

and the rest of the module files at this path:

C:\Windows\System32\WindowsPowerShell\v1.0\Modules\Act
iveDirectory\

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

```
Privilege Name Description State

SeShutdownPrivilege Shut down the system Disabled SeChangeNotifyPrivilege Remove computer from docking station Disabled SelndockPrivilege Remove computer from docking station Disabled SelnceaseNorkingSetPrivilege Increase a process working set Disabled SelnceaseNorkingSetPrivilege Change the time zone Disabled SelnceaseNorkingSetPrivilege Change a process working set Disabled SelnceaseNorkingSetPrivilege Change the time zone Disabled SelnceaseNorkingSetPrivilege Change the
```

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/ADModule/master/Import-

PowerShell 100.0%

ActiveDirectory.ps1');Import-ActiveDirectory

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

Terms Privacy Security Status Docs Contact Manage cookies Do not share my personal information