OFFENSIVE SECURITY EVASION TECHNIQUES PT.1

JOAS ANTONIO

Details

- This is an overview book, which only helps in research in the areas of avoidance, the objective is not to demonstrate any technique in practice, just to indicate.

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

Programming Concepts

- https://medium.com/@karan.02031993/7-programming-concepts-everyone-should-know-with-code-99066039e800
- https://webplatform.github.io/docs/concepts/general_programming/
- https://livecode.byu.edu/programmingconcepts/ControlStruct.php
- https://tinker.ly/important-programming-concepts-which-everyone-must-be-aware-of/

Programming Level

- https://bournetocode.com/projects/GCSE_Computing_Fundamentals/pages/3-2-9-class_prog_langs.html#:~:text=Programming%20languages%20can%20be%20divided,assembly%20languages%20and%20machine%20code
- https://en.wikipedia.org/wiki/High-level_programming_language
- https://www.javatpoint.com/classification-of-programming-languages
- https://www.youtube.com/watch?v=bUWCD45qniA&ab_channel=CSRocks

Windows Concept

- WOW64 utiliza quatro bibliotecas de 64 bits (Ntdll.dll, Wow64.dll, Wow64Win.dll e Wow64Cpu.dll) para emular a execução de código de 32 bits e realizar traduções entre o aplicativo e o Kernel.
- Em versões de 32 bits do Windows, a maioria dos aplicativos e bibliotecas nativos do Windows são armazenados em C: \ Windows \ System32. Em versões de 64 bits do Windows, programas nativos de 64 bits e DLLs são armazenados em C: \ Windows \ System32 e as versões de 32 bits são armazenadas em C: \ Windows \ SysWOW64.
- Como testadores de penetração, devemos permanecer cientes da arquitetura ou bitness de nossos alvos, uma vez que
- isso dita o tipo de shellcode e outro código compilado que podemos usar.

Windows Concept

- WOW64 utilizes four 64-bit libraries (Ntdll.dll, Wow64.dll, Wow64Win.dll and Wow64Cpu.dll) to emulate the execution of 32-bit code and perform translations between the application and the kernel. On 32-bit versions of Windows, most native Windows applications and libraries are stored in C:\Windows\System32. On 64-bit versions of Windows, 64-bit native programs and DLLs are stored in C:\Windows\System32 and 32-bit versions are stored in C:\Windows\SysWOW64. As penetration testers, we must remain aware of the architecture or bitness of our targets, since this dictates the type of shellcode and other compiled code that we can use.

Windows32 API

- https://docs.microsoft.com/en-us/windows/win32/apiindex/windows-api-list
- https://docs.microsoft.com/en-us/windows/win32/api/
- https://pt.wikipedia.org/wiki/API_do_Windows
- https://www.youtube.com/watch?v=rIoD6wWINto&ab_channel=b1nch3f
- https://www.youtube.com/watch?v=ml8UG_GqOvM&ab_channel=Samuli
- https://mentebinaria.gitbook.io/engenharia-reversa/windows-api
- https://riptutorial.com/winapi

Windows Registry

- https://en.wikipedia.org/wiki/Windows_Registry
- https://www.computerhope.com/jargon/r/registry.htm
- https://medium.com/@lucideus/windows-registry-forensic-analysis-part-1-windows-forensics-manual-2018-2cb4da210125

Client Code Execution with Office

https://enigma0x3.net/2014/01/22/using-office-macros-for/

https://attack.mitre.org/techniques/T1203/

https://www.youtube.com/watch?v=hvqwpXhFGXs&ab_channel=MotasemHamdan-CyberSecurityTrainer

https://github.com/moohax/Code-Execution

Payload Types

- https://medium.com/@PenTest_duck/offensive-msfvenom-from-generating-shellcode-to-creating-trojans-4be10179bb86#:~:text=Staged%20payloads%20send%20a%20small,the%20rest%20of%20the%20payload.&text=Stageless%20payloads%20send%20the%20entire,attacker%20to%20provide%20more%20data.
- https://blog.rapid7.com/2015/03/25/stageless-meterpreter-payloads/

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

HTML Smuggling

https://secureteam.co.uk/articles/information-assurance/what-is-html-smuggling/

https://www.ired.team/offensive-security/defense-evasion/file-smuggling-with-html-and-javascript

https://outflank.nl/blog/2018/08/14/html-smuggling-explained/

https://threatpost.com/active-malware-campaign-html-smuggling/158439/

https://techgenix.com/duri-html-smuggling-attack/

https://www.securityweek.com/ongoing-campaign-uses-html-smuggling-malware-delivery

https://github.com/ZeddYu/HTTP-Smuggling-Lab

https://github.com/SofianeHamlaoui/Pentest-Notes/blob/master/offensive-security/defense-evasion/file-smuggling-with-html-and-javascript.md

Phishing Pretexting

https://github.com/L4bF0x/PhishingPretexts

https://www.csoonline.com/article/3546299/what-is-pretexting-definition-examples-and-prevention.html

https://www.vadesecure.com/en/blog/pretexting-5-examples-of-social-engineering-tactics

Execute Shellcode in Word Memory

https://www.contextis.com/en/blog/a-beginners-guide-to-windows-shellcode-execution-techniques

https://modexp.wordpress.com/2019/06/24/inmem-exec-dll/

https://blog.cystack.net/word-based-malware-attack/

https://bittherapy.net/post/malicious-document-analysis-macro-to-shellcode/

https://null-byte.wonderhowto.com/how-to/execute-code-microsoft-word-document-without-security-warnings-0180495/

https://labs.nettitude.com/blog/from-macro-to-malware-a-step-by-step-analysis/

https://github.com/bdamele/shellcodeexec

https://github.com/csandker/inMemoryShellcode

Powershell Shellcode Attack

https://github.com/praetorian-inc/pentestly/blob/master/scripts/Invoke-Shellcode.ps1

https://www.trustedsec.com/blog/native-powershell-x86-shellcode-injection-on-64-bit-platforms/

https://tstillz.medium.com/analyzing-obfuscated-powershell-with-shellcode-1b6cb8ab5ab0

https://cybergeeks.tech/powershell-scripts-used-to-run-malicious-shellcode-reverse-shell-vs-bind-shell/

https://pentestlab.blog/tag/shellcode/

https://gist.github.com/mattifestation/0fb1f24778f1978b8e4e

https://www.defcon.org/images/defcon-21/dc-21-presentations/Bialek/DEFCON-21-Bialek-PowerPwning-Post-Exploiting-by-Overpowering-Powershell.pdf

https://redteaming.co.uk/2020/07/05/poshc2-shellcode-and-binary-patching/

https://cybergeeks.tech/powershell-scripts-used-to-run-malicious-shellcode-reverse-shell-vs-bind-shell

Jscript Meterpreter Dropper

https://github.com/hlldz/SpookFlare

https://github.com/Cn33liz/JSMeter

https://sectechno.com/spookflare-tool-to-bypass-client-side-security-measures/

https://khast3x.club/posts/2020-06-27-Cross-Platform-Dropper/

https://www.offensive-security.com/metasploit-unleashed/vbscript-infection-methods/

https://blog.rapid7.com/2018/05/03/hiding-metasploit-shellcode-to-evade-windows-defender/

https://www.hacking.land/2018/05/spookflare-v20-loader-dropper-generator.html

Shellcode Runner C#

https://github.com/HackingThings/SneakyExec

https://gist.github.com/netbiosX/5f19a3e8762b6e3fd25782d8c37b1663

https://www.ired.team/offensive-security/code-execution/using-msbuild-to-execute-shellcode-in-c

https://www.fergonez.net/post/shellcode-csharp

https://hausec.com/2020/10/30/using-a-c-shellcode-runner-and-confuserex-to-bypass-uac-while-evading-av/

Process Injection and Migration

https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All.pdf

https://www.elastic.co/pt/blog/ten-process-injection-techniques-technical-survey-common-and-trending-process

https://attack.mitre.org/techniques/T1055/001/

https://attack.mitre.org/techniques/T1055/

https://blog.cobaltstrike.com/2019/08/21/cobalt-strikes-process-injection-the-details/

https://www.powershellempire.com/?page_id=273

http://blog.carnal0wnage.com/2011/07/process-injection-outside-of-metasploit.html

https://www.itpro.co.uk/security/31080/windows-based-cli-susceptible-to-process-injection-attack

Process Injection and Migration 2

https://www.blackhat.com/presentations/bh-usa-07/Butler_and_Kendall/Presentation/bh-usa-07-butler_and_kendall.pdf

https://i.blackhat.com/USA-19/Thursday/us-19-Kotler-Process-Injection-Techniques-Gotta-Catch-Them-All-wp.pdf

https://i.blackhat.com/eu-19/Thursday/eu-19-Block-Detecting-Un-Intentionally-Hidden-Injected-Code-By-Examining-Page-Table-Entries.pdf

https://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Cerrudo/bh-eu-06-Cerrudo-up.pdf

DLL INJECTION

https://en.wikipedia.org/wiki/DLL_injection

https://www.ired.team/offensive-security/code-injection-process-injection/dll-injection

https://medium.com/@viniciuskmax/execut%C3%A1veis-amig%C3%A1veis-para-receber-ataques-process-hollowing-e-dll-injection-no-windows-ce29c14479f6

https://medium.com/bug-bounty-hunting/dll-injection-attacks-in-a-nutshell-71bc84ac59bd

https://www.apriorit.com/dev-blog/679-windows-dll-injection-for-api-hooks

http://blog.opensecurityresearch.com/2013/01/windows-dll-injection-basics.html

https://github.com/ihack4falafel/DLL-Injection

https://malcomvetter.medium.com/net-process-injection-1a1af00359bc

https://www.andreafortuna.org/2019/03/06/a-simple-windows-code-injection-example-written-in-c/

https://www.youtube.com/watch?v=CAkRsmhO2FI&ab_channel=GuidedHacking

https://github.com/marcin-chwedczuk/dll-inject

https://github.com/enkomio/ManagedInjector

REFLECTIVE DLL INJECTION

https://www.andreafortuna.org/2017/12/08/what-is-reflective-dll-injection-and-how-can-be-detected/

https://github.com/stephenfewer/ReflectiveDLLInjection

https://www.ired.team/offensive-security/code-injection-process-injection/reflective-dll-injection

https://0x00sec.org/t/reflective-dll-injection/3080

https://www.youtube.com/watch?v=p-ufU9W1i7Q&ab_channel=DebasishMandal

https://www.youtube.com/watch?v=ilRJRkMyzlA&ab_channel=DebasishMandal

https://www.youtube.com/watch?v=z9ayytxsItU&ab_channel=BenGreenberg

https://blog.f-secure.com/memory-injection-like-a-boss/

https://i.blackhat.com/USA-20/Thursday/us-20-Chen-Operation-Chimera-APT-Operation-Targets-Semiconductor-Vendors.pdf

https://www.microsoft.com/security/blog/2017/11/13/detecting-reflective-dll-loading-with-windows-defender-atp/

PROCESS HOLLOW

https://github.com/m0n0ph1/Process-Hollowing

https://attack.mitre.org/techniques/T1055/012/

https://www.youtube.com/watch?v=bExOwYRxE2w&ab_channel=MonnappaKA

https://www.youtube.com/watch?v=9L9I1T5QDg4&ab_channel=BlackHat

https://www.ired.team/offensive-security/code-injection-process-injection/process-hollowing-and-pe-image-relocations

https://cysinfo.com/detecting-deceptive-hollowing-techniques/

https://www.blackhat.com/docs/asia-17/materials/asia-17-KA-What-Malware-Authors-Don't-Want-You-To-Know-Evasive-Hollow-Process-Injection-wp.pdf

PROCESS HOLLOW 2

https://3xpl01tc0d3r.blogspot.com/2019/10/process-injection-part-iii.html

http://www.rohitab.com/discuss/topic/42237-understanding-process-hollowing/

https://www.youtube.com/watch?v=SPqD1c6G-U8&ab_channel=CyberDecode

https://www.youtube.com/watch?v=5IyGiEajltM&ab_channel=MohammedAlmodawah

https://github.com/secrary/InjectProc

AV Concepts

https://university.monstercloud.com/cyber-security/types-of-antiviruses/

https://softwarelab.org/what-is-antivirus-software/

https://en.wikipedia.org/wiki/Antivirus_software

https://www.numbones.com/2019/01/antivirus.html

https://www.baboo.com.br/seguranca-digital/conteudo-essencial-seguranca-digital/como-funcionam-os-antivirus/

Metasploit Encoders

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

https://null-byte.wonderhowto.com/how-to/hack-like-pro-metasploit-for-aspiring-hacker-part-5-msfvenom-0159520/

https://securityboulevard.com/2020/02/evading-antivirus-with-better-meterpreter-payloads/

https://www.blackhat.com/presentations/bh-usa-08/Smith_Ames/BH_US_08_Smith_Ames_Meta-Post_Exploitation.pdf

https://www.blackhat.com/presentations/bh-dc-10/Moore_HD/BlackHat-DC-2010-Moore-Metasploit-and-Money-wp.pdf

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

https://www.fireeye.com/blog/threat-research/2019/10/shikata-ga-nai-encoder-still-going-strong.html

https://www.rapid7.com/globalassets/_pdfs/whitepaperguide/rapid7-whitepaper-metasploit-framework-encapsulating-av-techniques.pdf

https://resources.infosecinstitute.com/wp-content/uploads/Advanced-Pentesting-Techniques-with-Metasploit.pdf

AV Signature

obscuresec: Finding Simple AV Signatures with PowerShell (obscuresecurity.blogspot.com)

https://www.lmgsecurity.com/common-antivirus-bypass-techniques/

https://dl.packetstormsecurity.net/papers/bypass/bypassing-av.pdf

https://offs3cg33k.medium.com/antivirus-evasion-bypass-techniques-b547cc51c371

https://null-byte.wonderhowto.com/how-to/hack-like-pro-bypass-antivirus-software-by-disguising-exploits-signature-0141122/

https://medium.com/@bluedenkare/1-click-meterpreter-exploit-chain-with-beef-and-av-amsi-bypass-96b0eb61f1b6

Metasploit Encryptor

https://blog.rapid7.com/2019/11/21/metasploit-shellcode-grows-up-encrypted-and-authenticated-c-shells/

https://github.com/MrMugiwara/Metasploit-Encryption

https://hakin9.org/xeexe-undetectable-xor-encrypting-with-custom-key-fud-metasploit-rat/

https://www.youtube.com/watch?v=qtM0hpv5Vt4&ab_channel=BlackHat

https://thedarksource.com/msfvenom-cheat-sheet-create-metasploit-payloads/

https://hacker.house/lab/windows-defender-bypassing-for-meterpreter/

https://medium.com/@PenTest_duck/offensive-msfvenom-from-generating-shellcode-to-creating-trojans-4be10179bb86

Bypass AV with C#

https://damonmohammadbagher.medium.com/bypass-all-anti-viruses-by-encrypted-payloads-with-c-278654f633f0

https://medium.com/@carlosprincipal1/how-to-bypass-antivirus-av-2020-easy-method-69749892928b

https://www.linkedin.com/pulse/bypass-all-anti-viruses-encrypted-payloads-c-damon-mohammadbagher/

https://www.youtube.com/watch?v=g3Q9Jqi3sis&ab_channel=LoveCrypter

https://github.com/Ch0pin/AVIator

https://github.com/lockfale/DotNetAVBypass-Master

https://dione.lib.unipi.gr/xmlui/bitstream/handle/unipi/12797/Panagopoulos_1727.pdf?sequence=3&isAllowed=y

https://book.hacktricks.xyz/windows/av-bypass

Build bypass AV with C#

https://www.xanthus.io/post/building-an-obfuscator-to-evade-windows-defender

https://s3cur3th1ssh1t.github.io/Customizing_C2_Frameworks/

https://ethicalhackingguru.com/how-to-use-confuser-ex-to-bypass-antivirus/

https://offensivedefence.co.uk/posts/covenant-profiles-templates/

https://cognosec.com/bypassing-symantec-endpoint-protection-for-fun-profit-defense-evasion/

https://github.com/alphaSeclab/anti-av

https://github.com/Techryptic/AV_Bypass

https://0x00sec.org/t/new-av-bypass-techniques/9608

Bypass AV with VBA

https://www.youtube.com/watch?v=UoMzCyB2IvE&ab_channel=MotasemHamdan-CyberSecurityTrainer

https://www.youtube.com/watch?v=9MvakIrbX0Q&ab_channel=MattN

https://www.youtube.com/watch?v=Zl7zWa8au28&ab_channel=Sevagas

https://www.youtube.com/watch?v=m3R3LDIrroQ&ab_channel=Sevagas

http://blog.sevagas.com/?Launch-shellcodes-and-bypass-Antivirus-using-MacroPack-Pro-VBA-payloads

https://medium.com/maverislabs/yet-another-update-to-bypass-amsi-in-vba-19ddf9065c04

https://infosecwriteups.com/fun-with-creating-a-vbs-payload-to-bypass-endpoint-security-and-other-layers-44afd724de1b

https://outflank.nl/blog/2019/04/17/bypassing-amsi-for-vba/

https://github.com/sevagas/macro_pack

https://blog.focal-point.com/how-to-build-obfuscated-macros-for-your-next-social-engineering-campaign

Bypass AV with VBA 2

https://www.certego.net/en/news/advanced-vba-macros/

https://i.blackhat.com/eu-19/Wednesday/eu-19-Lagadec-Advanced-VBA-Macros-Attack-And-Defence-2.pdf

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

https://i.blackhat.com/USA-19/Wednesday/us-19-Bernal-Detecting-Malicious-Files-With-YARA-Rules-As-They-Traverse-the-Network-wp.pdf

https://i.blackhat.com/asia-19/Thu-March-28/bh-asia-Hegt-MS-Office-in-Wonderland.pdf

https://www.blackhat.com/docs/us-16/materials/us-16-Bulazel-AVLeak-Fingerprinting-Antivirus-Emulators-For-Advanced-Malware-Evasion.pdf

https://i.blackhat.com/USA-19/Wednesday/us-19-Burke-ClickOnce-And-Youre-In-When-Appref-Ms-Abuse-Is-Operating-As-Intended-wp.pdf

AMSI Concept

https://docs.microsoft.com/en-us/windows/win32/amsi/antimalware-scan-interface-portal

https://medium.com/@two06/amsi-as-a-service-automating-av-evasion-2e2f54397ff9

https://docs.microsoft.com/en-us/windows/win32/amsi/how-amsi-helps

https://www.blackhat.com/docs/us-16/materials/us-16-Mittal-AMSI-How-Windows-10-Plans-To-Stop-Script-Based-Attacks-And-How-Well-It-Does-It.pdf

AMSI Bypass

https://i.blackhat.com/briefings/asia/2018/asia-18-Tal-Liberman-Documenting-the-Undocumented-The-Rise-and-Fall-of-AMSI.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/us-18/Wed-August-8/us-18-Graeber-Subverting-Sysmon-Application-Of-A-Formalized-Security-Product-Evasion-Methodology-wp.pdf

https://i.blackhat.com/briefings/asia/2018/asia-18-bohannon-invoke_dosfuscation_techniques_for_fin_style_dos_level_cmd_obfuscation.pdf

https://medium.com/@byte_St0rm/adventures-in-the-wonderful-world-of-amsi-25d235eb749c

https://medium.com/@gamer.skullie/bypassing-amsi-with-an-unconventional-powershell-cradle-6bd15a17d8b9

AMSI Bypass 2

https://www.contextis.com/en/blog/amsi-bypass

https://infosecwriteups.com/bypass-amsi-in-powershell-a-nice-case-study-f3c0c7bed24d

https://blog.f-secure.com/hunting-for-amsi-bypasses/

https://blog.securityevaluators.com/creating-av-resistant-malware-part-2-1ba1784064bc

https://enigma0x3.net/2017/07/19/bypassing-amsi-via-com-server-hijacking/

https://github.com/S3cur3Th1sSh1t/Amsi-Bypass-Powershell

https://github.com/rasta-mouse/AmsiScanBufferBypass

https://github.com/0xB455/AmsiBypass

AMSI Bypass 3

https://github.com/0r13lc0ch4v1/HideFromAMSI

https://github.com/Joefreedy/AMSI-Bypass

https://github.com/WayneJLee/CsharpAmsiBypass

https://www.youtube.com/watch?v=0W9wkamknfM&ab_channel=PenTestPartnersLLP

https://www.unma.sk/posts/amsi-bypass/

https://hakin9.org/http-revshell-powershell-reverse-shell-using-http-s-protocol-with-amsi-bypass-and-proxy-aware/

https://blog.ironmansoftware.com/protect-amsi-bypass/

Obfuscation

https://github.com/CBHue/PyFuscation

https://github.com/danielbohannon/Invoke-Obfuscation

https://medium.com/@ammadb/invoke-obfuscation-hiding-payloads-to-avoid-detection-87de291d61d3

https://www.youtube.com/watch?v=uE8IAxM_BhE&ab_channel=Hacktivity-ITSecurityFestival

https://www.youtube.com/watch?v=PMh0_59jD2U&ab_channel=nullcon

https://www.youtube.com/watch?v=1-sb0jXPzjU&ab_channel=CQUREAcademy

https://www.vadesecure.com/en/blog/malware-analysis-understanding-code-obfuscation-techniques

Obfuscation 2

https://www.danielbohannon.com/blog-1/2017/12/2/the-invoke-obfuscation-usage-guide

https://pentestit.com/invoke-obfuscation-powershell-command-script-obfuscator/

https://www.varonis.com/blog/powershell-obfuscation-stealth-through-confusion-part-i/

https://securityintelligence.com/an-example-of-common-string-and-payload-obfuscation-techniques-in-malware/

https://blog.malwarebytes.com/threat-analysis/2013/03/obfuscation-malwares-best-friend/

https://ditrizna.medium.com/red-team-use-case-of-open-source-weaponization-5b22b0e287a5

Obfuscation 3

https://3xpl01tc0d3r.blogspot.com/2020/08/introduction-to-obfuscator.html

https://github.com/r00t-3xp10it/hacking-material-books/blob/master/obfuscation/simple_obfuscation.md

https://thewover.github.io/Introducing-Donut/

https://www.fireeye.com/blog/threat-research/2019/10/staying-hidden-on-the-endpoint-evading-detection-with-shellcode.html

https://res-4.cloudinary.com/eventpower/image/upload/v1/19ncs/presentation_files/sao3ktg3tjrhairwd7hb.pptx.pdf

https://medium.com/@vikrant.navalgund/encoded-obfuscated-shellcode-securitytube-linux-assembly-expert-32-bit-exercise-4-568c5a18149a

Obfuscation 4

https://www.andreafortuna.org/2017/09/06/unibyav-shellcode-obfuscation-using-python/

https://breakdev.org/x86-shellcode-obfuscation-part-1/

https://www.hackingloops.com/msfvenom/#:~:text=Obfuscation%20is%20the%20concept%20that,some%20lesser%20anti%2Dvirus%20software

https://null-byte.wonderhowto.com/how-to/bypass-antivirus-software-by-obfuscating-your-payloads-with-graffiti-0215787/

https://www.youtube.com/watch?v=xNhQMwC0BLo&ab_channel=NullByte

https://www.youtube.com/watch?v=BNrGd55TBio&ab_channel=graylagx2

https://www.youtube.com/watch?v=Tl4zUQ9u1lg&ab_channel=portalmafiacom

https://www.hak5.org/gear/duck/optimizing-and-obfuscating-payloads-usb-rubber-ducky-101

Obfuscation 5

https://www.youtube.com/watch?v=mJZCNqcO10A&ab_channel=RedTeamVillage

https://www.youtube.com/watch?v=umN1wV-TzW4&ab_channel=BHack

https://www.youtube.com/watch?v=0SvX6F80qg8&ab_channel=BlackHat

https://www.youtube.com/watch?v=x97ejtv56xw&ab_channel=BlackHat

https://www.youtube.com/watch?v=l5sMPGjtKn0&ab_channel=BlackHat

https://www.youtube.com/watch?v=mej5L9PE1fs&ab_channel=BlackHat

https://www.youtube.com/watch?v=iva16Bg5imQ&ab_channel=Christiaan008

https://www.youtube.com/watch?v=v7XcyCjUTWk&ab_channel=DEFCONConference

https://www.youtube.com/watch?v=0RADvfJysuA&ab_channel=JohnHammond

Powershell Unmanaged

https://github.com/leechristensen/UnmanagedPowerShell

https://www.optiv.com/explore-optiv-insights/blog/unmanaged-powershell-binaries-and-endpoint-protection

https://www.youtube.com/watch?v=7tvfb9poTKg&ab_channel=RaphaelMudge

https://blog.cobaltstrike.com/2016/05/18/cobalt-strike-3-3-now-with-less-powershell-exe/

https://adsecurity.org/?p=2921

Powershell CLM Bypass

https://www.secjuice.com/powershell-constrainted-language-mode-bypass-using-runspaces/

https://www.mdsec.co.uk/2018/09/applocker-clm-bypass-via-com/

https://github.com/padovah4ck/PSByPassCLM

https://www.ired.team/offensive-security/code-execution/powershell-constrained-language-mode-bypass

https://blog.netspi.com/15-ways-to-bypass-the-powershell-execution-policy/

https://www.linkedin.com/pulse/powershell-bypass-constrained-language-mode-rotem-simhi/?articleId=6610158125347549184

Conclusion

- This book aims to help you in your studies, whether for certification, research or even acquire more skills.

- Several materials were used and consulted to create this small PDF that several parts. I can say that it is based on materials from EC-COUNCIL, Offensive Security, eLearnsecurity, SANS.