



samratashok / ADModule Public



Code






&lt;



- \_\_\_\_\_
- \_\_\_\_\_
- \_\_\_\_\_

## Page 1 of 3

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-00C04FB98AF9}, 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/ADModule/master/Import-

● PowerShell 100.0%

## 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/Import-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={31B2F340-0160-11D2-945F-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

