【AD】【列舉】PowerView.ps1

下載：

https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

教學：

https://bookstack.treemanou.com/books/treemanoscp/page/ch21-active-directory-introduction-and-enumeration#bkmrk-21.3-manual-enumerat

Get-NetComputer

```
################################################
# 載入記憶體
PS C:\Tools> Import-Module .\PowerView.ps1

################################################
# 提供有關域的基本信息
PS C:\Tools> Get-NetDomain

Forest                  : corp.com
DomainControllers       : {DC1.corp.com}
Children                : {}
DomainMode              : Unknown
DomainModeLevel         : 7
Parent                  :
PdcRoleOwner            : DC1.corp.com
RidRoleOwner            : DC1.corp.com
InfrastructureRoleOwner : DC1.corp.com
Name                    : corp.com

################################################
# 獲取域中所有用戶的列表
PS C:\Tools> Get-NetUser

logoncount            : 113
iscriticalsystemobject : True
description           : Built-in account for administering the computer/domain
distinguishedname     : CN=Administrator,CN=Users,DC=corp,DC=com
objectclass           : {top, person, organizationalPerson, user}
lastlogontimestamp    : 9/13/2022 1:03:47 AM
name                  : Administrator
################################################
# 獲取域中所有用戶的列表
PS C:\Tools> Get-NetUser | select cn,pwdlastset,lastlogon

cn            pwdlastset            lastlogon
--            ----------            ---------
Administrator 8/16/2022 5:27:22 PM  9/14/2022 2:37:15 AM
Guest         12/31/1600 4:00:00 PM 12/31/1600 4:00:00 PM
krbtgt        9/2/2022 4:10:48 PM   12/31/1600 4:00:00 PM
dave          9/7/2022 9:54:57 AM   9/14/2022 2:57:28 AM
stephanie     9/2/2022 4:23:38 PM   12/31/1600 4:00:00 PM

PS C:\Tools> Get-NetUser -SPN | select samaccountname,serviceprincipalname

samaccountname serviceprincipalname
-------------- --------------------
krbtgt         kadmin/changepw
iis_service    {HTTP/web04.corp.com, HTTP/web04, HTTP/web04.corp.com:80}

################################################
# 列舉群組
PS C:\Tools> Get-NetGroup | select cn
```

```
cn
--
...
Key Admins

################################################
# 列舉群組("Sales Department")
PS C:\Tools> Get-NetGroup "Sales Department" | select member

member
------
{CN=Development Department,DC=corp,DC=com, CN=pete,CN=Users,
DC=corp,DC=com, CN=stephanie,CN=Users,DC=corp,DC=com}

################################################
# 搜索操作系統和主機名
PS C:\Tools> Get-NetComputer | select dnshostname,operatingsystem,operatingsystemversion

dnshostname       operatingsystem             operatingsystemversion
-----------       ---------------             ----------------------
DC1.corp.com      Windows Server 2022 Standard 10.0 (20348)
web04.corp.com    Windows Server 2022 Standard 10.0 (20348)
FILES04.corp.com  Windows Server 2022 Standard 10.0 (20348)
client74.corp.com Windows 11 Pro               10.0 (22000)
client75.corp.com Windows 11 Pro               10.0 (22000)
CLIENT76.corp.com Windows 10 Pro               10.0 (16299)

################################################
# 掃描網絡，試圖確定我們當前用戶是否在域中的任何計算機上具有管理權限
PS C:\Tools> Find-LocalAdminAccess
client74.corp.com

################################################
# 查找域中的一些機器，看看我們是否能找到任何已登錄的用戶
# 失敗
PS C:\Tools> Get-NetSession -ComputerName web04 -Verbose
VERBOSE: [Get-NetSession] Error: Access is denied
# 成功
PS C:\Tools> Get-NetSession -ComputerName client74
CName       : \\192.168.50.75
UserName    : stephanie
Time        : 8
IdleTime    : 0
ComputerName : client74

################################################
# 查找域中的共享
PS C:\Tools> Find-DomainShare

Name          Type Remark               ComputerName
----          ---- ------               ------------
ADMIN$   2147483648 Remote Admin         DC1.corp.com
C$       2147483648 Default share        DC1.corp.com
IPC$     2147483651 Remote IPC           DC1.corp.com
```

- **Get-ObjectAcl** :列舉ACE（Access Control Entry）
- **Convert-SidToName**: SID 轉換為實際的網域對象名稱

PowerView中使用Get-ObjectAcl來列舉ACE（Access Control Entry）是一種強大的方法，它允許我們查看特定對象的許可權設置。在你的命令中，你正在尋找你自己的用戶帳戶（Identity）的ACE。

讓我們運行下面的命令，看看你自己的帳戶有哪些ACE：

```
# Get-ObjectAcl -Identity {username}
PS C:\Tools> Get-ObjectAcl -Identity stephanie
```

```
PS C:\Tools> Get-ObjectAcl -Identity stephanie

...
ObjectDN               : CN=stephanie,CN=Users,DC=corp,DC=com
ObjectSID              : S-1-5-21-1987370270-658905905-1781884369-1104
ActiveDirectoryRights  : ReadProperty
ObjectAceFlags         : ObjectAceTypePresent
ObjectAceType          : 4c164200-20c0-11d0-a768-00aa006e0529
InheritedObjectAceType : 00000000-0000-0000-0000-000000000000
BinaryLength           : 56
AceQualifier           : AccessAllowed
IsCallback             : False
OpaqueLength           : 0
AccessMask             : 16
SecurityIdentifier     : S-1-5-21-1987370270-658905905-1781884369-553
AceType                : AccessAllowedObject
AceFlags               : None
IsInherited            : False
InheritanceFlags       : None
PropagationFlags       : None
AuditFlags             : None
...
```

輸出的量可能看似龐大，因為我們列舉了每一個授予或拒絕對 Stephanie 某種權限的 ACE。雖然有許多屬性似乎可能有用，但我們主要關心的是在清單 58 的截斷輸出中突顯的那些。

輸出列舉了兩個安全標識符（SID），這是代表 AD 中對象的 5 個唯一值。第一個（位於突顯的 ObjectSID 屬性中）包含值 "S-1-5-21-1987370270-658905905-1781884369-1104"，這相當難以閱讀。為了理解這個 SID，我們可以使用 PowerView 的 Convert-SidToName 命令將其轉換為實際的網域對象名稱：

```
PS C:\Tools> Convert-SidToName S-1-5-21-1987370270-658905905-1781884369-1104
```

```
PS C:\Tools> Convert-SidToName S-1-5-21-1987370270-658905905-1781884369-1104
CORP\stephanie
```

轉換顯示，ObjectSID 屬性中的 SID 屬於我們目前使用的 stephanie 使用者。ActiveDirectoryRights 屬性描述了應用於對象的權限類型。為了找出在這種情況下誰具有 ReadProperty 權限，我們需要將 SecurityIdentifier 的值進行轉換。

讓我們使用 PowerView 將其轉換為一個可讀的名稱：

```
PS C:\Tools> Convert-SidToName S-1-5-21-1987370270-658905905-1781884369-553
CORP\RAS and IAS Servers
```

根據 PowerView，SecurityIdentifier 屬性中的 SID 屬於一個名為 RAS and IAS Servers 的預設 AD 群組。

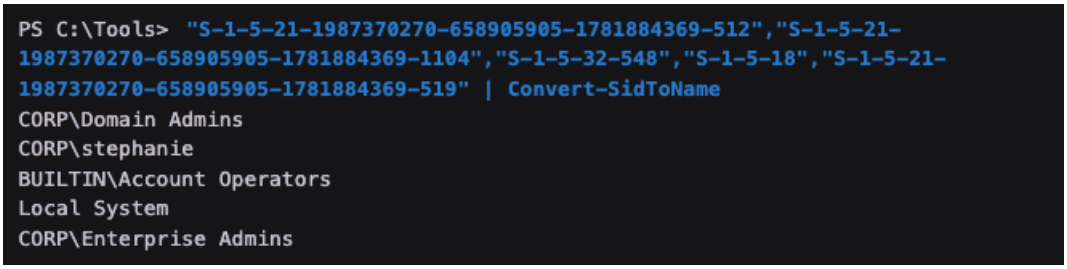
```
PS C:\Tools> Get-ObjectAcl -Identity "Management Department" | ? {$_.ActiveDirectoryRights -eq "GenericAll"} | select SecurityIdentifier,ActiveDirectoryRights
```

```
PS C:\Tools> Get-ObjectAcl -Identity "Management Department" | ?
{$_.ActiveDirectoryRights -eq "GenericAll"} | select
SecurityIdentifier,ActiveDirectoryRights

SecurityIdentifier                            ActiveDirectoryRights
------------------                            ---------------------
S-1-5-21-1987370270-658905905-1781884369-512            GenericAll
S-1-5-21-1987370270-658905905-1781884369-1104           GenericAll
S-1-5-32-548                                            GenericAll
S-1-5-18                                                GenericAll
S-1-5-21-1987370270-658905905-1781884369-519            GenericAll
```

在這個情況下，我們有總共五個對象對 Management Department 對象擁有 GenericAll 權限。為了理解這一點，讓我們將所有的 SID 轉換成實際的名稱：

```
PS C:\Tools> "S-1-5-21-1987370270-658905905-1781884369-512"
,"S-1-5-21-1987370270-658905905-1781884369-1104"
,"S-1-5-32-548","S-1-5-18","S-1-5-21-1987370270-658905905-1781884369-519"
| Convert-SidToName
```



修訂版本 #8
★由 treeman 建立於 11 ﷺQ﷿G﷿﷿ 2023 23:31:47
✎由 treeman 更新於 7 ﷺ@﷿﷿ 2024 19:30:26