

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/POWER_SHELL](https://github.com/LazyWinAdmin/PowerShell) (SCRIPTS)
- [HTTPS://GITHUB.COM/CLYMB3R/POWER_SHELL](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/APREND-POWER_SHELL-DO-ZERO/](https://www.udemy.com/course/aprenda-powershell-do-zero/)
- [HTTPS://WWW.UDEMY.COM/COURSE/AUTOMATIZANDO-ADMINISTRACAO-COM-POWER_SHELL-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=METASPLOITATIO
N](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!