PowerSploit/Recon at master · PowerShellMafia/PowerSploit

By HarmJ0y

Archived: 2026-04-05 20:28:44 UTC

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 identifier (SID)
Convert-ADName                  -   converts object names between a variety of formats
ConvertFrom-UACValue            -   converts a UAC int value to human readable form
Add-RemoteConnection            -   pseudo "mounts" a connection to a remote path using the specified credential
```

```
Remove-RemoteConnection         -   destroys a connection created by New-RemoteConnection
Invoke-UserImpersonation        -   creates a new "runas /netonly" type logon and impersonates the token
Invoke-RevertToSelf             -   reverts any token impersonation
Get-DomainSPNTicket             -   request the kerberos ticket for a specified service principal name (SPN)
Invoke-Kerberoast               -   requests service tickets for kerberoast-able accounts and returns extracted
Get-PathAcl                     -   get the ACLs for a local/remote file path with optional group recursion
```

Domain/LDAP Functions:

```
 Get-DomainDNSZone               -   enumerates the Active Directory DNS zones for a given domain
Get-DomainDNSRecord             -   enumerates the Active Directory DNS records for a given zone
Get-Domain                      -   returns the domain object for the current (or specified) domain
Get-DomainController            -   return the domain controllers for the current (or specified) domain
Get-Forest                      -   returns the forest object for the current (or specified) forest
Get-ForestDomain                -   return all domains for the current (or specified) forest
Get-ForestGlobalCatalog         -   return all global catalogs for the current (or specified) forest
Find-DomainObjectPropertyOutlier-   inds user/group/computer objects in AD that have 'outlier' properties set
Get-DomainUser                  -   return all users or specific user objects in AD
New-DomainUser                  -   creates a new domain user (assuming appropriate permissions) and returns the
Set-DomainUserPassword          -   sets the password for a given user identity and returns the user object
Get-DomainUserEvent             -   enumerates account logon events (ID 4624) and Logon with explicit credential
Get-DomainComputer              -   returns all computers or specific computer objects in AD
Get-DomainObject                -   returns all (or specified) domain objects in AD
Set-DomainObject                -   modifies a gven property for a specified active directory object
Get-DomainObjectAcl             -   returns the ACLs associated with a specific active directory object
Add-DomainObjectAcl             -   adds an ACL for a specific active directory object
Find-InterestingDomainAcl       -   finds object ACLs in the current (or specified) domain with modification rig
Get-DomainOU                    -   search for all organization units (OUs) or specific OU objects in AD
Get-DomainSite                  -   search for all sites or specific site objects in AD
Get-DomainSubnet                -   search for all subnets or specific subnets objects in AD
Get-DomainSID                   -   returns the SID for the current domain or the specified domain
Get-DomainGroup                 -   return all groups or specific group objects in AD
New-DomainGroup                 -   creates a new domain group (assuming appropriate permissions) and returns th
Get-DomainManagedSecurityGroup  -   returns all security groups in the current (or target) domain that have a ma
Get-DomainGroupMember           -   return the members of a specific domain group
Add-DomainGroupMember           -   adds a domain user (or group) to an existing domain group, assuming appropri
Get-DomainFileServer            -   returns a list of servers likely functioning as file servers
Get-DomainDFSShare              -   returns a list of all fault-tolerant distributed file systems for the curren
```

GPO functions

```
 Get-DomainGPO                       -   returns all GPOs or specific GPO objects in AD
Get-DomainGPOLocalGroup             -   returns all GPOs in a domain that modify local group memberships thr
Get-DomainGPOUserLocalGroupMapping  -   enumerates the machines where a specific domain user/group is a memb
```

```
Get-DomainGPOComputerLocalGroupMapping  -   takes a computer (or GPO) object and determines what users/groups ar
Get-DomainPolicy                        -   returns the default domain policy or the domain controller policy fo
```

Computer Enumeration Functions

```
 Get-NetLocalGroup                   -   enumerates the local groups on the local (or remote) machine
Get-NetLocalGroupMember             -   enumerates members of a specific local group on the local (or remote) ma
Get-NetShare                        -   returns open shares on the local (or a remote) machine
Get-NetLoggedon                     -   returns users logged on the local (or a remote) machine
Get-NetSession                      -   returns session information for the local (or a remote) machine
Get-RegLoggedOn                     -   returns who is logged onto the local (or a remote) machine through enume
Get-NetRDPSession                   -   returns remote desktop/session information for the local (or a remote) m
Test-AdminAccess                    -   rests if the current user has administrative access to the local (or a r
Get-NetComputerSiteName             -   returns the AD site where the local (or a remote) machine resides
Get-WMIRegProxy                     -   enumerates the proxy server and WPAD conents for the current user
Get-WMIRegLastLoggedOn              -   returns the last user who logged onto the local (or a remote) machine
Get-WMIRegCachedRDPConnection       -   returns information about RDP connections outgoing from the local (or re
Get-WMIRegMountedDrive              -   returns information about saved network mounted drives for the local (or
Get-WMIProcess                      -   returns a list of processes and their owners on the local or remote mach
Find-InterestingFile                -   searches for files on the given path that match a series of specified cr
```

Threaded 'Meta'-Functions

```
 Find-DomainUserLocation             -   finds domain machines where specific users are logged into
Find-DomainProcess                  -   finds domain machines where specific processes are currently running
Find-DomainUserEvent                -   finds logon events on the current (or remote domain) for the specified u
Find-DomainShare                    -   finds reachable shares on domain machines
Find-InterestingDomainShareFile     -   searches for files matching specific criteria on readable shares in the
Find-LocalAdminAccess               -   finds machines on the local domain where the current user has local admi
Find-DomainLocalGroupMember         -   enumerates the members of specified local group on machines in the domai
```

Domain Trust Functions:

```
 Get-DomainTrust                     -   returns all domain trusts for the current domain or a specified domain
Get-ForestTrust                     -   returns all forest trusts for the current forest or a specified forest
Get-DomainForeignUser               -   enumerates users who are in groups outside of the user's domain
Get-DomainForeignGroupMember        -   enumerates groups with users outside of the group's domain and returns e
Get-DomainTrustMapping              -   this function enumerates all trusts for the current domain and then enum
```

Source: https://github.com/PowerShellMafia/PowerSploit/tree/master/Recon