder and Registre Keys

<https://medium.com/r3d-buck3t/abuse-service-registry-acls-windows-privesc-f88079140509>

<https://book.hacktricks.xyz/windows/windows-local-privilege-escalation/privilege-escalation-with-autorun-binaries>

<https://book.hacktricks.xyz/windows/windows-local-privilege-escalation>

<https://pentestlab.blog/category/privilege-escalation/>

<https://dmcxblue.gitbook.io/red-team-notes/persistence/registry-keys-startup-folder>

<https://www.semperis.com/blog/group-policy-privilege-escalation/>

<https://infosecwriteups.com/privilege-escalation-in-windows-380bee3a2842>

Logon Scripts

<https://blog.gdssecurity.com/labs/2015/1/26/badsamba-exploiting-windows-startup-scripts-using-a-maliciou.html>

<https://github.com/frizb/Windows-Privilege-Escalation>

<https://www.hackingarticles.in/window-privilege-escalation-automated-script/>

<https://rahmatnurfauzi.medium.com/windows-privilege-escalation-scripts-techniques-30fa37bd194>

<https://dmcxblue.gitbook.io/red-team-notes/persistence/logon-scripts>

<https://hakin9.org/privesccheck-privilege-escalation-enumeration-script-for-windows/>

Screensaver

<https://blogs.msmvps.com/donna/2004/11/24/microsoft-windows-logon-screensaver-local-privilege-escalation-vulnerability/>

<https://packetstormsecurity.com/files/137387/League-Of-Legends-Screensaver-File-Permission-Privilege-Escalation.html>

<https://www.w4rri0r.com/sequence-of-commands/privilege-escalation-attacks.html>

DLL Proxying

<https://itm4n.github.io/dll-proxying/>

<https://kevinalmansa.github.io/application%20security/DLL-Proxying/>

<https://www.ired.team/offensive-security/persistence/dll-proxying-for-persistence>

<https://github.com/tothi/dll-hijack-by-proxying>

<https://milosilo.com/hacking/microsoft-teams-proxy-dll-hijacking/>

<https://www.youtube.com/watch?v=raLnL4DdvKU>

<https://www.youtube.com/watch?v=tSdyfaJ7T50>

<https://www.cynet.com/attack-techniques-hands-on/dlls-and-ways-they-can-hurt-us/>

Component object model

<https://research.nccgroup.com/2020/04/15/cve-2019-1381-and-cve-2020-0859-how-misleading-documentation-led-to-a-broken-patch-for-a-windows-arbitrary-file-disclosure-vulnerability/>

<https://www.elastic.co/guide/en/security/7.x/component-object-model-hijacking.html>

<https://attack.mitre.org/techniques/T1559/001/>

<https://dmcxblue.gitbook.io/red-team-notes/execution/com>



Persistence Techniques

<https://www.linkedin.com/in/joas-antonio-dos-santos>

Eleveted Schedule Task

<https://www.windowstricks.in/2018/08/how-to-run-the-powershell-script-in-scheduled-task-with-run-as-administrator.html>

<https://stackoverflow.com/questions/62245797/how-to-setup-a-powershell-script-in-windows-task-scheduler-with-admin-permission>

<https://superuser.com/questions/1640613/how-to-run-a-powershell-script-with-elevated-access-using-task-scheduler>

<https://blog.netwrix.com/2018/07/03/how-to-automate-powershell-scripts-with-task-scheduler/>

https://www.reddit.com/r/PowerShell/comments/6qvp30/task_schedule_powershell_script_with_admin_rights/

<https://o365reports.com/2019/08/02/schedule-powershell-script-task-scheduler/>

<https://pentestlab.blog/2019/11/04/persistence-scheduled-tasks/>

<https://www.elastic.co/guide/en/security/current/persistence-via-telemetrycontroller-scheduled-task-hijack.html>

<https://attack.mitre.org/techniques/T1053/005/>

Multiaction Task

<https://securitybyexpert.com/windows-persistence-multi-action-scheduled-task/>

<https://www.fireeye.com/blog/threat-research/2019/09/sharpersist-windows-persistence-toolkit.html>

<https://www.igi-global.com/dictionary/assessment-of-task-persistence/50930>

<https://techdocs.broadcom.com/us/en/symantec-security-software/identity-security/identity-manager/14-4/configuring/task-persistence.html>

<https://www.elastic.co/guide/en/security/7.x/persistence-via-telemetrycontroller-scheduled-task-hijack.html>

WMI Event Subscription

<https://pentestlab.blog/2020/01/21/persistence-wmi-event-subscription/>

<https://www.elastic.co/guide/en/security/current/persistence-via-wmi-event-subscription.html>

<https://medium.com/threatpunter/detecting-removing-wmi-persistence-60ccbb7dff96>

<https://www.mdsec.co.uk/2019/05/persistence-the-continued-or-prolonged-existence-of-something-part-3-wmi-event-subscription/>

<https://in.security/an-intro-into-abusing-and-identifying-wmi-event-subscriptions-for-persistence/>

<https://liberty-shell.com/sec/2019/06/16/wmi-persistence/>

<https://techcommunity.microsoft.com/t5/microsoft-defender-for-endpoint/asr-in-intune-for-quot-block-persistence-through-wmi-event/m-p/2068130>

<https://microsoftintune.uservoice.com/forums/291681-ideas/suggestions/40862476-asr-rule-block-persistence-through-wmi-event-subs>

https://www.rapid7.com/db/modules/exploit/windows/local/wmi_persistence/

Appcert DLLS

<https://www.elastic.co/guide/en/security/current/registry-persistence-via-appcert-dll.html>

<https://attack.mitre.org/techniques/T1546/009/>

<https://pentestlab.blog/2020/01/07/persistence-appinit-dlls/>

<https://eqllib.readthedocs.io/en/latest/analytics/14f90406-10a0-4d36-a672-31cabe149f2f.html>

https://github.com/ewilded/Windows_persistence/blob/master/REGISTRY.md

<https://dmfrsecurity.com/2021/01/02/review-red-team-operator-windows-persistence-course-by-sektor7-institute/>

Appinit DLLS

<https://eforensicsmag.com/appinit-dll-injection-by-siddharth-sharma/>

<https://attack.mitre.org/techniques/T1546/010/>

<https://www.elastic.co/guide/en/security/current/registry-persistence-via-appinit-dll.html>

<https://eqllib.readthedocs.io/en/latest/analytics/822dc4c5-b355-4df8-bd37-29c458997b8f.html>

<https://github.com/redcanaryco/atomic-red-team/blob/master/atomics/T1546.010/T1546.010.md>

https://github.com/akapv/atomic-red-team/blob/master/Windows/Persistence/AppInit_DLLs.md

<https://docs.microsoft.com/en-us/windows/win32/dlls/secure-boot-and-appinit-dlls>

<https://www.cyberhuntingguide.net/t1546010.html>

Netsh Helper DLL

<https://pentestlab.blog/2019/10/29/persistence-netsh-helper-dll/>

<https://attack.mitre.org/techniques/T1546/007/>

<https://www.ired.team/offensive-security/persistence/t1128-netsh-helper-dll>

<https://github.com/rtcrowley/Offensive-Netsh-Helper>

<https://dmcxblue.gitbook.io/red-team-notes-2-0/red-team-techniques/persistence/t1546-event-triggered-execution/netsh-helper-dll>

<https://www.hackingarticles.in/windows-persistence-using-netsh/>

https://www.reddit.com/r/netsec/comments/donwj5/persistence_netsh_helper_dll/

<https://liberty-shell.com/sec/2018/07/28/netshlep/>

<https://eqllib.readthedocs.io/en/latest/analytics/5f9a71f4-f5ef-4d35-aff8-f67d63d3c896.html>

Time Provider Persistence

<https://www.ired.team/offensive-security/persistence/t1209-hijacking-time-providers>

<https://pentestlab.blog/2019/10/22/persistence-time-providers/>

<https://attack.mitre.org/techniques/T1547/003/>

<https://github.com/elastic/detection-rules/issues/853>

<https://github.com/endgameinc/eqlib/blob/master/eqlib/analytics/persistence/T1209-persistence-time-providers.toml>

<https://institute.sektor7.net/rto-windows-persistence>

<https://medium.com/@gabriel.pirjolescu/demystifying-windows-malware-hunting-part-1-detecting-persistence-with-osquery-b53573c2aac0>

Port Monitors

<https://pentestlab.blog/2019/10/28/persistence-port-monitors/#:~:text=Interaction%20with%20the%20service%20is,configuration%2C%20data%20and%20monitor%20files.>

<https://www.hackingarticles.in/windows-persistence-port-monitors/>

<https://posts.slayerlabs.com/monitor-persistence/>

<https://github.com/airzero24/PortMonitorPersist>

<https://www.ired.team/offensive-security/persistence/t1013-addmonitor>

<https://windows-internals.com/printdemon-cve-2020-1048/>

Isa-as-a-persistence

<https://adsecurity.org/?p=1760>

<https://attack.mitre.org/tactics/TA0003/>

<https://pentestlab.blog/2019/10/21/persistence-security-support-provider/>

<https://www.elastic.co/guide/en/security/current/potential-Isa-authentication-package-abuse.html>

<https://lifars.com/2021/01/common-malware-persistence-techniques/>

<https://www.csoononline.com/article/3393268/how-to-outwit-attackers-using-two-windows-registry-settings.html>

[https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565\(v=ws.11\)](https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh994565(v=ws.11))

https://www.ndss-symposium.org/wp-content/uploads/2017/09/P01_3.pdf

Metasploit Persistence

<https://www.hackingarticles.in/multiple-ways-to-persistence-on-windows-10-with-metasploit/>

<https://www.offensive-security.com/metasploit-unleashed/meterpreter-service/>

<https://www.offensive-security.com/metasploit-unleashed/persistent-backdoors/>

<https://www.hackers-arise.com/how-to-make-the-meterpreter-persistent>

<https://securityonline.info/automated-persistent-backdoor-metasploit/>

<https://secnhack.in/technique-to-persistence-on-windows-10-with-metasploit/>

<https://pentestlab.blog/2020/02/04/persistence-waitfor/>

<https://www.rapid7.com/db/modules/exploit/windows/local/persistence/>

<https://ways2hack.com/metasploit-framework/>