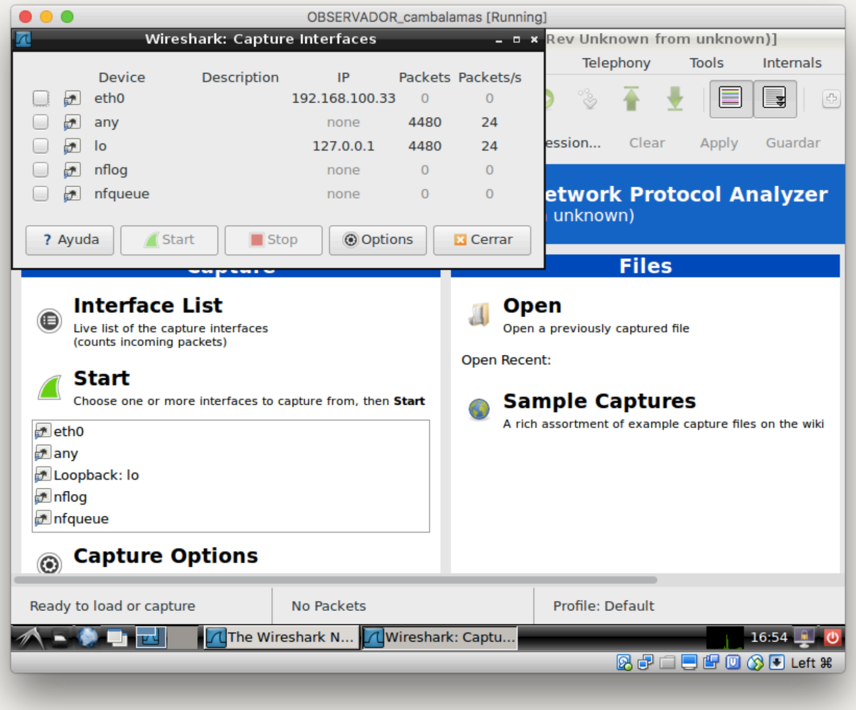
Daniel Camba Lamas

WireShark

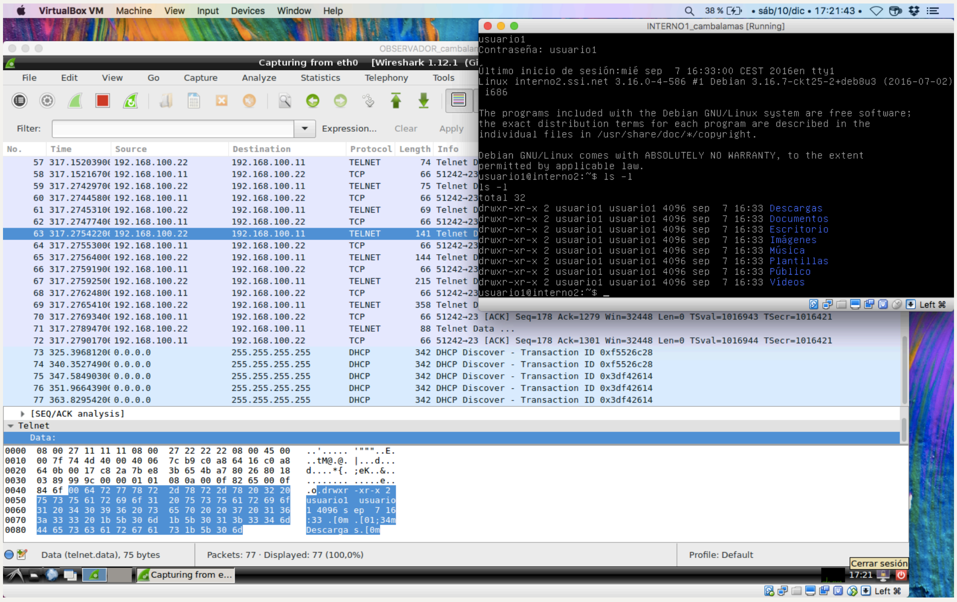
Empezando la caputra de paquetes!!!



Wireshark: Capture Interfaces

	Device	Description	IP	Packets	Packets/s
□	eth0		192.168.100.33	0	0
□	any		none	4480	24
□	lo		127.0.0.1	4480	24
□	nflog		none	0	0
□	nfqueue		none	0	0

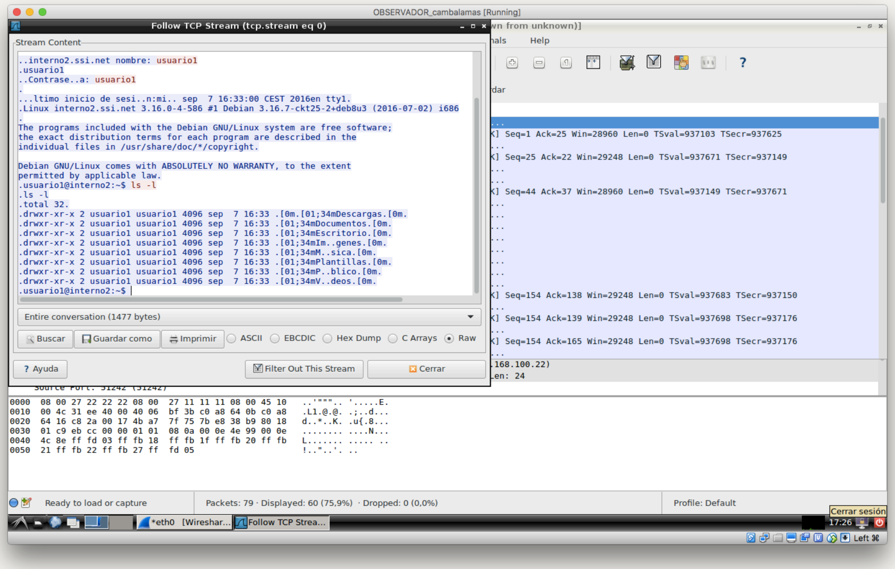
La conexión por Telnet no está encriptada, por lo que podemos leer mucha información de los paquetes, en la siguiente captura el recuadro seleccionado de wireshark, contiene el user y la pass utilizada (*usuario1, usuario1*)



```
No.   Time           Source          Destination      Protocol Length Info
   57 317.1520390( 192.168.100.22  192.168.100.11   TELNET      74 Telnet D
   58 317.1521670( 192.168.100.11  192.168.100.22   TCP         66 51242→23
   59 317.2742970( 192.168.100.22  192.168.100.11   TELNET      75 Telnet D
   60 317.2744580( 192.168.100.11  192.168.100.22   TCP         66 51242→23
   61 317.2745310( 192.168.100.22  192.168.100.11   TELNET      69 Telnet D
   62 317.2747740( 192.168.100.11  192.168.100.22   TCP         66 51242→23
   63 317.2754220( 192.168.100.22  192.168.100.11   TELNET     141 Telnet D
   64 317.2755300( 192.168.100.11  192.168.100.22   TCP         66 51242→23
   65 317.2756400( 192.168.100.22  192.168.100.11   TELNET     144 Telnet D
   66 317.2759190( 192.168.100.11  192.168.100.22   TCP         66 51242→23
   67 317.2759250( 192.168.100.22  192.168.100.11   TELNET     215 Telnet D
   68 317.2762480( 192.168.100.11  192.168.100.22   TCP         66 51242→23
   69 317.2765410( 192.168.100.22  192.168.100.11   TELNET     358 Telnet D
   70 317.2769340( 192.168.100.11  192.168.100.22   TCP         66 51242→23 [ACK] Seq=178 Ack=1279 Win=32448 Len=0 TSval=1016943 TSecr=1016421
   71 317.2789470( 192.168.100.22  192.168.100.11   TELNET      88 Telnet Data ...
   72 317.2790170( 192.168.100.11  192.168.100.22   TCP         66 51242→23 [ACK] Seq=178 Ack=1301 Win=32448 Len=0 TSval=1016944 TSecr=1016421
   73 325.3968120( 0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0xf5526c28
   74 340.3527490( 0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0xf5526c28
   75 347.5849030( 0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0x3df42614
   76 351.9664390( 0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0x3df42614
   77 363.8295420( 0.0.0.0         255.255.255.255  DHCP       342 DHCP Discover - Transaction ID 0x3df42614
  ▸ [SEQ/ACK analysis]
▾ Telnet
    Data:
0000  08 00 27 11 11 11 08 00  27 22 22 22 08 00 45 00   ..'..... '"""..E.
0010  00 7f 74 4d 40 00 40 06  7c b9 c0 a8 64 16 c0 a8   ..tM@.@. |...d...
0020  64 0b 00 17 c8 2a 7b e8  3b 65 4b a7 80 26 80 18   d....*{. ;eK..&..
0030  03 89 99 9c 00 00 01 01  08 0a 00 0f 82 65 00 0f   ........ .....e..
0040  84 6f 00 64 72 77 78 72  2d 78 72 2d 78 20 32 20   .o.drwxr -xr-x 2
0050  75 73 75 61 72 69 6f 31  20 75 73 75 61 72 69 6f   usuario1  usuario
0060  31 20 34 30 39 36 20 73  65 70 20 20 37 20 31 36   1 4096 s ep  7 16
0070  3a 33 33 20 1b 5b 30 6d  1b 5b 30 31 3b 33 34 6d   :33 .[0m .[01;34m
0080  44 65 73 63 61 72 67 61  73 1b 5b 30 6d            Descarga s.[0m

Data (telnet.data), 75 bytes    Packets: 77 · Displayed: 77 (100,0%)
```

```
usuario1
Contraseña: usuario1

Último inicio de sesión:mié sep  7 16:33:00 CEST 2016en tty1
Linux interno2.ssi.net 3.16.0-4-586 #1 Debian 3.16.7-ckt25-2+deb8u3 (2016-07-02)
 i686

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.
usuario1@interno2:~$ ls -l
ls -l
total 32
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Descargas
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Documentos
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Escritorio
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Imágenes
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Música
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Plantillas
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Público
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Vídeos
usuario1@interno2:~$ _
```

Y como no está cifrada la comunicación, visualizamos sin menor problema la información que, en este caso, se le mostró al usuario por pantalla.

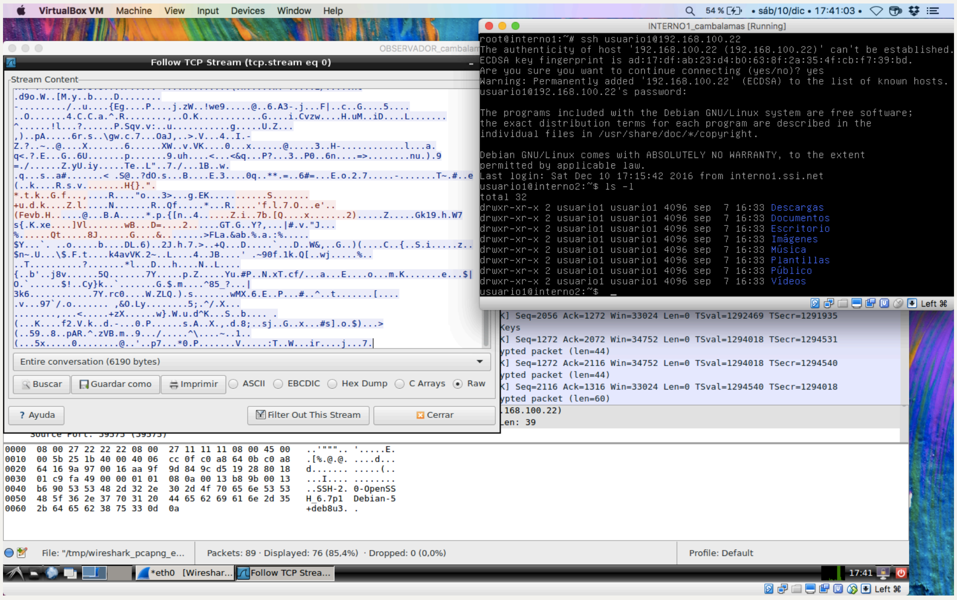


```
..interno2.ssi.net nombre: usuario1
.usuario1
..Contrase..a: usuario1
.
...ltimo inicio de sesi..n:mi.. sep  7 16:33:00 CEST 2016en tty1.
.Linux interno2.ssi.net 3.16.0-4-586 #1 Debian 3.16.7-ckt25-2+deb8u3 (2016-07-02) i686
.
The programs included with the Debian GNU/Linux system are free software;
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.
.usuario1@interno2:~$ ls -l
.ls -l
.total 32.
.drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 .[0m.[01;34mDescargas.[0m.
.drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 .[01;34mDocumentos.[0m.
.drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 .[01;34mEscritorio.[0m.
.drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 .[01;34mIm..genes.[0m.
.drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 .[01;34mM..sica.[0m.
.drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 .[01;34mPlantillas.[0m.
.drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 .[01;34mP..blico.[0m.
.drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 .[01;34mV..deos.[0m.
.usuario1@interno2:~$
```

```
...
K] Seq=1 Ack=25 Win=28960 Len=0 TSval=937103 TSecr=937625
...
K] Seq=25 Ack=22 Win=29248 Len=0 TSval=937671 TSecr=937149
...
...
K] Seq=44 Ack=37 Win=28960 Len=0 TSval=937149 TSecr=937671
...
...
...
...
...
...
...
...
K] Seq=154 Ack=138 Win=29248 Len=0 TSval=937683 TSecr=937150
...
K] Seq=154 Ack=139 Win=29248 Len=0 TSval=937698 TSecr=937176
...
K] Seq=154 Ack=165 Win=29248 Len=0 TSval=937698 TSecr=937176
...
.168.100.22)
Len: 24
```

```
0000  08 00 27 22 22 22 08 00  27 11 11 11 08 00 45 10   ..'""".. '.....E.
0010  00 4c 31 ee 40 00 40 06  bf 3b c0 a8 64 0b c0 a8   .L1.@.@. .;..d...
0020  64 16 c8 2a 00 17 4b a7  7f 75 7b e8 38 b9 80 18   d..*..K. .u{.8...
0030  01 c9 eb cc 00 00 01 01  08 0a 00 0e 4e 99 00 0e   ........ ....N...
0040  4c 8e ff fd 03 ff fb 18  ff fb 1f ff fb 20 ff fb   L....... ..... ..
0050  21 ff fb 22 ff fb 27 ff  fd 05                     !..".."'. ..
```

Si la conexión es SSH al caputrarla obtendremos cierta información útil del equipo pero al ir encriptada la comunicación no podemos leer la información que se le muestra al usuario.



```
root@interno1:~# ssh usuario1@192.168.100.22
The authenticity of host '192.168.100.22 (192.168.100.22)' can't be established.
ECDSA key fingerprint is ad:17:df:ab:23:d4:b0:63:8f:2a:35:4f:cb:f7:39:bd.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.100.22' (ECDSA) to the list of known hosts.
usuario1@192.168.100.22's password:

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: Sat Dec 10 17:15:42 2016 from interno1.ssi.net
usuario1@interno2:~$ ls -l
total 32
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Descargas
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Documentos
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Escritorio
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Imágenes
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Música
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Plantillas
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Público
drwxr-xr-x 2 usuario1 usuario1 4096 sep  7 16:33 Vídeos
usuario1@interno2:~$ _
```

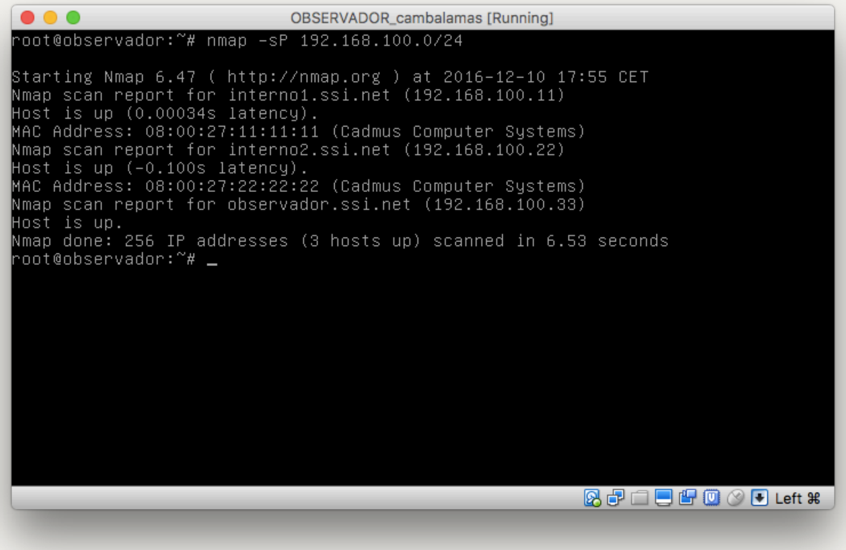
```
.d9o.W..[M.y..b....D........
-........./..u....{Eg....P....j.zW..!we9.....@..6.A3-.j...F|..c..G....5....
..O.......4.C.C.a.^.R.......,..O.K...........G....i.Cvzw....H.uM..iD....L.......
^......!l...?......P.Sqv.v:..u...........g.....U.Z...
,)..pA.....6r.s..\gw.c.7...OaJ,..>.V...4..I.-
Z.?..~..@....X.......6......XW..v.VK....0...x......@.....3..H-.............l...a.
q<.?.E...G..6U.......p.......9.uh....<...<&q...P?...3..P0..6n....=>........nu.).9
=./......Z.yU.iy.....Te..L"..7./...1B..w.
.q...s..a#.......< .S@..?dO.s...B....E.3....0q..**.=..6#=...E.o.2.7.....-.......T~.#..e
(..k....R.s.v........H{}.".
*.t.k..G.f...,....R...."o...3>...g.EK............S.......
+u.d.k....Z.l.....N.......R..Qf.....*...R.....'f.l.7.O...e'..
(Fevb.H......@...B.A.....*.p.{[n..4.......Z.i..7b.[Q....x.......2).....Z.....Gk19.h.W7
s{.K.xe....]Vl.......wB...D=....2.......GT.G..Y?,...|#.v."J...
%......Qt.....8J......G....&........>FLa.&ab.%.a.:%.....
$Y...`. ..o.....b....DL.6)..2J.h.7.>..+Q...D.....`...D..W&,..G..)(....C..{..S.i.....z..
$n~.U...\$.F.t....k4avVK.2~..L....4..JB....' .~90f.1k.Q[..wj.....%..
..T..........?.......*l...D...h....N..L....
{..b'..j8v......5Q.......7Y.....p.Z.....Yu.#P..N.xT.cf/...a...E....o...m.K.......e...$|
O.`......$!..Cy}k..`.......G.$.m....^85_?...|
3k6............7Y.rc0....W.ZLQ.).s.......wMX.6.E..P...#..^..t.......[....
.v...97`/.o....... ,&O.Ly........5;.^/.X...
........,..<.....+zX......w}.W.u.d^K...S..b.... .
(...K....f2.V.k..d.-...0.P......s.A..X.,.d.8;..sj..G..x...#s].o.$)...>
(..59..8..pAR.^.zVB.m..9.../.....^\....~..1..
(...5x.....0........@..'..p7...*0.P.......V.....:T..W...ir....j...7.
```

```
K] Seq=2056 Ack=1272 Win=33024 Len=0 TSval=1292469 TSecr=1291935
Keys
K] Seq=1272 Ack=2072 Win=34752 Len=0 TSval=1294018 TSecr=1294531
ypted packet (len=44)
K] Seq=1272 Ack=2116 Win=34752 Len=0 TSval=1294018 TSecr=1294540
ypted packet (len=44)
K] Seq=2116 Ack=1316 Win=33024 Len=0 TSval=1294540 TSecr=1294018
ypted packet (len=60)
.168.100.22)
Len: 39
```

```
0000  08 00 27 22 22 22 08 00  27 11 11 11 08 00 45 00   ..'""".. '.....E.
0010  00 5b 25 1b 40 00 40 06  cc 0f c0 a8 64 0b c0 a8   .[%.@.@. ....d...
0020  64 16 9a 97 00 16 aa 9f  9d 84 9c d5 19 28 80 18   d....... .....(..
0030  01 c9 fa 49 00 00 01 01  08 0a 00 13 b8 9b 00 13   ...I.... ........
0040  b6 90 53 53 48 2d 32 2e  30 2d 4f 70 65 6e 53 53   ..SSH-2. 0-OpenSS
0050  48 5f 36 2e 37 70 31 20  44 65 62 69 61 6e 2d 35   H_6.7p1  Debian-5
0060  2b 64 65 62 38 75 33 0d  0a                        +deb8u3. .
```

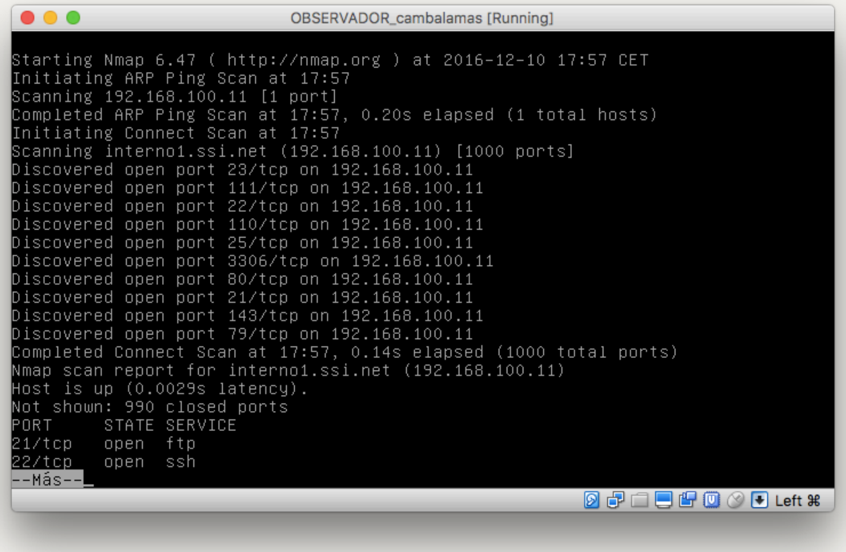
Nmap

Obtención de IPs

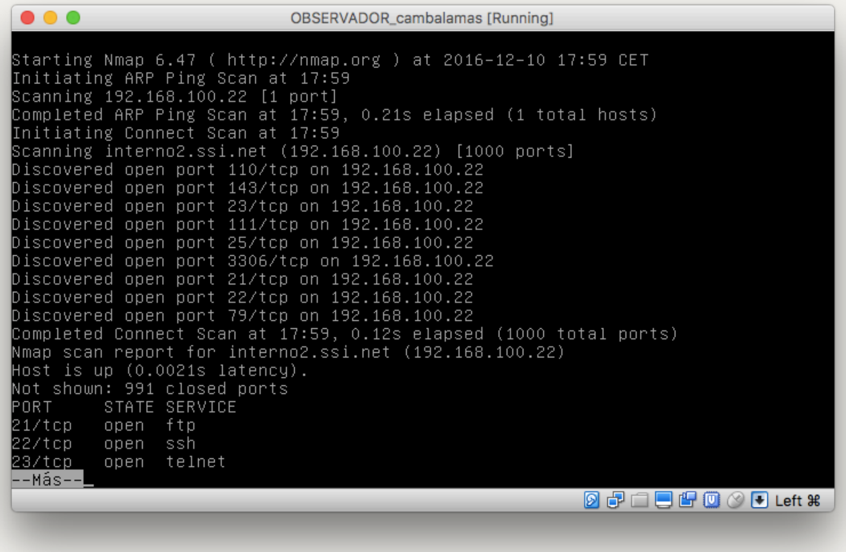


```
root@observador:~# nmap -sP 192.168.100.0/24

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 17:55 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.00034s latency).
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)
Nmap scan report for interno2.ssi.net (192.168.100.22)
Host is up (-0.100s latency).
MAC Address: 08:00:27:22:22:22 (Cadmus Computer Systems)
Nmap scan report for observador.ssi.net (192.168.100.33)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.53 seconds
root@observador:~# _
```

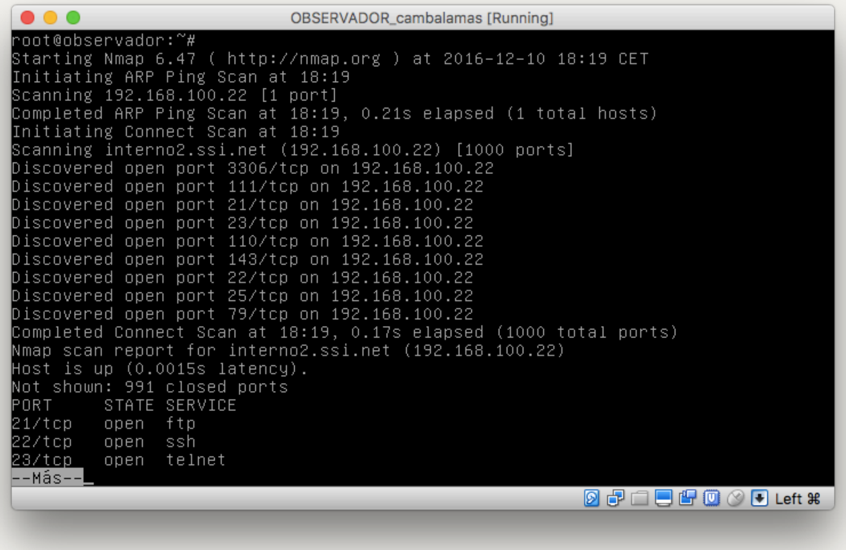
Escaneo de puertos.



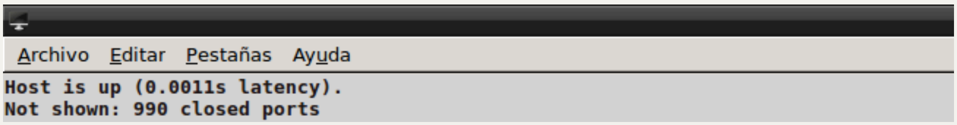
```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 17:57 CET
Initiating ARP Ping Scan at 17:57
Scanning 192.168.100.11 [1 port]
Completed ARP Ping Scan at 17:57, 0.20s elapsed (1 total hosts)
Initiating Connect Scan at 17:57
Scanning interno1.ssi.net (192.168.100.11) [1000 ports]
Discovered open port 23/tcp on 192.168.100.11
Discovered open port 111/tcp on 192.168.100.11
Discovered open port 22/tcp on 192.168.100.11
Discovered open port 110/tcp on 192.168.100.11
Discovered open port 25/tcp on 192.168.100.11
Discovered open port 3306/tcp on 192.168.100.11
Discovered open port 80/tcp on 192.168.100.11
Discovered open port 21/tcp on 192.168.100.11
Discovered open port 143/tcp on 192.168.100.11
Discovered open port 79/tcp on 192.168.100.11
Completed Connect Scan at 17:57, 0.14s elapsed (1000 total ports)
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.0029s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
--Más--_
```



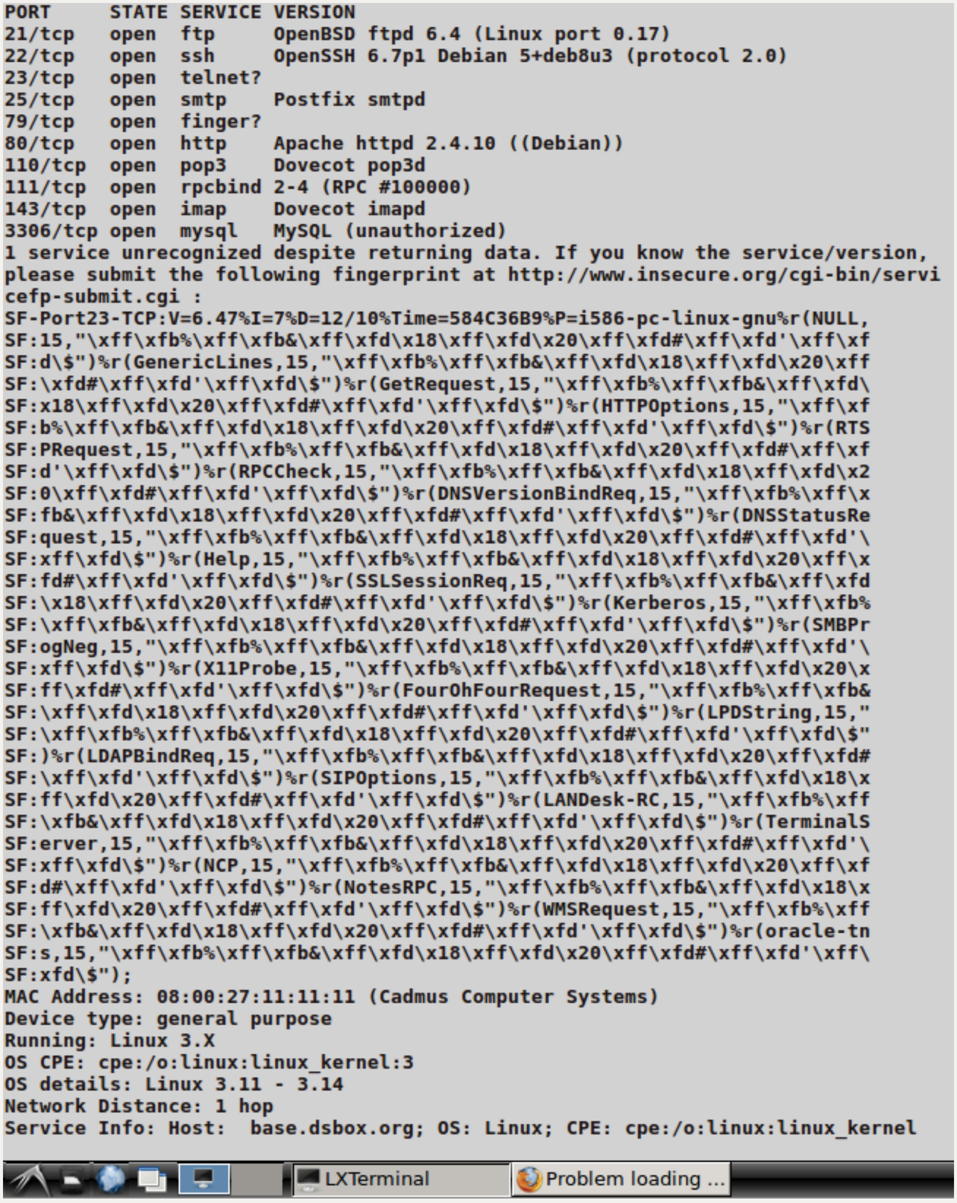
```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 17:59 CET
Initiating ARP Ping Scan at 17:59
Scanning 192.168.100.22 [1 port]
Completed ARP Ping Scan at 17:59, 0.21s elapsed (1 total hosts)
Initiating Connect Scan at 17:59
Scanning interno2.ssi.net (192.168.100.22) [1000 ports]
Discovered open port 110/tcp on 192.168.100.22
Discovered open port 143/tcp on 192.168.100.22
Discovered open port 23/tcp on 192.168.100.22
Discovered open port 111/tcp on 192.168.100.22
Discovered open port 25/tcp on 192.168.100.22
Discovered open port 3306/tcp on 192.168.100.22
Discovered open port 21/tcp on 192.168.100.22
Discovered open port 22/tcp on 192.168.100.22
Discovered open port 79/tcp on 192.168.100.22
Completed Connect Scan at 17:59, 0.12s elapsed (1000 total ports)
Nmap scan report for interno2.ssi.net (192.168.100.22)
Host is up (0.0021s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
--Más--_
```



```
root@observador:~#
Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 18:19 CET
Initiating ARP Ping Scan at 18:19
Scanning 192.168.100.22 [1 port]
Completed ARP Ping Scan at 18:19, 0.21s elapsed (1 total hosts)
Initiating Connect Scan at 18:19
Scanning interno2.ssi.net (192.168.100.22) [1000 ports]
Discovered open port 3306/tcp on 192.168.100.22
Discovered open port 111/tcp on 192.168.100.22
Discovered open port 21/tcp on 192.168.100.22
Discovered open port 23/tcp on 192.168.100.22
Discovered open port 110/tcp on 192.168.100.22
Discovered open port 143/tcp on 192.168.100.22
Discovered open port 22/tcp on 192.168.100.22
Discovered open port 25/tcp on 192.168.100.22
Discovered open port 79/tcp on 192.168.100.22
Completed Connect Scan at 18:19, 0.17s elapsed (1000 total ports)
Nmap scan report for interno2.ssi.net (192.168.100.22)
Host is up (0.0015s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
--Más--_
```

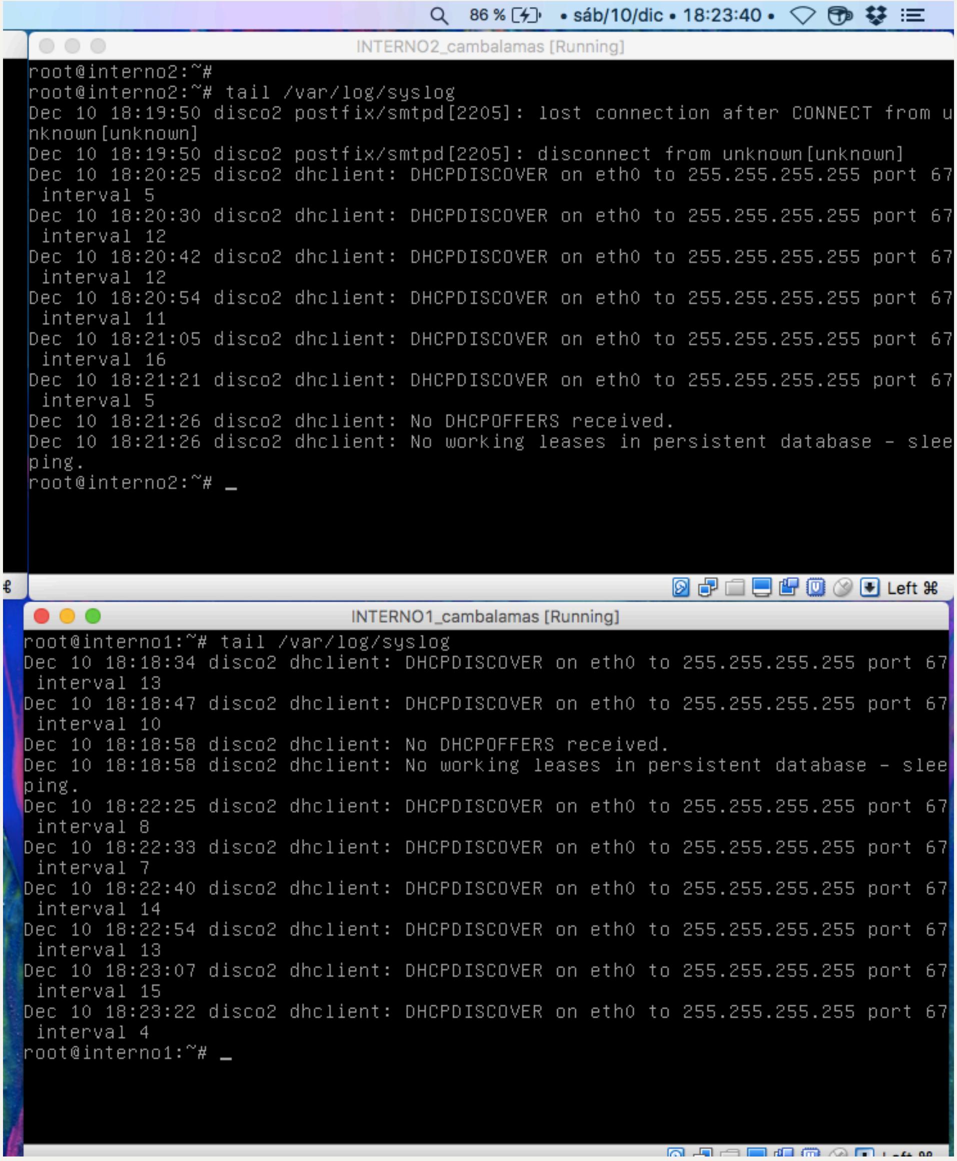


```
Host is up (0.0011s latency).
Not shown: 990 closed ports
```



```
PORT     STATE SERVICE VERSION
21/tcp   open  ftp     OpenBSD ftpd 6.4 (Linux port 0.17)
22/tcp   open  ssh     OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
23/tcp   open  telnet?
25/tcp   open  smtp    Postfix smtpd
79/tcp   open  finger?
80/tcp   open  http    Apache httpd 2.4.10 ((Debian))
110/tcp  open  pop3    Dovecot pop3d
111/tcp  open  rpcbind 2-4 (RPC #100000)
143/tcp  open  imap    Dovecot imapd
3306/tcp open  mysql   MySQL (unauthorized)
1 service unrecognized despite returning data. If you know the service/version,
please submit the following fingerprint at http://www.insecure.org/cgi-bin/servi
cefp-submit.cgi :
SF-Port23-TCP:V=6.47%I=7%D=12/10%Time=584C36B9%P=i586-pc-linux-gnu%r(NULL,
SF:15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xf
SF:d\$")%r(GenericLines,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff
SF:\xfd#\xff\xfd'\xff\xfd\$")%r(GetRequest,15,"\xff\xfb%\xff\xfb&\xff\xfd\
SF:x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(HTTPOptions,15,"\xff\xf
SF:b%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(RTS
SF:PRequest,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xf
SF:d'\xff\xfd\$")%r(RPCCheck,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x2
SF:0\xff\xfd#\xff\xfd'\xff\xfd\$")%r(DNSVersionBindReq,15,"\xff\xfb%\xff\x
SF:fb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(DNSStatusRe
SF:quest,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\
SF:xff\xfd\$")%r(Help,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\x
SF:fd#\xff\xfd'\xff\xfd\$")%r(SSLSessionReq,15,"\xff\xfb%\xff\xfb&\xff\xfd
SF:\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(Kerberos,15,"\xff\xfb%
SF:\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(SMBPr
SF:ogNeg,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\
SF:xff\xfd\$")%r(X11Probe,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\x
SF:ff\xfd#\xff\xfd'\xff\xfd\$")%r(FourOhFourRequest,15,"\xff\xfb%\xff\xfb&
SF:\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(LPDString,15,"
SF:\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$"
SF:)%r(LDAPBindReq,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#
SF:\xff\xfd'\xff\xfd\$")%r(SIPOptions,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\x
SF:ff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(LANDesk-RC,15,"\xff\xfb%\xff
SF:\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(TerminalS
SF:erver,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\
SF:xff\xfd\$")%r(NCP,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xf
SF:d#\xff\xfd'\xff\xfd\$")%r(NotesRPC,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\x
SF:ff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(WMSRequest,15,"\xff\xfb%\xff
SF:\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\xfd\$")%r(oracle-tn
SF:s,15,"\xff\xfb%\xff\xfb&\xff\xfd\x18\xff\xfd\x20\xff\xfd#\xff\xfd'\xff\
SF:xfd\$");
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 3.X
OS CPE: cpe:/o:linux:linux_kernel:3
OS details: Linux 3.11 - 3.14
Network Distance: 1 hop
Service Info: Host:  base.dsbox.org; OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Rastros en el log.



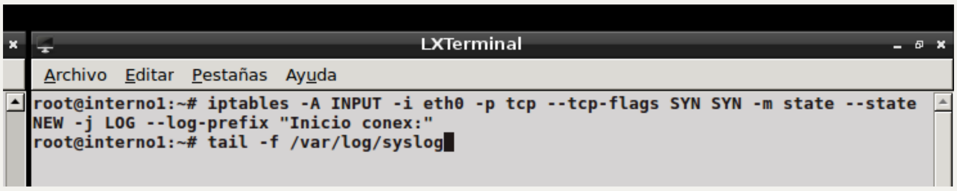
86 % • sáb/10/dic • 18:23:40 •
INTERNO2_cambalamas [Running]
Left ⌘
INTERNO1_cambalamas [Running]

```
root@interno2:~#
root@interno2:~# tail /var/log/syslog
Dec 10 18:19:50 disco2 postfix/smtpd[2205]: lost connection after CONNECT from u
nknown[unknown]
Dec 10 18:19:50 disco2 postfix/smtpd[2205]: disconnect from unknown[unknown]
Dec 10 18:20:25 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 5
Dec 10 18:20:30 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 12
Dec 10 18:20:42 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 12
Dec 10 18:20:54 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 11
Dec 10 18:21:05 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 16
Dec 10 18:21:21 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 5
Dec 10 18:21:26 disco2 dhclient: No DHCPOFFERS received.
Dec 10 18:21:26 disco2 dhclient: No working leases in persistent database - slee
ping.
root@interno2:~# _
```

```
root@interno1:~# tail /var/log/syslog
Dec 10 18:18:34 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 13
Dec 10 18:18:47 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 10
Dec 10 18:18:58 disco2 dhclient: No DHCPOFFERS received.
Dec 10 18:18:58 disco2 dhclient: No working leases in persistent database - slee
ping.
Dec 10 18:22:25 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 8
Dec 10 18:22:33 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 7
Dec 10 18:22:40 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 14
Dec 10 18:22:54 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 13
Dec 10 18:23:07 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 15
Dec 10 18:23:22 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 4
root@interno1:~# _
```

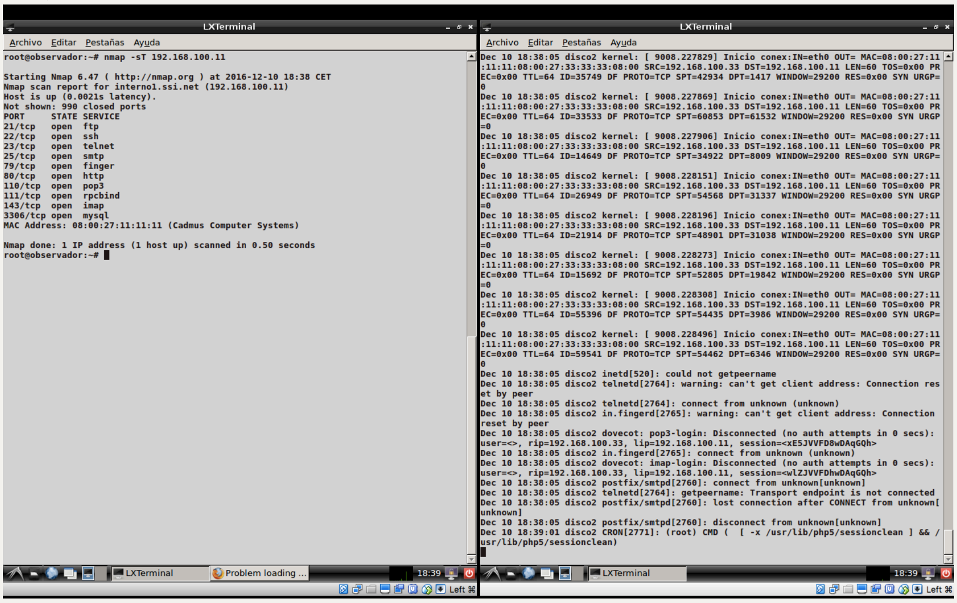
Visualización activa de distintos escaneos.

Activamos la detección SYN utilizando el siguiente comando de IPTABLES.



```
root@interno1:~# iptables -A INPUT -i eth0 -p tcp --tcp-flags SYN SYN -m state --state
NEW -j LOG --log-prefix "Inicio conex:"
root@interno1:~# tail -f /var/log/syslog
```

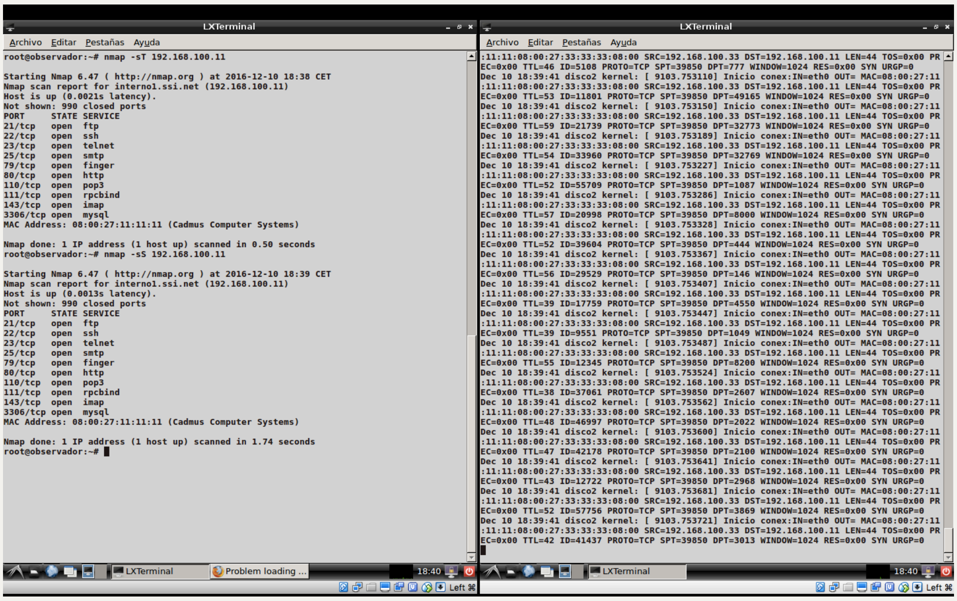
Utilizando -sT, podemos ver calramente como el rastro dejado en el log es muy notorio.



```
root@observador:~# nmap -sT 192.168.100.11

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 18:38 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.0021s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
79/tcp   open  finger
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
3306/tcp open  mysql
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
root@observador:~# █
```

```
Dec 10 18:38:05 disco2 kernel: [ 9008.227829] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PR
EC=0x00 TTL=64 ID=35749 DF PROTO=TCP SPT=42934 DPT=1417 WINDOW=29200 RES=0x00 SYN URGP=
0
Dec 10 18:38:05 disco2 kernel: [ 9008.227869] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PR
EC=0x00 TTL=64 ID=33533 DF PROTO=TCP SPT=60853 DPT=61532 WINDOW=29200 RES=0x00 SYN URGP
=0
Dec 10 18:38:05 disco2 kernel: [ 9008.227906] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PR
EC=0x00 TTL=64 ID=14649 DF PROTO=TCP SPT=34922 DPT=8009 WINDOW=29200 RES=0x00 SYN URGP=
0
Dec 10 18:38:05 disco2 kernel: [ 9008.228151] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PR
EC=0x00 TTL=64 ID=26949 DF PROTO=TCP SPT=54568 DPT=31337 WINDOW=29200 RES=0x00 SYN URGP
=0
Dec 10 18:38:05 disco2 kernel: [ 9008.228196] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PR
EC=0x00 TTL=64 ID=21914 DF PROTO=TCP SPT=48901 DPT=31038 WINDOW=29200 RES=0x00 SYN URGP
=0
Dec 10 18:38:05 disco2 kernel: [ 9008.228273] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PR
EC=0x00 TTL=64 ID=15692 DF PROTO=TCP SPT=52805 DPT=19842 WINDOW=29200 RES=0x00 SYN URGP
=0
Dec 10 18:38:05 disco2 kernel: [ 9008.228308] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PR
EC=0x00 TTL=64 ID=55396 DF PROTO=TCP SPT=54435 DPT=3986 WINDOW=29200 RES=0x00 SYN URGP=
0
Dec 10 18:38:05 disco2 kernel: [ 9008.228496] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=60 TOS=0x00 PR
EC=0x00 TTL=64 ID=59541 DF PROTO=TCP SPT=54462 DPT=6346 WINDOW=29200 RES=0x00 SYN URGP=
0
Dec 10 18:38:05 disco2 inetd[520]: could not getpeername
Dec 10 18:38:05 disco2 telnetd[2764]: warning: can't get client address: Connection res
et by peer
Dec 10 18:38:05 disco2 telnetd[2764]: connect from unknown (unknown)
Dec 10 18:38:05 disco2 in.fingerd[2765]: warning: can't get client address: Connection
reset by peer
Dec 10 18:38:05 disco2 dovecot: pop3-login: Disconnected (no auth attempts in 0 secs):
user=<>, rip=192.168.100.33, lip=192.168.100.11, session=<xE5JVVFD8wDAqGQh>
Dec 10 18:38:05 disco2 in.fingerd[2765]: connect from unknown (unknown)
Dec 10 18:38:05 disco2 dovecot: imap-login: Disconnected (no auth attempts in 0 secs):
user=<>, rip=192.168.100.33, lip=192.168.100.11, session=<wlZJVVFDhwDAqGQh>
Dec 10 18:38:05 disco2 postfix/smtpd[2760]: connect from unknown[unknown]
Dec 10 18:38:05 disco2 telnetd[2764]: getpeername: Transport endpoint is not connected
Dec 10 18:38:05 disco2 postfix/smtpd[2760]: lost connection after CONNECT from unknown[
unknown]
Dec 10 18:38:05 disco2 postfix/smtpd[2760]: disconnect from unknown[unknown]
Dec 10 18:39:01 disco2 CRON[2771]: (root) CMD (  [ -x /usr/lib/php5/sessionclean ] && /
usr/lib/php5/sessionclean)
█
```

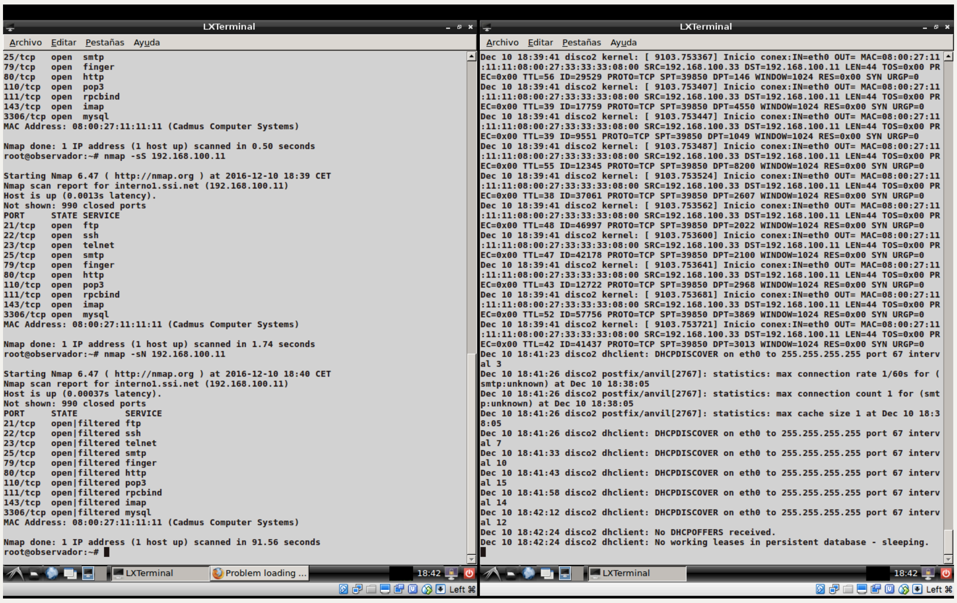
Utilizando -sS, como activamos su detección con IPTABLES, produce el mismo tipo de entradas que la prueba anterior.



```
root@observador:~# nmap -sT 192.168.100.11

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 18:38 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.0021s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
79/tcp   open  finger
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
3306/tcp open  mysql
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
root@observador:~# nmap -sS 192.168.100.11

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 18:39 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.0013s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
79/tcp   open  finger
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
3306/tcp open  mysql
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
root@observador:~# █
```

```
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=46 ID=5108 PROTO=TCP SPT=39850 DPT=777 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753110] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=53 ID=11801 PROTO=TCP SPT=39850 DPT=49165 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753150] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=59 ID=21739 PROTO=TCP SPT=39850 DPT=32773 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753189] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=54 ID=33960 PROTO=TCP SPT=39850 DPT=32769 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753227] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=52 ID=55709 PROTO=TCP SPT=39850 DPT=1087 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753286] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=57 ID=20998 PROTO=TCP SPT=39850 DPT=8000 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753328] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=52 ID=39604 PROTO=TCP SPT=39850 DPT=444 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753367] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=56 ID=29529 PROTO=TCP SPT=39850 DPT=146 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753407] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=39 ID=17759 PROTO=TCP SPT=39850 DPT=4550 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753447] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=39 ID=9551 PROTO=TCP SPT=39850 DPT=1049 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753487] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=55 ID=12345 PROTO=TCP SPT=39850 DPT=8200 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753524] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=38 ID=37061 PROTO=TCP SPT=39850 DPT=2607 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753562] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=48 ID=46997 PROTO=TCP SPT=39850 DPT=2022 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753600] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=47 ID=42178 PROTO=TCP SPT=39850 DPT=2100 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753641] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=43 ID=12722 PROTO=TCP SPT=39850 DPT=2968 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753681] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=52 ID=57756 PROTO=TCP SPT=39850 DPT=3869 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753721] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=42 ID=41437 PROTO=TCP SPT=39850 DPT=3013 WINDOW=1024 RES=0x00 SYN URGP=0
█
```

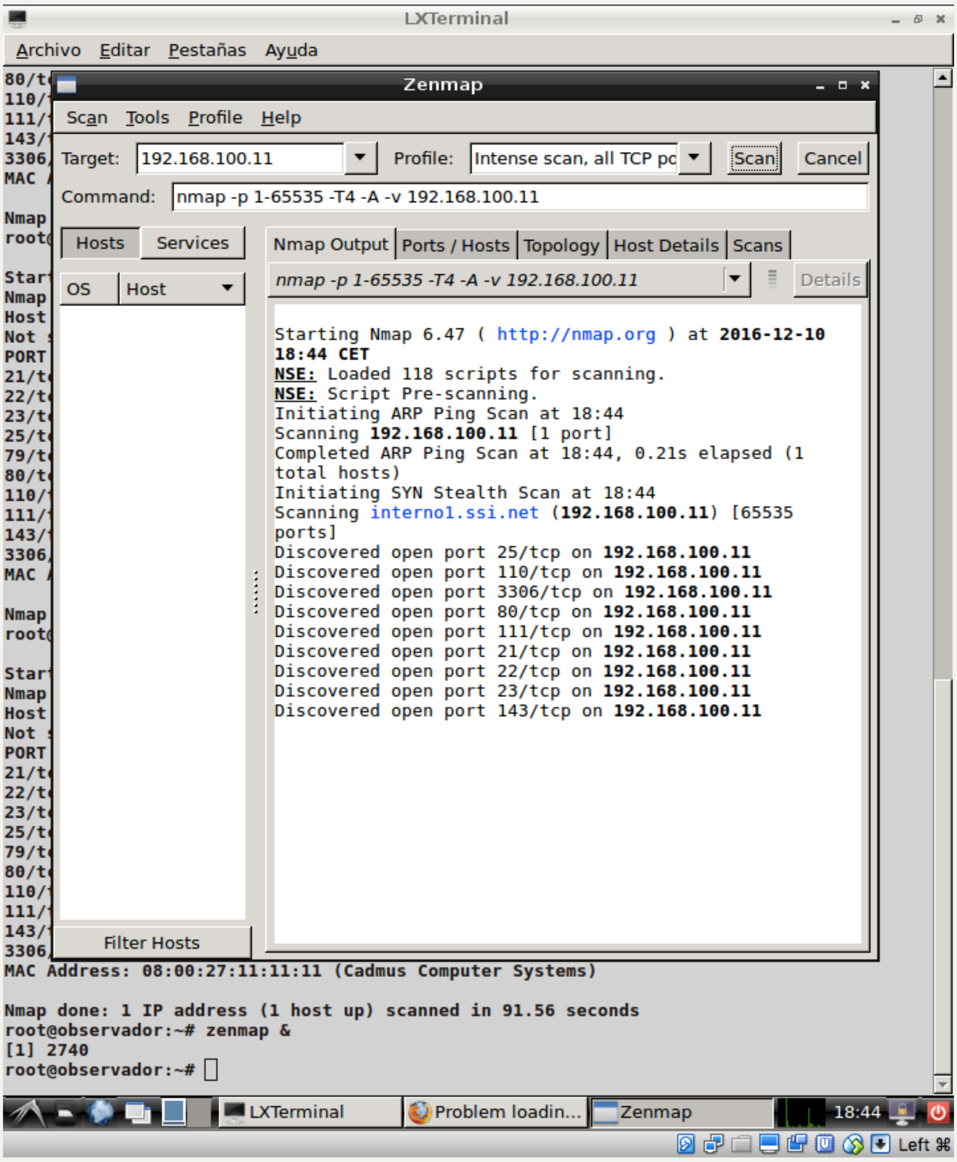
Utilizando -sN se obtiene la misma información y aunque en el log se graba igual la conexión, el volumen de info dejada en el log del otro equipo es minima.



```
25/tcp   open  smtp
79/tcp   open  finger
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
3306/tcp open  mysql
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 0.50 seconds
root@observador:~# nmap -sS 192.168.100.11

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 18:39 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.0013s latency).
Not shown: 990 closed ports
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
79/tcp   open  finger
80/tcp   open  http
110/tcp  open  pop3
111/tcp  open  rpcbind
143/tcp  open  imap
3306/tcp open  mysql
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 1.74 seconds
root@observador:~# nmap -sN 192.168.100.11

Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10 18:40 CET
Nmap scan report for interno1.ssi.net (192.168.100.11)
Host is up (0.00037s latency).
Not shown: 990 closed ports
PORT     STATE         SERVICE
21/tcp   open|filtered ftp
22/tcp   open|filtered ssh
23/tcp   open|filtered telnet
25/tcp   open|filtered smtp
79/tcp   open|filtered finger
80/tcp   open|filtered http
110/tcp  open|filtered pop3
111/tcp  open|filtered rpcbind
143/tcp  open|filtered imap
3306/tcp open|filtered mysql
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 91.56 seconds
root@observador:~# 
```

```
Dec 10 18:39:41 disco2 kernel: [ 9103.753367] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=56 ID=29529 PROTO=TCP SPT=39850 DPT=146 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753407] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=39 ID=17759 PROTO=TCP SPT=39850 DPT=4550 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753447] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=39 ID=9551 PROTO=TCP SPT=39850 DPT=1049 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753487] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=55 ID=12345 PROTO=TCP SPT=39850 DPT=8200 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753524] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=38 ID=37061 PROTO=TCP SPT=39850 DPT=2607 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753562] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=48 ID=46997 PROTO=TCP SPT=39850 DPT=2022 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753600] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=47 ID=42178 PROTO=TCP SPT=39850 DPT=2100 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753641] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=43 ID=12722 PROTO=TCP SPT=39850 DPT=2968 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753681] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=52 ID=57756 PROTO=TCP SPT=39850 DPT=3869 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:39:41 disco2 kernel: [ 9103.753721] Inicio conex:IN=eth0 OUT= MAC=08:00:27:11
:11:11:08:00:27:33:33:33:08:00 SRC=192.168.100.33 DST=192.168.100.11 LEN=44 TOS=0x00 PR
EC=0x00 TTL=42 ID=41437 PROTO=TCP SPT=39850 DPT=3013 WINDOW=1024 RES=0x00 SYN URGP=0
Dec 10 18:41:23 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interv
al 3
Dec 10 18:41:26 disco2 postfix/anvil[2767]: statistics: max connection rate 1/60s for (
smtp:unknown) at Dec 10 18:38:05
Dec 10 18:41:26 disco2 postfix/anvil[2767]: statistics: max connection count 1 for (smt
p:unknown) at Dec 10 18:38:05
Dec 10 18:41:26 disco2 postfix/anvil[2767]: statistics: max cache size 1 at Dec 10 18:3
8:05
Dec 10 18:41:26 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interv
al 7
Dec 10 18:41:33 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interv
al 10
Dec 10 18:41:43 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interv
al 15
Dec 10 18:41:58 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interv
al 14
Dec 10 18:42:12 disco2 dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interv
al 12
Dec 10 18:42:24 disco2 dhclient: No DHCPOFFERS received.
Dec 10 18:42:24 disco2 dhclient: No working leases in persistent database - sleeping.
```

Vía GUI puede hacerse lo mismo utilizando ZENMAP.



Target: 192.168.100.11
Profile: Intense scan, all TCP pc
Command: nmap -p 1-65535 -T4 -A -v 192.168.100.11

```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-12-10
18:44 CET
NSE: Loaded 118 scripts for scanning.
NSE: Script Pre-scanning.
Initiating ARP Ping Scan at 18:44
Scanning 192.168.100.11 [1 port]
Completed ARP Ping Scan at 18:44, 0.21s elapsed (1
total hosts)
Initiating SYN Stealth Scan at 18:44
Scanning interno1.ssi.net (192.168.100.11) [65535
ports]
Discovered open port 25/tcp on 192.168.100.11
Discovered open port 110/tcp on 192.168.100.11
Discovered open port 3306/tcp on 192.168.100.11
Discovered open port 80/tcp on 192.168.100.11
Discovered open port 111/tcp on 192.168.100.11
Discovered open port 21/tcp on 192.168.100.11
Discovered open port 22/tcp on 192.168.100.11
Discovered open port 23/tcp on 192.168.100.11
Discovered open port 143/tcp on 192.168.100.11
```

```
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 91.56 seconds
root@observador:~# zenmap &
[1] 2740
root@observador:~# 
```