

Practica 3

Adrian Anchuela

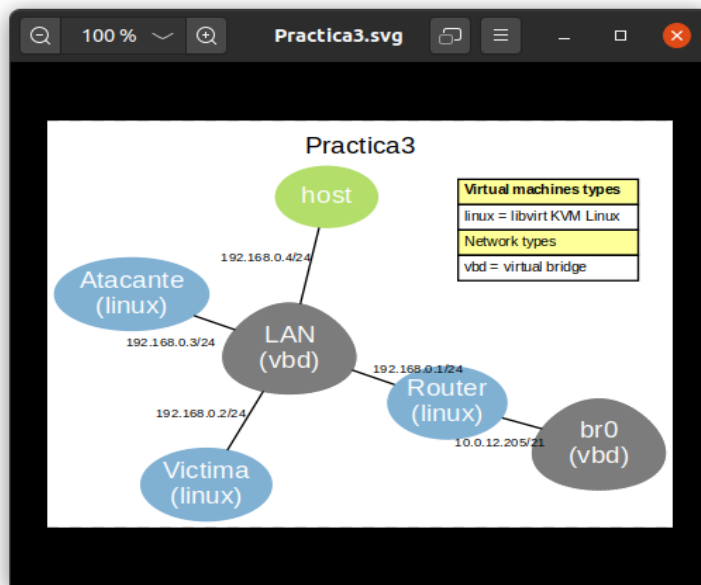
1. A partir de la salida de esta orden, indique a continuación las direcciones IP de los equipos conectados en la red (identifique el equipo VÍCTIMA y el equipo ATACANTE).

Victima: 192.168.0.2/24

Atacante: 192.168.0.3/24

Router: 192.168.0.1/24

Host: 192.168.0.4/24



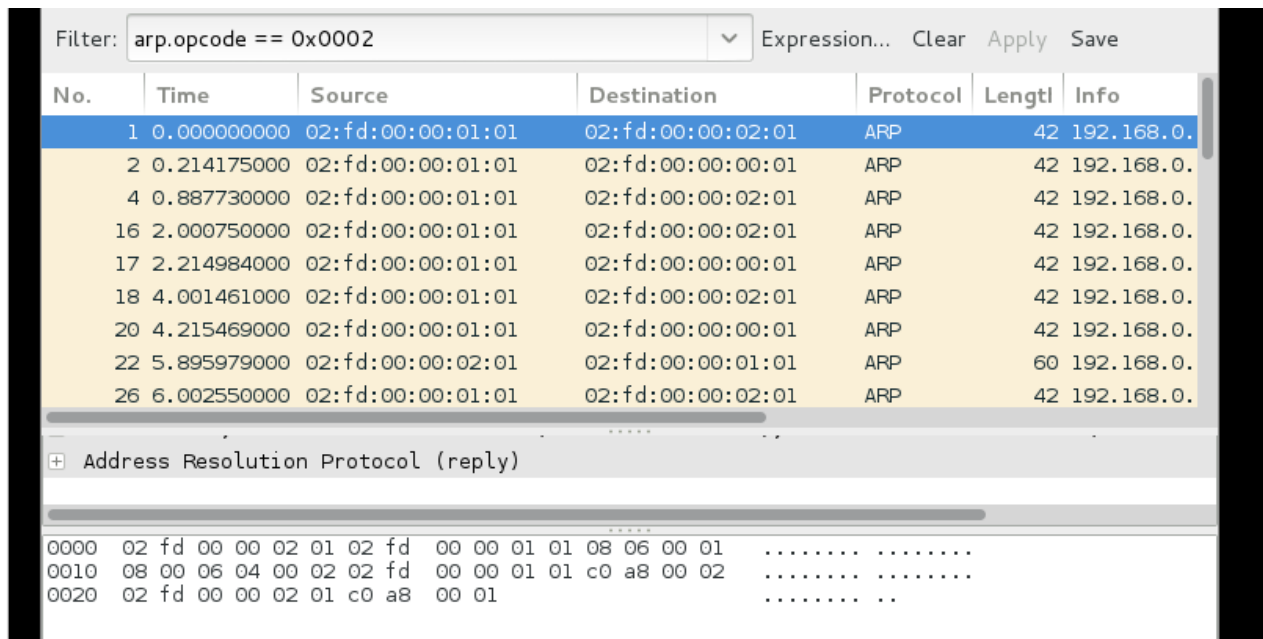
2. ¿Qué le está mostrando?: (es posible que para llenar las tablas de arp tenga que utilizar la orden ping entre los distintos equipos)

```
vnx@Victima: ~  
File Edit Tabs Help  
vnx@Victima:~$ sudo arp -na  
[sudo] password for vnx:  
? (192.168.0.1) at 02:fd:00:00:02:01 [ether] on eth1  
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1  
vnx@Victima:~$
```

3. Repita la operación para el equipo ATACANTE. ¿Qué le está mostrando?:

```
root@Atacante:~# sudo arp -na
? (192.168.0.1) at 02:fd:00:00:02:01 [ether] on eth1
? (192.168.0.4) at 02:00:00:97:e6:96 [ether] on eth1
? (192.168.0.2) at 02:fd:00:00:00:01 [ether] on eth1
root@Atacante:~#
```

evidencia_ARP_0.cap



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	02:fd:00:00:01:01	02:fd:00:00:02:01	ARP	42	192.168.0.1 → 192.168.0.2
2	0.214175000	02:fd:00:00:01:01	02:fd:00:00:00:01	ARP	42	192.168.0.1 → 192.168.0.1
4	0.887730000	02:fd:00:00:01:01	02:fd:00:00:02:01	ARP	42	192.168.0.1 → 192.168.0.2
16	2.000750000	02:fd:00:00:01:01	02:fd:00:00:02:01	ARP	42	192.168.0.1 → 192.168.0.2
17	2.214984000	02:fd:00:00:01:01	02:fd:00:00:00:01	ARP	42	192.168.0.1 → 192.168.0.1
18	4.001461000	02:fd:00:00:01:01	02:fd:00:00:02:01	ARP	42	192.168.0.1 → 192.168.0.2
20	4.215469000	02:fd:00:00:01:01	02:fd:00:00:00:01	ARP	42	192.168.0.1 → 192.168.0.1
22	5.895979000	02:fd:00:00:02:01	02:fd:00:00:01:01	ARP	60	192.168.0.2 → 192.168.0.1
26	6.002550000	02:fd:00:00:01:01	02:fd:00:00:02:01	ARP	42	192.168.0.1 → 192.168.0.2

Address Resolution Protocol (reply)

0000 02 fd 00 00 02 01 02 fd 00 00 01 01 08 06 00 01
0010 08 00 06 04 00 02 02 fd 00 00 01 01 c0 a8 00 02
0020 02 fd 00 00 02 01 c0 a8 00 01

4. Explique lo que está sucediendo, recuerde que debe dejar estas dos terminales abiertas para que se produzca el envenenamiento continuo:

Escribiendo el comando `sudo arpspoof -t IP_víctima IP_router` podemos ver como la dirección mac del atacante se convierte en la misma que el router. Haciendo creer a la víctima que el router somos nosotros.

ARPs spoof se usa para enviar mensajes ARP falsos a la máquina de la víctima engañándola para que envíe su tráfico a la máquina del atacante por otra puerta de enlace en la red.

5.1 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 router. 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:

```
vx@Victima:~$ sudo arp -na
[sudo] password for vx:
? (192.168.0.4) at 02:00:00:62:db:20 [ether] on eth1
? (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
vx@Victima:~$ sudo arp -na
? (192.168.0.4) at 02:00:00:62:db:20 [ether] on eth1
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
? (192.168.0.1) at 02:fd:00:00:01:01 [ether] on eth1
vx@Victima:~$
```

5.2 ROUTER:

```
vx@Router:~$ sudo arp -na
? (10.0.12.214) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.207) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.209) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.202) at 02:fd:00:00:02:02 [ether] on eth2
? (192.168.0.2) at 02:fd:00:00:01:01 [ether] on eth1
? (10.0.12.211) at <incomplete> on eth2
? (10.0.12.204) at <incomplete> on eth2
? (10.0.12.206) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.8.1) at dc:9f:db:28:bc:59 [ether] on eth2
? (10.0.12.208) at <incomplete> on eth2
? (10.0.12.201) at 02:fd:00:00:02:02 [ether] on eth2
? (10.0.12.210) at 02:fd:00:00:02:02 [ether] on eth2
? (192.168.0.3) at 02:fd:00:00:01:01 [ether] on eth1
? (10.0.12.212) at 02:fd:00:00:02:02 [ether] on eth2
vx@Router:~$
```

6. Justifique los valores de las tablas ARP anteriores ¿qué está sucediendo?:

Estamos haciendo que el equipo de la víctima crea que la MAC del router y del equipo atacante es el mismo, y al router le estamos haciendo creer que el equipo de la víctima y del atacante es el mismo.

7. Explique qué está sucediendo y por qué cree que sucede esto:

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

Porque tenemos que actuar como router por lo cual nuestra función ha de ser la misma, recibir paquetes y mandarlos de vuelta hacia la víctima.

El comando `echo 1 > /proc/sys/net/ipv4/ip_forward` nos permite habilitar el reenvío de paquetes.

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

Es un ataque MITM pasivo debido a que simplemente somos un pasadizo entre dos puntos, podemos interceptar la información que se esta intercambiando pero no estamos haciendo nada por alterar o modificar la comunicación que se esta produciendo.

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.

No se ha podido capturar las credenciales de inicio de sesión debido a que la pagina sigue el protocolo https la cual proporciona confidencialidad de datos y de comunicación.

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.

Debido a que he podido capturar las imágenes podemos confirmar que http no proporciona confidencialidad de datos, es un protocolo que proporciona confidencialidad de comunicación, pero es susceptible a Phishing.

