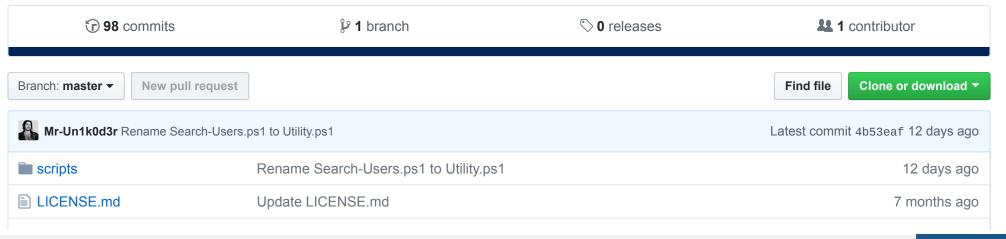


Powershell script that search through the Windows event logs for specific user



README.md

Red Team Powershell Scripts

```
Search-EventForUser.ps1: Powershell script that search through the Windows event logs for specific user(s) Search-FullNameToSamAccount.ps1: Full name to SamAccountName Search-UserPassword.ps1: Search LDAP for userPassword field Remote-WmiExecute.ps1: Execute command remotely using WMI Take-Screenshot.ps1: Take a screenshot (PNG) Get-BrowserHomepage.ps1: Get browser homepage Get-IEBookmarks.ps1: List all Internet Explorer bookmarks URLs Invoke-ADPasswordBruteForce.ps1: Test users password Utility.ps1: Contain several cmdlets
```

Search-EventForUser.ps1 Usage

```
module-import .\Search-EventForUser.ps1; Search-EventForUser -TargetUser "MrUn1k0d3r"
module-import .\Search-EventForUser.ps1; "MrUn1k0d3r" | Search-EventForUser
module-import .\Search-EventForUser.ps1; Search-EventForUser -TargetUser MrUn1k0d3r -ComputerName DC01
module-import .\Search-EventForUser.ps1; Search-EventForUser -TargetUser MrUn1k0d3r -FindDC true
```

```
module-import .\Search-EventForUser.ps1; "god", "mom" | Search-EventForUser -FindDC true
module-import .\Search-EventForUser.ps1; "god", "mom" | Search-EventForUser -FindDC true -Username DOMAIN\a
```

The -User parameter support single user or a list of users from pipeline

Search-FullNameToSamAccount.ps1 Usage

```
module-import .\Search-FullNameToSamAccount.ps1; Search-FullNameToSamAccount -Filter *god*
module-import .\Search-FullNameToSamAccount.ps1; "god", "mom" | Search-FullNameToSamAccount
```

Search-UserPassword.ps1 Usage

```
module-import .\Search-UserPassword.ps1; Search-UserPassword -Username *god*
module-import .\Search-UserPassword.ps1; "god", "mom" | Search-UserPassword
```

Remote-WmiExecute.ps1 Usage

```
module-import .\Remote-WmiExecute.ps1; Remote-WmiExecute -ComputerName victim01 -Payload "cmd.exe /c whoami
```

Take-Screenshot.ps1 Usage

module-import .\Take-Screenshot.ps1; Take-Screenshot -Path C:\test.png

Get-BrowserHomepage.ps1 Usage

module-import .\Get-BrowserHomepage.ps1; Get-BrowserHomepage

Get-IEBookmarks.ps1 Usage

module-import .\Get-IEBookmarks.ps1; Get-IEBookmarks

Invoke-ADPasswordBruteForce.ps1 Usage

```
module-import .\Invoke-ADPasswordBruteForce; Invoke-ADPasswordBruteForce -Username "mr.un1k0d3r" -Password
module-import .\Invoke-ADPasswordBruteForce; "neo", "morpheus" | Invoke-ADPasswordBruteForce -Password "pass
module-import .\Invoke-ADPasswordBruteForce; "neo", "morpheus" | Invoke-ADPasswordBruteForce -Password "pass
```

Utility.ps1

Contain de following cmdlets

Search-EventForUser

Search-FullNameToSamAccount

Ldap-GetProperty

Search-UserPassword

Dump-UserEmail

Dump-Computers

Dump-UserName

Todo

- 1. Remote-WmiExecute.ps1:
- Improve errors handling (Access Denied etc...)
- 2. Take-Screenshot.ps1:
- Handle multiple screens

Credit

Mr.Un1k0d3r RingZer0 Team