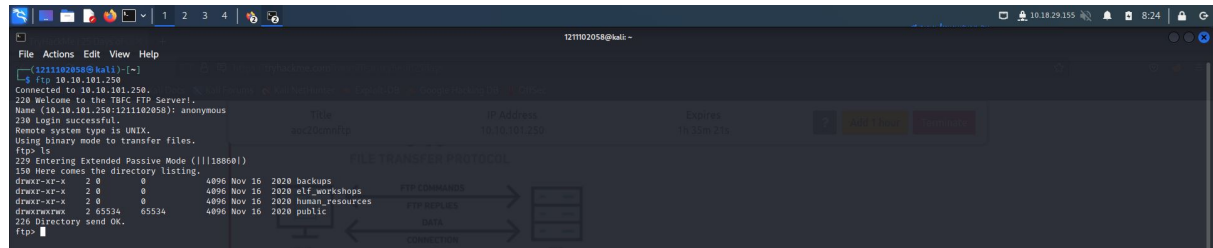


# Day 9 - [Networking] Anyone can be Santa!

Tool used: kali Linux, Firefox, netcat

## Solution/Walkthrough:

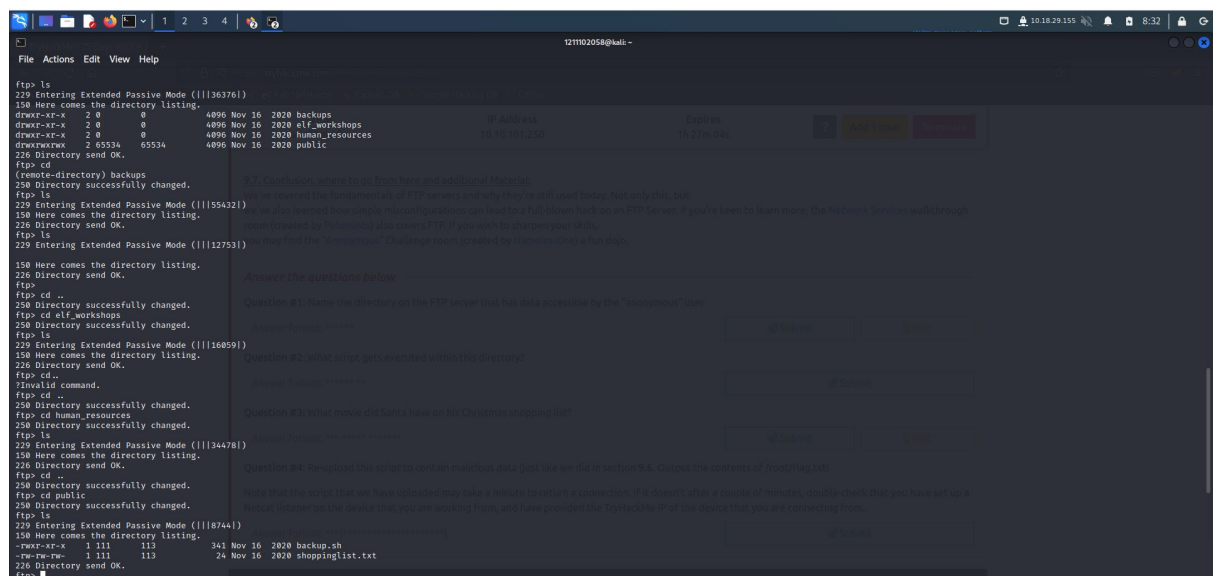
### Q1



```
1271102058@kali: ~  
File Actions Edit View Help  
1271102058@kali: ~  
$ ftp 10.10.101.250  
Connected to 10.10.101.250.  
220 Welcome to the TDFC FTP Server!  
Name (10.10.101.250:1271102058): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||18860|)  
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  
drwxr-xr-x  2 65534  65534  4096 Nov 16  2020 public  
226 Directory send OK.  
ftp>
```

Open kali linux, use command <ftp IP [address]> to connect with the provided IP address. When connected, use anonymous as the name to login in using anonymous mode. Then use command<ls>. The list of directories is shown.

### Q2



```
1271102058@kali: ~  
File Actions Edit View Help  
1271102058@kali: ~  
$ ftp 10.10.101.250  
Connected to 10.10.101.250.  
220 Welcome to the TDFC FTP Server!  
Name (10.10.101.250:1271102058): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||136376|)  
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  
drwxr-xr-x  2 65534  65534  4096 Nov 16  2020 public  
226 Directory send OK.  
ftp> cd  
(remote-directory) backups  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||155432|)  
150 Here comes the directory listing.  
226 Directory send OK.  
ftp> ls  
229 Entering Extended Passive Mode (|||12753|)  
150 Here comes the directory listing.  
226 Directory send OK.  
ftp> cd ..  
250 Directory successfully changed.  
ftp> cd elf_workshops  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||16899|)  
150 Here comes the directory listing.  
226 Directory send OK.  
ftp> cd ..  
250 Directory successfully changed.  
ftp> cd human_resources  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||34478|)  
150 Here comes the directory listing.  
226 Directory send OK.  
ftp> cd ..  
250 Directory successfully changed.  
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||8744|)  
150 Here comes the directory listing.  
-rwxr-xr-x  1 111    113    341 Nov 16  2020 backup.sh  
-rwe-rw-rw- 1 111    113    24 Nov 16  2020 shoppinglist.txt  
226 Directory send OK.  
ftp>
```

Test the directories one-by-one. The directories that are accessible will show the data without using any password.

### Q3

```
229 Entering Extended Passive Mode (|||8744|)
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> █
```

In the data provided, there are 2 directories listed. The file with .sh extension is a shell script, which is able to be executed.

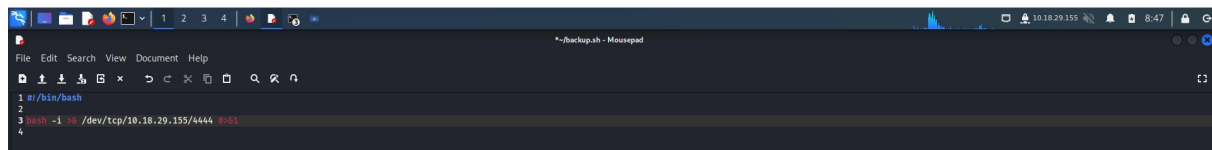
### Q4

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||33639|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*****|
226 Transfer complete.
341 bytes received in 00:00 (1.63 KiB/s)
ftp> shoppinglist.txt
?Invalid command.
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||64493|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |*****|
226 Transfer complete.
24 bytes received in 00:00 (0.11 KiB/s)
ftp> █
```

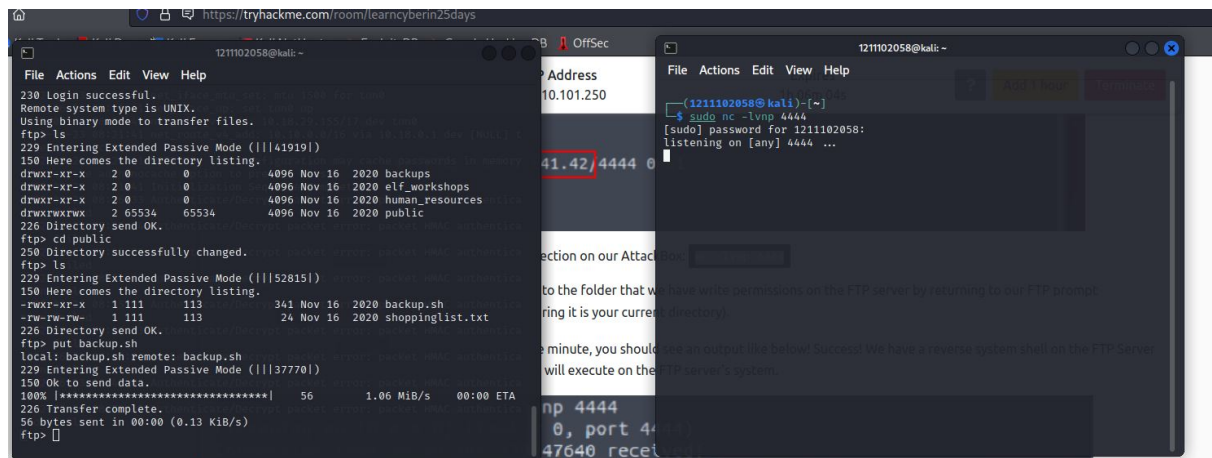
```
File  Actions  Edit  View  Help
-rwxr-xr-x   1 111   113   341 Nov 16  2020 backup.sh
(1211102058@kali)-[~]
└─$ ls
backup.sh  Documents  'panel request'  Public  Videos
big.txt   Downloads  panel.request    shoppinglist.txt  wordlist
Desktop   Music     Pictures         Templates
-rw-rw-rw-   1 111   113   24 Nov 16  2020 shoppinglist.txt
(1211102058@kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie
```

Examine both files by downloading both using the <get> command. Then read the file and the movie name is discovered.

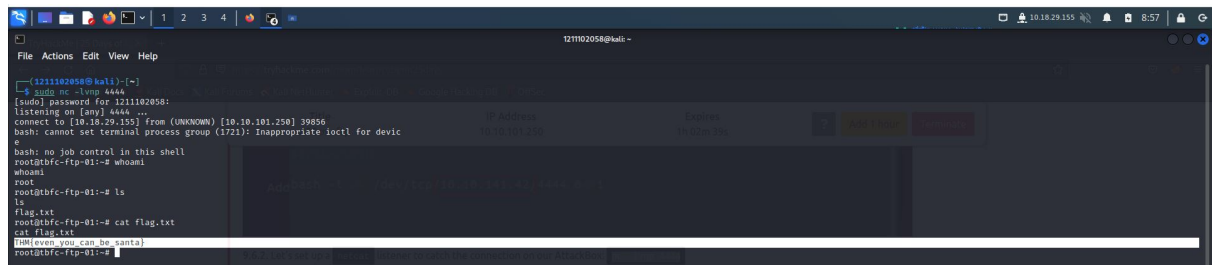
## Q5



Open the backup.sh file. Edit the original IP address into our own IP address.



Resend back the edited shell script using <put> command on ftp server. After transfer complete, open netcat listener and wait.



After access is granted from the server, we examine the server data. A file named file.txt is found. Read the file, the flag is shown. Catch the flag.