PSP0201

Week 3

Writeup

Group Name: F4urDeveloper

Members:

ID	NAME	ROLE
1211101242	RAJA FITRI HAZIQ BIN RAJA MOHD FUAD	LEADER
1211104237	ALIA MAISARA BINTI SHAHRIN	MEMBER
1211102287	TERRENCE CHENG	MEMBER
1211101153	MISCHELLE THANUSHA JULIUS	MEMBER

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

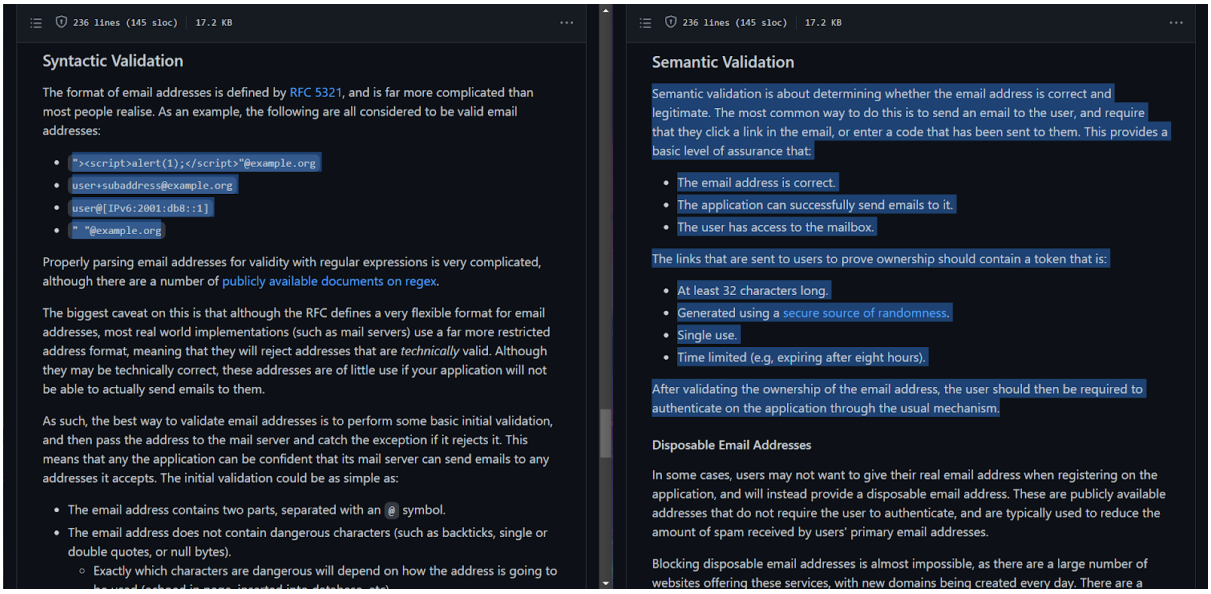
Tools used: THM Machine/Kali Linux/Mozilla Firefox/Zaproxy

Solution/Walktrough:

Question 1:

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

The answers for Syntactic and Semantic Validation can be found in the statement shown in the image below (highlighted for viewing purposes).



Question 2:

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

The regular expression used to validate a US Zip code can be found as shown in the image below (highlighted for viewing purposes).

Question 3:

What vulnerability type was used to exploit the application?

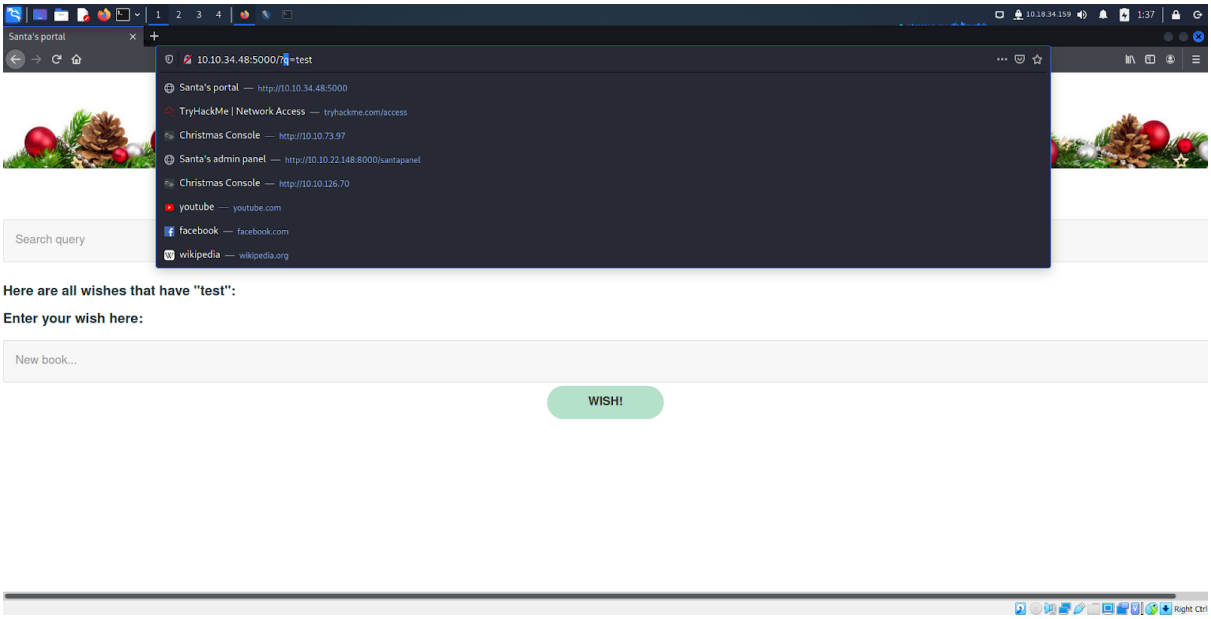
The vulnerability type that was used to exploit the application can be found as shown in the image below (highlighted for viewing purposes).

Stored XSS works when a certain malicious JavaScript is submitted and later on stored directly on the website. For example, comments on a blog post, user nicknames in a chat room, or contact details on a customer order. In other words, in any content that persistently exists on the website and can be viewed by victims.

Question 4:

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

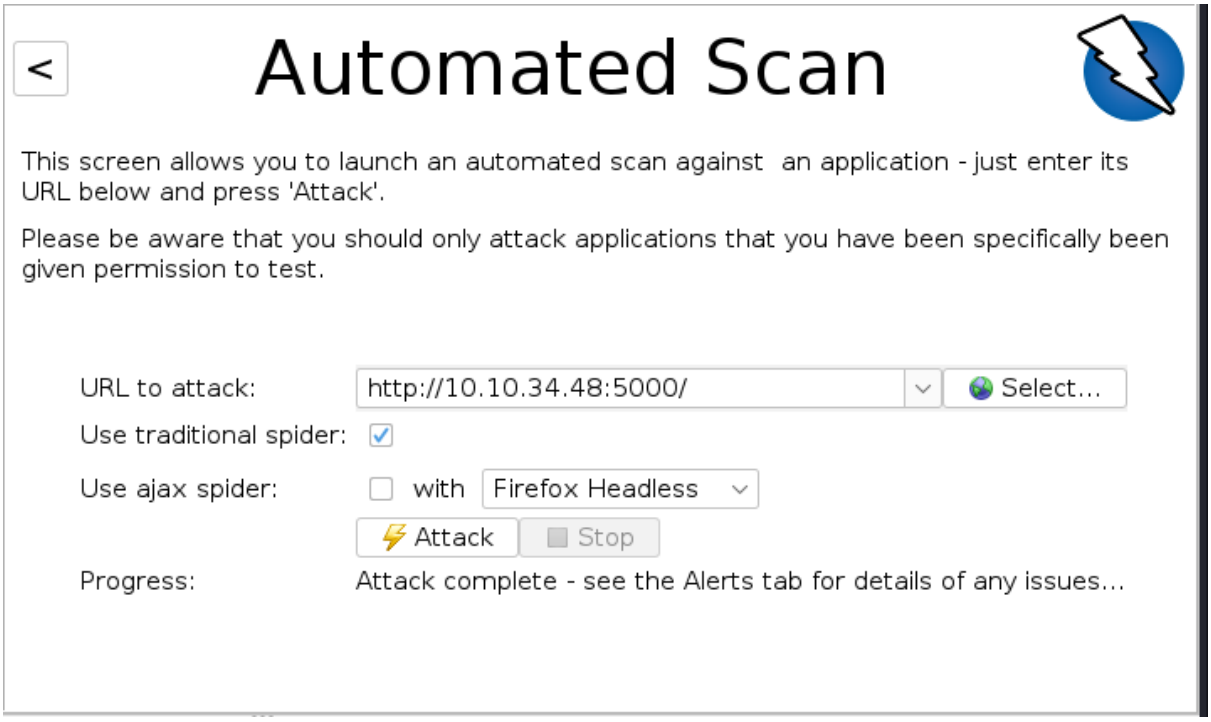
In order to find the query string, one must input any type of text in the 'Search query' section. Entering the typed text will pop up the query string in the search bar on top of the website as shown in the image below.



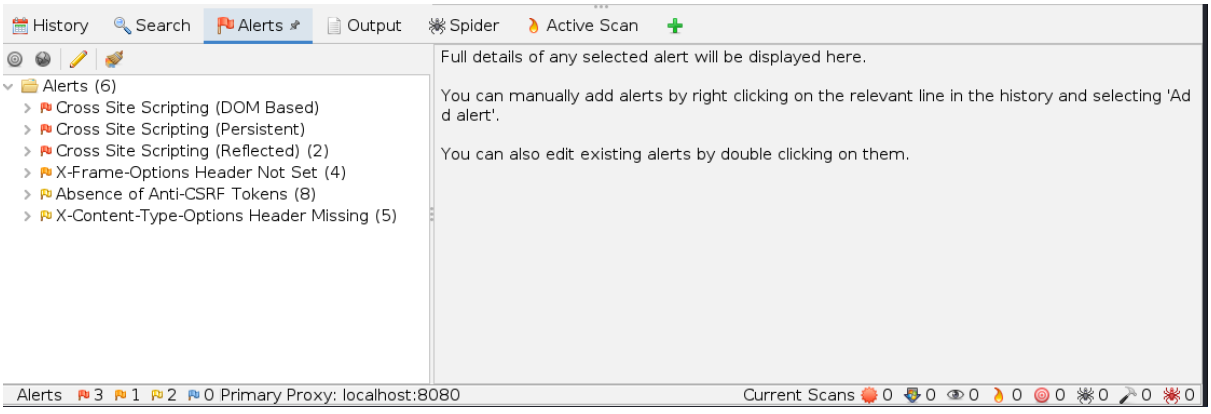
Question 5:

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

Click the 'Automated Scan' option and type in the website's address in the 'URL to attack' section. After doing so, press the 'Attack' button to start the attack on the website.



After waiting for a few seconds, click on the 'Alerts' tab to identify how many XSS alerts of high priority are available 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"?

The answer for this particular question can be found either through Google or having Javascript knowledge. As shown in the image below, typing in <script>alert('PSP0201')</script> is the correct way of making 'PSP0201' appears as the wish.

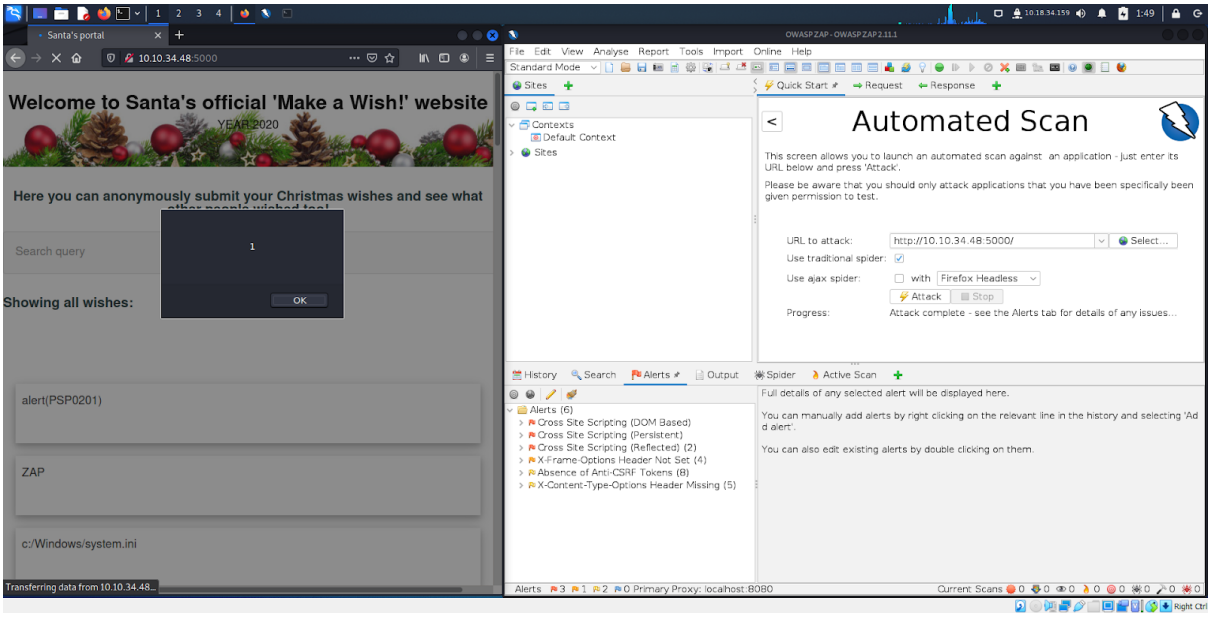
What is alert function in JavaScript?

The alert() method **displays an alert box with a message and an OK button**. The alert() method is used when you want information to come through to the user.

Question 7:

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

Closing and revisiting the website again will make the text in the black box appear. Therefore, the XSS attack still persist.



Thought Process/Methodology:

Based on question 1 and question 2, the answer for those two particular questions can be found by looking through OWASP Cheat Sheet. As for question 3, the hint for the answer can be found in the THM website under Day 6 section. After opening up the website by typing in the IP Address:5000 in the search bar, we are exposed to the page titled ‘Santa’s Portal’. In order to find the query string that we can abuse, we must type in anything that we want in the ‘Search query’ section and press Enter. The query string should appear in the search bar (q). Finding the amount of XSS alerts of high priority require us to start an attack on the website with Zaproxy. After clicking the ‘Automated Scan’ option, we are able to type in the URL link to attack. After doing so, we can simply go to the ‘Alerts’ tab to find the amount of XSS alerts asked in the question. Question 6’s answer can be found by doing a bit of researching through

Google. The correct function to make ‘PSP0201’ appear in the wish text box should be alert(). Last but not least, we can confirm that the XSS attack persist by closing and revisiting the website as a black box with the text ‘1’ pops up in the main page.

Day 7: Networking - The Grinch Really Did Steal Christmas

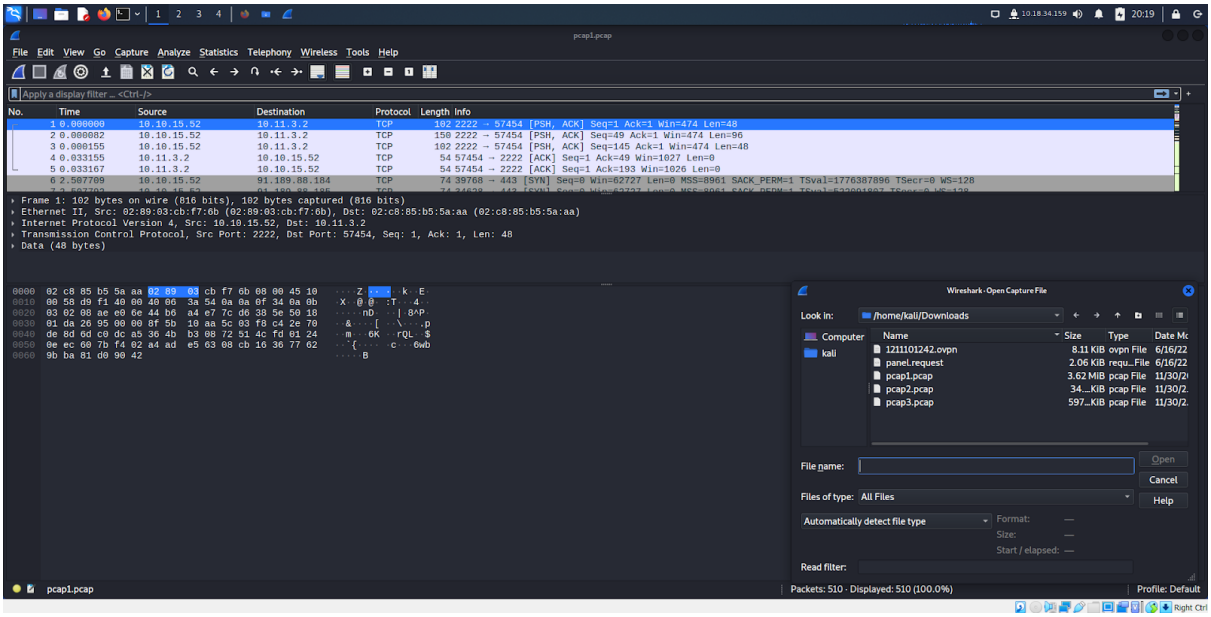
Tools used: Kali Linux/THM Task Files/Wireshark

Solution/Walkthrough:

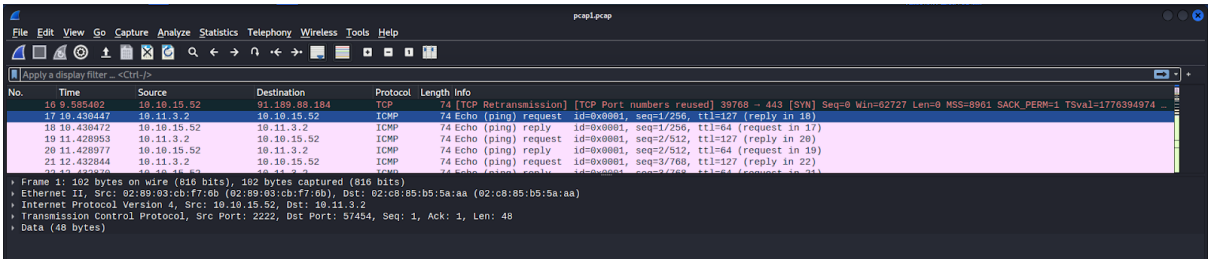
Question 1:

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

By default, Wireshark is not installed in Kali Linux. Therefore, use the following command ‘sudo apt install wireshark’ to install Wireshark in order to complete this task. After doing so, open up Wireshark and use the ‘drag and drop’ method to open up the downloaded task file from THM which is ‘pcap1.pcap’ to capture it.



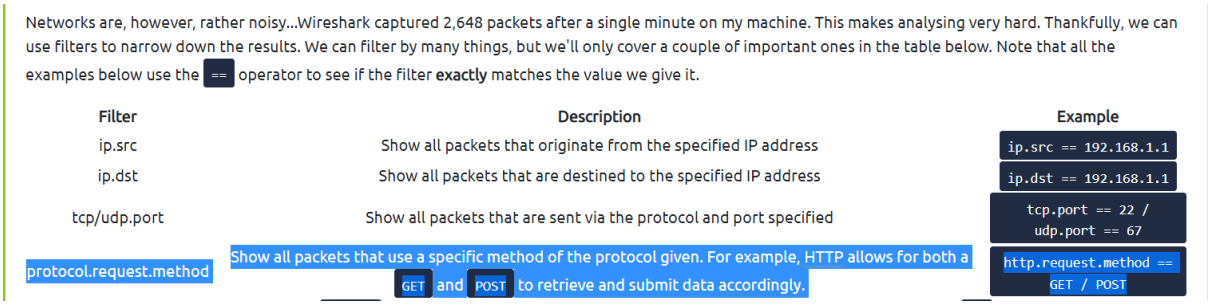
After capturing the file, scroll down until you see the first IP address that initiates an ICMP/ping



Question 2:

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

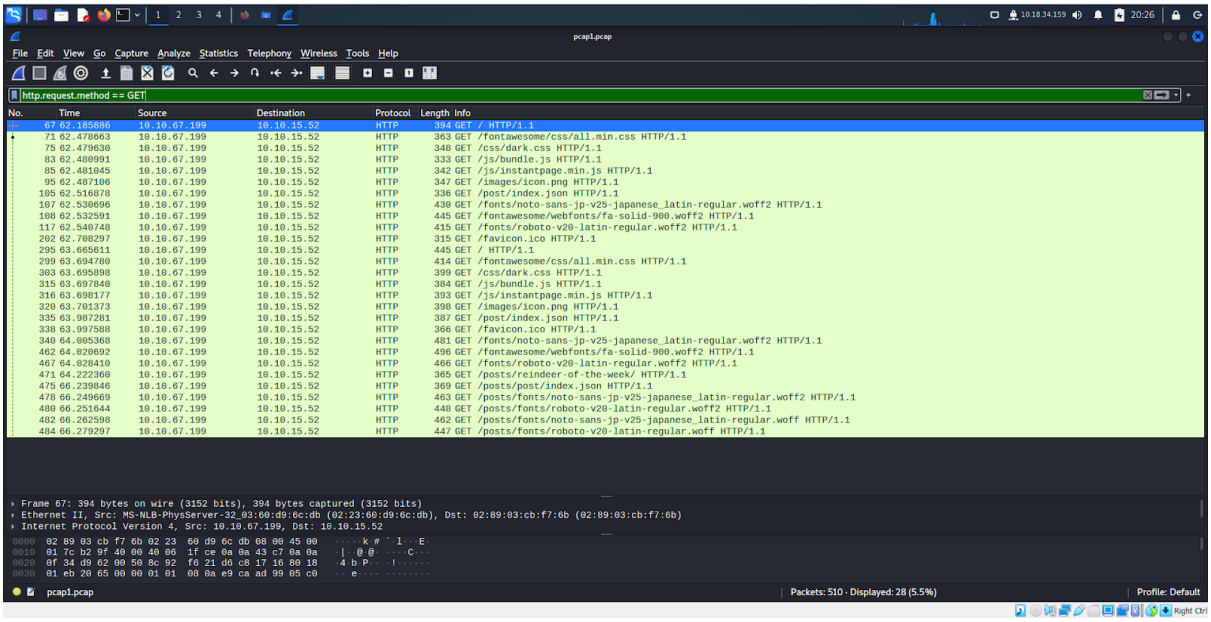
The appropriate filter that we would use to see HTTP GET requests in our "pcap1.pcap" file should be http.request.method == GET as shown in the image below.



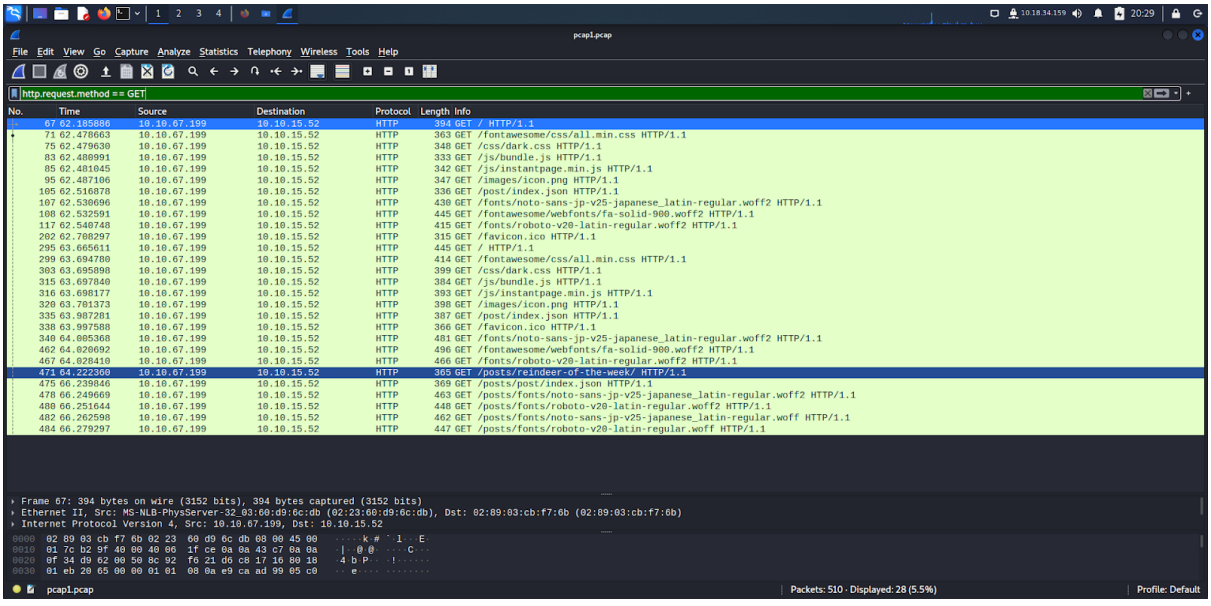
Question 3:

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?

Type in the following filter in Wireshark to get all of the information as shown in the image below.



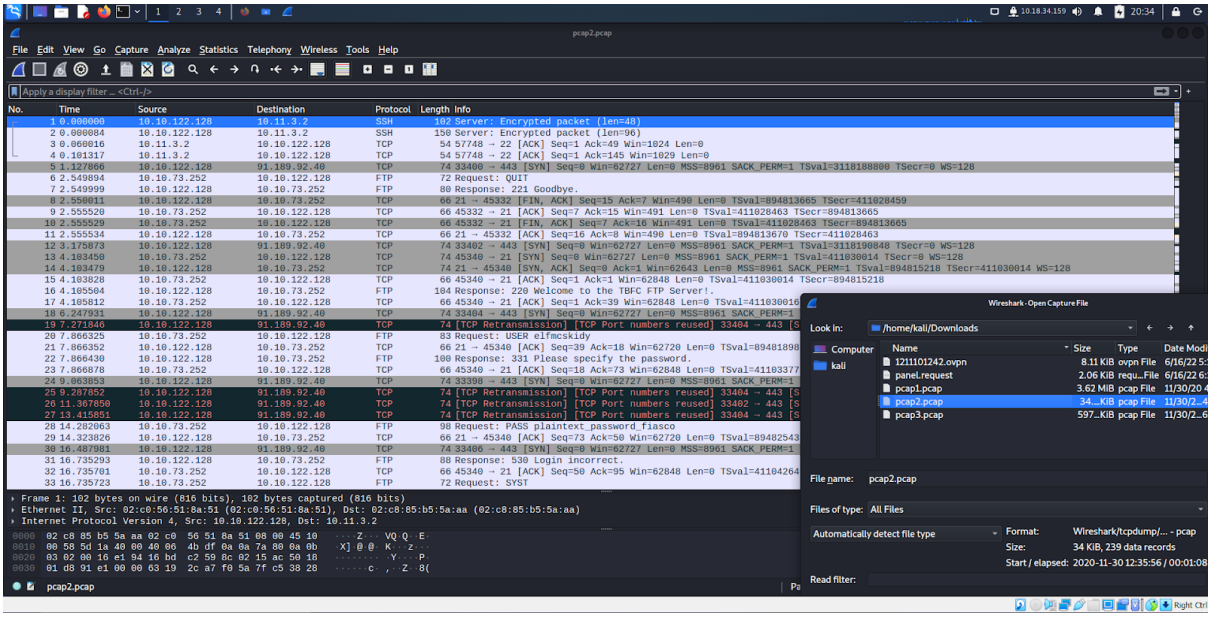
The name of the article that the IP address "10.10.67.199" visited should be as shown in the image below.



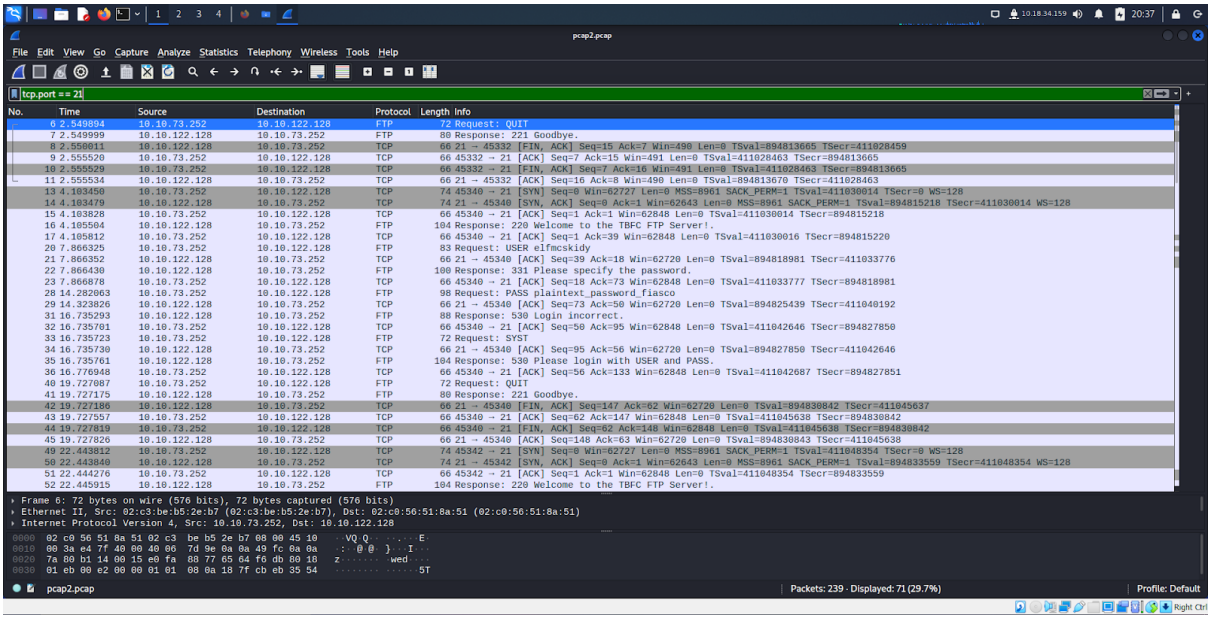
Question 4:

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

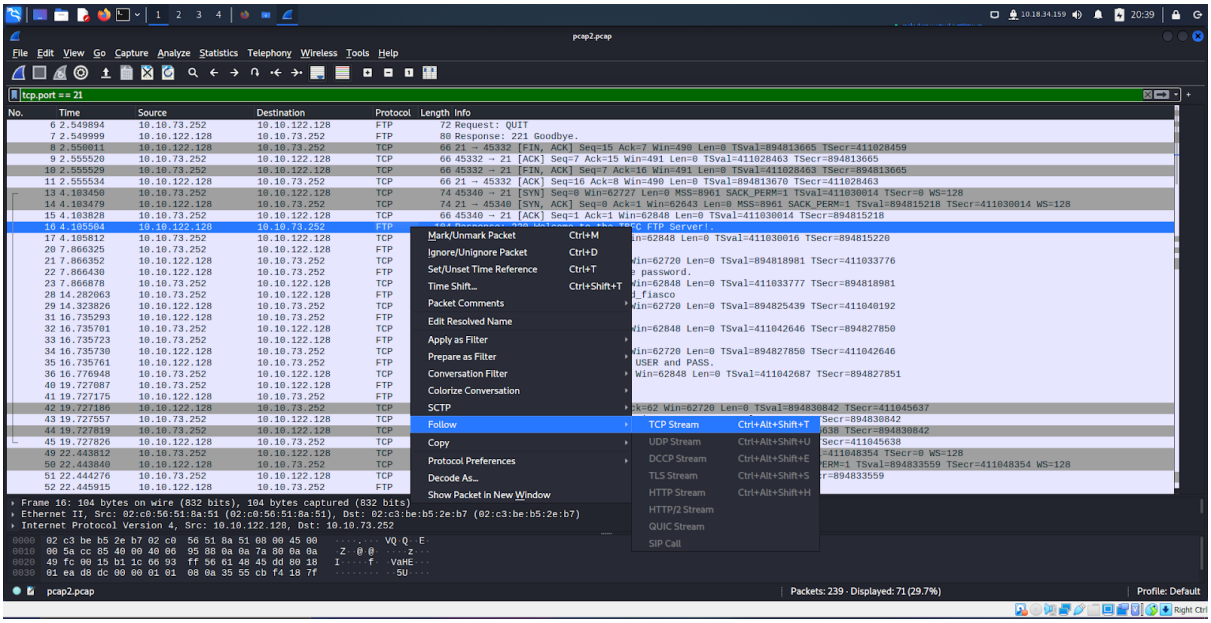
Open up "pcap2.pcap" by using the ‘drag and drop’ method.



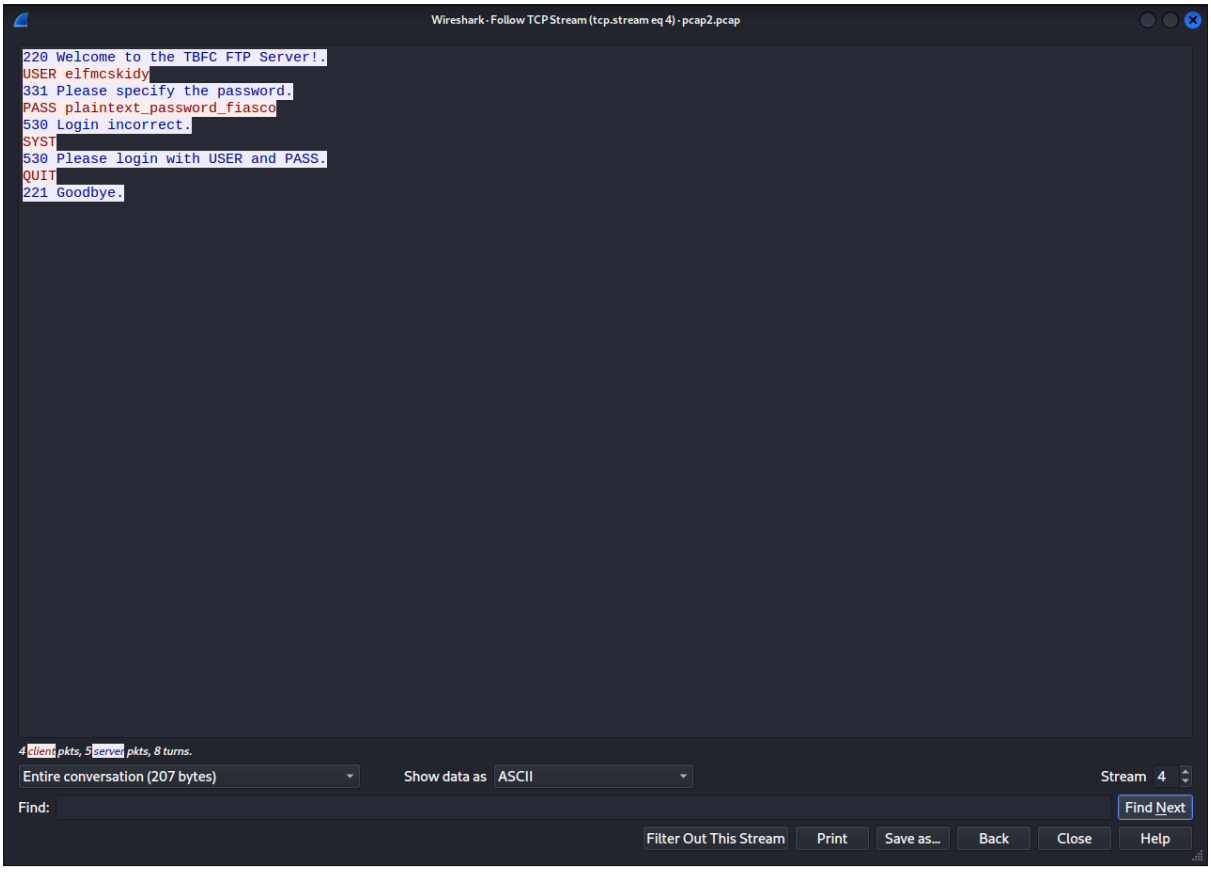
Use the following filter to get rid of the irrelevant data and make our finding much easier.



Find the FTP traffic that showed user login successful attempt. Right click the FTP traffic, click Follow and click TCP stream to find the leaked password.



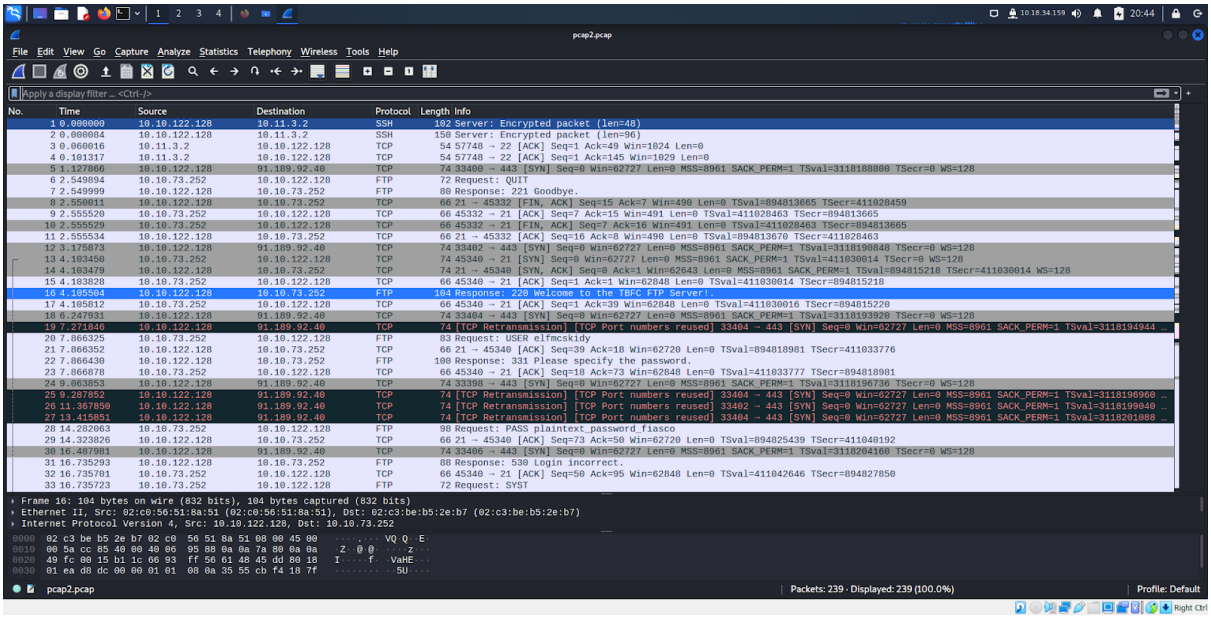
A new pop up should appear with the information needed as shown in the image below.



Question 5:

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

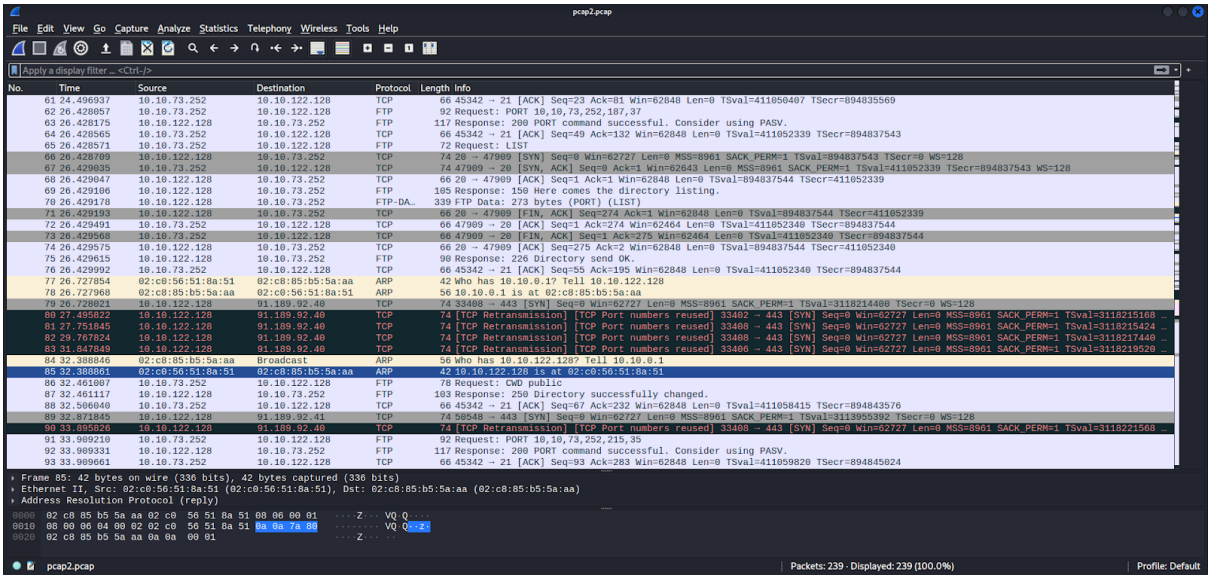
The protocol that is encrypted can be found by removing the filter used in the previous question and by identifying the first result in Wireshark as shown in the image below.



Question 6:

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

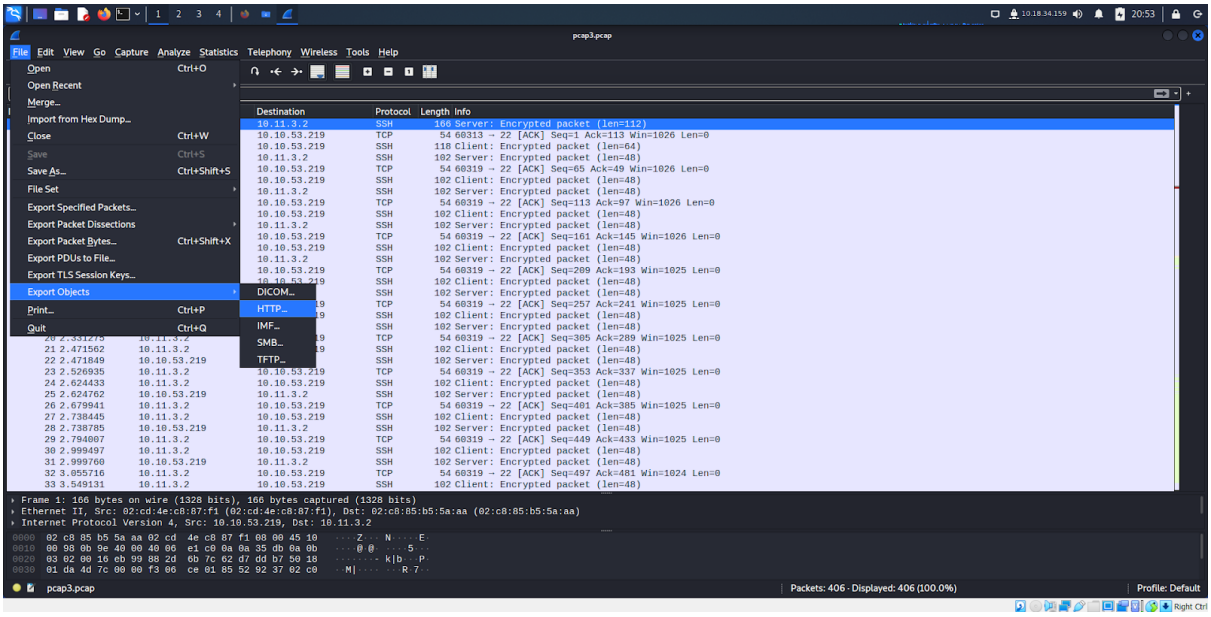
Scroll down the find the correct ARP communications with ‘Who has 10.10.122.128? Tell 10.10.10.1. ‘ as its info. The answer can be found on the second ARP communications as shown in the image below.



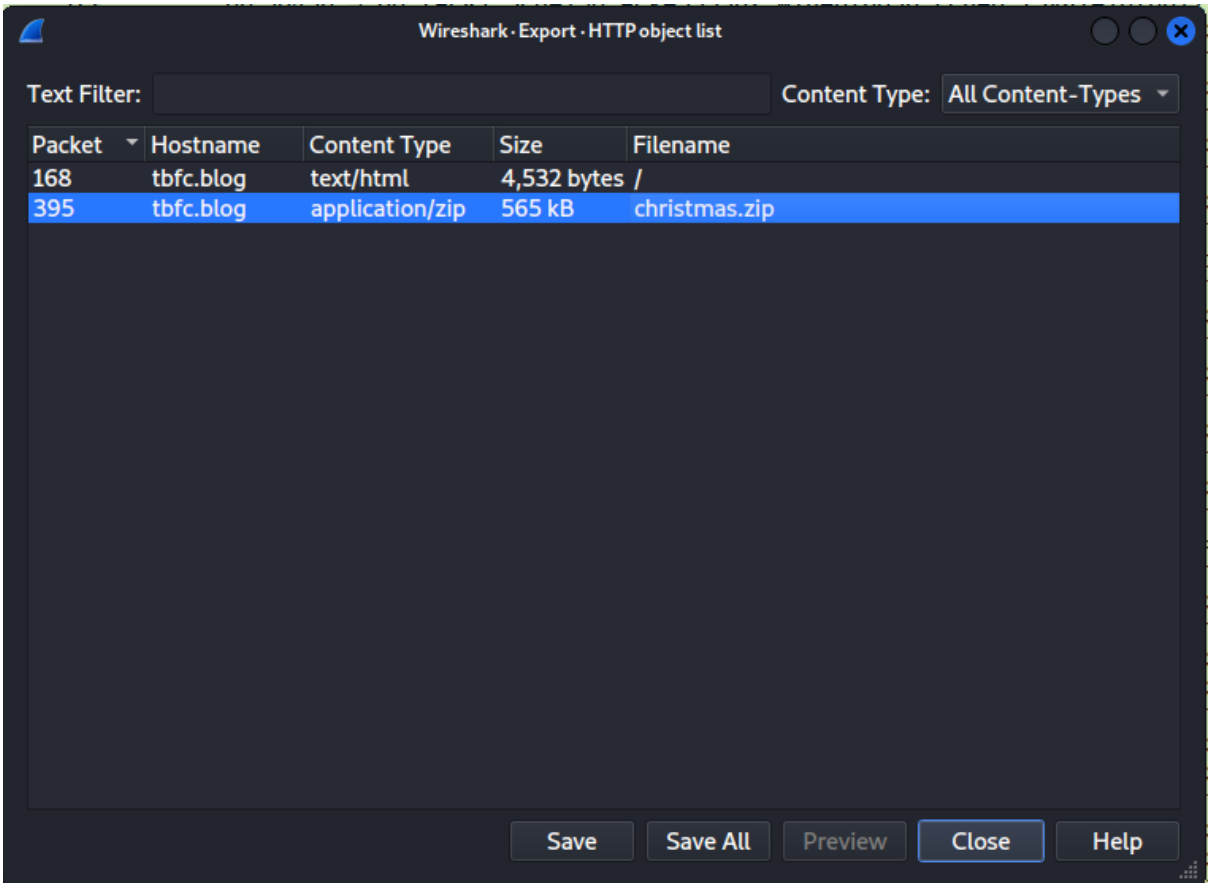
Question 7:

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

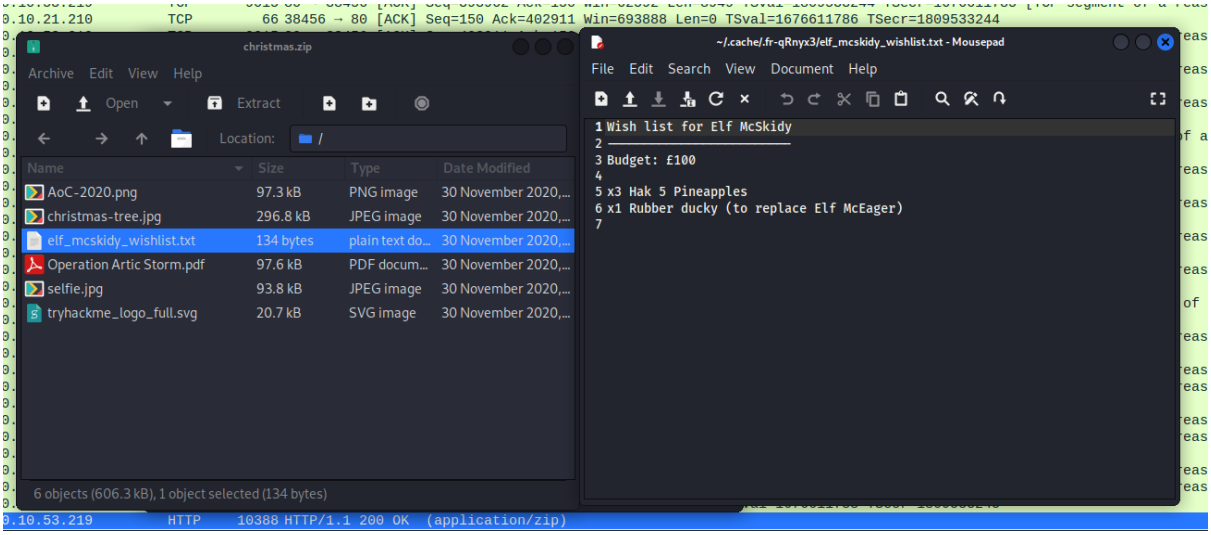
To make our job easier, go to File -> Export Objects -> HTTP.



Save the highlighted zip file in any directory one prefers.



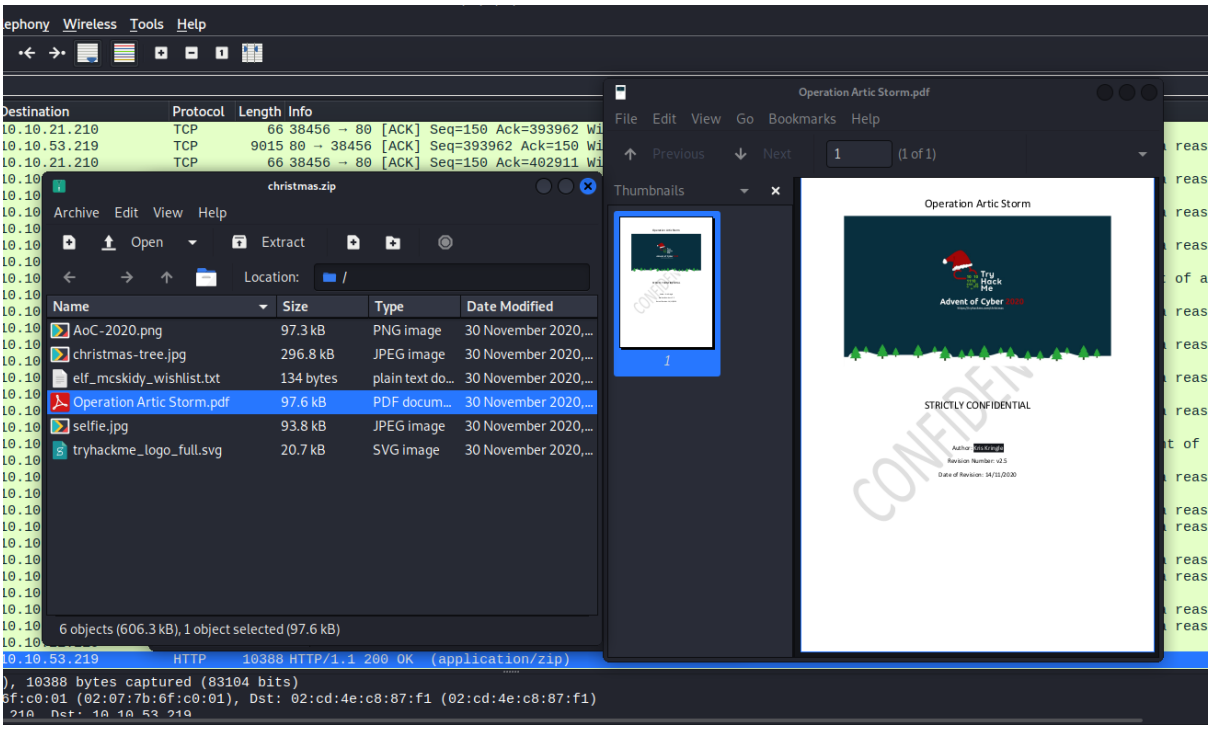
Open up the saved zip file and open the elf_mcskidy_wishlist.txt file to find the answer as shown in the image below.



Question 8:

Who is the author of Operation Artic Storm?

In the same directory, open up the Operation Artic Storm.pdf pdf file to find the author's name as show in the image below.



Thought Process/Methodology:

In order to get the definite answer for question 1, we need to install Wireshark in Kali Linux as it is not installed by default. This can be simply done by going to the terminal and typing in the following command 'sudo apt install wireshark'. After doing so, open up Wireshark and use the 'drag and drop' method to open up the 'pcap1.pcap' file found by downloading the Task Files given in THM to capture it. After opening up the file, scroll down until you see the first IP address that initiates an ICMP/ping (10.11.3.2 should be the answer). As for question 2, the answer can be found by reading through Day 7 as the hint is already given in one of the statements/tables (http.request.method == GET should be the answer). As for question 3, we need to type in the filter we obtained from previous question to find the correct article that the IP Address '10.10.67.199' visited. After doing so, scroll down until you see reindeer-of-the-week as the answer. As for question 4, first and foremost, we need to open up the second file which is 'pcap2.pcap' by using the 'drag and drop' method. Since there is a lot of data irrelevant to the question asked, we can use the following filter 'tcp.port == 21' to make our finding much easier. Find the FTP traffic that showed a successful user login attempt. Right click the FTP traffic, click Follow and click TCP stream to find the leaked password. A new pop up will appear containing the password (plaintext_password_fiasco should be the answer). As for question 5, we need to remove the filter used in the previous question and the first

result should be the protocol we are looking for. As for question 6, scroll down the find the correct ARP communications with ‘Who has 10.10.122.128? Tell 10.10.10.1. ‘ as its info. The answer can be found on the second ARP communications just below the first one we identified which is 02:c0:56:51:8a:51. As for question 7 and question 8, both of these can be done simultaneously by going to File -> Export Objects -> HTTP to narrow down the possible file we need the most. Save the christmas.zip file in any directory one prefers and open it up to see both the elf_mcskidy_wishlist.txt (open it up to obtain the answer for question 7)and Operation Artic Storm.pdf (open it up to obtain the answer for question 8) files.

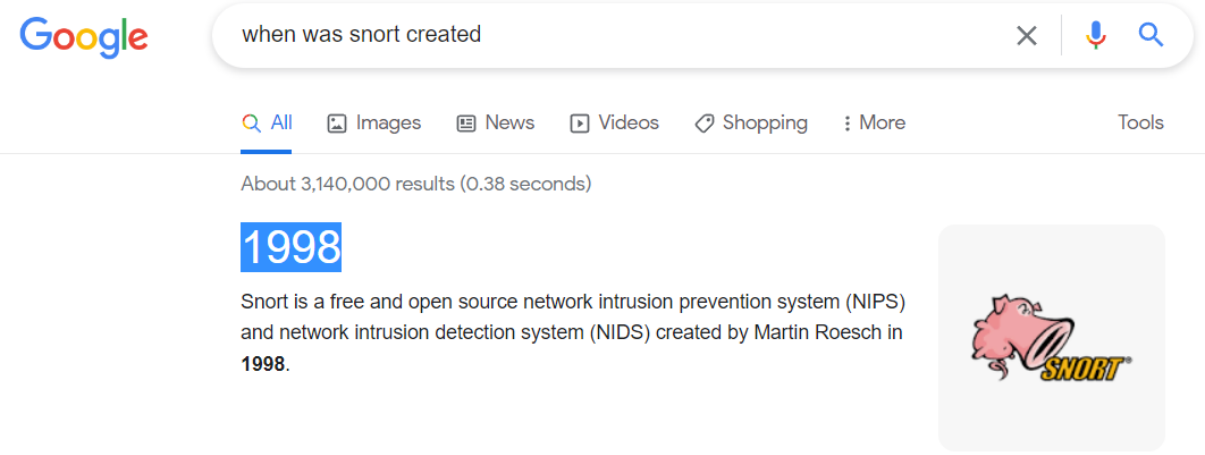
Day 8: Networking - What's Under the Christmas Tree?

Tools used: THM Machine/Kali Linux/Mozilla Firefox/Nmap

Solution/Walkthrough:

Question 1

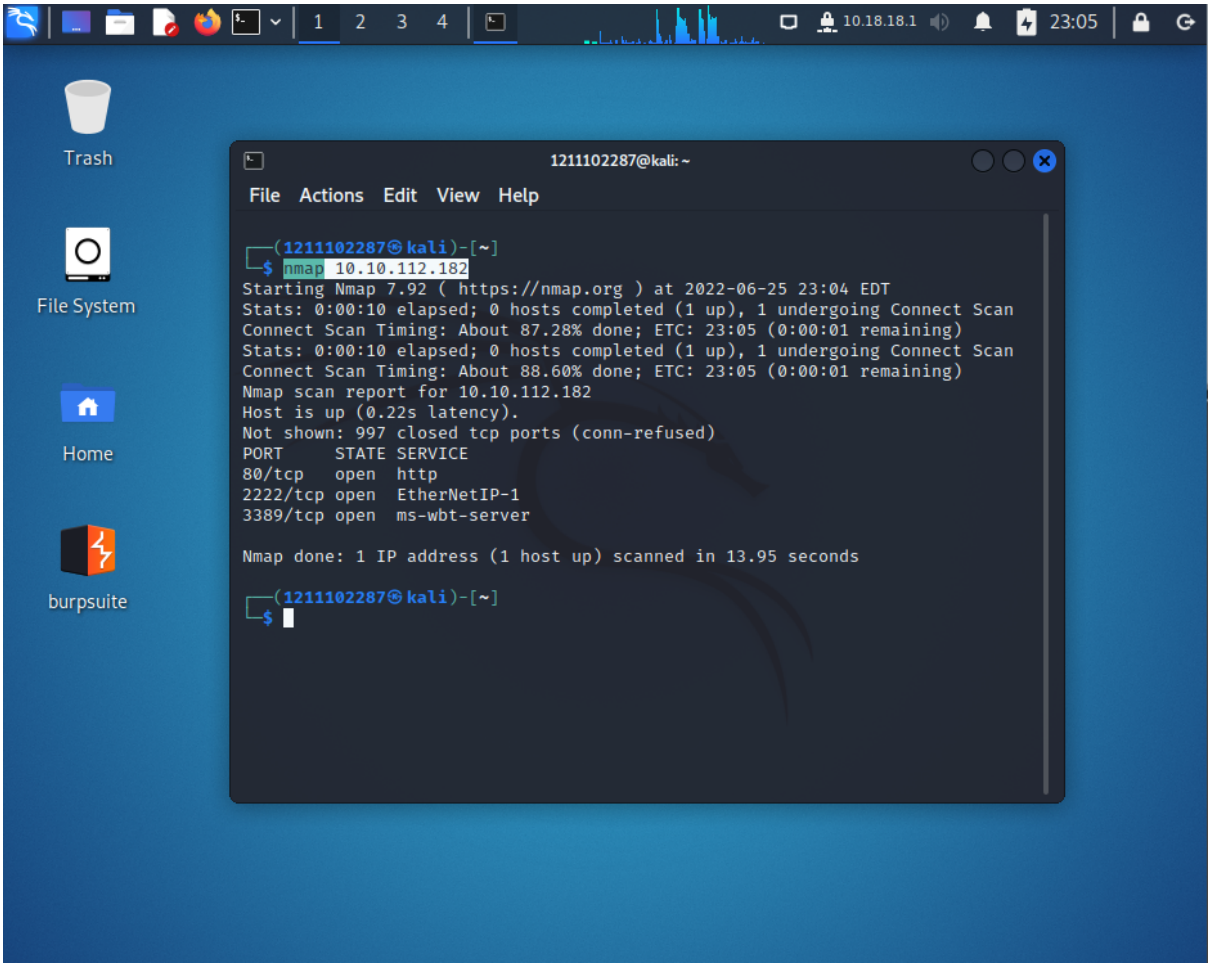
When was Snort created?



By searching on Google, Snort can be known to be created in the year **1998** which is highlighted in the picture.

Question 2

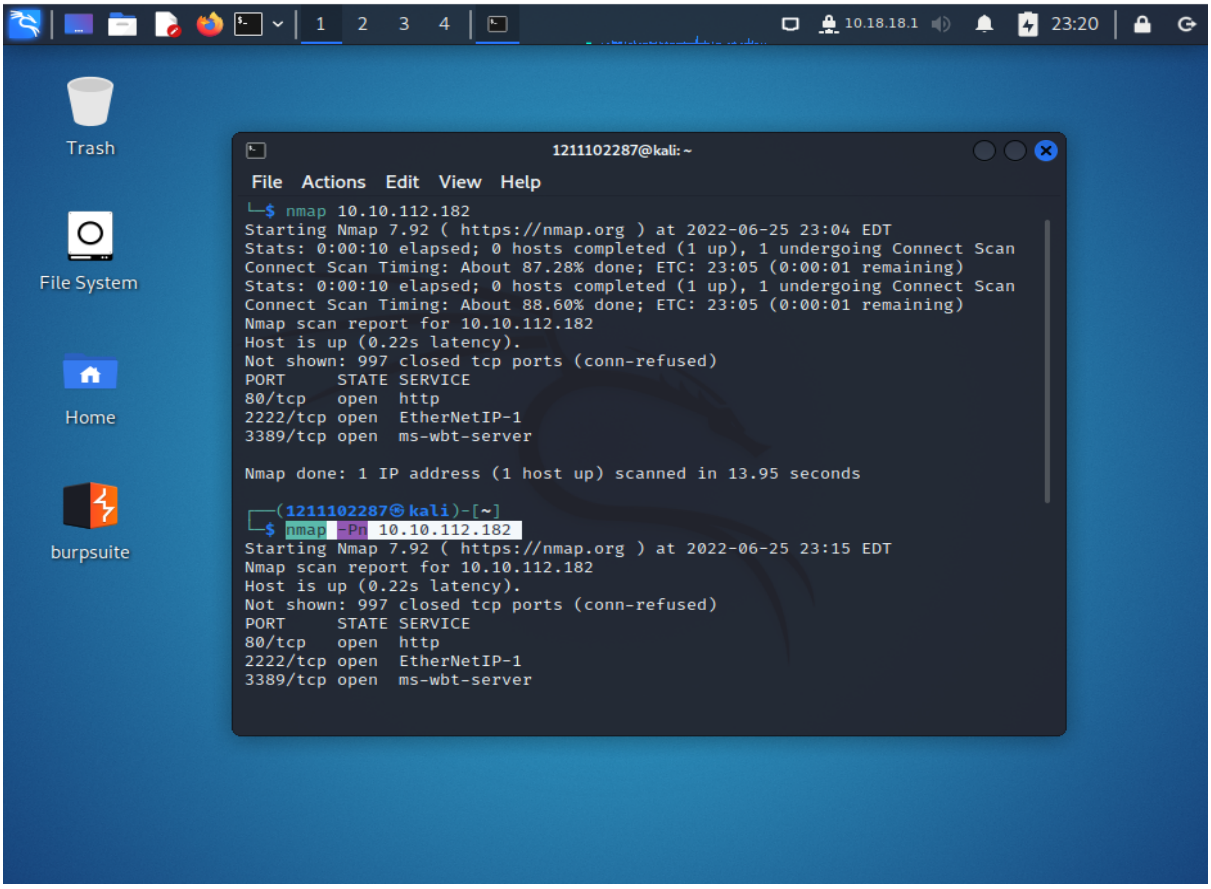
Using Nmap on MACHINE_IP , what are the port numbers of the three services running?



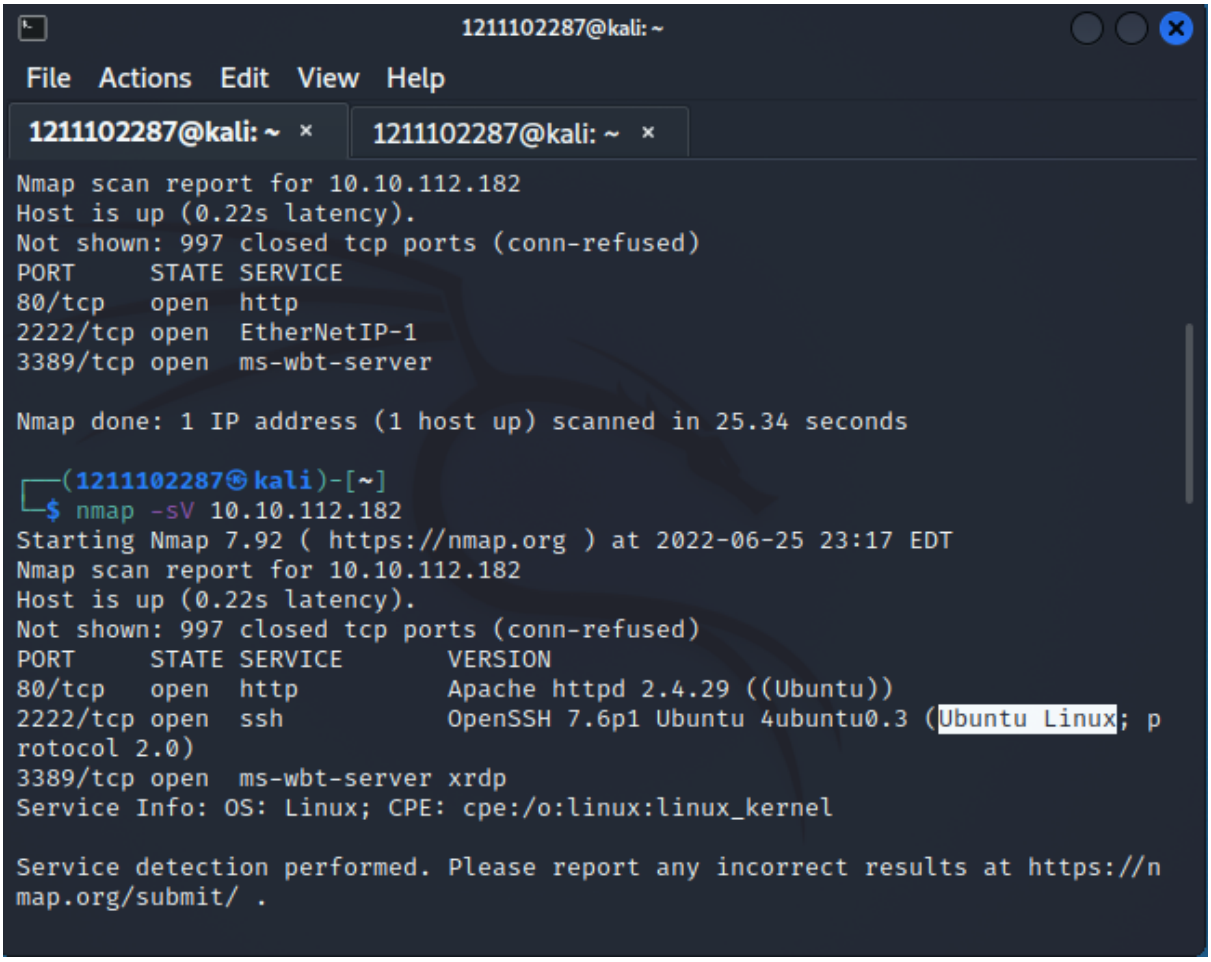
Insert the command nmap followed by the IP address (10.10.112.182) in the terminal window to run a scan and find the Services which are running. The Port numbers could be seen in the terminal **(80.2222.3389)**.

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?



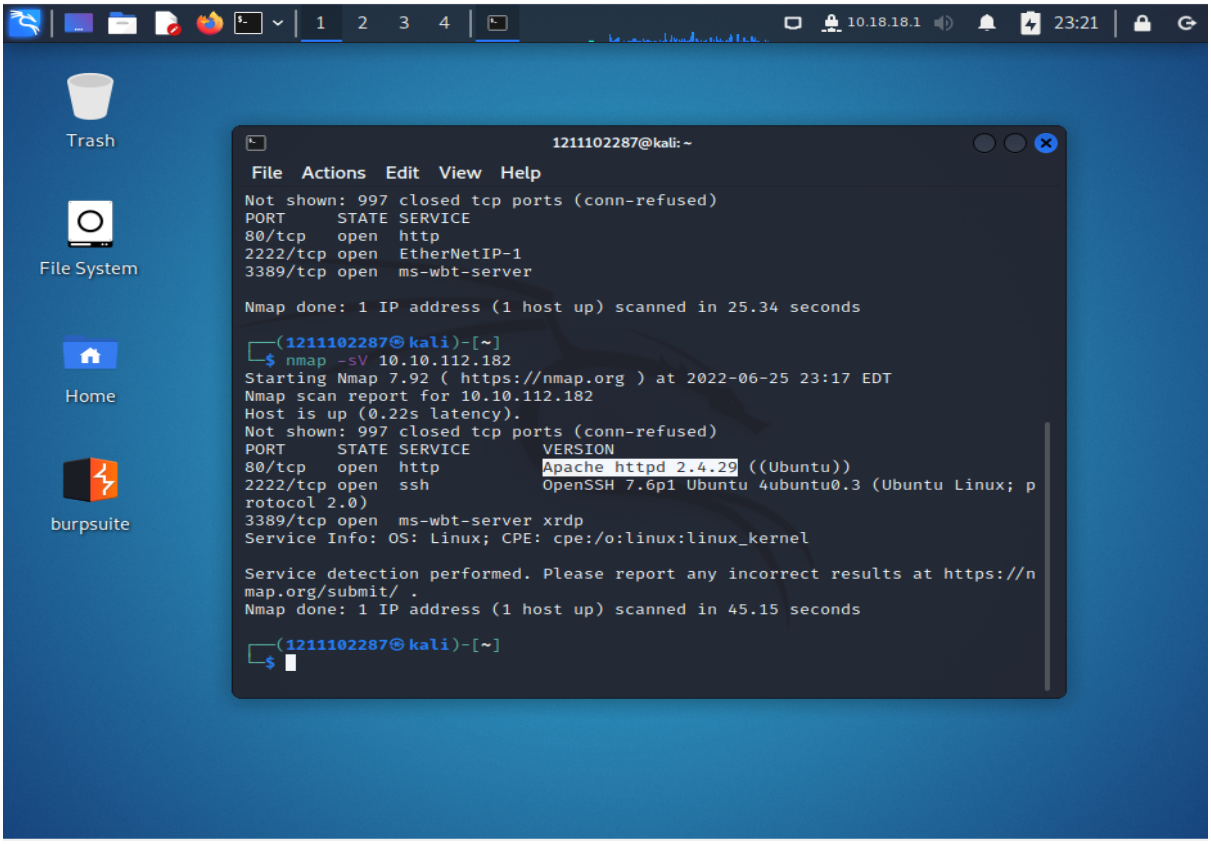
The -Pn flag is used to scan and determine whether the host is up.



By using the Nmap's TCP Scan, the Flag **-sV** used after the command nmap allows us to scan the host and perform version fingerprinting. The name (highlighted) in the terminal window is the name of the Linux distribution that is running.

Question 4

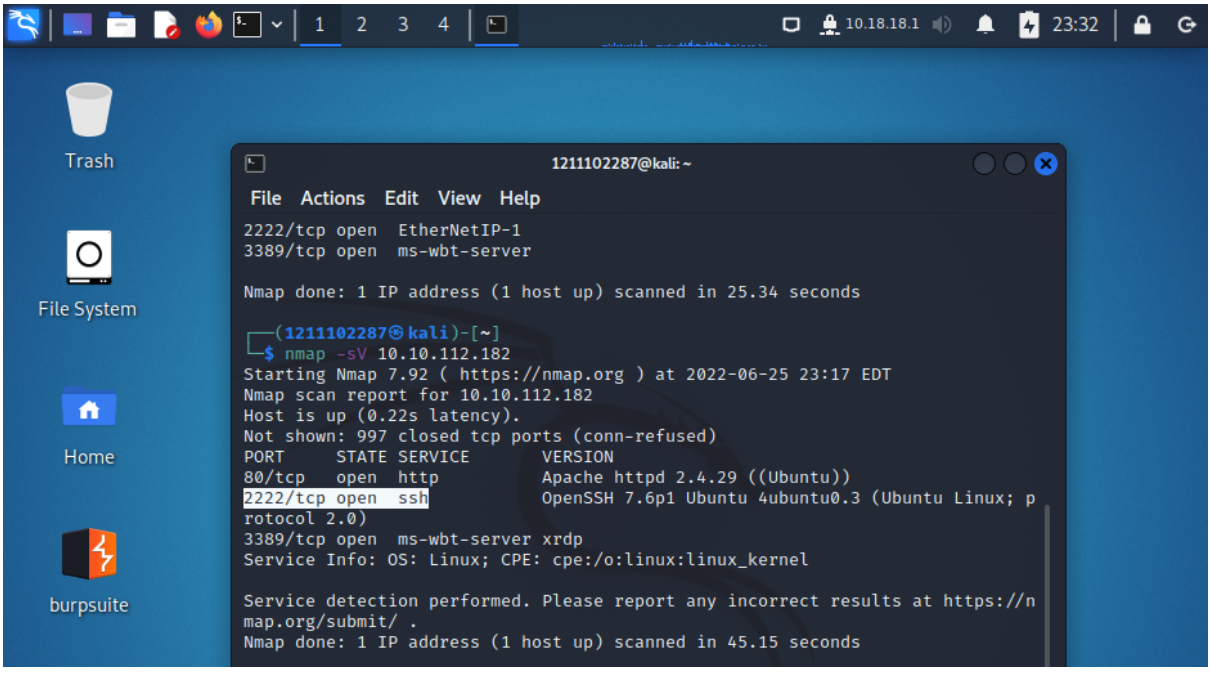
What is the version of Apache?



The Apache version is shown in the terminal window (which is being highlighted)

Question 5

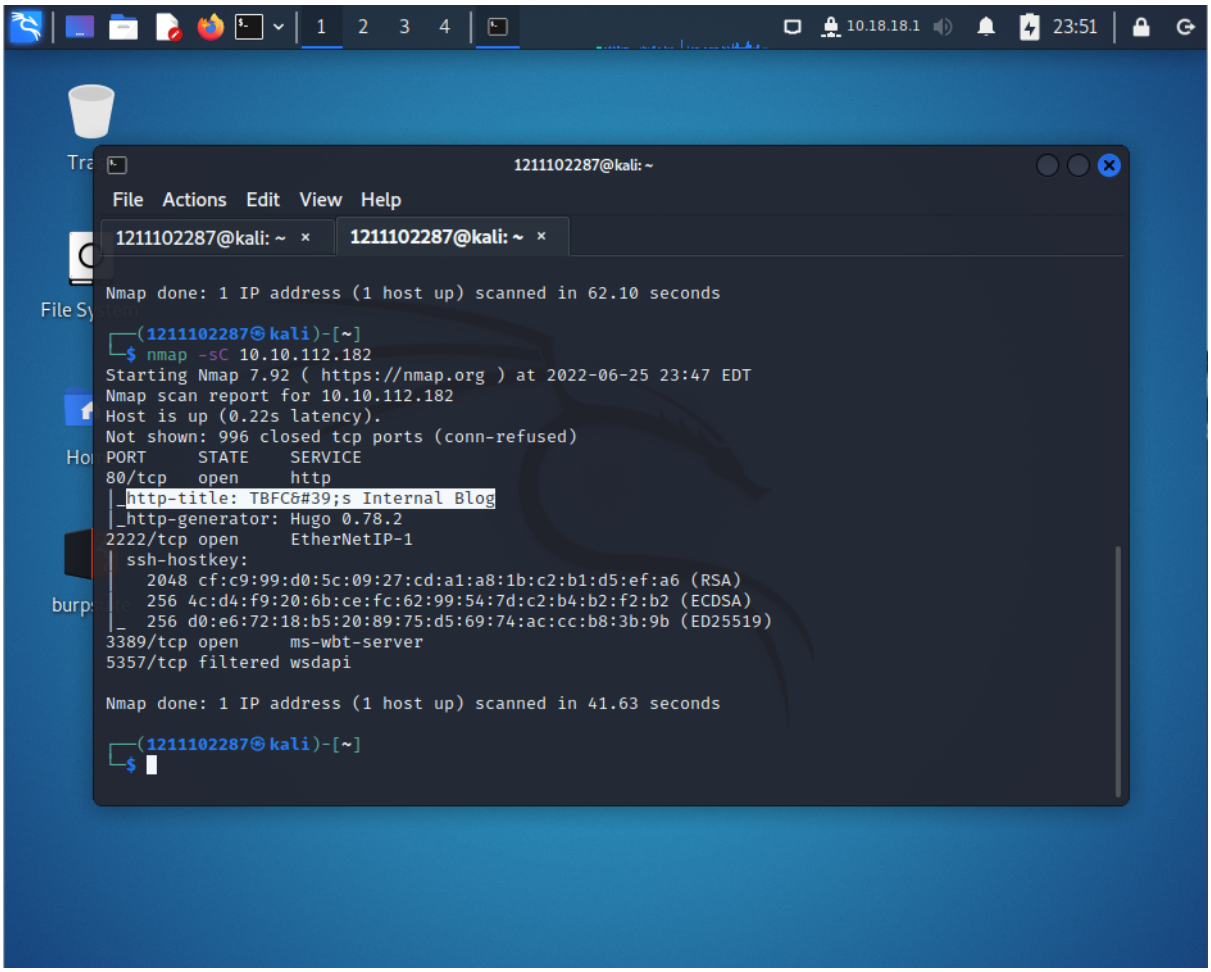
What is running on port 2222?



On Port 2222, we can see **SSH** is running on it.

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?



With Nmap's Network Scripting Engine (NSE), to do a brief and full scanning or checking on the host to retrieve some information, the script “-sC " is inserted after the command nmap in the terminal window. We could see the HTTP-TITLE of the web server, and based on the value returned, we know the website is used for **Blog**.

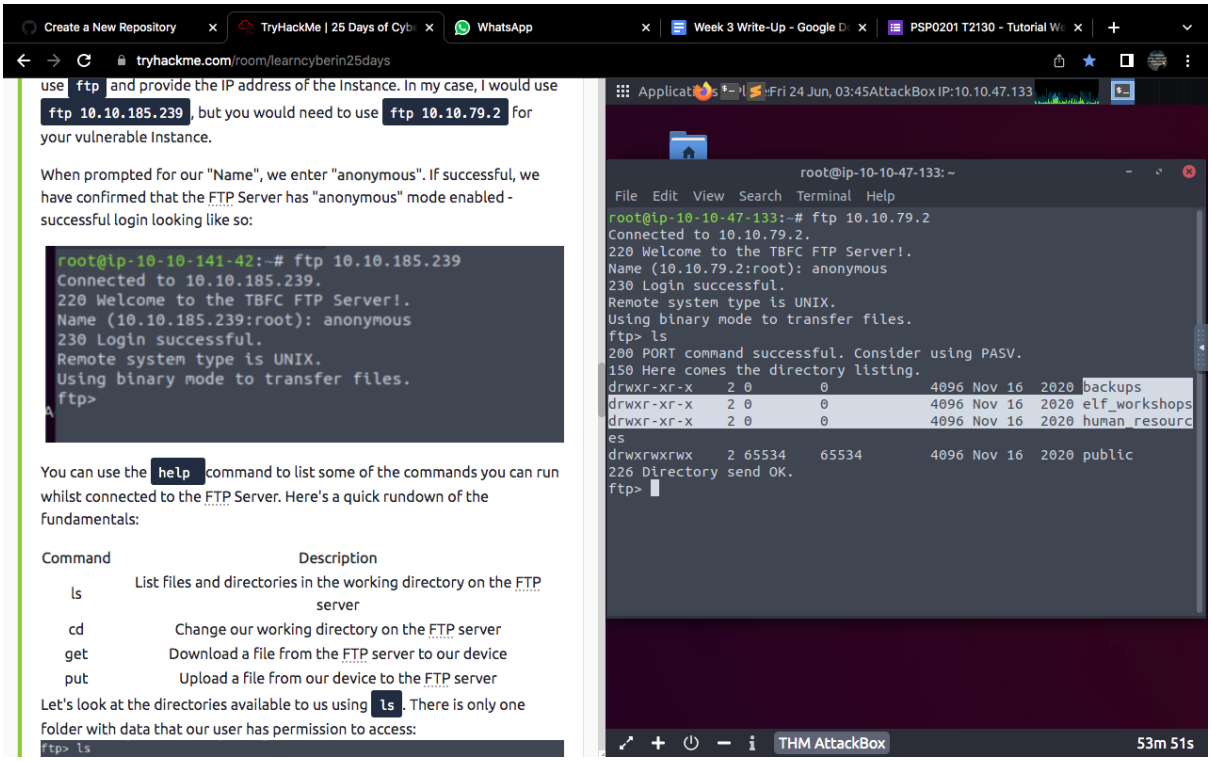
Thought Process/Methodology:

The date when SNORT was created could be found through Google searches which is 1998. To scan and find the Services which are running, the command nmap followed by the IP address is used in the terminal window. The Port numbers could be seen in the terminal under the PORT section. From the hint of the question, we could use the -Pn flag to scan and determine whether the host is up. By using the Nmap's TCP Scan, we should know that the Flag -sV is used after the command nmap and it will let us scan the host and perform version fingerprinting. The name in the terminal window will be shown for the Linux distribution that is running. The Apache version is also shown in the terminal window. Scrolling down the terminal, we could see that the Port 2222 is running with SSH. With Nmap's Network Scripting Engine (NSE), to do a brief and full scanning or checking on the host to retrieve some information, the script “-sC " is inserted after the command nmap in the terminal window. We could see the HTTP-TITLE of the web server, and based on the value returned, we know the website is used for Blog.

Day 9 - [Networking] Anyone can be Santa!

Solution/walkthrough

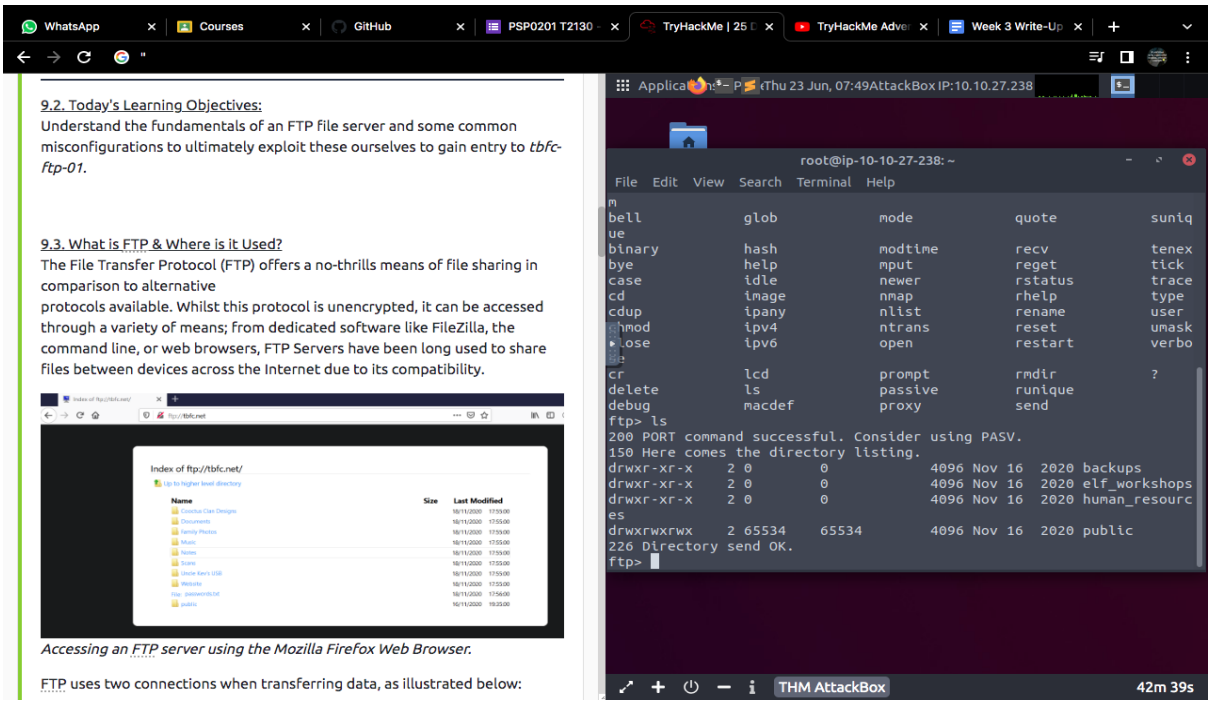
Question 1
What are the directories you found on the FTP site?



The directories we can find on the ftp site right after we type the “anonymous” are backups, elf_workshops and human_resources.

Question 2

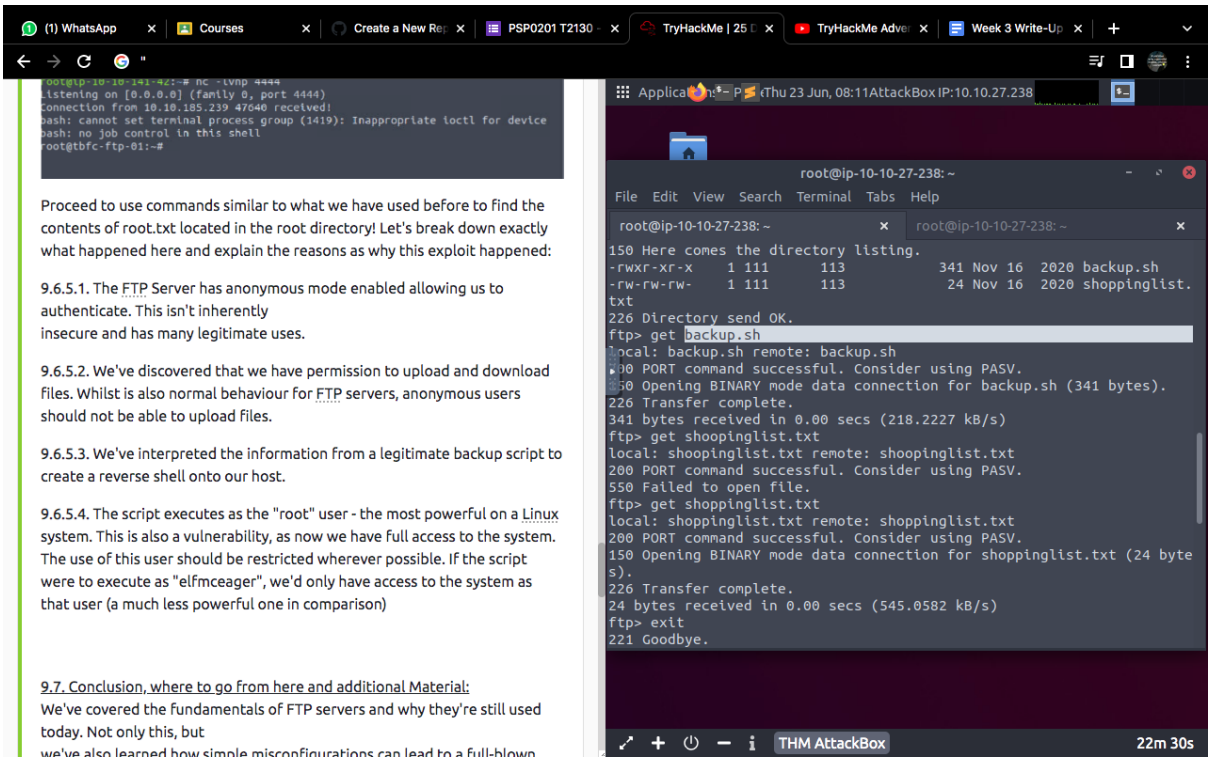
Name the directory on the FTP server that has data accessible by the "anonymous" user



The name of the directory on the ftp server is public which has data accessible by the “anonymous” user.

Question 3

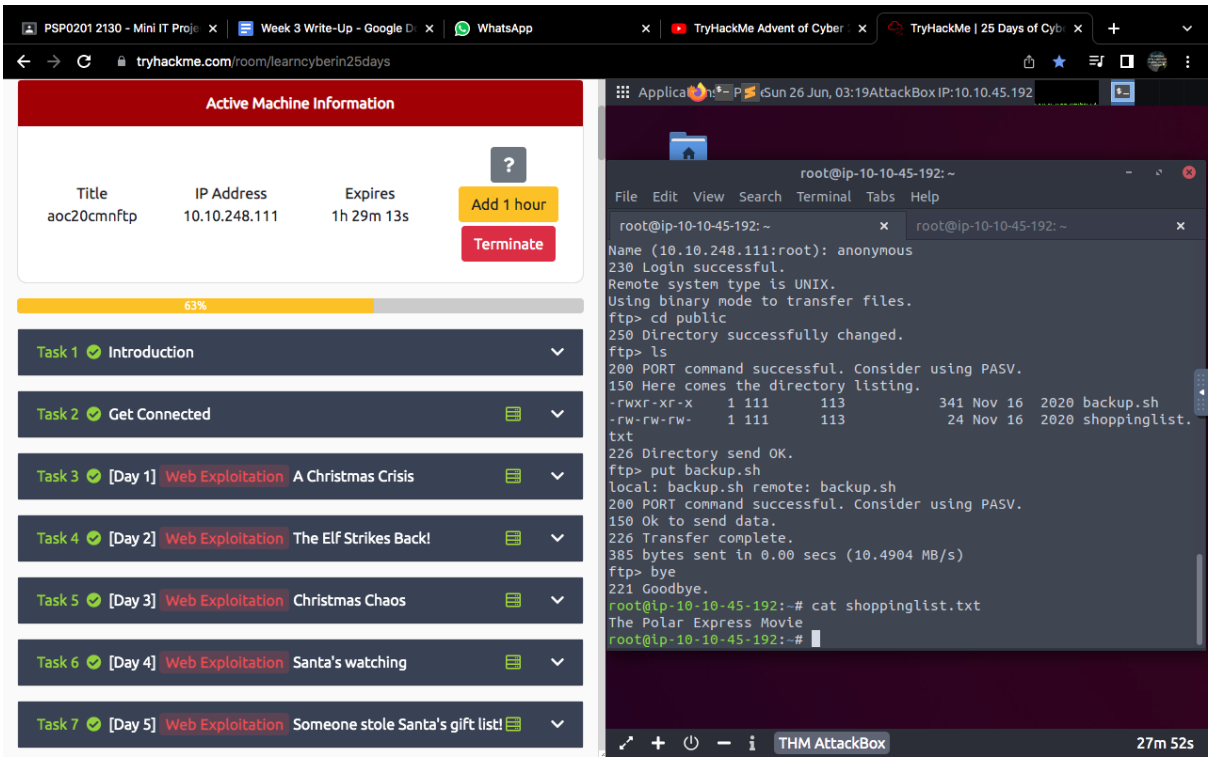
What script gets executed within this directory?



The backup.sh script gets executed within this directory as per highlighted in the terminal.

Question 4

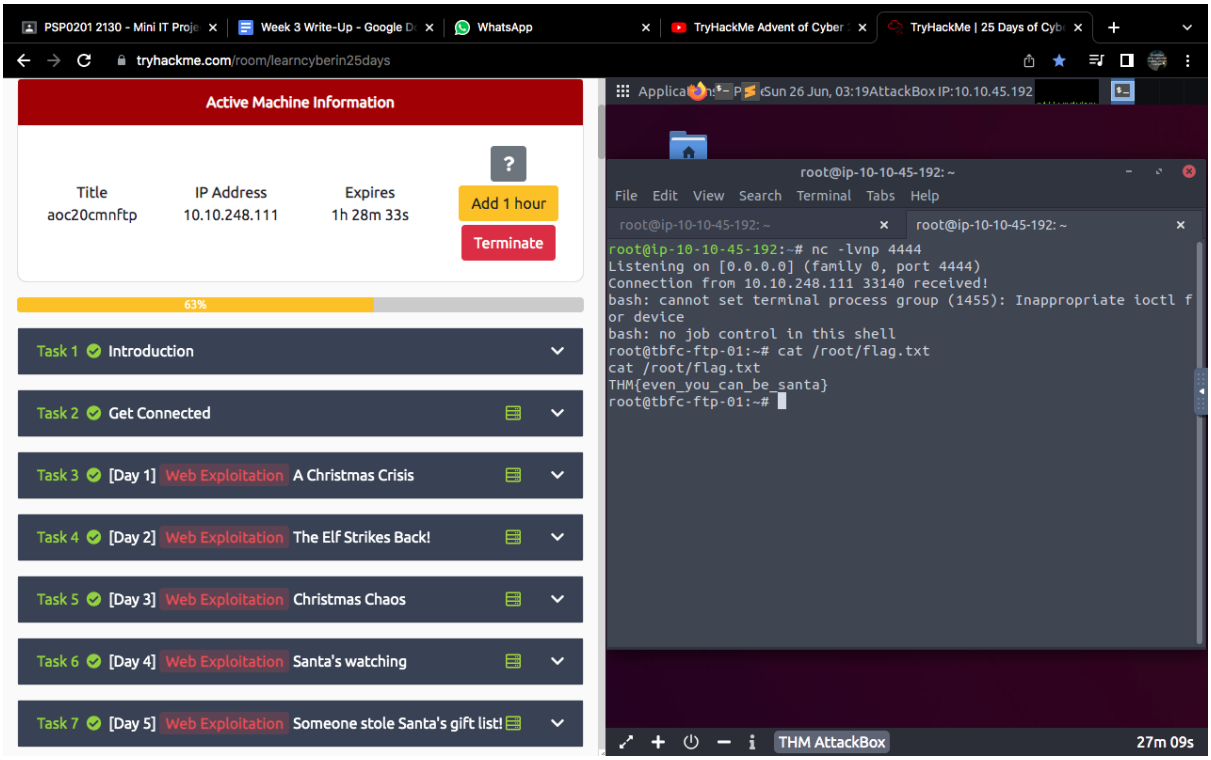
What movie did Santa have on his Christmas shopping list?



The Polar Express was the movie Santa had on his Christmas shopping list.

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!



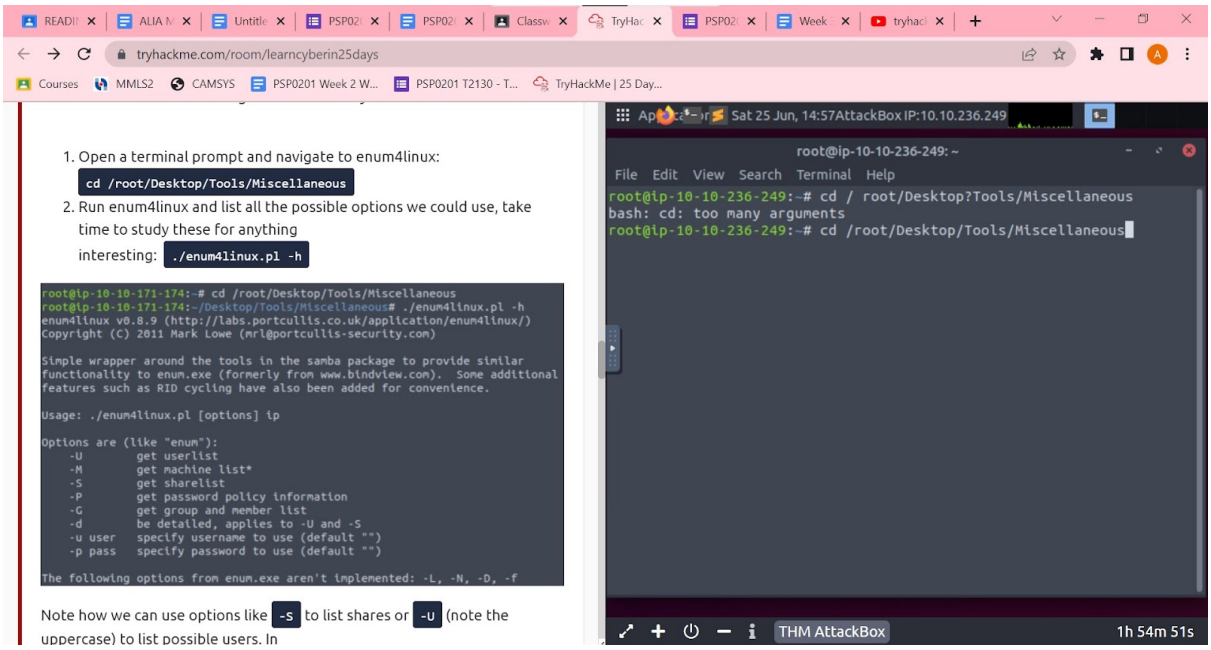
Thought Process/Methodology:

According to question 1 we have to go to the ftp ip address in the terminal and press anonymous and choose ls in order to ding the directories in the ftp site. As for question 2, type in ls in the ftp terminal so that we can get the directory on the FTP server that has data accessible by the "anonymous" user .Next , for question 3, to know what script gets executed within this directory is the get backup.sh directory. According to question 4, to find the movie that was in Santa's shopping list, type in cat shopping list.txt so that we will be able to find the movie which is The Polar Express Movie. For the last question which is about to find the flag, we have to go to the new terminal and type in /root/flag.txt to find out the flag for this question.

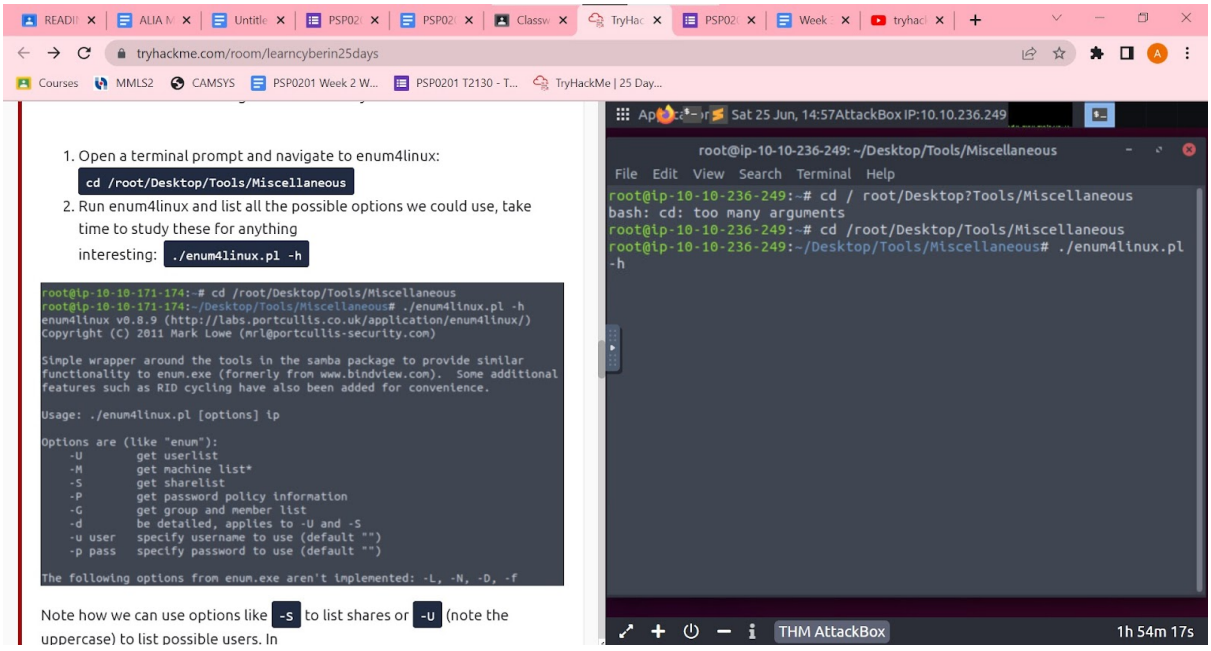
Day 10 : Networking - Don’t be sElfish!

Tools used : THM Attackbox, Chrome

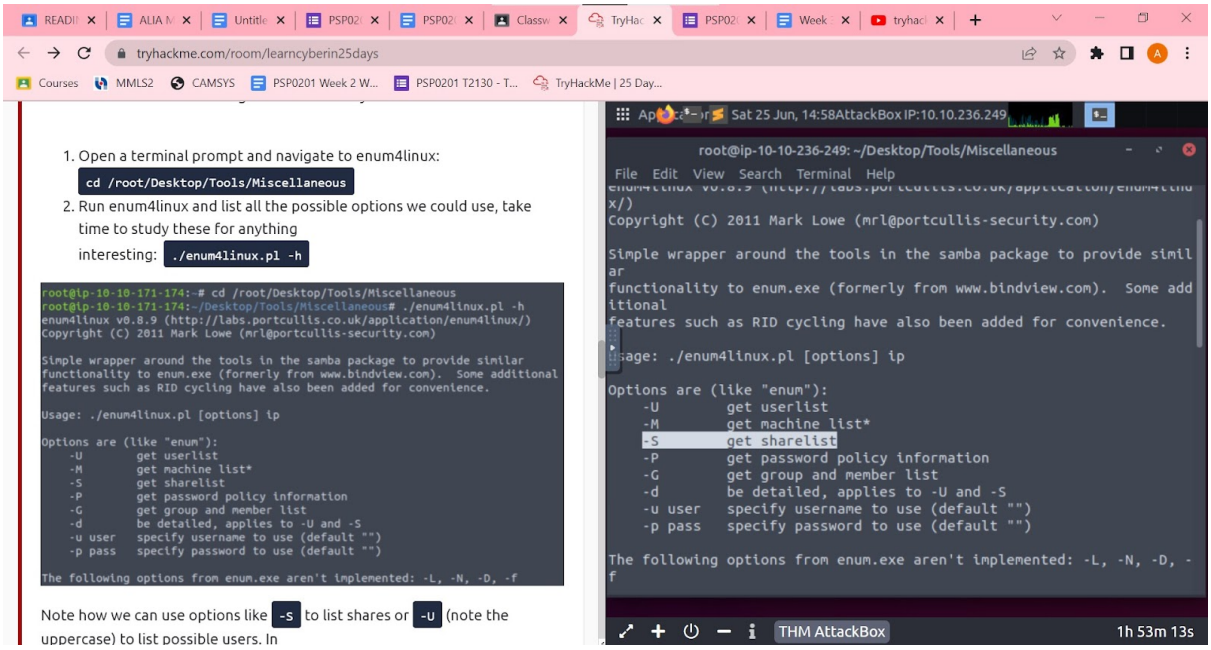
Question 1 : Examine the help options for enum4linux. Match the following flags with the descriptions.



Open /root/Desktop/Tools/Miscellaneous directory



Use enum4linux.pl -h to get help and get the list of command available



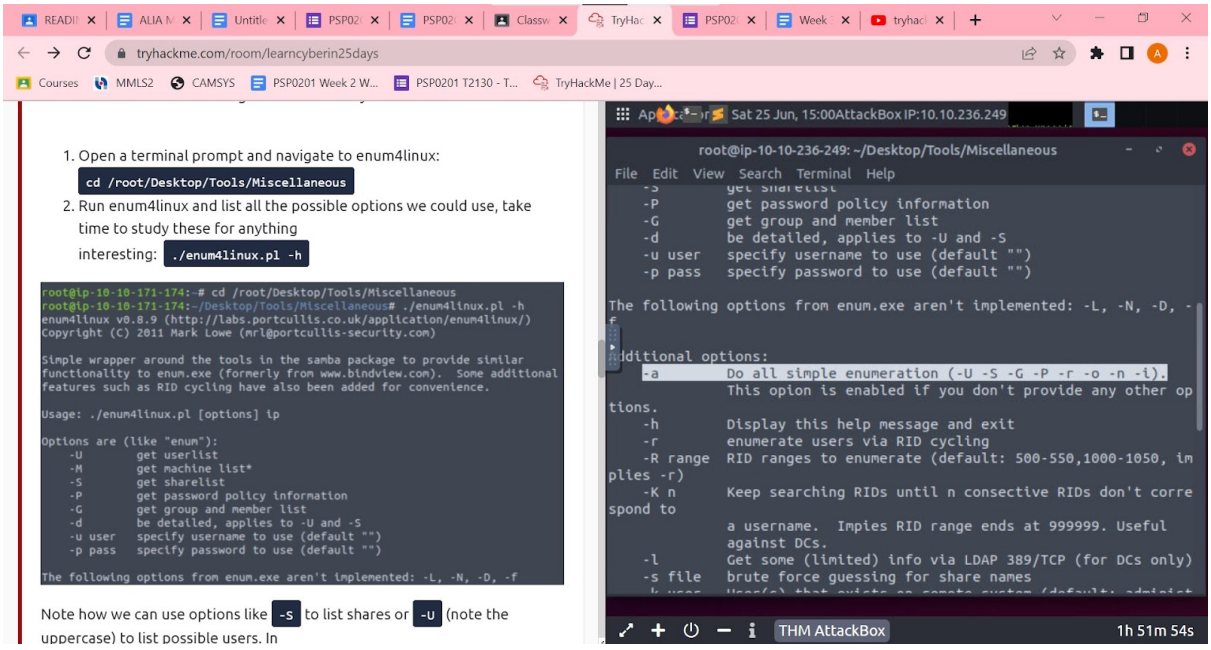
1. Open a terminal prompt and navigate to enum4linux:
   `cd /root/Desktop/Tools/Miscellaneous`
2. Run enum4linux and list all the possible options we could use, take time to study these for anything interesting: `./enum4linux.pl -h`

```
root@ip-10-10-171-174:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-171-174:~/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
```

Note how we can use options like `-S` to list shares or `-U` (note the uppercase) to list possible users. In

```
root@ip-10-10-236-249: ~/Desktop/Tools/Miscellaneous
File  Edit  View  Search  Terminal  Help
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.

sage: ./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
```

THM AttackBox 1h 53m 13s



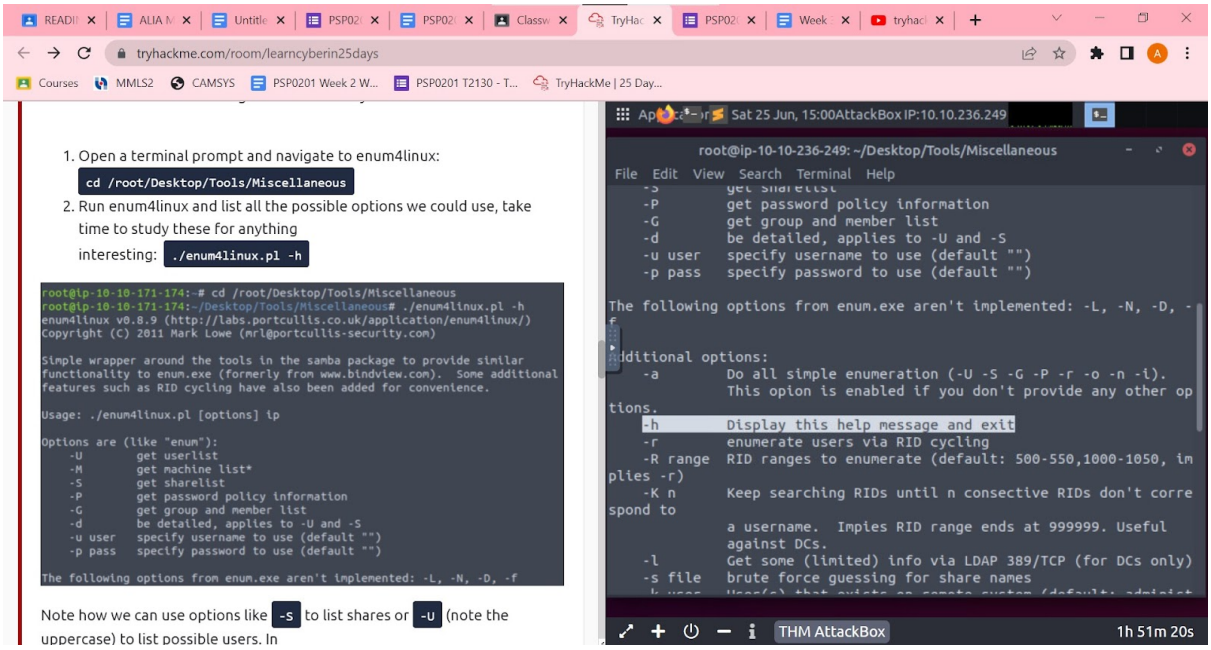
1. Open a terminal prompt and navigate to enum4linux:
   `cd /root/Desktop/Tools/Miscellaneous`
2. Run enum4linux and list all the possible options we could use, take time to study these for anything interesting: `./enum4linux.pl -h`

```
root@ip-10-10-171-174:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-171-174:~/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
```

Note how we can use options like `-S` to list shares or `-U` (note the uppercase) to list possible users. In

```
root@ip-10-10-236-249: ~/Desktop/Tools/Miscellaneous
File  Edit  View  Search  Terminal  Help
    -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

dditional 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 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)
    -K n      Keep searching RIDs until n consective RIDs don't corre
spond 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
```

THM AttackBox 1h 51m 54s



1. Open a terminal prompt and navigate to enum4linux:
   `cd /root/Desktop/Tools/Miscellaneous`
2. Run enum4linux and list all the possible options we could use, take time to study these for anything interesting: `./enum4linux.pl -h`

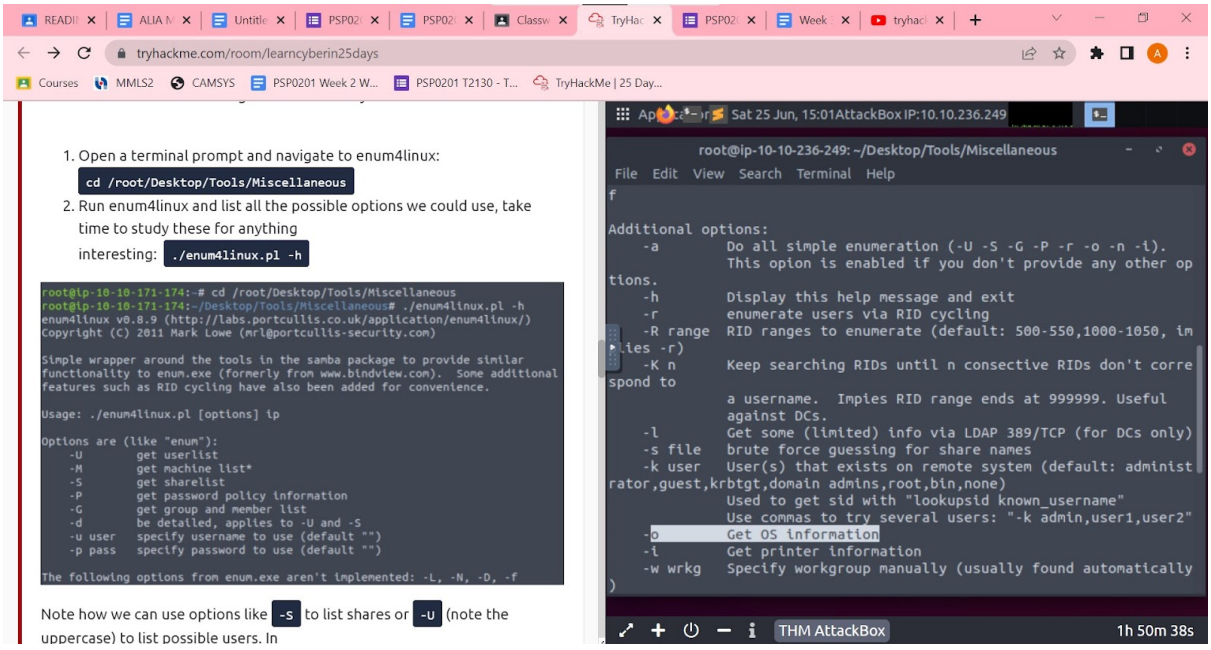
```
root@ip-10-10-171-174:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-171-174:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

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
```

Note how we can use options like `-S` to list shares or `-U` (note the uppercase) to list possible users. In

```
root@ip-10-10-236-249: ~/Desktop/Tools/Miscellaneous
File  Edit  View  Search  Terminal  Help
    -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 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)
    -K n      Keep searching RIDs until n consective RIDs don't corre
spond 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
```

Sat 25 Jun, 15:00 AttackBox IP:10.10.236.249

THM AttackBox 1h 51m 20s



1. Open a terminal prompt and navigate to enum4linux:
   `cd /root/Desktop/Tools/Miscellaneous`
2. Run enum4linux and list all the possible options we could use, take time to study these for anything interesting: `./enum4linux.pl -h`

```
root@ip-10-10-171-174:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-171-174:~/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
```

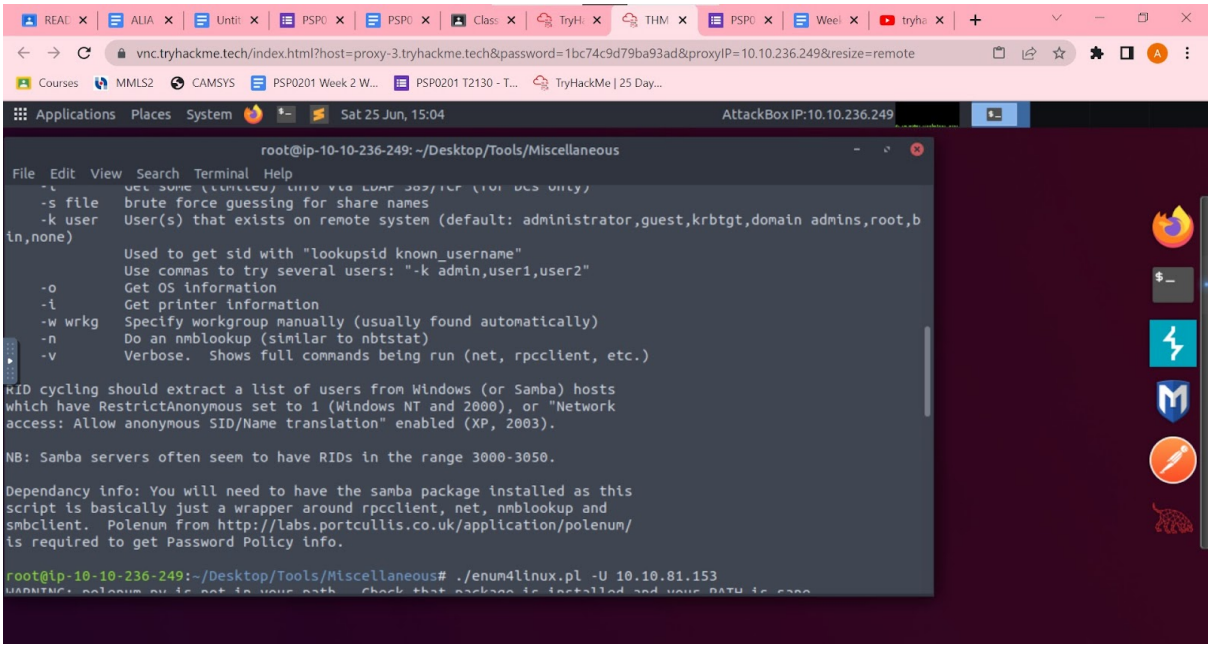
Note how we can use options like `-S` to list shares or `-U` (note the uppercase) to list possible users. In

```
root@ip-10-10-236-249: ~/Desktop/Tools/Miscellaneous
File  Edit  View  Search  Terminal  Help
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 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)
    -K n      Keep searching RIDs until n consective RIDs don't corre
spond 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: administ
rator,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
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically
)
```

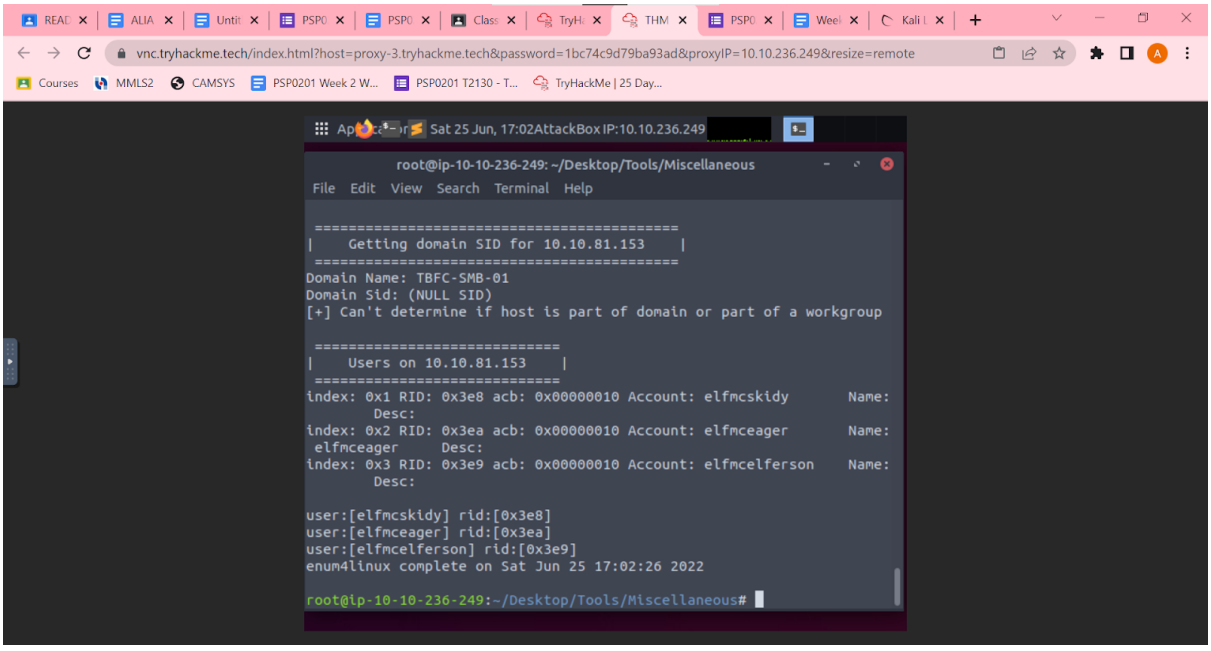
Sat 25 Jun, 15:01 AttackBox IP:10.10.236.249

THM AttackBox 1h 50m 38s

Question 2 : Using enum4linux, how many users are there on the Samba server?

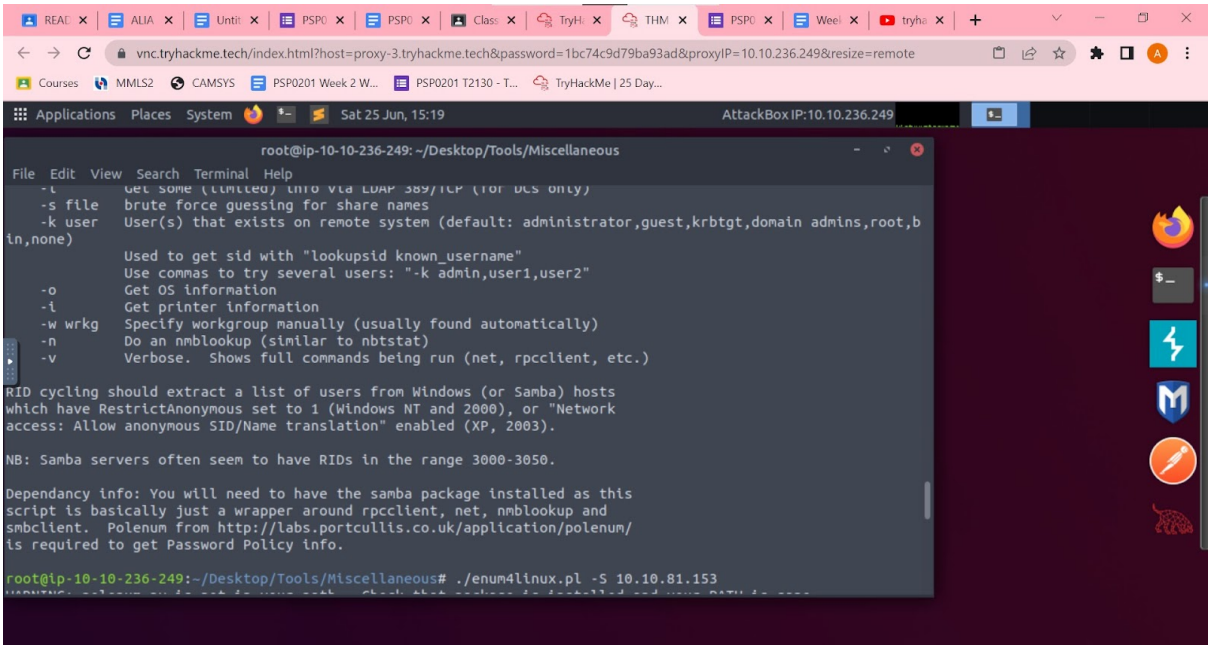


Use enum4linux.pl -U to get a list of username

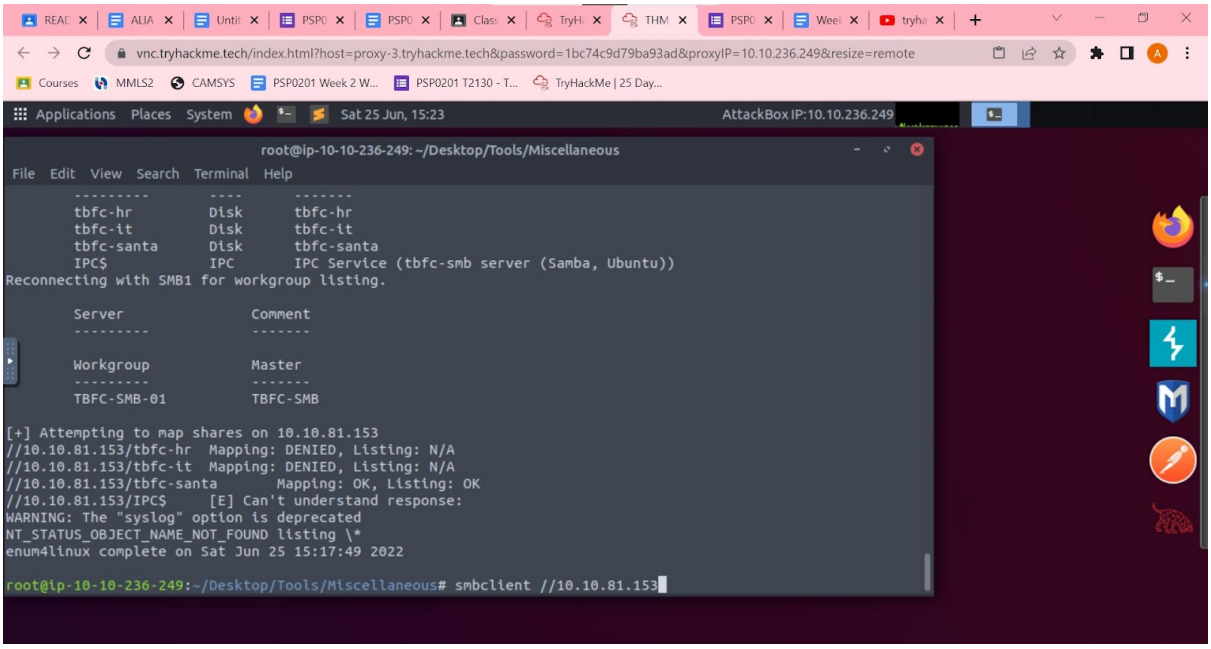


The number of users in this server is 3

Question 3 : Now how many "shares" are there on the Samba server?

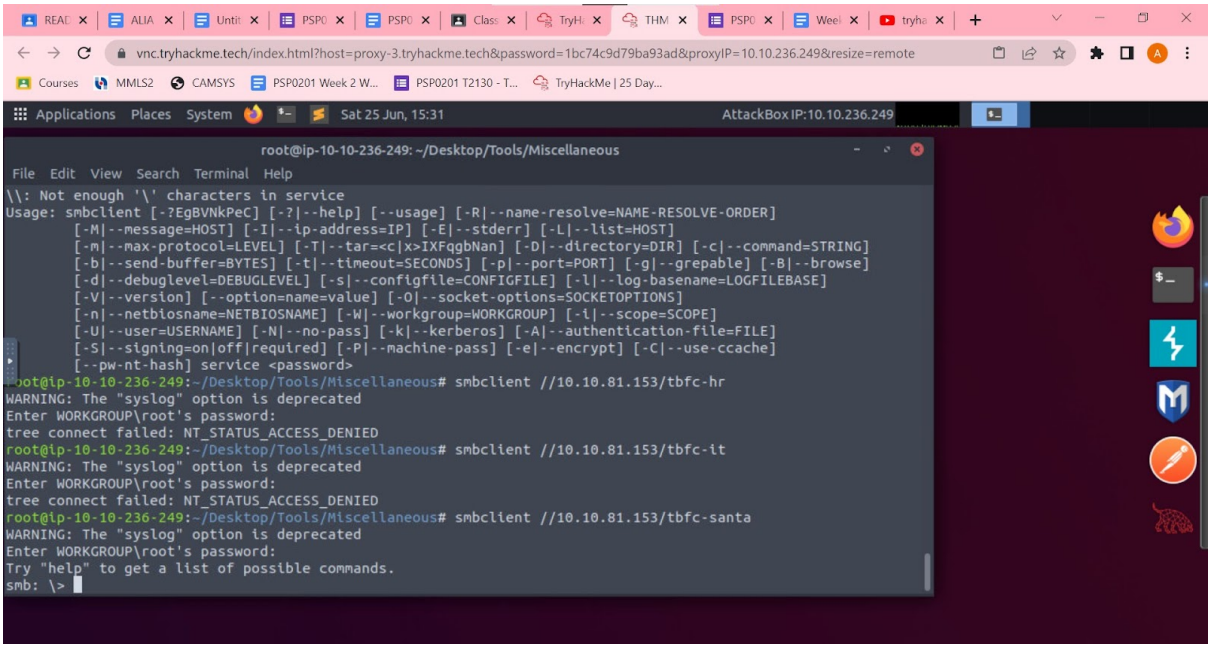


Use enum4linux.pl -s to get a list of the shares that this server has



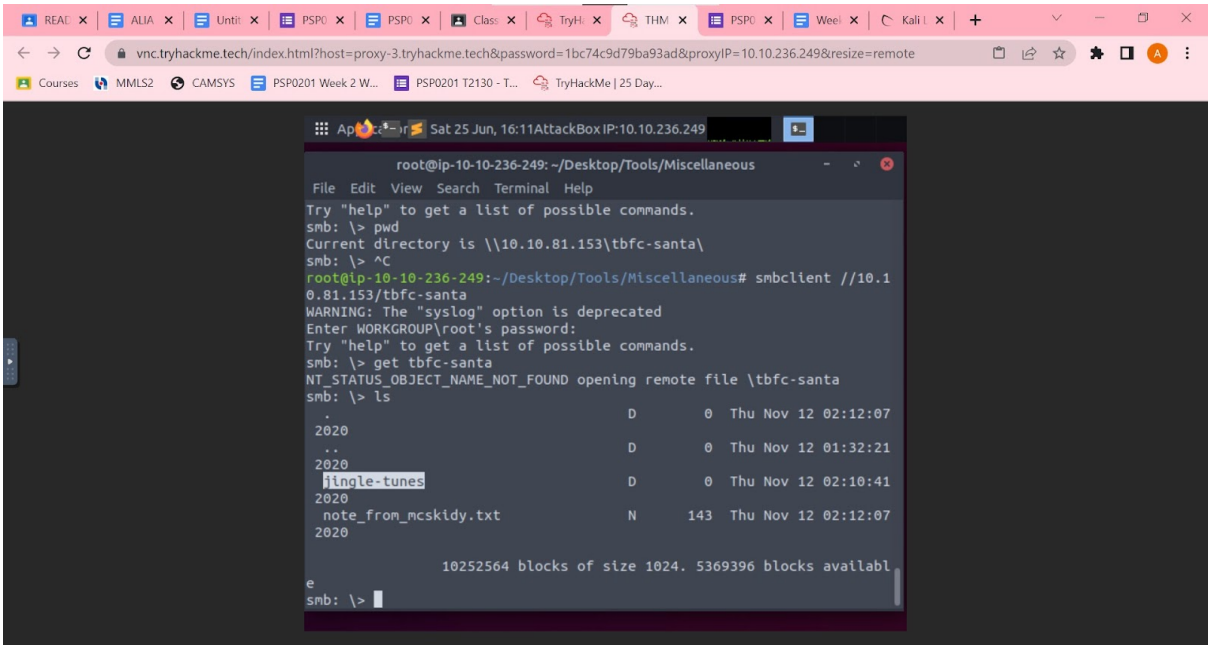
The list of share this server has is 4

Question 4: Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?



The share that doesn't require a password is tbfc-santa

Question 5: Log in to this share, what directory did ElfMcSkidy leave for Santa?



After logging in to the share, we used ls command to get a list of directories that exist in this share. The directory that ElfMcSkidy leave for Santa is jingle-tunes

Thought Process/Methodology:

Enum4linux is a very important command that can help you a lot with your work. To know further about enum4linux, we used the help command to get a list of commands that can be used for our mission. To get a list of users on the server, we use the -u command from

enum4linux. After getting the list of users that are in the server, we also find the shares from the server by using the -s command. Using smbclient, we tried to log in to all the shares in the server to find one that doesn’t require a password which is tbfc-santa. After we successfully log in to the share, we get a list of directories that was given to santa by using the ls command.