Sign in

This repository has been archived by the owner on Jan 21, 2021. It is now read-only.

PowerShellMafia / **PowerSploit** Public archive

Notifications | Fork 4.6k | Star 11.9k

Code | Issues 67 | Pull requests 37 | Actions | Projects | Security | Insights

PowerSplolit / **Recon** /

Name	Last commit message	Last commit date
..		
Dictionaries		
Get-ComputerDetail.ps1		
Get-HttpStatus.ps1		
Invoke-CompareAttributesForClass.ps1		
Invoke-Portscan.ps1		
Invoke-ReverseDnsLookup.ps1		
PowerView.ps1		
README.md		
Recon.psd1		
Recon.psm1		

README.md

To install this module, drop the entire Recon folder into one of your module directories. The default PowerShell module paths are listed in the $Env:PSModulePath environment variable.

The default per-user module path is: "$Env:HomeDrive$Env:HOMEPATH\Documents\WindowsPowerShell\Modules" The default computer-level module path is: "$Env:windir\System32\WindowsPowerShell\v1.0\Modules"

To use the module, type `Import-Module Recon`

To see the commands imported, type `Get-Command -Module Recon`

For help on each individual command, Get-Help is your friend.

Note: The tools contained within this module were all designed such that they can be run individually. Including them in a module simply lends itself to increased portability.

PowerView

PowerView is a PowerShell tool to gain network situational awareness on Windows domains. It contains a set of pure-PowerShell replacements for various windows "net *" commands, which utilize PowerShell AD hooks and underlying Win32 API functions to perform useful Windows domain functionality.

It also implements various useful metafunctions, including some custom-written user-hunting functions which will identify where on the network specific users are logged into. It can also check which machines on the domain the current user has local administrator access on. Several functions for the enumeration and abuse of domain trusts also exist. See function descriptions for appropriate usage and available options. For detailed output of underlying functionality, pass the -Verbose or -Debug flags.

For functions that enumerate multiple machines, pass the -Verbose flag to get a progress status as each host is enumerated. Most of the "meta" functions accept an array of hosts from the pipeline.

Misc Functions:

```
Export-PowerViewCSV             -   thread-safe CSV append
Resolve-IPAddress               -   resolves a hostname to an IP
ConvertTo-SID                   -   converts a given user/group name to a security
Convert-ADName                  -   converts object names between a variety of for
ConvertFrom-UACValue            -   converts a UAC int value to human readable for
Add-RemoteConnection            -   pseudo "mounts" a connection to a remote path
```

```
Remove-RemoteConnection         -   destroys a connection created by New-RemoteConn
Invoke-UserImpersonation        -   creates a new "runas /netonly" type logon and
Invoke-RevertToSelf             -   reverts any token impersonation
Get-DomainSPNTicket             -   request the kerberos ticket for a specified ser
Invoke-Kerberoast               -   requests service tickets for kerberoast-able a
Get-PathAcl                     -   get the ACLs for a local/remote file path with
```

Domain/LDAP Functions:

```
Get-DomainDNSZone               -   enumerates the Active Directory DNS zones for
Get-DomainDNSRecord             -   enumerates the Active Directory DNS records fo
Get-Domain                      -   returns the domain object for the current (or
Get-DomainController            -   return the domain controllers for the current
Get-Forest                      -   returns the forest object for the current (or
Get-ForestDomain                -   return all domains for the current (or specifi
Get-ForestGlobalCatalog         -   return all global catalogs for the current (or
Find-DomainObjectPropertyOutlier-   inds user/group/computer objects in AD that ha
Get-DomainUser                  -   return all users or specific user objects in A
New-DomainUser                  -   creates a new domain user (assuming appropriat
Set-DomainUserPassword          -   sets the password for a given user identity an
Get-DomainUserEvent             -   enumerates account logon events (ID 4624) and
Get-DomainComputer              -   returns all computers or specific computer obj
Get-DomainObject                -   returns all (or specified) domain objects in A
Set-DomainObject                -   modifies a gven property for a specified activ
Get-DomainObjectAcl             -   returns the ACLs associated with a specific ac
Add-DomainObjectAcl             -   adds an ACL for a specific active directory ob
Find-InterestingDomainAcl       -   finds object ACLs in the current (or specified
Get-DomainOU                    -   search for all organization units (OUs) or spe
Get-DomainSite                  -   search for all sites or specific site objects
Get-DomainSubnet                -   search for all subnets or specific subnets obj
Get-DomainSID                   -   returns the SID for the current domain or the
Get-DomainGroup                 -   return all groups or specific group objects in
New-DomainGroup                 -   creates a new domain group (assuming appropria
Get-DomainManagedSecurityGroup  -   returns all security groups in the current (or
Get-DomainGroupMember           -   return the members of a specific domain group
Add-DomainGroupMember           -   adds a domain user (or group) to an existing d
Get-DomainFileServer            -   returns a list of servers likely functioning a
Get-DomainDFSShare              -   returns a list of all fault-tolerant distribut
```

GPO functions

```
Get-DomainGPO                           -   returns all GPOs or specific GPO objec
Get-DomainGPOLocalGroup                 -   returns all GPOs in a domain that modi
Get-DomainGPOUserLocalGroupMapping      -   enumerates the machines where a specif
Get-DomainGPOComputerLocalGroupMapping  -   takes a computer (or GPO) object and d
Get-DomainPolicy                        -   returns the default domain policy or t
```

Computer Enumeration Functions

```
Get-NetLocalGroup                   -   enumerates the local groups on the local (
Get-NetLocalGroupMember             -   enumerates members of a specific local grou
Get-NetShare                        -   returns open shares on the local (or a rem
Get-NetLoggedon                     -   returns users logged on the local (or a re
Get-NetSession                      -   returns session information for the local
Get-RegLoggedOn                     -   returns who is logged onto the local (or a
Get-NetRDPSession                   -   returns remote desktop/session information
Test-AdminAccess                    -   rests if the current user has administrati
Get-NetComputerSiteName             -   returns the AD site where the local (or a
Get-WMIRegProxy                     -   enumerates the proxy server and WPAD conen
Get-WMIRegLastLoggedOn              -   returns the last user who logged onto the
Get-WMIRegCachedRDPConnection       -   returns information about RDP connections
Get-WMIRegMountedDrive              -   returns information about saved network mou
Get-WMIProcess                      -   returns a list of processes and their owne
Find-InterestingFile                -   searches for files on the given path that
```

Threaded 'Meta'-Functions

```
Find-DomainUserLocation             -   finds domain machines where specific users
Find-DomainProcess                  -   finds domain machines where specific proce
Find-DomainUserEvent                -   finds logon events on the current (or remo
Find-DomainShare                    -   finds reachable shares on domain machines
Find-InterestingDomainShareFile     -   searches for files matching specific crite
Find-LocalAdminAccess               -   finds machines on the local domain where t
Find-DomainLocalGroupMember         -   enumerates the members of specified local
```

Domain Trust Functions:

```
Get-DomainTrust                     -   returns all domain trusts for the current
Get-ForestTrust                     -   returns all forest trusts for the current
Get-DomainForeignUser               -   enumerates users who are in groups outside
```

```
Get-DomainForeignGroupMember         -   enumerates groups with users outside of th
Get-DomainTrustMapping               -   this function enumerates all trusts for th
```