

PSP0201  
Week 2 write up

Group name: Supreme Chickens

ID	NAME	ROLE
1211103024	Yap Jack	Leader
1211102425	Ang Hui Yee	MEMBER
1211101198	Fam YI Qi	MEMBER
1211103978	Yong Dick Shen	MEMBER

## Day6 [WEB EXPLOITATION] Be careful with what you wish on a Christmas night

### Solutions/Walkthrough

Tools used: Kali Linux, OWASP Zap

Q1 Examine the OWASP Cheat Sheet. Match the input validation level with the correct description.

SOLUTION: Based on the information given in owasp cheat sheet

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?

SOLUTIONS: Based on the information given in owasp cheat sheet

Java Regex Usage Example:

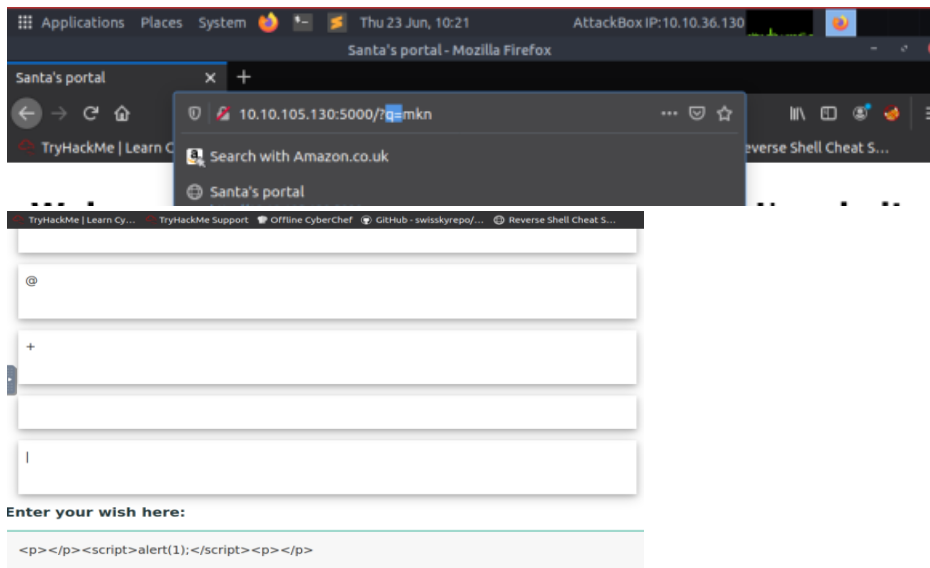
Example validating the parameter "zip" using a regular expression.

```
private static final Pattern zipPattern = Pattern.compile("^\\d{5}(-\\d{4})?$");  
  
public void doPost( HttpServletRequest request, HttpServletResponse response) {
```

Q3 What vulnerability type was used to exploit the application?

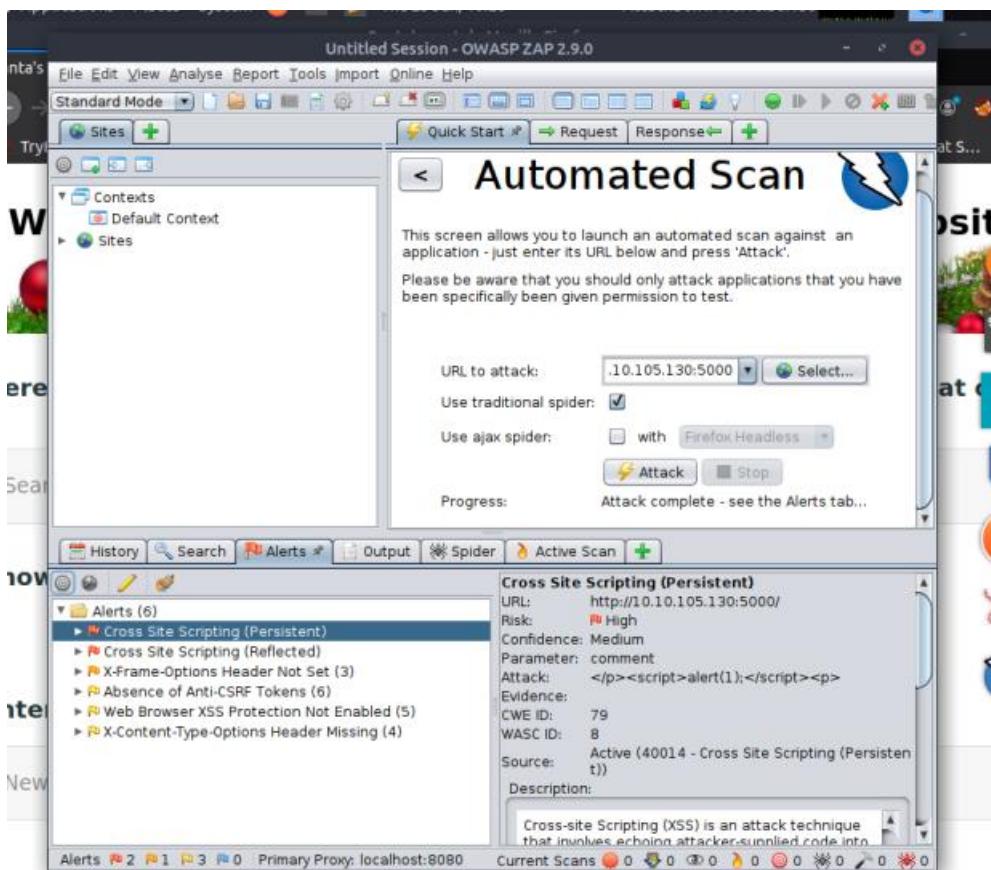
Q4 What query string can be abused to craft a reflected XSS?

SOLUTIONS: We can see from the URL the query string "q" can be abused. The inputs we entered are all showed below which means it is storing the data.



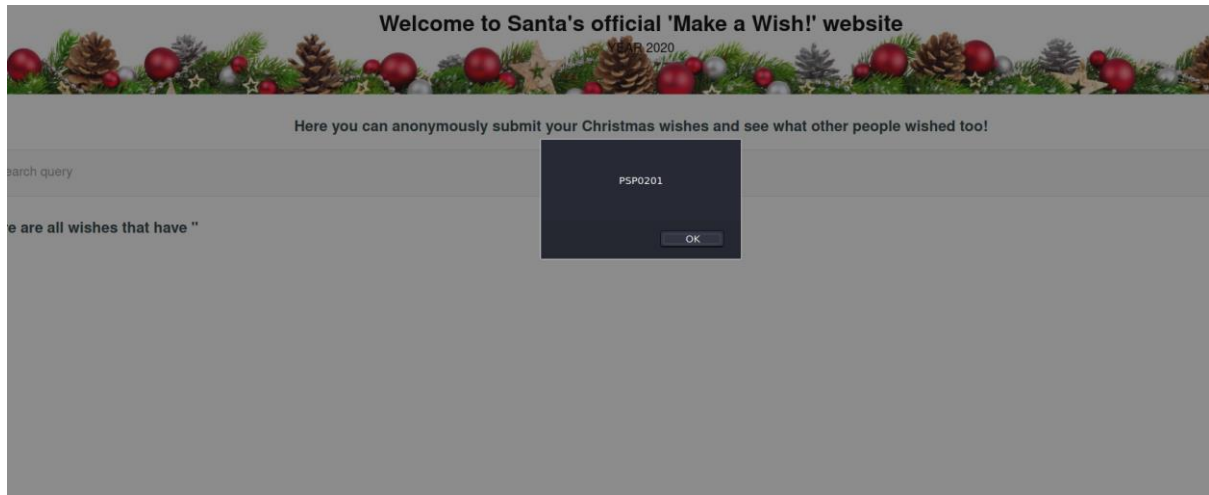
Q5 Run a ZAP(zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan

SOLUTION: I found there's two alerts



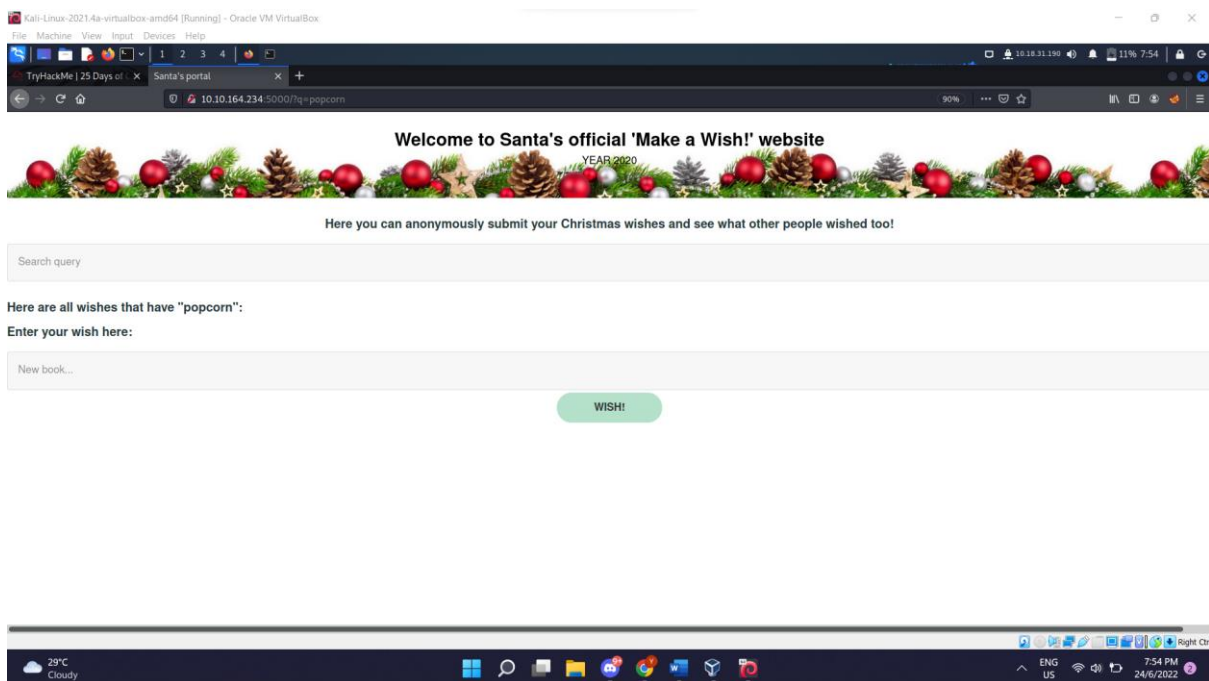
Q6 What JavaScript code should you put in the wish box if you want to show an alert saying “PSP0201”?

SOULTION: using `<script>alert(“PSP0201”)</script>` as the input



Q7 Close your browser and revisit the site MACHINE-IP:5000 again. Does your XSS attack persist?

SOLUTION: No, I reopen my browser but nothing happened.

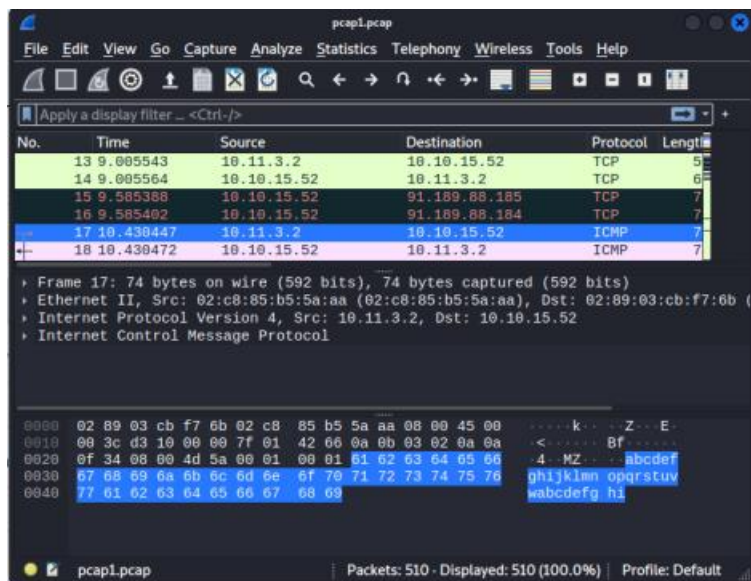


# DAY7- [NETWORKING] The Grinch Really did Steal Christmas

Tools used: Kali Linux, Wireshark

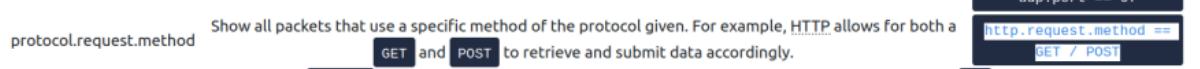
Q1 Open “pcap1.pcap” in Wireshark. What is the IP address that initiates an ICMP/ping?

SOLUTION: Open the file given with Wireshark and search through ICMP/ping, I have found the IP address



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

SOLUTION: Based on the info, we should use `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?

SOLUTION: Using the filter shown below, I was able to get the value

http.request.method == GET && ip.src == 10.10.67.199						
No.	Time	Source	Destination	Protocol	Length	Info
316	63.698177	10.10.67.199	10.10.15.52	HTTP	393	GET /js/instantpage.min.js HTTP/1.1
320	63.701373	10.10.67.199	10.10.15.52	HTTP	398	GET /images/icon.png HTTP/1.1
335	63.987281	10.10.67.199	10.10.15.52	HTTP	387	GET /post/index.json HTTP/1.1
338	63.997588	10.10.67.199	10.10.15.52	HTTP	366	GET /favicon.ico HTTP/1.1
348	64.085368	10.10.67.199	10.10.15.52	HTTP	481	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
462	64.020692	10.10.67.199	10.10.15.52	HTTP	496	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
467	64.028416	10.10.67.199	10.10.15.52	HTTP	466	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
471	64.222360	10.10.67.199	10.10.15.52	HTTP	365	GET /posts/reindeer-of-the-week/ HTTP/1.1

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

SOLUTION: Searching through one by one, I was able to get the password.

No.	Time	Source	Destination	Protocol	Length	Info
19	7.271846	10.10.122.128	91.189.92.49	TCP	74	[TCP Retransmission] 33484 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118196736 TSecr=0
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfmcskidy
21	7.866352	10.10.122.128	10.10.73.252	TCP	66	21 → 45340 [ACK] Seq=39 Ack=18 Win=62720 Len=0 TSval=894818981 TSecr=411833776
22	7.866430	10.10.122.128	10.10.73.252	FTP	100	Response: 331 Please specify the password.
23	7.866878	10.10.73.252	10.10.122.128	TCP	66	45340 → 21 [ACK] Seq=18 Ack=73 Win=62848 Len=0 TSval=411833777 TSecr=894818981
24	9.863853	10.10.122.128	91.189.92.49	TCP	74	33398 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118196736 TSecr=0
25	9.287852	10.10.122.128	91.189.92.49	TCP	74	[TCP Retransmission] 33484 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118196736 TSecr=0
26	11.367850	10.10.122.128	91.189.92.49	TCP	74	[TCP Retransmission] 33482 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118196736 TSecr=0
27	13.415851	10.10.122.128	91.189.92.49	TCP	74	[TCP Retransmission] 33484 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118196736 TSecr=0
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco

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

SOLUTION: Go through one by one, I found the encrypted protocol name

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)
2	0.000904	10.10.122.128	10.11.3.2	TCP	54	57748 → 22 [ACK] Seq=1 Ack=49 Win=1824 Len=0
3	0.060816	10.11.3.2	10.10.122.128	TCP	54	57748 → 22 [ACK] Seq=1 Ack=145 Win=1029 Len=0
4	0.101317	10.11.3.2	10.10.122.128	TCP	74	33486 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118188809 TSecr=0 WS=128
5	1.127866	10.10.122.128	91.189.92.49	TCP	74	33486 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118188809 TSecr=0 WS=128
6	2.548894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
8	2.550981	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [FIN,ACK] Seq=15 Ack=7 Win=0 Len=0 TSval=894813665 TSecr=411828459
9	2.555520	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [ACK] Seq=7 Ack=15 Win=491 Len=0 TSval=411828463 TSecr=894813665
10	2.555529	10.10.73.252	10.10.122.128	TCP	66	45332 → 21 [FIN,ACK] Seq=7 Ack=16 Win=491 Len=0 TSval=411828463 TSecr=894813665
11	2.555534	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [ACK] Seq=16 Ack=8 Win=0 Len=0 TSval=894813678 TSecr=411828463
12	3.175973	10.10.122.128	91.189.92.49	TCP	74	33492 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118196844 TSecr=0 WS=128

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

SOLUTION: After examine the ARP communications slowly, the Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at 02:07:7b:6f:c0:01

No.	Time	Source	Destination	Protocol	Length	Info
157	10.078298	10.11.3.2	10.10.53.219	TCP	54	68319 → 22 [ACK] Seq=2465 Ack=2529 Win=1027 Len=0
158	10.132357	10.11.3.2	10.10.53.219	TCP	54	68319 → 22 [ACK] Seq=2465 Ack=2577 Win=1026 Len=0
159	11.652350	10.11.3.2	10.10.53.219	SSH	102	Client: Encrypted packet (len=48)
160	11.652586	10.10.53.219	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)
161	11.664408	02:cd:4e:c8:87:f1	Broadcast	ARP	42	Who has 10.10.21.210? Tell 10.10.53.219
162	11.664534	MS-NLB-PhysServer-0...	02:cd:4e:c8:87:f1	ARP	42	10.10.21.219 is at 02:07:7b:6f:c0:01

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

Q8: Who is the author of Operation Artic Storm?

SOLUTION: To find his Wishlist, I exported the HTTP object list and found two items which is a Christmas zip and a dictionary. After I opened the zip, I found the Wishlist and info about Operation Artic Storm



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

```

~/.cache/fr-k1FR1e1f_mcskid_y-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 |

```

# Operation Artic Storm



**STRICTLY CONFIDENTIAL**

Author: [Kris Kringle](#)

Revision Number: v2.5

Date of Revision: 14/11/2020

## DAY8 – [NETWORKING] WHAT IS UNDER THE CHRISTMAS TREE?

TOOLS USED: KALI LINUX, NMAP

Q1: When was Snort created?

SOLUTION: According to Google, it is created in 1998

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

SOLUTION: I used the command “nmap IP” to get the result below

```
File Actions Edit View Help
Connect Scan Timing: About 42.76% done; ETC: 10:24 (0:00:20 remaining)
Stats: 0:00:20 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 58.56% done; ETC: 10:24 (0:00:15 remaining)
Stats: 0:00:27 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 82.90% done; ETC: 10:24 (0:00:06 remaining)
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 92.28% done; ETC: 10:24 (0:00:03 remaining)
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 97.65% done; ETC: 10:24 (0:00:01 remaining)
Stats: 0:00:34 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 98.63% done; ETC: 10:24 (0:00:00 remaining)
Stats: 0:00:35 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 10:24 (0:00:00 remaining)
Stats: 0:00:36 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 10:24 (0:00:00 remaining)
Nmap scan report for 10.10.29.221
Host is up (0.29s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNet/IP-1
3389/tcp  open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 36.76 seconds
kali@kali:~$
```

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?

Q4: What is the version of Apache?

SOLUTION: the version of Apache and Ubuntu which is the mostly likely distribution to be running are all shown in the data output.

```
NSE Timing: About 99.66% done; ETC: 11:22 (0:00:00 remaining)
Nmap scan report for 10.10.205.120
Host is up (0.47s latency).
Not shown: 984 closed tcp ports (conn-refused)
PORT      STATE SERVICE
26/tcp    filtered rsftp
80/tcp    open  http
| http-enum:
|   /css/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|   /images/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|   /js/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|   /page/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
|   - /src/: Potentially interesting directory w/ listing on 'apache/2.4.29 (ubuntu)'
| http-internal-ip-disclosure:
```

Q5: What is running on port 2222?

SOLUTION: SSH



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?

SOLUTION: Guessing from the HTTP title, it should be a blog.

```
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
(kali@kali)-[~]
└─$ nmap -sV -sC 10.10.205.120
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-23 11:34 EDT
Stats: 0:00:31 elapsed; 0 hosts completed (1 up), 1 undergoing Connect Scan
Connect Scan Timing: About 99.99% done; ETC: 11:34 (0:00:00 remaining)
Nmap scan report for 10.10.205.120
Host is up (0.21s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT      STATE SERVICE VERSION
80/tcp    open  http      Apache httpd 2.4.29 ((Ubuntu))
|_ http-title: TBFC6839'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)
```

## DAY9 – [NETWORKING] ANYONE CAN BE SANTA

### TOOLS USED: KALI LINUX, FTP

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

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

SOLUTION: Use FTP to connect to the Ip address and login as anonymous. After that use ls command to see the directories.

```
(kali@kali)-[~]
└─$ ftp 10.10.77.28
Connected to 10.10.77.28.
220 Welcome to the TBFC FTP Server!.
Name (10.10.77.28: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.
```

Q3: What script gets executed within this directory?

SOLUTION: The only script within this directory is backup.sh  
meanwhile the other one is a txt.file

```
(kali@kali)-[~] ddress Expires 50m 58s
$ ftp 10.10.199.109
Connected to 10.10.199.109.
220 Welcome to the TBFC FTP Server!.
Name (10.10.199.109: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>
```

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

SOLUTION: After get the txt.file, we can check the information in the file using cat command.

```
(kali@kali)-[~]
$ ls
%2f.html Desktop Downloads Music Pictures santa shell.jpeg.php Templates
christmas.zip Documents hs_err_pid11718.log OP Public shel.jpg.php shoppinglist.txt Videos

(kali@kali)-[~]
$ nano backup.sh

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

(kali@kali)-[~]
$
```

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

SOLUTION: After uploaded the reverse shell , we got our malicious data which is the flag.

```
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.249.124 59828 received!
bash: cannot set terminal process group (1288): Inappropriate ioctl for device
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:~#^C
```

# DAY10 – [NETWORKING] DON'T BE SELFISH

## TOOLS USED: KALILINUX, ENUM4LINUX

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

### SOLUTIONS:

```
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).
-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
```

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

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

SOLUTION: Uses the command `./enum4linux.pl -U` (to list possible users)/`-S` (to list shares) `MACHINE_IP`

```
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy      Name: Desc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager      Name: elfmceager Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson  Name: Desc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Fri Jun 24 10:20:08 2022
```

```

10.10.188.128 41m 10s
Sharename      Type      Comment
-----
tbfc-hr        Disk      tbfc-hr
tbfc-it        Disk      tbfc-it
tbfc-santa     Disk      tbfc-santa
IPC$           IPC       IPC Service (tbfc-smb server (Samba, Ubuntu))
Reconnecting with SMB1 for workgroup listing.

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

```

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

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

SOLUTION: Uses this command to each of the sharename `smbclient //REPLACE_INSTANCE_IP_ADDRESS/**sharename* to login . After that use ls command to check what directory elf leave for Santa.`

```

(kali@kali)-[~/enum4linux]
$ smbclient //10.10.188.128/tbfc-santa
Enter WORKGROUP\kali's password:
Try "help" to get a list of possible commands.
smb: \> help
?
allinfo      altname      archive      backup
blocksize    cancel       case_sensitive cd            chmod
chown        close       del          deltree      dir
du           echo        exit         get          getfacl
geteas       hardlink    help         history      iosize
lcd          link        lock         lowercase    ls
l            mask        md           mget         mkdir
more         mput        newer        notify       open
posix        posix_encrypt posix_open   posix_mkdir  posix_rmdir
posix_unlink posix_whoami print        prompt       put
pwd          queue       quit         readlink     readlink
rd           recurse    reget       rename       reput
rm           rmdir      showacls    setea        setmode
scopy        stat        symlink     tar          tarmode
timeout      translate  unlock      volume       vuid
wdel         logon       listconnect showconnect  tcon
tdis         tid         utimes      logoff       ..
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

```