

PINNED

to Domain Compromise

Pass the Hash with Machine\$ Accounts

BloodHound with Kali Linux: 101

Backdooring AdminSDHolder for Persistence

Active Directory Enumeration with AD Module without RSAT or Admin Privileges

Enumerating AD Object Permissions with dscls

Active Directory Password Spraying

Active Directory Lab with Hyper-V and PowerShell

ADCS + PetitPotam NTLM Relay: Obtaining krbtgt Hash with Domain Controller Machine Certificate

From Misconfigured Certificate Template to Domain Admin

Shadow Credentials

Abusing Trust Account\$: Accessing Resources on a Trusted Domain from a Trusting Domain

OFFENSIVE SECURITY

Red Team Infrastructure

Initial Access

Code Execution

Code & Process Injection

Defense Evasion

Enumeration and Discovery

Privilege Escalation

Credential Access & Dumping

Lateral Movement

Persistence

Exfiltration

REVERSING, FORENSICS & MISC

Internals

Cloud

Neo4j

Dump Virtual Box Memory

AES Encryption Using Crypto++ .lib in Visual Studio C++

Reversing Password Checking Routine

Active Directory Enumeration with AD Module without RSAT or Admin Privileges

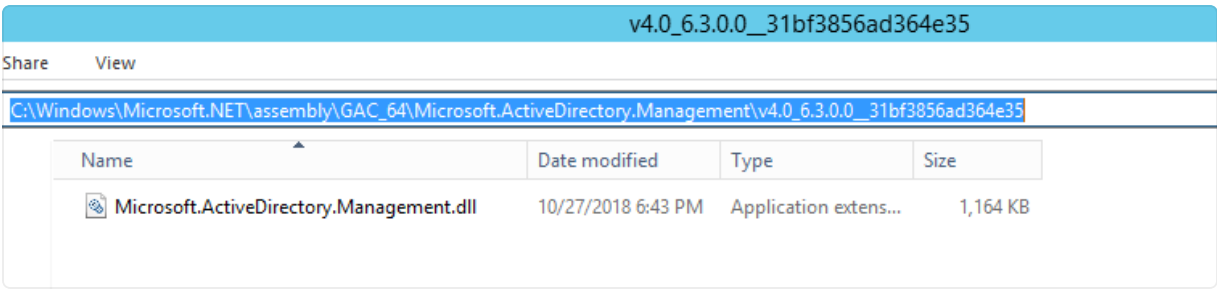
This lab shows how it is possible to use Powershell to enumerate Active Directory with Powershell's `Active Directory` module on a domain joined machine that does not have Remote Server Administration Toolkit (RSAT) installed on it. Installing RSAT requires admin privileges and is actually what makes the AD Powershell module available and this lab shows how to bypass this obstacle.

Execution

The secret to being able to run AD enumeration commands from the AD Powershell module on a system without RSAT installed, is the DLL located in

```
C:\Windows\Microsoft.NET\assembly\GAC_64\Microsoft.ActiveDirectory.Managem
ent
```

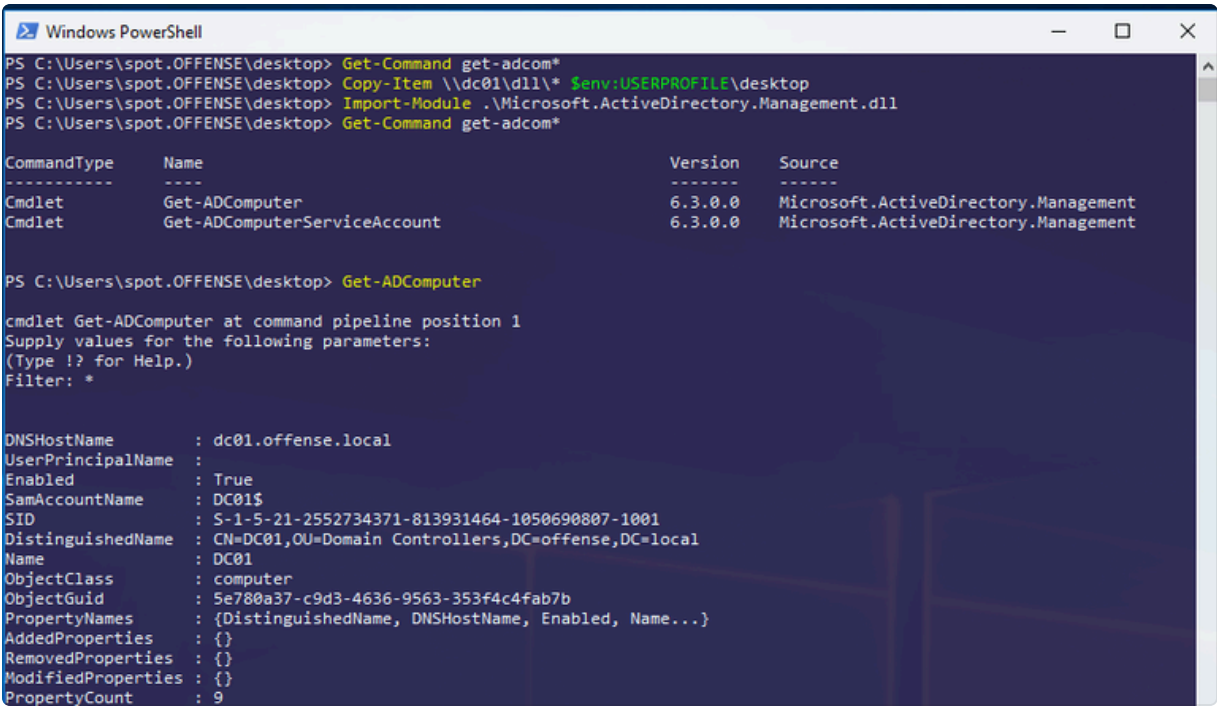
on a system that **has the RSAT** installed:



This means that we can just grab the DLL from the system with RSAT and drop it on the system we want to enumerate from (that does not have RSAT installed) and simply import that DLL as a module:

```
Import-Module .\Microsoft.ActiveDirectory.Management.dll
```

Note how before we import the module, `Get-Command get-adcom*` returns nothing, but that changes once we import the module:



As mentioned earlier, this does

This site uses cookies to deliver its service and to analyse traffic. By browsing this site, you accept the [privacy policy](#).

AcceptReject

```
Windows PowerShell
PS C:\Users\spot.OFFENSE\desktop> net user spot /domain
The request will be processed at a domain controller for domain offense.local.

User name                spot
Full Name                spot
Comment
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        03/01/2019 20:10:52
Password expires         Never
Password changeable      03/01/2019 20:10:52
Password required        Yes
User may change password Yes


Workstations allowed     All
Logon script
User profile
Home directory
Last logon               03/02/2019 14:17:16

Logon hours allowed      All

Local Group Memberships
Global Group memberships *Domain Users
The command completed successfully.

PS C:\Users\spot.OFFENSE\desktop>
```

Download Management.DLL


1MB

Microsoft.ActiveDirectory.Management.dll

Microsoft.ActiveDirectory.Management.dll

Reference

<https://scriptdotsh.com/index.php/2019/01/01/active-directory-penetration-doj-ad-environment-enumeration-1/>
scriptdotsh.com

>

Previous

< Backdooring AdminSDHolder for Persistence

Next

Enumerating AD Object Permissions with dscls >

Last updated 5 years ago

This site uses cookies to deliver its service and to analyse traffic. By browsing this site, you accept the [privacy policy](#).

X