Bootcamp Analista SOC Nivel 1 - 2025

Comunidad DOJO - WoSEC Panamá

Nombre y Apellido: Ingrid Kaufmann

Email: ingridkaufmannok@gmail.com

Agosto 2025

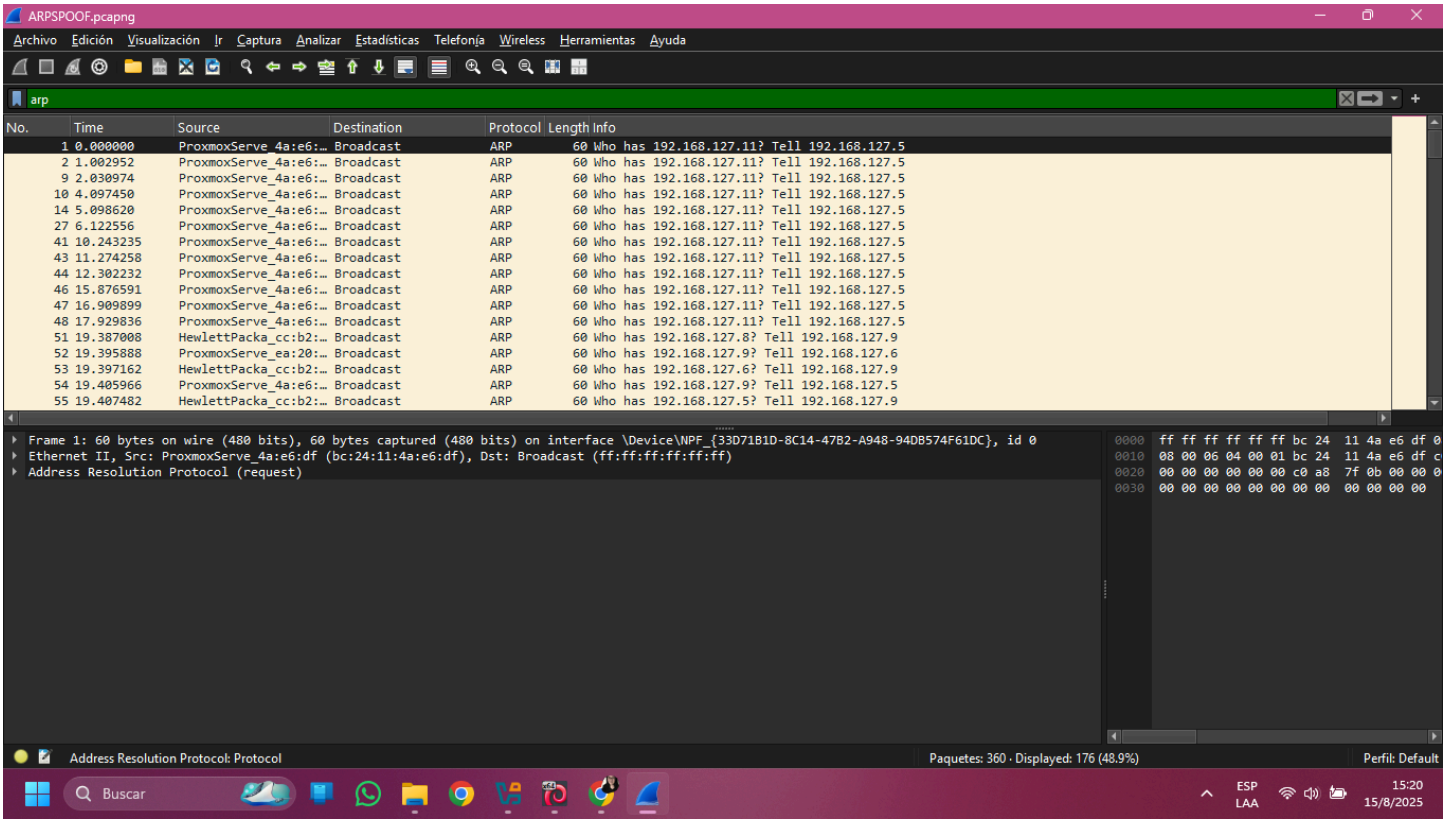
¿Cuál es la MAC Address del atacante?

MAC Address: **bc:24:11:52:16:9a**

Host: **ProxmoxServe 52:16:9a**

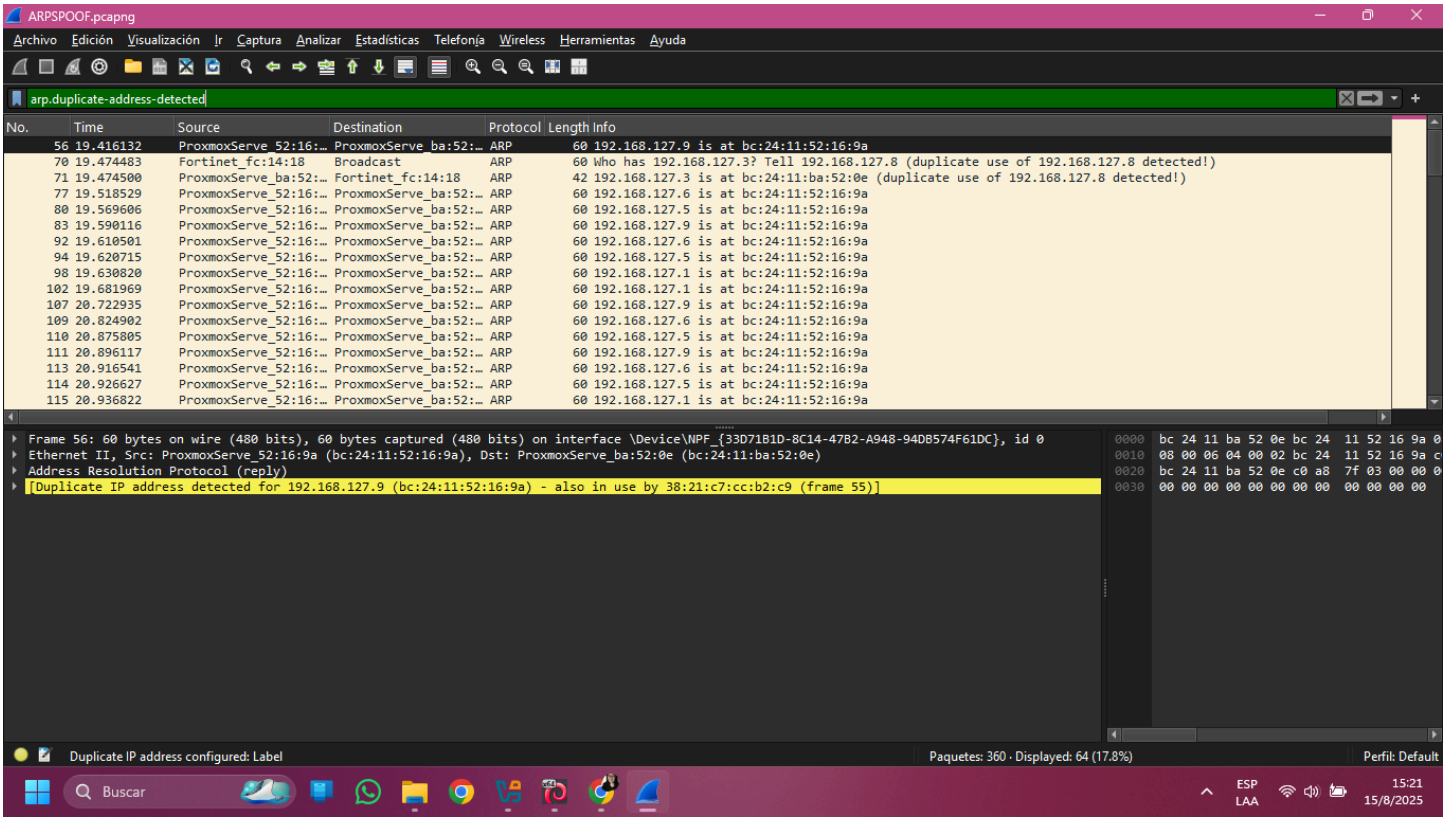
Evidencia N.º 1:

Al aplicar el filtro **arp**, este muestra solo dicho tráfico (requests y replies). Sirve para realizar búsquedas más limpias y eliminar todo lo que no sea arp.



Evidencia N.º 2:

Con el filtro **arp.duplicate-address-detected**, se puede visualizar como dos hosts reclaman la misma IP. Los ataques de tipo spoof suelen duplicar las IPs, así que esto es llamativo.



Conclusión:

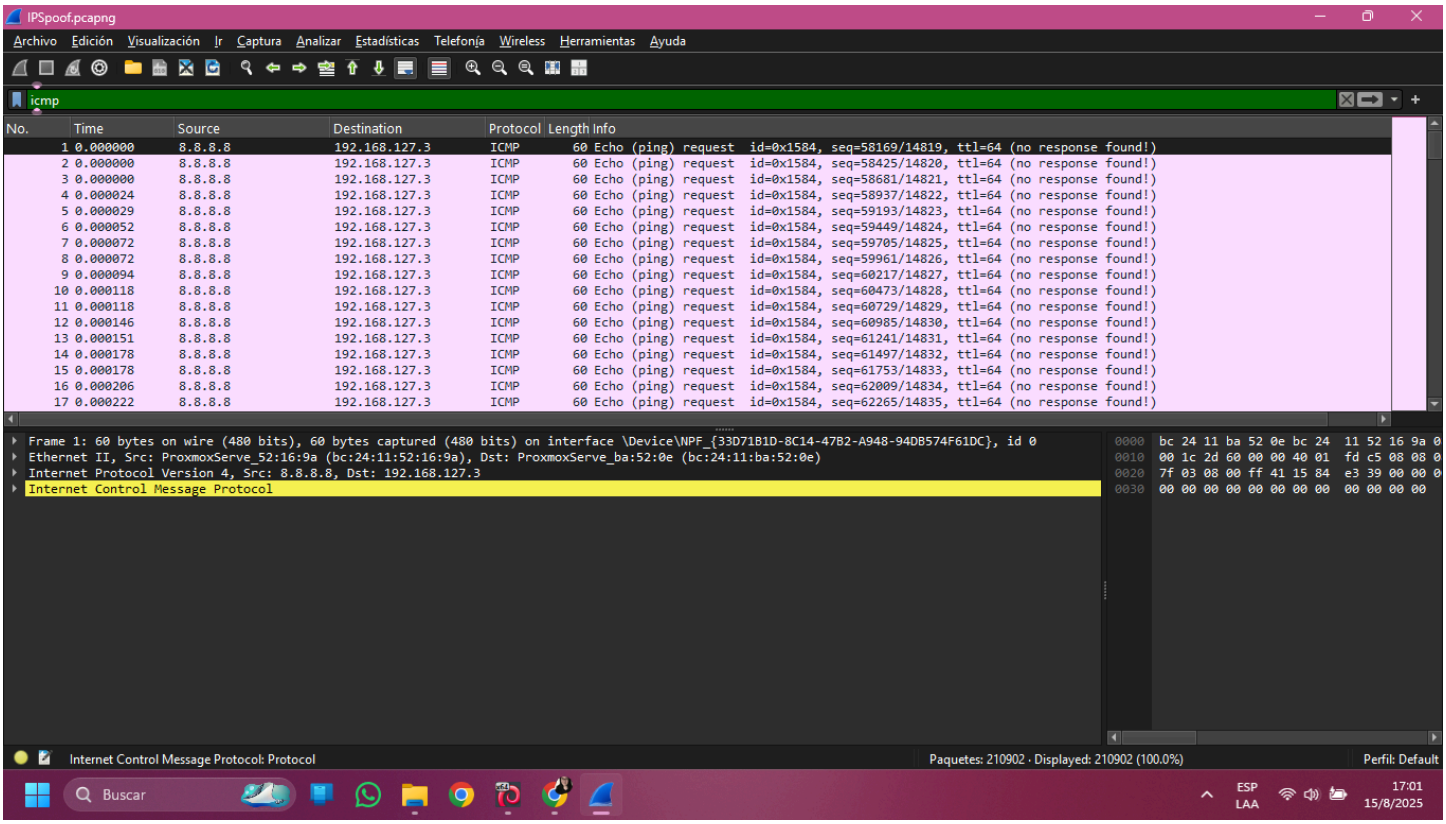
Un ataque ARP spoof puede mostrar múltiples IPs diferentes asociadas a la misma MAC, o la misma IP apareciendo con distintas MACs en poco tiempo, como se puede ver en la evidencia. Existen distintos filtros que se pueden utilizar como: arp.opcode == 1 (muestra solicitudes), arp.opcode == 2 (muestra respuestas), eth.addr == MAC sospechosa (filtra todo el tráfico de una sola MAC), entre otros.

¿Cuál es el sistema operativo del atacante?

Sistema Operativo: **Linux**

Evidencia N.º 1:

El filtro **icmp** muestra las solicitudes y respuestas de ping, lo que hace más fácil inspeccionar TTL.



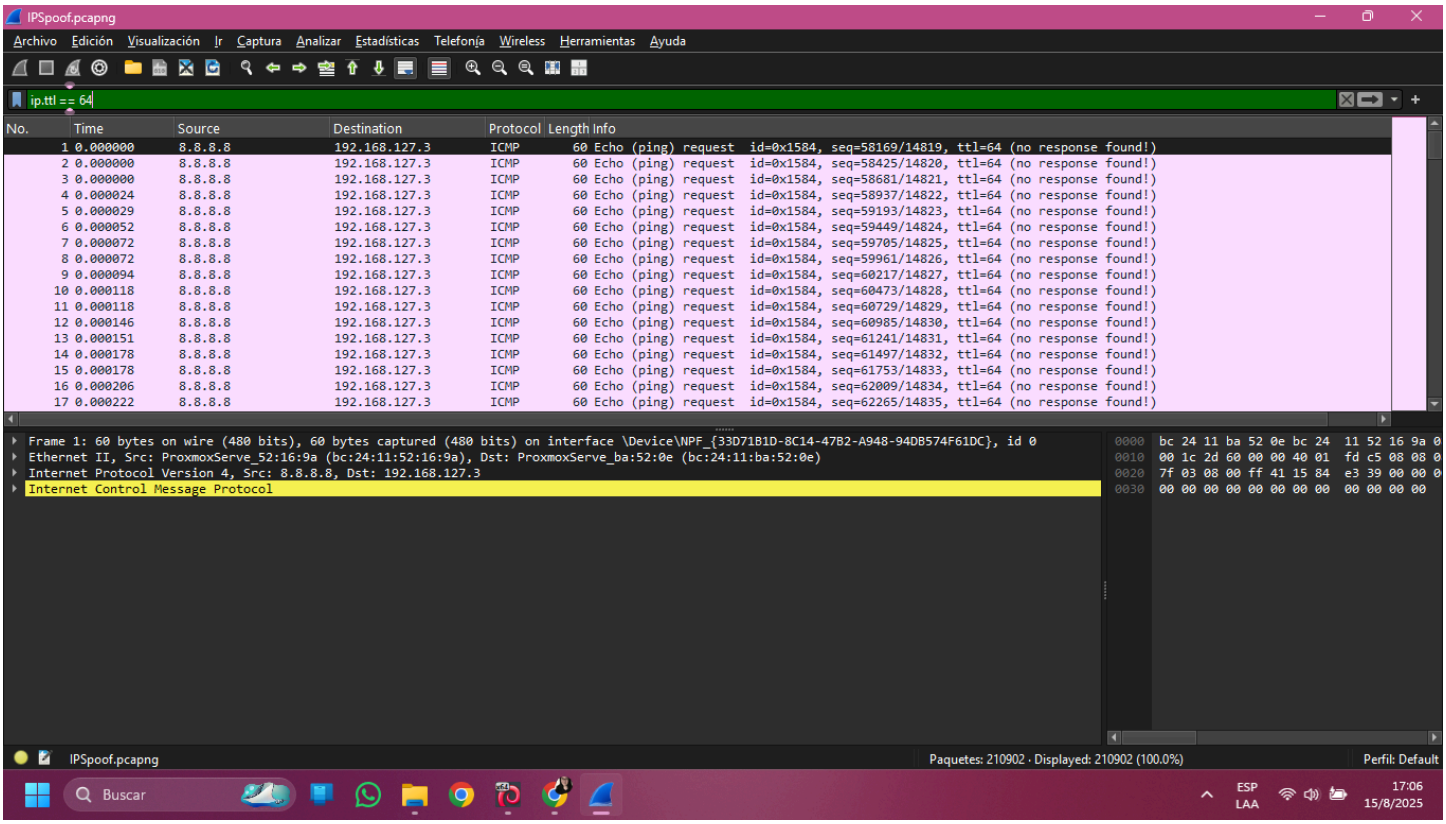
Evidencia N.º 2:

Aplicando **ip.ttl == 64** se puede buscar directamente sobre el TTL específico (en este caso 64). Los TTL asignados son:

64 = **Linux/Unix**

128 = **Windows**

255 = **Cisco**



Conclusión:

El ataque que se pudo detectar es del tipo IP spoofing, donde el atacante envía paquetes haciéndose pasar por una IP pública, en este caso la 8.8.8.8. El análisis revela la MAC real y un TTL de 64, valor típico de sistemas Linux/Unix. También se pudo determinar por el nombre **ProxmoxServe**, que se está hablando de una tarjeta de red o interfaz virtual fabricada por **Proxmox Server Solutions**, siendo este un sistema de virtualización tipo Linux.