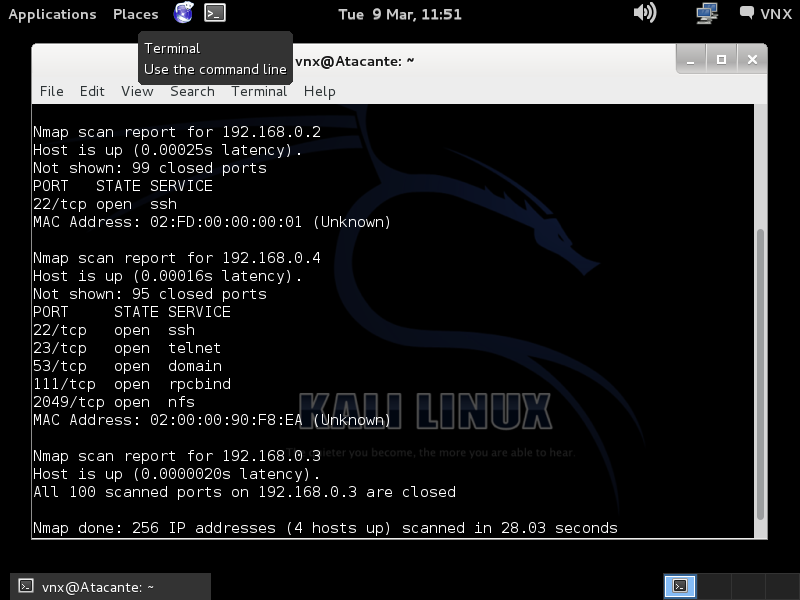
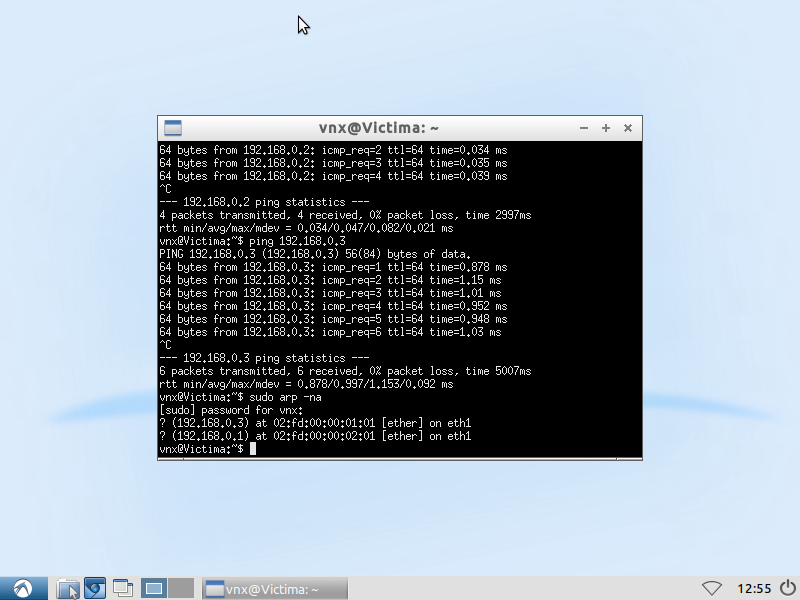
|  |  |  |
| --- | --- | --- |
| **NOMBRE** | **APELLIDOS** | **DNI** |
| Laura | Ramos Martinez | 03201266B |

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

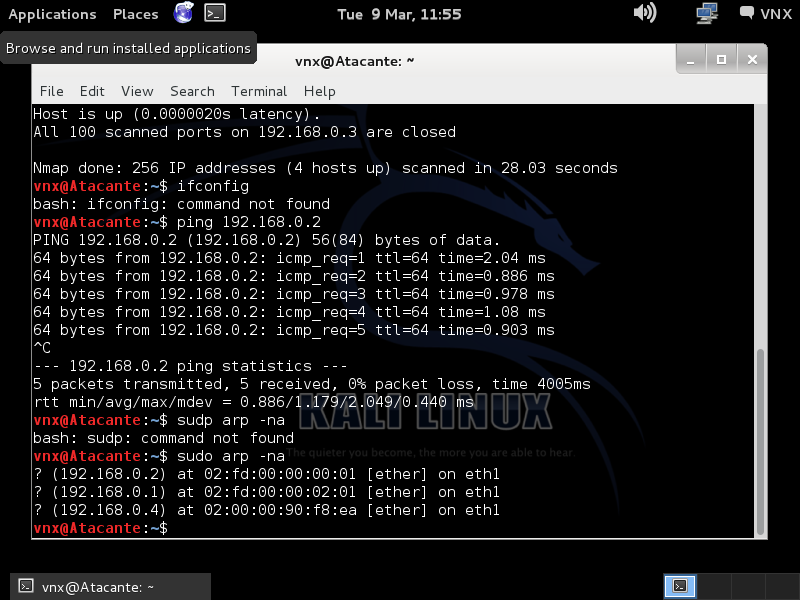
1. En nuestro caso, lo vamos a emplear para determinar víctimas potenciales. Abra un terminal y ejecute la orden nmap -F 192.168.0.0/24   
   A partir de la salida de esta orden, indique a continuación las direcciones IP de los equipos conectados en la red:



1. 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

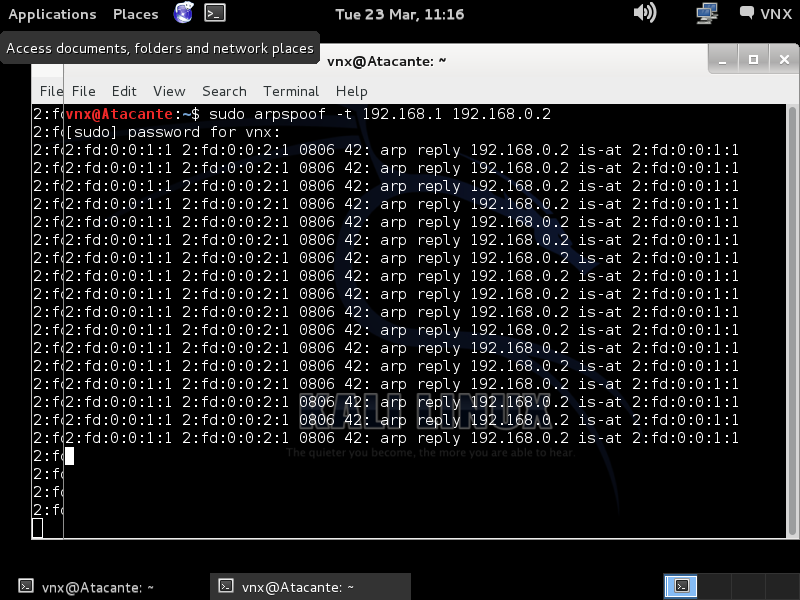


1. Repita la operación para el equipo atacante. ¿Qué le está mostrando?



Muestra la dirección IP y MAC de las maquinas conectadas a la red (Victima, Router y conexión a la red), además de en qué canal están conectados.

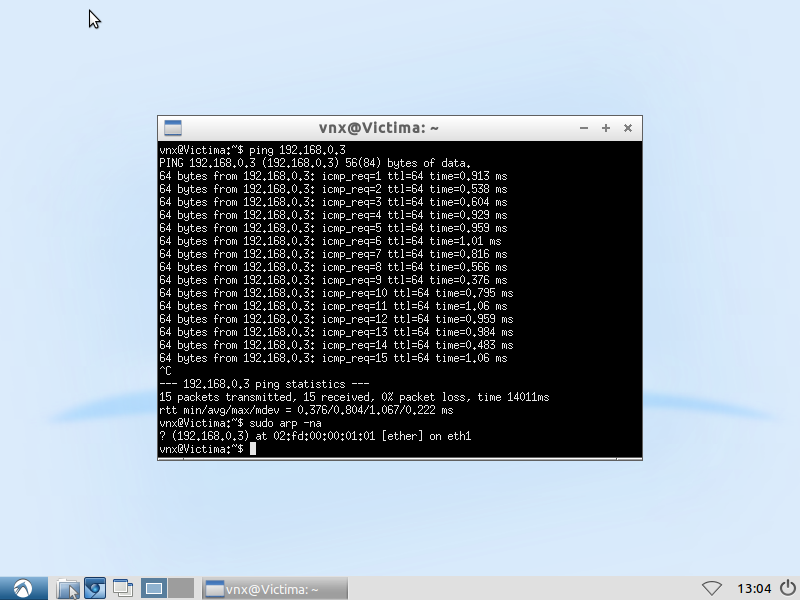
1. Copie la salida de *una de las órdenes* anteriores y explique qué hacen ambas:



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.

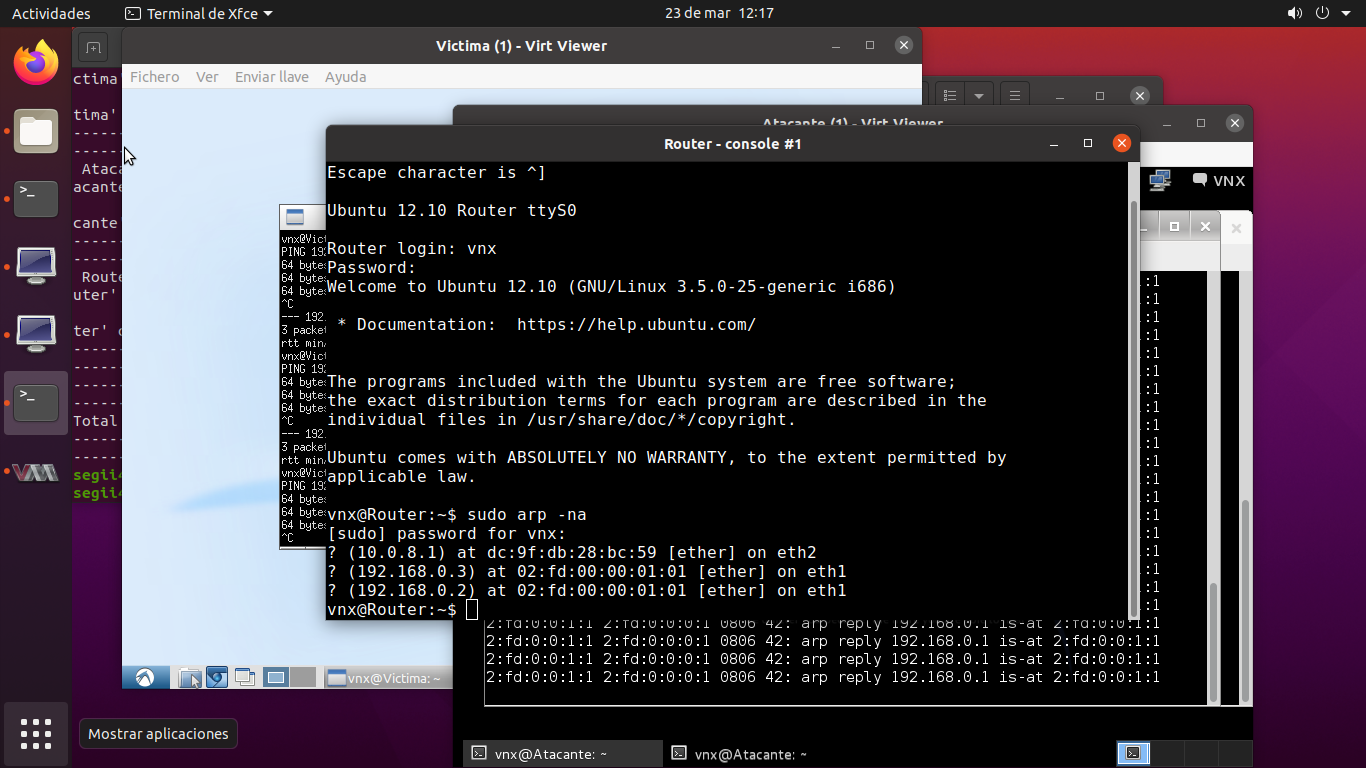
1. En estos momentos, el envenenamiento estaría teniendo lugar. Vamos a **comprobar si está o no funcionando**. Para ello, consulte de nuevo la caché ARP de los equipos víctima y atacante. Si todo ha ido bien, debería observar cómo el ataque ha surtido efecto y ha cambiado el contenido de la tabla. Copie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

**VÍCTIMA:**



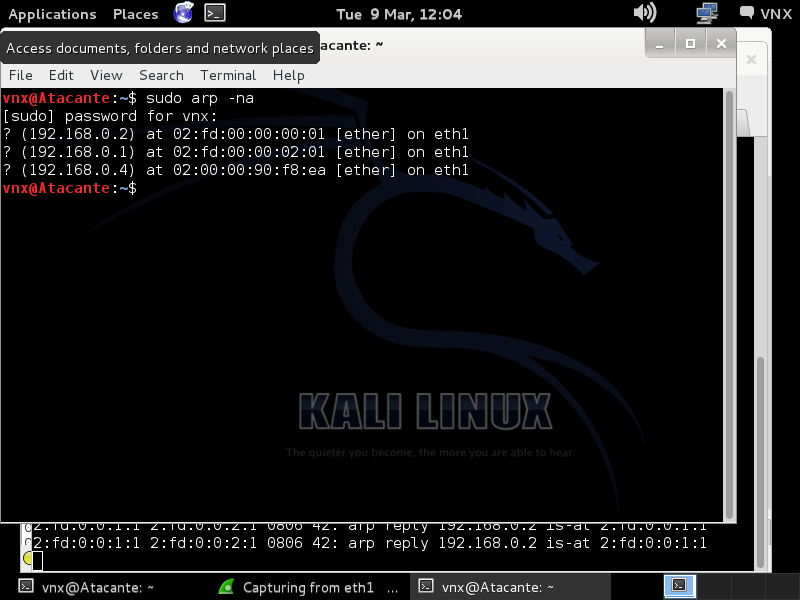
Efectivamente podemos ver que ahora solo aparece la dirección del Atacante.

**ROUTER:**



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

**ATACANTE:**



Y por ultimo, el atacante sí que puede ver tanto al router y a la victima, con sus direcciones físicas correspondientes.

1. 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.

1. 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.

1. 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).

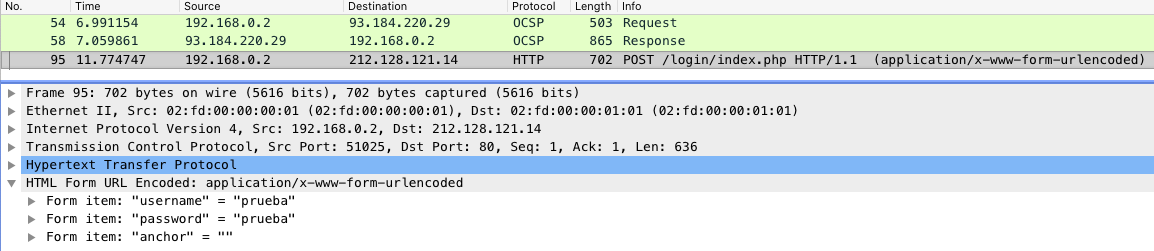
1. Indique si el ataque realizado es un ataque activo o pasivo. Explique qué se puede conseguir con este ataque:

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.

1. 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 contendidos el usuario y contraseña es el nº 95.



1. ¿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.