

DFIAP - FACULDADE DE INFORMÁTICA E ADMINISTRAÇÃO PAULISTA
DEFESA CIBERNÉTICA



PROVAS GS 2023-2
CTF WARGAMES

RAMYREZ GUIMARÃES SANTANA
553022

SÃO PAULO/SP
2023

LISTA DE ILUSTRAÇÕES

Figura 1 - Arquivo Oculto.	4
Figura 2 - Página Inicial.	5
Figura 3- Página Inicial.	6
Figura 4 - DNS	7
Figura 5 - Job Schedule	8
Figura 6 - Reverse e Vida.	9
Figura 7 - User Request.	10
Figura 8 – Hash Base64.	11
Figura 9 – Hash Base32.	12
Figura 10 - Cifra de César.	13
Figura 11 – Wireshark.	14
Figura 12 - Wireshark Windows Error.	15
Figura 13 – Aperi'Solve.	16
Figura 14 - Aperi'Solve Strings.	17
Figura 15 – Cyber Magia Quebrando o Arquivo Zipado.	18
Figura 16 - Cyber Magia Extraíndo o Arquivo Zipado.	19
Figura 17 – Wireshark Test Oculto.	20

SUMÁRIO

1.	INTRODUÇÃO	3
2.	MUNDO LINUX 1.....	4
2.1.	CTF ARQUIVO OCULTO.....	4
3.	MUNDO LINUX 2.....	5
3.1.	CTF PÁGINA INICIAL.....	5
4.	MUNDO LINUX 3.....	7
4.1.	CTF DNS	7
5.	MUNDO LINUX 4.....	8
5.1.	CTF JOB SCHEDULE	8
6.	MUNDO LINUX 5.....	9
6.1.	CTF REVERSE E VIDA.....	9
7.	MUNDO LINUX 6.....	10
7.1.	CTF USER REQUEST	10
8.	DESAFIO NOTA 13	11
8.1.	CTF DESAFIO NOTA 13 	11
9.	SOM DA REDE.....	14
9.1.	CTF SOM DA REDE	14
10.	WINDOWS ERROR.....	15
10.1.	CTF WINDOWS ERROR.....	15
11.	MR. ROBOT	16
11.1.	CTF MR. ROBOT	16
11.2.	CTF MR. ROBOT	17
12.	CYBER MAGIA.....	18
12.1.	CTF CYBER MAGIA	18
13.	TEST OCULTO	20
13.1.	CTF TEST OCULTO	20
	CONCLUSÕES FINAIS.....	21
13.2.	CONCLUSÕES FINAIS	21

1. INTRODUÇÃO

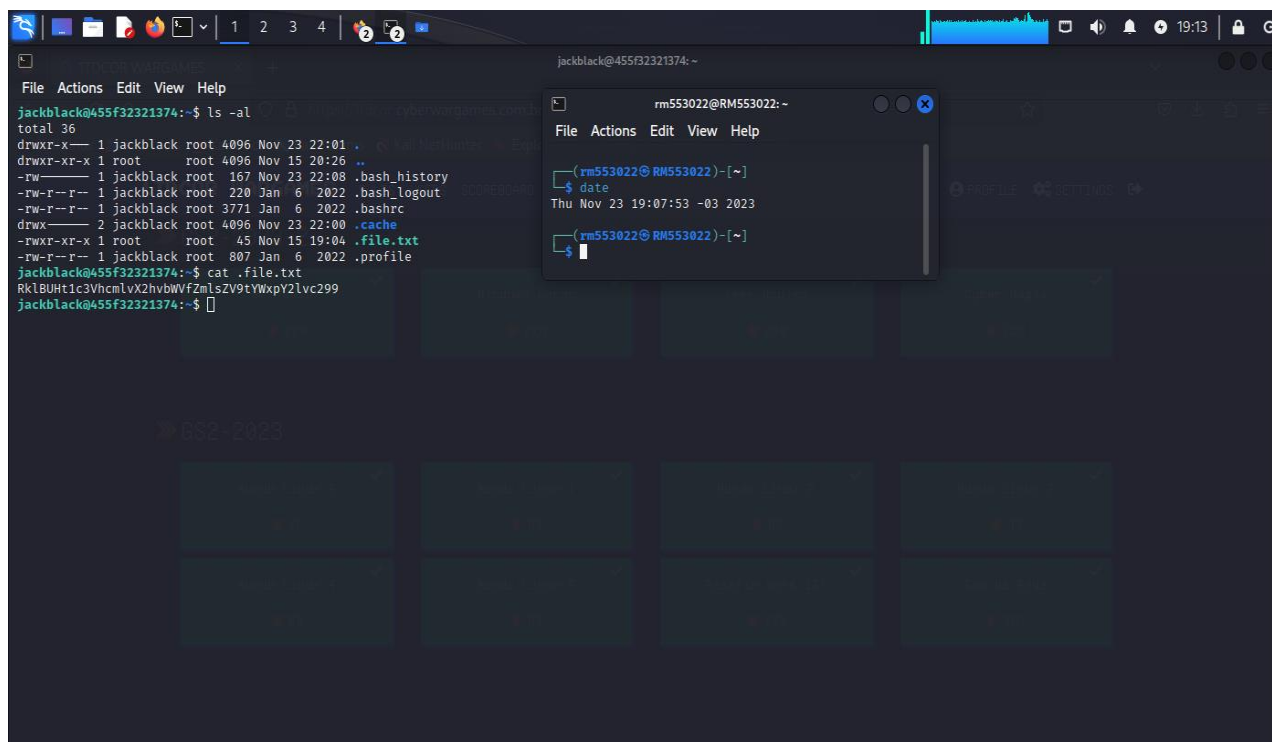
Este relatório tem como objetivo apresentar, com a ajuda de imagens de descrição detalhada, como foram solucionados os CTF'S da prova GS 2023-2.

2. MUNDO LINUX 1

2.1. CTF ARQUIVO OCULTO

Neste CTF, tinha como o objetivo de encontrar o arquivo oculto. Dessa maneira a resposta então foi obtida de forma rápida como podemos ver na imagem a seguir:

Figura 1 - Arquivo Oculto.



Fonte - `ssh jackblack@167.71.17.59 -p 2003`.

Ao localizar o arquivo `file.txt`, foi possível visualizar o Hash Base 64, com isso, utilizando-se da ferramenta Hash Identifier, ao decodar `RklBUHt1c3VhcmlvX2hvbWVfZmlsZV9tYWxpY2lvc299`.

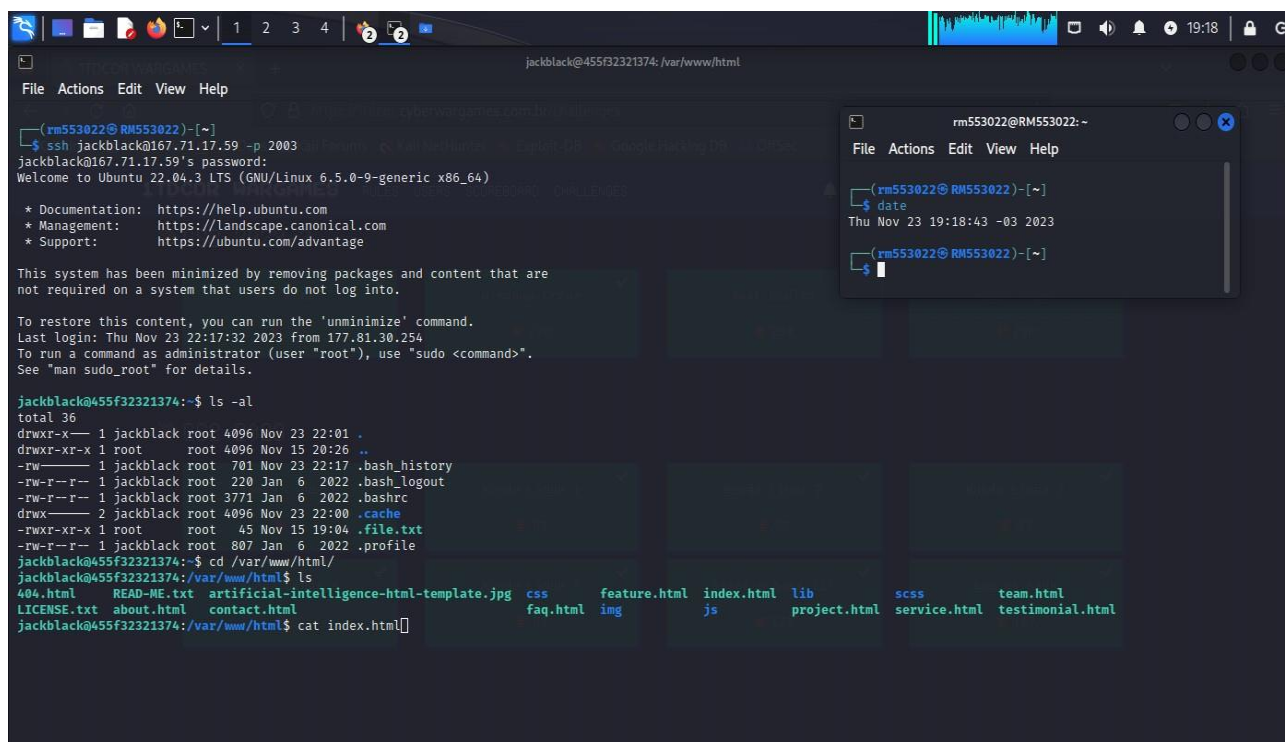
Teve como resposta `FIAP{usuario_home_file_malicioso}`, para o CTF em questão.

3. MUNDO LINUX 2

3.1. CTF PÁGINA INICIAL

Neste CTF, tinha como o objetivo a página inicial. Dessa maneira a resposta então foi obtida de forma rápida como podemos ver nas imagens a seguir:

Figura 2 - Página Inicial.



```
jackblack@455f32321374: /var/www/html
File Actions Edit View Help

(rm553022@RM553022)-[~]
$ ssh jackblack@167.71.17.59 -p 2003
jackblack@167.71.17.59's password:
Welcome to Ubuntu 22.04.3 LTS (GNU/Linux 6.5.0-9-generic x86_64)

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

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

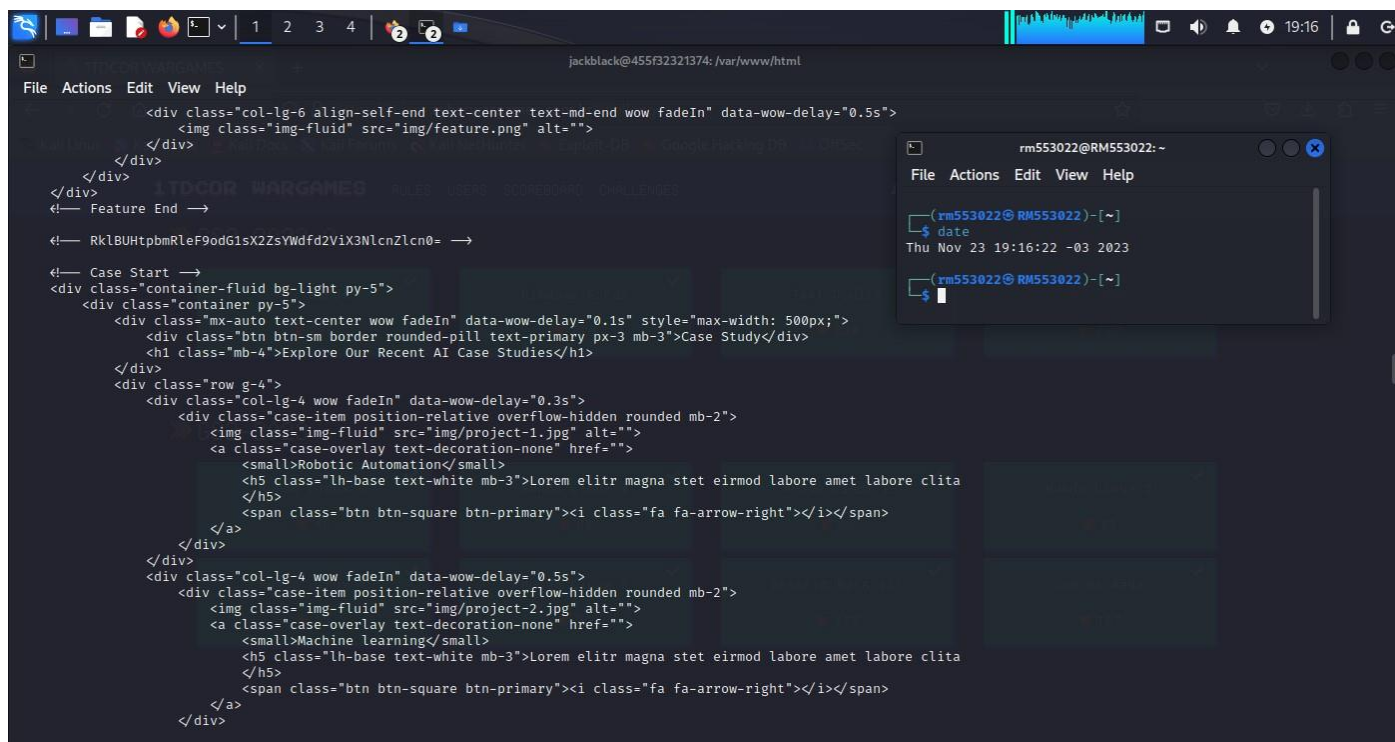
To restore this content, you can run the 'unminimize' command.
Last login: Thu Nov 23 22:17:32 2023 from 177.81.30.254
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jackblack@455f32321374:~$ ls -al
total 36
drwxr-x--- 1 jackblack root 4096 Nov 23 22:01 .
drwxr-xr-x 1 root    root 4096 Nov 15 20:26 ..
-rw----- 1 jackblack root 701 Nov 23 22:17 .bash_history
-rw-r--r-- 1 jackblack root 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 jackblack root 3771 Jan 6 2022 .bashrc
drwx----- 2 jackblack root 4096 Nov 23 22:00 .cache
-rwxr-xr-x 1 root    root 45 Nov 15 19:04 .file.txt
-rw-r--r-- 1 jackblack root 807 Jan 6 2022 .profile
jackblack@455f32321374:~$ cd /var/www/html/
jackblack@455f32321374:/var/www/html$ ls
404.html  README.txt  artificial-intelligence-html-template.jpg  css  feature.html  index.html  lib  scss  team.html
LICENSE.txt  about.html  contact.html  faq.html  img  js  project.html  service.html  testimonial.html
jackblack@455f32321374:/var/www/html$ cat index.html[]
```

Fonte - ssh jackblack@167.71.17.59 -p 2003.

No caminho /var/www/html, localizando-se o index.html, ao executar e analisar foi possível localizar um Hash Base64, conforme a imagem a seguir:

Figura 3 - Página Inicial.



Fonte - ssh jackblack@167.71.17.59 -p 2003.

Decodando o Hash Base64 RklBUHtpbmRleF9odG1sX2ZsYWdfd2ViX3NlcnZlcn0=, foi possível encontrar a seguinte resposta, FIAP{index_html_flag_web_server}.

4. MUNDO LINUX 3

4.1. CTF DNS

Neste CTF, tinha como o objetivo o DNS. Dessa maneira a resposta então foi obtida de forma rápida como podemos ver nas imagens a seguir:

Figura 4 - DNS

```

jackblack@c9f3d394c908:/etc$ ls
PackageKit  cron.d  ethertypes  hosts.allow  libaudit.conf  mke2fs.conf  passwd-  rc2.d  shadow  sysctl.conf
X11         cron.daily  fonts  hosts.deny  localtime  modules-load.d  perl  rc3.d  shadow-shells  sysctl.d
adduser.conf  crontab  fstab  inputrc  logcheck  mtab  php  rc4.d  ssh  systemd
alternatives  dbus-1  gal.conf  init.d  login.defs  netconfig  pm  rc5.d  skel  terminfo
apache2       debconf.conf  group  issue.net  logrotate.d  networkd-dispatcher  polkit-1  rc6.d  ssl  timezone
apt           default  group-gshadow  kernel  lsb-release  networks  profile  rcS.d  subgid  tmpfiles.d
bash.bashrc  deluser.conf  gshadow  ld.so.cache  magic  nsswitch.conf  rmt  resolv.conf  subuid  ucf.conf
bindresvport.blacklist  dhcp  gss  ld.so.conf  machine-id  os-release  rpc  sudo.conf  sudo_logsrvd.conf  ufw
binfmt.d     dpkg  host.conf  ld.so.conf.d  mailcap  pam.conf  security  sudoers  xattr.conf
ca-certificates  e2scrub.conf  hostname  ldap  mime.types  passw  services  sudoers.d  xdg
cloud        environment  hosts  legal
jackblack@c9f3d394c908:/etc$ cat hosts
127.0.0.1    localhost
::1         localhost ip6-localhost ip6-loopback
fe00::0     ip6-localnet
ff00::0     ip6-mcastprefix
ff02::0     ip6-allnodes
ff02::1     ip6-allrouters
127.0.0.2    RklBUHtyZXNvbHZlX2Ruc19saW51eF9kbN9
192.168.176.2  c9f3d394c908
jackblack@c9f3d394c908:/etc$

rm553022@RM553022: ~
File Actions Edit View Help
$ date
Thu Nov 23 19:26:08 -03 2023
$

```

Fonte - ssh jackblack@167.71.17.59 -p 2003.

Verificando o caminho, /etc/hosts:127.0.0.2, ao entrar em hosts, é localizado uma Hash Base64

RklBUHtyZXNvbHZlX2Ruc19saW51eF9kbN9, ao decodar, a seguinte resposta é encontrada, FIAP{resolve_dns_linux_dns}.

5. MUNDO LINUX 4

5.1. CTF JOB SCHEDULE

Neste CTF, tinha como o objetivo o Job Schedule. Dessa maneira a resposta então foi obtida de forma rápida como podemos ver nas imagens a seguir:

Figura 5 - Job Schedule

```

jackblack@c9f3d394c908:/etc$ ls
PackageKit      cron.d          ethertypes      hosts.allow     libaudit.conf   mke2fs.conf     passwd-rc2.d    shadow          sysctl.conf
X11             cron.daily      fonts           hosts.deny      localtime       modules-load.d  perl-rc3.d      shadow-rc3.d    sysctl.d
adduser.conf    cronab          fstab           init.d          logcheck        mtab            php-rc4.d       shells          systemd
alternatives    dbus-1         group          inputrc         login.defs      netconfig       pm-rc5.d        skel            terminfo
apache2         debconf.conf   group-         issue          lsb-release     networkd-dispatcher polkit-1-rc6.d  ssl            timezone
apt             bindresvport.blacklist default        gshadow         ld.so.cache     networks        profile-rc5.d   subuid          tmpfiles.d
binfmt.d        bindresvport.blacklist dhcp           gss             ld.so.conf      nsswitch.conf   rpc            sudo.conf       ucf.conf
ca-certificates dpkg           host.conf       ld.so.conf.d    magic.mime       pam.conf        security-rc5.d  subuid          update-motd.d
ca-certificates.e2scrub.conf environment     ldap             ld.so.conf.d    mailcap          pam.d           selinux        sudoers.d      xattr.conf
cloud           ca-certificates.e2scrub.conf environment     ldap             ld.so.conf.d    mailcap          pam.d           selinux        sudoers.d      xattr.conf
jackblack@c9f3d394c908:/etc$ cat crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
# You can also override PATH, but by default, newer versions inherit it from the environment
#PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .----- minute (0 - 59)
# |----- hour (0 - 23)
# |----- day of month (1 - 31)
# |----- month (1 - 12) OR jan,feb,mar,apr ...
# |----- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# * * * * * user-name command to be executed
17 * * * * root cd / && run-parts --report /etc/cron.hourly
25 6 * * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.daily; }
47 6 * * 7 root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.weekly; }
52 6 1 * * root test -x /usr/sbin/anacron || { cd / && run-parts --report /etc/cron.monthly; }
45 6 1 0 0 root echo RklBUHtqb2Jfc2NoZWZ1bGVfdGFza19saW51eF9mYWNPbH0= > /dev/null
jackblack@c9f3d394c908:/etc$

```

Fonte - ssh jackblack@167.71.17.59 -p 2003.

Rastreando os diretórios, foi possível notar o seguinte caminho /ect/, ls, entrando em group, é onde se encontra o Hash Base64, conforme imagem a seguir:

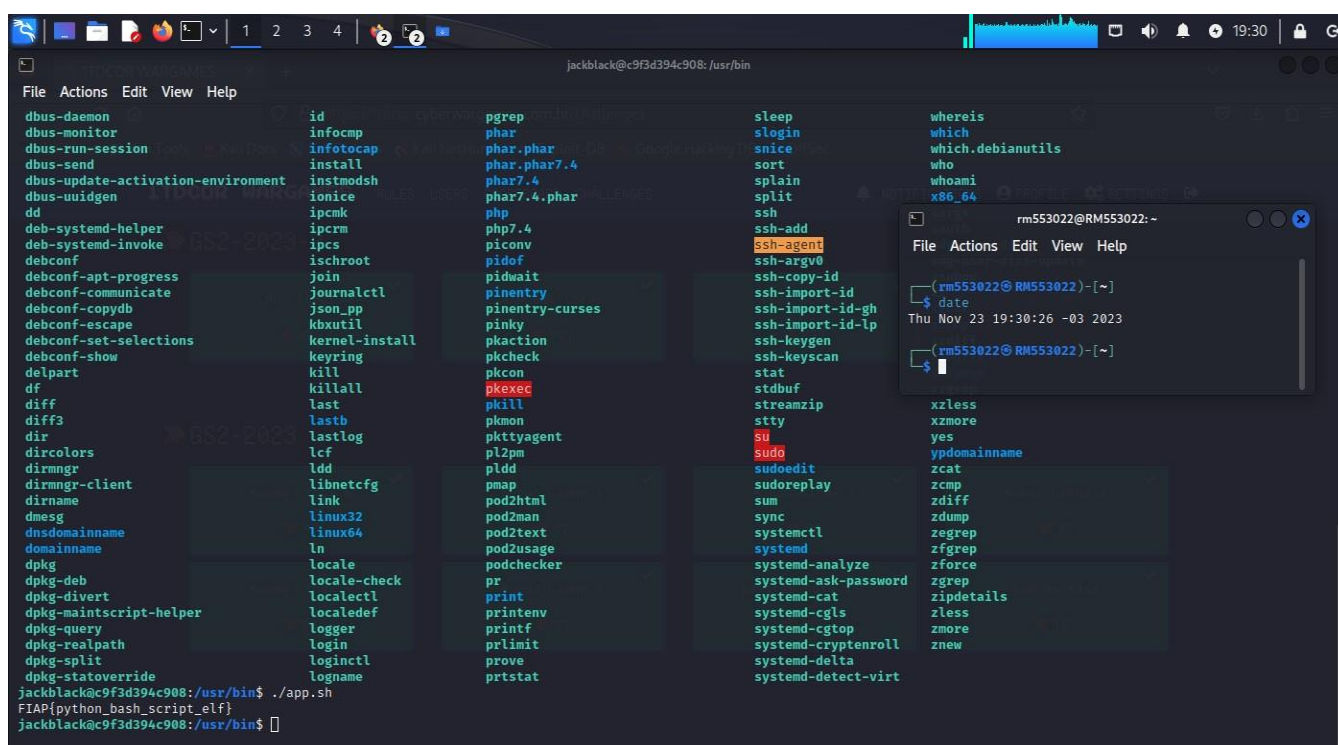
Decodando o Hash RklBUHtqb2Jfc2NoZWZ1bGVfdGFza19saW51eF9mYWNPbH0=, foi possível encontrar a seguinte resposta, FIAP{job_schedule_task_linux_facil}.

6. MUNDO LINUX 5

6.1. CTF REVERSE E VIDA

Neste CTF, tinha como o objetivo o Reverse e Vida. Dessa maneira a resposta então foi obtida de forma rápida como podemos ver nas imagens a seguir:

Figura 6 - Reverse e Vida.



Fonte - ssh jackblack@167.71.17.59 -p 2003.

Rastreando o seguinte caminho `/usr/bin/`, ls, é possível notar que ao executar `app.sh` que é um script em shell, ele trás a seguinte resposta, `FIAP{python_bash_script_elf}`.

7. MUNDO LINUX 6

7.1. CTF USER REQUEST

Neste CTF, tinha como o objetivo o User Request. Dessa maneira a resposta então foi obtida de forma rápida como podemos ver nas imagens a seguir:

Figura 7 - User Request.

```

jackblack@c9f3d394c908: /etc$ cat passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin)/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
_apt:x:100:65534::/nonexistent:/usr/sbin/nologin
systemd-network:x:101:102:systemd Network Management,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:102:103:systemd Resolver,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:104::/nonexistent:/usr/sbin/nologin
systemd-timesync:x:104:105:systemd Time Synchronization,,:/run/systemd:/usr/sbin/nologin
sshd:x:105:65534::/run/sshd:/usr/sbin/nologin
jackblack:x:1000:0:/home/ubuntu:/bin/bash
RklBUHtsaW51eF9yb290X3NoYWVvd259:x:1001:999::/home/ubuntu:/bin/bash
jackblack@c9f3d394c908: /etc$

rm553022@RM553022: ~$ date
Thu Nov 23 19:33:08 -03 2023

```

Fonte - ssh jackblack@167.71.17.59 -p 2003.

Rastreando o seguinte caminho, etc/, ls, é possível notar que o arquivo group, contém informações, ao entrar nele, ele traz um Hash Base64.

Decodando o Hash RklBUHtsaW51eF9yb290X3NoYWVvd259, foi possível encontrar a seguinte resposta, FIAP{linux_root_shadown}.

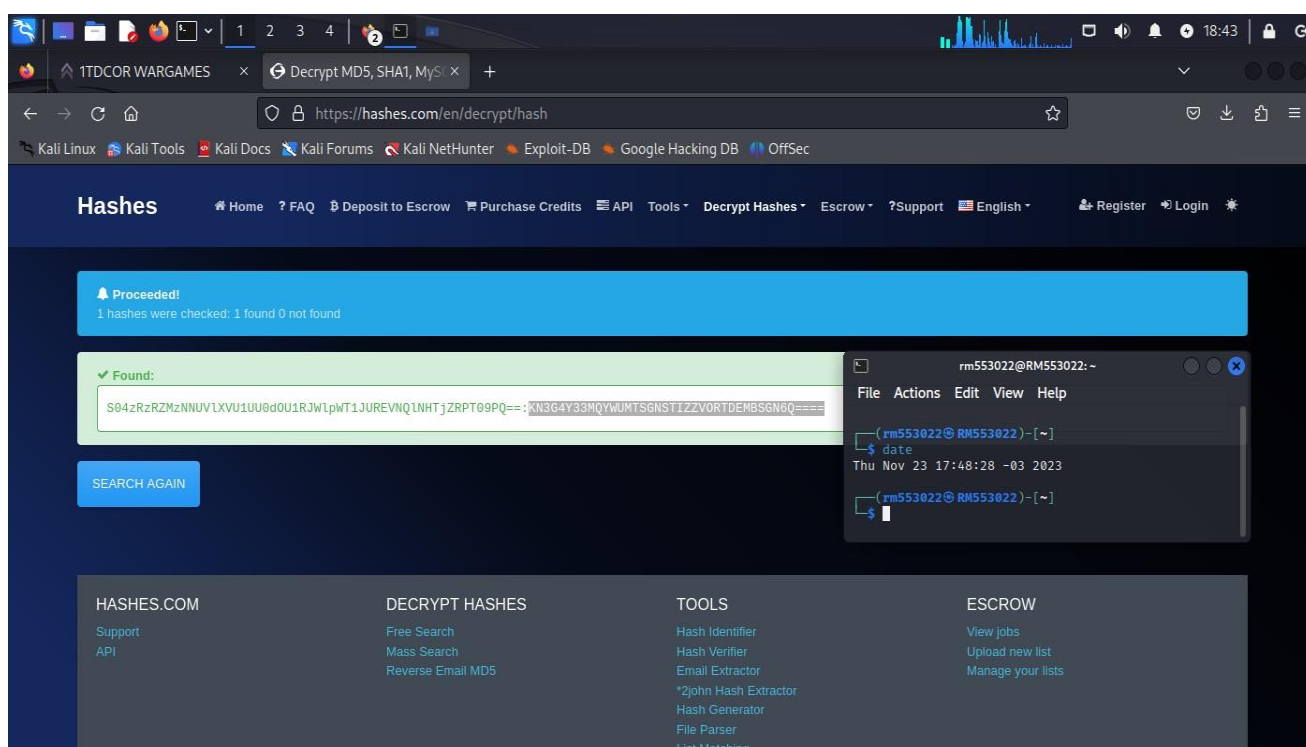
8. DESAFIO NOTA 13

8.1. CTF DESAFIO NOTA 13|

Neste CTF, tem como objetivo de desvendar o código malicioso da máquina monitorada pelo time de Cyber, código encontrado. S04zRzRZMzNNUVIXVU1UU0dOU1RJWlpWT1JUREVNQINHTjZRPT09PQ==

Dessa maneira, com o arquivo de log disponível para análise, a resposta então foi obtida de forma rápida como podemos ver na imagem a seguir:

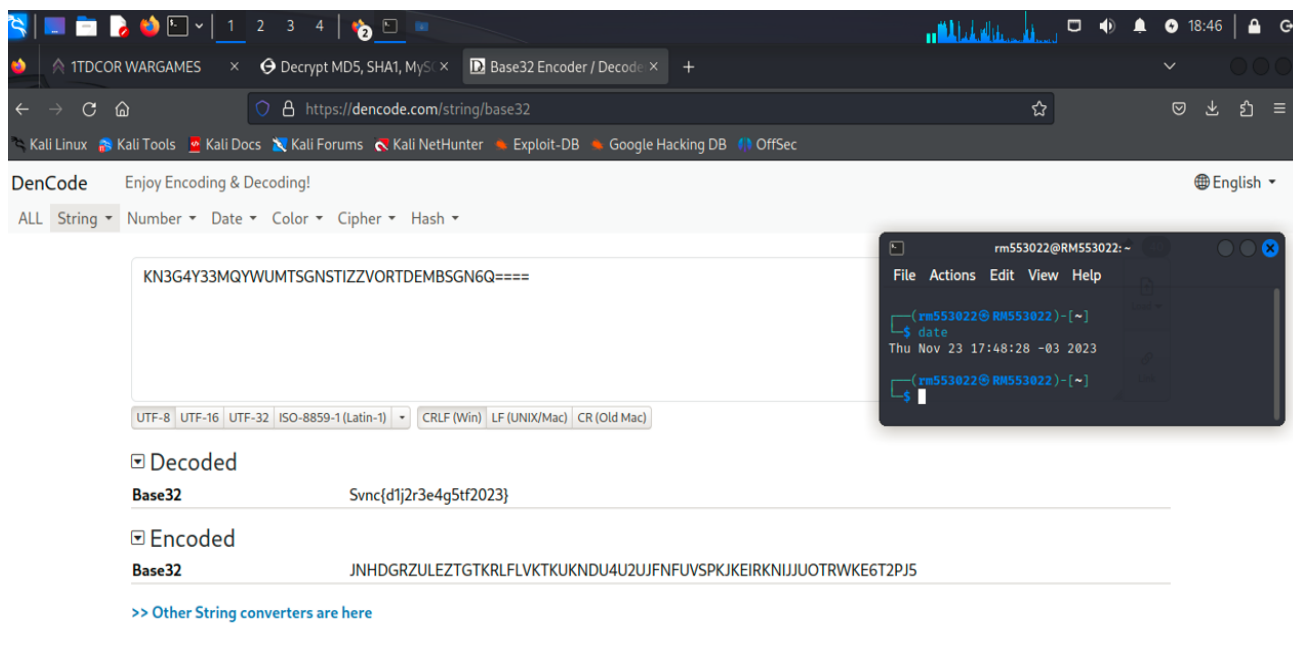
Figura 8 – Hash Base64.



Fonte - Hash Type Identifier.

É possível notar que se trata de um Hash Base64, ao decodar ele trás um Hash Base 32, então, o código malicioso, está camuflado em 3 camadas diferentes, como será possível ver na imagem a seguir:

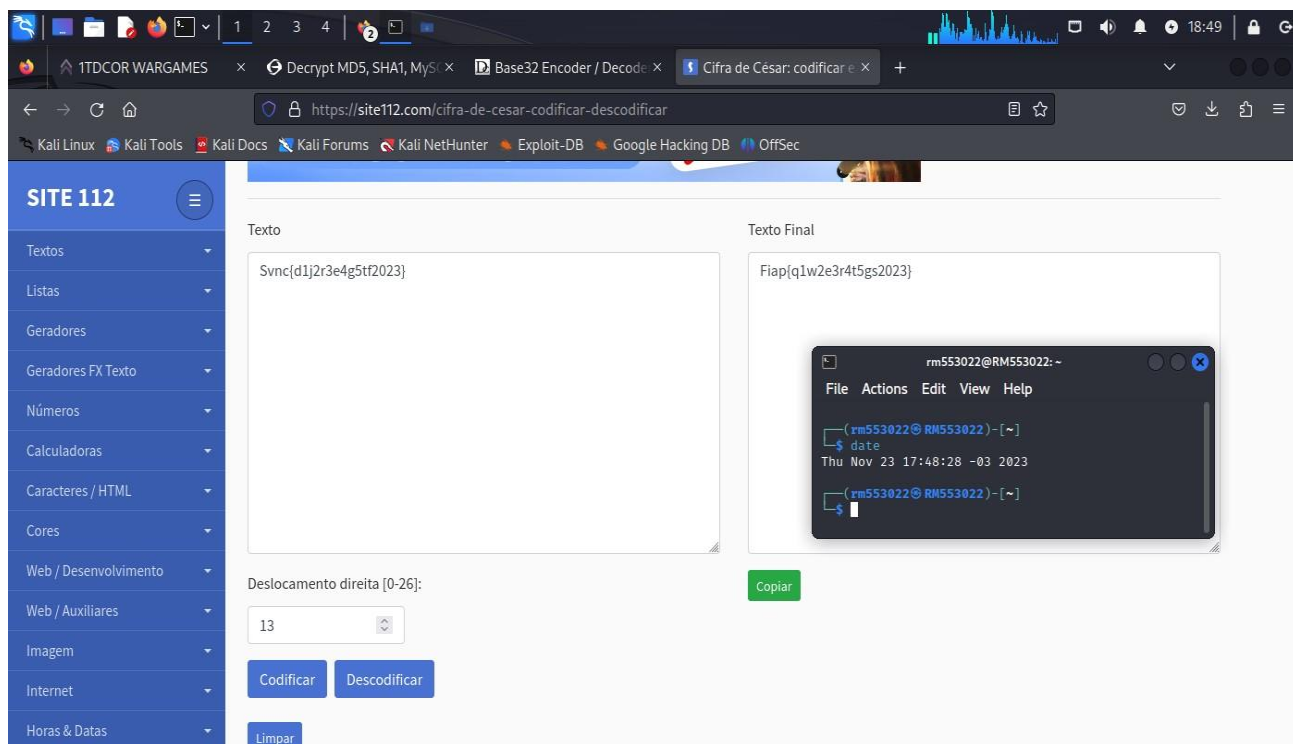
Figura 9 – Hash Base32.



Fonte – Dencode.

Agora é possível notar, que se trata de uma Cifra de César, então será necessário, também decodificar, para se chegar ao resultado.

Figura 10 - Cifra de César.



Fonte – Site 112.

Após passar por essas 3 camadas de decodificar, foi possível chegar ao resultado do CTF e a resposta obtida foi a seguinte, FIAP{q1w2e3r4t5gs2023}.

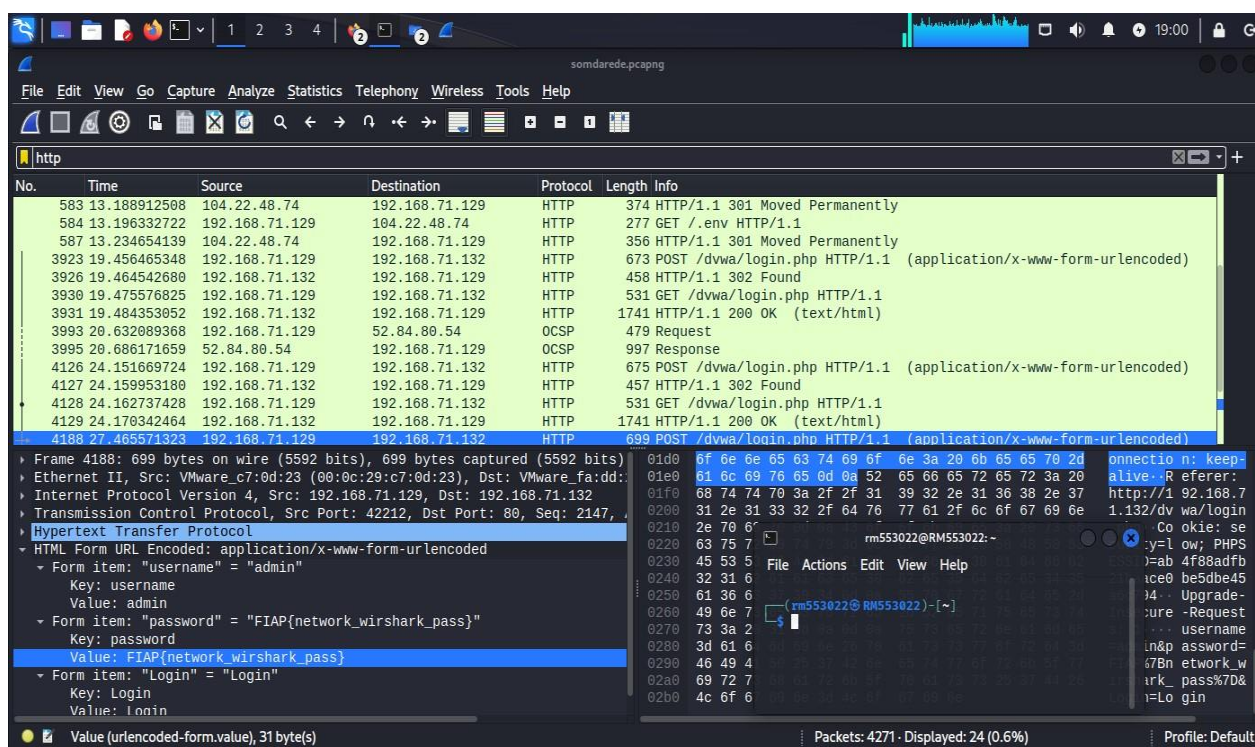
9. SOM DA REDE

9.1. CTF SOM DA REDE

Neste CTF, tem como objetivo relacionado ao log, encontrar o acesso e senha que foi capturada.

Dessa maneira, com o arquivo de log disponível para análise, A resposta então foi obtida de forma rápida como podemos ver na imagem a seguir:

Figura 11 – Wireshark.



Fonte – Arquivo de log Som da Rede.

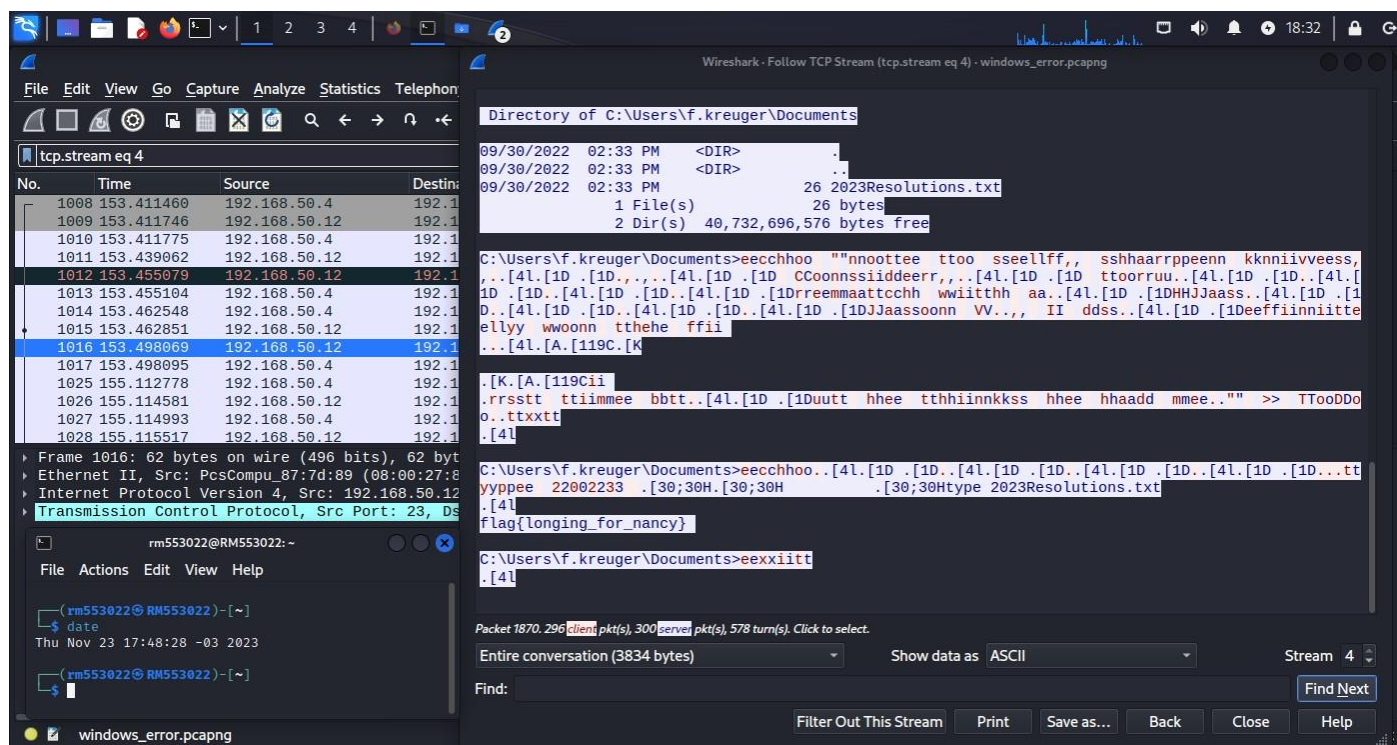
Seguindo o protocolo HTTP, foi aplicada uma análise nas linhas correspondente ao POST, verificando uma possível transferência de dados pela web, assim encontrando o valor: FIAP{network_wirshark_pass}.

10. WINDOWS ERROR

10.1. CTF WINDOWS ERROR

Neste CTF, tem como objetivo de encontrar o erro que está no servidor relacionado ao log. Dessa maneira, com o arquivo de log disponível para análise, A resposta então foi obtida de forma rápida conforme imagem a seguir:

Figura 12 - Wireshark Windows Error.



Fonte – Arquivo de Log Windows Error.

Após aplicar a analyze com o scan em tcp.stream, ao verificar as linhas correspondente ao IP 192.168.50.12, classificando elas como retransmissão, suspeitando do comportamento, foi necessário, aplicar mais uma analyze utilizando o wireshark nas linhas que foram filtradas, chegando na linha, tcp.stream eq4, é encontrado a resposta como flag, flag{loging_for_nancy}, apenas necessário traduzir para FIAP{loging_for_nancy}.

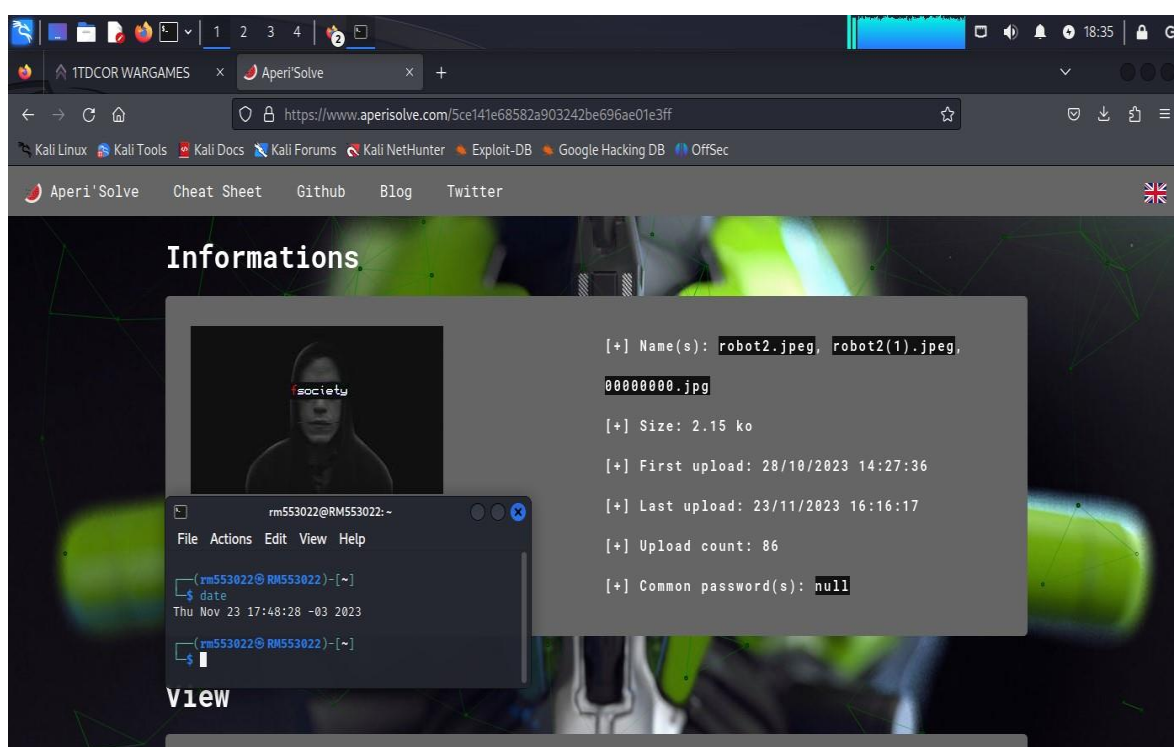
11. MR. ROBOT

11.1. CTF MR. ROBOT

Neste CTF, tem como objetivo, encontrar os segredos cruciais na imagem, que foi escondida.

Dessa maneira, com o arquivo de log disponível para análise, A resposta então foi obtida de forma rápida conforme as imagens a seguir:

Figura 13 – Aperi'Solve.

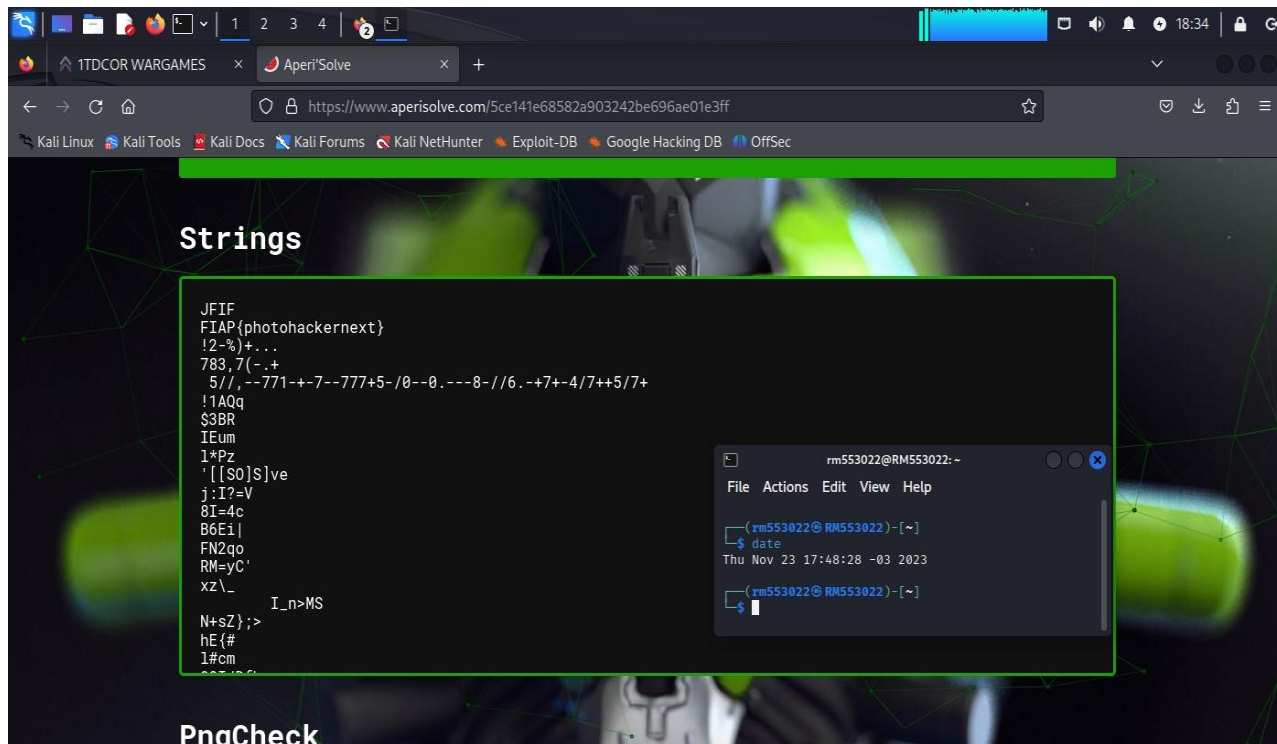


Fonte – Imagem disponibilizada pelo CTF.

Seguindo o conceito, que foi utilizado a esteganografia na imagem, para esconder informações nela, utilizando a ferramenta Aperi'solve, é possível obter as informações que foram camufladas, conforme a próxima figura ilustrativa, tem como exemplo as strings que pode ser localizada.

11.2. CTF MR. ROBOT

Figura 14 - Aperi'Solve Strings.



Fonte - Fonte – Imagem disponibilizada pelo CTF.

Foi possível notar que `FIAP{photohackernext}`, estando como parte camuflada dentro da String, então, com isso foi possível localizar e aplicar a flag no CTF.

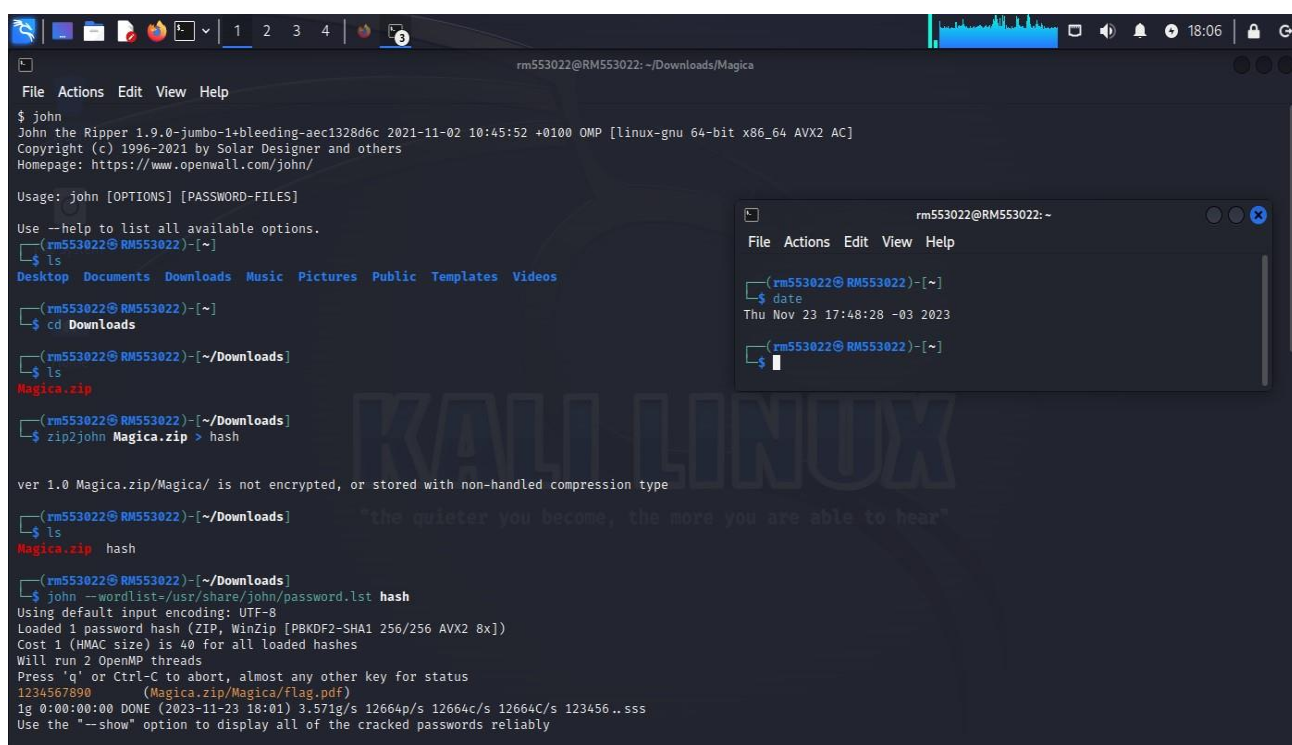
12. CYBER MAGIA

12.1. CTF CYBER MAGIA

Neste CTF, tem como objetivo, encontrar uma forma de quebrar um arquivo zipado.

Dessa maneira, com o arquivo de log disponível para análise, A reposta então foi obtida de forma rápida conforme as imagens a seguir:

Figura 15 – Cyber Magia Quebrando o Arquivo Zipado.



```

$ john
John the Ripper 1.9.0-jumbo-1+bleeding-aec1328d6c 2021-11-02 10:45:52 +0100 OMP [linux-gnu 64-bit x86_64 AVX2 AC]
Copyright (c) 1996-2021 by Solar Designer and others
Homepage: https://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]

Use --help to list all available options.
(rms53022@rms53022)~$ ls
Desktop Documents Downloads Music Pictures Public Templates Videos
(rms53022@rms53022)~$ cd Downloads
(rms53022@rms53022)~/Downloads$ ls
Magica.zip
(rms53022@rms53022)~/Downloads$ zip2john Magica.zip > hash

ver 1.0 Magica.zip/Magica/ is not encrypted, or stored with non-handled compression type
(rms53022@rms53022)~/Downloads$ ls
Magica.zip hash
(rms53022@rms53022)~/Downloads$ john --wordlist=/usr/share/john/password.lst hash
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Cost 1 (HMAC size) is 40 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
1234567890 (Magica.zip/Magica/Flag.pdf)
1g 0:00:00:00 DONE (2023-11-23 18:01) 3.571g/s 12664p/s 12664c/s 12664C/s 123456..sss
Use the "--show" option to display all of the cracked passwords reliably
  
```

Fonte - ssh jackblack@167.71.17.59 -p 2003.

Utilizando a ferramenta John, foi possível aplicar uma wordlist própria da ferramenta, conforme os comandos, é localizada a senha para extrair então o arquivo e assim poder ter acesso ao conteúdo.

Figura 16 - Cyber Magia Extraindo o Arquivo Zipado.

```

rm553022@RM553022: ~/Downloads/Magica
File Actions Edit View Help

rm553022@RM553022:~/Downloads
$ 7z x -p1234567890 Magica.zip

7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale=C.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs Intel(R) Core(TM) i5-8265U CPU @ 1.60GHz (806EB),ASM,AES-NI)

Scanning the drive for archives:
1 file, 396 bytes (1 KiB)

Extracting archive: Magica.zip
-
Path = Magica.zip
Type = zip
Physical Size = 396

Everything is Ok

Folders: 1
Files: 1
Size: 40
Compressed: 396

rm553022@RM553022:~/Downloads
$ ls
Magica  Magica.zip  hash

rm553022@RM553022:~/Downloads
$ cd Magica

rm553022@RM553022:~/Downloads/Magica
$ ls
flag.pdf

rm553022@RM553022:~/Downloads/Magica
$ cat flag.pdf
IZEUCUD3MFPW2YLHNFQV6ZLTORQV63TPL5QXE7I=

rm553022@RM553022:~/Downloads/Magica

```

Fonte - ssh jackblack@167.71.17.59 -p 2003.

Após extração do arquivo zipado, foi possível localizar o Hash Base64.

IZEUCUD3MFPW2YLHNFQV6ZLTORQV63TPL5QXE7I=, ao decodar, a seguinte resposta é obtida, FIAP{a_magia_esta_no_ar}.

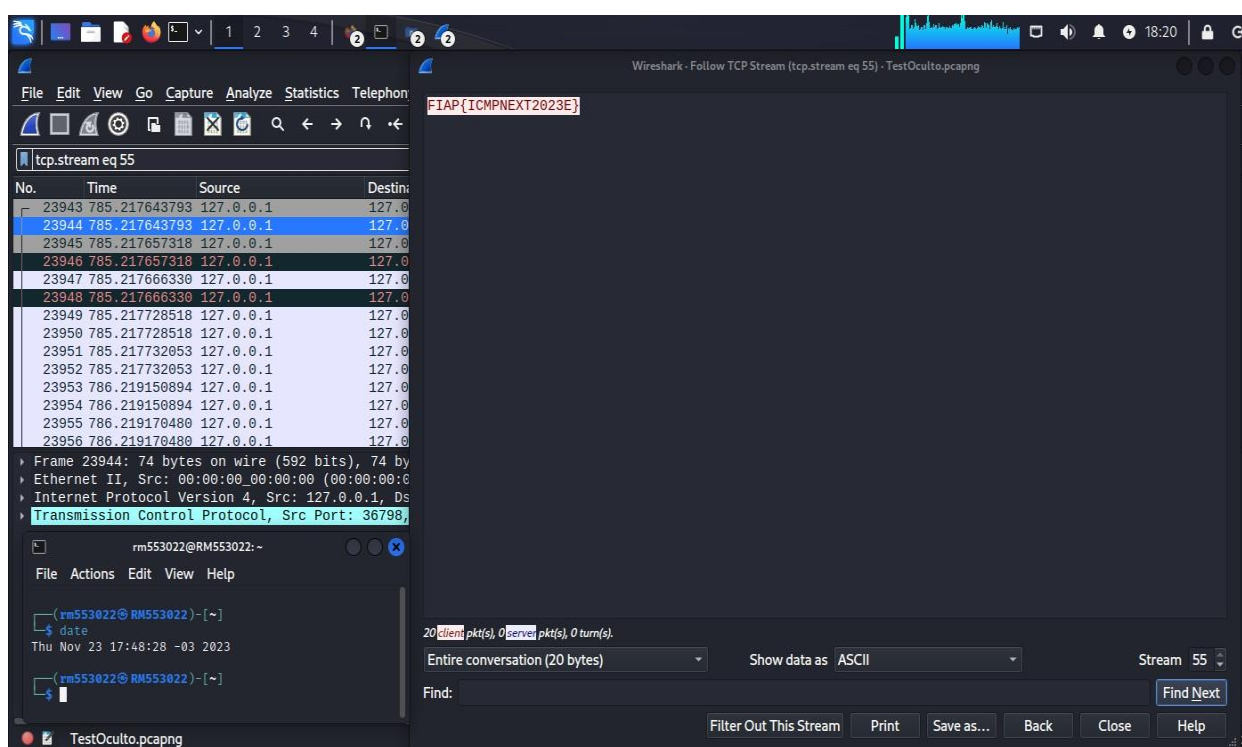
13. TEST OCULTO

13.1. CTF TEST OCULTO

Neste CTF, tem como objetivo, encontrar a forma que o invasor está exfiltrando dados.

Dessa maneira, com o arquivo de log disponível para análise, a resposta então foi obtida de forma rápida conforme a imagem a seguir:

Figura 17 – Wireshark Test Oculito.



Fonte - Arquivo de Log Test Ocult.

Após aplicar a analyze com o scan em tcp.stream, ao verificar as linhas correspondente ao IP 172.0.0.1, classificando elas como retransmissão, suspeitando do comportamento, foi necessário, aplicar mais uma analyze utilizando o wireshark nas linhas que foram filtradas, chegando na linha, tcp.stream eq55, é encontrado a resposta, FIAP{ICMPNEXT2023E}.

CONCLUSÕES FINAIS

13.2. CONCLUSÕES FINAIS

Em face das reflexões e investigações empreendidas ao longo deste estudo, é possível afirmar que a participação no ambiente acadêmico da FIAP proporcionou uma experiência enriquecedora e desafiadora. A integração ao Centro de Tecnologia e Formação Superior (CTFS) foi determinante para a construção de conhecimentos sólidos e aprimoramento de habilidades fundamentais.

Os desafios encontrados no percurso acadêmico, notadamente no contexto do CTFS, revelaram-se cruciais para o desenvolvimento pessoal e profissional. Cada obstáculo superado representou uma oportunidade de crescimento, destacando a resiliência e a capacidade de adaptação como ferramentas essenciais na trajetória do aprendizado.

Ao refletir sobre os desafios enfrentados, é inegável a contribuição significativa dessas experiências para a consolidação de uma base sólida de conhecimento. A FIAP, como instituição comprometida com a excelência educacional, proporcionou um ambiente propício para a superação de desafios, instigando a busca incessante pelo aprimoramento e aquisição de competências necessárias para enfrentar os dilemas contemporâneos.

O aprendizado adquirido durante o percurso acadêmico na FIAP transcendeu a mera assimilação de conceitos teóricos, revelando-se como um processo dinâmico de construção de saberes. A interação com professores qualificados, a troca de experiências com colegas e a aplicação prática dos conhecimentos adquiridos foram elementos fundamentais para a consolidação de uma formação integral.

Em suma, a trajetória na FIAP, aliada à experiência no CTFS, proporcionou não apenas a aquisição de competências técnicas, mas também o desenvolvimento de habilidades interpessoais e o fortalecimento do espírito empreendedor. Os desafios superados ao longo desse percurso representam conquistas valiosas que, indubitavelmente, contribuirão para o enfrentamento bem-sucedido dos desafios futuros, consolidando-se como alicerces sólidos para uma trajetória profissional promissora.