ATAQUE ARP SPOOFING POR KALI LINUX
EDER LEON HUILLCA AYMA

1. IDENTIFICO A MI PC (SERÁ VULNERADA), MI GATEWAY (router) y A MI ATACANTE (KALI)

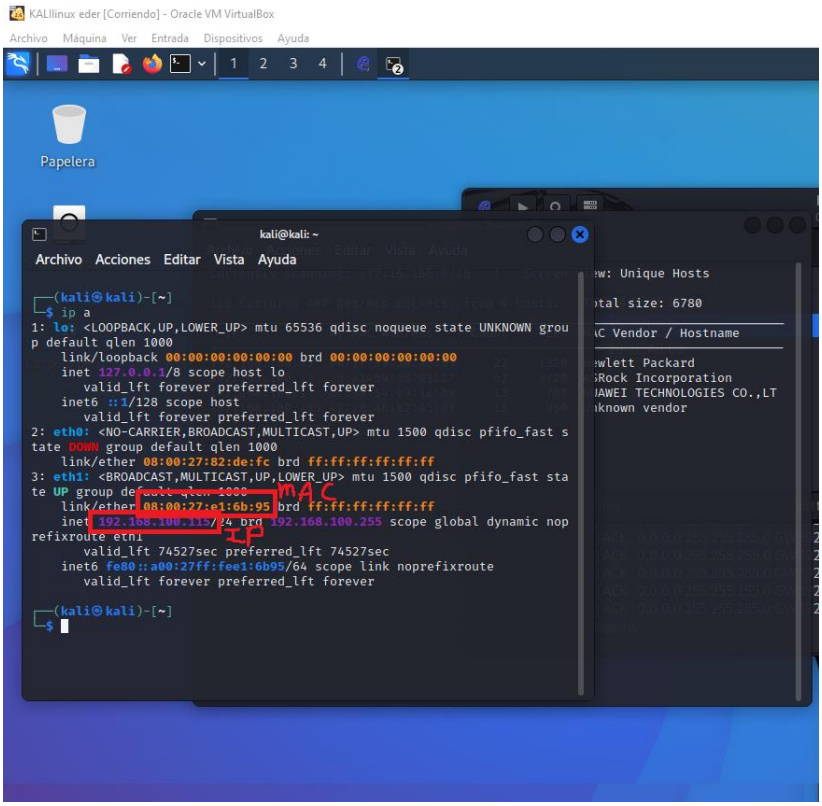


Fig1. Ip y mac de mi Kali (atacante)

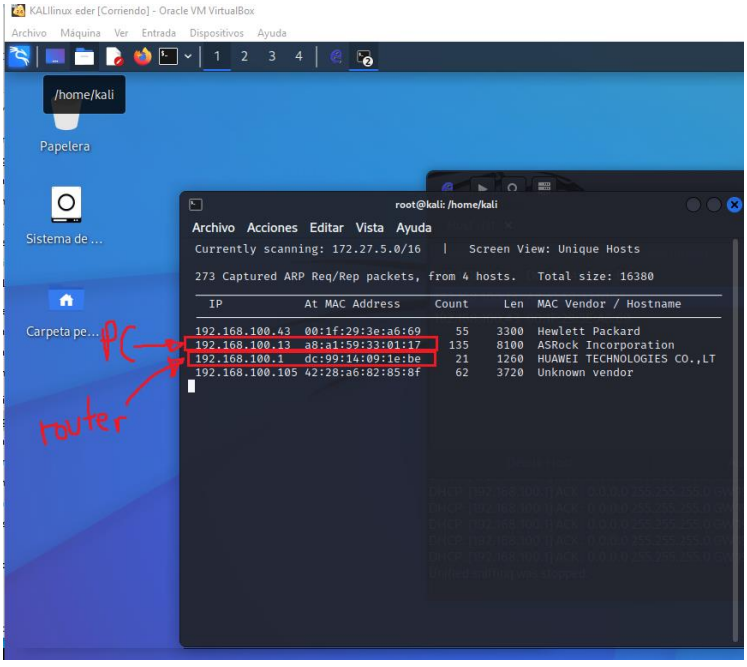


Fig2. Ip y mac de mi PC y Gateway

2. SCANEO EN ETTERCAP, TARGETEO y ACTIVO ARP POISONING

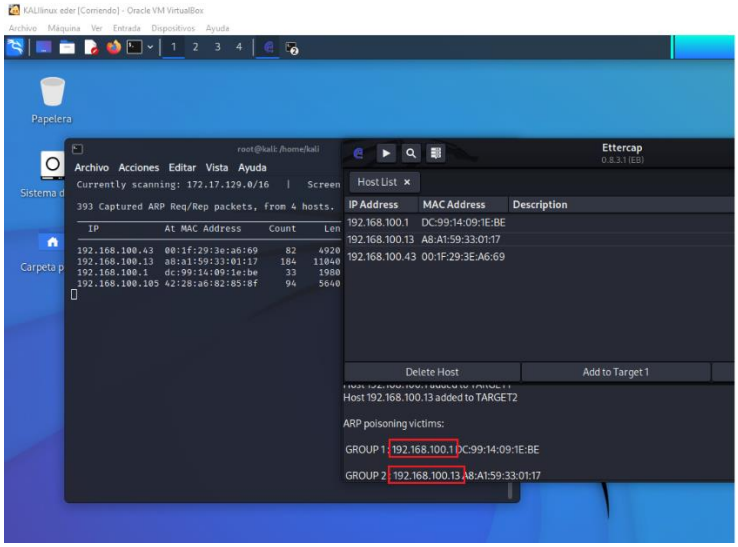
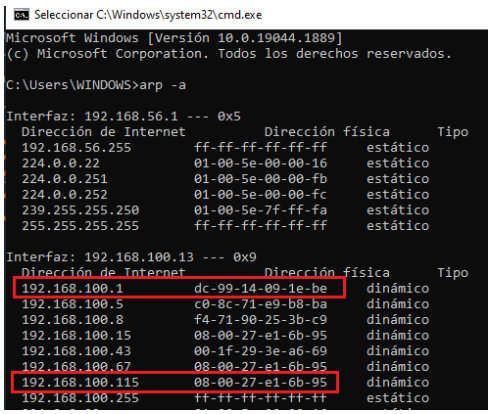
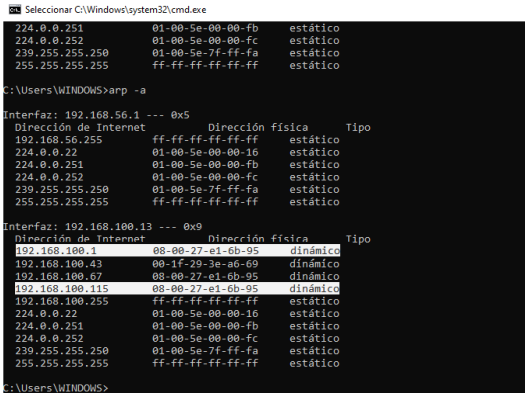


Fig3. Seleccionado de Targets

3. Identifico los cambios en la tabla MAC.





ANTES DESPUÉS

4. Procedo a entrar a una página http, para ver si puedo ver la información que trasladan los protocolos http de la pc al router (credenciales de sesión)

Fig6. Escogí esta página porque usa protocolo http

5. Capturo el tráfico mediante Wireshark

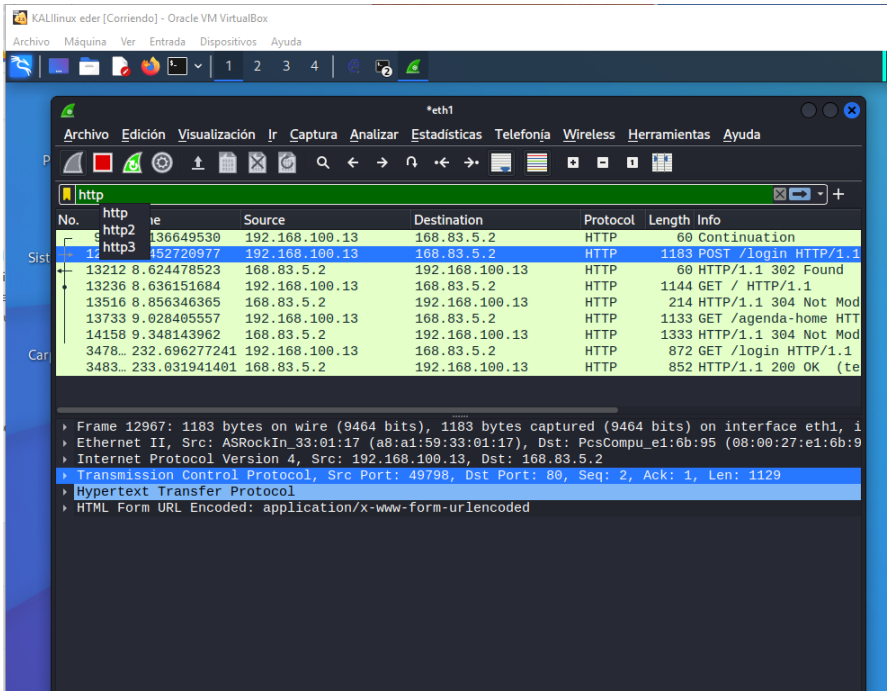


Fig7. Tráfico exclusivamente de protocolos HTTP

6. Busco en cualquier de ellos la opción de seguir flujo en uno de los datagramas con protocolo HTTP

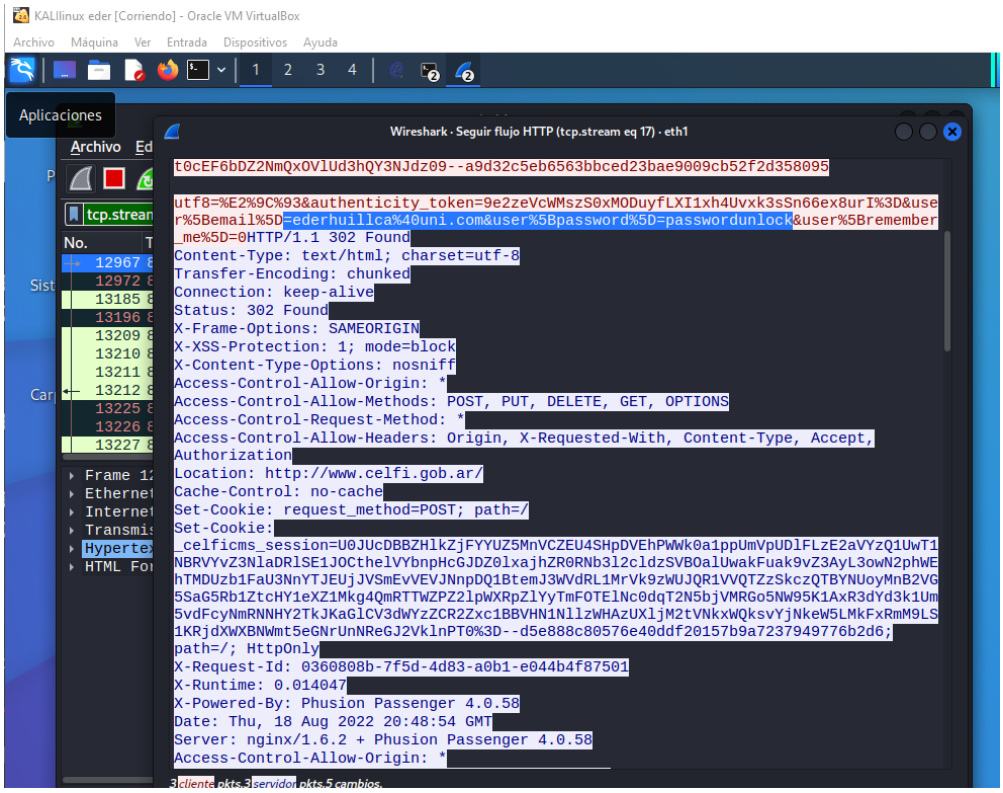


Fig8. Seguir Flujo de Datagrama HTTP

Conclusiones:

- Efectivamente podemos ver el correo que ingresé y la contraseña:
  ederhuillca@uni.com
  passwordunlock.
- Se puede realizar el ataque de cualquier dispositivo, incluido si está conectado a nuestra red lan via wifii ya que sigue perteneciendo a nuestra red.
- Al realizar el ataque, al inicio podía mapear la ip y mac de mi celular y de dispositivos inalámbricos conectados a mi red, pero al cabo de segundos, éstos se desconectaban de manera automática de mi red, quitando toda conexión vía Wireless, por lo que intuyo que hay una protección para éste tipo de casos.