

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

Q

Sign in

Sign up

This repository has been archived by the owner on Jan 21, 2021.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

Files

master

Go to file

> AntivirusBypass

> CodeExecution

> Exfiltration

> Mayhem

> Persistence

> Privesc

> Recon

> Dictionaries

Get-ComputerDetail.ps1

Get-HttpStatus.ps1

Invoke-CompareAttributesForCl...

Invoke-Portscan.ps1

Invoke-ReverseDnsLookup.ps1

PowerView.ps1

README.md

Recon.psd1

Recon.psm1

> ScriptModification

> Tests

> docs

.gitignore

LICENSE

PowerSploit.psd1

PowerSploit.psm1

PowerSploit.pssproj

PowerSploit.sln

README.md

mkdocs.yml

PowerSploit / Recon

HarmJ0y swapped default kerberoasting output formatsf94a5d2 · 6 years agoHistory

Name	Last commit message	Last commit date
..		
Dictionaries	Added additional recon dictionaries	12 years ago
Get-ComputerDetail.ps1	For ./Recon/ :	8 years ago
Get-HttpStatus.ps1	For ./Recon/ :	8 years ago
Invoke-CompareAttributesForClas...	Added Invoke-CompareAttributesForClas...	8 years ago
Invoke-Portscan.ps1	Merge pull request #243 from cfalta/master	7 years ago
Invoke-ReverseDnsLookup.ps1	For ./Recon/ :	8 years ago
PowerView.ps1	swapped default kerberoasting output for...	6 years ago
README.md	Added Set-DomainUserPassword to reset ...	8 years ago
Recon.psd1	For ./Recon/ :	8 years ago
Recon.psm1	Normalized all scripts to ASCII encoding	11 years ago

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

Page 1 of 3


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 SID	
Convert-ADName	-	converts object names between a variety of formats	
ConvertFrom-UACValue	-	converts a UAC int value to human readable	
Add-RemoteConnection	-	pseudo "mounts" a connection to a remote machine	
Remove-RemoteConnection	-	destroys a connection created by New-RemoteConnection	
Invoke-UserImpersonation	-	creates a new "runas /netonly" type impersonation	
Invoke-RevertToSelf	-	reverts any token impersonation	
Get-DomainSPNTicket	-	request the kerberos ticket for a specific service	
Invoke-Kerberoast	-	requests service tickets for kerberos accounts	
Get-PathAcl	-	get the ACLs for a local/remote file	

### Domain/LDAP Functions:

Get-DomainDNSZone	-	enumerates the Active Directory DNS zones	
Get-DomainDNSRecord	-	enumerates the Active Directory DNS records	
Get-Domain	-	returns the domain object for the current domain	
Get-DomainController	-	return the domain controllers for the current domain	
Get-Forest	-	returns the forest object for the current forest	
Get-ForestDomain	-	return all domains for the current forest	
Get-ForestGlobalCatalog	-	return all global catalogs for the current forest	
Find-DomainObjectPropertyOutlier	-	finds user/group/computer objects in the domain with unusual properties	
Get-DomainUser	-	return all users or specific user objects	
New-DomainUser	-	creates a new domain user (assuming password is provided)	
Set-DomainUserPassword	-	sets the password for a given user in the domain	
Get-DomainUserEvent	-	enumerates account logon events (ID 4624)	
Get-DomainComputer	-	returns all computers or specific computer objects	
Get-DomainObject	-	returns all (or specified) domain objects	
Set-DomainObject	-	modifies a given property for a specific domain object	
Get-DomainObjectAcl	-	returns the ACLs associated with a specific domain object	
Add-DomainObjectAcl	-	adds an ACL for a specific active directory object	
Find-InterestingDomainAcl	-	finds object ACLs in the current domain	
Get-DomainOU	-	search for all organization units (OUs) in the domain	
Get-DomainSite	-	search for all sites or specific site objects	
Get-DomainSubnet	-	search for all subnets or specific subnet objects	
Get-DomainSID	-	returns the SID for the current domain	
Get-DomainGroup	-	return all groups or specific group objects	
New-DomainGroup	-	creates a new domain group (assuming password is provided)	
Get-DomainManagedSecurityGroup	-	returns all security groups in the current domain	
Get-DomainGroupMember	-	return the members of a specific domain group	
Add-DomainGroupMember	-	adds a domain user (or group) to an existing domain group	
Get-DomainFileServer	-	returns a list of servers likely functioning as file servers	
Get-DomainDFSShare	-	returns a list of all fault-tolerant distributed file shares	

### GPO functions

Get-DomainGPO	-	returns all GPOs or specific GPO	
Get-DomainGPOLocalGroup	-	returns all GPOs in a domain	
Get-DomainGPOUserLocalGroupMapping	-	enumerates the machines where a GPO is applied	
Get-DomainGPOComputerLocalGroupMapping	-	takes a computer (or GPO) object and returns the GPOs it is applied to	
Get-DomainPolicy	-	returns the default domain policy	

### Computer Enumeration Functions

Get-NetLocalGroup	- enumerates the local groups on t
Get-NetLocalGroupMember	- enumerates members of a specific
Get-NetShare	- returns open shares on the local
Get-NetLoggedon	- returns users logged on the loca
Get-NetSession	- returns session information for
Get-RegLoggedOn	- returns who is logged onto the l
Get-NetRDPSession	- returns remote desktop/session i
Test-AdminAccess	- rests if the current user has ad
Get-NetComputerSiteName	- returns the AD site where the lo
Get-WMIRegProxy	- enumerates the proxy server and
Get-WMIRegLastLoggedOn	- returns the last user who logged
Get-WMIRegCachedRDPConnection	- returns information about RDP co
Get-WMIRegMountedDrive	- returns information about saved
Get-WMIProcess	- returns a list of processes and
Find-InterestingFile	- searches for files on the given

### Threaded 'Meta'-Functions

Find-DomainUserLocation	- finds domain machines where spec
Find-DomainProcess	- finds domain machines where spec
Find-DomainUserEvent	- finds logon events on the curren
Find-DomainShare	- finds reachable shares on domain
Find-InterestingDomainShareFile	- searches for files matching spec
Find-LocalAdminAccess	- finds machines on the local doma
Find-DomainLocalGroupMember	- enumerates the members of specif

### Domain Trust Functions:

Get-DomainTrust	- returns all domain trusts for th
Get-ForestTrust	- returns all forest trusts for th
Get-DomainForeignUser	- enumerates users who are in grou
Get-DomainForeignGroupMember	- enumerates groups with users out
Get-DomainTrustMapping	- this function enumerates all tru