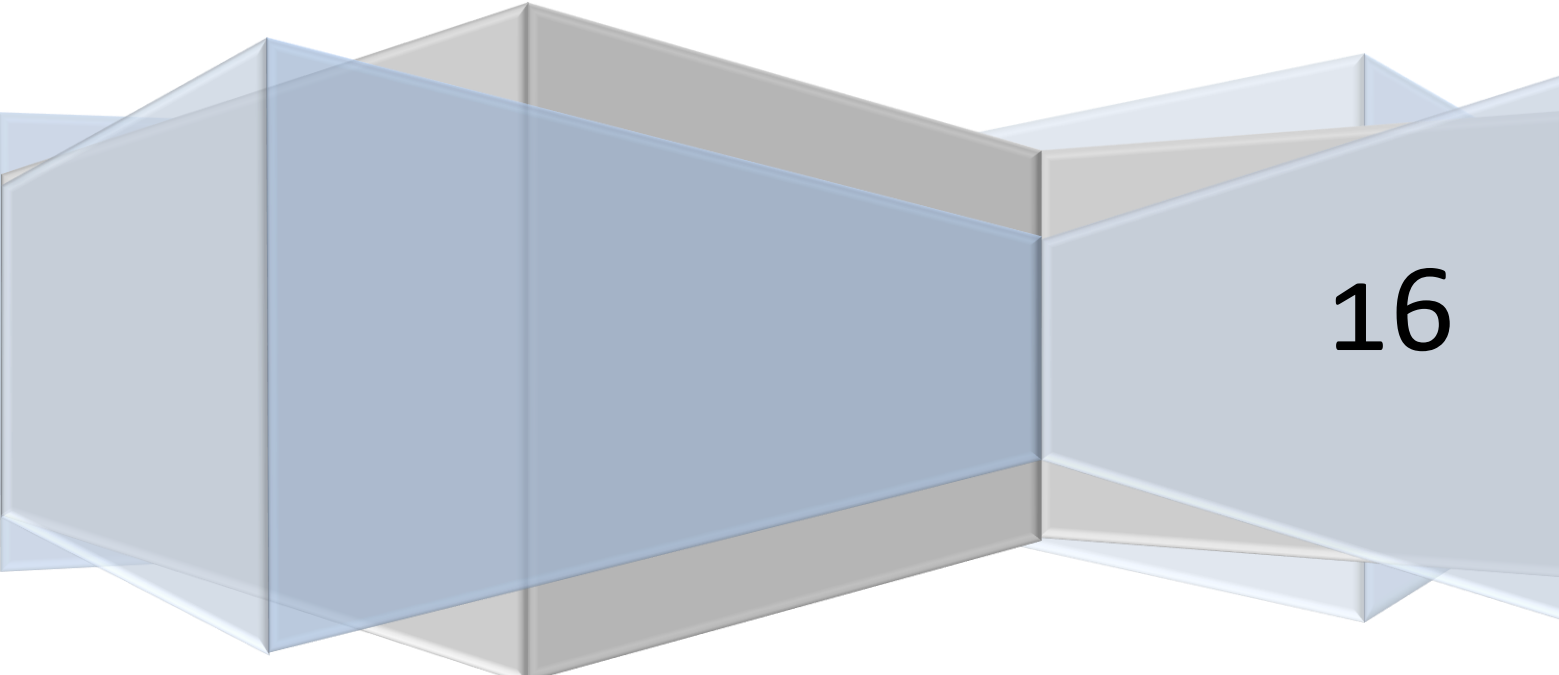


# SEGURIDAD INFORMÁTICA

## Práctica 2

**Jorge Andrés Galindo - 679155**

**Javier Aranda García - 679184**



16

## Parte I: Extracción de información

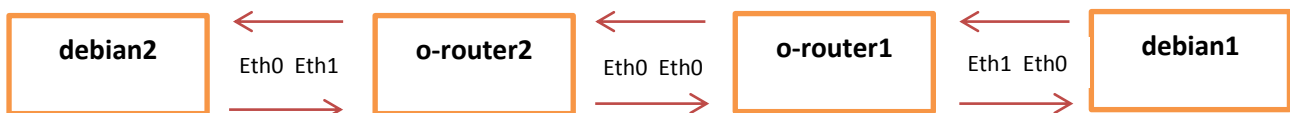
---

En esta primera parte de la práctica, mediante herramientas de líneas de comandos, se va a obtener información de red de las 4 máquinas virtuales proporcionadas. Para ello, en primer lugar, se localizó los ficheros de interfaces, que al ser máquinas Debian y OpenBSD, se encontraban en distintos lugares:

- Debian: /etc/network/interfaces
- OpenBSD: /etc/hostname.em0 y /etc/hostname.em1

Posteriormente, abriendo los distintos ficheros de los interfaces, se obtuvo la información de la ip de cada uno:

- debian1
  - ip: 192.168.200.2
    - netmask: 255.255.255.0
    - gateway: 192.168.200.1
- debian2
  - ip: 192.168.201.2
    - netmask: 255.255.255.0
    - gateway: 192.168.201.1
- o-router1
  - ip:192.168.200.1 (eth1)
    - netmask: 255.255.255.0
    - gateway: 0
  - ip:192.168.100.1 (eth0)
    - netmask: 255.255.255.0
    - gateway: 0
- o-router2
  - ip: 192.168.201.1 (eth1)
    - netmask: 255.255.255.0
    - gateway: 0
  - ip: 192.168.100.2 (eth0)
    - netmask: 255.255.255.0
    - gateway: 0



Para comprobar definitivamente que estas eran las interfaces de cada una de las máquinas, se ejecutó el comando “ifconfig” pasando su salida al comando “less” para poder ver el resultado entero por pantalla. Al ejecutarlo, se pudieron ver en cada una de las máquinas las distintas interfaces, así como su máscara de red y la dirección de “broadcast”.

A continuación, se obtuvo la “IP routing table” mediante el comando “netstat -rn”, consiguiendo los siguientes resultados:

- debian1:

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
0.0.0.0	192.168.200.1	0.0.0.0	UG	0	0	0	eth0
192.168.200.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

En la tabla se puede ver que, los paquetes que corresponden la dirección ip 192.168.200.0 con su correspondiente máscara, van al gateway por defecto por la interfaz 0 (indicado con 0.0.0.0). Sin embargo, los paquetes que no coinciden con la ip nombrada, son mandados también por la interfaz 0, pero en este caso, al gateway con dirección ip 192.168.200.1.

- debian2:

Kernel IP routing table							
Destination	Gateway	Genmask	Flags	MSS	Window	irtt	Iface
0.0.0.0	192.168.201.1	0.0.0.0	UG	0	0	0	eth0
192.168.201.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0

En el caso de la máquina “debian2” ocurre algo similar, salvo porque al encaminador por defecto van los paquetes con ip 192.168.201.0 (con su respectiva máscara), y el resto son mandados al encaminador 192.168.201.1.

- o-router1:

192.168.100/24	192.168.100.1	UC	1	3	—	4	em0
192.168.100.1	08:00:27:ad:9f:05	UHL1	0	2	—	1	em0
192.168.100.2	08:00:27:2e:1d:71	UHLc	1	5	—	4	em0
192.168.100.255	192.168.100.1	UHb	0	0	—	1	em0
192.168.200/24	192.168.200.1	UC	1	0	—	4	em1
192.168.200.1	08:00:27:d5:8b:04	UHL1	0	4	—	1	em1
192.168.200.2	08:00:27:ca:92:77	UHLc	0	6	—	4	em1
192.168.200.255	192.168.200.1	UHb	0	0	—	1	em1

En la máquina “o-router1”, al ser “openBSD”, la tabla tiene un formato distinto. Los paquetes que corresponden con la dirección ip 192.168.100.0 (mediante la máscara), tienen como dirección la del gateway 192.168.100.1 a través de la interfaz 1. Sin embargo, por la interfaz 2, son mandados los paquetes que coinciden con 192.168.200.0 al gateway con dirección ip 192.168.200.1.

- o-router2:

192.168.100/24	192.168.100.2	UC	1	3	—	4	em0
192.168.100.1	08:00:27:ad:9f:05	UHLc	1	5	—	4	em0
192.168.100.2	08:00:27:2e:1d:71	UHL1	0	2	—	1	em0
192.168.100.255	192.168.100.2	UHb	0	0	—	1	em0
192.168.201/24	192.168.201.1	UC	1	0	—	4	em1
192.168.201.1	08:00:27:df:b7:62	UHL1	0	6	—	1	em1
192.168.201.2	08:00:27:43:fc:b0	UHLc	0	6	—	4	em1
192.168.201.255	192.168.201.1	UHb	0	0	—	1	em1

Finalmente, de igual modo que la máquina “o-router2”, la tabla muestra que los paquetes con ip que coincide con 192.168.100.0 son mandados mediante la intefaz 0 al encaminador 192.168.100.2. Los que corresponden con 192.168.201.0 por la interfaz 1 a su respectivo gateway.

Además, cabe comentar que se utilizó el comando “netstat –ap”, que mostraba las conexiones abiertas en cada puerto, pero no se va a comentar nada de ello en este punto de la práctica, ya que posteriormente se realizará un escaneo de los puertos en todas las máquinas.

Posteriormente, se utilizó el comando “ping” para saber a qué máquinas se podía acceder desde una dada, siguiendo la siguiente sintaxis:

ping <dirección ip>

Y finalmente se consiguieron los siguientes resultados:

- debian1:
  - ping 192.168.200.2 (ping a si misma): respuesta satisfactoria.
  - ping 192.168.200.1 (ping a o-router1): respuesta satisfactoria.
  - ping 192.168.100.2 (ping a o-router2): respuesta satisfactoria.
  - ping 192.168.201.2 (ping a debian2): respuesta satisfactoria.
- o-router1:
  - ping 192.168.200.2 (ping a debian1): respuesta satisfactoria.
  - ping 192.168.200.1 (ping a si misma): respuesta satisfactoria.
  - ping 192.168.100.2 (ping a o-router2): respuesta satisfactoria.
  - ping 192.168.201.2 (ping a debian2): respuesta satisfactoria.
- o-router2:
  - ping 192.168.200.2 (ping a debian1): respuesta satisfactoria.
  - ping 192.168.200.2 (ping a debian2): respuesta satisfactoria.
  - ping 192.168.100.1 (ping a o-router1): respuesta satisfactoria.
  - ping 192.168.201.1 (ping a si misma): respuesta satisfactoria.
- debian2:
  - ping 192.168.201.1 (ping a o-router2): respuesta satisfactoria.
  - ping 192.168.100.1 (ping a o-router1): respuesta satisfactoria.
  - ping 192.168.200.2 (ping a o-debian1): respuesta satisfactoria.
  - ping 192.168.201.2 (ping a si misma): respuesta satisfactoria.

Para obtener información detallada de las rutas que sigue un paquete, y comprobar además que las direcciones ip de las distintas interfaces obtenidas eran las correctas, se utilizó el comando “traceroute”. Debido a que son cuatro máquinas, y las rutas disponibles ya se han mostrado con el comando ping, se va a mostrar tan solo la salida obtenida al mandar un paquete de debian1 a debian2 y viceversa.

```
traceroute to 192.168.201.2 (192.168.201.2), 30 hops max, 60 byte packets
 1  192.168.200.1 (192.168.200.1)  0.360 ms  0.478 ms  0.440 ms
 2  192.168.100.2 (192.168.100.2)  0.654 ms  0.646 ms  0.614 ms
 3  192.168.201.2 (192.168.201.2)  1.046 ms  1.044 ms  1.037 ms
```

En la imagen se ve el camino que sigue un paquete mandado desde debian1 a debian2, siguiendo los siguientes pasos:

debian1	o-router1	o-router2	debian2
192.168.200.2	192.168.200.1	192.168.100.2	192.168.201.2
eth0	eth1	eth0	eth0

```

traceroute to 192.168.200.2 (192.168.200.2), 30 hops max, 60 byte packets
 1  192.168.201.1 (192.168.201.1)  0.315 ms  0.291 ms  0.278 ms
 2  192.168.100.1 (192.168.100.1)  0.757 ms  0.747 ms  0.737 ms
 3  192.168.200.2 (192.168.200.2)  1.129 ms  1.120 ms  1.107 ms

```

Y en esta imagen, se aprecia el camino inverso; es decir, desde debian1 a debian2.

debian2	o-router2	o-router1	debian1
192.168.201.2	192.168.201.1	192.168.100.1	192.168.200.2
eth0	eth1	eth0	eth0

Como último punto de este apartado de la práctica, se ha procedido al escaneo de los puertos de todas las máquinas. Para ello, se ha utilizado el comando “nmap” visto ya en la anterior práctica de la asignatura. La sintaxis concreta utilizada ha sido la siguiente:

```
nmap -p 1-65535 -T4 -A -v <dirección ip>
```

En este comando se indica mediante parámetros lo siguiente:

- -p: se deben escanear todos los puertos en el rango 1-65535.
- -T4: hace que el escaneo sea más rápido ya que indica que se encuentra en una red rápida y fiable.
- -A: hace que detecte el sistema operativo de la máquina y que realice un análisis de versiones.
- -v: se muestra mayor información por pantalla.
- -<dirección ip>: dirección ip de la máquina a escanear.

A continuación se muestran los resultados obtenidos al usar el comando desde debian2 al resto de máquinas.

- o-router2:

```

Not shown: 65534 closed ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.3 (protocol 2.0)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)

```

Se puede apreciar que la máquina “o-router2” únicamente tiene abierto el puerto 22, en el que se está ejecutando un servicio ssh (en concreto la versión 7.3).

- o-router1:

```

Not shown: 63480 closed ports, 2054 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.3 (protocol 2.0)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)

```

En cuanto a “o-router1”, puede observarse que se trata del mismo caso que “o-router2”, únicamente se tiene el servicio ssh en el puerto 22, sin embargo, “o-router1” tiene 2054 puertos abiertos en lugar de solamente 1.

- Debian1:

```

Not shown: 63559 closed ports, 1972 filtered ports
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 6.7p1 Debian 5+deb8u3 (protocol 2.0)
|_ssh-hostkey: ERROR: Script execution failed (use -d to debug)
80/tcp    open  http      nginx 1.6.2
|_http-methods: No Allow or Public header in OPTIONS response (status code 405)
|_http-title: Welcome to nginx on Debian!
111/tcp   open  rpcbind  2-4 (RPC #100000)
|_rpcinfo:
|   program version  port/proto  service
|   100000  2,3,4      111/tcp    rpcbind
|   100000  2,3,4      111/udp    rpcbind
|   100024  1          48452/tcp  status
|_  100024  1          50320/udp  status
48452/tcp open  status  1 (RPC #100024)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

```

Como se puede apreciar en la imagen, “debian1” tiene 1972 puertos abiertos. Entre estos puertos tiene software escuchando en los puertos 22 (ssh), 80(http), 111 (rpcbind) y 48452 en el que se encuentra corriendo un servicio de información sobre el estado del sistema operativo.

Además, se han realizado más escaneos distintos desde la máquina “debian2” al resto:

Sondeo TCP ACK: se utiliza para mapear reglas de cortafuegos, y para determinar si son cortafuegos con inspección de estados y qué puertos están filtrados (“nmap -sA”):

- Debian1: se han escaneado 1000 puertos y ninguno se filtra.

```

root@debian2:~# nmap -sA 192.168.200.2

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-29 11:10 CEST
Nmap scan report for 192.168.200.2
Host is up (0.00051s latency).
All 1000 scanned ports on 192.168.200.2 are unfiltered
Nmap done: 1 IP address (1 host up) scanned in 17.04 seconds

```

- o-router1: se han escaneado 1000 puertos y ninguno se filtra.

```

root@debian2:~# nmap -sA 192.168.200.1

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-29 11:11 CEST
Nmap scan report for 192.168.200.1
Host is up (0.00035s latency).
All 1000 scanned ports on 192.168.200.1 are unfiltered
Nmap done: 1 IP address (1 host up) scanned in 57.64 seconds

```

- o-router2: se han escaneado 1000 puertos y ninguno se filtra.

```

root@debian2:~# nmap -sA 192.168.201.1

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-29 11:13 CEST
Nmap scan report for 192.168.201.1
Host is up (0.00069s latency).
All 1000 scanned ports on 192.168.201.1 are unfiltered
MAC Address: 08:00:27:DF:B7:62 (Cadmus Computer Systems)
Nmap done: 1 IP address (1 host up) scanned in 14.46 seconds

```

Sondeo de protocolo IP: permite determinar qué protocolos (TCP, ICMP...) soportan los sistemas objetivo. No es un sondeo de puertos, ya que lo que cambia los números de protocolo IP en lugar de los números de puerto TCP o UDP ("nmap -sO).

- Debian1: se han encontrado 246 protocolos cerrados y una serie de protocolos abiertos o filtrados.

```
root@debian2:~# nmap -sO 192.168.200.2

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-29 11:17 CEST
Warning: 192.168.200.2 giving up on port because retransmission cap hit (10).
Nmap scan report for 192.168.200.2
Host is up (0.0011s latency).
Not shown: 246 closed protocols
PROTOCOL STATE      SERVICE
1      open      icmp
2      open|filtered igmp
6      open      tcp
17     open      udp
55     open|filtered mobile
58     open|filtered ipv6-icmp
103    open|filtered pim
112    open|filtered vrrp
118    open|filtered stp
136    open|filtered udplite

Nmap done: 1 IP address (1 host up) scanned in 303.58 seconds
```

- o-router1: en esta máquina, al contrario que en "debian1", se han encontrado más protocolos soportados, y 241 cerrados.

```
root@debian2:~# nmap -sO 192.168.200.1

Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-29 11:25 CEST
Nmap scan report for 192.168.200.1
Host is up (0.0055s latency).
Not shown: 241 closed protocols
PROTOCOL STATE      SERVICE
1      open      icmp
2      open|filtered igmp
4      open|filtered ip
6      open      tcp
17     open      udp
41     open|filtered ipv6
47     open|filtered gre
50     open|filtered esp
51     open|filtered ah
55     open|filtered mobile
58     open|filtered ipv6-icmp
97     open|filtered etherip
112    open|filtered vrrp
137    open|filtered mpls-in-ip
240    open|filtered unknown

Nmap done: 1 IP address (1 host up) scanned in 20.22 seconds
```

- o-router2: se han obtenido exactamente los mismos resultados que en “o-router1”.

```
Starting Nmap 6.47 ( http://nmap.org ) at 2016-10-29 11:27 CEST
Nmap scan report for 192.168.201.1
Host is up (0.030s latency).
Not shown: 241 closed protocols

```

PROTOCOL	STATE	SERVICE
1	open	icmp
2	open filtered	igmp
4	open filtered	ip
6	open	tcp
17	open	udp
41	open filtered	ipv6
47	open filtered	gre
50	open filtered	esp
51	open filtered	ah
55	open filtered	mobile
58	open filtered	ipv6-icmp
97	open filtered	etherip
112	open filtered	vrrp
137	open filtered	mpls-in-ip
240	open filtered	unknown

```
MAC Address: 08:00:27:DF:B7:62 (Cadmus Computer Systems)

Nmap done: 1 IP address (1 host up) scanned in 20.23 seconds
```



## Parte II: Política de seguridad con cortafuegos

---

En esta parte, se ha modificado el fichero “/etc/pf.conf” para crear una política de cortafuegos en la maquina “o-router1”, mediante la cual se va denegar el acceso al servicio ssh de algunas máquinas. Para indicar la política a seguir en el fichero “pf.conf” se ha usado la siguiente sintaxis:

pass/block in/out quick on <interfaz> <protocolo> from <ip> to <ip> port <puerto>

- pass/block: se indica si se debe dejar pasar el paquete o bloquearlo.
- in/out: se indica si el paquete sobre el que se debe actuar está entrando o saliendo del “interfaz” indicado.
- quick: indica que en cuanto algún paquete coincida con lo indicado en la línea no se compare con el resto de indicaciones.
- protocolo: indica el protocolo que se usará.
- from y to: se indica de que dirección ip procede la petición y a qué dirección se dirige mediante respectivamente (any si no importa la dirección).
- port: puerto al que está dirigido el paquete.

Con todo esto en cuenta se ha modificado el fichero “pf.conf” añadiendo las siguientes líneas:

```
#Bloquea todo el trafico desde Debian1 a o-router2
block in quick on em1 proto tcp from 192.168.200.2 to 192.168.100.2 port ssh
block in quick on em1 proto tcp from 192.168.200.2 to 192.168.201.1 port ssh
#Bloquea todo el trafico desde Debian2 a o-router1
block in quick on em0 proto tcp from 192.168.201.2 to 192.168.200.1 port ssh
block in quick on em0 proto tcp from 192.168.201.2 to 192.168.100.1 port ssh
#Bloquea trafico de o-router1 a Debian2 y o-router2
block out quick on em0 proto tcp from 192.168.100.1 to any port ssh
#Bloquea todo el trafico procedente de o-router2
block in quick on em0 proto tcp from 192.168.100.2 to any port ssh
pass in all
```

Una vez añadidas estas líneas, se ha usado el comando “pfctl -f /etc/pf.conf” que carga las nuevas indicaciones que se han añadido al fichero. De este modo, se ha bloqueado el acceso de algunas máquinas al servicio ssh de otras. Además, se ha incluido al final la línea “pass in all” que permite que los paquetes que no cumplan las demás indicaciones puedan pasar el firewall.

Finalmente se han comprobado todas las conexiones entre las máquina, obteniendo resultados satisfactorios al cumplirse todas las políticas de firewall indicadas:

- En debian2:
  - ssh user@192.168.200.2: acceso permitido (ssh de debian2 a debian1).
  - ssh user@192.168.200.1: acceso denegado (ssh de debian2 a o-router1).
  - ssh user@192.168.201.1: acceso permitido (ssh de debian2 a o-router2).
- En debian1:
  - ssh user@192.168.201.2: acceso permitido (ssh de debian1 a debian2).
  - ssh user@192.168.100.1: acceso permitido (ssh de debian1 a o-router1).

- ssh user@192.168.100.2: acceso denegado (ssh de debian1 a o-router2).
- En o-router2:
  - ssh user@192.168.200.1: acceso denegado (ssh de o-router2 a o-router1).
  - ssh user@192.168.200.2: acceso denegado (ssh de o-router2 a debian1).
  - ssh user@192.168.201.2: acceso permitido (ssh de o-router2 a debian2).