2017

SEGURIDAD INFORMÁTICA

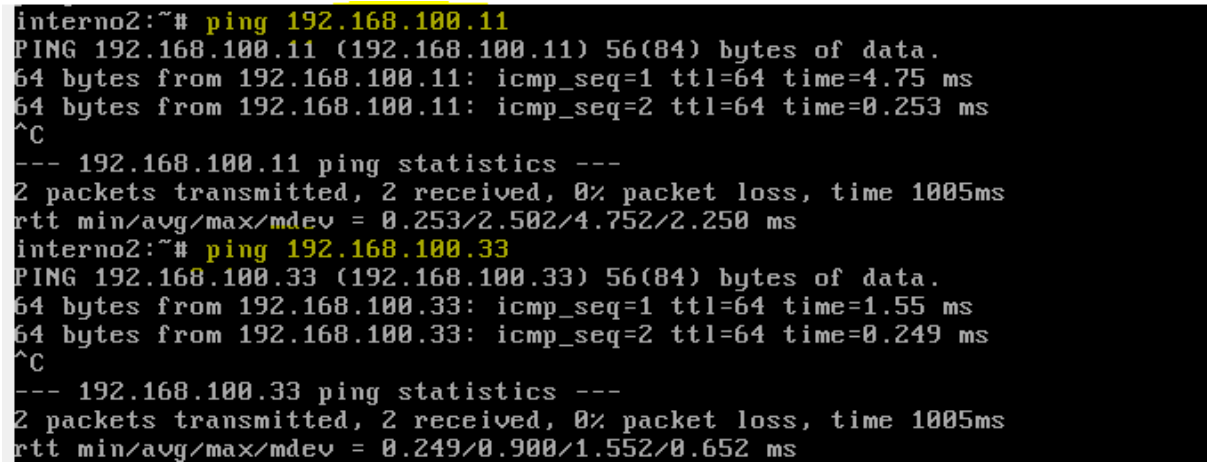
ORQUÍDEA SEIJAS

CONTENIDO

1. INTRODUCCIÓN: CONFIGURACIÓN PREVIA

Para la realización del ejercicio 1 tanto como del ejercicio 2, fue necesario crear y configurar las máquinas virtuales asociadas a los mismos, de forma que se pudo simular una pequeña red. Estas máquinas virtuales son: interno1, con una dirección IP correspondiente a 192.168.100.11, interno2, con una dirección IP correspondiente a 192.168.100.22, y observador, con una dirección IP correspondiente a 192.168.100.33. Los equipos interno1 e interno2 eran las máquinas legítimas, conectadas a una red interna, y el observador era la máquina atacante, que trataba de espiar el tráfico de dicha red.

Tras los pasos de configuración necesarios, se comprobó que era posible comunicarse con cualquiera de las máquinas, haciendo *ping*, tal y como se puede ver en la figura a continuación:

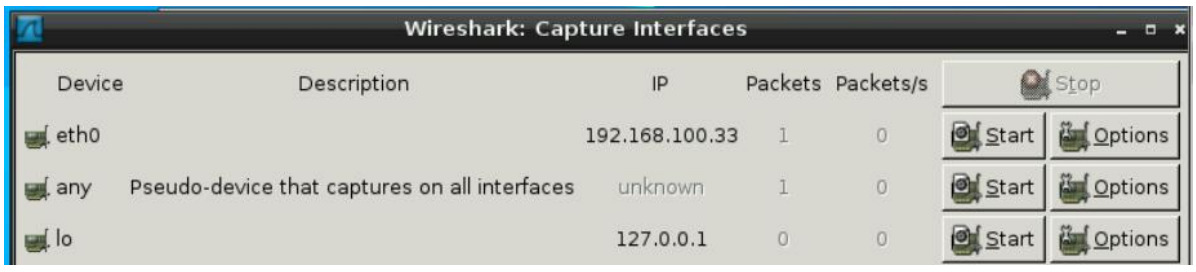


2. EJERCICIO 1

El primer ejercicio consistió en el uso de la herramienta WIRESHARK desde el equipo atacante, observador, para interceptar tráfico TELNET, HTTP y SSH entre los equipos legítimos. Esta herramienta es un *sniffer* y analizador de protocolos que recopila, analiza, extrae y presenta el contenido de los paquetes que fluyen por la red.

a. ACCIONES REALIZADAS Y RESULTADOS OBTENIDOS

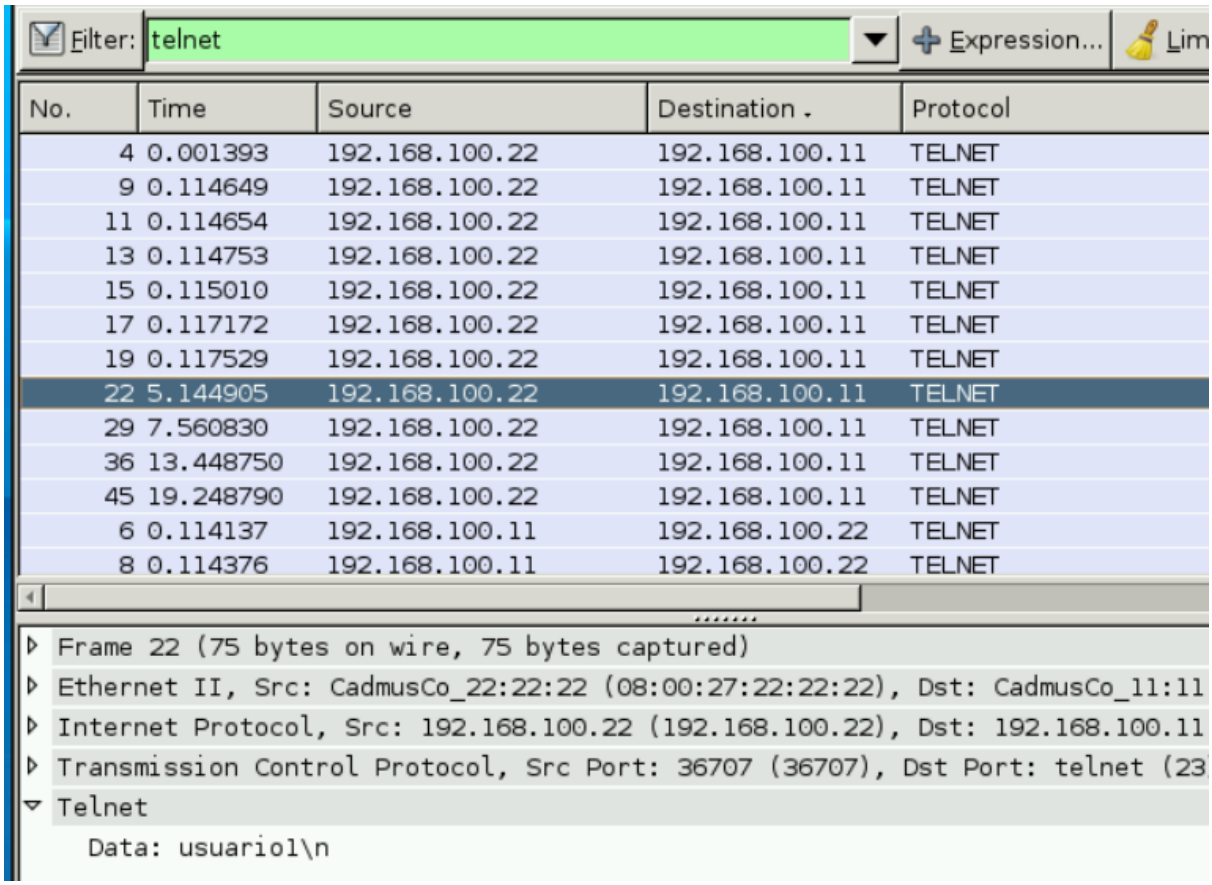
En primer lugar, se inició el entorno gráfico y se arrancó WIRESHARK, desde observador. A continuación, se inició la escucha de red utilizando la opción *Capture* del menú y haciendo click en *Interfaces*. Así, se pudo acceder al menú que se ve en la imagen adjuntada a continuación:



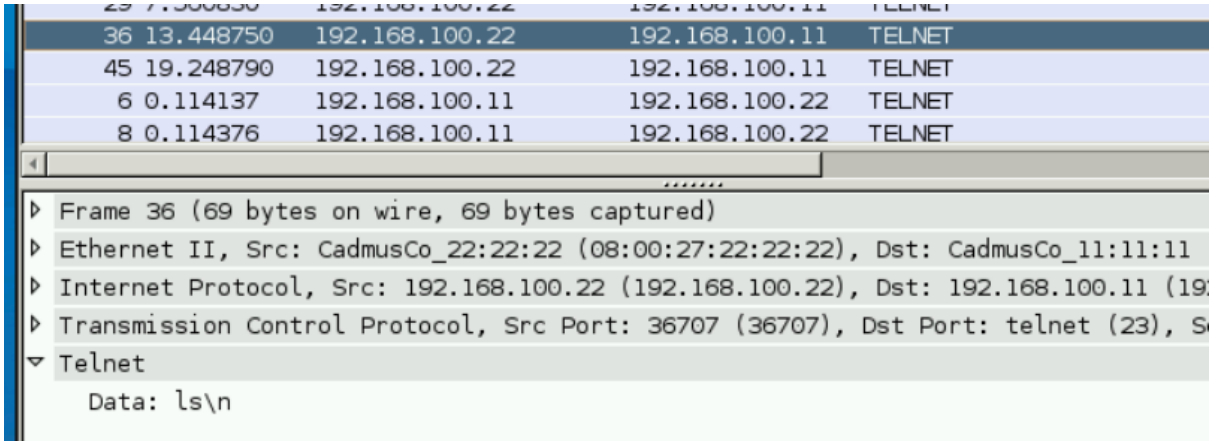
Llegados a este punto, fue necesario iniciar la escucha, haciendo click en el botón *Start* asociado a la interfaz eth0. Se comprobó el funcionamiento de la intercepción con los protocolos citados anteriormente.

i. TELNET

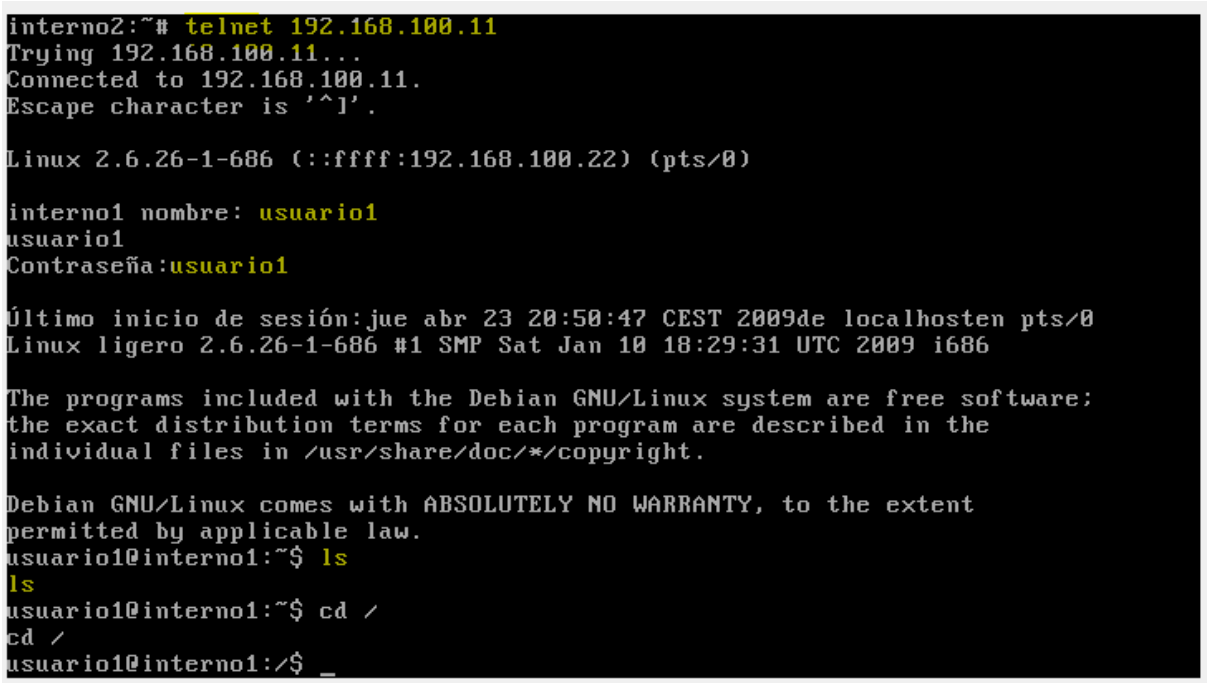
En primer lugar, se interceptaron paquetes de TELNET, desde interno2 hacia interno1, tal y como se pude observar en la imagen adjuntada a continuación:



Tal y como se puede ver en la imagen, no existe ningún tipo de encriptación o codificación que impida ver el contenido del mensaje, ya que se puede ver “Data: usuario1\n” sin ningún problema. Este protocolo no tiene protección de la información en ningún caso, lo que fue posible apreciar tanto al iniciar la conexión como al ejecutar comandos en la sesión TELNET, lo que se puede ver en la imagen siguiente:

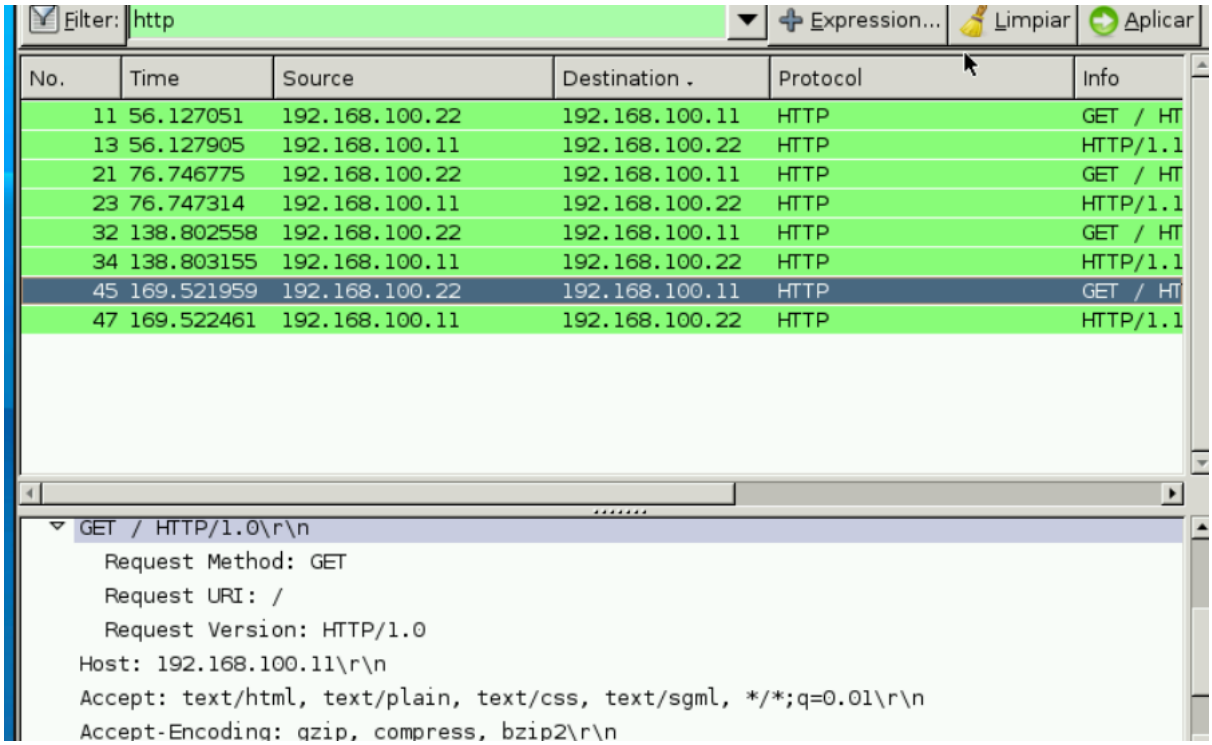


Por otra parte, desde la red interna, es decir: desde interno2 hacia interno1, se realizaron las siguientes acciones, reflejadas en las capturas previamente explicadas:



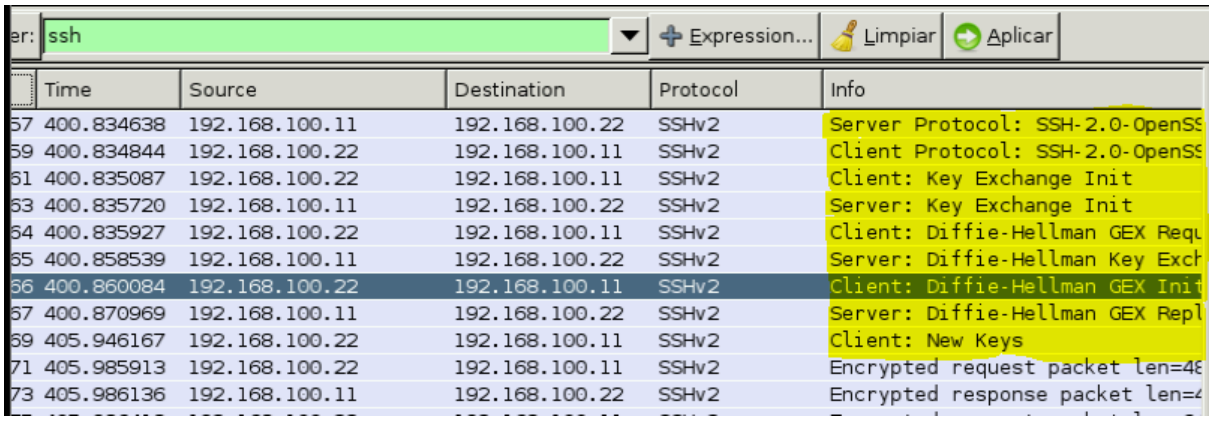
ii. HTTP

El segundo protocolo utilizado para realizar pruebas con WIRESHARK fue HTTP. Para ello fue necesario realizar una conexión web desde interno2 a interno1, utilizando un navegador en modo texto. Tal y como se puede ver en la imagen adjuntada a continuación, el mensaje no está ni cifrado ni encriptado, por lo que se puede leer claramente su contenido.



iii. SSH

Finalmente, se observaron los paquetes asociados a una conexión SSH. Esta conexión es segura, es decir: está encriptada. Es por ello que los pasos a realizar para obtener esta conexión serán distintos a los de los protocolos explicados previamente. En primer lugar, fue necesario realizar la conexión, lo que se hizo desde el equipo interno1 al equipo interno2. Los mensajes intercambiados fueron los siguientes y se explicarán con más detalle a continuación:



En primer lugar, se estableció el protocolo SSH a utilizar, en este caso: SSH-2.0-OpenSSH_5.11p1 Debian -5 por parte del servidor y del cliente, tal y como se puede ver en las imágenes adjuntadas a continuación:

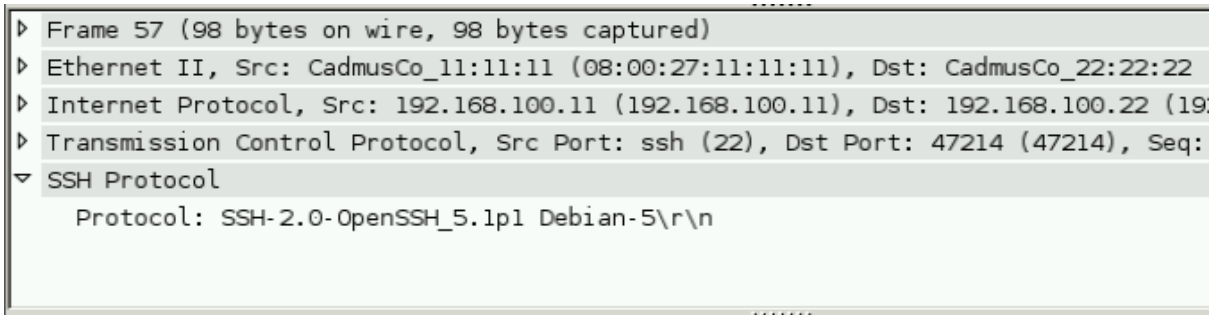


Ilustración 1 Servidor (interno1)

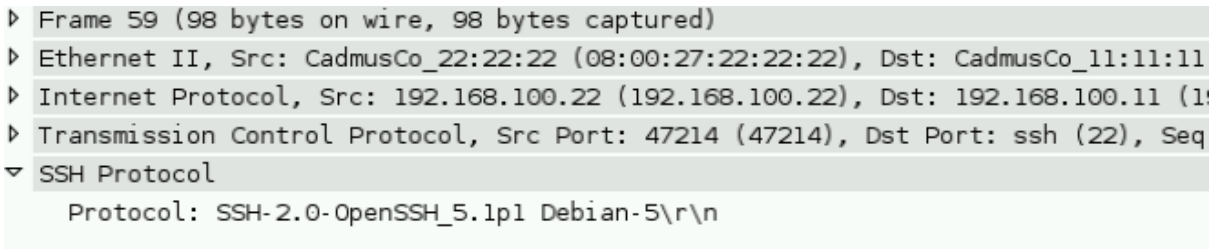
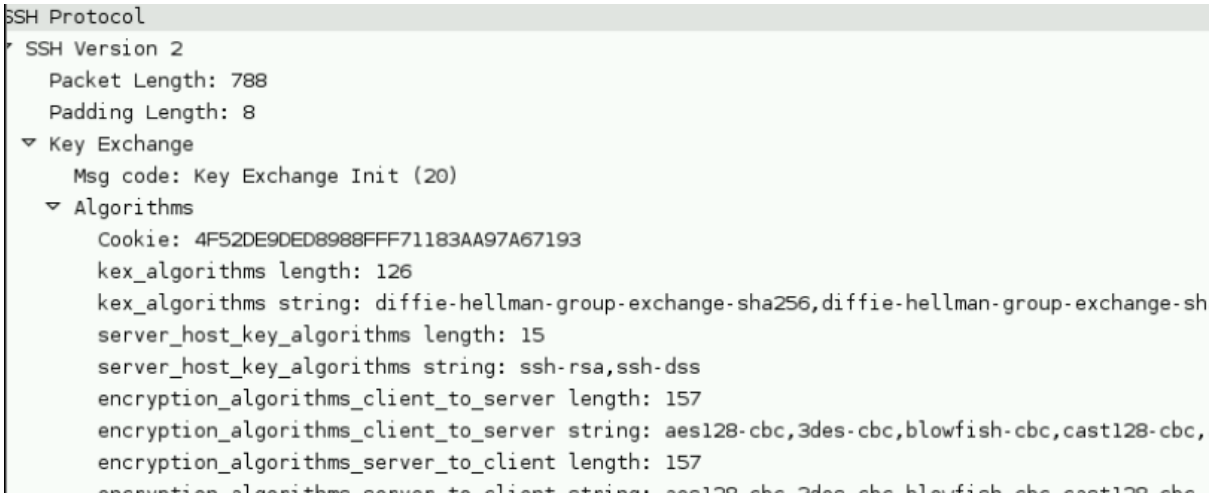
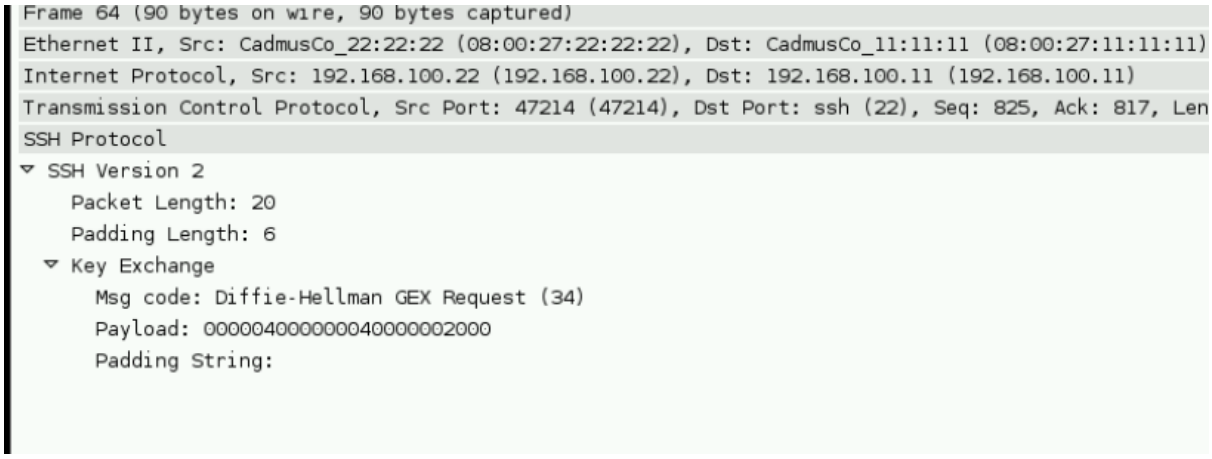


Ilustración 2 Cliente (interno2)

A continuación, tanto el cliente como el servidor inician el intercambio de claves. El contenido del mensaje en el cliente es el siguiente:

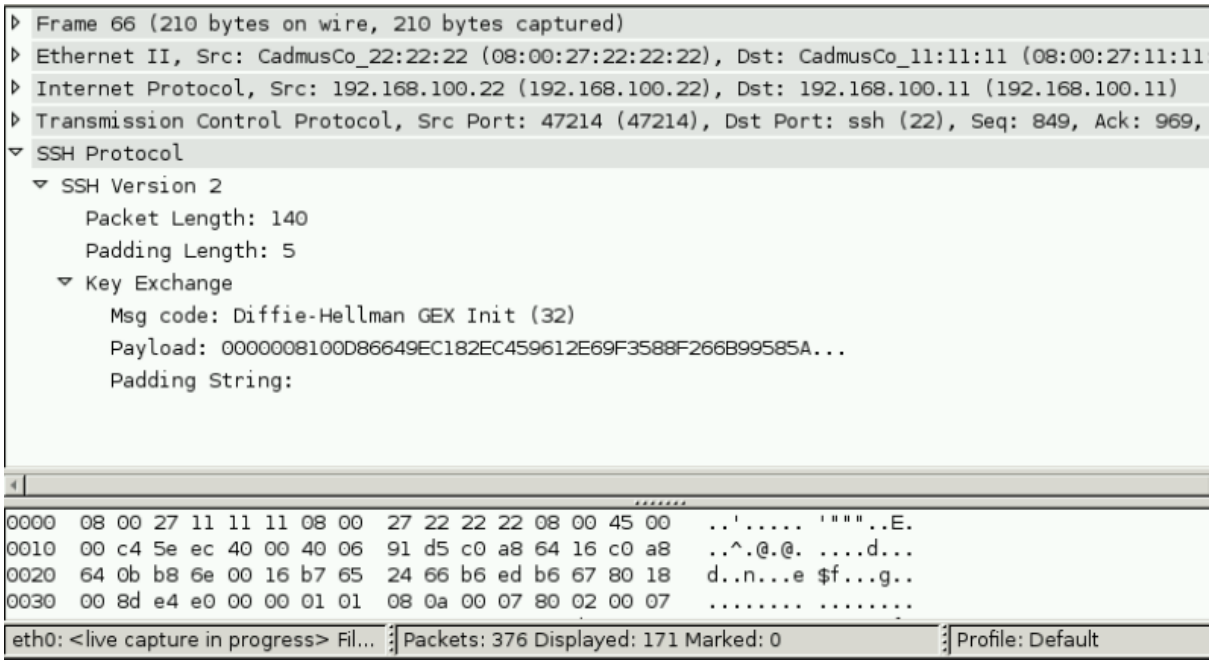


Para intercambiar claves, se utiliza Diffie-Hellman, tal y como se pude ver en la imagen de inicio de intercambio de claves en *kex_algorithms string*. En primer lugar, el cliente procede a realizar una petición de intercambio de grupo de Diffie-Hellman. Esto se puede ver en la imagen adjuntada a continuación:

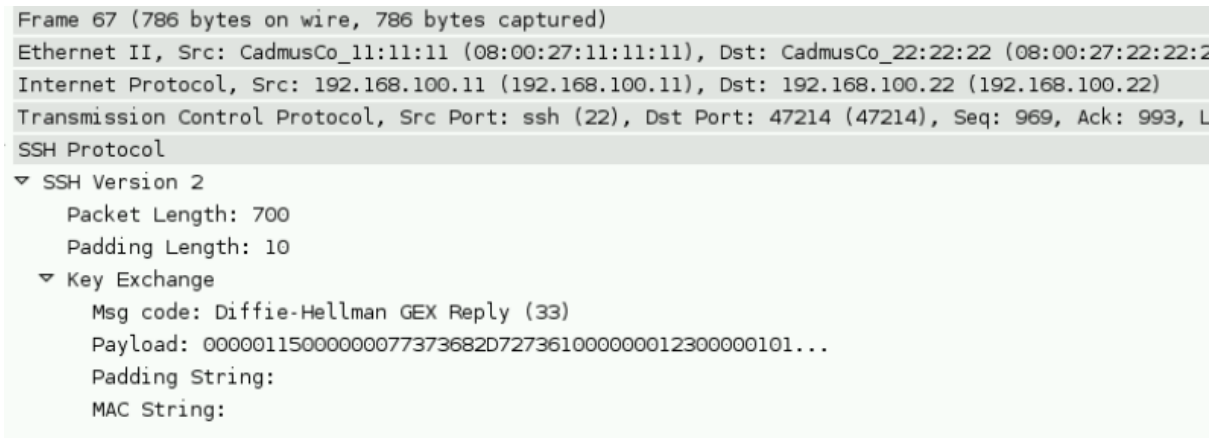


A continuación, el servidor responde a la petición:

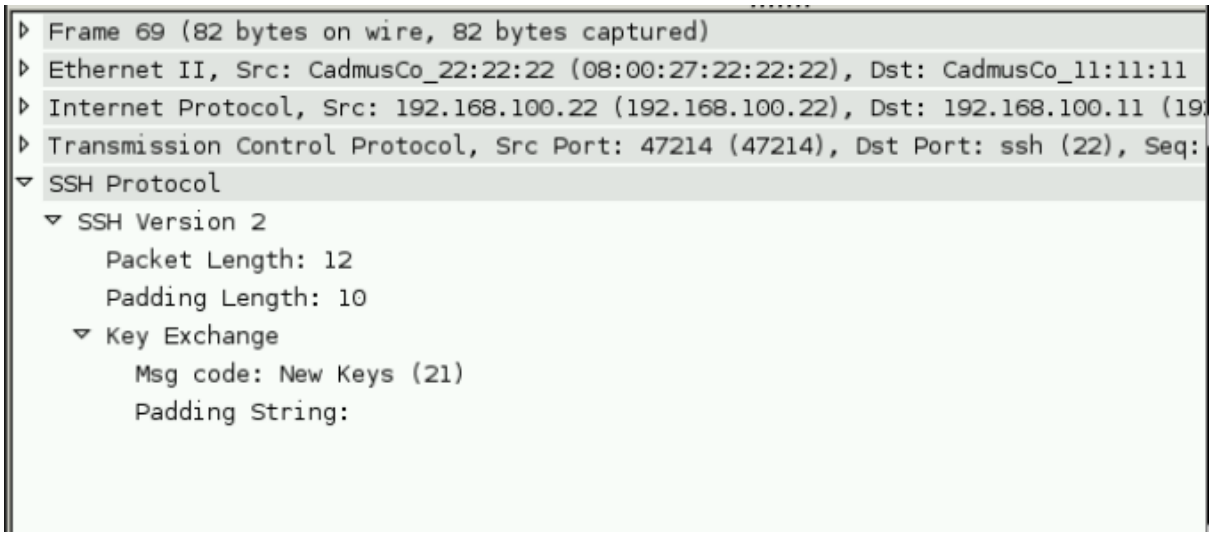
A continuación, se produce un mensaje de inicio intercambio de grupo Diffie-Hellman por parte del cliente, para generar las llaves definitivas para la comunicación:



Así pues, se produce una respuesta por parte del servidor y se generan las llaves definitivas a utilizar en la comunicación:



Finalmente, el cliente envía un mensaje asociado a las nuevas llaves:



Llegados a este punto, todos los mensajes enviados a continuación están cifrados y, por lo tanto, es imposible conocer su contenido a simple vista.

b. CONCLUSIONES GLOBALES

Así pues, tras realizar pruebas con los tres protocolos, es necesario hacer notar que tanto Telnet como HTTP no tienen mensajes encriptados. Esto provoca que sean vulnerables al uso de analizadores de tráfico de red. Es por ello se solo se debería utilizar SSH y la versión segura de HTTP (HTTPS) para comunicaciones, puesto que estos protocolos sí están encriptados y por lo tanto, no son vulnerables al uso de analizadores de tráfico de red.

3. EJERCICIO 2

Este ejercicio consistió en el uso de la herramienta de escaneo de puertos NMAP para obtener información de los equipos y servicios de la red.

a. ACCIONES REALIZADAS Y RESULTADOS OBTENIDOS

i. Escaneo tipo *Ping*

En primer lugar, se realizó un escaneado tipo *Ping*, con la opción -sP, para identificar las máquinas que componían la red. Tal y como se puede ver a continuación, las máquinas que componen la red son interno1, interno2 y observador.

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

Starting Nmap 4.62 ( http://nmap.org ) at 2017-12-24 11:30 CET
Host 192.168.100.11 appears to be up.
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)
Host 192.168.100.22 appears to be up.
MAC Address: 08:00:27:22:22:22 (Cadmus Computer Systems)
Host 192.168.100.33 appears to be up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 31.229 seconds
```

El escaneo no deja rastro en ninguno de los elementos escaneados, así que iniciamos el servidor inetutils-inetd para ello. Así pues, tal y como se puede ver en la imagen adjuntada, los últimos cambios realizados en el fichero de log son del día de la realización de la práctica (24 de diciembre):

```
interno2:~# tail /var/log/syslog
Dec 24 11:30:38 ligero dhclient: No DHCPOFFERS received.
Dec 24 11:30:38 ligero dhclient: No working leases in persistent database - slee
ping.
Dec 24 11:33:33 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 3
Dec 24 11:33:36 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 8
Dec 24 11:33:44 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 10
Dec 24 11:33:54 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 21
Dec 24 11:34:15 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 8
Dec 24 11:34:23 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 11
Dec 24 11:34:34 ligero dhclient: No DHCPOFFERS received.
Dec 24 11:34:34 ligero dhclient: No working leases in persistent database - slee
ping.
```

```
interno1:~# tail /var/log/syslog
Dec 24 11:29:23 ligero dhclient: No DHCPOFFERS received.
Dec 24 11:29:23 ligero dhclient: No working leases in persistent database - slee
ping.
Dec 24 11:32:32 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 4
Dec 24 11:32:36 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 4
Dec 24 11:32:40 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 8
Dec 24 11:32:48 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 15
Dec 24 11:33:03 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 20
Dec 24 11:33:23 ligero dhclient: DHCPDISCOVER on eth0 to 255.255.255.255 port 67
 interval 10
Dec 24 11:33:33 ligero dhclient: No DHCPOFFERS received.
Dec 24 11:33:33 ligero dhclient: No working leases in persistent database - slee
ping.
```

ii. Escaneo tipo *TCP connect*

A continuación, se realiza un escaneo tipo *TCP connect*, con el fin de determinar qué puertos están abiertos. Para interno1, se obtiene la siguiente información:

```
Scanning 192.168.100.11 [1 port]
Completed ARP Ping Scan at 11:38, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:38
Completed Parallel DNS resolution of 1 host. at 11:38, 13.00s elapsed
Initiating Connect Scan at 11:38
Scanning 192.168.100.11 [1715 ports]
Discovered open port 22/tcp on 192.168.100.11
Discovered open port 23/tcp on 192.168.100.11
Discovered open port 80/tcp on 192.168.100.11
Completed Connect Scan at 11:38, 1.16s elapsed (1715 total ports)
Host 192.168.100.11 appears to be up ... good.
Interesting ports on 192.168.100.11:
Not shown: 1712 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
23/tcp open  telnet
80/tcp open  http
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 14.255 seconds
           Raw packets sent: 1 (42B) | Rcvd: 1 (42B)
```

Tal y como se puede ver, esta máquina tiene abiertos tres puertos: 22, 23 y 80.

El rastro que queda en el log de interno1 es el siguiente. Tal y como se pude ver, se realiza un cambio a las 11:38, hora a la que se realizó el análisis.

```
Dec 24 11:33:33 ligero dhclient: No working leases in persistent database - slee
ping.
Dec 24 11:38:27 ligero telnetd[2142]: getpeername: Transport endpoint is not con
nected
```

Para interno2, realizando el mismo tipo de escaneo, se obtiene la siguiente información:

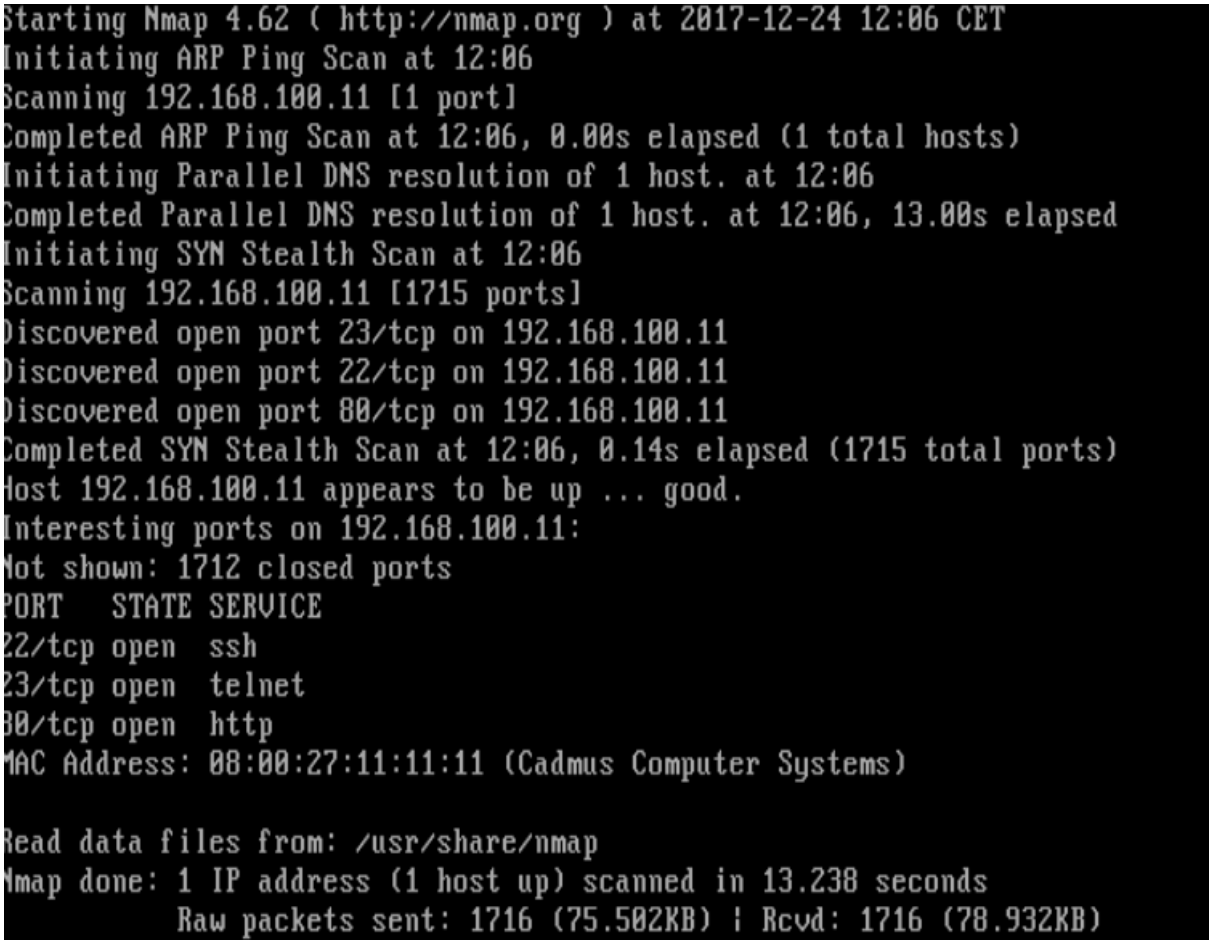
```
observador:~# nmap -sT -v 192.168.100.22

Starting Nmap 4.62 ( http://nmap.org ) at 2017-12-24 12:04 CET
Initiating ARP Ping Scan at 12:04
Scanning 192.168.100.22 [1 port]
Completed ARP Ping Scan at 12:04, 0.00s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 12:04
Completed Parallel DNS resolution of 1 host. at 12:04, 13.00s elapsed
Initiating Connect Scan at 12:04
Scanning 192.168.100.22 [1715 ports]
Discovered open port 22/tcp on 192.168.100.22
Completed Connect Scan at 12:04, 0.14s elapsed (1715 total ports)
Host 192.168.100.22 appears to be up ... good.
Interesting ports on 192.168.100.22:
Not shown: 1714 closed ports
PORT   STATE SERVICE
22/tcp open  ssh
MAC Address: 08:00:27:22:22:22 (Cadmus Computer Systems)

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 13.240 seconds
           Raw packets sent: 1 (42B) | Rcvd: 1 (42B)
```

Tal y como se puede ver, en este caso solo hay un puerto abierto. Lo que es consistente ya que de interno1 se habían abierto los puertos asociados a TELNET, HTTP y SSH, mientras que de interno2 solo estaba abierto SSH. El cambio asociado en el backlog a este escaneo, en interno2, es el siguiente:

```
Dec 24 12:04:48 ligero dhclient: No DHCPOFFERS received.
Dec 24 12:04:48 ligero dhclient: No working leases in persistent database - slee
ping.
```

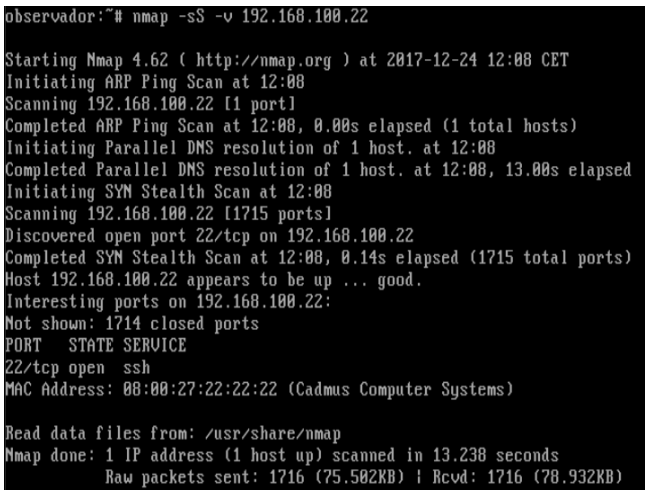
iii. Escaneo silencioso

A continuación, se repitió el escaneo de puertos, realizando un escaneo silencioso. Para interno1 se obtuvieron los siguientes resultados:



No se produce ningún cambio, el último mensaje, tras ejecutar *tail*, es el mismo que había previamente:

Para interno 2 se obtienen los mismos resultados



```
Dec 24 12:04:48 ligero dhclient: No DHCPOFFERS received.
Dec 24 12:04:48 ligero dhclient: No working leases in persistent database - slee
ping.
interno2:~#
```

iv. Escaneo para obtener información del sistema operativo y la versión concreta de los servicios activados

Para interno1 se obtienen las versiones concretas de los protocolos cuyos puertos tiene abiertos y además, se obtiene el sistema operativo, tal y como se puede ver a continuación:

```
observador:~# nmap -sT -O -sV 192.168.100.11

Starting Nmap 4.62 ( http://nmap.org ) at 2017-12-24 12:10 CET
Interesting ports on 192.168.100.11:
Not shown: 1712 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
23/tcp open  telnet  BSD-derived telnetd
80/tcp open  http    Apache httpd 2.2.9 ((Debian))
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-Port22-TCP:V=4.62%I=7%D=12/24%Time=5A3F8B39%P=i686-pc-linux-gnu%r(NULL,
SF:20,"SSH-2\.0-OpenSSH_5\.1p1\x20Debian-5\r\n");
MAC Address: 08:00:27:11:11:11 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.24
Uptime: 0.100 days (since Sun Dec 24 09:46:48 2017)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 21.653 seconds
```

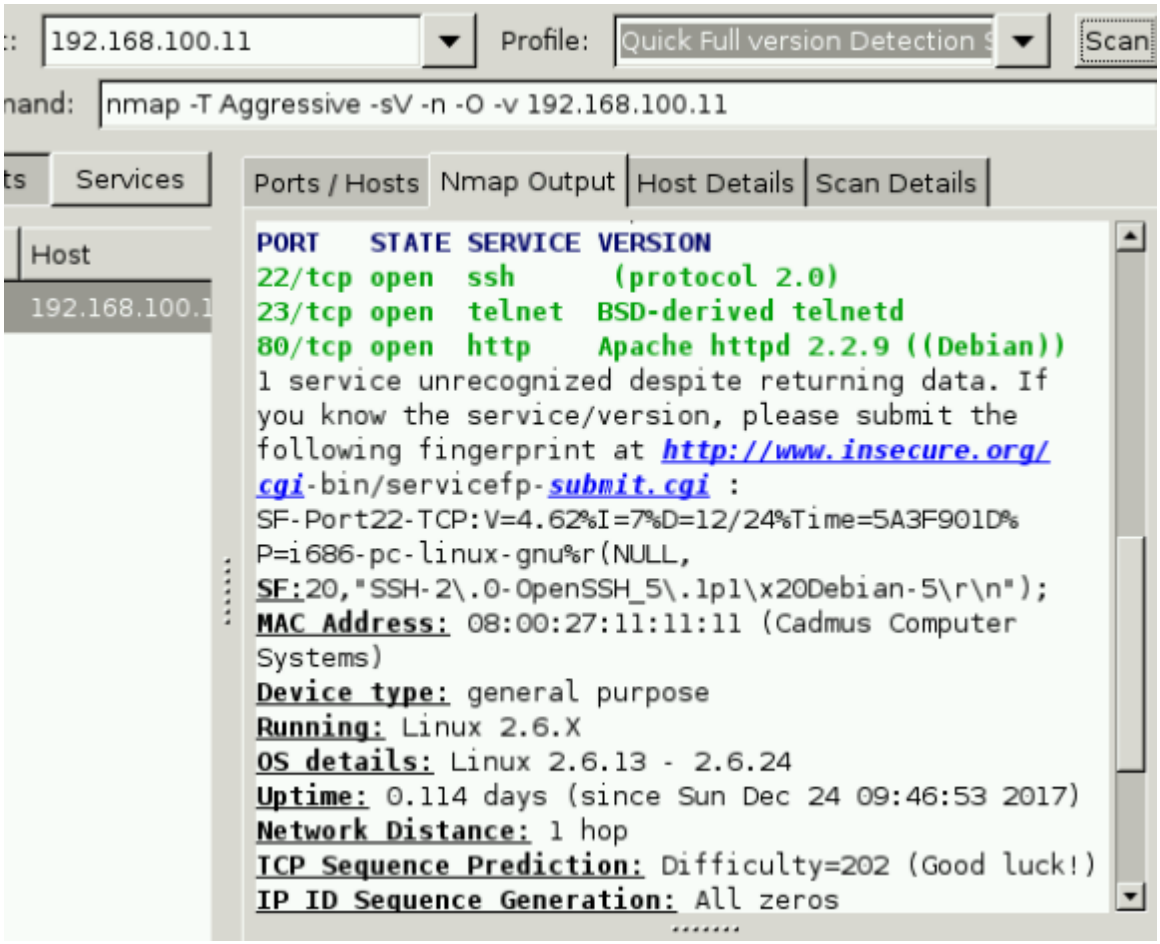
Esto es peligroso ya que cabe la posibilidad de que haya vulnerabilidades conocidas asociadas a una versión concreta de software y, si es posible ver detalladamente la versión de cada uno de los protocolos o sistema operativo, cabe la posibilidad de que esta se explote.

Para interno2 se obtuvo el mismo tipo de informació:

```
observador:~# nmap -sT -O -sV 192.168.100.22

Starting Nmap 4.62 ( http://nmap.org ) at 2017-12-24 12:15 CET
Interesting ports on 192.168.100.22:
Not shown: 1714 closed ports
PORT   STATE SERVICE VERSION
22/tcp open  ssh     (protocol 2.0)
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-Port22-TCP:V=4.62%I=7%D=12/24%Time=5A3F8C47%P=i686-pc-linux-gnu%r(NULL,
SF:20,"SSH-2\.0-OpenSSH_5\.1p1\x20Debian-5\r\n");
MAC Address: 08:00:27:22:22:22 (Cadmus Computer Systems)
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.13 - 2.6.24
Uptime: 0.104 days (since Sun Dec 24 09:45:38 2017)
Network Distance: 1 hop

OS and Service detection performed. Please report any incorrect results at http:
//nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.574 seconds
observador:~#
```

v. Interfaz gráfico para NMAP

La GUI permite obtener la misma información que a través de línea de comandos, pero presentada de forma más cómoda y legible.



b. CONCLUSIONES GLOBALES

En primer lugar, es necesario hacer notar que no se deberían abrir más puertos de los necesarios. Al realizar el análisis de puertos es posible observar el estado y, si un puerto que no debería estar abierto, lo está, se puede producir un fallo de seguridad. Así pues, como medida de seguridad básica, no se debería abrir ningún puerto que no sea necesario.

Como medida de seguridad más avanzada, es recomendable establecer un cortafuegos para evitar que se ejecute el comando sobre la red. Sin embargo, si el cortafuegos presenta vulnerabilidades, existe la posibilidad de que un usuario experimentado utilice Nmap para evadir estos cortafuegos, ya que Nmap tiene herramientas para ello.

REFERENCIAS

- NMAP.ORG, https://nmap.org. [Visitado por última vez: 24/12/2017]