

MITM CON SCAPY Y SSLSTRIP

NOMBRE	APELLIDOS	DNI
Laura	Ramos Martínez	03201266B

PUESTO: 02

GRUPO: 4

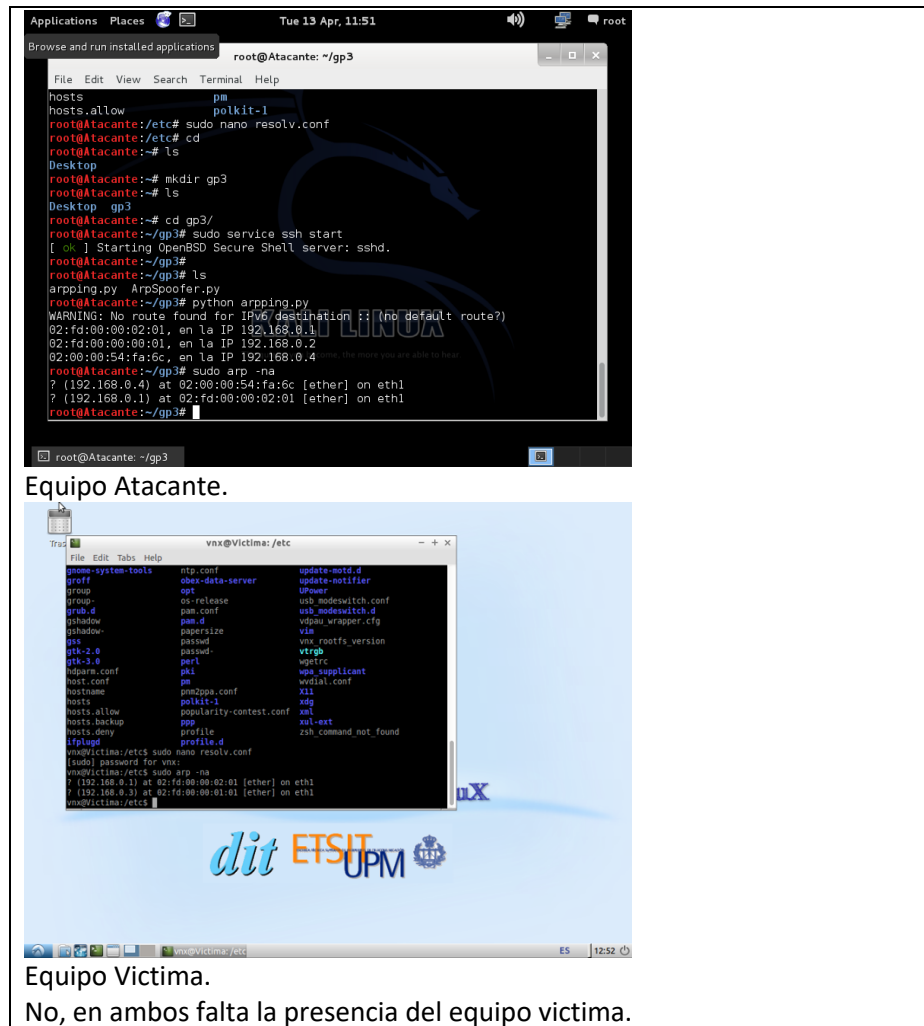
GRADO: GII

1. Indique el resultado de ejecutar este script que aparece en pantalla y explique que está mostrando



El script de Python ejecutado realiza un escaneo ARP de la red, mostrando por terminal los valores de IP de los dispositivos presentes (Victima y Router)

2. Escriba la tabla de ARP de ambos equipos. ¿Qué observa? ¿Es correcta? ¿Por qué?



Equipo Atacante.

```

root@Atacante: ~/gp3
root@Atacante:~# arp
? (192.168.0.4) at 02:00:00:54:fa:6c [ether] on eth1
? (192.168.0.1) at 02:fd:00:00:02:01 [ether] on eth1
root@Atacante:~#

```

Equipo Victima.

```

vnx@Victima: /etc
vnx@Victima:/etc$ arp
? (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:/etc$

```

No, en ambos falta la presencia del equipo victima.

3. Para completar y modificar el anterior script, escriba los valores de:

IP VÍCTIMA: 192.168.0.2

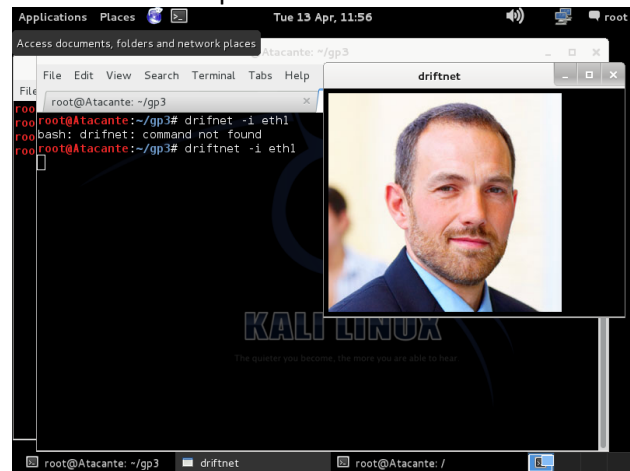
MAC VÍCTIMA: 02:fd:00:00:03:01

MAC ATACANTE: 02:fd:00:00:01:01

IP ROUTER: 192.168.0.1

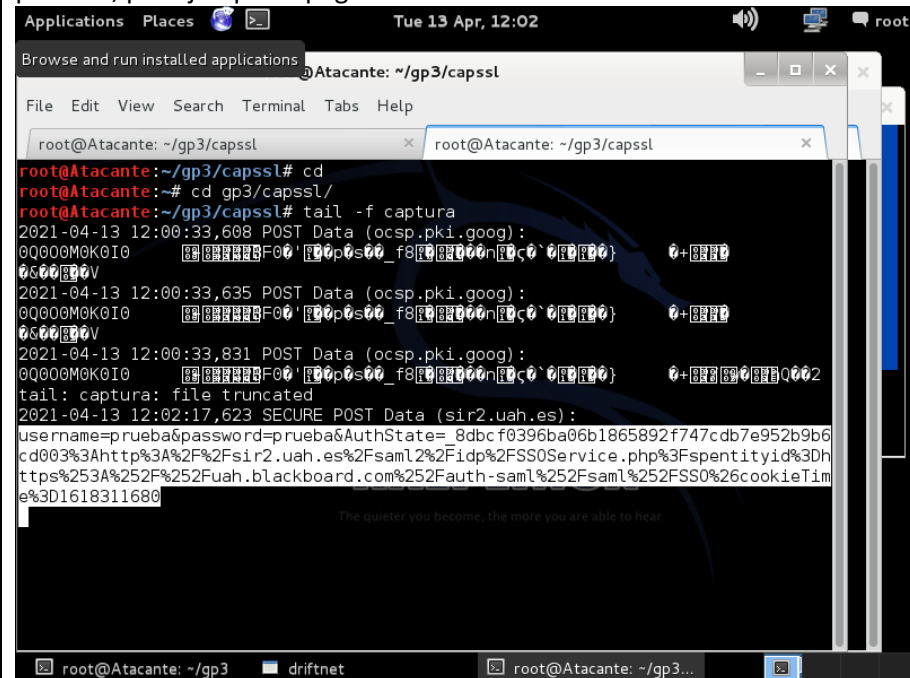
4. Explique lo que está sucediendo, comprobando en el equipo VÍCTIMA y en el ROUTER que se está produciendo el envenenamiento de ARP.

Se produce el envenenamiento ARP, los paquetes destinados a y originados de la víctima están siendo interceptados por el equipo Atacante, que tiene acceso completo a ellos:



5. ¿Qué está sucediendo? ¿Qué sucede con las peticiones HTTPS?

Si el equipo víctima intenta realizar una petición HTTPS esta queda capturada por el Atacante, teniendo este acceso total al contenido de la petición, por ejemplo la pagina de Blackboard UAH:



6. Indique si desde la máquina ATACANTE puede capturar las credenciales de acceso (usuario y contraseña) que ha introducido para acceder a 'Aula Virtual'.

Sí, tal como aparece en la captura anterior, se pueden capturar los credenciales de acceso en texto plano.

7. Indique las páginas que ha probado y cuál ha sido el funcionamiento del proceso en la captura de credenciales:

Probé las páginas Gmail (mail.google.com), Facebook (Facebook.com), Twitter (twitter.com) e Instagram (Instagram.com) y ninguna de ellas me permitió acceder a los credenciales.

8. ¿Ha encontrado alguna web que sólo permita acceder obligatoriamente por HTTPS? ¿Qué solución plantea ante este problema? ¿Qué es HSTS? ¿Solventa el problema?