

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.

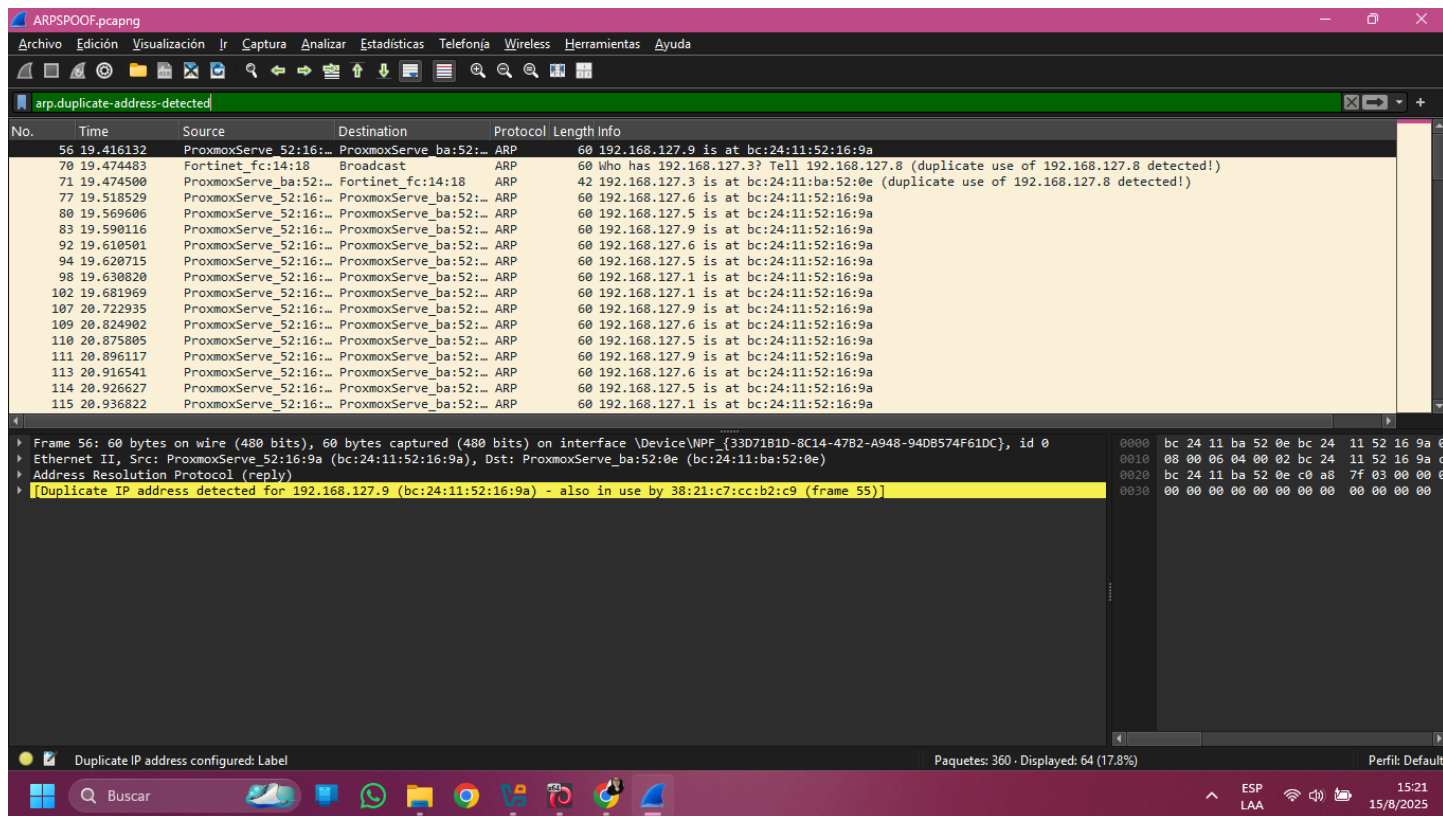
The screenshot shows the Wireshark network protocol analyzer interface. The top menu bar includes 'Archivo', 'Edición', 'Visualización', 'Ir', 'Captura', 'Analizar', 'Estadísticas', 'Telefonía', 'Wireless', 'Herramientas', and 'Ayuda'. The toolbar contains various icons for file operations, navigation, and analysis. The filter bar at the top of the packet list shows the filter 'arp'. The packet list displays 55 packets, all of which are ARP requests (Type 1) from 'ProxmoxServe_4a:e6:df' to 'Broadcast'. The selected packet (No. 1) is expanded, showing the following details:

- Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{33D71B1D-8C14-4782-A948-94D8574F61DC}, id 0
- Ethernet II, Src: ProxmoxServe_4a:e6:df (bc:24:11:4a:e6:df), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Address Resolution Protocol (request)

The packet bytes pane shows the raw data in hexadecimal and ASCII format. The status bar at the bottom indicates 'Paquetes: 360 · Displayed: 176 (48.9%)' and 'Perfit: Default'. The Windows taskbar at the bottom shows the date and time as 15:20 on 15/8/2025.

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:

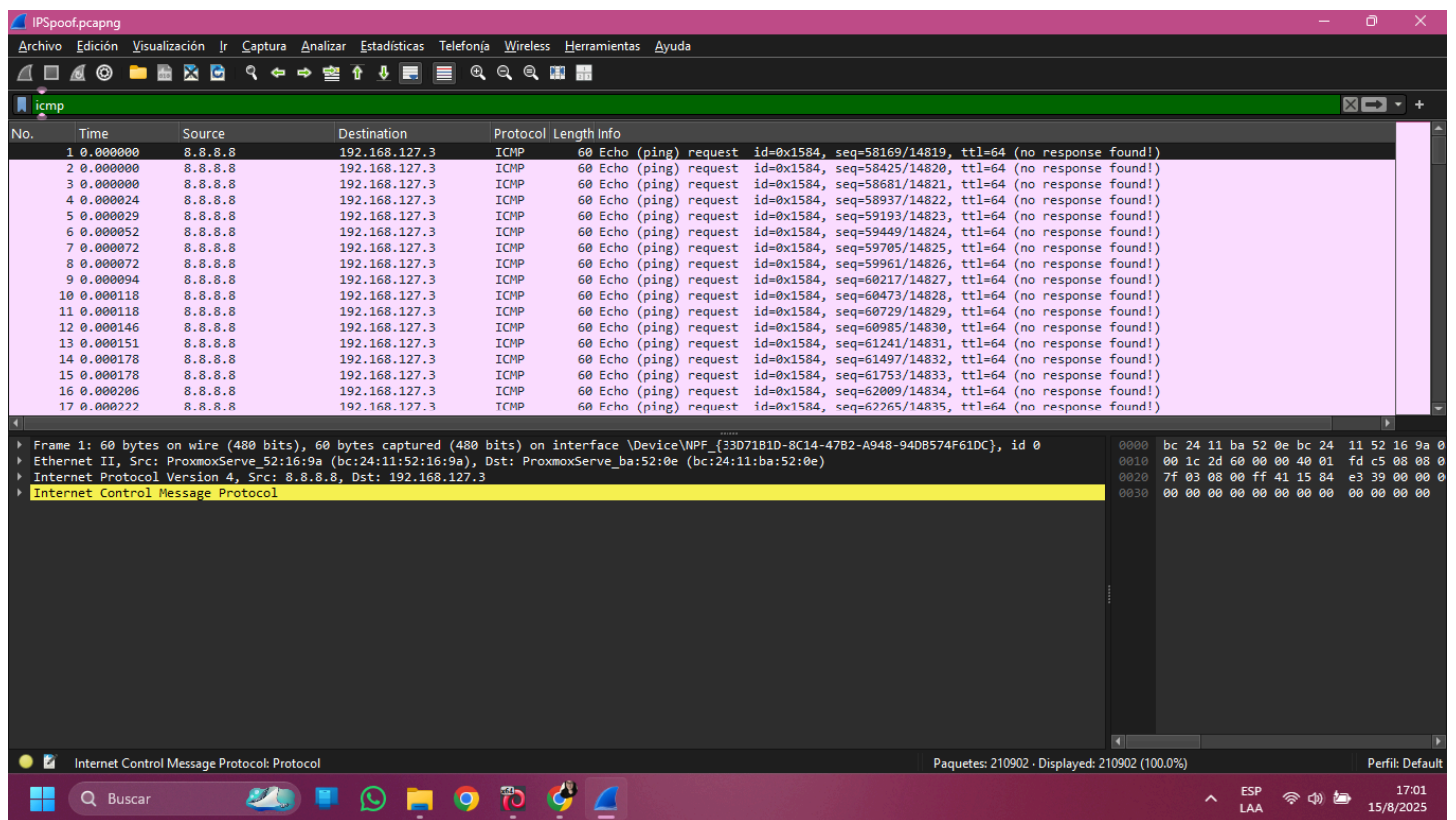
Un ataque ARP spoof puede mostrar múltiples IPs diferentes asociadas a la misma MAC, o la misma IP apareciendo con distintas MACs en poco tiempo, como se puede ver en la evidencia. Existen distintos filtros que se pueden utilizar como: `arp.opcode == 1` (muestra solicitudes), `arp.opcode == 2` (muestra 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**

The screenshot displays a Wireshark capture of network traffic. The top menu bar includes options like Archivo, Edición, Visualización, Ir, Captura, Analizar, Estadísticas, Telefonía, Wireless, Herramientas, and Ayuda. The main window is divided into three panes: Packet List, Packet Details, and Packet Bytes.

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=58169/14819, ttl=64 (no response found!)
2	0.000000	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=58425/14820, ttl=64 (no response found!)
3	0.000000	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=58681/14821, ttl=64 (no response found!)
4	0.000024	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=58937/14822, ttl=64 (no response found!)
5	0.000029	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=59193/14823, ttl=64 (no response found!)
6	0.000052	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=59449/14824, ttl=64 (no response found!)
7	0.000072	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=59705/14825, ttl=64 (no response found!)
8	0.000072	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=59961/14826, ttl=64 (no response found!)
9	0.000094	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=60217/14827, ttl=64 (no response found!)
10	0.000118	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=60473/14828, ttl=64 (no response found!)
11	0.000118	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=60729/14829, ttl=64 (no response found!)
12	0.000146	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=60985/14830, ttl=64 (no response found!)
13	0.000151	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=61241/14831, ttl=64 (no response found!)
14	0.000178	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=61497/14832, ttl=64 (no response found!)
15	0.000178	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=61753/14833, ttl=64 (no response found!)
16	0.000206	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=62009/14834, ttl=64 (no response found!)
17	0.000222	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=62265/14835, ttl=64 (no response found!)

Packet Details:

- Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{33D7181D-8C14-47B2-A948-94D8574F61DC}, id 0
- Ethernet II, Src: ProxmoxServe_52:16:9a (bc:24:11:52:16:9a), Dst: ProxmoxServe_ba:52:0e (bc:24:11:ba:52:0e)
- Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.127.3
- Internet Control Message Protocol

Packet Bytes:

```

0000  bc 24 11 ba 52 0e bc 24 11 52 16 9a 0
0010  00 1c 2d 60 00 00 40 01 fd c5 08 08 0
0020  7f 03 08 00 ff 41 15 84 e3 39 00 00 0
0030  00 00 00 00 00 00 00 00 00 00 00 00
  
```

The bottom status bar shows "Paquetes: 210902 · Displayed: 210902 (100.00%)". The taskbar at the bottom includes a search bar and various application icons.

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.