PSP0201 Week 3 Writeup

Group Name: SupremeChickens

Members

ID	Name	Role
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	Member
1211101198	Fam YI Qi	Member
1211103978	DIckshen	Member

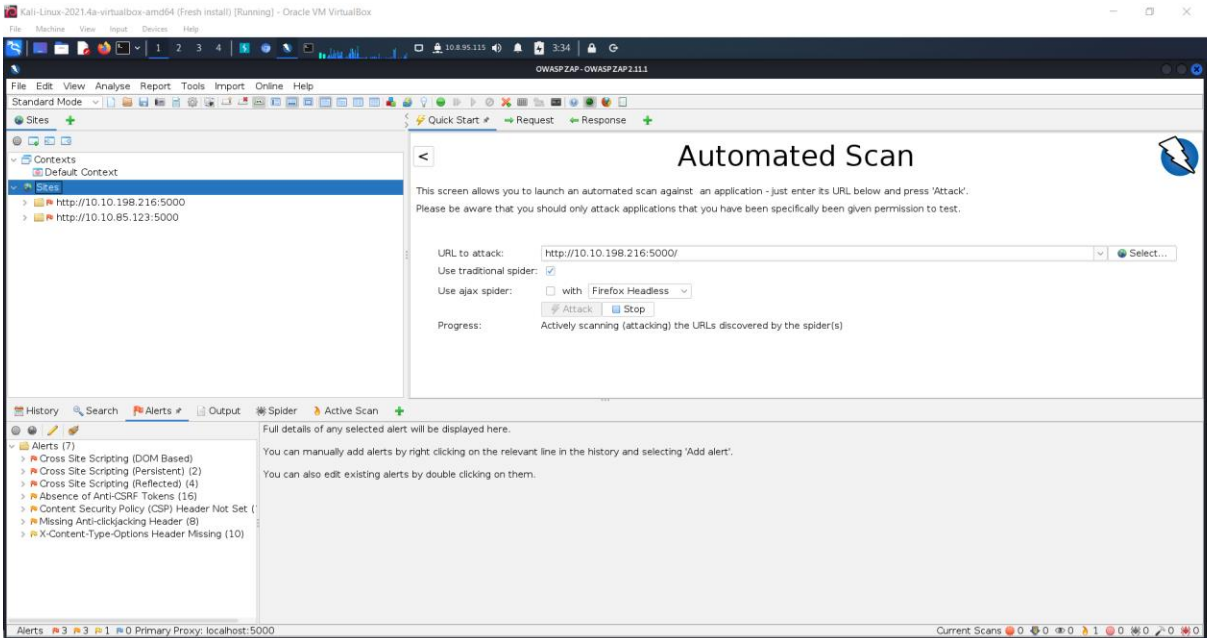
Day 6: Web Exploitation - Be careful with what you wish on a Christmas night

Tools used: Kali Linux, Chrome

Solution/walkthrough:

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

A5: 2



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
3:34
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
http://10.10.198.216:5000
http://10.10.85.123:5000
History
Search
Alerts
Output
Spider
Active Scan
Attack
Stop
Select...

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://10.10.198.216:5000/

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

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

```
Alerts (7)
  Cross Site Scripting (DOM Based)
  Cross Site Scripting (Persistent) (2)
  Cross Site Scripting (Reflected) (4)
  Absence of Anti-CSRF Tokens (16)
  Content Security Policy (CSP) Header Not Set (
  Missing Anti-clickjacking Header (8)
  X-Content-Type-Options Header Missing (10)
```

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevant line in the history and selecting 'Add alert'.

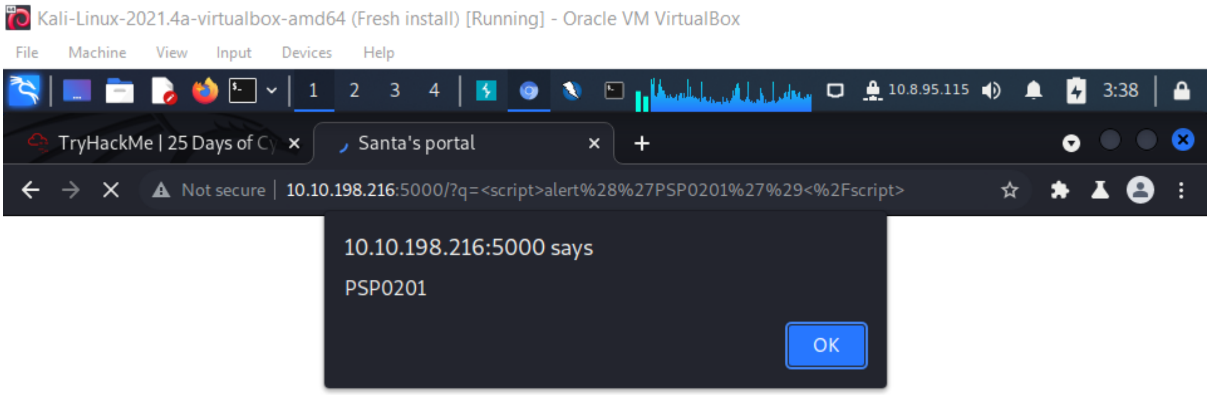
You can also edit existing alerts by double clicking on them.

Alerts 3 3 1 0 Primary Proxy: localhost:5000

Current Scans 0 0 0 1 0 0 0 0

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

A6: <script>alert('PSP0201')</script>



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

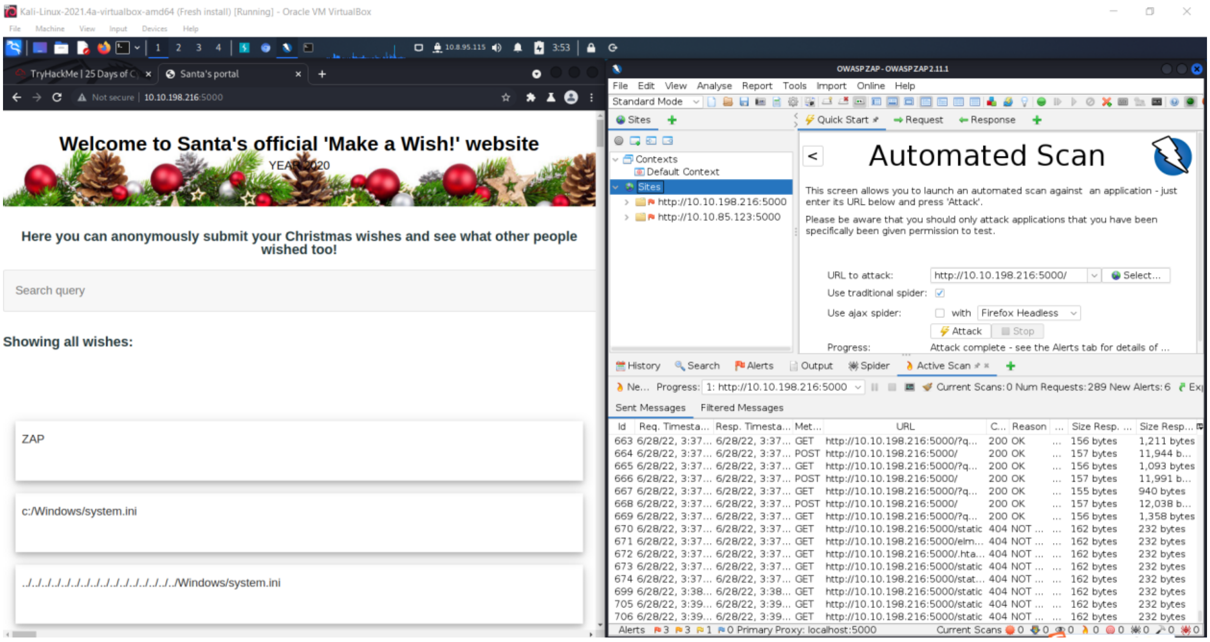
10.10.198.216:5000/?q=<script>alert%28%27PSP0201%27%29<%2Fscript>

10.10.198.216:5000 says

PSP0201

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

A7: No



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

10.10.198.216:5000

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:

ZAP

c:/Windows/system.ini

../../../../../../../../../../../../../../../../Windows/system.ini

OWASP ZAP - OWASP ZAP 2.11.1

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://10.10.198.216:5000/

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Attack complete - see the Alerts tab for details of ...

Sites: http://10.10.198.216:5000, http://10.10.85.123:5000

Progress: 1: http://10.10.198.216:5000 Current Scans: 0 Num Requests: 289 New Alerts: 6

Id	Req. Timesta...	Resp. Timesta...	Met...	URL	C...	Reason	...	Size Resp. ...	Size Resp...
663	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/?q...	200	OK	...	156 bytes	1,211 bytes
664	6/28/22, 3:37...	6/28/22, 3:37...	POST	http://10.10.198.216:5000/	200	OK	...	157 bytes	11,944 b...
665	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/?q...	200	OK	...	156 bytes	1,093 bytes
666	6/28/22, 3:37...	6/28/22, 3:37...	POST	http://10.10.198.216:5000/	200	OK	...	157 bytes	11,991 b...
667	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/?q...	200	OK	...	155 bytes	940 bytes
668	6/28/22, 3:37...	6/28/22, 3:37...	POST	http://10.10.198.216:5000/	200	OK	...	157 bytes	12,038 b...
669	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/?q...	200	OK	...	156 bytes	1,358 bytes
670	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/static	404	NOT ...	...	162 bytes	232 bytes
671	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/elm...	404	NOT ...	...	162 bytes	232 bytes
672	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/.hta...	404	NOT ...	...	162 bytes	232 bytes
673	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/static	404	NOT ...	...	162 bytes	232 bytes
674	6/28/22, 3:37...	6/28/22, 3:37...	GET	http://10.10.198.216:5000/stat...	404	NOT ...	...	162 bytes	232 bytes
699	6/28/22, 3:38...	6/28/22, 3:38...	GET	http://10.10.198.216:5000/static	404	NOT ...	...	162 bytes	232 bytes
705	6/28/22, 3:39...	6/28/22, 3:39...	GET	http://10.10.198.216:5000/static	404	NOT ...	...	162 bytes	232 bytes
706	6/28/22, 3:39...	6/28/22, 3:39...	GET	http://10.10.198.216:5000/static	404	NOT ...	...	162 bytes	232 bytes

Alerts 3 3 1 0 Primary Proxy: localhost:5000

Thought Process/Methodology:

First, I access the OWASP cheatsheet series and check the regular expression used to validate a US Zip code. Then, I go to the back-up server to key in random words in the query box to check what query string can be abused to craft a reflected XSS. Afterwards, I open ZAP and start automated scan to check how many XSS alerts of high priority are in the scan. Next, I know that the command for showing alert is <script>alert()</script>. Therefore, I key in <script>alert('PSP0201')</script> to show an alert saying 'PSP0201'. Then, I close my browser and revisit the site MACHINE-IP:5000 again, the XSS attack is not persisting anymore.

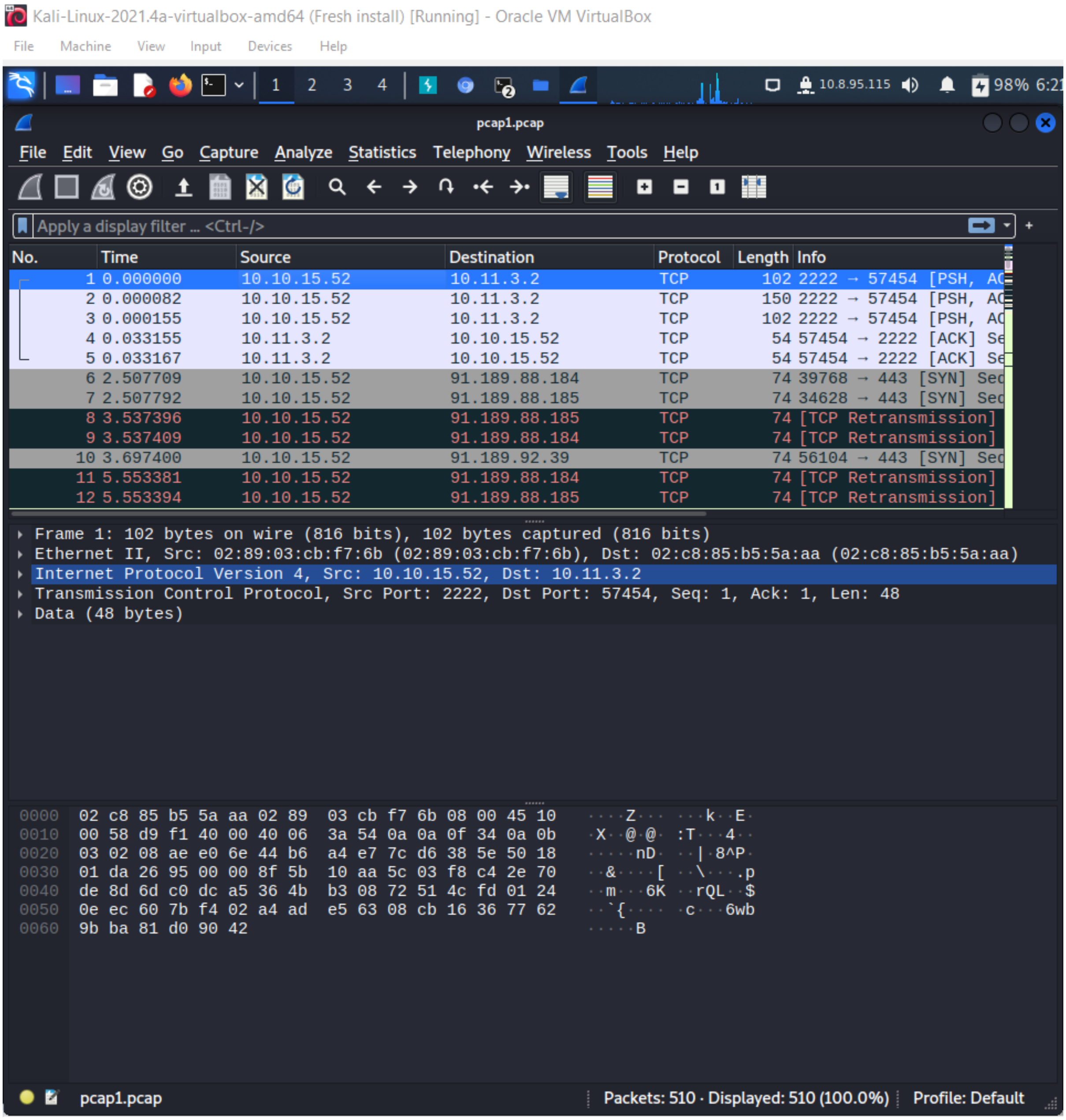
Day 7: Networking The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Chrome

Solution/walkthrough:

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

A1: 10.11.3.2



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
98% 6:2
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time       Source        Destination    Protocol Length Info
   1 0.000000   10.10.15.52   10.11.3.2      TCP       102 2222 → 57454 [PSH, AC
   2 0.000082   10.10.15.52   10.11.3.2      TCP       150 2222 → 57454 [PSH, AC
   3 0.000155   10.10.15.52   10.11.3.2      TCP       102 2222 → 57454 [PSH, AC
   4 0.033155   10.11.3.2     10.10.15.52    TCP        54 57454 → 2222 [ACK] Se
   5 0.033167   10.11.3.2     10.10.15.52    TCP        54 57454 → 2222 [ACK] Se
   6 2.507709   10.10.15.52   91.189.88.184  TCP        74 39768 → 443 [SYN] Seq
   7 2.507792   10.10.15.52   91.189.88.185  TCP        74 34628 → 443 [SYN] Seq
   8 3.537396   10.10.15.52   91.189.88.185  TCP        74 [TCP Retransmission]
   9 3.537409   10.10.15.52   91.189.88.184  TCP        74 [TCP Retransmission]
  10 3.697400   10.10.15.52   91.189.92.39   TCP        74 56104 → 443 [SYN] Seq
  11 5.553381   10.10.15.52   91.189.88.184  TCP        74 [TCP Retransmission]
  12 5.553394   10.10.15.52   91.189.88.185  TCP        74 [TCP Retransmission]
```

```
› 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 (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, Len: 48
› 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
```

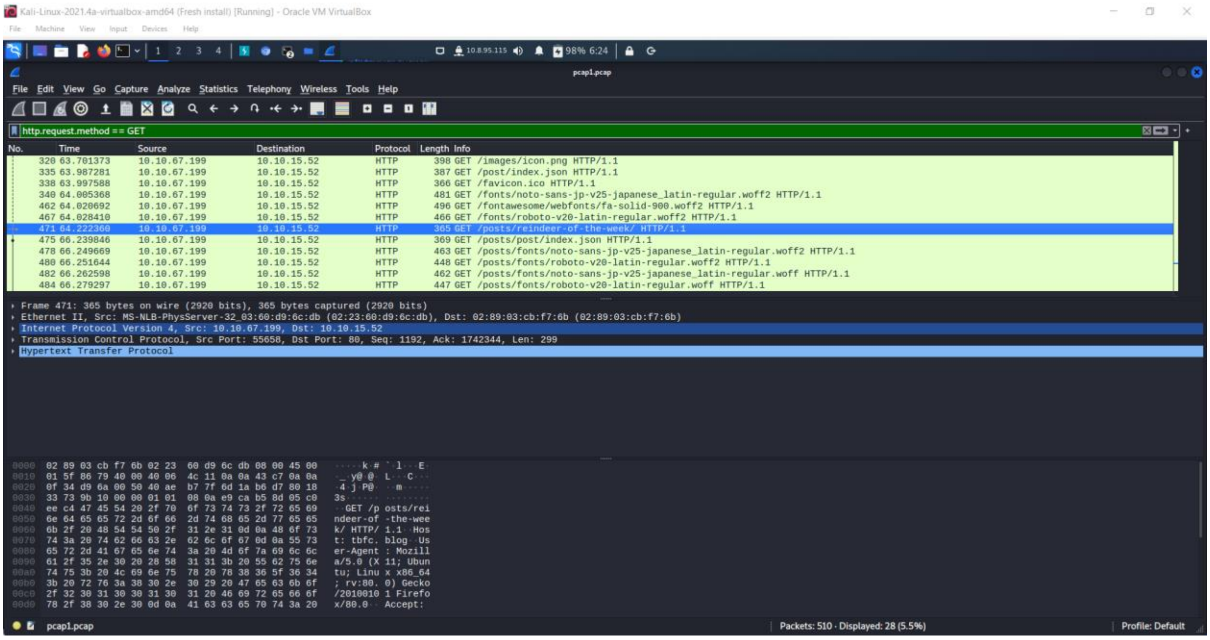
pcap1.pcap | Packets: 510 · Displayed: 510 (100.0%) | Profile: Default

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

A2: http.request.method == GET

Q3: Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

A3: reindeer-of-the-week



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
98% 6:24
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == GET
```

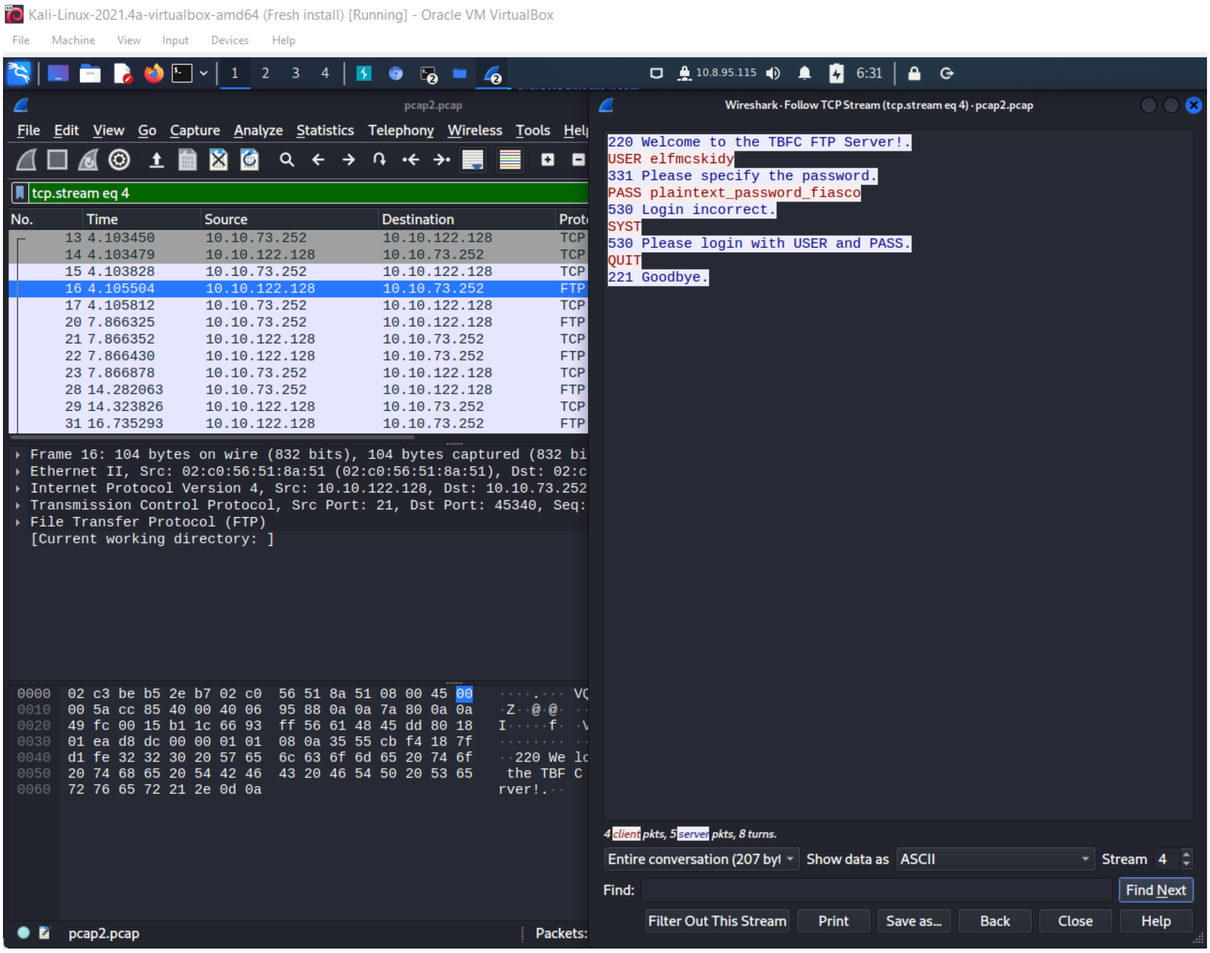
```
No.     Time       Source          Destination     Protocol  Length Info
    320 63.701373  10.10.67.199    10.10.15.52     HTTP      398 GET /images/icon.png HTTP/1.1
    335 63.987281  10.10.67.199    10.10.15.52     HTTP      387 GET /post/index.json HTTP/1.1
    338 63.997588  10.10.67.199    10.10.15.52     HTTP      366 GET /favicon.ico HTTP/1.1
    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
    482 66.262598  10.10.67.199    10.10.15.52     HTTP      462 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff HTTP/1.1
    484 66.279297  10.10.67.199    10.10.15.52     HTTP      447 GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1
```

```
▸ Frame 471: 365 bytes on wire (2920 bits), 365 bytes captured (2920 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: 55658, Dst Port: 80, Seq: 1192, Ack: 1742344, Len: 299
▸ Hypertext Transfer Protocol
```

```
0000  02 89 03 cb f7 6b 02 23  60 d9 6c db 08 00 45 00   ·····k·# `·l···E·
0010  01 5f 86 79 40 00 40 06  4c 11 0a 0a 43 c7 0a 0a   ·_·y@·@· L···C···
0020  0f 34 d9 6a 00 50 40 ae  b7 7f 6d 1a b6 d7 80 18   ·4·j·P@· ··m·····
0030  33 73 9b 10 00 00 01 01  08 0a e9 ca b5 8d 05 c0   3s······ ········
0040  ee c4 47 45 54 20 2f 70  6f 73 74 73 2f 72 65 69   ··GET /p osts/rei
0050  6e 64 65 65 72 2d 6f 66  2d 74 68 65 2d 77 65 65   ndeer-of -the-wee
0060  6b 2f 20 48 54 54 50 2f  31 2e 31 0d 0a 48 6f 73   k/ HTTP/ 1.1··Hos
0070  74 3a 20 74 62 66 63 2e  62 6c 6f 67 0d 0a 55 73   t: tbfc. blog··Us
0080  65 72 2d 41 67 65 6e 74  3a 20 4d 6f 7a 69 6c 6c   er-Agent : Mozill
0090  61 2f 35 2e 30 20 28 58  31 31 3b 20 55 62 75 6e   a/5.0 (X 11; Ubun
00a0  74 75 3b 20 4c 69 6e 75  78 20 78 38 36 5f 36 34   tu; Linu x x86_64
00b0  3b 20 72 76 3a 38 30 2e  30 29 20 47 65 63 6b 6f   ; rv:80. 0) Gecko
00c0  2f 32 30 31 30 30 31 30  31 20 46 69 72 65 66 6f   /2010010 1 Firefo
00d0  78 2f 38 30 2e 30 0d 0a  41 63 63 65 70 74 3a 20   x/80.0·· Accept:
```

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

A4: paintext_password_fiasco


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
6:31
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap2.pcap

tcp.stream eq 4

```
No.  Time          Source          Destination     Proto
  13 4.103450      10.10.73.252    10.10.122.128   TCP
  14 4.103479      10.10.122.128   10.10.73.252    TCP
  15 4.103828      10.10.73.252    10.10.122.128   TCP
  16 4.105504      10.10.122.128   10.10.73.252    FTP
  17 4.105812      10.10.73.252    10.10.122.128   TCP
  20 7.866325      10.10.73.252    10.10.122.128   FTP
  21 7.866352      10.10.122.128   10.10.73.252    TCP
  22 7.866430      10.10.122.128   10.10.73.252    FTP
  23 7.866878      10.10.73.252    10.10.122.128   TCP
  28 14.282063     10.10.73.252    10.10.122.128   FTP
  29 14.323826     10.10.122.128   10.10.73.252    TCP
  31 16.735293     10.10.122.128   10.10.73.252    FTP
```

```
▸ Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bi
▸ Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c
▸ Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq:
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  02 c3 be b5 2e b7 02 c0  56 51 8a 51 08 00 45 00   ····.··· VQ
0010  00 5a cc 85 40 00 40 06  95 88 0a 0a 7a 80 0a 0a   ·Z··@·@· ··
0020  49 fc 00 15 b1 1c 66 93  ff 56 61 48 45 dd 80 18   I·····f· ·V
0030  01 ea d8 dc 00 00 01 01  08 0a 35 55 cb f4 18 7f   ········ ··
0040  d1 fe 32 32 30 20 57 65  6c 63 6f 6d 65 20 74 6f   ··220 We lc
0050  20 74 68 65 20 54 42 46  43 20 46 54 50 20 53 65    the TBF C
0060  72 76 65 72 21 2e 0d 0a                            rver!.··
```

pcap2.pcap | Packets:

```
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
331 Please specify the password.
PASS plaintext_password_fiasco
530 Login incorrect.
SYST
530 Please login with USER and PASS.
QUIT
221 Goodbye.
```

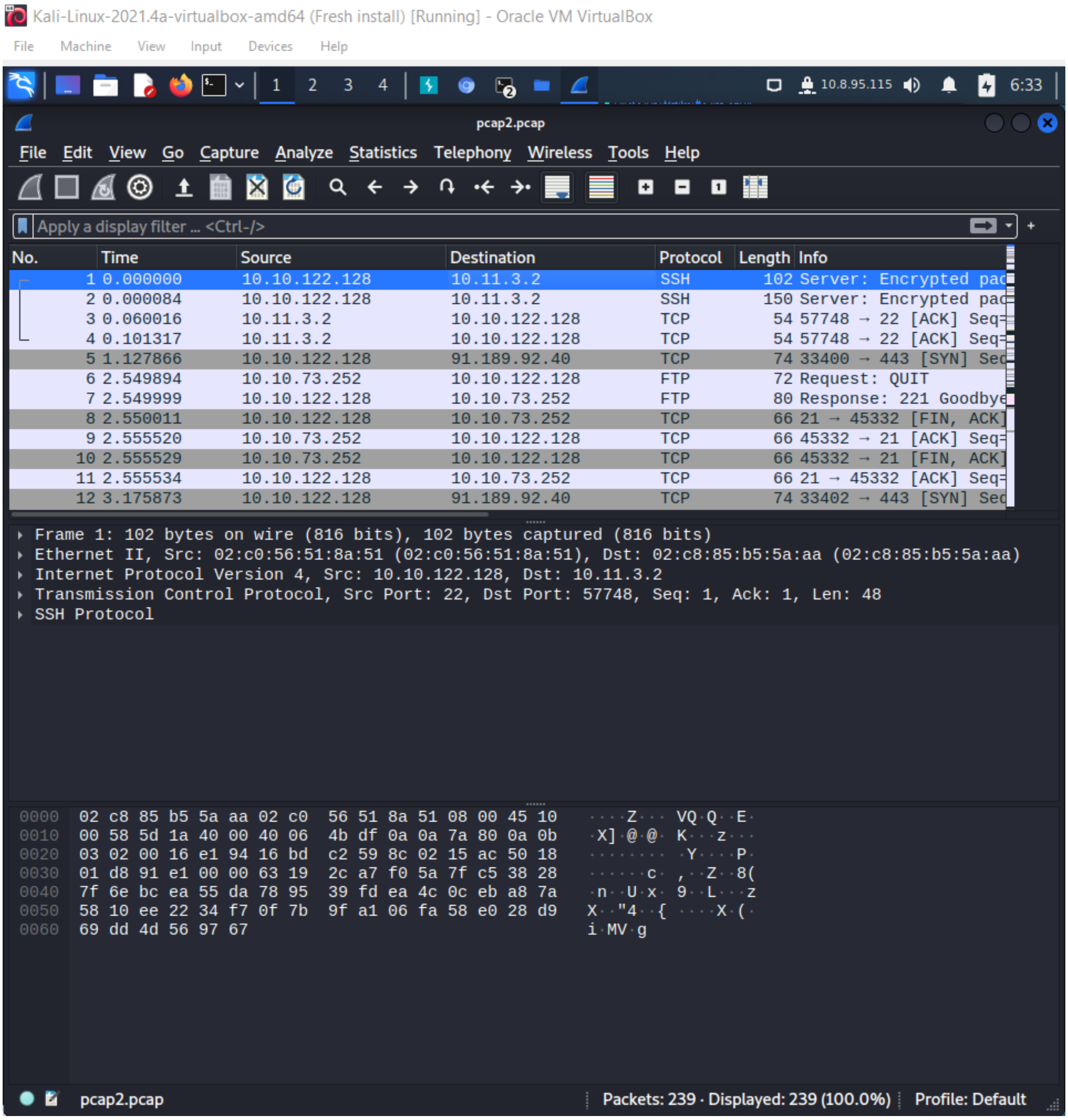
4 client pkts, 5 server pkts, 8 turns.

Entire conversation (207 byt | Show data as: ASCII | Stream 4

Find:

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

A5: SSH



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
6:33
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.   Time      Source          Destination     Protocol Length Info
    1 0.000000  10.10.122.128   10.11.3.2       SSH       102 Server: Encrypted pac
    2 0.000084  10.10.122.128   10.11.3.2       SSH       150 Server: Encrypted pac
    3 0.060016  10.11.3.2       10.10.122.128   TCP        54 57748 → 22 [ACK] Seq=
    4 0.101317  10.11.3.2       10.10.122.128   TCP        54 57748 → 22 [ACK] Seq=
    5 1.127866  10.10.122.128   91.189.92.40    TCP        74 33400 → 443 [SYN] Seq
    6 2.549894  10.10.73.252    10.10.122.128   FTP        72 Request: QUIT
    7 2.549999  10.10.122.128   10.10.73.252    FTP        80 Response: 221 Goodbye
    8 2.550011  10.10.122.128   10.10.73.252    TCP        66 21 → 45332 [FIN, ACK]
    9 2.555520  10.10.73.252    10.10.122.128   TCP        66 45332 → 21 [ACK] Seq=
   10 2.555529  10.10.73.252    10.10.122.128   TCP        66 45332 → 21 [FIN, ACK]
   11 2.555534  10.10.122.128   10.10.73.252    TCP        66 21 → 45332 [ACK] Seq=
   12 3.175873  10.10.122.128   91.189.92.40    TCP        74 33402 → 443 [SYN] Seq
```

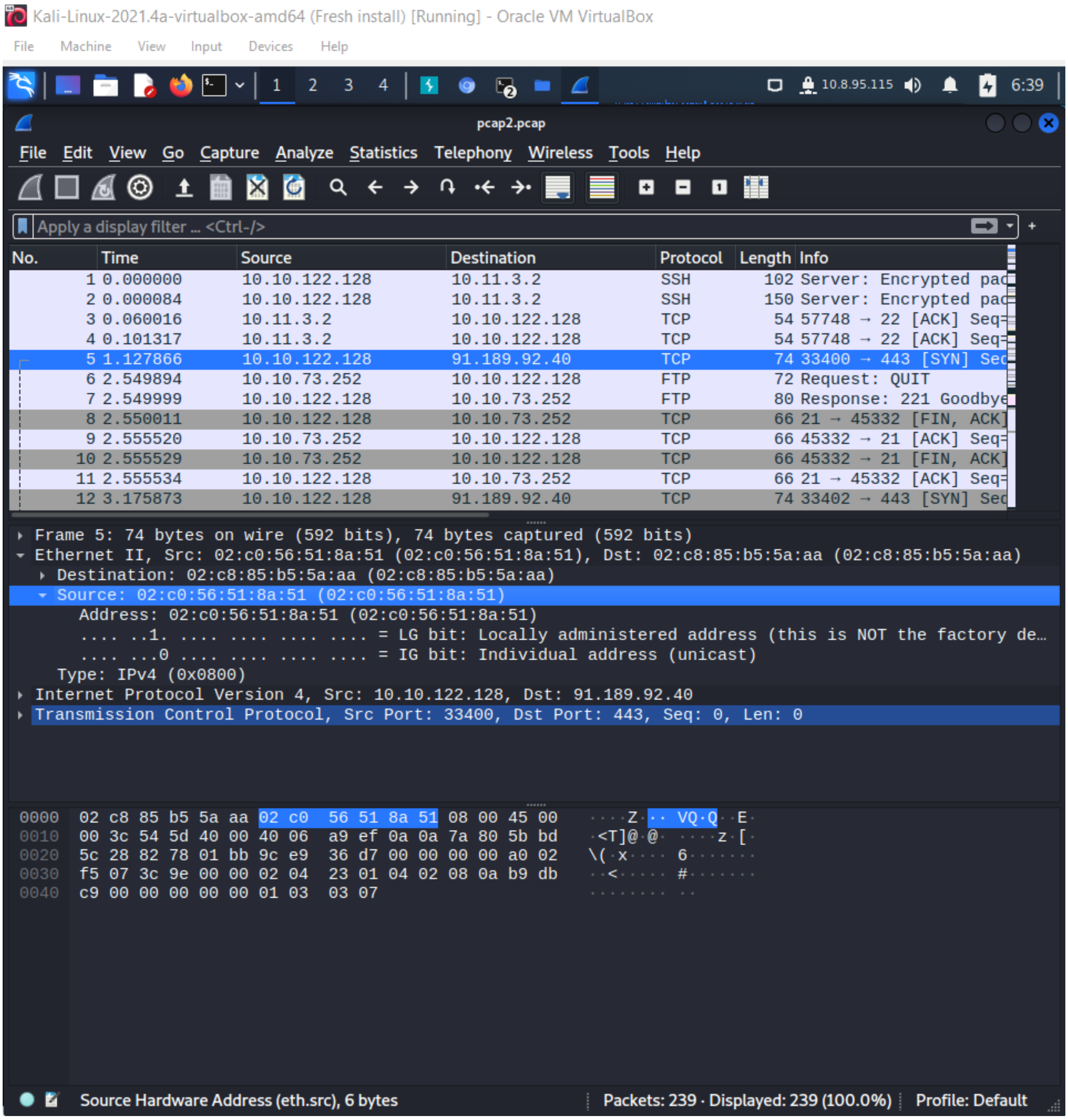
```
Frame 1: 102 bytes on wire (816 bits), 102 bytes captured (816 bits)
Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.11.3.2
Transmission Control Protocol, Src Port: 22, Dst Port: 57748, Seq: 1, Ack: 1, Len: 48
SSH Protocol
```

```
0000  02 c8 85 b5 5a aa 02 c0  56 51 8a 51 08 00 45 10   ····Z···  VQ·Q··E·
0010  00 58 5d 1a 40 00 40 06  4b df 0a 0a 7a 80 0a 0b   ·X]·@·@·  K···z···
0020  03 02 00 16 e1 94 16 bd  c2 59 8c 02 15 ac 50 18   ········  ·Y····P·
0030  01 d8 91 e1 00 00 63 19  2c a7 f0 5a 7f c5 38 28   ······c·  ,··Z··8(
0040  7f 6e bc ea 55 da 78 95  39 fd ea 4c 0c eb a8 7a   ·n··U·x·  9··L···z
0050  58 10 ee 22 34 f7 0f 7b  9f a1 06 fa 58 e0 28 d9   X··"4··{  ····X·(·
0060  69 dd 4d 56 97 67                                   i·MV·g
```

```
pcap2.pcap    Packets: 239 · Displayed: 239 (100.0%)    Profile: Default
```

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

A6: 02:c0:56:51:8a:51


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115 6:39
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

```
No.  Time        Source          Destination     Protocol Length Info
   1 0.000000    10.10.122.128   10.11.3.2       SSH      102 Server: Encrypted pac
   2 0.000084    10.10.122.128   10.11.3.2       SSH      150 Server: Encrypted pac
   3 0.060016    10.11.3.2       10.10.122.128   TCP       54 57748 → 22 [ACK] Seq=
   4 0.101317    10.11.3.2       10.10.122.128   TCP       54 57748 → 22 [ACK] Seq=
   5 1.127866    10.10.122.128   91.189.92.40    TCP       74 33400 → 443 [SYN] Sec
   6 2.549894    10.10.73.252    10.10.122.128   FTP       72 Request: QUIT
   7 2.549999    10.10.122.128   10.10.73.252    FTP       80 Response: 221 Goodbye
   8 2.550011    10.10.122.128   10.10.73.252    TCP       66 21 → 45332 [FIN, ACK]
   9 2.555520    10.10.73.252    10.10.122.128   TCP       66 45332 → 21 [ACK] Seq=
  10 2.555529    10.10.73.252    10.10.122.128   TCP       66 45332 → 21 [FIN, ACK]
  11 2.555534    10.10.122.128   10.10.73.252    TCP       66 21 → 45332 [ACK] Seq=
  12 3.175873    10.10.122.128   91.189.92.40    TCP       74 33402 → 443 [SYN] Sec
```

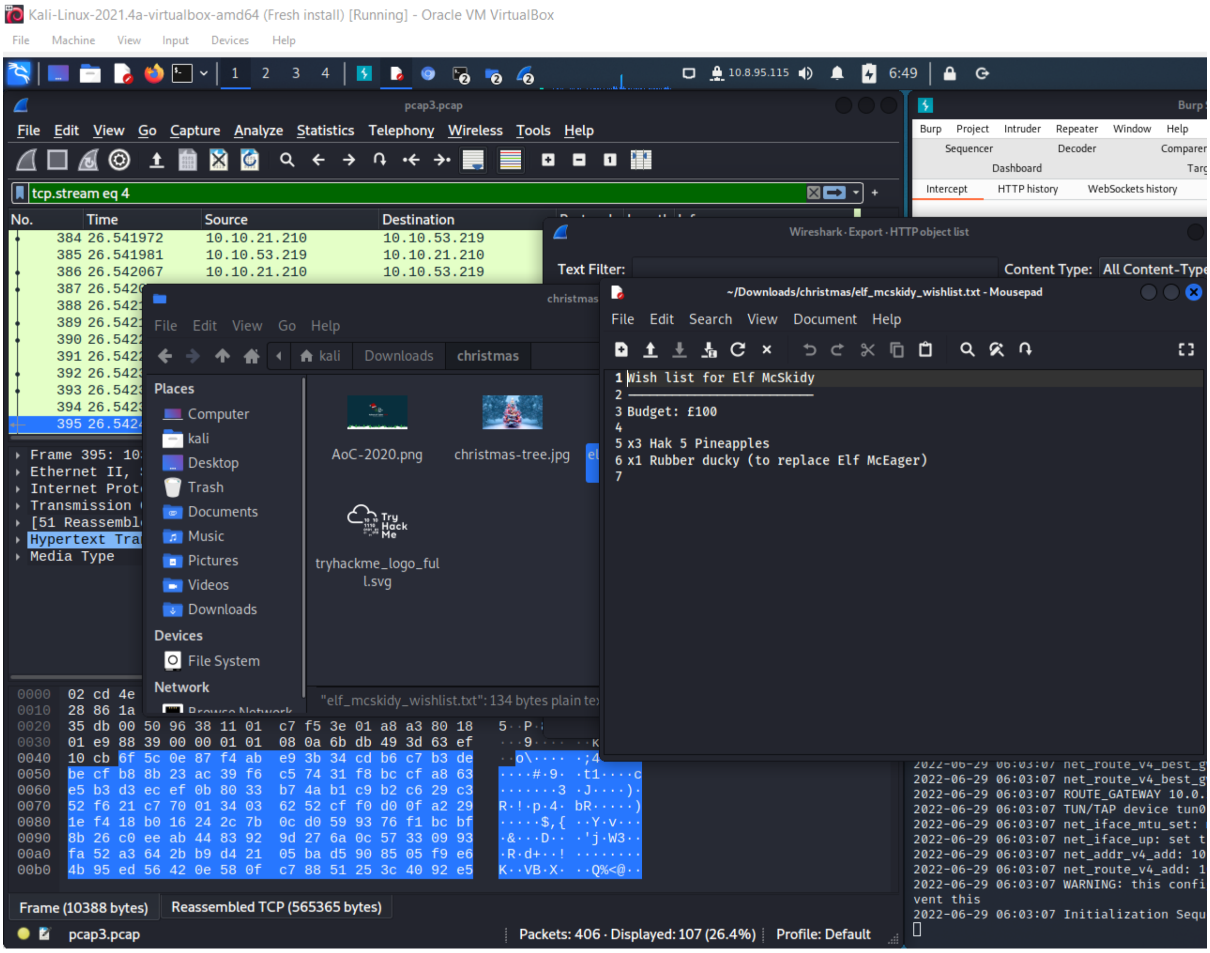
```
› Frame 5: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
⌄ Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
  › Destination: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
  ⌄ Source: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)
      Address: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)
      .... ..1. .... .... .... .... = LG bit: Locally administered address (this is NOT the factory de…
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
› Internet Protocol Version 4, Src: 10.10.122.128, Dst: 91.189.92.40
› Transmission Control Protocol, Src Port: 33400, Dst Port: 443, Seq: 0, Len: 0
```

```
0000  02 c8 85 b5 5a aa 02 c0  56 51 8a 51 08 00 45 00   ····Z··· VQ·Q··E·
0010  00 3c 54 5d 40 00 40 06  a9 ef 0a 0a 7a 80 5b bd   ·<T]@·@· ····z·[·
0020  5c 28 82 78 01 bb 9c e9  36 d7 00 00 00 00 a0 02   \(·x···· 6·······
0030  f5 07 3c 9e 00 00 02 04  23 01 04 02 08 0a b9 db   ··<····· #·······
0040  c9 00 00 00 00 00 01 03  03 07                     ········ ··
```

Source Hardware Address (eth.src), 6 bytes | Packets: 239 · Displayed: 239 (100.0%) | Profile: Default

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

A7: rubber ducky


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
6:49
pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Burp
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer
Dashboard Targ
Intercept HTTP history WebSockets history
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Type
christmas
File Edit View Go Help
kali Downloads christmas
Places
Computer
kali
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network
AoC-2020.png
christmas-tree.jpg
tryhackme_logo_full.svg
~/Downloads/christmas/elf_mcskidy_wishlist.txt - Mousepad
File Edit Search View Document Help
Frame (10388 bytes)
Reassembled TCP (565365 bytes)
pcap3.pcap
Packets: 406 · Displayed: 107 (26.4%)
Profile: Default

tcp.stream eq 4

```
No.   Time       Source          Destination
  384 26.541972  10.10.21.210    10.10.53.219
  385 26.541981  10.10.53.219    10.10.21.210
  386 26.542067  10.10.21.210    10.10.53.219
  387 26.542(
  388 26.5421
  389 26.5421
  390 26.5422
  391 26.5422
  392 26.5423
  393 26.5423
  394 26.5423
  395 26.542
```

```
▸ Frame 395: 10:
▸ Ethernet II, :
▸ Internet Prot
▸ Transmission (
▸ [51 Reassembl
▸ Hypertext Tra
▸ Media Type
```

```
0000  02 cd 4e
0010  28 86 1a
0020  35 db 00 50 96 38 11 01  c7 f5 3e 01 a8 a3 80 18   5··P·
0030  01 e9 88 39 00 00 01 01  08 0a 6b db 49 3d 63 ef   ···9····  ··K
0040  10 cb 6f 5c 0e 87 f4 ab  e9 3b 34 cd b6 c7 b3 de   ··o\····  ·;4
0050  be cf b8 8b 23 ac 39 f6  c5 74 31 f8 bc cf a8 63   ····#·9·  ·t1····c
0060  e5 b3 d3 ec ef 0b 80 33  b7 4a b1 c9 b2 c6 29 c3   ·······3  ·J····)·
0070  52 f6 21 c7 70 01 34 03  62 52 cf f0 d0 0f a2 29   R·!·p·4·  bR·····)
0080  1e f4 18 b0 16 24 2c 7b  0c d0 59 93 76 f1 bc bf   ·····$,{  ··Y·v···
0090  8b 26 c0 ee ab 44 83 92  9d 27 6a 0c 57 33 09 93   ·&···D··  ·'j·W3··
00a0  fa 52 a3 64 2b b9 d4 21  05 ba d5 90 85 05 f9 e6   ·R·d+··!  ········
00b0  4b 95 ed 56 42 0e 58 0f  c7 88 51 25 3c 40 92 e5   K··VB·X·  ··Q%<@··
```

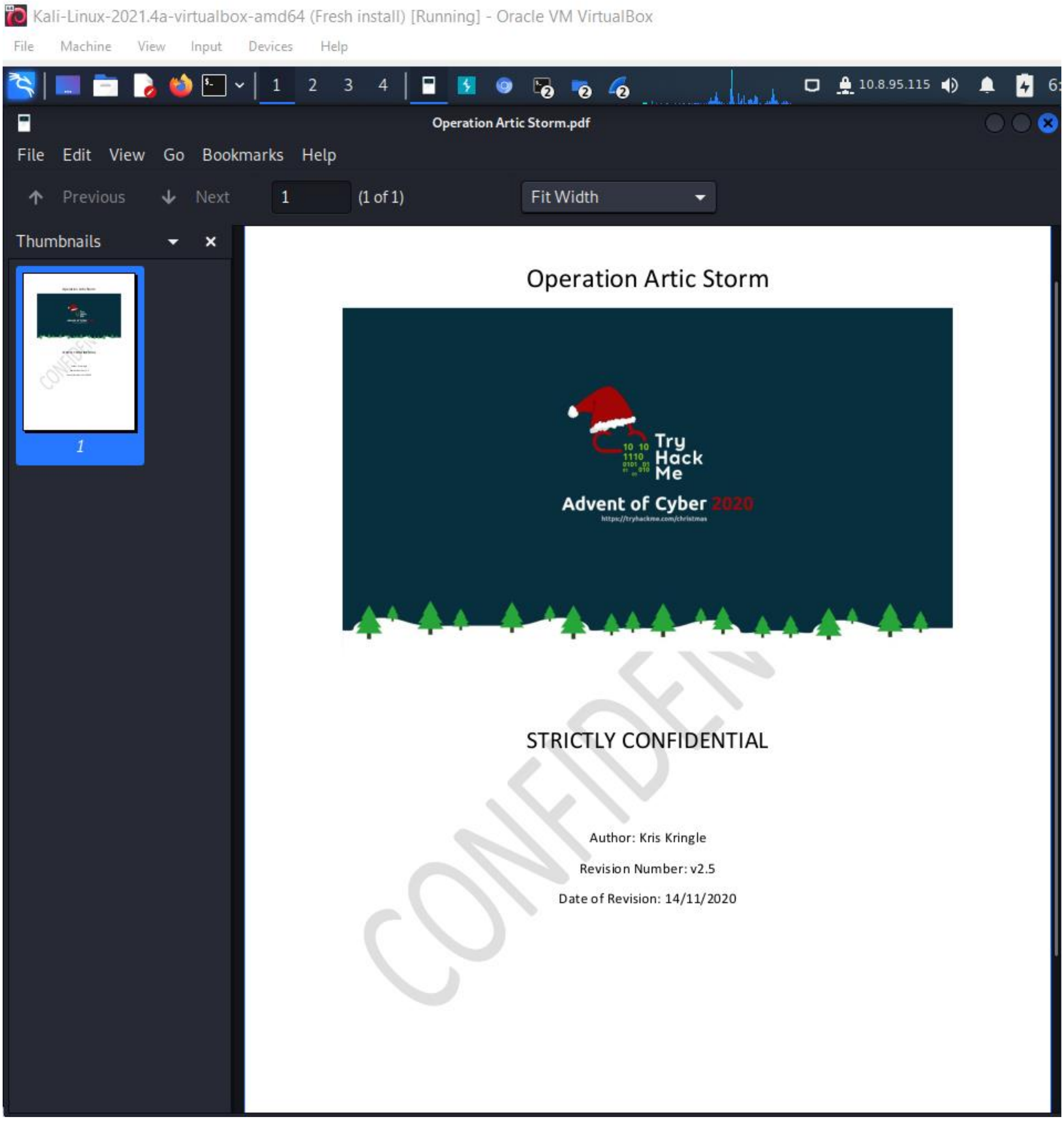
"elf_mcskidy_wishlist.txt": 134 bytes plain tex

```
Wish list for Elf McSkidy
-------------------------

Budget: £100

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

```
2022-06-29 06:03:07 net_route_v4_best_g
2022-06-29 06:03:07 net_route_v4_best_g
2022-06-29 06:03:07 ROUTE_GATEWAY 10.0.
2022-06-29 06:03:07 TUN/TAP device tun0
2022-06-29 06:03:07 net_iface_mtu_set:
2022-06-29 06:03:07 net_iface_up: set t
2022-06-29 06:03:07 net_addr_v4_add: 10
2022-06-29 06:03:07 net_route_v4_add: 1
2022-06-29 06:03:07 WARNING: this confi
vent this
2022-06-29 06:03:07 Initialization Sequ
```

Q8: Who is the author of Operation Artic Storm?

A8: Kris Kringle



Operation Artic Storm

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Thought Process/Methodology:

First, I download the zip file from TryHackMe website and unzip it. I get pcap1, 2, 3 file. Then, I install Wireshark and use it to open pcap 1 file. And I see the IP address that initiates an ICMP/ping. Then, I apply a display filter ‘http.request.method == GET’ to get the name of the article that the IP address ’10.10.67.199’. Next, I open pcap 2 file, apply the display filter ‘tcp.port == 21’ to get the password leaked during the login process. Next, I open pcap 3 file to export christmas.zip and unzip it to get Elf McSkidy's wishlist that will be used to replace Elf McEager.

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

Tools used: Kali Linux, Chrome

Solution/walkthrough:

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

80, 2222, 3389

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

Ubuntu

Q4: What is the version of Apache?

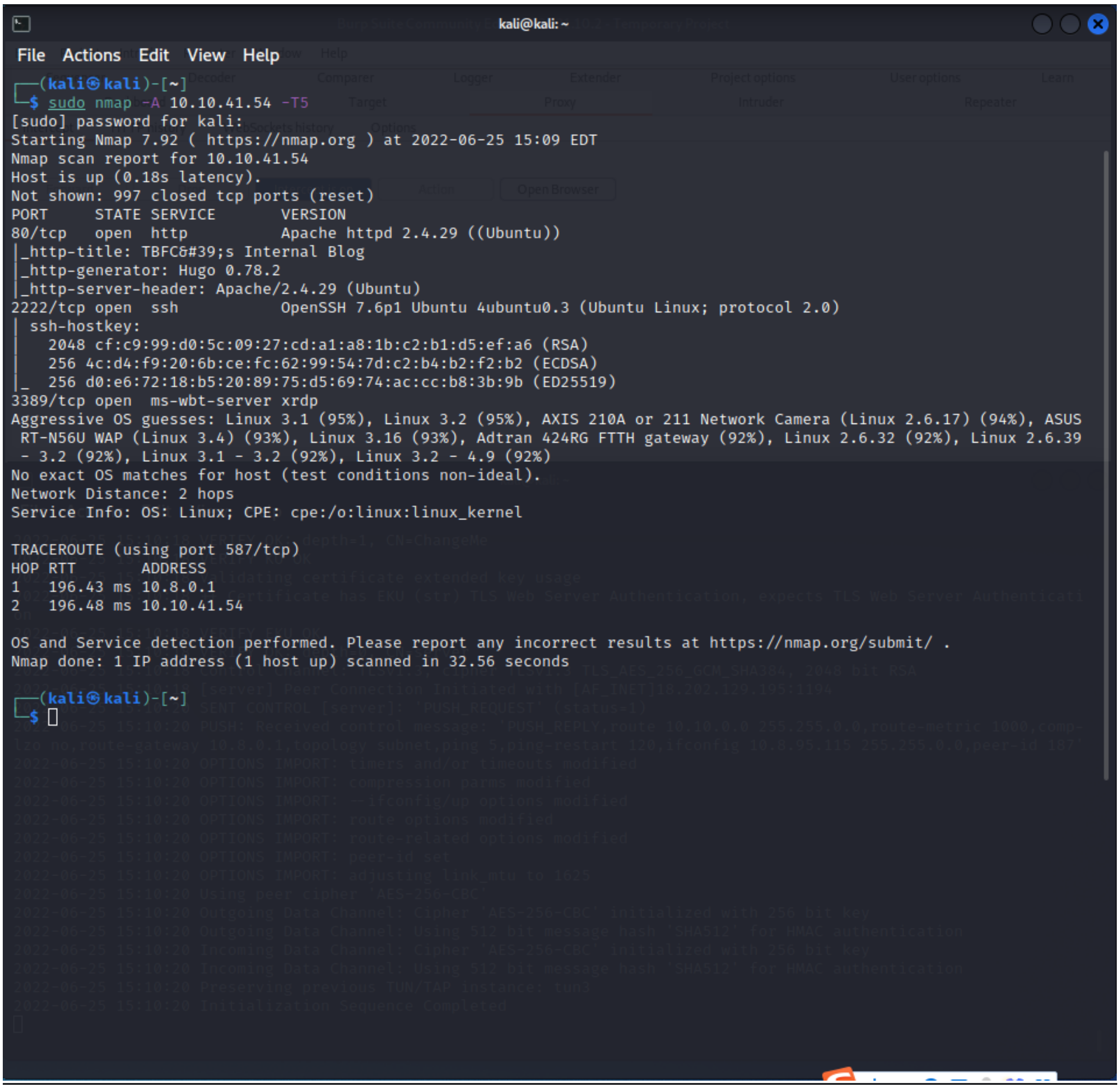
2.4.29

Q5: What is running on port 2222?

SSH

Q6: Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver. Based on the value returned, what do we think this website might be used for?

blog



```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.10.41.54 -T5
[sudo] password for kali:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-25 15:09 EDT
Nmap scan report for 10.10.41.54
Host is up (0.18s latency).
Not shown: 997 closed tcp ports (reset)
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-title: TBFC&#39;s Internal Blog
|_http-generator: Hugo 0.78.2
|_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
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS
 RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Adtran 424RG FTTH gateway (92%), Linux 2.6.32 (92%), Linux 2.6.39
 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 587/tcp)
HOP RTT       ADDRESS
1   196.43 ms 10.8.0.1
2   196.48 ms 10.10.41.54

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.56 seconds

┌──(kali㉿kali)-[~]
└─$ 
```

Thought Process/Methodology:

First, I open the terminal and key in ‘sudo nmap –A [MACHINE-IP] –T5’, and it shows everything to me.

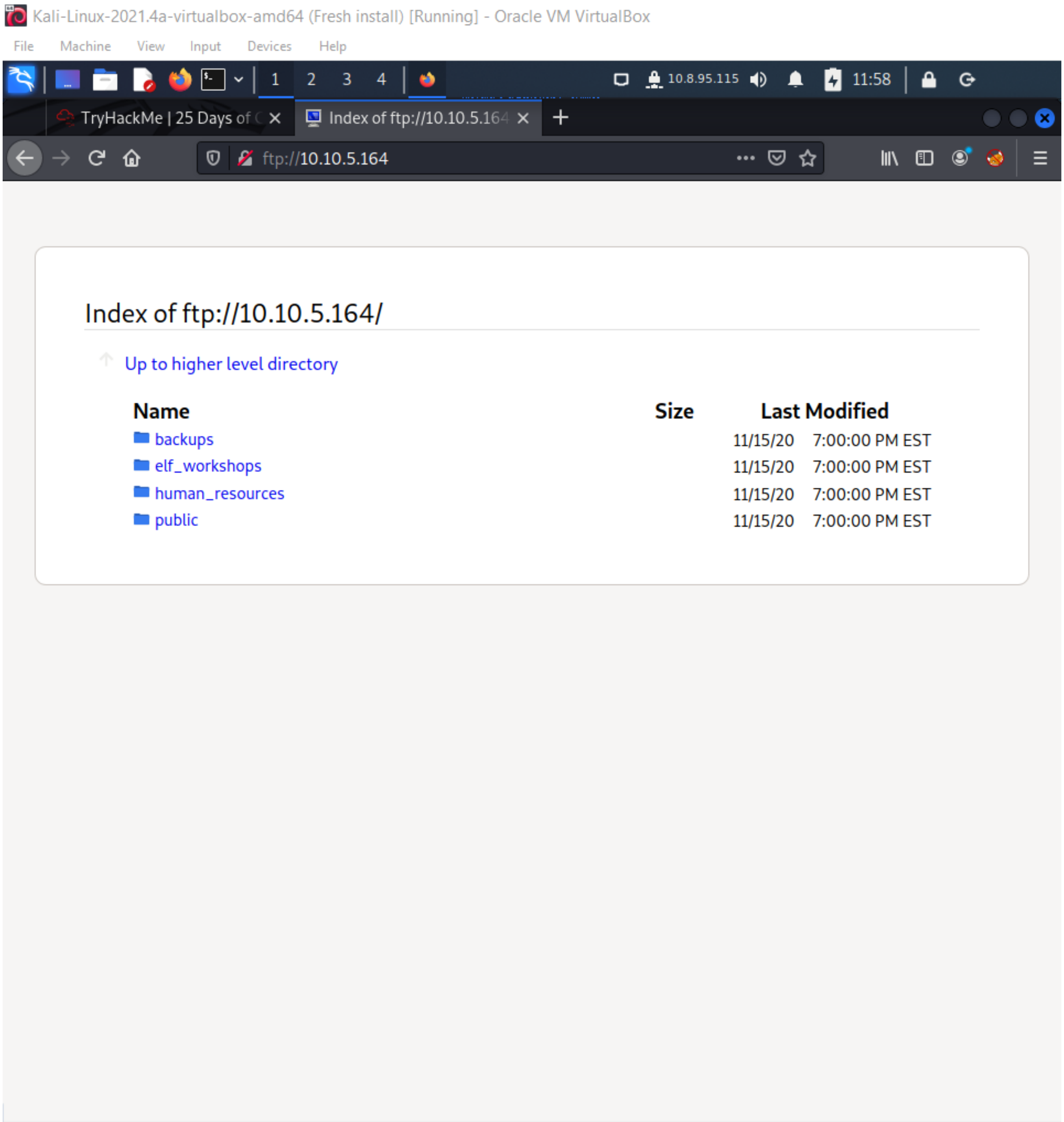
Day 9: Networking - Anyone can be Santa!

Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: What are the directories you found on the FTP site?

A1: backups, elf_workshops, human_resources, public



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
11:58
TryHackMe | 25 Days of C
Index of ftp://10.10.5.164
ftp://10.10.5.164

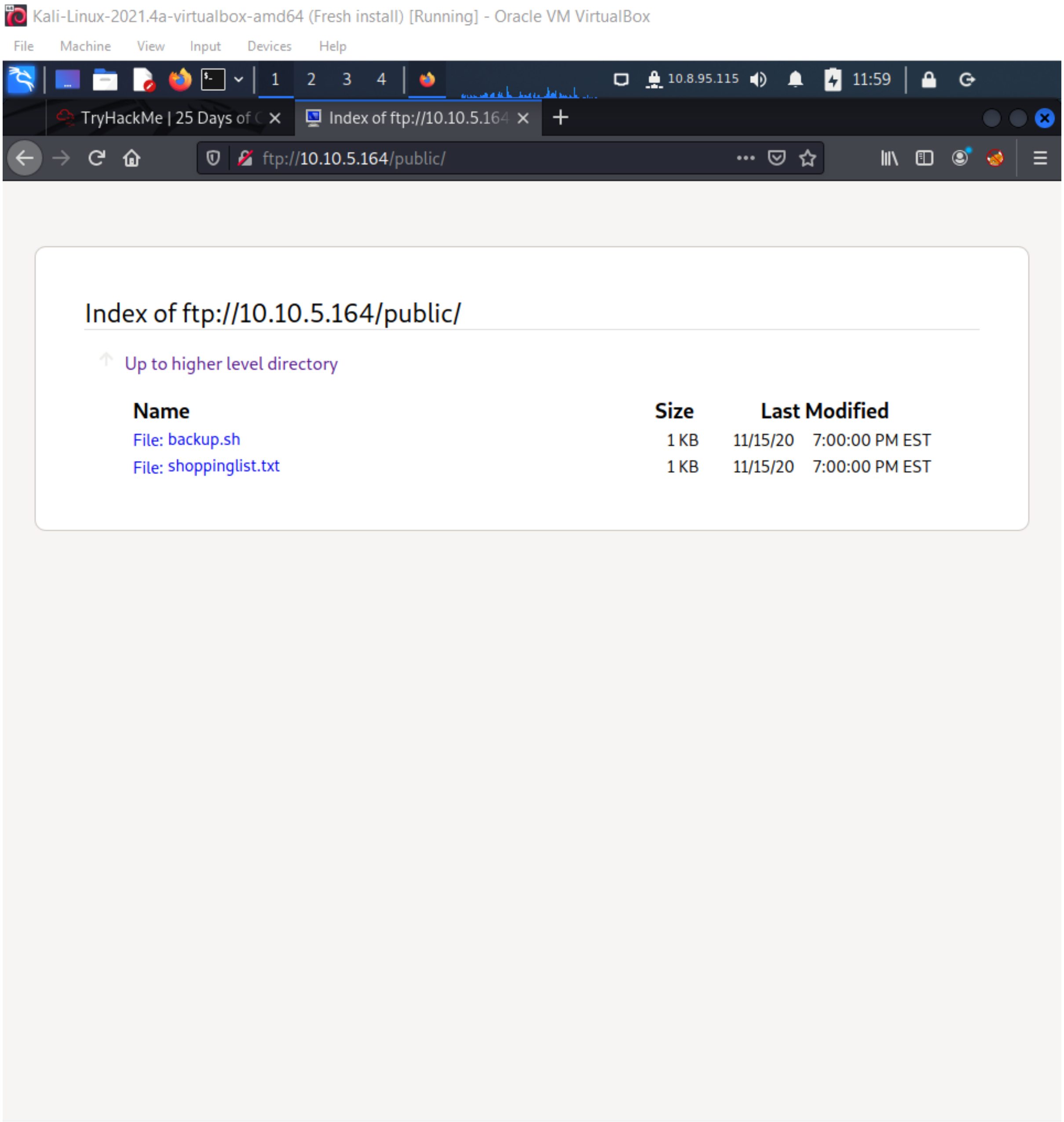
Index of ftp://10.10.5.164/

Up to higher level directory

Name	Size	Last Modified
backups		11/15/20 7:00:00 PM EST
elf_workshops		11/15/20 7:00:00 PM EST
human_resources		11/15/20 7:00:00 PM EST
public		11/15/20 7:00:00 PM EST

Q2: Name the directory on the FTP server that has data accessible by the "anonymous" user

A2: public


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
1
2
3
4
10.8.95.115
11:59
TryHackMe | 25 Days of C
Index of ftp://10.10.5.164
ftp://10.10.5.164/public/

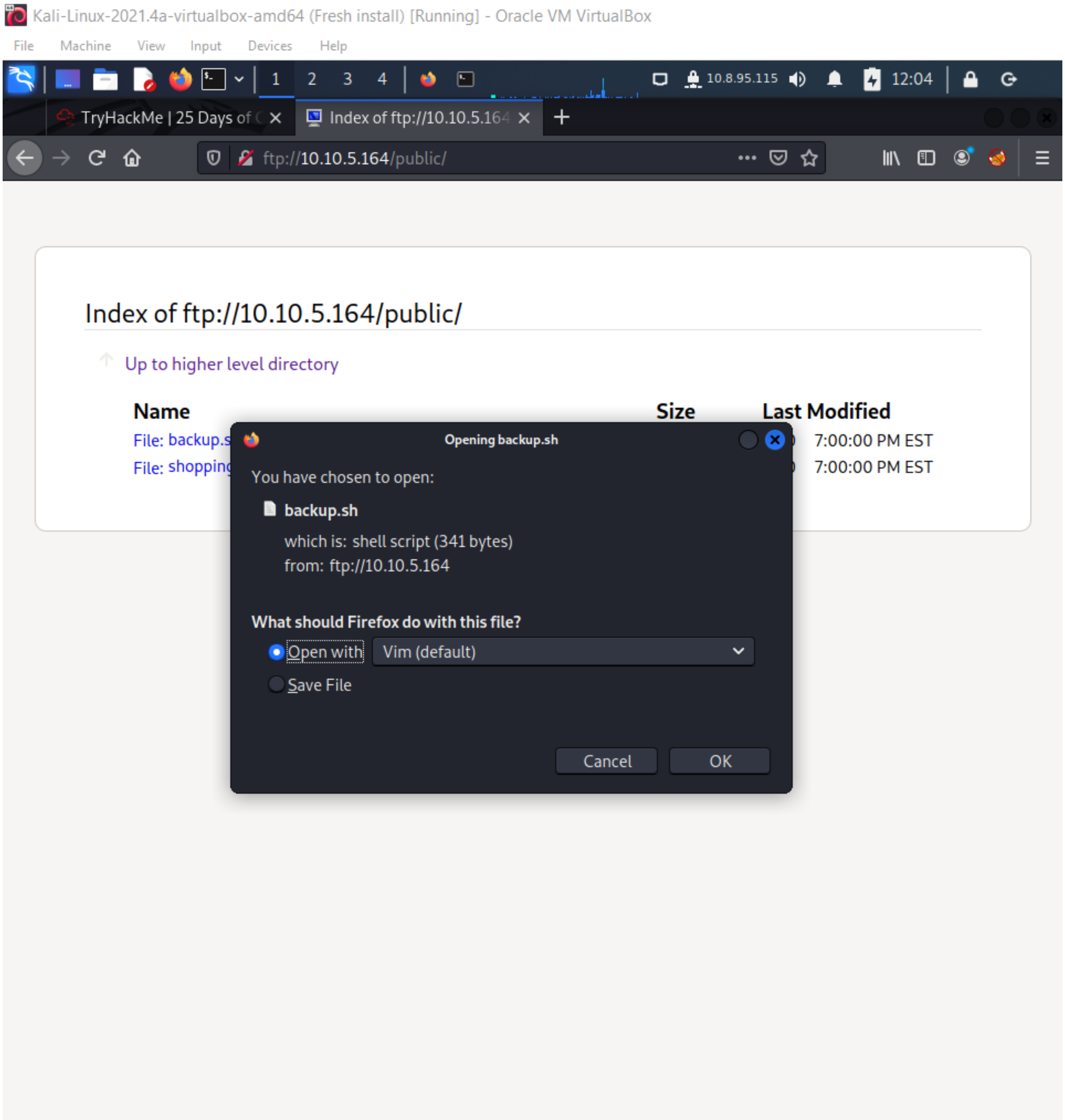
Index of ftp://10.10.5.164/public/

Up to higher level directory

Name	Size	Last Modified
File: backup.sh	1 KB	11/15/20 7:00:00 PM EST
File: shoppinglist.txt	1 KB	11/15/20 7:00:00 PM EST

Q3: What script gets executed within this directory?

A3: backup.sh



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox

File Machine View Input Devices Help
1 2 3 4
10.8.95.115
12:04
TryHackMe | 25 Days of C
Index of ftp://10.10.5.164
ftp://10.10.5.164/public/

Index of ftp://10.10.5.164/public/

Up to higher level directory

Name	Size	Last Modified
File: backup.s		7:00:00 PM EST
File: shopping		7:00:00 PM EST

Opening backup.sh

You have chosen to open:

backup.sh

which is: shell script (341 bytes)
from: ftp://10.10.5.164

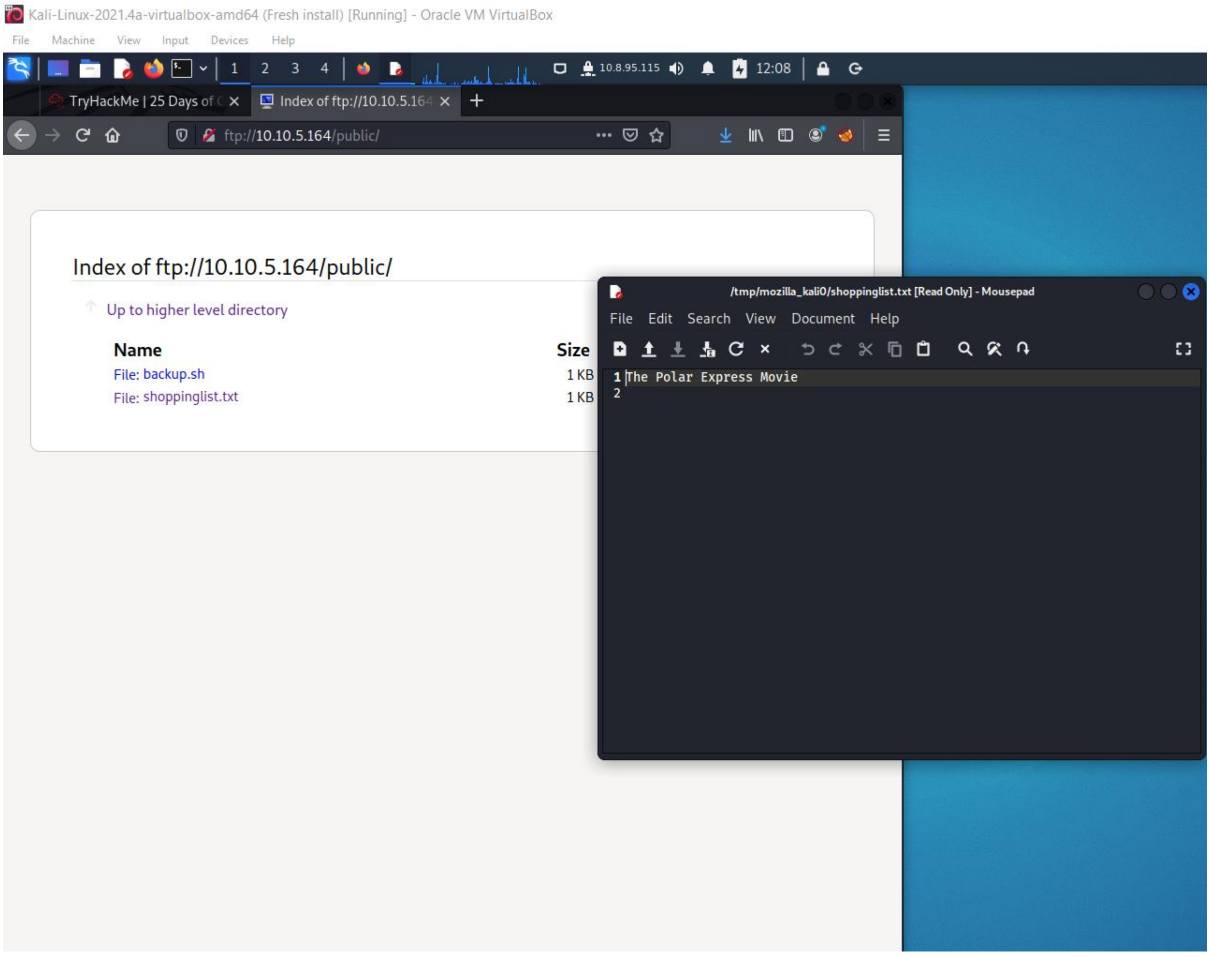
What should Firefox do with this file?

● Open with Vim (default)

○ Save File

Q4: What movie did Santa have on his Christmas shopping list?

A4: The Polar Express Movie


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
12:08
TryHackMe | 25 Days of C
Index of ftp://10.10.5.164
ftp://10.10.5.164/public/
/tmp/mozilla_kali0/shoppinglist.txt [Read Only] - Mousepad
File Edit Search View Document Help

Index of ftp://10.10.5.164/public/

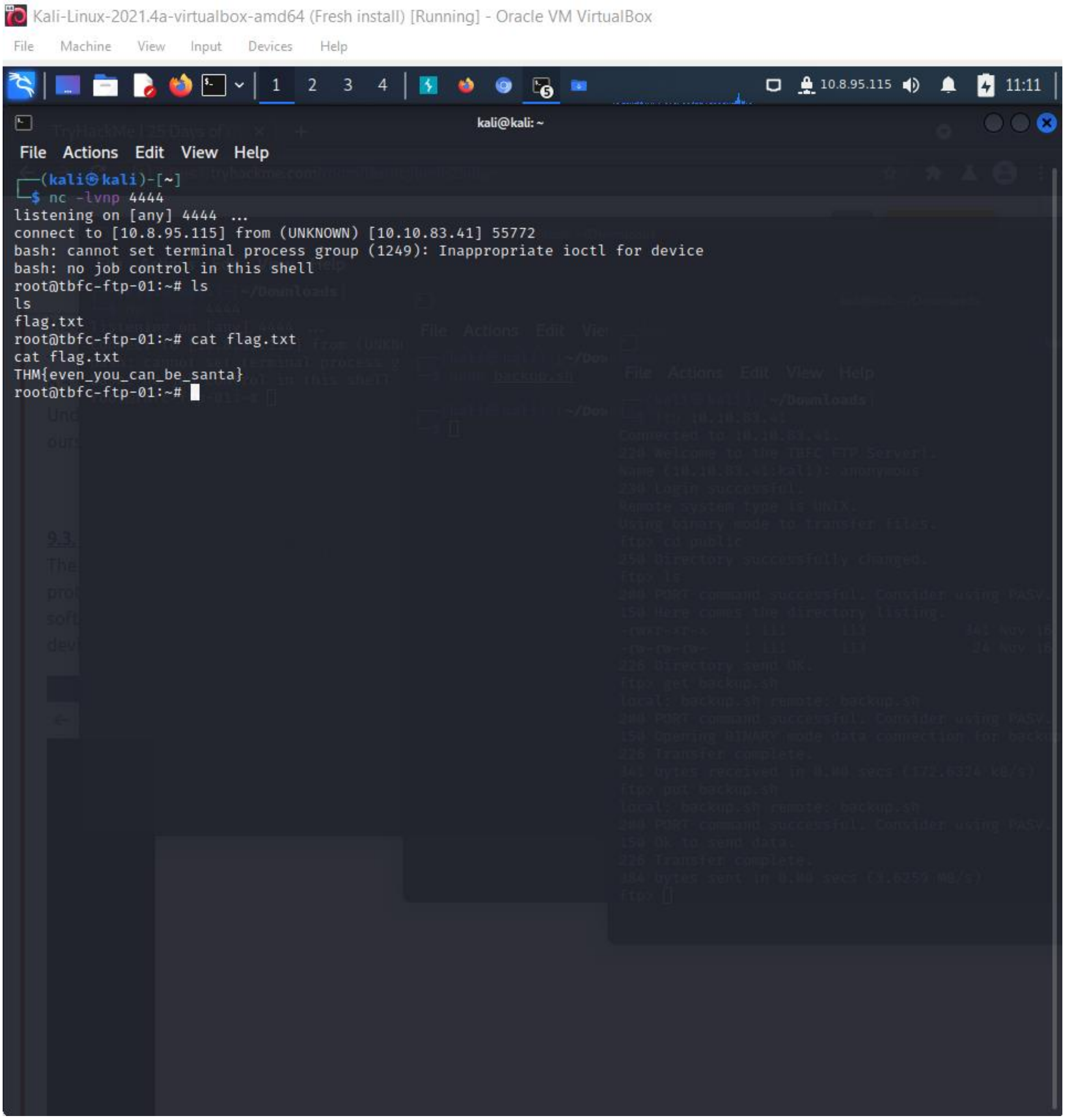
Up to higher level directory

Name	Size
File: backup.sh	1 KB
File: shoppinglist.txt	1 KB

```
The Polar Express Movie

```

Q5: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

A5: THM{even_you_can_be_santa}


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
11:11
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.95.115] from (UNKNOWN) [10.10.83.41] 55772
bash: cannot set terminal process group (1249): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# cat flag.txt
cat flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~# 
```

Thought Process/Methodology:

First, I key in ftp://[MACHINE-IP] to check the information I need. Afterwards, I open first terminal and key in ftp [MACHINE-IP], change directory into ‘public’ and get backup.sh. Then, I use the command ‘nano’ to change the content of backup.sh. Then, I open second terminal and key in ‘nc –lvnp 4444’. Later, I put back the backup.sh into the ‘public’. After a while, the second terminal shows the flag.txt. I use the command ‘cat’ to check what the content inside the flag.txt is.

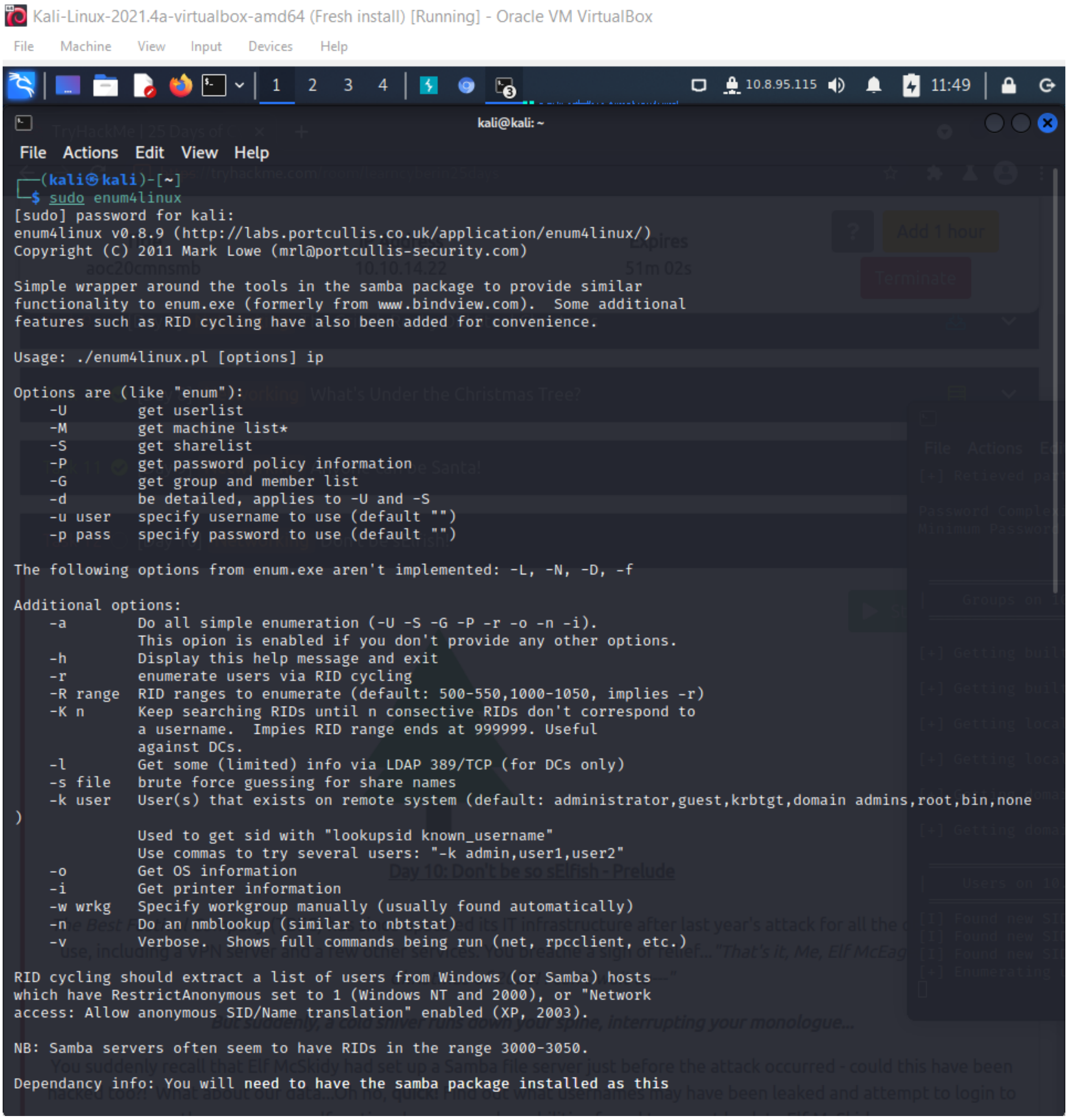
Day 10: Networking - Don't be sElfish!

Tools used: Kali Linux, Chrome

Solution/walkthrough:

Q1: Examine the help options for enum4linux. Match the following flags with the descriptions.

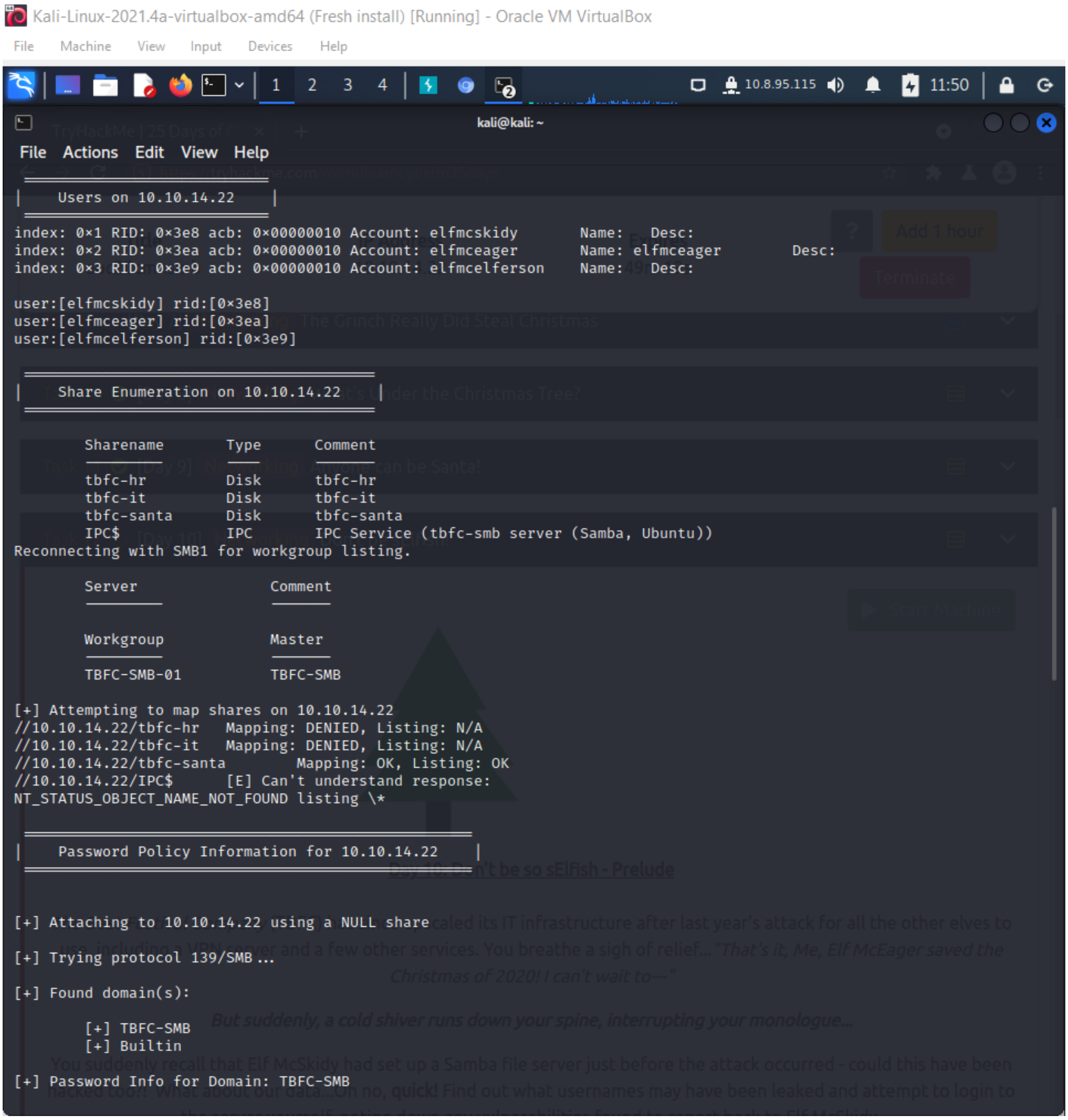
A1:


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File
Machine
View
Input
Devices
Help
10.8.95.115
11:49
kali@kali: ~
File
Actions
Edit
View
Help

```
┌──(kali㉿kali)-[~]
└─$ sudo enum4linux
[sudo] password for kali:
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -p pass   specify password to use (default "")

The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This opion is enabled if you don't provide any other options.
    -h        Display this help message and exit
    -r        enumerate users via RID cycling
    -R range  RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
    -K n      Keep searching RIDs until n consective RIDs don't correspond to
              a username.  Impies RID range ends at 999999. Useful
              against DCs.
    -l        Get some (limited) info via LDAP 389/TCP (for DCs only)
    -s file   brute force guessing for share names
    -k user   User(s) that exists on remote system (default: administrator,guest,krbtgt,domain admins,root,bin,none
)
              Used to get sid with "lookupsid known_username"
              Use commas to try several users: "-k admin,user1,user2"
    -o        Get OS information
    -i        Get printer information
    -w wrkg   Specify workgroup manually (usually found automatically)
    -n        Do an nmblookup (similar to nbtstat)
    -v        Verbose.  Shows full commands being run (net, rpcclient, etc.)

RID cycling should extract a list of users from Windows (or Samba) hosts
which have RestrictAnonymous set to 1 (Windows NT and 2000), or "Network
access: Allow anonymous SID/Name translation" enabled (XP, 2003).

NB: Samba servers often seem to have RIDs in the range 3000-3050.

Dependancy info: You will need to have the samba package installed as this
```

Q2: Using enum4linux, how many users are there on the Samba server?

A2: 3

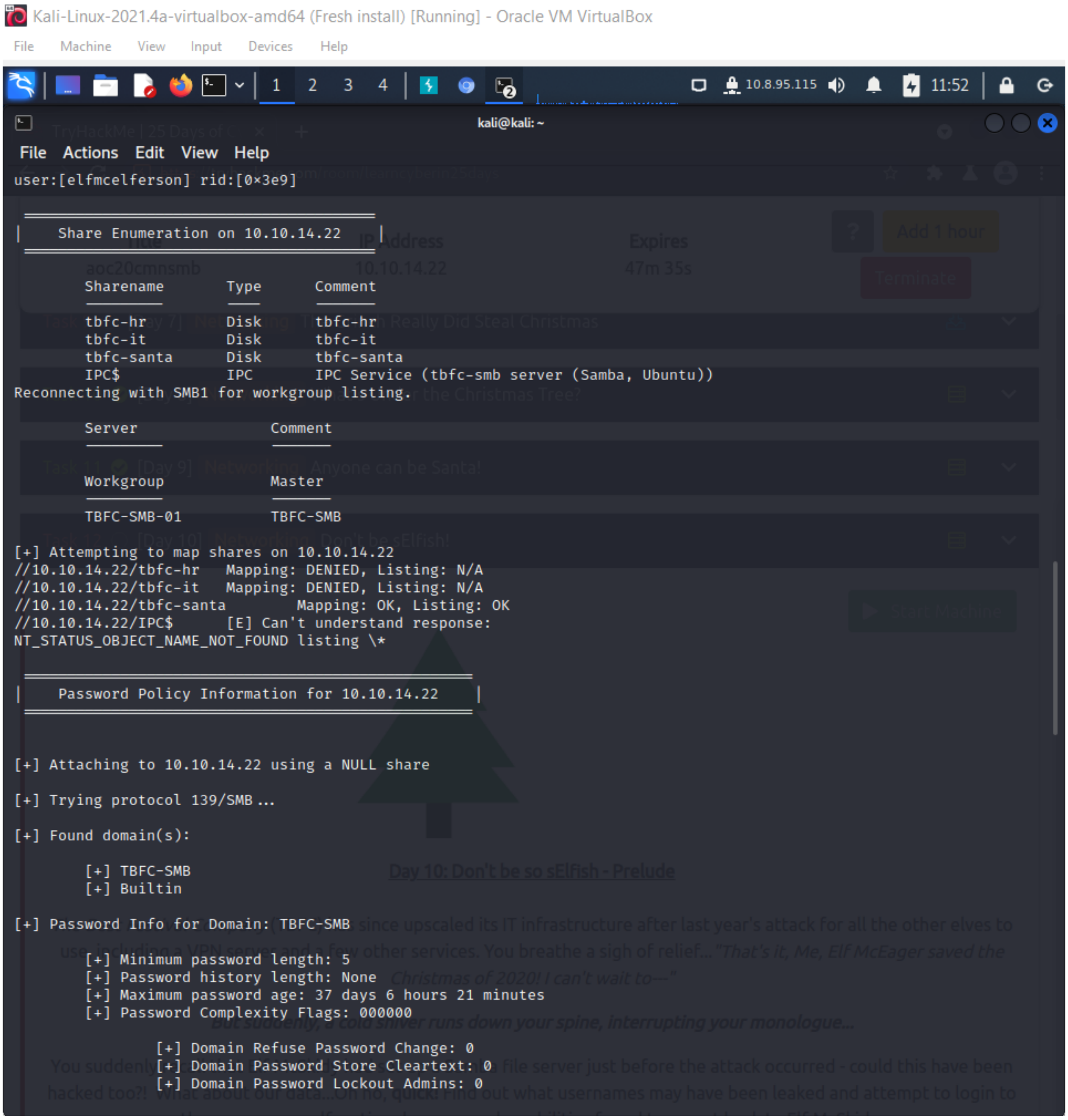


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
11:50
kali@kali: ~
File Actions Edit View Help

```
 ==============================
|    Users on 10.10.14.22    |
 ==============================
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: elfmcskidy       Name:   Desc:
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: elfmceager       Name: elfmceager        Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: elfmcelferson    Name:   Desc:

user:[elfmcskidy] rid:[0×3e8]
user:[elfmceager] rid:[0×3ea]
user:[elfmcelferson] rid:[0×3e9]

 ==========================================
|    Share Enumeration on 10.10.14.22    |
 ==========================================

        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 10.10.14.22
//10.10.14.22/tbfc-hr   Mapping: DENIED, Listing: N/A
//10.10.14.22/tbfc-it   Mapping: DENIED, Listing: N/A
//10.10.14.22/tbfc-santa        Mapping: OK, Listing: OK
//10.10.14.22/IPC$      [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ====================================================
|    Password Policy Information for 10.10.14.22    |
 ====================================================


[+] Attaching to 10.10.14.22 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] TBFC-SMB
        [+] Builtin

[+] Password Info for Domain: TBFC-SMB
```

<u>Q3: Now how many "shares" are there on the Samba server?</u>

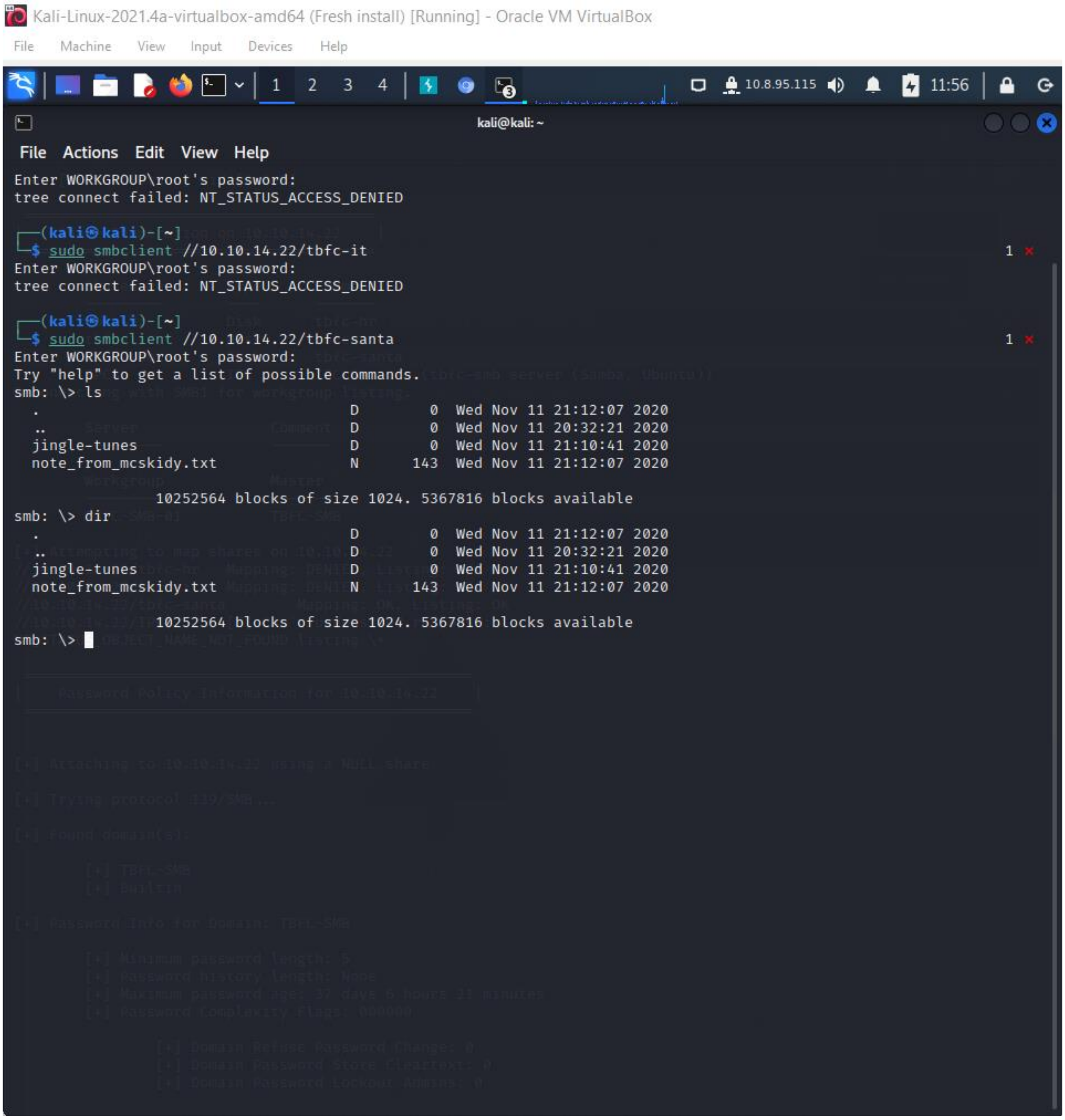
A3: 4


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
1 2 3 4
10.8.95.115
11:52
kali@kali: ~
File Actions Edit View Help

```
user:[elfmcelferson] rid:[0×3e9]

 ========================================
|    Share Enumeration on 10.10.14.22    |
 ========================================

        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 10.10.14.22
//10.10.14.22/tbfc-hr   Mapping: DENIED, Listing: N/A
//10.10.14.22/tbfc-it   Mapping: DENIED, Listing: N/A
//10.10.14.22/tbfc-santa        Mapping: OK, Listing: OK
//10.10.14.22/IPC$      [E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*

 ===================================================
|    Password Policy Information for 10.10.14.22    |
 ===================================================


[+] Attaching to 10.10.14.22 using a NULL share

[+] Trying protocol 139/SMB ...

[+] Found domain(s):

        [+] TBFC-SMB
        [+] Builtin

[+] Password Info for Domain: TBFC-SMB

        [+] Minimum password length: 5
        [+] Password history length: None
        [+] Maximum password age: 37 days 6 hours 21 minutes
        [+] Password Complexity Flags: 000000

                [+] Domain Refuse Password Change: 0
                [+] Domain Password Store Cleartext: 0
                [+] Domain Password Lockout Admins: 0
```

Q4: Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

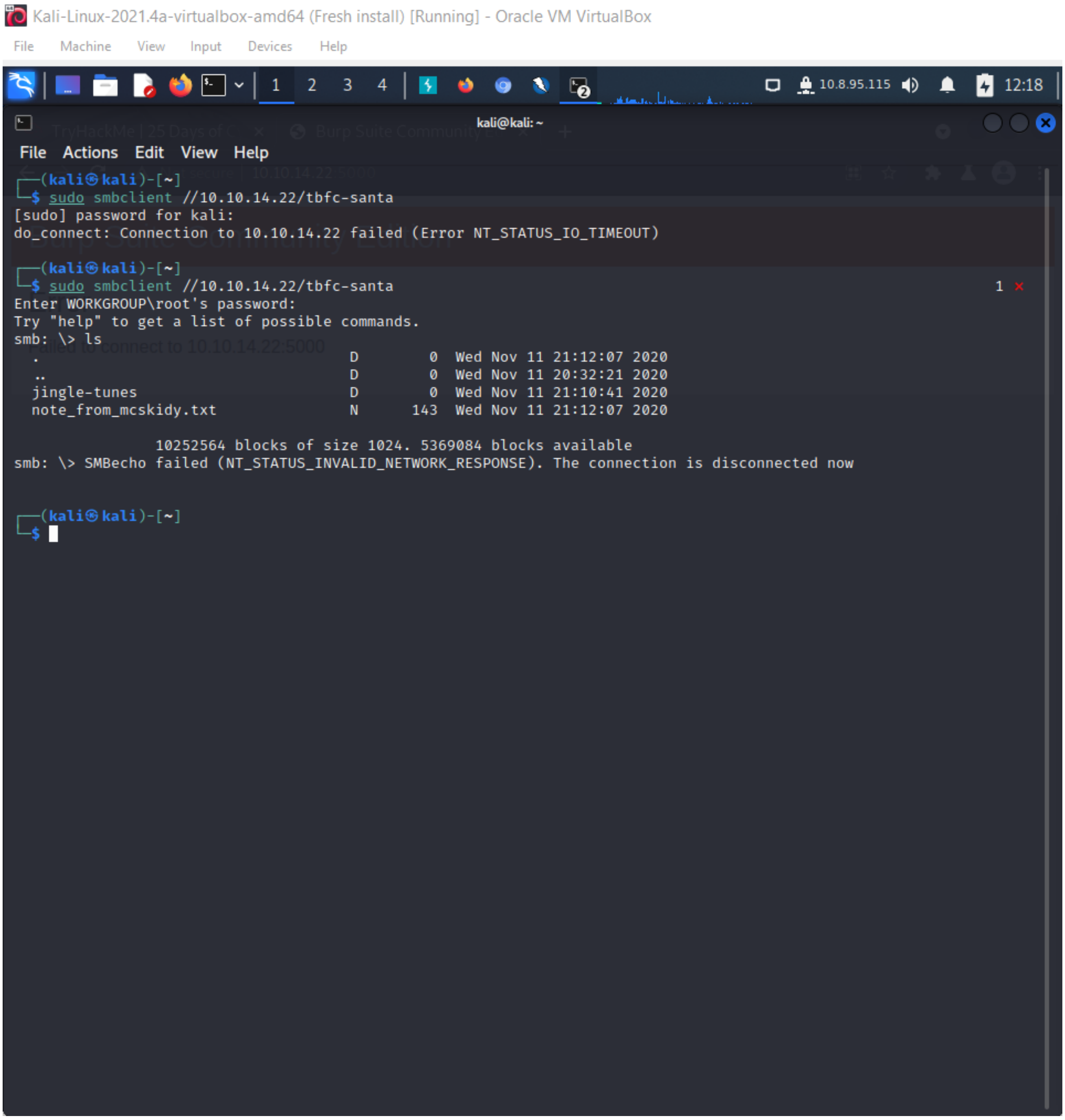
A4: tbfc-santa


Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
11:56
kali@kali: ~
File Actions Edit View Help

```
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ sudo smbclient //10.10.14.22/tbfc-it                                    1 ×
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED

┌──(kali㉿kali)-[~]
└─$ sudo smbclient //10.10.14.22/tbfc-santa                                 1 ×
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020

                10252564 blocks of size 1024. 5367816 blocks available
smb: \> dir
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020

                10252564 blocks of size 1024. 5367816 blocks available
smb: \> █
```

Q5: Log in to this share, what directory did ElfMcSkidy leave for Santa?

A5: jingle-tunes



Kali-Linux-2021.4a-virtualbox-amd64 (Fresh install) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
10.8.95.115
12:18
kali@kali: ~
File Actions Edit View Help

```
┌──(kali㉿kali)-[~]
└─$ sudo smbclient //10.10.14.22/tbfc-santa
[sudo] password for kali:
do_connect: Connection to 10.10.14.22 failed (Error NT_STATUS_IO_TIMEOUT)

┌──(kali㉿kali)-[~]
└─$ sudo smbclient //10.10.14.22/tbfc-santa                                                    1 ×
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020

                10252564 blocks of size 1024. 5369084 blocks available
smb: \> SMBecho failed (NT_STATUS_INVALID_NETWORK_RESPONSE). The connection is disconnected now


┌──(kali㉿kali)-[~]
└─$ 
```

Thought Process/Methodology:

First, I open the terminal and key in ‘sudo enum4linux’ and it shows the help message and the information I need. Then, I key in ‘sudo smbclient //[MACHINE-IP]/[SHARENAME]’ by using different sharenames showed in the terminal one by one. I find that tbfc-santa doesn’t require a password to login to the shares on the Samba server. After logging into this share, I found jingle-tunes did ElfMcSkidy leave for Santa.