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

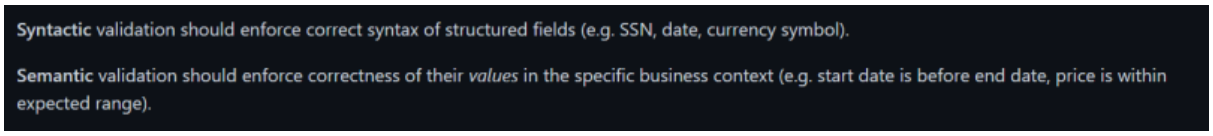
Day6 [WEB EXPLOITATION] Be careful with what you wish on a Christmas night

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



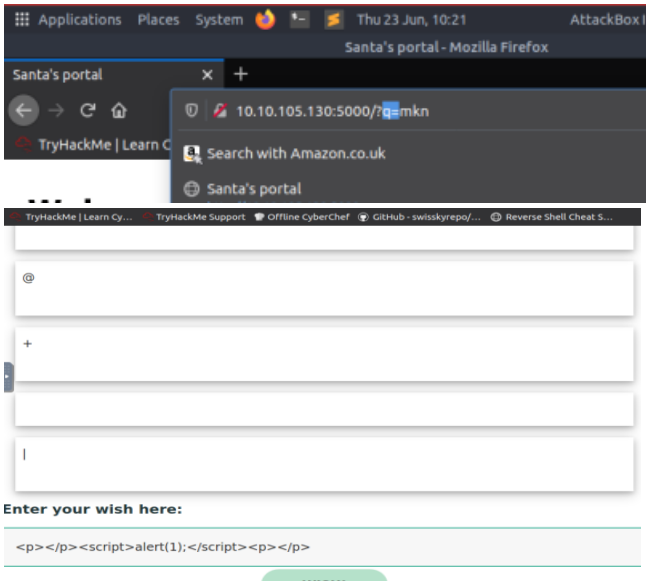
Q2 Examine the OWASP Cheat Sheet. What is the regular expression used to validate a US Zip code?

SOLUTIONS: Based on the information given in owasp cheat sheet

Q3 What vulnerability type was used to exploit the application?

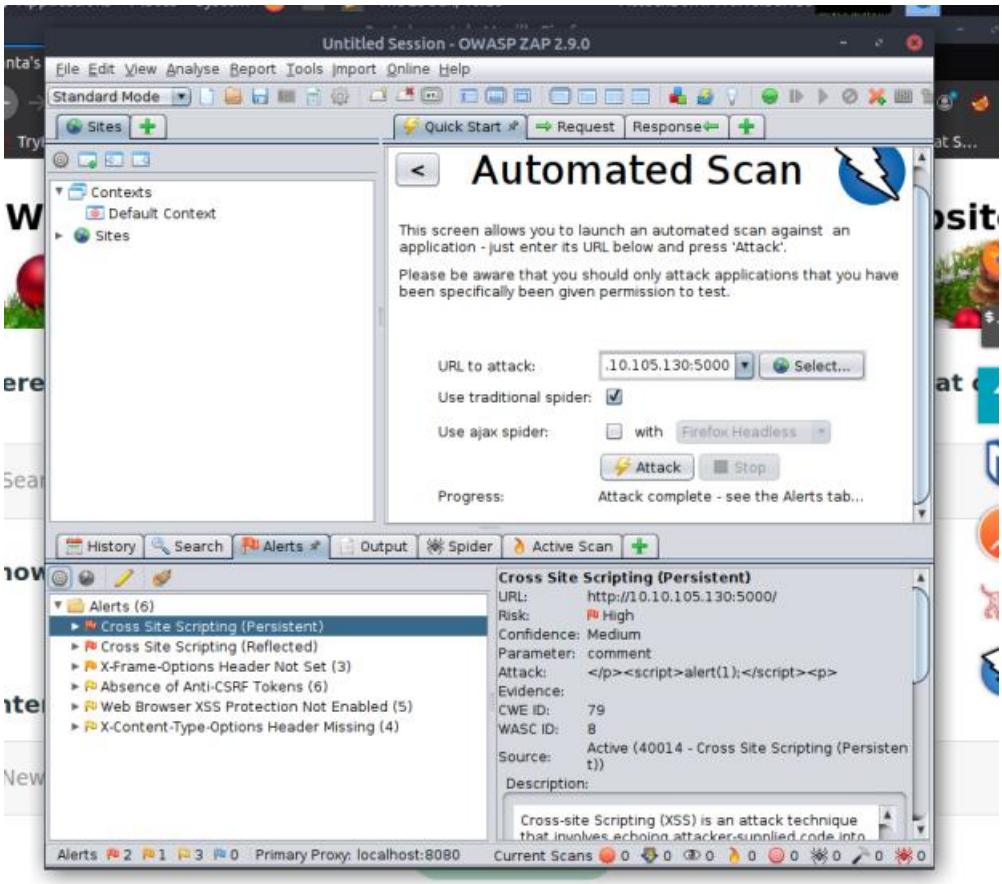
Q4 What query string can be abused to craft a reflected XSS?

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.



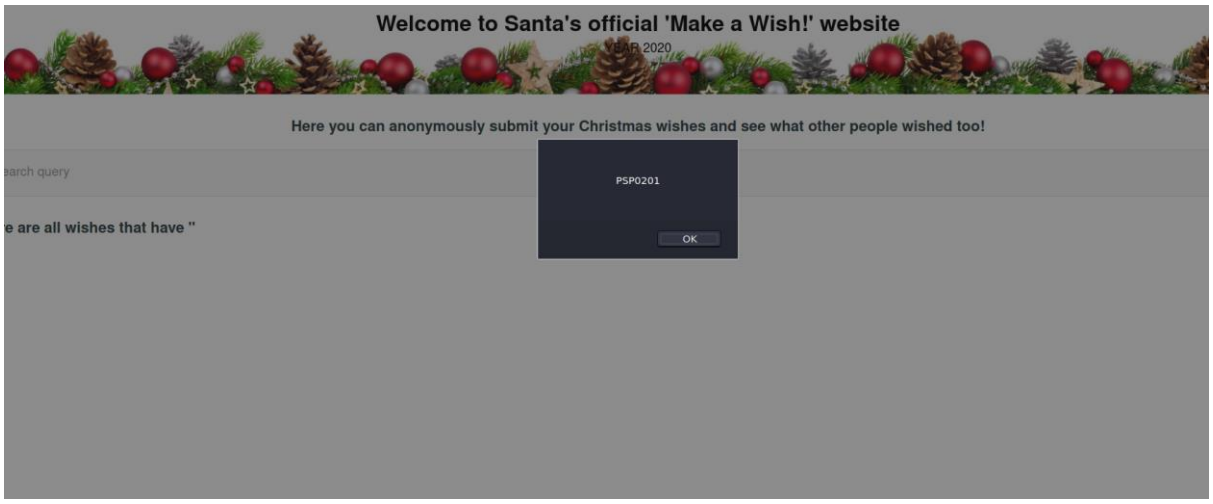
Q5 Run a ZAP(zaproxy) automated scan on the target. How many XSS alerts of high priority are in the scan

SOLUTION: I found there's two alerts



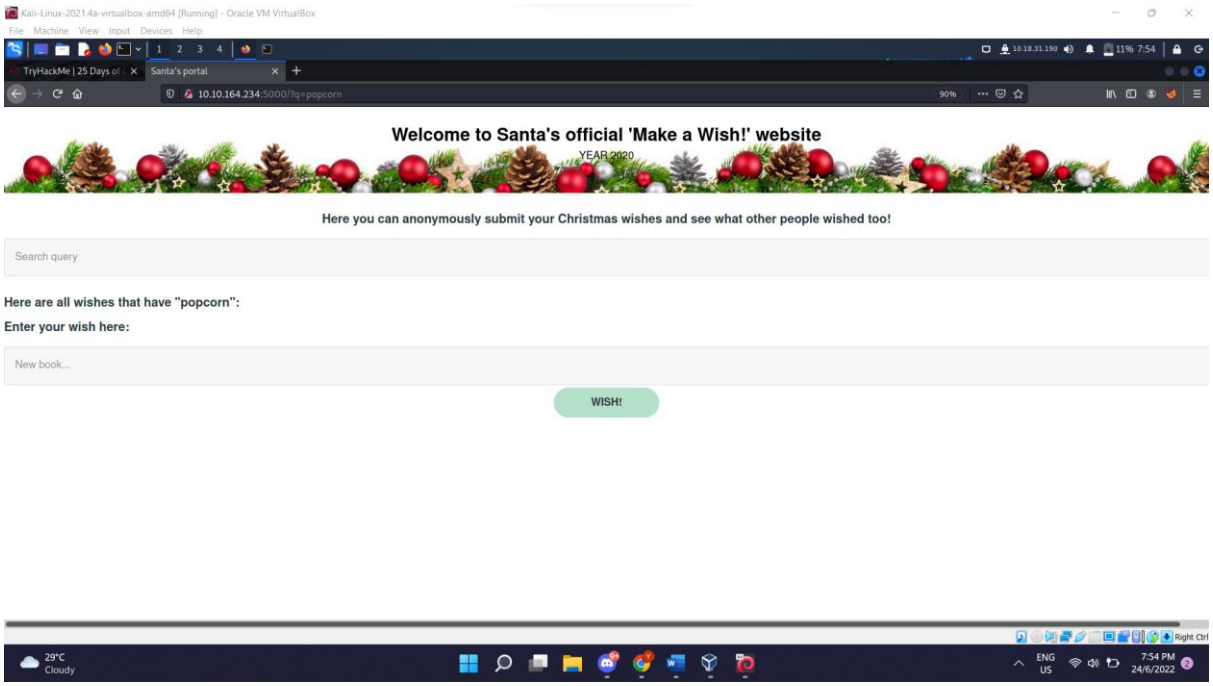
Q6 What JavaScript code should you put in the wish box if you want to show an alert saying “PSP0201”?

SOULUTION: 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.

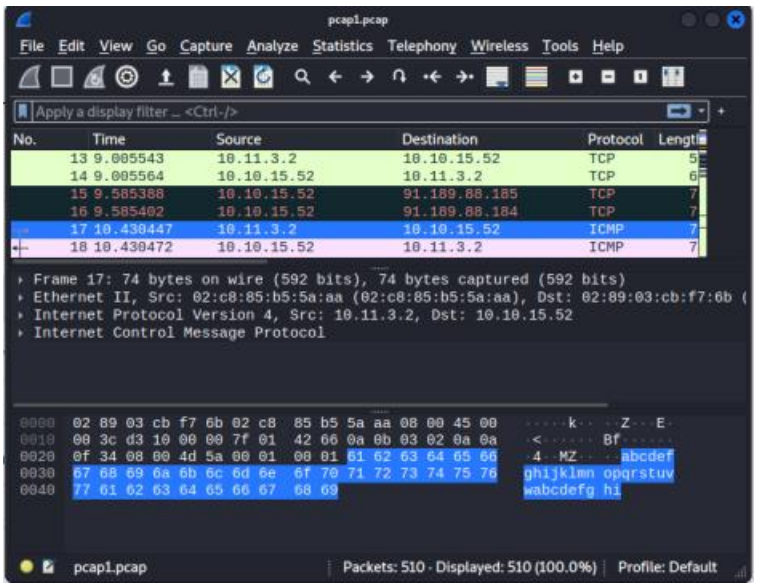


DAY7- [NETWORKING] The Grinch Really did Steal Christmas

Tools used: Kali Linux, Wireshark

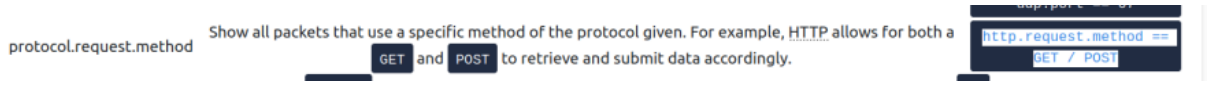
Q1 Open “pcap1.pcap” in Wireshark. What is the IP address that initiates an ICMP/ping?

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



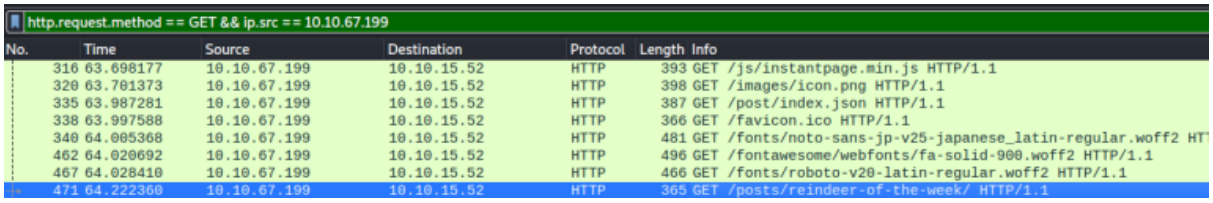
Q2 If we only wanted to see HTTP GET requests in our ‘pcap1.pcap” file, what filter would we use?

SOLUTION: Based on the info, we should use http. request. method == get



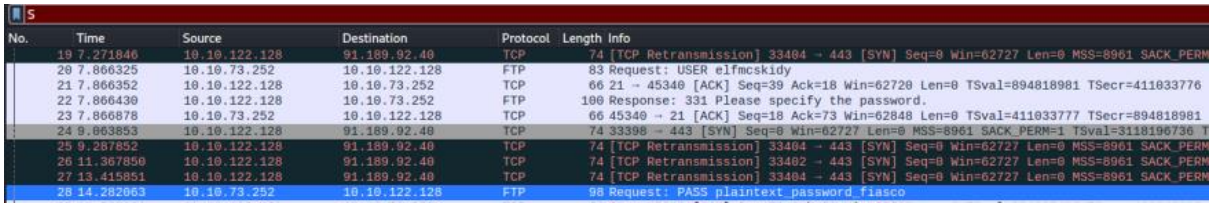
Q3 Now apply this filter to "pcap1.pcap" in Wireshark, what is the name of the article that the IP address "10.10.67.199" visited?

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



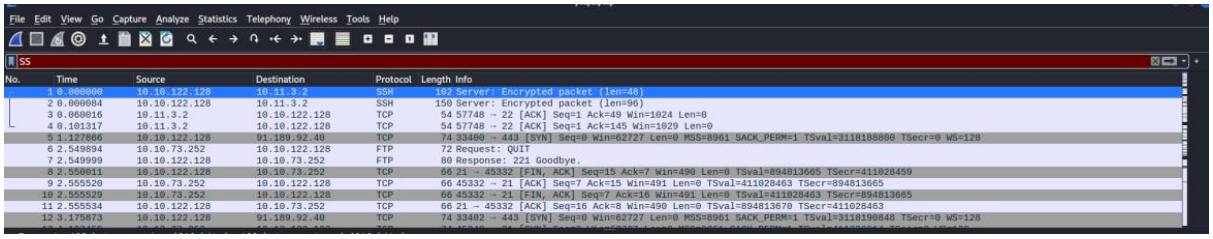
Q4 Let's begin analysing "pcap2.pcap". Look at the captured FTP traffic; what password was leaked during the login process?

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



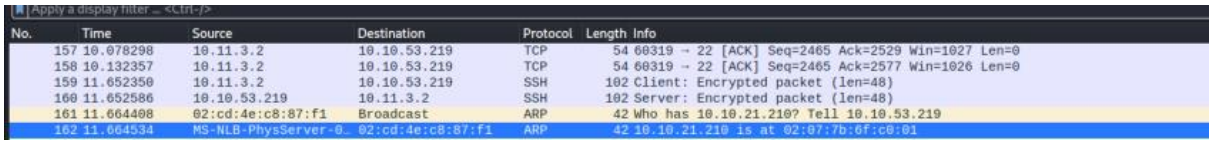
Q5: Continuing with our analysis of "pcap2.pcap", what is the name of the protocol that is encrypted?

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



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

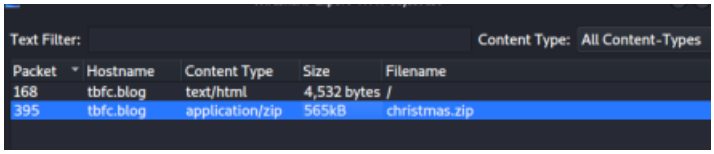
SOLUTION: After examine the ARP communications slowly, the Who has 10.10.122.128? Tell 10.10.10.1. Answer: 10.10.122.128 is at 02:07:7b:6f:c0:01

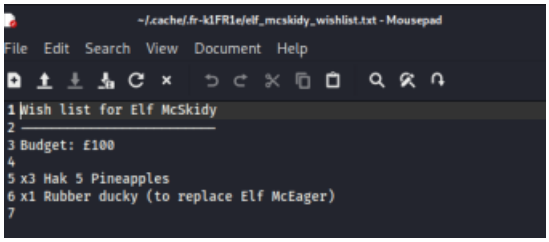


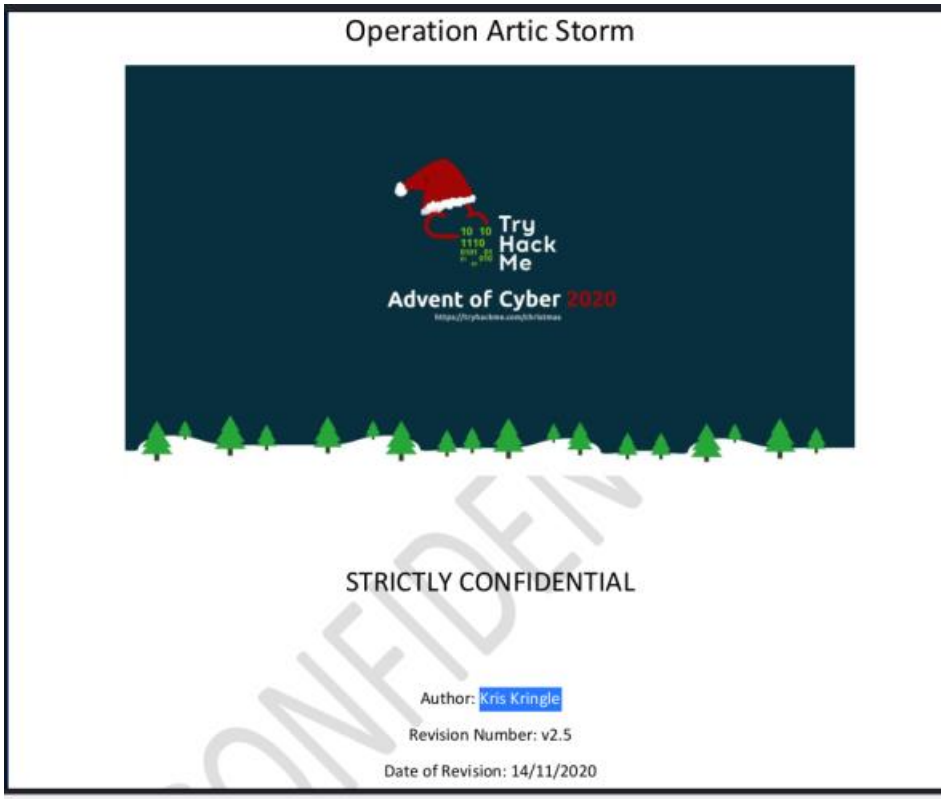
Q7: Analyse "pcap3.pcap" and recover Christmas! What is on Elf McSkidy's Wishlist that will be used to replace Elf McEager?

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-k1FR1e/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


Operation Artic Storm
Try Hack Me
Advent of Cyber 2020
STRICTLY CONFIDENTIAL
Author: Kris Kringle
Revision Number: v2.5
Date of Revision: 14/11/2020

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

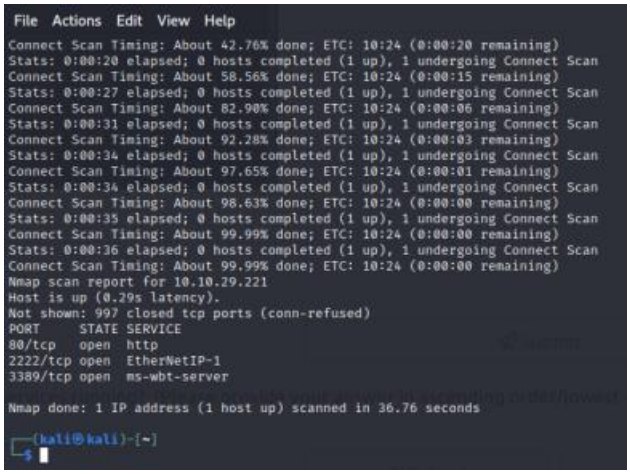
TOOLS USED: KALI LINUX, NMAP

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?

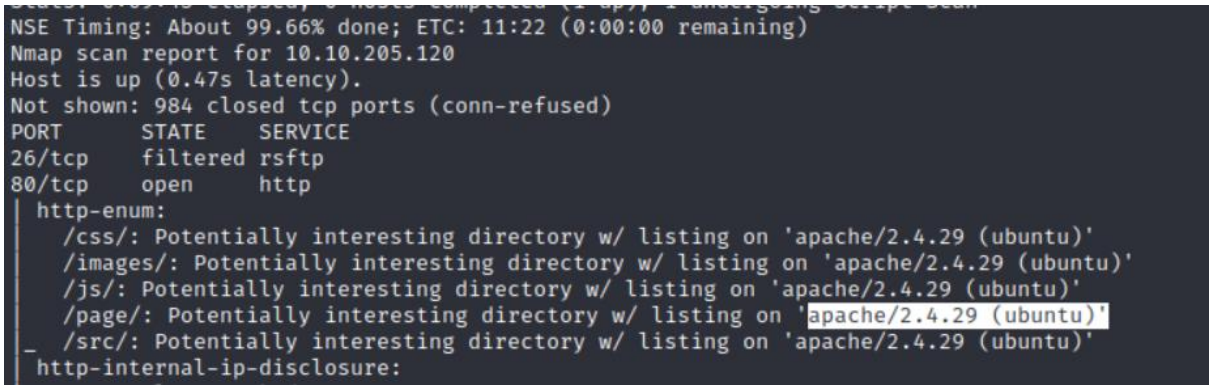
SOLUTION: I used the command “nmap IP” to get the result below



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.

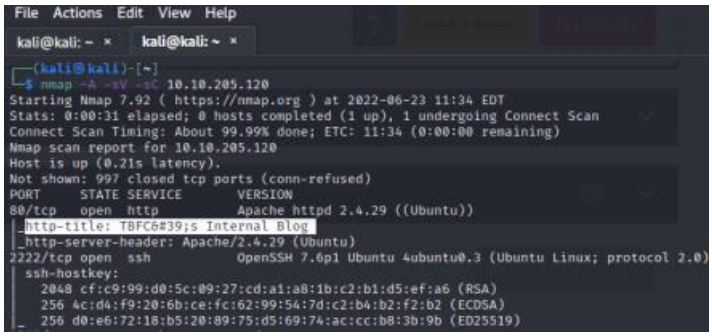


Q5: What is running on port 2222?

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 tittle, it should be a blog.



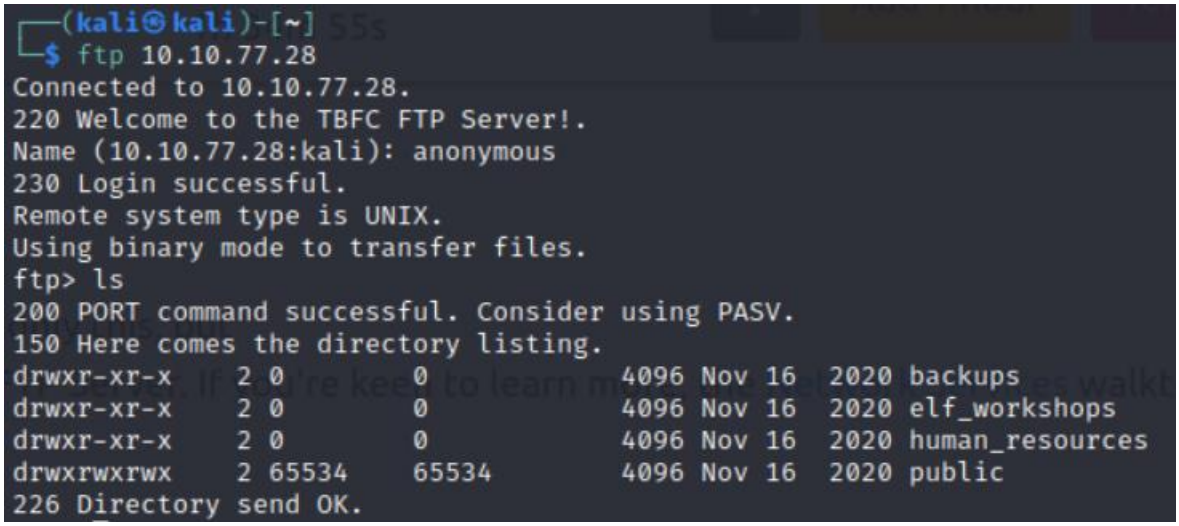
DAY9 – [NETWORKING] ANYONE CAN BE SANTA

TOOLS USED: KALI LINUX, FTP

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

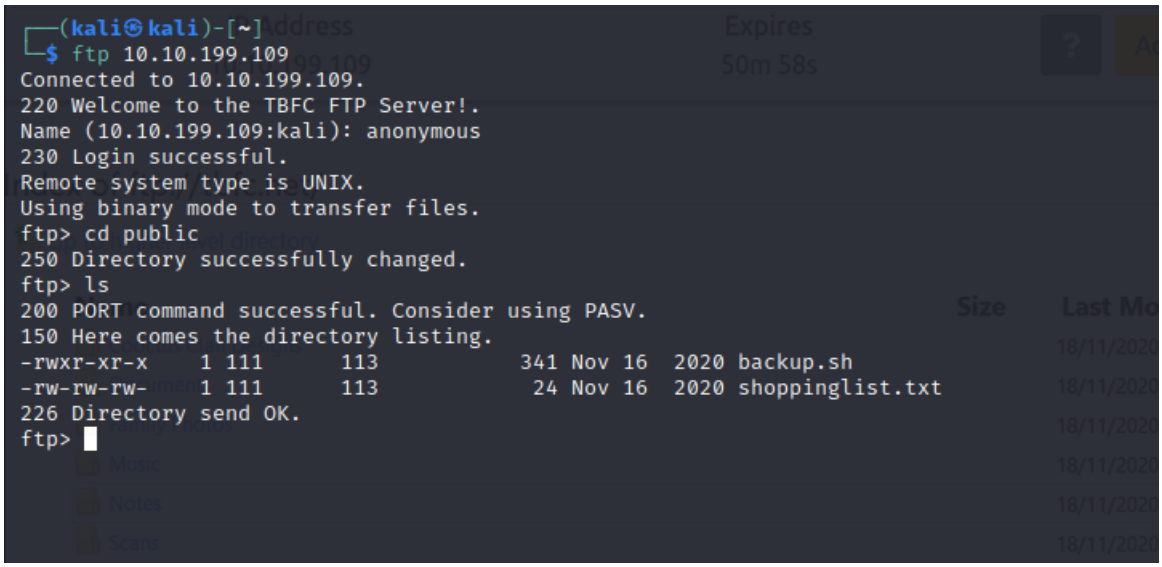
Q2: Name the directory on the FTP server that has data accessible by the "anonymous" user

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



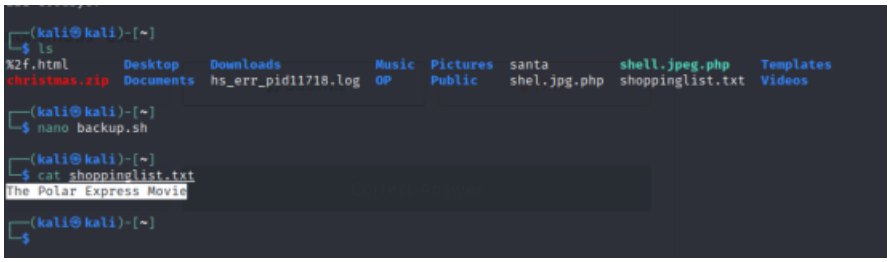
Q3: What script gets executed within this directory?

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



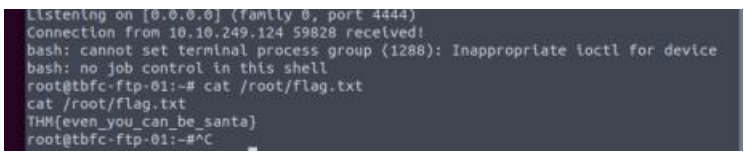
Q4: What movie did Santa have on his Christmas shopping list?

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



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.

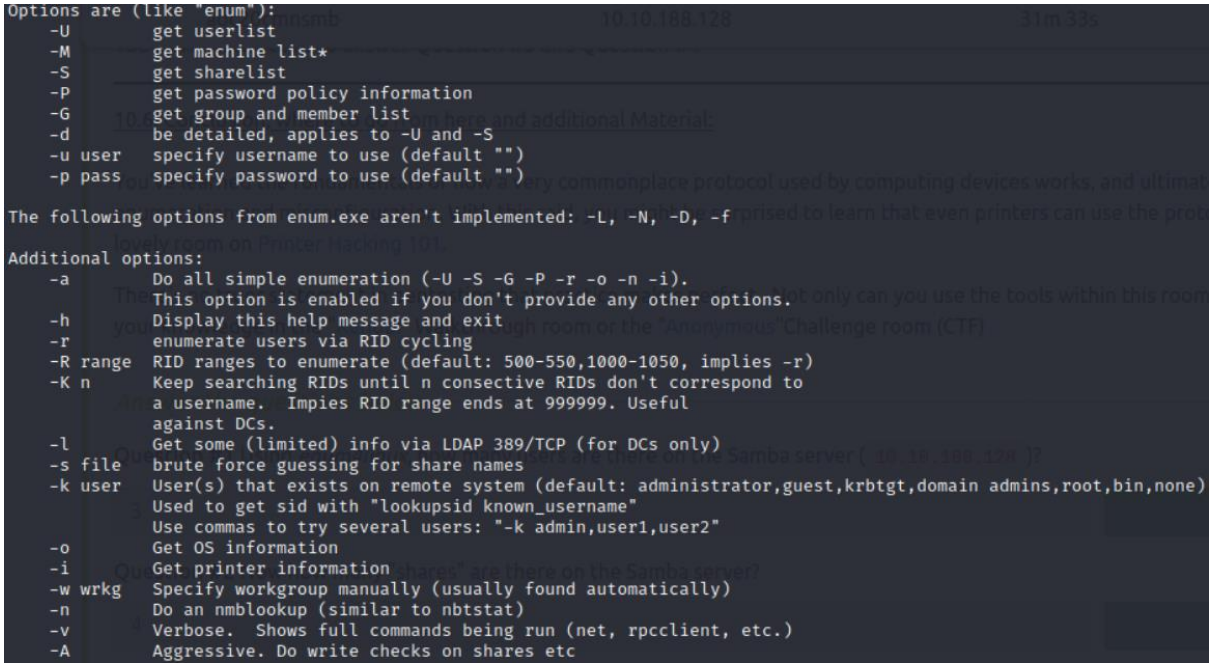


DAY10 – [NETWORKING] DON'T BE SELFISH

TOOLS USED: KALILINUX, ENUM4LINUX

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

SOLUTIONS:

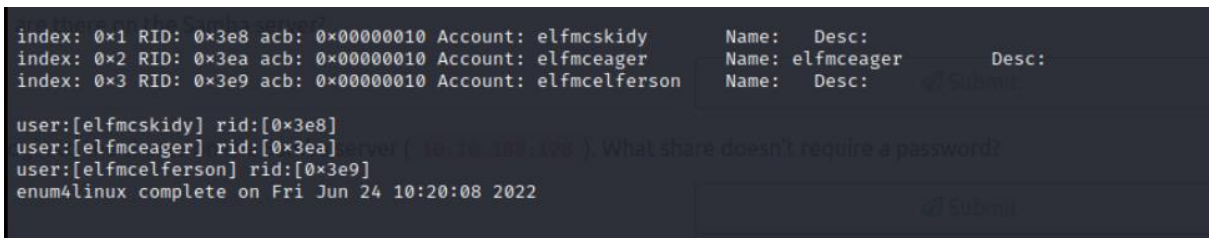


```
Options are (like "enum"):
    -U        get userlist
    -M        get machine list*
    -S        get sharelist
    -P        get password policy information
    -G        get group and member list
    -d        be detailed, applies to -U and -S
    -u user   specify username to use (default "")
    -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).
              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 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.)
    -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.p1 -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
```

```
        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            q              queue          quit           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
```