

【powershell】PowerView

```
PS C:\Tools> Import-Module .\PowerView.ps1
```

```
PS C:\Tools> Get-NetDomain
PS C:\Tools> Get-NetUser
PS C:\Tools> Get-NetUser "Trade"
PS C:\Tools> Get-NetUser | select cn
PS C:\Tools> Get-NetUser | select cn,pwdlastset,lastlogon
PS C:\Tools> Get-NetGroup | select cn
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}
```

```
PS C:\Tools> Get-NetComputer | select operatingsystem,dnshostname
```

operatingsystem	dnshostname
Windows Server 2022 Standard	DC1.corp.com
Windows Server 2022 Standard	web04.corp.com
Windows Server 2022 Standard	FILES04.corp.com
Windows 11 Pro	client74.corp.com
Windows 11 Pro	client75.corp.com
Windows 10 Pro	CLIENT76.corp.com

```
PS C:\Tools> Get-NetComputer | select dnshostname,operatingsystem,operatingsystemversion
```

```
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)

查看登入帳戶在哪台機器有admin帳號

```
PS C:\Tools> Find-LocalAdminAccess
```

```
client74.corp.com
```

尋找domain機器分享資料夾

```
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
NETLOGON	0	Logon server share	DC1.corp.com
SYSVOL	0	Logon server share	DC1.corp.com
ADMIN\$	2147483648	Remote Admin	web04.corp.com
backup	0		web04.corp.com
C\$	2147483648	Default share	web04.corp.com
IPC\$	2147483651	Remote IPC	web04.corp.com
ADMIN\$	2147483648	Remote Admin	FILES04.corp.com

```
PS C:\Tools> Get-NetSession -ComputerName files04 -v
VERBOSE: [Get-NetSession] Error: Access is denied
```

```
PS C:\Tools> Get-NetSession -ComputerName web04 -v
VERBOSE: [Get-NetSession] Error: Access is denied
```

```
PS C:\Tools> Get-Acl -Path HKLM:SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\ | fl
```

#輸出顯示了擁有FullControl或ReadKey權限的組和用戶，這意味著它們都可以讀取SrvsvcSessionInfo密鑰本身。

```
PS C:\Tools> Get-Acl -Path
HKLM:SYSTEM\CurrentControlSet\Services\LanmanServer\DefaultSecurity\ | fl

Path      :
Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet
\Services\LanmanServer\DefaultSecurity\
Owner     : NT AUTHORITY\SYSTEM
Group     : NT AUTHORITY\SYSTEM
Access    : BUILTIN\Users Allow ReadKey
            BUILTIN\Administrators Allow FullControl
            NT AUTHORITY\SYSTEM Allow FullControl
            CREATOR OWNER Allow FullControl
            APPLICATION PACKAGE AUTHORITY\ALL APPLICATION PACKAGES Allow ReadKey
            S-1-15-3-1024-1065365936-1281604716-3511738428-1654721687-432734479-
3232135806-4053264122-3456934681 Allow ReadKey
```

讓我們運行下面的命令，看看你自己的帳戶有哪些ACE：

```
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
...
```

枚舉SPN的另一種方法是讓PowerView枚舉域中的所有帳戶。為了獲取清晰的SPN列表，我們可以將輸出導入select，並選擇samaccountname和serviceprincipalname屬性：

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

```
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}
```

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。

為了生成清晰且易於管理的輸出，我們將使用 PowerShell 的 -eq 標誌來過濾 ActiveDirectoryRights 屬性，僅顯示等於 GenericAll 的值。然後，我們將結果通道到 select，僅顯示 SecurityIdentifier 和 ActiveDirectoryRights 屬性：

```
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
```

```
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
CORP\Domain Admins
CORP\stephanie
BUILTIN\Account Operators
Local System
CORP\Enterprise Admins
```

我們將使用 PowerView 的 Find-DomainShare 函數來查找域中的共享。我們也可以添加 -CheckShareAccess 標誌以僅顯示對我們可用的共享。但是，暫時我們將跳過此標誌以返回一個完整的列表，包括我們以後可能攻擊的共享。請注意，使用 PowerView 查找共享並列舉它們可能需要一些時間。

```
PS C:\Tools> Find-DomainShare
```

```
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
NETLOGON      0 Logon server share DC1.corp.com
SYSVOL        0 Logon server share DC1.corp.com
ADMIN$        2147483648 Remote Admin      web04.corp.com
backup        0                                     web04.corp.com
C$            2147483648 Default share     web04.corp.com
IPC$          2147483651 Remote IPC        web04.corp.com
ADMIN$        2147483648 Remote Admin      FILES04.corp.com
C             0                                     FILES04.corp.com
C$            2147483648 Default share     FILES04.corp.com
docshare      0 Documentation purposes FILES04.corp.com
IPC$          2147483651 Remote IPC        FILES04.corp.com
Tools         0                                     FILES04.corp.com
Users         0                                     FILES04.corp.com
Windows       0                                     FILES04.corp.com
ADMIN$        2147483648 Remote Admin      client74.corp.com
C$            2147483648 Default share     client74.corp.com
IPC$          2147483651 Remote IPC        client74.corp.com
ADMIN$        2147483648 Remote Admin      client75.corp.com
C$            2147483648 Default share     client75.corp.com
IPC$          2147483651 Remote IPC        client75.corp.com
sharing       0                                     client75.corp.com
```

清單 67 顯示了來自三台不同伺服器和一些客戶端的共享。儘管其中一些是默認的域共享，我們應該調查每個共享，尋找有趣的信息。