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=gl6-8AXlfL4&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=MotasemHamdan-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-ArI&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.gomplx.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

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=JkIA7eWeVoY&ab_channel=AnkitJoshi

PenTest AD

- https://medium.com/@daniela.mh20/attacktive-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/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_l5TCgw3wo&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.aptive.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+Scheduled+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.ivoidwarranties.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=IelRK-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-cheetsheets
- 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