

PSP0201

Week 3

Report

Group Name : Cipher

Members :

| ID | Name | Role |
|------------|------------------------------|--------|
| 1211103064 | MUHAMAD AIMAN BIN MOHD EHWAL | Leader |
| 1211103085 | MUHAMMAD FARID BIN JAYATAN | Member |
| 1211103373 | MUHAMMAD ALIF BIN KHABALI | Member |
| 1211103451 | ARIF MUHRIZ BIN SYAMSUL FOZY | Member |

Day 6 : Web Exploitation - Be Careful With What You Wish On A Christmas Night

Tool Used : Kali Linux, Firefox

Solution / Walkthrough :

Question 1 & 2

What vulnerability type was used to exploit the application?

stored crosssite scripting

Correct Answer

Here you can anonymously submit your Christmas wishes and see what other people wished too!

wow

When we type anything in the query section, we will get a parameter of 'q'

10.10.207.173:5000/?q=wow

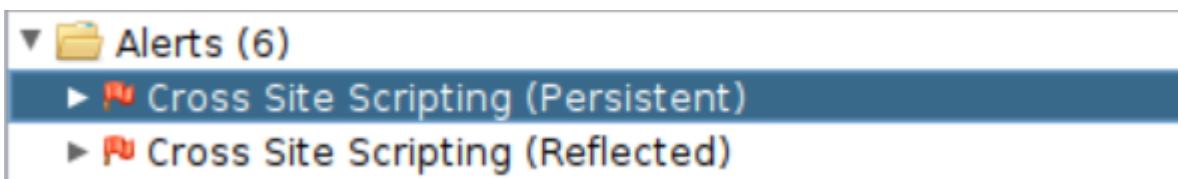
What query string can be abused to craft a reflected XSS?

q

Correct Answer

💡 Hint

Question 3



There are two types of XSS scripting in the scan which are persistent and reflected

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

2

Correct Answer

Thought Process / Methodology : After launching the website, we can get the query string that is abused to craft a reflected XSS by typing something in the query section. Then, we launch the OWASP ZAP application to run a ZAP (zaproxy) automated scan on the target. It will then show the amount of XSS alerts that are in the scan.

Day 7 : Networking - The Grinch Really Did Steal Christmas

Tool Used : Kali Linux, Firefox

Solution / Walkthrough :

Question 1 & 2



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

10.11.3.2

Correct Answer

The source is coming from 10.11.3.2

protocol.request.method

Show all packets that use a specific method of the protocol given. For example, HTTP allows for both a

GET and POST

to retrieve and submit data accordingly.

http.request.method ==
GET / POST

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

http.request.method == GET

Correct Answer

💡 Hint

Question 3

HTTP

365 GET /posts/reindeer-of-the-week/ HTTP/1.1

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?

reindeer-of-the-week

Correct Answer

💡 Hint

Question 4

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

Question 5

```
SSH      102 Server: Encrypted packet (len=48)
SSH      150 Server: Encrypted packet (len=96)
```

Question 7

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

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

Thought Process / Methodology : After downloading the zip file, open the file "pcap1.pcap" in wireshark. It will show the IP address that initiates an ICMP/ping. We then use "http.request.method == GET" to see HTTP GET requests in our "pcap1.pcap" file. After applying the filter, we can get the name of the article that the IP address "10.10.67.199" visited. After that, we use the filter "tcp.port == 21" in the file "pcap2.pcap" to get the password that was leaked during the login process.

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

Tool Used : Kali Linux, Firefox

Solution / Walkthrough :

Question 1

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.

Snort was created in 1998.

Question 2

```
└─(1211103064㉿kali)-[~]
$ nmap 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:47 EDT
Stats: 0:00:42 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 72.87% done; ETC: 23:48 (0:00:16 remaining)
Nmap scan report for 10.10.125.174
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 68.49 seconds
```

We got it by using the command **nmap** on the **Machine_ip**.

Question 3

```
└─(1211103064㉿kali)-[~]
$ nmap -Pn 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:50 EDT
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.80% done; ETC: 23:51 (0:00:02 remaining)
Nmap scan report for 10.10.125.174
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 37.16 seconds
```

We use **-Pn** to determine if the host is up or not.

Question 4

```
(1211103064㉿kali)-[~]
$ nmap -A 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:52 EDT
Nmap scan report for 10.10.125.174
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
2222/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
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 44.65 seconds
```

```
(1211103064㉿kali)-[~]
$ nmap -sV 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:56 EDT
Nmap scan report for 10.10.125.174
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
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
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 34.34 seconds
```

We experiment with different scan settings such as **-A** and **-sV** and comparing the outputs between those two scan settings.

Question 5

```
└─(1211103064㉿kali)-[~]
$ nmap -sV 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:56 EDT
Nmap scan report for 10.10.125.174
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
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
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 34.34 seconds
```

We get the name of the linux that is running through the scan that we did earlier.

Question 6

```
└─(1211103064㉿kali)-[~]
$ nmap -A 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:52 EDT
Nmap scan report for 10.10.125.174
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http          Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
2222/tcp  open  ssh          OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|_  256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
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 44.65 seconds
```

The website is used for blog. We get it by using the nmap scan.

Question 7

```
[~] $ nmap --script ftp-proftpd-backdoor -p 21 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:55 EDT
Nmap scan report for 10.10.125.174
Host is up (0.22s latency).

PORT      STATE SERVICE
21/tcp    closed  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.57 seconds
```

```
[~] $ nmap -A -sV -sC 10.10.125.174
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-21 23:45 EDT
Stats: 0:00:40 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 33.33% done; ETC: 23:46 (0:00:12 remaining)
Nmap scan report for 10.10.125.174
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-title: TBFC's Internal Blog
|_http-server-header: Apache/2.4.29 (Ubuntu)
2222/tcp  open  ssh        OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux;
protocol 2.0)
| ssh-hostkey:
|   2048 cf:c9:99:d0:5c:09:27:cd:a1:a8:1b:c2:b1:d5:ef:a6 (RSA)
|   256 4c:d4:f9:20:6b:ce:fc:62:99:54:7d:c2:b4:b2:f2:b2 (ECDSA)
|   256 d0:e6:72:18:b5:20:89:75:d5:69:74:ac:cc:b8:3b:9b (ED25519)
3389/tcp  open  ms-wbt-server xrdp
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 54.41 seconds
```

We tried using different script to get more information about the server.

Thought Process / Methodology :

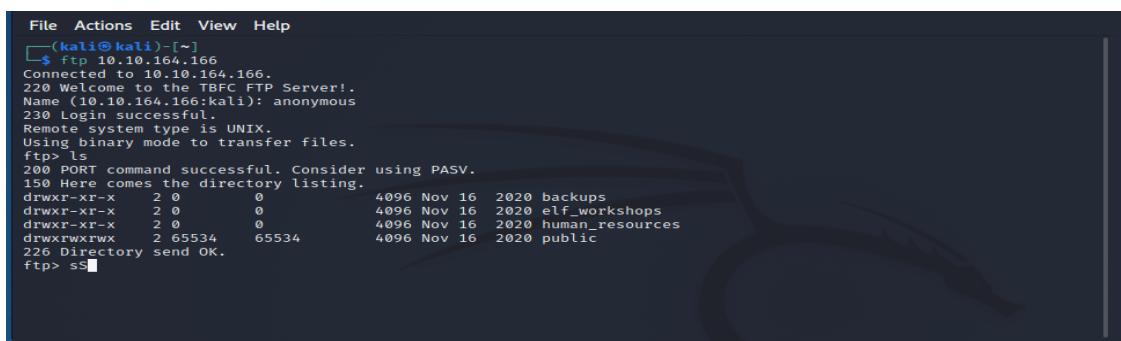
Firstly, we opened the terminal prompt and we used **nmap** to scan the **MACHINE_IP**. We got all the answers by using nmap scan except for the first question. We used **nmap** scan on the **MACHINE_IP** to get the ports number of the three services running. We used **nmap** command **-Pn** to run a scan and provided us the flag to ignore ICMP being used to determine if the host is up or not. After that we experiment with different scan settings such as -A and -Sv whilst comparing the outputs of it. We determine the name of the Linux distribution that is running by using **nmap** too. After that we used **nmap** scan to figure out what the website is used for. Lastly, we tried using different script.

Day 9 : Networking - Anyone can be Santa!

Tool Used : Kali Linux, Firefox

Solution / Walkthrough :

Question 1



```
File Actions Edit View Help
└─(kali㉿kali)-[~]
└─$ ftp 10.10.164.166
Connected to 10.10.164.166.
220 Welcome to the TBFC FTP Server!.
Name (10.10.164.166: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> ss
```

Accessible directory : “Public”

Question 2

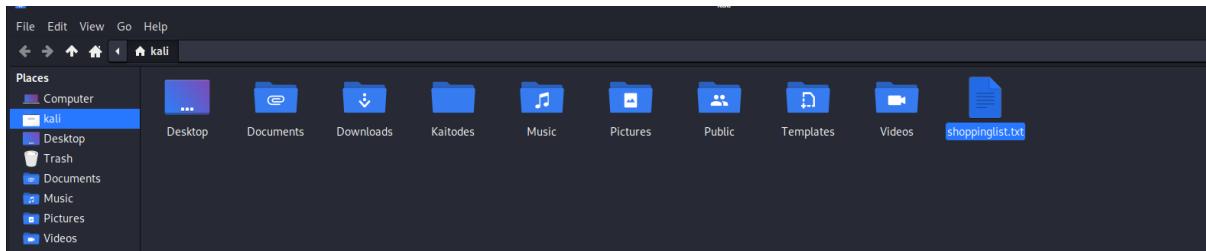
```
File Actions Edit View Help
Name (10.10.164.166:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Nov 16  2020 backups
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> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rxr-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> 
```

Two files were discovered. The file with “.sh” is the script found in the directory.

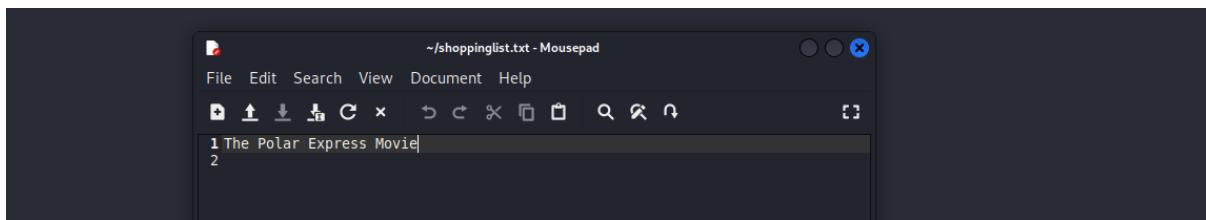
Question 3

```
File Actions Edit View Help
150 Here comes the directory listing.
drwxr-xr-x  2 0      0      4096 Nov 16  2020 backups
drwxr-xr-x  2 0      0      4096 Nov 16  2020 elf_workshops
drwxr-xr-x  2 0      0      4096 Nov 16  2020 human_resources
drwxrwxrwx  2 65534  65534  4096 Nov 16  2020 public
226 Directory send OK.
ftp> cd public
250 Directory successfully changed.
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-rxr-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 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 (6.3776 kB/s)
ftp> 
```

Download the “shoppinglist.txt” .

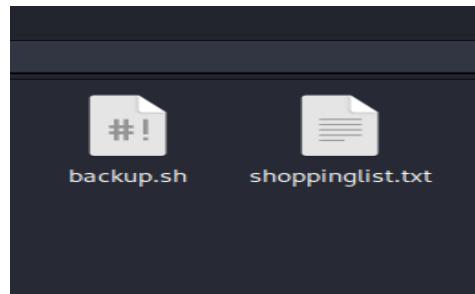


Open the file.

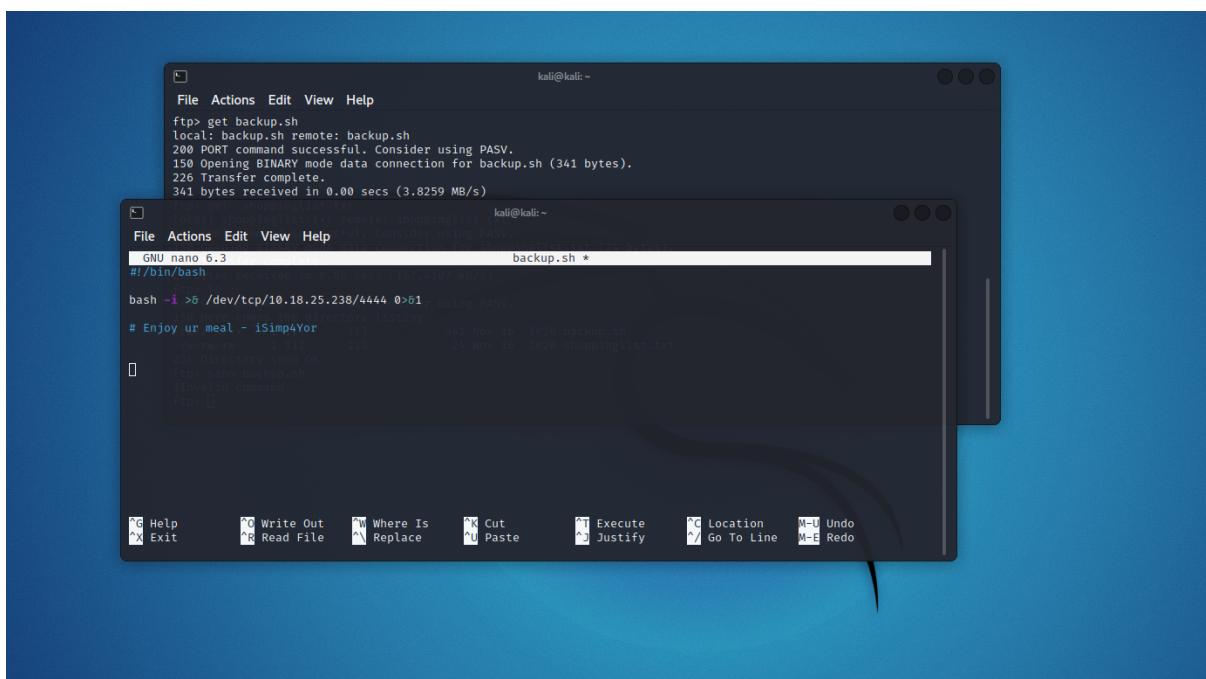
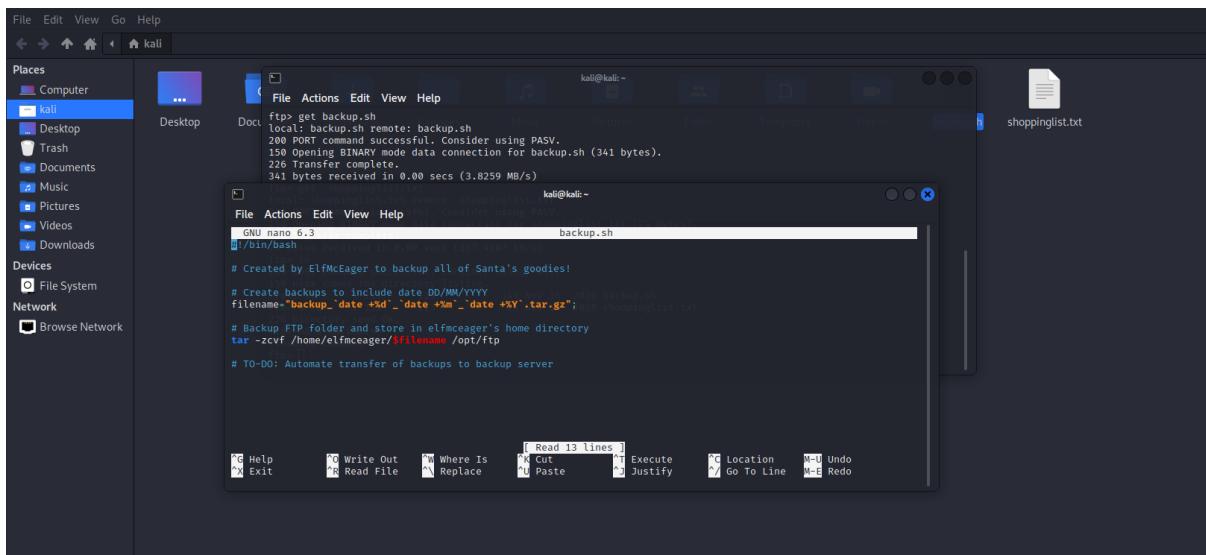


The title is “The Polar Express”

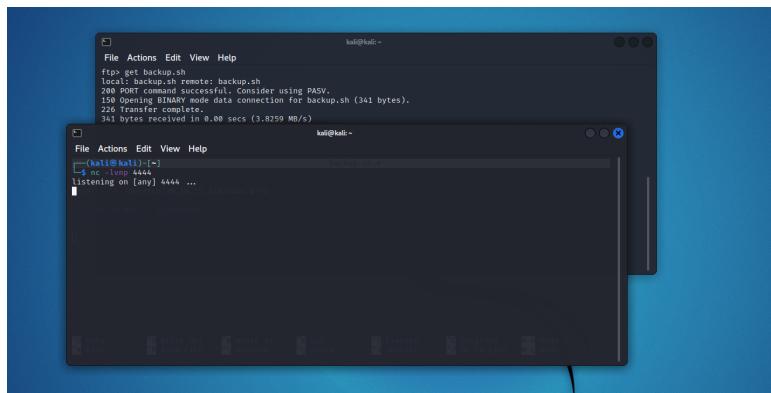
Question 4



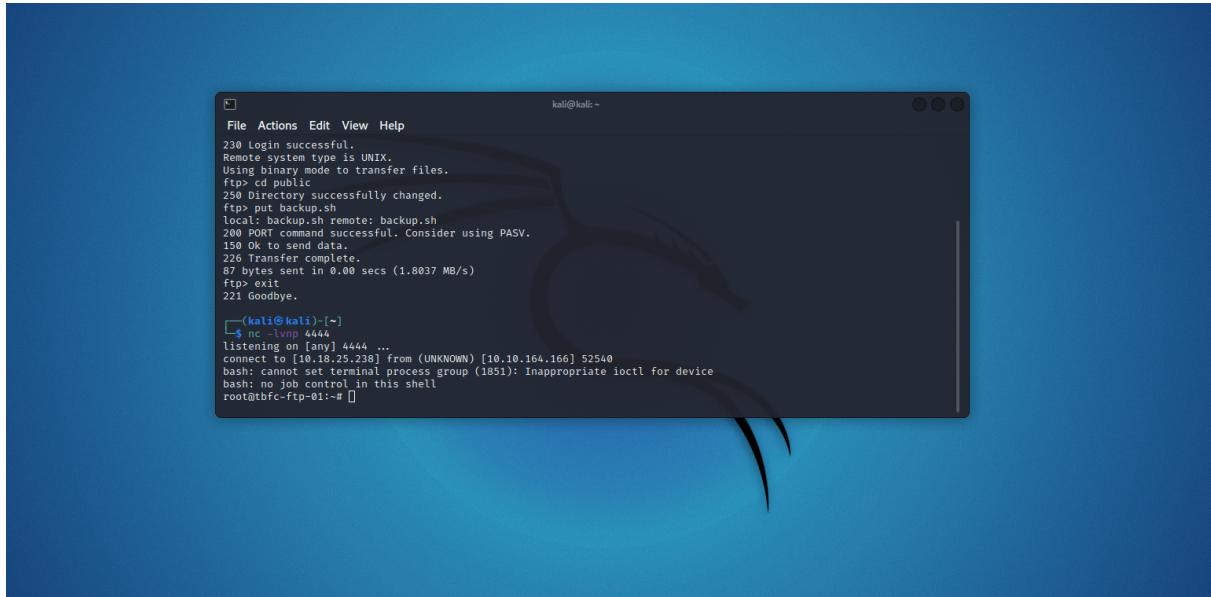
Download the backup.sh using `ftp> get backup.sh`



We change the content of this script to as above and use our own machine IP



Set a netcat listener and listen to any 4444



Send new script with syntax ftp> cd public , ftp> put backup.sh
Exit the ftp and listen to netcat.

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

Enter “cat /root/flag.txt” . Claim the flag.

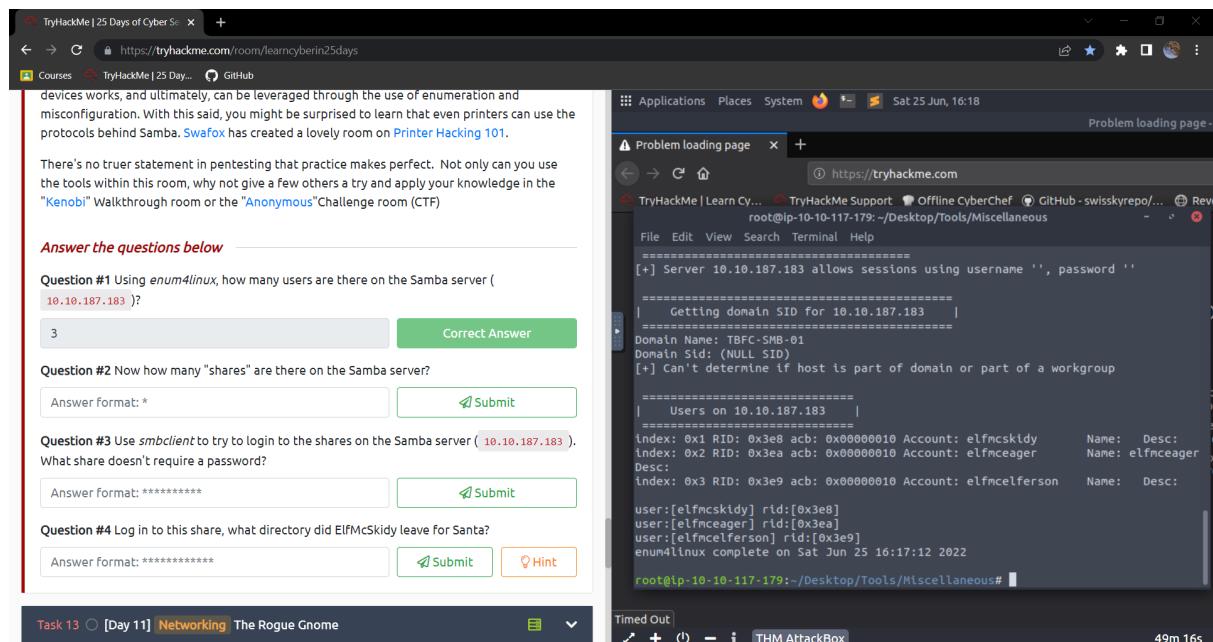
Thought Process / Methodology :

After we open the terminal on Kali Linux, we put the command “ftp” alongside IP that has been given from the THM 25 Days challenge. When asked for a name, we type “anonymous” then we can enter . After that we listed the directories using “ftp> ls” and found an anonymously-accessible directory named “Public” . We changed the directory using the command “ftp> cd public” and relisted what we could find. We found out two files which are “backup.sh” and “shoppinglist.txt” . We download them using the command “ftp> get {files name}” . We opened the shoppinglist.txt file and found a movie named “The Polar Express” . After that, we opened the terminal and type “nano backup.sh” and changed the content to as above. We setted up a netcat listener to listen to 4444 then we sent the new backup.sh to the same public directory using the commands “ftp> cd public” and “ftp> put backup.sh” . After a few minutes, netcat was connected. Lastly, we put the command “cat /root/flag.txt” and were able to claim the flag of THM{even_you_can_be_santa}.

Day 10 : Networking - Don't Be sElfish!

Tool Used : Kali Linux, Firefox, Attackbox
Solution / Walkthrough :

Question 1



The screenshot shows the TryHackMe interface. On the left, there's a challenge room for 'Learn Cyber in 25 days' with several questions about Samba and enum4linux. On the right, a terminal window is open on a Kali Linux machine (IP 10.10.10.117) running enum4linux against a target server (IP 10.10.187.183). The terminal output shows domain SID enumeration and user enumeration results.

```
[+] Server 10.10.187.183 allows sessions using username '', password ''
=====
| Getting domain SID for 10.10.187.183 |
=====
Domain Name: TBFC-SMB-01
Domain SId: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup
=====
| Users on 10.10.187.183 |
=====
Index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name:   Desc:
Index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmcceager    Name:   Desc:
Desc:
Index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson  Name:   Desc:
user:[elfmcskidy] rid:[0x3e8]
user:[elfmcceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Sat Jun 25 16:17:12 2022
root@ip-10-10-117-179:~/Desktop/Tools/Miscellaneous#
```

By using the enum4linux command which is `./enum4linux.pl -U MACHINE_IP`, we are able to get how many users are there on the server.

Question 2

The screenshot shows the TryHackMe interface. On the left, a challenge room titled "Learn Cyber in 25 Days" is displayed. It contains several questions related to enum4linux and smbclient. On the right, a terminal window titled "Problem loading page" is open, showing the output of a smbclient command against a Samba server at 10.10.187.183. The terminal output includes share enumeration and a warning about the deprecated "syslog" option. A "Timed Out" message is visible at the bottom of the terminal window.

By using the enum4linux command which is `./enum4linux.pl -S MACHINE_IP`, we are able to get how many “shares” are there on the server.

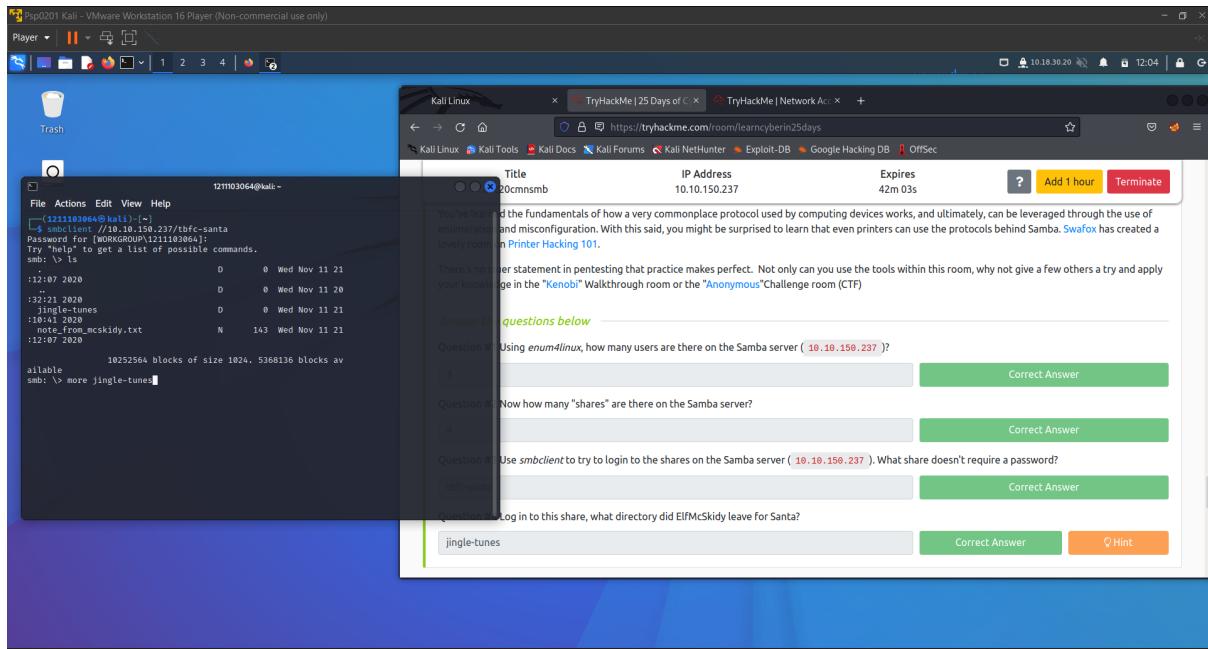
Question 3

The screenshot shows a Kali Linux VM running in a VMware Player window. The terminal window on the left shows the user has run the enum4linux command against the IP 10.10.150.237, resulting in share enumeration. The browser window on the right shows the TryHackMe challenge room for "Learn Cyber in 25 Days". The terminal session is integrated into the challenge room interface, allowing the user to interact with both simultaneously.

We use the smbclient tool which is **smbclient**

//INSTANCE_IP_ADDRESS/sharename**** . We replace the “**sharename**” with the name of the “share” we wish to access. Share that doesn’t require a password is **tbfc-santa** .

Question 4



After log in into the “share” , we do command **ls** to get the list files and directories in the current location. The directory that ElfMcskidy left for Santa is **jingle-tunes**.

Thought Process / Methodology :

We opened the terminal prompt first and then we navigate to **enum4linux**. We run **enum4linux** and lists all the options by using the **./enum4linux.pl** . After that we used command **./enum4linux.pl -U MACHINE-IP** to get the userlist and then we used the command **./enum4linux.pl -S MACHINE_IP** to get the sharelist from the Samba server. We used smbclient tool script which is **smbclient //INSTANCE_IP_ADDRESS/**sharename**** to log in into the correct share that doesn't require a password, we replace sharename with the “share” we wish to access and we just press “enter” when the system asks us for the password. The correct share will let us log in into the account without a password. After logging into the “share” which is **tbfc-santa**, we do command **ls** to get the correct directory which is **jingle-tunes**.

Extra Questions :

Day 6 :

Question 1

Input validation strategies

Input validation should be applied on both **syntactical** and **Semantic** level.

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).

Question 2

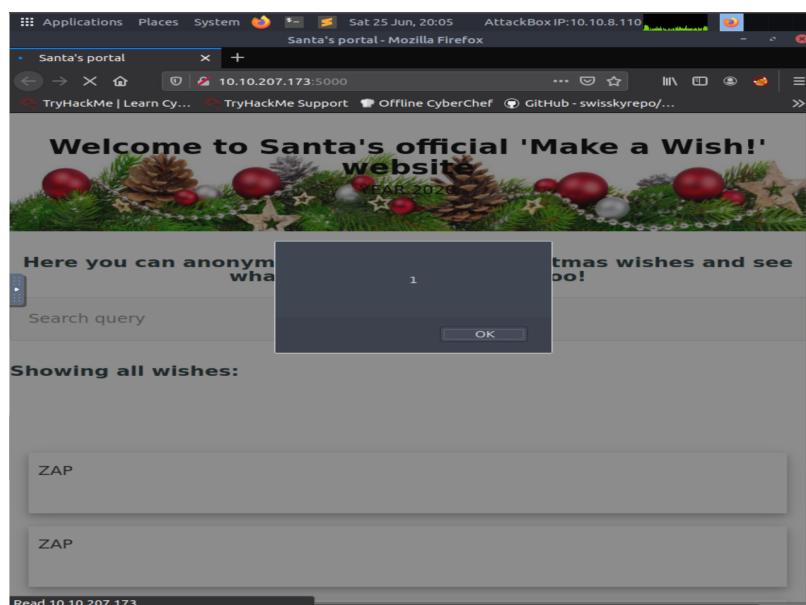
Validating a U.S. Zip Code (5 digits plus optional -4)

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

Question 6

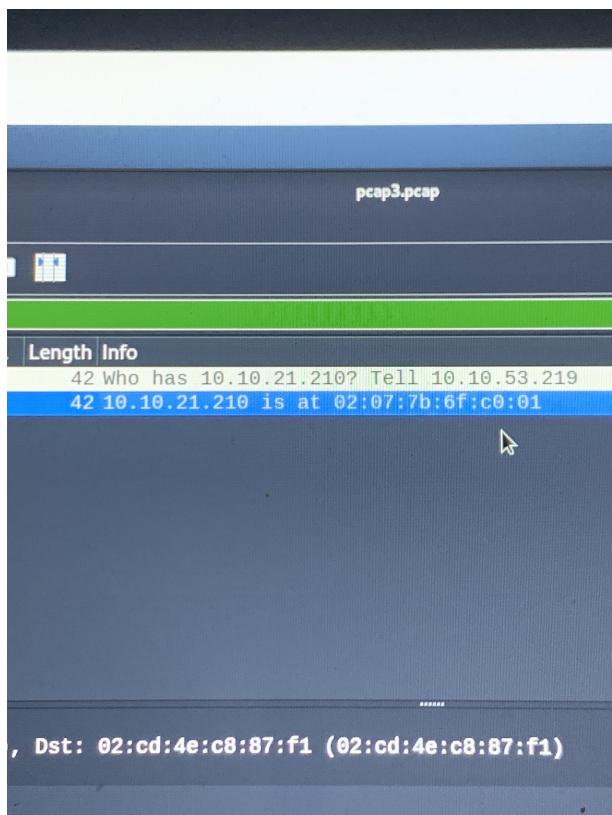
```
10.10.100.27/reflected?keyword=<script>alert(1)</script>
```

Question 7



Day 7 :

Question 6



pcap3.pcap

Length Info

42 Who has 10.10.21.210? Tell 10.10.53.219
42 10.10.21.210 is at 02:07:7b:6f:c0:01

, Dst: 02:cd:4e:c8:87:f1 (02:cd:4e:c8:87:f1)

Question 8

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Day 8 :

Question 4

```
PORT      STATE SERVICE      VERSION
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: Hugo 0.78.2
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: TBFC's Internal Blog
```

Question 5

8.8. Defending against Nmap Scans

The practice of security through obscurity doesn't work here. Whilst it may seem logical to attempt to hide a service by changing its port number to something other than the standard (such as changing SSH from port 22 to 2222), the service will still be fingerprinted during an Nmap scan (albeit slightly later on). Unfortunately, you cannot get the best of both worlds in having a service available yet hidden.

Fortunately, open-source Intrusion Detection (IDS) & Prevention Systems (IPS) such as [Snort](#) and [Suricata](#) allows blue-teamers to protect their networks using network monitoring. For example, you would install these services on firewalls such as [pfSense](#):



Day 10 :

Question 1

```
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 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. 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)
Used to get sid with "lookupsid known_username"
Used 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
```