

NOMBRE	APELLIDOS	DNI
Laura	Ramos Martinez	03201266B

GRUPO: \_\_\_\_\_

- En nuestro caso, lo vamos a emplear para determinar víctimas potenciales. Abra un terminal y ejecute la orden `nmap -F 192.168.0.0/24`  
A partir de la salida de esta orden, indique a continuación las direcciones IP de los equipos conectados en la red:

```

Applications  Places  Tue 9 Mar, 11:51  VNX
Terminal
Use the command line
vnx@Atacante: ~
File Edit View Search Terminal Help

Nmap scan report for 192.168.0.2
Host is up (0.00025s latency).
Not shown: 99 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 02:FD:00:00:00:01 (Unknown)

Nmap scan report for 192.168.0.4
Host is up (0.00016s latency).
Not shown: 95 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
23/tcp    open  telnet
53/tcp    open  domain
111/tcp   open  rpcbind
2049/tcp  open  nfs
MAC Address: 02:00:00:90:F8:EA (Unknown)

Nmap scan report for 192.168.0.3
Host is up (0.0000020s latency).
All 100 scanned ports on 192.168.0.3 are closed

Nmap done: 256 IP addresses (4 hosts up) scanned in 28.03 seconds

vnx@Atacante: ~

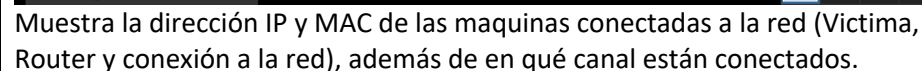
```

- Una vez hayan arrancado, sitúese en el equipo “VÍCTIMA” (diríjase a la consola o ábrala directamente desde *virt-manager*). Ejecute la siguiente orden para consultar su caché arp  
`$sudo arp -na`

```

vnx@Victima: ~
64 bytes from 192.168.0.2: icmp_req=2 ttl=64 time=0.034 ms
64 bytes from 192.168.0.2: icmp_req=3 ttl=64 time=0.035 ms
64 bytes from 192.168.0.2: icmp_req=4 ttl=64 time=0.039 ms
^C
--- 192.168.0.2 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 2997ms
rtt min/avg/max/mdev = 0.034/0.047/0.082/0.021 ms
vnx@Victima:~$ ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data.
64 bytes from 192.168.0.3: icmp_req=1 ttl=64 time=0.878 ms
64 bytes from 192.168.0.3: icmp_req=2 ttl=64 time=1.15 ms
64 bytes from 192.168.0.3: icmp_req=3 ttl=64 time=1.01 ms
64 bytes from 192.168.0.3: icmp_req=4 ttl=64 time=0.952 ms
64 bytes from 192.168.0.3: icmp_req=5 ttl=64 time=0.948 ms
64 bytes from 192.168.0.3: icmp_req=6 ttl=64 time=1.03 ms
^C
--- 192.168.0.3 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5007ms
rtt min/avg/max/mdev = 0.878/0.997/1.153/0.092 ms
vnx@Victima:~$ sudo arp -na
[sudo] password for vnx:
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
? (192.168.0.1) at 02:fd:00:00:02:01 [ether] on eth1
vnx@Victima:~$

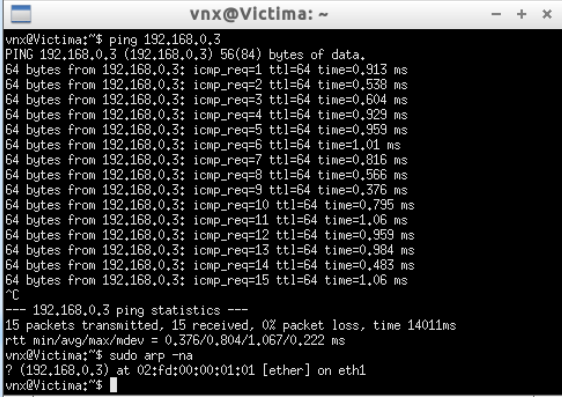
```



- [illegible]

Este par de ordenes hace que el equipo victima mande los paquetes al Atacante (pensando que es el router) y el router acepte estos paquetes del Atacante (pensando que son inalterados de la victima). Esto sitúa al equipo atacante entre los dos dispositivos (victima y router) dando la opción de visualizar, modificar o interceptar los paquetes.

5. En estos momentos, el envenenamiento estaría teniendo lugar. Vamos a **comprobar si está o no funcionando**. Para ello, consulte de nuevo la caché ARP de los equipos víctima y atacante. Si todo ha ido bien, debería observar cómo el ataque ha surtido efecto y ha cambiado el contenido de la tabla. Copie la salida de la orden `sudo arp -na` a continuación

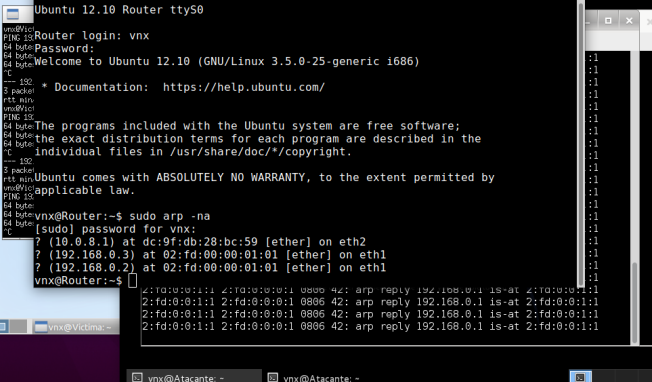
**VÍCTIMA:**


```

vnx@Victima:~$ ping 192.168.0.3
PING 192.168.0.3 (192.168.0.3) 56(84) bytes of data:
64 bytes from 192.168.0.3: icmp_req=1 ttl=64 time=0.913 ms
64 bytes from 192.168.0.3: icmp_req=2 ttl=64 time=0.538 ms
64 bytes from 192.168.0.3: icmp_req=3 ttl=64 time=0.604 ms
64 bytes from 192.168.0.3: icmp_req=4 ttl=64 time=0.929 ms
64 bytes from 192.168.0.3: icmp_req=5 ttl=64 time=0.959 ms
64 bytes from 192.168.0.3: icmp_req=6 ttl=64 time=1.01 ms
64 bytes from 192.168.0.3: icmp_req=7 ttl=64 time=0.816 ms
64 bytes from 192.168.0.3: icmp_req=8 ttl=64 time=0.566 ms
64 bytes from 192.168.0.3: icmp_req=9 ttl=64 time=0.376 ms
64 bytes from 192.168.0.3: icmp_req=10 ttl=64 time=0.795 ms
64 bytes from 192.168.0.3: icmp_req=11 ttl=64 time=1.06 ms
64 bytes from 192.168.0.3: icmp_req=12 ttl=64 time=0.959 ms
64 bytes from 192.168.0.3: icmp_req=13 ttl=64 time=0.984 ms
64 bytes from 192.168.0.3: icmp_req=14 ttl=64 time=0.483 ms
64 bytes from 192.168.0.3: icmp_req=15 ttl=64 time=1.06 ms
^C
--- 192.168.0.3 ping statistics ---
15 packets transmitted, 15 received, 0% packet loss, time 1401ms
rtt min/avg/max/mdev = 0.376/0.804/1.067/0.222 ms
vnx@Victima:~$ sudo arp -na
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
vnx@Victima:~$

```

Efectivamente podemos ver que ahora solo aparece la dirección del Atacante.

**ROUTER:**


```

Ubuntu 12.10 Router tty50
vnx@Router:~$ sudo arp -na
[sudo] password for vnx:
? (10.0.8.1) at dc:9f:db:28:bc:59 [ether] on eth2
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
? (192.168.0.2) at 02:fd:00:00:01:01 [ether] on eth1
vnx@Router:~$

```

Aquí podemos ver que sí aparecen las IP de atacante y víctima pero ambas direcciones corresponden a la misma dirección física, la del atacante

**ATACANTE :**

6. Justifique los valores de las tablas ARP anteriores:

Estos valores se deben a que el envenenamiento ARP está “engañando” al router y a la victima, haciendo que el primero piense que el atacante es la victima, y a la victima le hace creer que el atacante es el router.

7. Abra un navegador en el equipo “VÍCTIMA” e intente acceder a la URL <http://www.google.es/>. Explique el resultado obtenido:

La pagina no carga, ya que el equipo atacante no hace nada con los paquetes de la victima que le llegan, ni con los paquetes que el router pudiera mandar a la victima.

8. Explique por qué es necesario habilitar el reenvío de paquetes en el equipo “ATACANTE”:

Ya que los paquetes se quedaban “atascados” en el equipo atacante, es necesario instruirle a que los envíe al equipo apropiado (router, terminal o sí mismo).

9. Indique si el ataque realizado es un ataque activo o pasivo. Explique qué se puede conseguir con este ataque:

Es un ataque pasivo, ya que solo se lee el contenido de los paquetes, no se está modificando lo que contienen, esto pone en peligro la confidencialidad, pero no la integridad de los mensajes.

Se consigue tener acceso al contenido de los paquetes que la victima intercambia con el router.

10. Indique si desde la máquina atacante puede capturar las credenciales de acceso (usuario y contraseña) que ha introducido para acceder a ‘Aula Virtual’. Si su respuesta es afirmativa, indique en qué mensaje de la captura se encuentran dichos mensajes. Si su respuesta es negativa, justifique detalladamente su respuesta:

Se puede. El mensaje en el que están contenidos el usuario y contraseña es el nº 95.

No.	Time	Source	Destination	Protocol	Length	Info
54	6.991154	192.168.0.2	93.184.220.29	OCSP	503	Request
58	7.059861	93.184.220.29	192.168.0.2	OCSP	865	Response
95	11.774747	192.168.0.2	212.128.121.14	HTTP	702	POST /login/index.php HTTP/1.1 (application/x-www-form-urlencoded)

▶ Frame 95: 702 bytes on wire (5616 bits), 702 bytes captured (5616 bits)  
 ▶ Ethernet II, Src: 02:fd:00:00:00:01 (02:fd:00:00:00:01), Dst: 02:fd:00:00:01:01 (02:fd:00:00:01:01)  
 ▶ Internet Protocol Version 4, Src: 192.168.0.2, Dst: 212.128.121.14  
 ▶ Transmission Control Protocol, Src Port: 51025, Dst Port: 80, Seq: 1, Ack: 1, Len: 636  
 ▶ Hypertext Transfer Protocol  
 ▼ HTML Form URL Encoded: application/x-www-form-urlencoded  
 ▶ Form item: "username" = "prueba"  
 ▶ Form item: "password" = "prueba"  
 ▶ Form item: "anchor" = ""

11. ¿Ofrece el protocolo http un servicio de confidencialidad de datos?  
Responda a esta cuestión a partir de los resultados obtenidos en el ejemplo anterior:

No, no ofrece seguridad, encriptación ni ningún protocolo que permita asegurar la confidencialidad de los datos.