

Report PSP0201 T2130 - Tutorial Week 3

Group: **Marceline**

ID	Name	Role
1211100899	Muhammad Shahril Aiman	Leader
1211101533	Muhammad Aniq Fahmi	member
1211101303	Aiman Faris	member
1211102759	Muhammad Zaquan	member

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

Tools used: Kali Linux, Firefox, OWASP

Solution/walkthrough:

Question 1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

-enforce correct syntax of structured fields (SYNTHETIC)

-enforce correctness of their values in the specific business context (SEMANTIC)

The screenshot shows a Microsoft Edge browser window displaying the OWASP Input Validation Cheat Sheet. The page is titled "Email Address Validation". It contains two main sections: "Syntactic Validation" and "Semantic Validation".

Syntactic Validation: This section discusses the format of email addresses according to RFC 5321. It lists several examples of invalid email addresses:

- ">script>alert(1);</script>@example.org"
- "user+subaddress@example.org"
- "user@[IPv6:2001:db8::1]"
- " " @example.org"

It notes that properly parsing email addresses with regular expressions is very complicated. It also mentions a common misconception about mail servers rejecting technically valid but non-functional addresses.

Semantic Validation: This section discusses how to validate email addresses beyond syntactic rules. It lists several criteria:

- The email address contains two parts, separated by an '@' symbol.
- The email address does not contain dangerous characters (such as backticks, single or double quotes, or null bytes).
 - Exactly which characters are dangerous will depend on how the address is going to be used (echoed in page, inserted into database, etc).
- The domain part contains only letters, numbers, hyphens (-) and periods (.)
- The email address is a reasonable length:
 - The local part (before the '@') should be no more than 63 characters.
 - The total length should be no more than 254 characters.

A note at the bottom states: "Current validation is about determining whether the email address is correct and functional. The most common way to do this is to send an email."

QUESTION 2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

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

The screenshot shows a web browser window with multiple tabs open. The active tab is titled "Input Validation" from the OWASP Cheat Sheet Series. The page content includes a sidebar with a table of contents and several main sections with sub-content. One section, "Allow List Regular Expression Examples", contains a code example for validating a U.S. Zip code: `^\d{5}(-\d{4})? $`. Another section, "Java Regex Usage Example:", provides an example for validating the parameter "zip" using a regular expression.

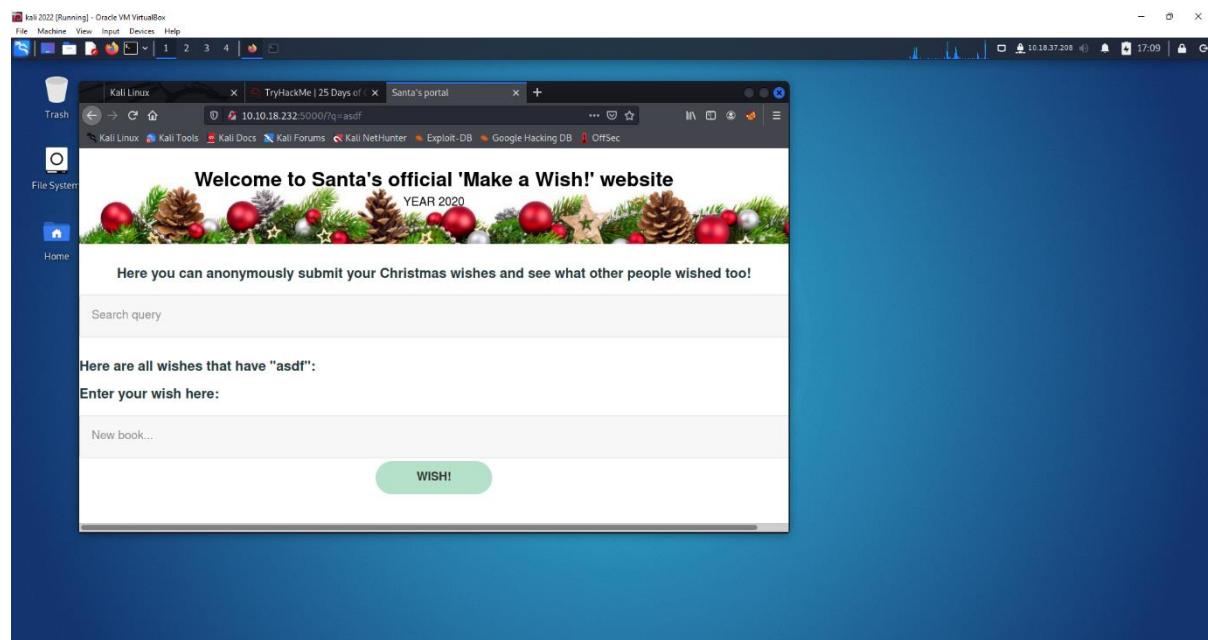
Question 3: What vulnerability type was used to exploit the application?

ANSWER: Stored

The screenshot shows a Kali Linux desktop environment with a web browser window open to a site titled "Santa's portal". The page features a decorative header with Christmas ornaments and a search bar. Below the search bar, there is a message: "Here are all wishes that have \"asdf\":". A list of wishes is displayed, including "Enter your wish here:" and "New book...". At the bottom of the page is a green button labeled "WISH!". The browser's address bar shows the URL `10.10.18.232:5000/?q=asdf`. The desktop background is dark blue, and the taskbar at the bottom shows various application icons.

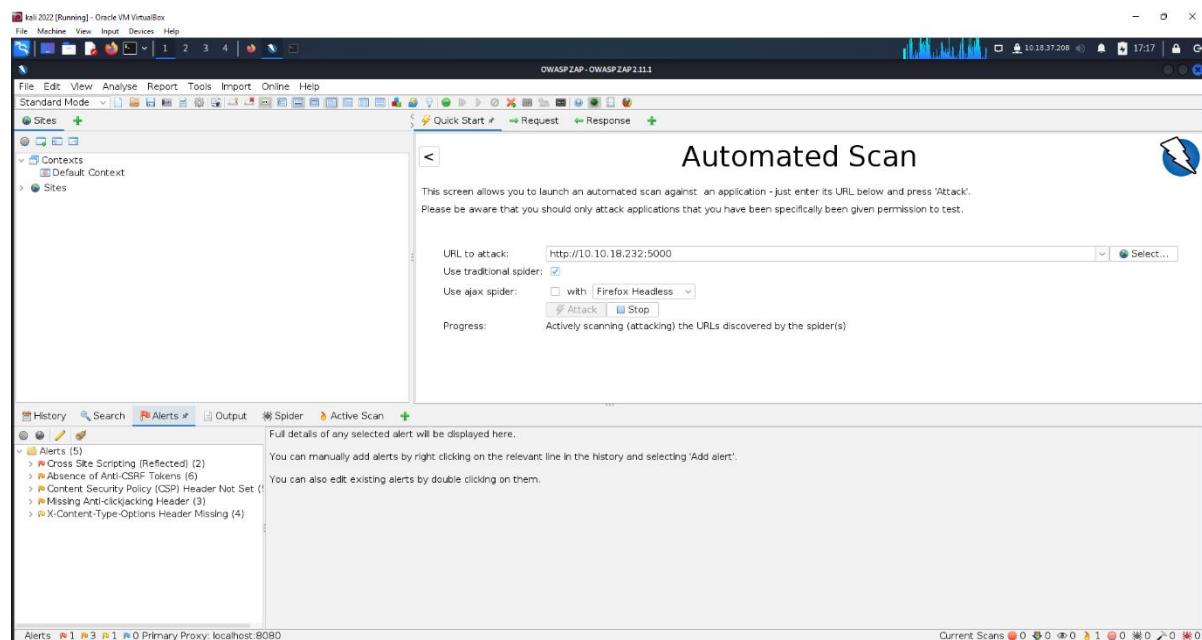
QUESTION 4: What query string can be abused to craft a reflected XSS?

ANSWER: q



QUESTION 5: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

ANSWER: 2



QUESTION 6: What JavaScript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

ANSWER: <script>alert('PSP2021')</script>

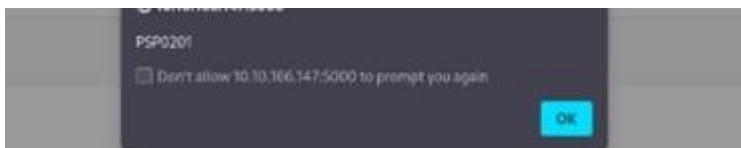
#jaVasCript://" + /* /' + /* */(/* */oNcliCk=alert(5397))//%0D%0A%0d%0a/\x3csVg/

#javascript:alert(5397)

Enter your wish here:

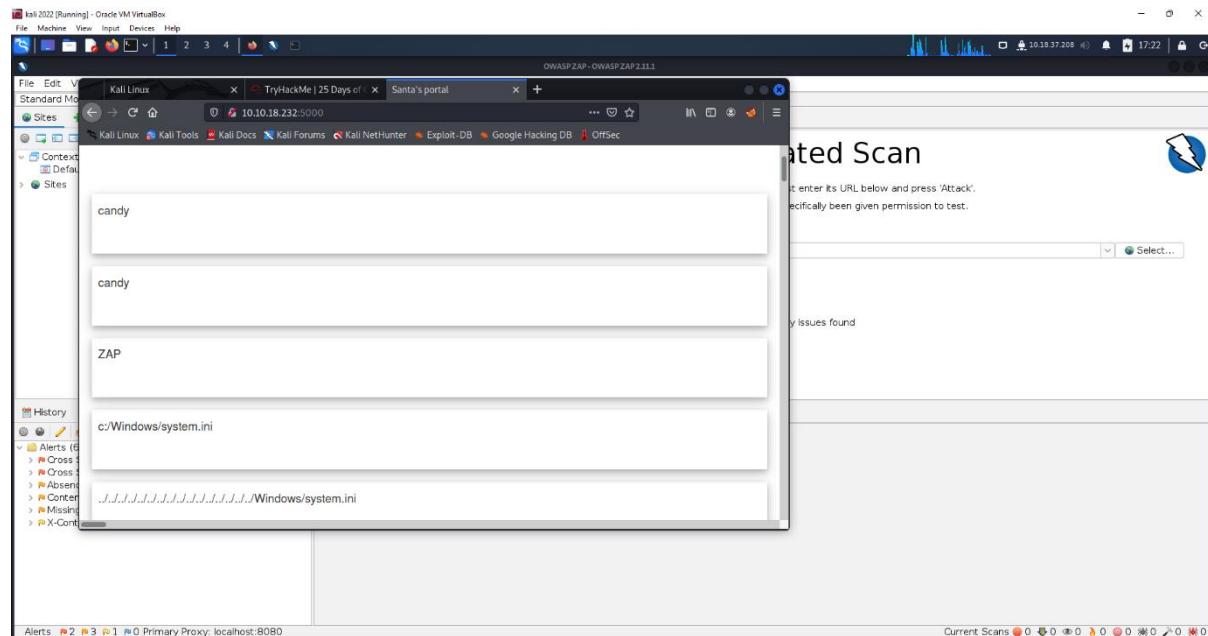
<script>alert("PSP0201")</script>

WISH!



QUESTION 7: Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?

ANSWER: YES



METHODOLOGY:

Firstly, I open the try hack and read the question. So, the first question, I read at the OWASP Cheat Sheet to answer the Q1. For Q2 I use the OWASP Cheat Sheet to check the regular expression used to validate a US Zip code. We check and get the answer for Q2. Then for Q3, I start the machine, got the Ip address and paste it to the Firefox. It will lead us to “welcome to Santa official make a wish website”. I put the wish that I wanted and enter it. Then, the data store and it means Stored vulnerability. So, for the Q4, I already entered my wish and its show the URL show “q” at first of the URL. So, the query string is “q” can be abused to craft a reflected XSS. For the Q5, I open the OWASP and put the ip address to scan the website at there and the OWASP will check there have error or not. They show 2 error at Alert Section. For the Q6, I open the Santa’s wish website to put the command at the wish, so the code that I put is “<script>alert('PSP2021')</script>”. After that, the website shows error. Lastly for the Q7, I re check the website and put a new wish at the Santa’s wish website, our XSS attack persist still can attack the website.

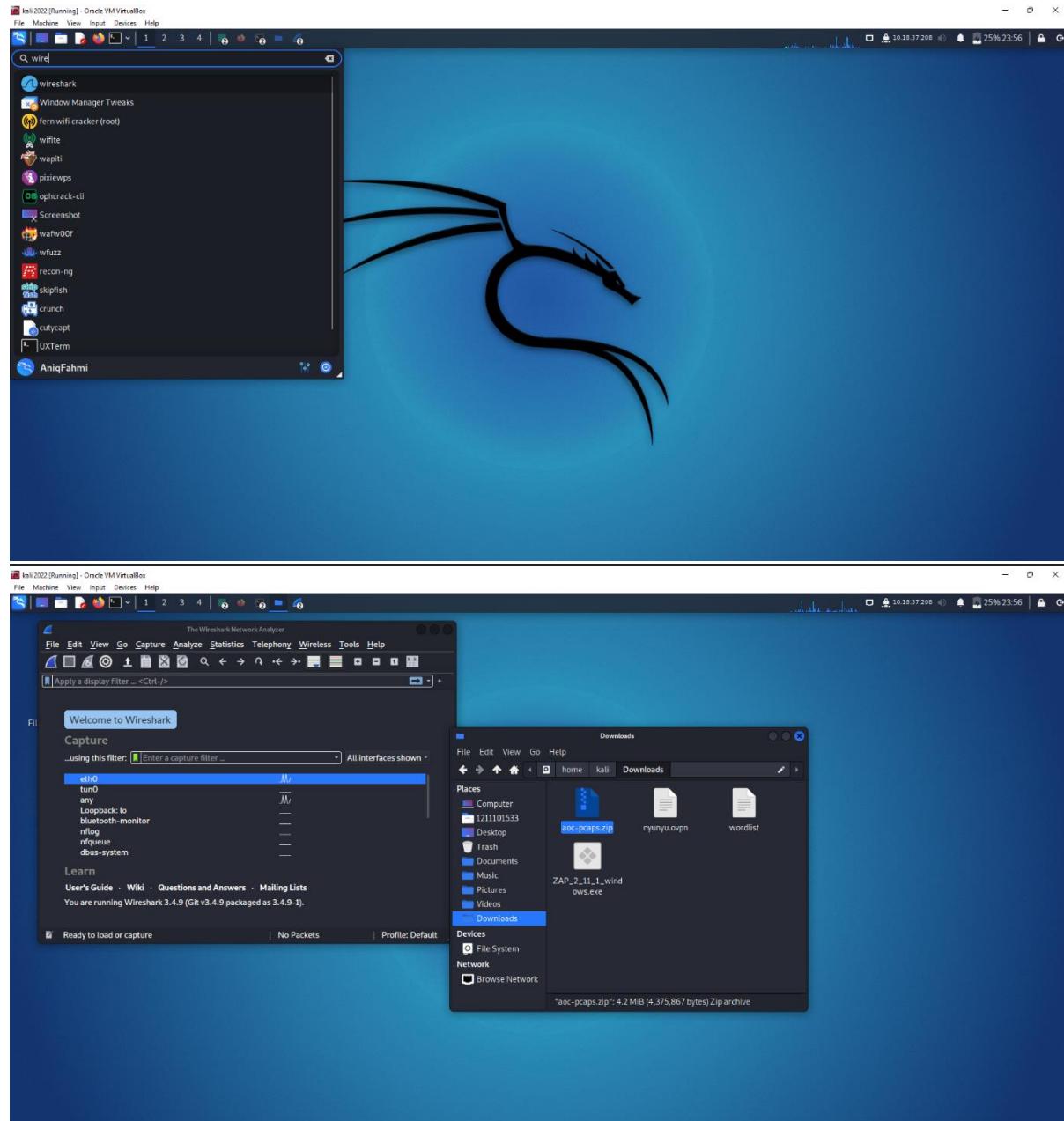
Day 7: Web Exploitation -- The Grinch Really Did Steal Christmas

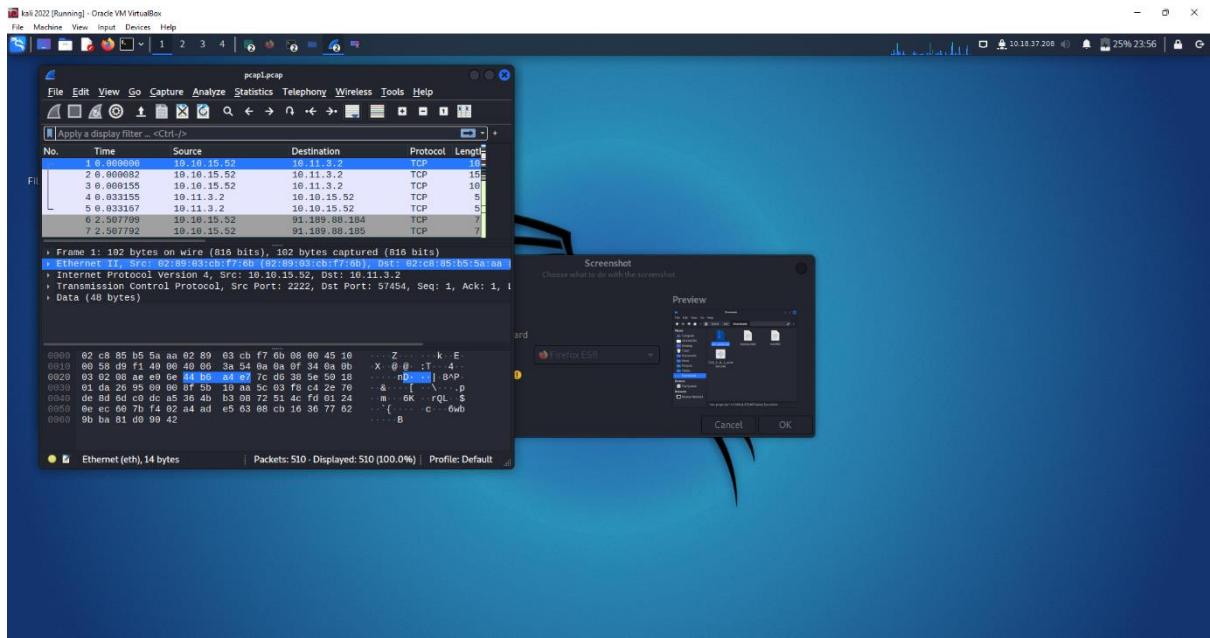
Tools used: Kali Linux, Firefox, Wireshark

Solution/walkthrough:

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

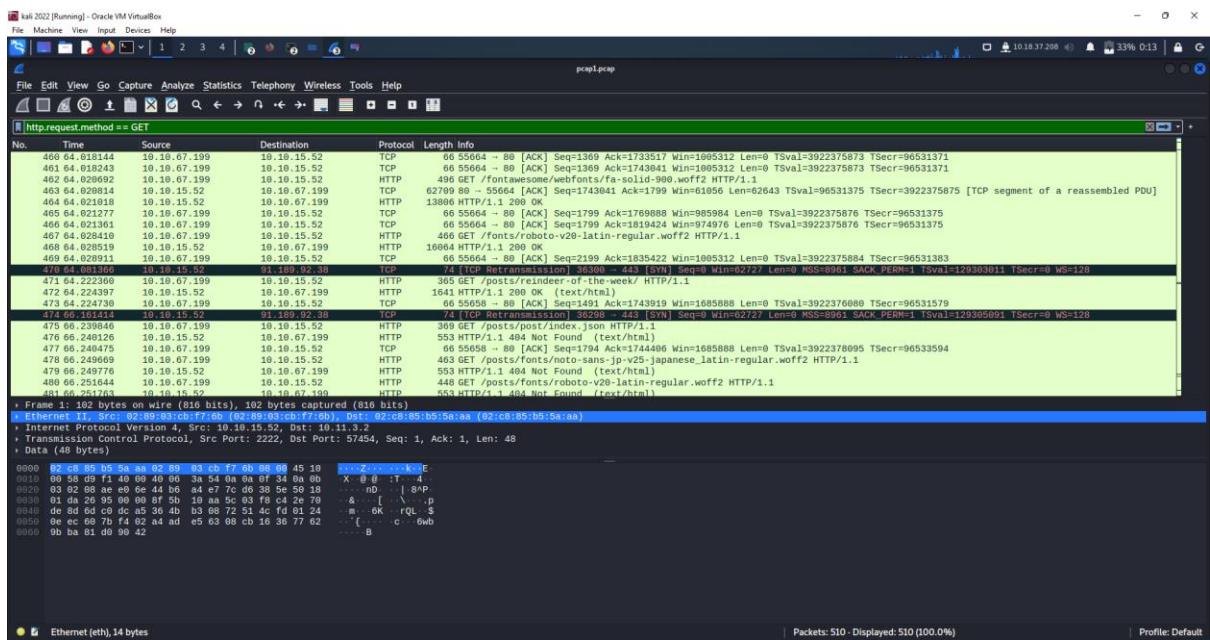
ANSWER: 10.11.3.2





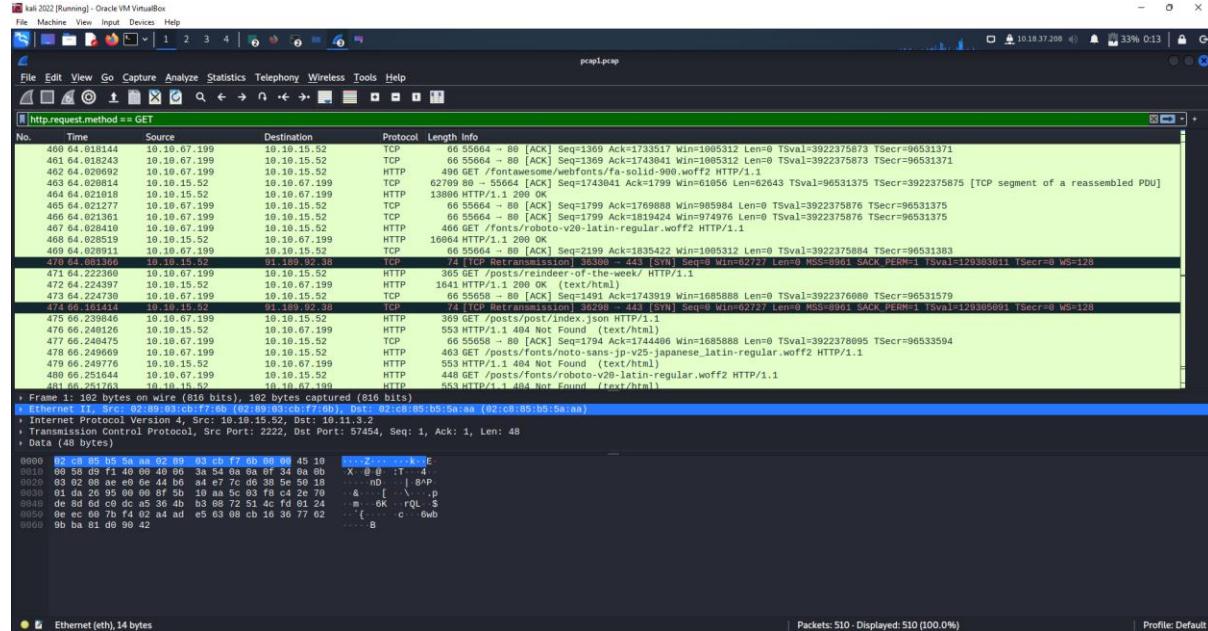
QUESTION 2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

ANSWER: http.request.method == GET



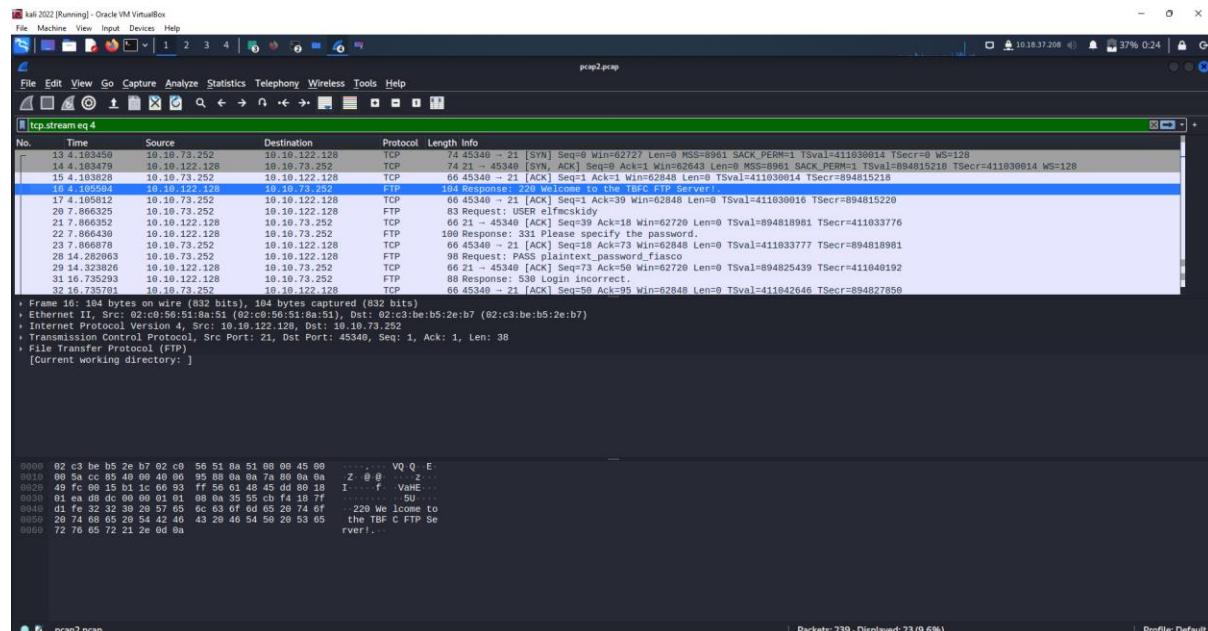
QUESTION 3: Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "**10.10.67.199**" visited

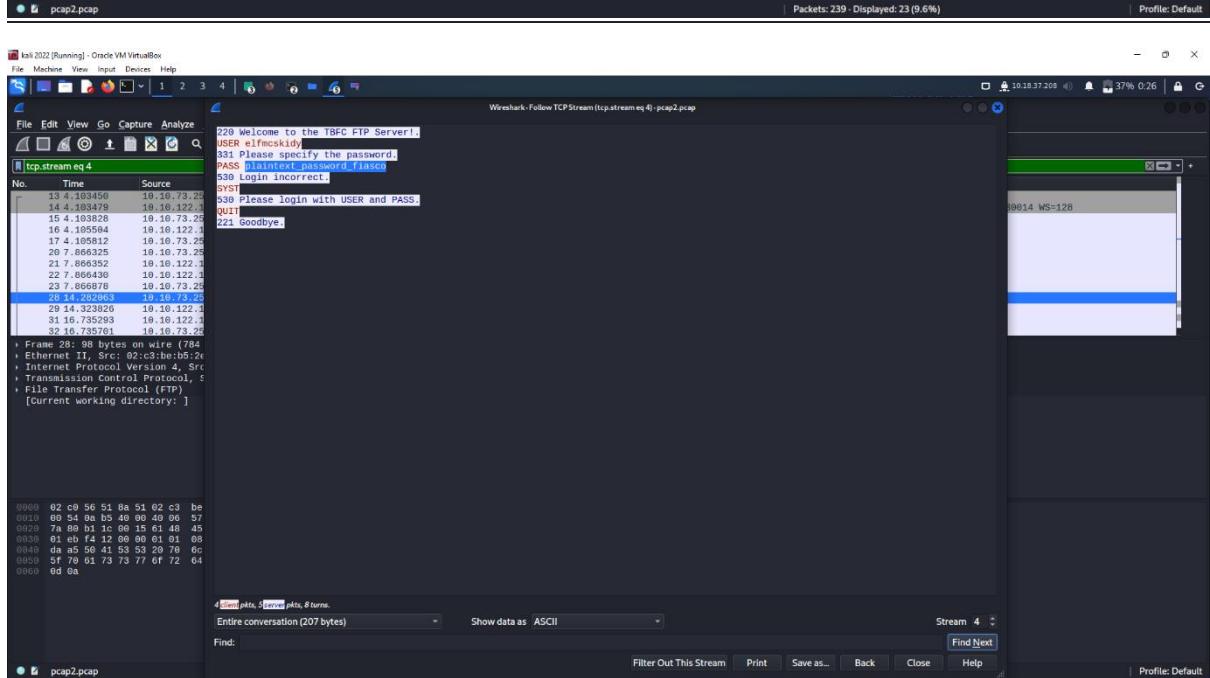
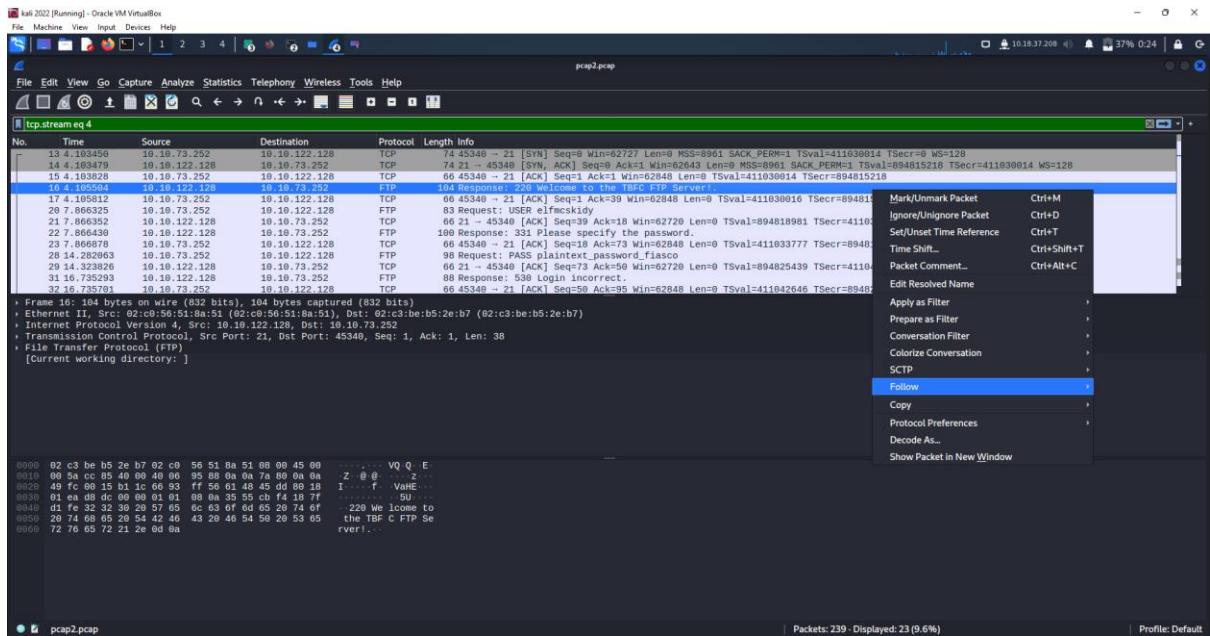
ANSWER: reindeer-of-the-week



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

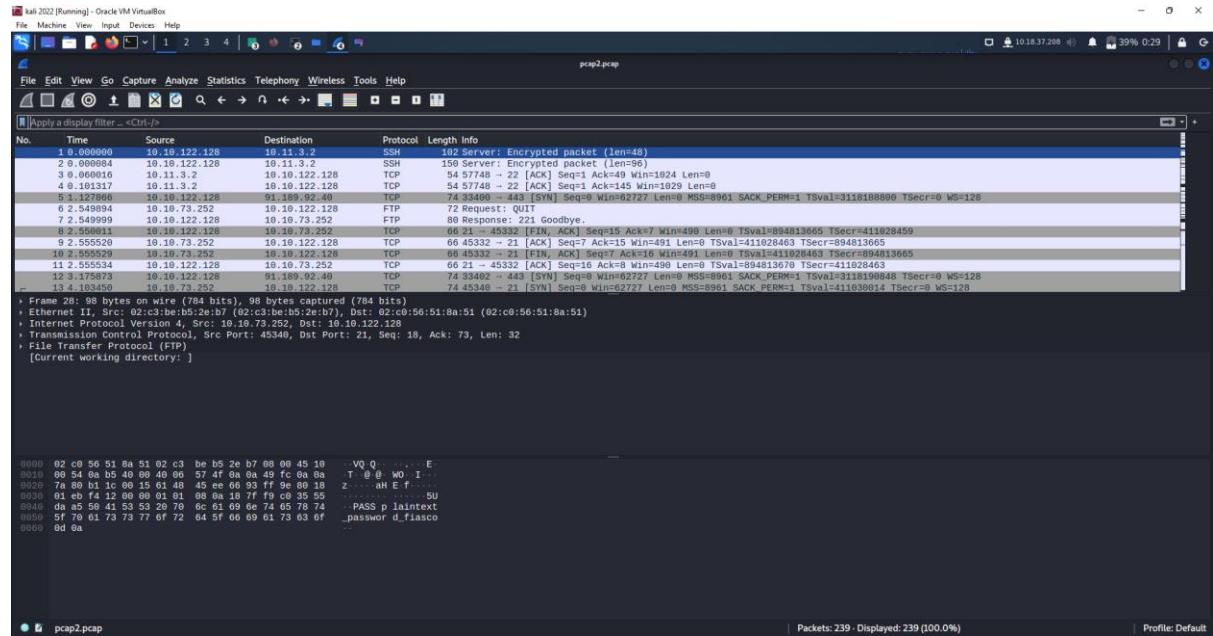
ANSWER: plaintext password fiasco





QUESTION 5 : Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

ANSWER: SSH



QUESTION 6: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1.

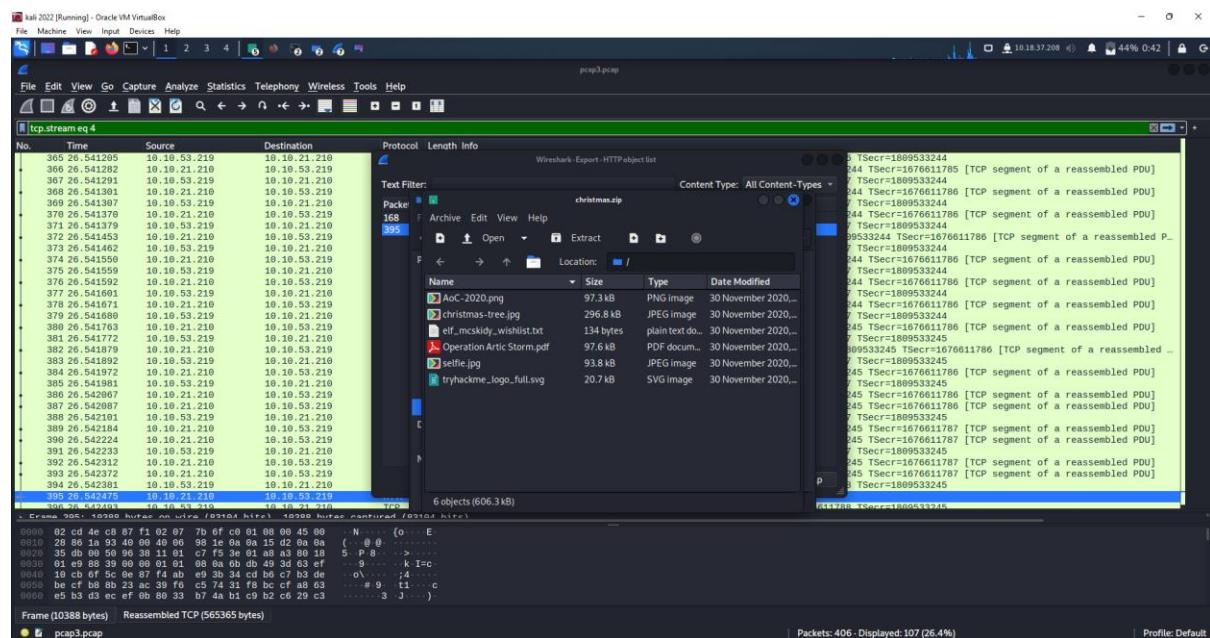
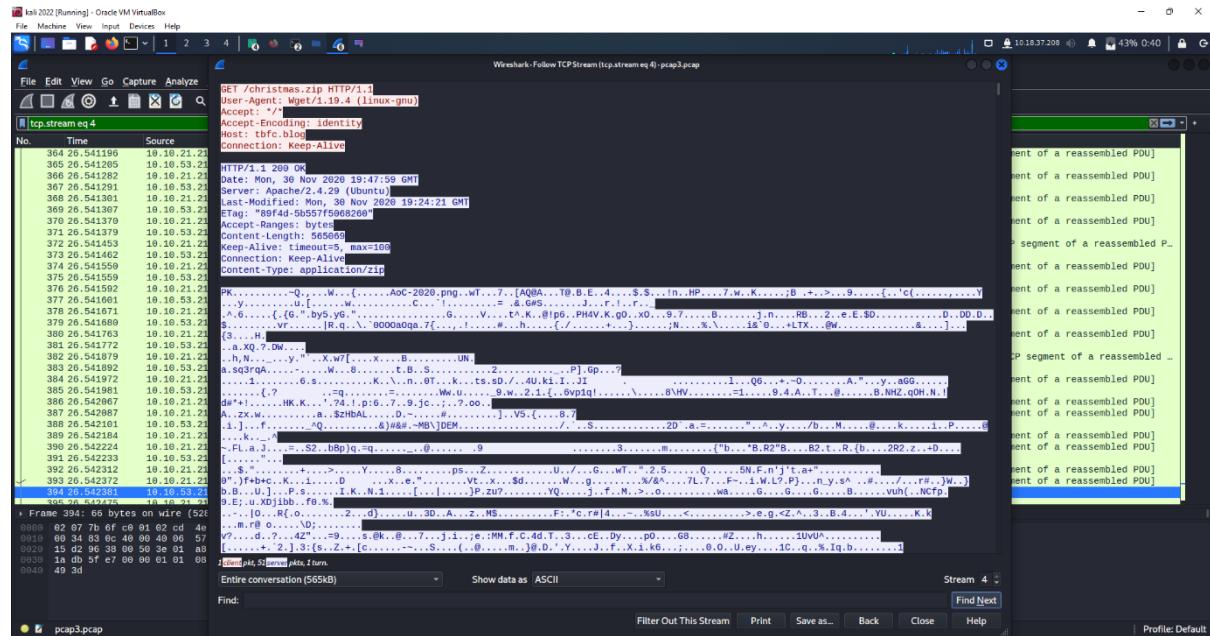
Answer: 10.10.122.128 is at

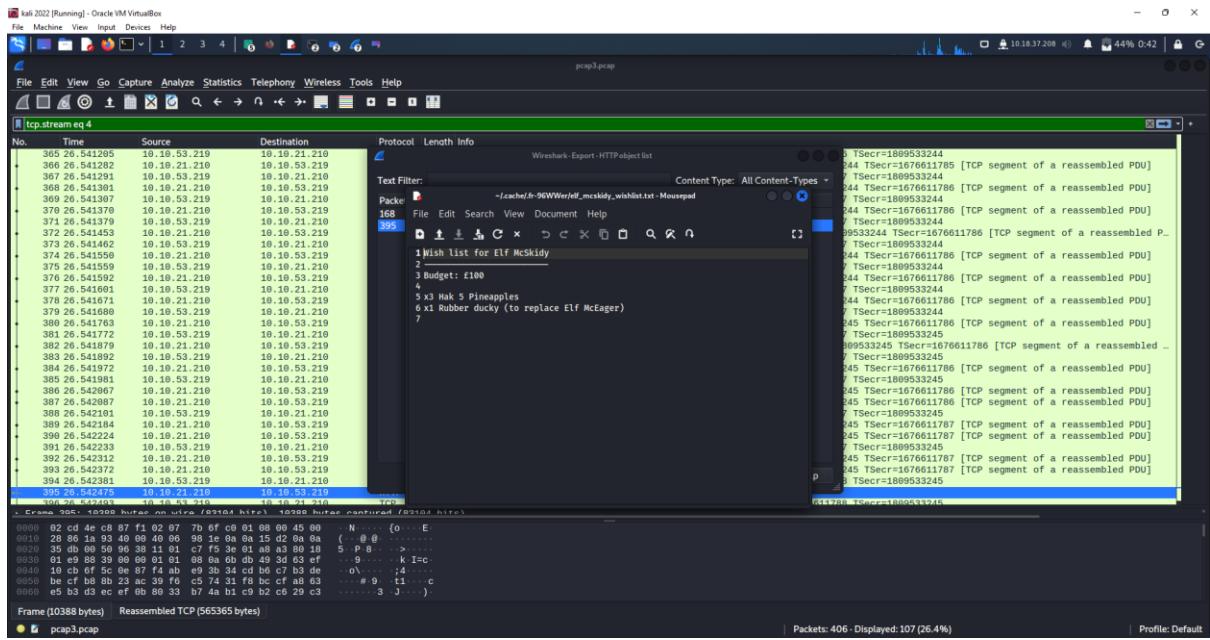
ANSWER: 02:c0:56:51:8a:51



QUESTION 7: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

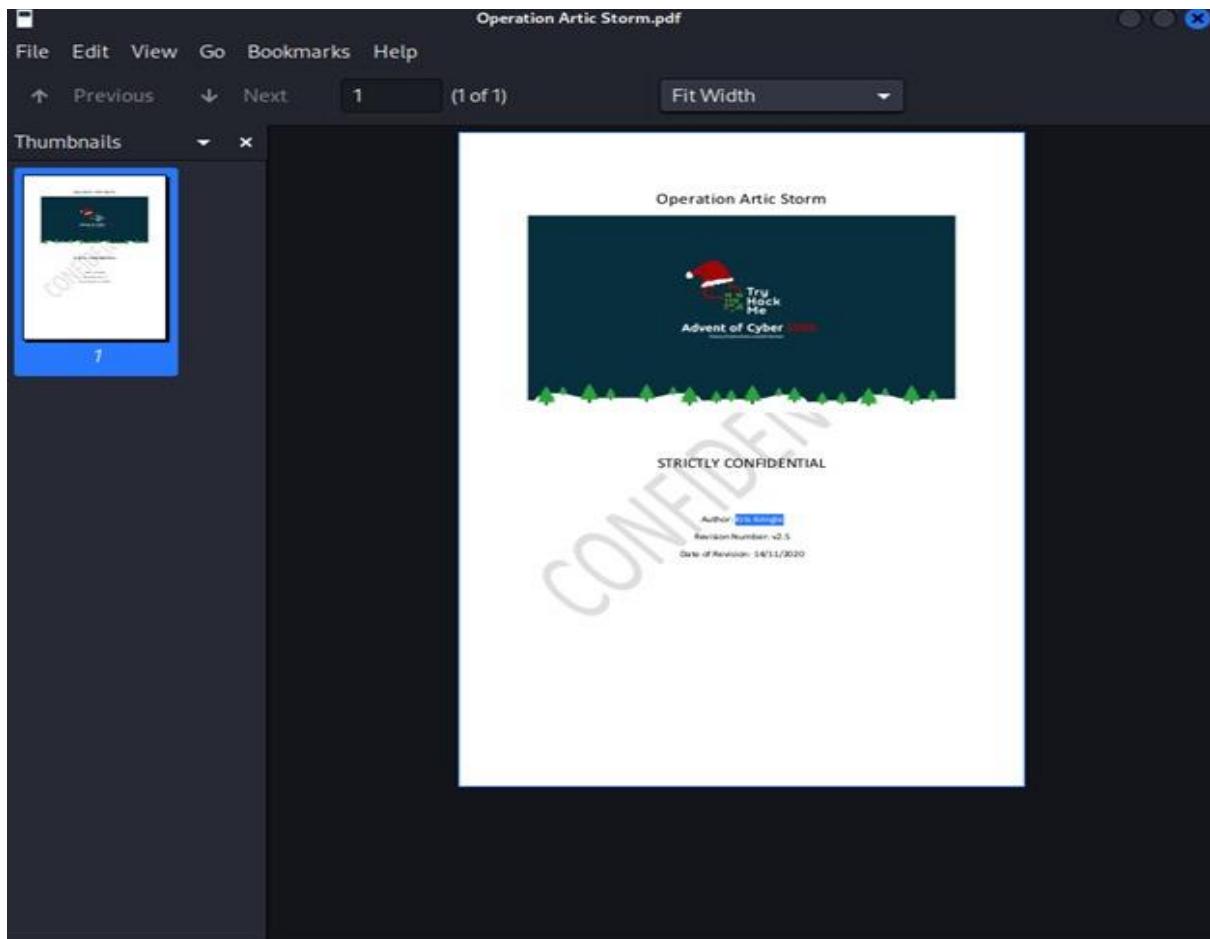
ANSWER: RUBBER DUCKY





QUESTION 8 : Who is the author of Operation Artic Storm?

ANSWER: Kris Kringle



METHODOLOGY:

Firstly, I open the try hack and read the question. I download the file that shows at the tryhackme.

After that, I open Wireshark at my application on my kali Linux. Then I open the pcap1.pcap at Wireshark and that's for the Q1. For the Q2, I use filter "http.request.method == GET" at the url section. This thing will show HTTP GET requests in our "pcap1.pcap" file. After that, the Q3 asked me to find the name of the article that the IP address "10.10.67.199" visited. The name of the article is "reindeer-of-the-week". So, for the Q4, I open the pcap2.pcap. I find where the login was successful. Then, I follow the IP address and lead us to the leaked password. For Q5, I checked the name of the protocol that is encrypted is SSH. After that Q6, I examine the ARP communication, and it says 02:c0:56:51:8a:51 at the Answer: 10.10.122.128. Then, for Q7, I open the code that leads us to Elf McEager, and we download it and shows the Wishlist of Elf McEager, at that text. For the last question, I open the file that I downloaded it at pcap3.pcap and open it. The author of Operation Artic Storm is Kris Kringle.

Day 8 - What's Under the Christmas Tree?

Tools used: AttackBox

Solution/Walkthrough:

Question 1:

When was Snort created?

=1998

Question 2:

Using Nmap on MACHINE IP, what are the port numbers of the three services running?

```
root@ip-10-10-23-213:~  
File Edit View Search Terminal Help  
2222/tcp open EtherNetIP-1  
3389/tcp open ms-wbt-server  
MAC Address: 02:5F:72:A4:E1:99 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds  
root@ip-10-10-23-213:~# -Pn 10.10.10.248  
-Pn: command not found  
root@ip-10-10-23-213:~# nmap -Pn 10.10.10.248  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 04:34 BST  
Nmap scan report for ip-10-10-10-248.eu-west-1.compute.internal (10.10.10.248)  
Host is up (0.00053s latency).  
Not shown: 997 closed ports  
PORT      STATE SERVICE  
80/tcp    open  http  
2222/tcp  open  EtherNetIP-1  
3389/tcp  open  ms-wbt-server  
MAC Address: 02:5F:72:A4:E1:99 (Unknown)  
  
Nmap done: 1 IP address (1 host up) scanned in 1.59 seconds  
root@ip-10-10-23-213:~# nmap -A 10.10.10.248  
  
Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 04:37 BST
```

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?

Using Nmap on 10.10.10.248, what are the port numbers of the three services running?
(Please provide your answer in ascending order/lowest > highest, separated by a comma)

80,2222,3389 **Correct Answer** **Hint**

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 such as `-A` and `-sV` whilst comparing the outputs given.

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?

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?

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

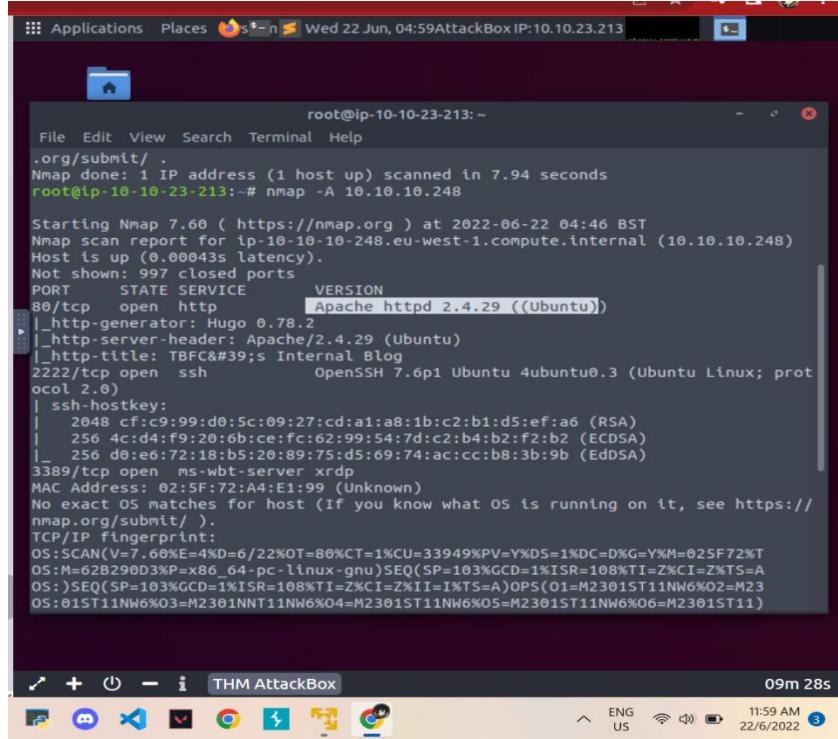
Now use different scripts against the remaining services to discover any further information about them

No answer needed **Completed**

File Edit View Search Terminal Help
.org/submit/ .
root@ip-10-10-23-213:~# nmap -A 10.10.10.248
Starting Nmap 7.60 (https://nmap.org) at 2022-06-22 04:46 BST
Nmap scan report for ip-10-10-10-248.eu-west-1.compute.internal (10.10.10.248)
Host is up (0.00043s latency).
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: TBF C's Internal Blog
2222/tcp open ssh OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|_ 2048 cff:9:99:d0:5c:09:27:cda:ai:a8:1b:c2:b1:d5:ef:a6 (RSA)
| 256 4cd4:f9:20:6b:ce:fc:62:99:54:69:7d: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: 02:5F:72:A4:E1:99 (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=7.60E=4000S=22KQT=18CU=23949NPV=YND5=1X0C=DKG=YKH=025F72ZNT
OS=N=62B29003MP=x86_64-pc-linux-gnu)SEQ(SP=103NGCD=1X1SR=108NTI=2NCI=ZNT5=A)OPS(O1=k23015T11W6K02=R23
OS=15ST11W6K01=M23015T11W6K04=M23015T11W6K05=M23015T11W6K06=M23015T11W6K07=M23015T11W6K08=M23015T11W6K09=M23015T11W6K10=M23015T11W6K11=M23015T11W6K12=M23015T11W6K13=M23015T11W6K14=M23015T11W6K15=M23015T11W6K16=M23015T11W6K17=M23015T11W6K18=M23015T11W6K19=M23015T11W6K20=M23015T11W6K21=M23015T11W6K22=M23015T11W6K23=M23015T11W6K24=M23015T11W6K25=M23015T11W6K26=M23015T11W6K27=M23015T11W6K28=M23015T11W6K29=M23015T11W6K30=M23015T11W6K31=M23015T11W6K32=M23015T11W6K33=M23015T11W6K34=M23015T11W6K35=M23015T11W6K36=M23015T11W6K37=M23015T11W6K38=M23015T11W6K39=M23015T11W6K40=M23015T11W6K41=M23015T11W6K42=M23015T11W6K43=M23015T11W6K44=M23015T11W6K45=M23015T11W6K46=M23015T11W6K47=M23015T11W6K48=M23015T11W6K49=M23015T11W6K50=M23015T11W6K51=M23015T11W6K52=M23015T11W6K53=M23015T11W6K54=M23015T11W6K55=M23015T11W6K56=M23015T11W6K57=M23015T11W6K58=M23015T11W6K59=M23015T11W6K60=M23015T11W6K61=M23015T11W6K62=M23015T11W6K63=M23015T11W6K64=M23015T11W6K65=M23015T11W6K66=M23015T11W6K67=M23015T11W6K68=M23015T11W6K69=M23015T11W6K70=M23015T11W6K71=M23015T11W6K72=M23015T11W6K73=M23015T11W6K74=M23015T11W6K75=M23015T11W6K76=M23015T11W6K77=M23015T11W6K78=M23015T11W6K79=M23015T11W6K80=M23015T11W6K81=M23015T11W6K82=M23015T11W6K83=M23015T11W6K84=M23015T11W6K85=M23015T11W6K86=M23015T11W6K87=M23015T11W6K88=M23015T11W6K89=M23015T11W6K90=M23015T11W6K91=M23015T11W6K92=M23015T11W6K93=M23015T11W6K94=M23015T11W6K95=M23015T11W6K96=M23015T11W6K97=M23015T11W6K98=M23015T11W6K99=M23015T11W6K100=M23015T11W6K101=M23015T11W6K102=M23015T11W6K103=M23015T11W6K104=M23015T11W6K105=M23015T11W6K106=M23015T11W6K107=M23015T11W6K108=M23015T11W6K109=M23015T11W6K110=M23015T11W6K111=M23015T11W6K112=M23015T11W6K113=M23015T11W6K114=M23015T11W6K115=M23015T11W6K116=M23015T11W6K117=M23015T11W6K118=M23015T11W6K119=M23015T11W6K120=M23015T11W6K121=M23015T11W6K122=M23015T11W6K123=M23015T11W6K124=M23015T11W6K125=M23015T11W6K126=M23015T11W6K127=M23015T11W6K128=M23015T11W6K129=M23015T11W6K130=M23015T11W6K131=M23015T11W6K132=M23015T11W6K133=M23015T11W6K134=M23015T11W6K135=M23015T11W6K136=M23015T11W6K137=M23015T11W6K138=M23015T11W6K139=M23015T11W6K140=M23015T11W6K141=M23015T11W6K142=M23015T11W6K143=M23015T11W6K144=M23015T11W6K145=M23015T11W6K146=M23015T11W6K147=M23015T11W6K148=M23015T11W6K149=M23015T11W6K150=M23015T11W6K151=M23015T11W6K152=M23015T11W6K153=M23015T11W6K154=M23015T11W6K155=M23015T11W6K156=M23015T11W6K157=M23015T11W6K158=M23015T11W6K159=M23015T11W6K160=M23015T11W6K161=M23015T11W6K162=M23015T11W6K163=M23015T11W6K164=M23015T11W6K165=M23015T11W6K166=M23015T11W6K167=M23015T11W6K168=M23015T11W6K169=M23015T11W6K170=M23015T11W6K171=M23015T11W6K172=M23015T11W6K173=M23015T11W6K174=M23015T11W6K175=M23015T11W6K176=M23015T11W6K177=M23015T11W6K178=M23015T11W6K179=M23015T11W6K180=M23015T11W6K181=M23015T11W6K182=M23015T11W6K183=M23015T11W6K184=M23015T11W6K185=M23015T11W6K186=M23015T11W6K187=M23015T11W6K188=M23015T11W6K189=M23015T11W6K190=M23015T11W6K191=M23015T11W6K192=M23015T11W6K193=M23015T11W6K194=M23015T11W6K195=M23015T11W6K196=M23015T11W6K197=M23015T11W6K198=M23015T11W6K199=M23015T11W6K200=M23015T11W6K201=M23015T11W6K202=M23015T11W6K203=M23015T11W6K204=M23015T11W6K205=M23015T11W6K206=M23015T11W6K207=M23015T11W6K208=M23015T11W6K209=M23015T11W6K210=M23015T11W6K211=M23015T11W6K212=M23015T11W6K213=M23015T11W6K214=M23015T11W6K215=M23015T11W6K216=M23015T11W6K217=M23015T11W6K218=M23015T11W6K219=M23015T11W6K220=M23015T11W6K221=M23015T11W6K222=M23015T11W6K223=M23015T11W6K224=M23015T11W6K225=M23015T11W6K226=M23015T11W6K227=M23015T11W6K228=M23015T11W6K229=M23015T11W6K230=M23015T11W6K231=M23015T11W6K232=M23015T11W6K233=M23015T11W6K234=M23015T11W6K235=M23015T11W6K236=M23015T11W6K237=M23015T11W6K238=M23015T11W6K239=M23015T11W6K240=M23015T11W6K241=M23015T11W6K242=M23015T11W6K243=M23015T11W6K244=M23015T11W6K245=M23015T11W6K246=M23015T11W6K247=M23015T11W6K248=M23015T11W6K249=M23015T11W6K250=M23015T11W6K251=M23015T11W6K252=M23015T11W6K253=M23015T11W6K254=M23015T11W6K255=M23015T11W6K256=M23015T11W6K257=M23015T11W6K258=M23015T11W6K259=M23015T11W6K260=M23015T11W6K261=M23015T11W6K262=M23015T11W6K263=M23015T11W6K264=M23015T11W6K265=M23015T11W6K266=M23015T11W6K267=M23015T11W6K268=M23015T11W6K269=M23015T11W6K270=M23015T11W6K271=M23015T11W6K272=M23015T11W6K273=M23015T11W6K274=M23015T11W6K275=M23015T11W6K276=M23015T11W6K277=M23015T11W6K278=M23015T11W6K279=M23015T11W6K280=M23015T11W6K281=M23015T11W6K282=M23015T11W6K283=M23015T11W6K284=M23015T11W6K285=M23015T11W6K286=M23015T11W6K287=M23015T11W6K288=M23015T11W6K289=M23015T11W6K290=M23015T11W6K291=M23015T11W6K292=M23015T11W6K293=M23015T11W6K294=M23015T11W6K295=M23015T11W6K296=M23015T11W6K297=M23015T11W6K298=M23015T11W6K299=M23015T11W6K300=M23015T11W6K301=M23015T11W6K302=M23015T11W6K303=M23015T11W6K304=M23015T11W6K305=M23015T11W6K306=M23015T11W6K307=M23015T11W6K308=M23015T11W6K309=M23015T11W6K310=M23015T11W6K311=M23015T11W6K312=M23015T11W6K313=M23015T11W6K314=M23015T11W6K315=M23015T11W6K316=M23015T11W6K317=M23015T11W6K318=M23015T11W6K319=M23015T11W6K320=M23015T11W6K321=M23015T11W6K322=M23015T11W6K323=M23015T11W6K324=M23015T11W6K325=M23015T11W6K326=M23015T11W6K327=M23015T11W6K328=M23015T11W6K329=M23015T11W6K330=M23015T11W6K331=M23015T11W6K332=M23015T11W6K333=M23015T11W6K334=M23015T11W6K335=M23015T11W6K336=M23015T11W6K337=M23015T11W6K338=M23015T11W6K339=M23015T11W6K340=M23015T11W6K341=M23015T11W6K342=M23015T11W6K343=M23015T11W6K344=M23015T11W6K345=M23015T11W6K346=M23015T11W6K347=M23015T11W6K348=M23015T11W6K349=M23015T11W6K350=M23015T11W6K351=M23015T11W6K352=M23015T11W6K353=M23015T11W6K354=M23015T11W6K355=M23015T11W6K356=M23015T11W6K357=M23015T11W6K358=M23015T11W6K359=M23015T11W6K360=M23015T11W6K361=M23015T11W6K362=M23015T11W6K363=M23015T11W6K364=M23015T11W6K365=M23015T11W6K366=M23015T11W6K367=M23015T11W6K368=M23015T11W6K369=M23015T11W6K370=M23015T11W6K371=M23015T11W6K372=M23015T11W6K373=M23015T11W6K374=M23015T11W6K375=M23015T11W6K376=M23015T11W6K377=M23015T11W6K378=M23015T11W6K379=M23015T11W6K380=M23015T11W6K381=M23015T11W6K382=M23015T11W6K383=M23015T11W6K384=M23015T11W6K385=M23015T11W6K386=M23015T11W6K387=M23015T11W6K388=M23015T11W6K389=M23015T11W6K390=M23015T11W6K391=M23015T11W6K392=M23015T11W6K393=M23015T11W6K394=M23015T11W6K395=M23015T11W6K396=M23015T11W6K397=M23015T11W6K398=M23015T11W6K399=M23015T11W6K400=M23015T11W6K401=M23015T11W6K402=M23015T11W6K403=M23015T11W6K404=M23015T11W6K405=M23015T11W6K406=M23015T11W6K407=M23015T11W6K408=M23015T11W6K409=M23015T11W6K410=M23015T11W6K411=M23015T11W6K412=M23015T11W6K413=M23015T11W6K414=M23015T11W6K415=M23015T11W6K416=M23015T11W6K417=M23015T11W6K418=M23015T11W6K419=M23015T11W6K420=M23015T11W6K421=M23015T11W6K422=M23015T11W6K423=M23015T11W6K424=M23015T11W6K425=M23015T11W6K426=M23015T11W6K427=M23015T11W6K428=M23015T11W6K429=M23015T11W6K430=M23015T11W6K431=M23015T11W6K432=M23015T11W6K433=M23015T11W6K434=M23015T11W6K435=M23015T11W6K436=M23015T11W6K437=M23015T11W6K438=M23015T11W6K439=M23015T11W6K440=M23015T11W6K441=M23015T11W6K442=M23015T11W6K443=M23015T11W6K444=M23015T11W6K445=M23015T11W6K446=M23015T11W6K447=M23015T11W6K448=M23015T11W6K449=M23015T11W6K450=M23015T11W6K451=M23015T11W6K452=M23015T11W6K453=M23015T11W6K454=M23015T11W6K455=M23015T11W6K456=M23015T11W6K457=M23015T11W6K458=M23015T11W6K459=M23015T11W6K460=M23015T11W6K461=M23015T11W6K462=M23015T11W6K463=M23015T11W6K464=M23015T11W6K465=M23015T11W6K466=M23015T11W6K467=M23015T11W6K468=M23015T11W6K469=M23015T11W6K470=M23015T11W6K471=M23015T11W6K472=M23015T11W6K473=M23015T11W6K474=M23015T11W6K475=M23015T11W6K476=M23015T11W6K477=M23015T11W6K478=M23015T11W6K479=M23015T11W6K480=M23015T11W6K481=M23015T11W6K482=M23015T11W6K483=M23015T11W6K484=M23015T11W6K485=M23015T11W6K486=M23015T11W6K487=M23015T11W6K488=M23015T11W6K489=M23015T11W6K490=M23015T11W6K491=M23015T11W6K492=M23015T11W6K493=M23015T11W6K494=M23015T11W6K495=M23015T11W6K496=M23015T11W6K497=M23015T11W6K498=M23015T11W6K499=M23015T11W6K500=M23015T11W6K501=M23015T11W6K502=M23015T11W6K503=M23015T11W6K504=M23015T11W6K505=M23015T11W6K506=M23015T11W6K507=M23015T11W6K508=M23015T11W6K509=M23015T11W6K510=M23015T11W6K511=M23015T11W6K512=M23015T11W6K513=M23015T11W6K514=M23015T11W6K515=M23015T11W6K516=M23015T11W6K517=M23015T11W6K518=M23015T11W6K519=M23015T11W6K520=M23015T11W6K521=M23015T11W6K522=M23015T11W6K523=M23015T11W6K524=M23015T11W6K525=M23015T11W6K526=M23015T11W6K527=M23015T11W6K528=M23015T11W6K529=M23015T11W6K530=M23015T11W6K531=M23015T11W6K532=M23015T11W6K533=M23015T11W6K534=M23015T11W6K535=M23015T11W6K536=M23015T11W6K537=M23015T11W6K538=M23015T11W6K539=M23015T11W6K540=M23015T11W6K541=M23015T11W6K542=M23015T11W6K543=M23015T11W6K544=M23015T11W6K545=M23015T11W6K546=M23015T11W6K547=M23015T11W6K548=M23015T11W6K549=M23015T11W6K550=M23015T11W6K551=M23015T11W6K552=M23015T11W6K553=M23015T11W6K554=M23015T11W6K555=M23015T11W6K556=M23015T11W6K557=M23015T11W6K558=M23015T11W6K559=M23015T11W6K560=M23015T11W6K561=M23015T11W6K562=M23015T11W6K563=M23015T11W6K564=M23015T11W6K565=M23015T11W6K566=M23015T11W6K567=M23015T11W6K568=M23015T11W6K569=M23015T11W6K570=M23015T11W6K571=M23015T11W6K572=M23015T11W6K573=M23015T11W6K574=M23015T11W6K575=M23015T11W6K576=M23015T11W6K577=M23015T11W6K578=M23015T11W6K579=M23015T11W6K580=M23015T11W6K581=M23015T11W6K582=M23015T11W6K583=M23015T11W6K584=M23015T11W6K585=M23015T11W6K586=M23015T11W6K587=M23015T11W6K588=M23015T11W6K589=M23015T11W6K590=M23015T11W6K591=M23015T11W6K592=M23015T11W6K593=M23015T11W6K594=M23015T11W6K595=M23015T11W6K596=M23015T11W6K597=M23015T11W6K598=M23015T11W6K599=M23015T11W6K600=M23015T11W6K601=M23015T11W6K602=M23015T11W6K603=M23015T11W6K604=M23015T11W6K605=M23015T11W6K606=M23015T11W6K607=M23015T11W6K608=M23015T11W6K609=M23015T11W6K610=M23015T11W6K611=M23015T11W6K612=M23015T11W6K613=M23015T11W6K614=M2301

Question 4:

What is the version of Apache?



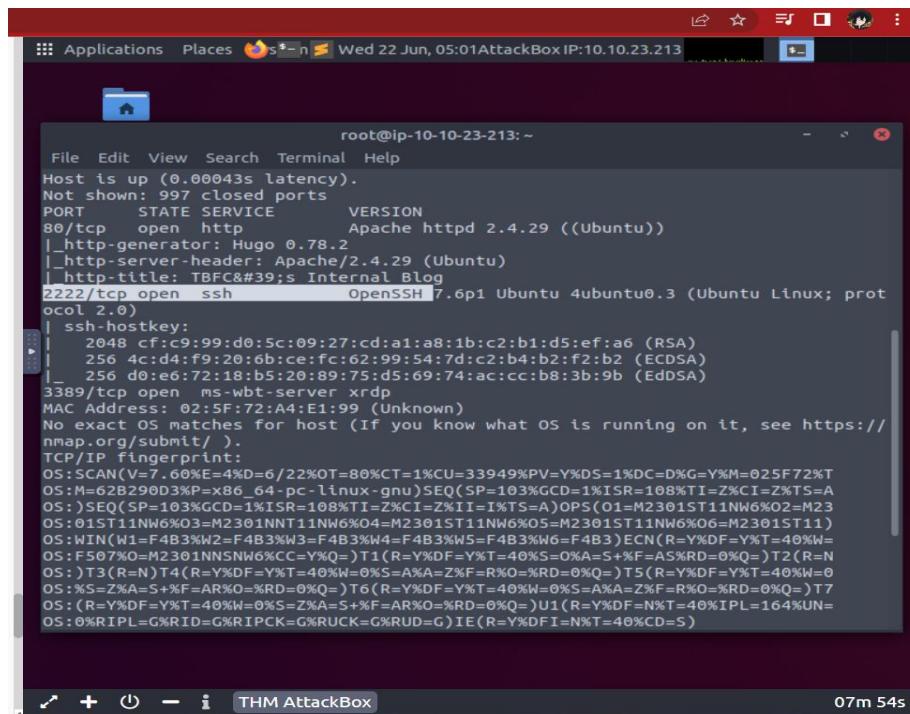
```
root@ip-10-10-23-213: ~
File Edit View Search Terminal Help
.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 7.94 seconds
root@ip-10-10-23-213:~# nmap -A 10.10.10.248

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-22 04:46 BST
Nmap scan report for ip-10-10-248.eu-west-1.compute.internal (10.10.10.248)
Host is up (0.00043s latency).
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's Internal Blog
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 (EdDSA)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:5F:72:A4:E1:99 (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=6/22%OT=80%CT=1%CU=33949%PV=Y%DS=1%DC=D%G=Y%M=025F72%TOS=M=62B290D3%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW6%O2=M23OS:)SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW6%O5=M2301ST11NW6%O6=M2301ST11)
```



Question 5:

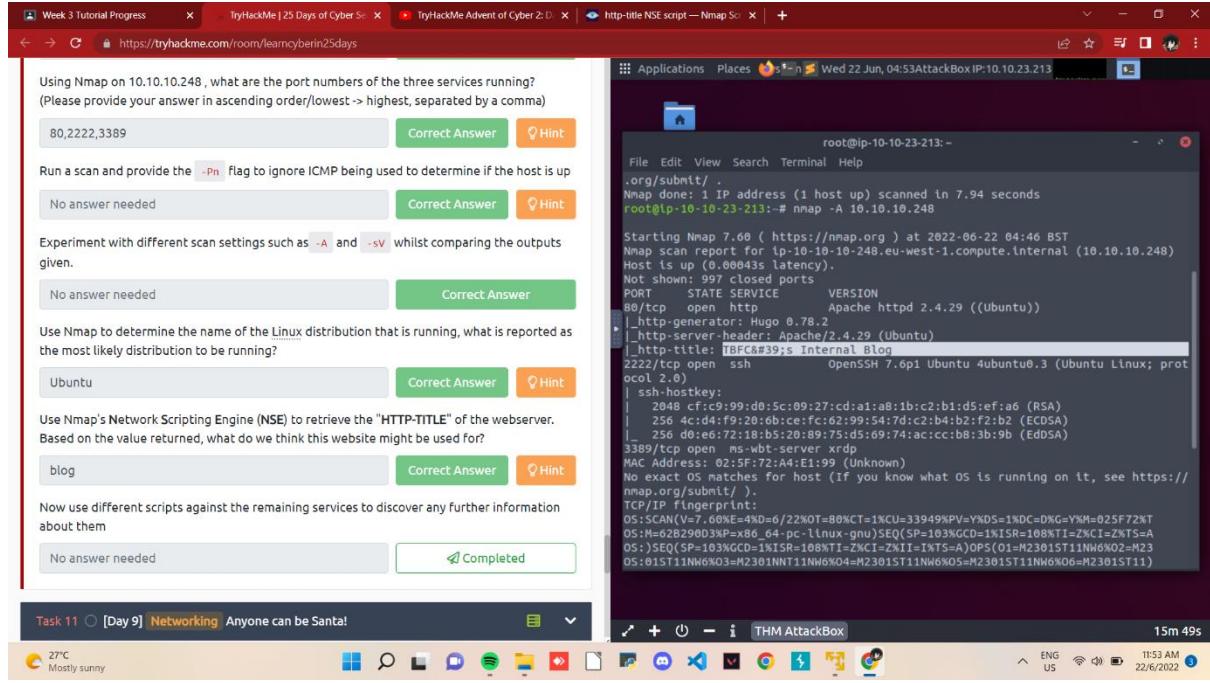
What is running on port 2222?



```
root@ip-10-10-23-213: ~
File Edit View Search Terminal Help
Host is up (0.00043s latency).
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's Internal Blog
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 (EdDSA)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:5F:72:A4:E1:99 (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=6/22%OT=80%CT=1%CU=33949%PV=Y%DS=1%DC=D%G=Y%M=025F72%TOS=M=62B290D3%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW6%O2=M23OS:)SEQ(SP=103%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW6%O5=M2301ST11NW6%O6=M2301ST11)OS:WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W0=F4B3)ECN(R=Y%DF=Y%T=40%W=OS:F507%O=M2301NNST11NW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%W=0%A=5+%F=AS%RD=0%Q=)T2(R=NOS:S%Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=2%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=A%A=2%F=R%O=%RD=0%Q=)T7(OS:S%Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=5)
```

Question 6:

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

METHODOLOGY

First of all, we started the Machine and the AttackBox waiting to obtain Ip address. Then, we open the terminal and run the scan using Nmap with the Ip provided to get the port numbers of the three services running it. Lastly, we scan again the Nmap with different scan settings using -A to retrieve the outputs to solve the name of the Linux distribution that is running, the version of Apache, type running of the port numbers and the value of the webserver.

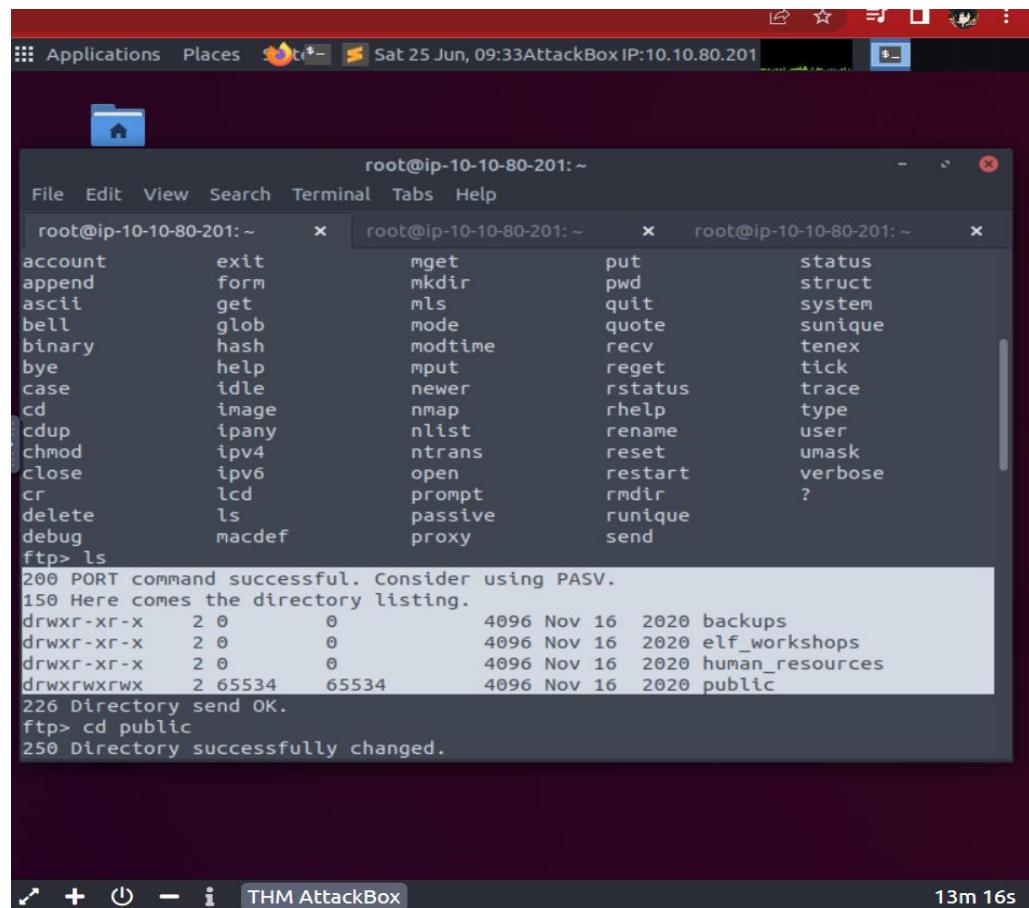
Day 9 – Anyone can be Santa!

Tools used: AttackBox

Solution/ Walkthrough:

Question 1:

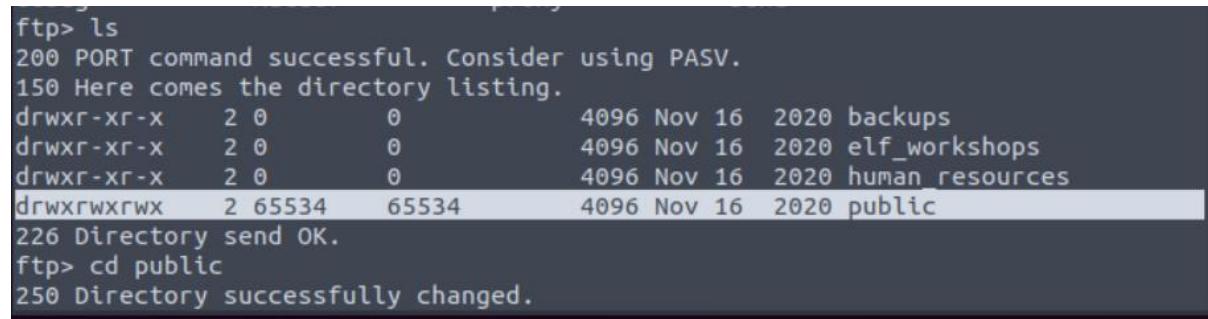
What are the directories you found on the FTP site?



```
root@ip-10-10-80-201:~      x  root@ip-10-10-80-201:~      x  root@ip-10-10-80-201:~      x
File Edit View Search Terminal Tabs Help
root@ip-10-10-80-201:~      x  root@ip-10-10-80-201:~      x  root@ip-10-10-80-201:~      x
account      exit      mget      put      status
append      form      mkdir      pwd      struct
ascii       get       mls       quit      system
bell        glob      mode      quote     unique
binary      hash      modtime   recv     tenex
bye         help      mput      reget    tick
case        idle      newer     rstatus   trace
cd          image     nmap      rhelp    type
cdup       ipany     nlist     rename   user
chmod      ipv4      ntrans    reset    umask
close      ipv6      open      restart  verbose
cr          lcd      prompt   runique  ?
delete     ls       passive  proxy
debug      macdef
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.
```

Question 2:

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

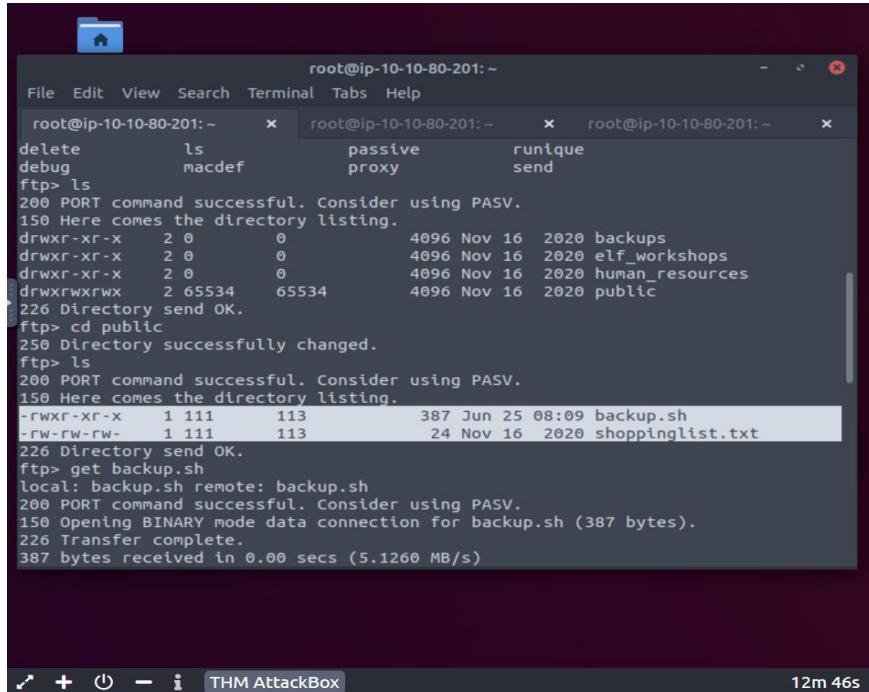


```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0          0          4096 Nov 16  2020 backups
drwxr-xr-x  2 0          0          4096 Nov 16  2020 elf_workshops
drwxr-xr-x  2 0          0          4096 Nov 16  2020 human_resources
drwxrwxrwx  2 65534     65534     4096 Nov 16  2020 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
```

Question 3:

What script gets executed within this directory?

=**backup.sh**

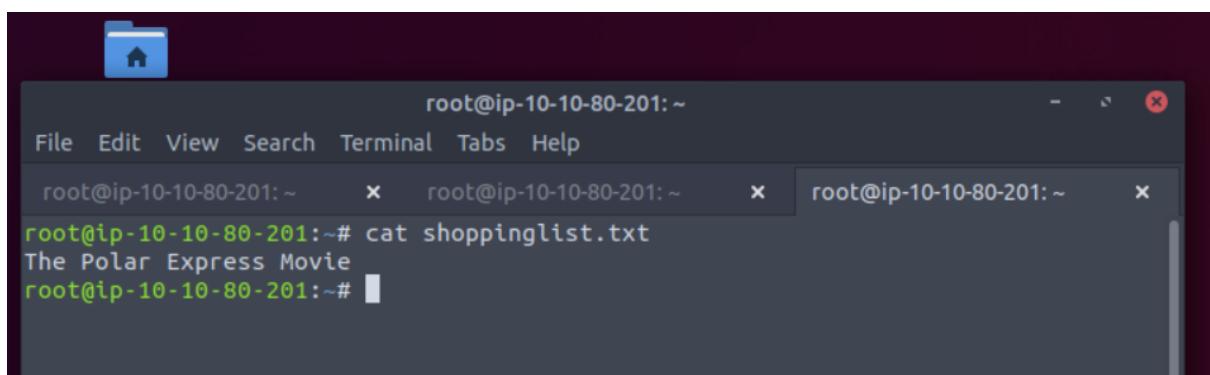


```
root@ip-10-10-80-201:~ x root@ip-10-10-80-201:~ x root@ip-10-10-80-201:~ x
File Edit View Search Terminal Tabs Help
root@ip-10-10-80-201:~ x root@ip-10-10-80-201:~ x root@ip-10-10-80-201:~ x
delete ls passive runique
debug macdef proxy send
ftp> ls
200 PORT command successful. Consider using PASV.
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 1 111 113 387 Jun 25 08:09 backup.sh
-rw-rw-rw- 1 111 113 24 Nov 16 2020 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (387 bytes).
226 Transfer complete.
387 bytes received in 0.00 secs (5.1260 MB/s)

12m 46s
```

Question 4:

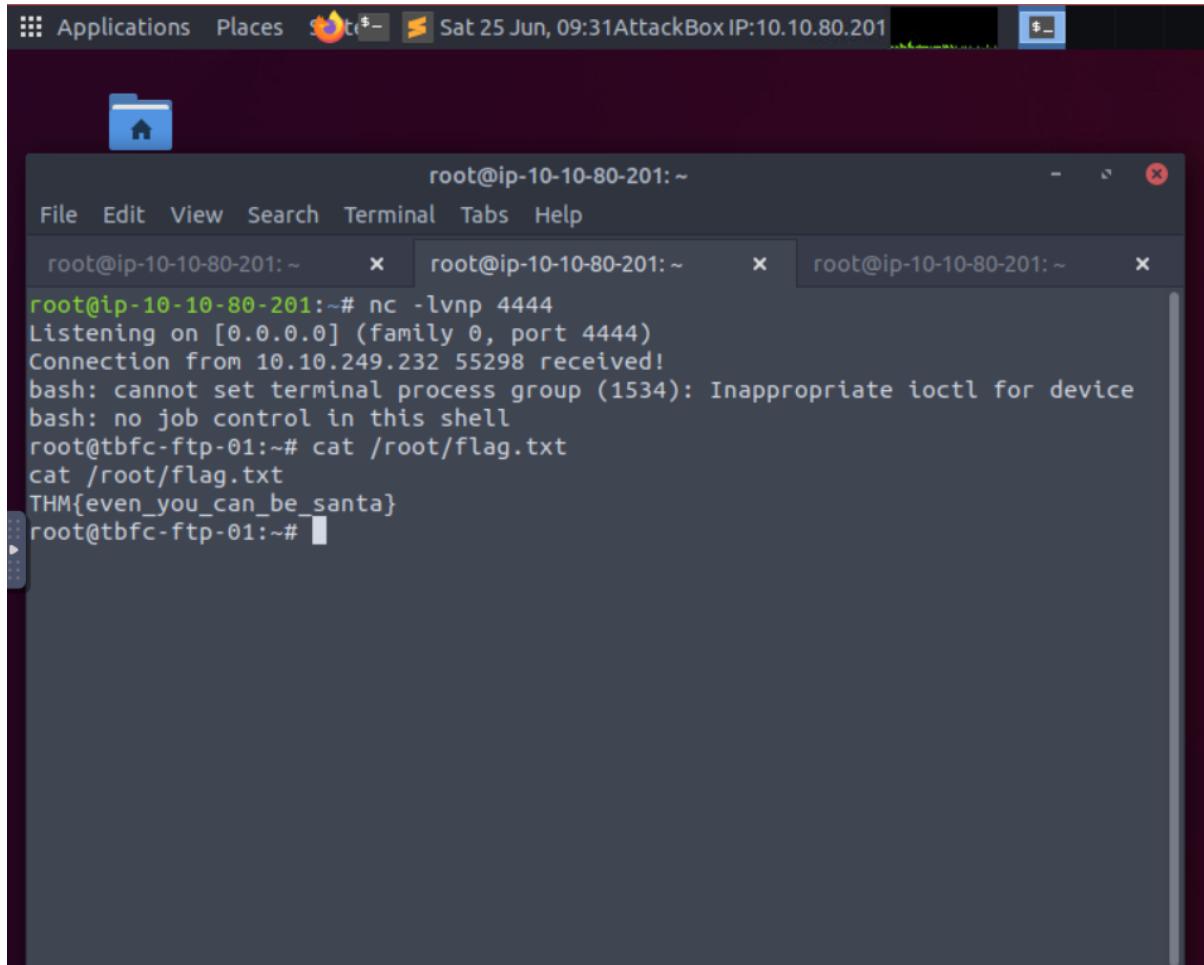
What movie did Santa have on his Christmas shopping list?



```
root@ip-10-10-80-201:~ x root@ip-10-10-80-201:~ x root@ip-10-10-80-201:~ x
File Edit View Search Terminal Tabs Help
root@ip-10-10-80-201:~ x root@ip-10-10-80-201:~ x root@ip-10-10-80-201:~ x
root@ip-10-10-80-201:~# cat shoppinglist.txt
The Polar Express Movie
root@ip-10-10-80-201:~#
```

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!)



The screenshot shows a terminal window titled "root@ip-10-10-80-201: ~". It has three tabs open, all showing the same command-line interface. The first tab shows a netcat listener being set up: "root@ip-10-10-80-201:~# nc -lvpn 4444". The second tab shows a connection from an IP address: "Connection from 10.10.249.232 55298 received!". The third tab shows the contents of the file "/root/flag.txt": "THM{even_you_can_be_santa}".

METHODOLOGY:

We run the Machine and the AttackBox. To connect, we simply use ftp and provide the IP address of the Instance. When prompted for our "Name", we enter "anonymous". If successful, we have confirmed that the FTP Server has "anonymous" mode enabled - successful login. We apply command "ls" to look at the directories available in the FTP server and find out which directory that has data accessible by the anonymous user. Then we use nano to see the scripts. By that we work pentesters cheatsheet to get a good command that will be executed by the server to generate a shell to our AttackBox, replacing the IP_ADDRESS with the TryHackMe IP. We set up a netcat listener to catch the connection on our AttackBox and return to our FTP prompt and employ put to put the file into that directory. Lastly, we go back to our netcat listener, wait for about one minute to succeed. Now we have a reverse system shell on the FTP Server as the most powerful user that we can re-upload the script by putting the output contents of /root/flag.txt!

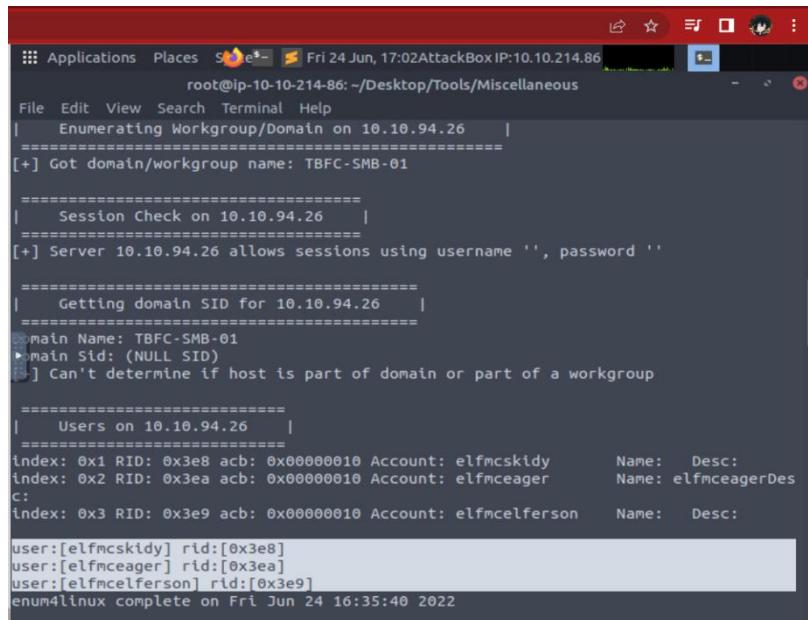
Day 10 - Don't be sElfish!

Tools used: AttackBox

Solution/ Walkthrough:

Question 2:

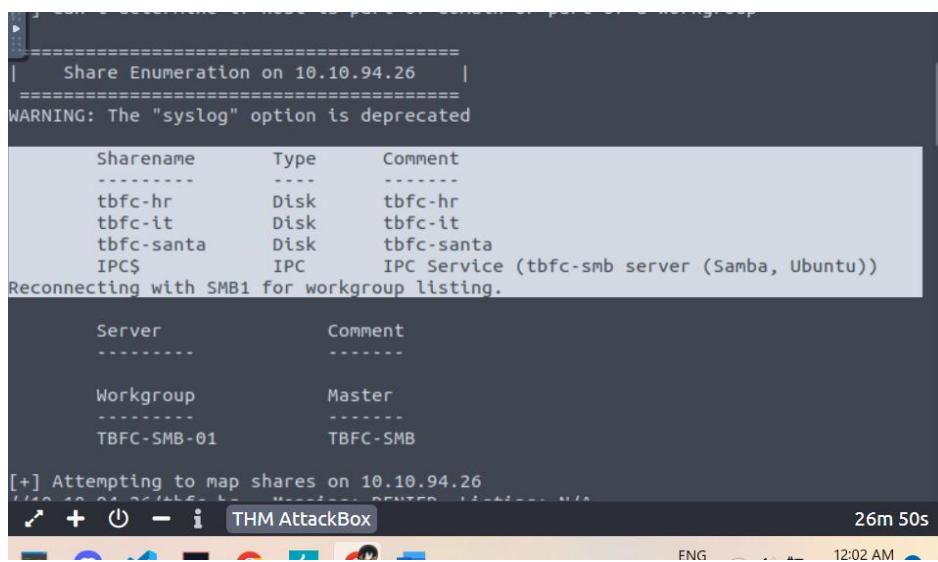
Using enum4linux, how many users are there on the Samba server?



```
root@ip-10-10-214-86:~/Desktop/Tools/Miscellaneous
[+] Got domain/workgroup name: TBFC-SMB-01
[+] Server 10.10.94.26 allows sessions using username '', password ''
[+] Can't determine if host is part of domain or part of a workgroup
[+] Users on 10.10.94.26
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager       Name: elfmceagerDes
c:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson    Name:   Desc:
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Fri Jun 24 16:35:40 2022
```

Question 3:

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



```
| Share Enumeration on 10.10.94.26 |
=====
WARNING: The "syslog" option is deprecated

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

      Server          Comment
      -----          -----
      Workgroup      Master
      -----          -----
      TBFC-SMB-01    TBFC-SMB

[+] Attempting to map shares on 10.10.94.26
26m 50s
```

Question 4:

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

→ C https://tryhackme.com/room/learncyberin25days

We will demonstrate below:

1. Remember that the IP address of the Samba server is that of the instance you deployed (10.10.94.26)
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
<code>ls</code>	List files and directories in the current location
<code>cd <directory></code>	Change our working directory
<code>pwd</code>	Output the full path to our working directory
<code>more <filename></code>	Find out more about the contents of a file. To close the open file, you press <code>:q</code>
<code>get <filename></code>	Download a file from a share
<code>put <filename></code>	Upload a file from a share

Applications Places Terminal Fri 24 Jun, 17:04 AttackBox IP:10.10.214.86

```
root@ip-10-10-214-86:~/Desktop/Tools/Miscellaneous# smbclient //10.10.94.26/tbfc-sa
nta
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
l          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
mask       mput        newer       notify      mkdir
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: \> 
```

THM AttackBox 25m 20s

Question 5:

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

→ C https://tryhackme.com/room/learncyberin25days

Answer the questions below

Question #1 Using `enum4linux`, how many users are there on the Samba server (10.10.94.26)?

3 Correct Answer

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

4 Correct Answer

Question #3 Use `smbclient` to try to login to the shares on the Samba server (10.10.94.26). What share doesn't require a password?

tbfc-santa Correct Answer

Question #4 Log in to this share, what directory did ElfMcSkidy leave for Santa?

jingle-tunes Correct Answer Hint

Task 13 ○ [Day 11] Networking The Rogue Gnome

Task 14 ○ [Day 12] Networking Ready, set, elf.

Task 15 ○ [Day 13] Networking Coal for Christmas

Task 16 ○ [Day 14] OSINT Where's Rudolph?

Applications Places Terminal Fri 24 Jun, 17:04 AttackBox IP:10.10.214.86

```
root@ip-10-10-214-86:~/Desktop/Tools/Miscellaneous# smbclient //10.10.94.26/tbfc-sa
nta
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> help
l          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
mask       mput        newer       notify      mkdir
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
.
..
[jingle-tunes]
note_from_msksidy.txt
10252564 blocks of size 1024. 5369400 blocks available
smb: \> 
```

THM AttackBox 25m 06s

METHODOLOGY:

As usual we started the Machine and the AttackBox, then we open a terminal prompt and navigate to enum4linux: cd /root/Desktop/Tools/Miscellaneous. We continue running enum4linux using (./enum4linux.pl -h) to study all the list possible options we can use. Next, we want to find out who can be used to access the server through Samba: (./enum4linux.pl -U [the Ip address]) then enum4linux showed four users in the Samba server. Now we want to know how many “shares” in the Samba server so we use (./enum4linux.pl -S [Ip address]) to obtain the share list. Moving on we use the smbclient tool to accessing the share that doesn’t require a password. Lastly, we use command “ls” in the smbclient tools to receive the directory.