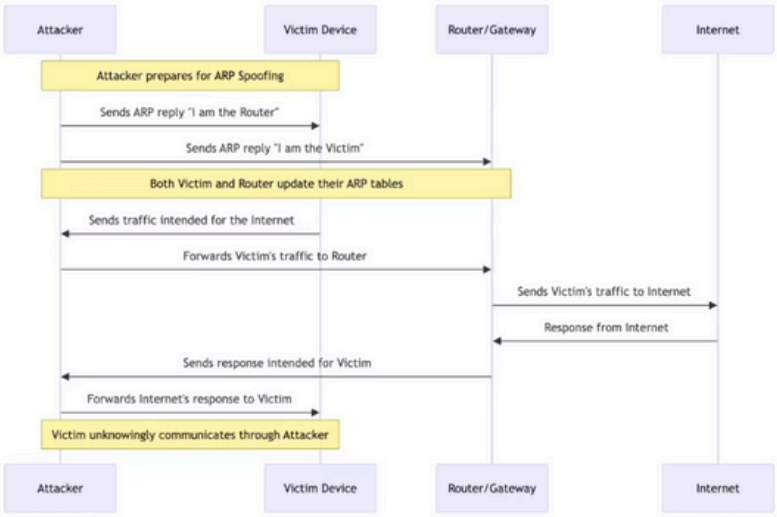
ARP Spoofing

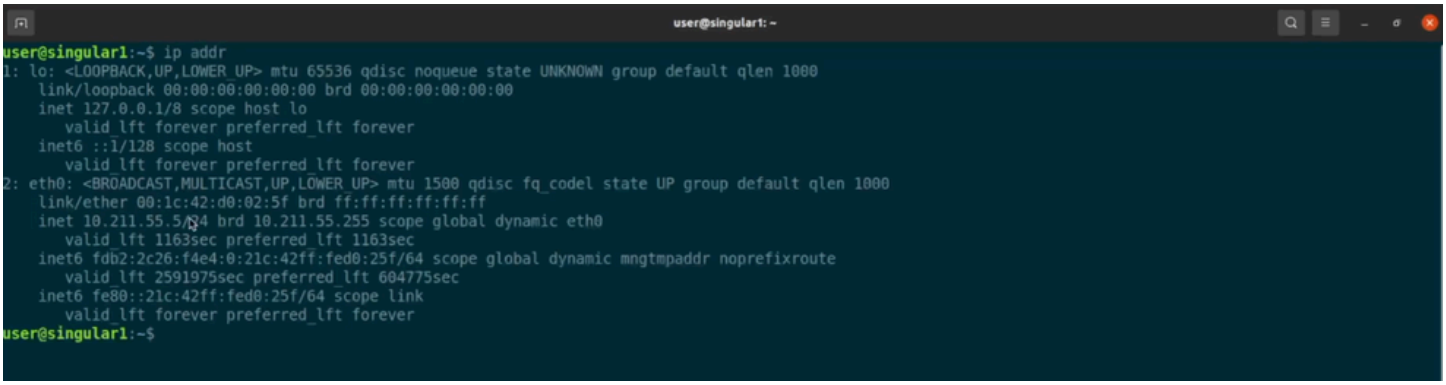
An ARP spoofing attack works by deceiving a network by sending fake ARP (Address Resolution Protocol) messages, allowing the attacker to intercept, modify, or block data intended for another computer on the network by impersonating that computer.



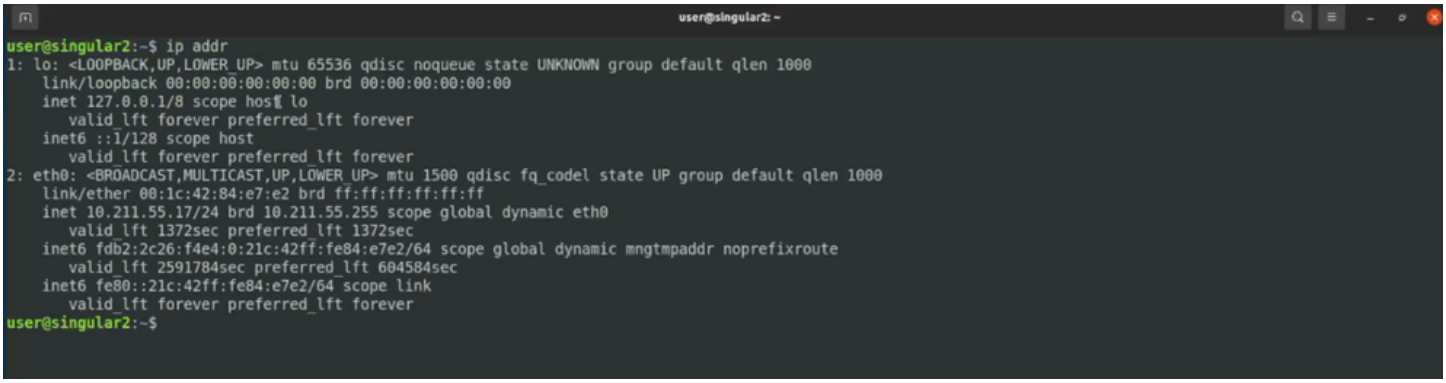
ARP Spoofing attack
Picture source: own creation

Vamos a ver cómo se desarrolla un ataque ARP spoofing suando dos maquinas ubuntu (se diferencian por el diferente color de la terminal).

Ésta máquina sera el servidor que será atacado:



Ésta máquina será la atacante:

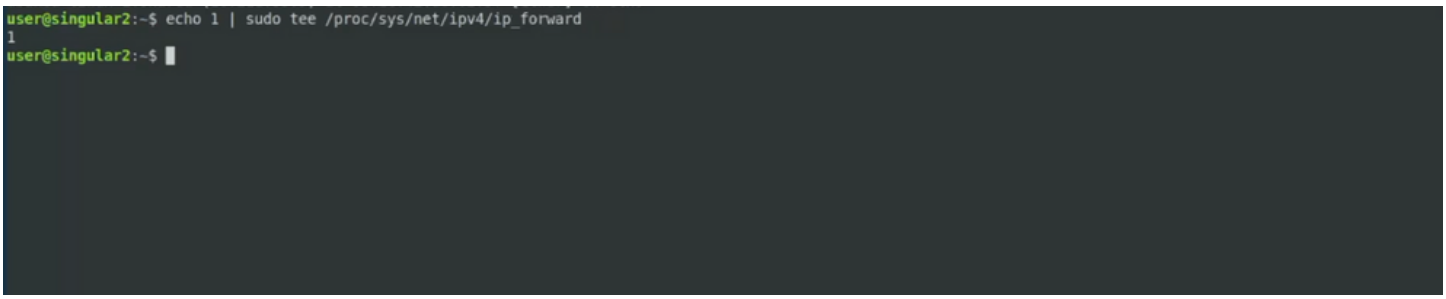


Vamos a verificar la conectividad con un ping:

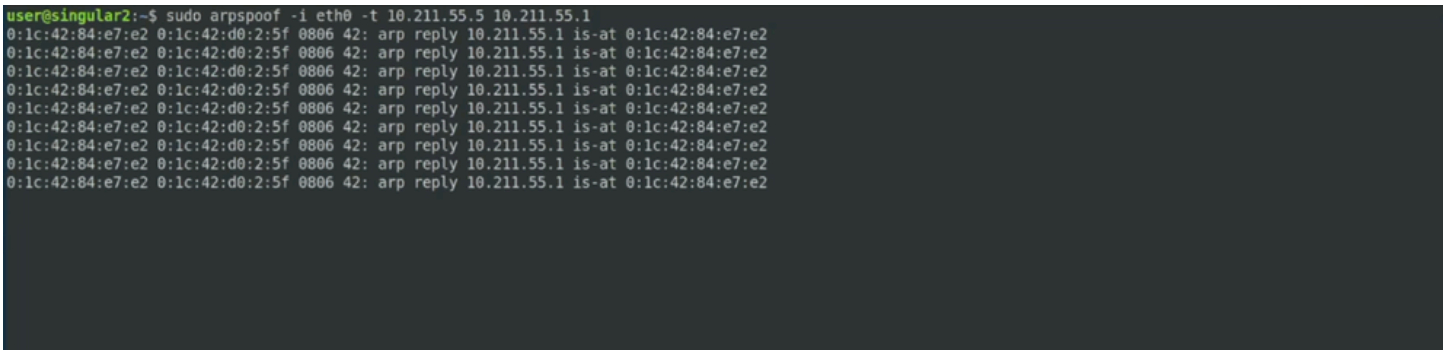
usamos el comando arp para ver las maquinas que se pueden comunicar dentro de la red e identificar la victima, primero lo instalamos:

ARP nos da la dirección mac del gateway, esencial:

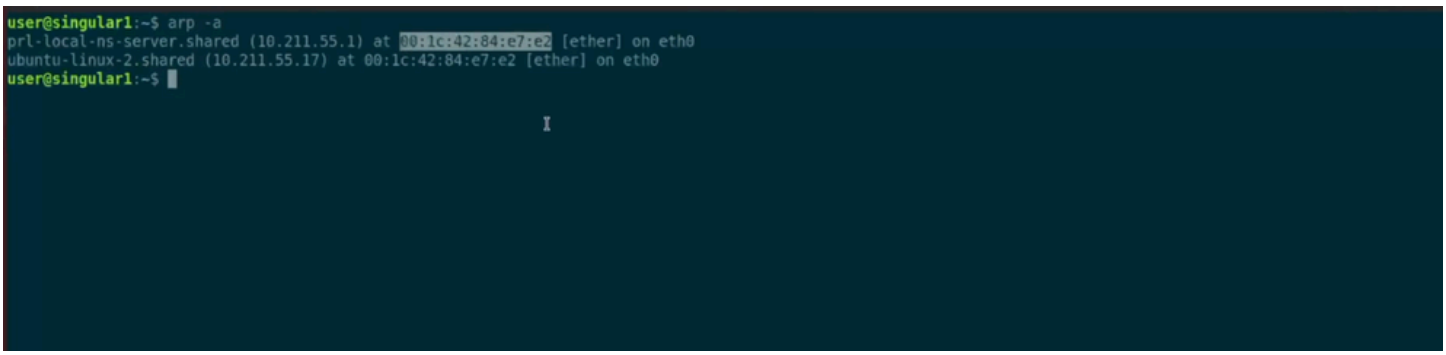
Ahora hay que habilitar el ip forwarding, para que los paquetes de datos fluyan correctamente entre la victima y el gateway real mientras el atacante intercepta el tráfico:



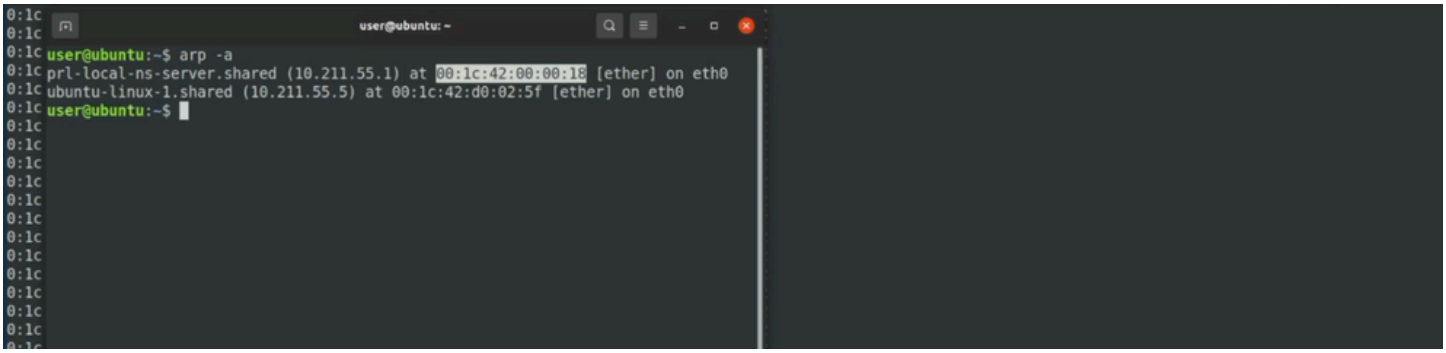
Ahora vamos a hacer el arp spoofing enviando peticiones arp falsificadas para asociar la mac del atacante en la tabla arp de la victima:



Vamos a la maquina victima para comprobar que al hacer el arp -a la direccion de gateway tiene que ser la terminada en e2 (para verificar que el spoofing ha sido un exito o no):



Debería aparecer ésta direccion mac, pero cómo hemos hecho el arp spoofing aparece la terminada en e2:



Ahora la victima ya esta comprometida, todo se va a redigir hacia la maquina de ataque, volvemos a la maquina de ataque y levantamos un tcpdump para capturar el trafico arp o ip, así que la máquina de ataque tiene una terminal con el arp spoofing en curso y otra terminal con el tcpdump escuchando el tráfico:

Con tcpdump veremos la información que hemos conseguido con el spoofing y podemos volcar la información conseguida en un documento usando un comando específico.

Cómo podemos mitigar un arp spoofing?

ARP Spoofingmitigacion measures

Authentication-based Network Security: Implement authentication solutions, such as IEEE 802.1X, to verify the identity of devices and users before allowing them access to the network.

Anomalous ARP Monitoring and Detection: Utilize network monitoring tools that can detect and alert on unusual changes in ARP tables, which could indicate an ARP spoofing attempt.

Suspicious ARP Traffic Filtering: Configure rules on network devices to block or filter ARP traffic that appears suspicious, such as ARP responses from multiple MAC addresses for the same IP address.

VLAN Implementation: Use network segmentation via VLANs to reduce the attack surface and limit the propagation of malicious ARP packets across the network.