



COMUNIDAD DOJO

Primer Laboratorio de Análisis Forense

Ejercicio de Spoofing

Nombre: Eduardo Jurado
Correo: eduardoj2056@gmail.com
Fecha: August 14, 2025

1. ¿Cuál es la dirección MAC del atacante? Justifique con evidencias de las capturas ARPSPOOF.pcagna e IPSpoof.pcagna.

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

Evidencia técnica:

- Al aplicar el filtro `arp.opcode == 2` en Wireshark, se observan múltiples respuestas ARP donde distintas direcciones IP (192.168.127.9, 192.168.127.8, 192.168.127.6, etc.) anuncian el mismo MAC address `bc:24:11:52:16:9a`.
- En una red legítima, cada dirección IP debe corresponder a un único MAC address. La aparición de un solo MAC address reclamando múltiples IPs es indicativo claro de ARP spoofing.
- Wireshark identifica este MAC como `ProxmoxServe_52:16:9a`, sugiriendo una tarjeta de red virtual de Proxmox.

No.	Time	Source	Destination	Protocol	Length	Info
166	45.245829	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.9 is at bc:24:11:52:16:9a
167	45.296559	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.8 is at bc:24:11:52:16:9a
168	45.347150	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:52:16:9a
169	45.397864	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:52:16:9a
170	45.418212	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.9 is at bc:24:11:52:16:9a
171	45.428340	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.8 is at bc:24:11:52:16:9a
172	45.438519	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:52:16:9a
173	45.448749	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:52:16:9a
174	45.458934	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.1 is at bc:24:11:52:16:9a
175	45.509703	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.1 is at bc:24:11:52:16:9a
176	53.159180	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.9 is at 38:21:c7:cc:b2:c9
177	53.209666	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.8 is at e8:ed:d6:fc:14:18
178	53.260256	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:ea:20:71
179	53.311037	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:4a:e6:df
180	53.331292	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.9 is at 38:21:c7:cc:b2:c9
181	53.341308	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.8 is at e8:ed:d6:fc:14:18
182	53.351604	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:ea:20:71
183	53.361531	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:4a:e6:df
184	53.371663	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.1 is at 04:d5:90:b1:08:4e
185	53.422263	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.1 is at 04:d5:90:b1:08:4e
186	54.462729	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.9 is at 38:21:c7:cc:b2:c9
187	54.513428	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.8 is at e8:ed:d6:fc:14:18
188	54.564086	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:ea:20:71
189	54.614738	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:4a:e6:df
190	54.634919	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.9 is at 38:21:c7:cc:b2:c9
191	54.645053	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.8 is at e8:ed:d6:fc:14:18
192	54.655283	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:ea:20:71
193	54.665348	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:4a:e6:df
194	54.675423	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.1 is at 04:d5:90:b1:08:4e
195	54.726023	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.1 is at 04:d5:90:b1:08:4e
222	55.760721	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.9 is at 38:21:c7:cc:b2:c9
223	55.817574	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.8 is at e8:ed:d6:fc:14:18
224	55.868351	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:ea:20:71
225	55.919094	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:4a:e6:df
226	55.939172	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.9 is at 38:21:c7:cc:b2:c9
227	55.949405	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.8 is at e8:ed:d6:fc:14:18
228	55.959523	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:ea:20:71
229	55.969604	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:4a:e6:df
230	55.979817	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.1 is at 04:d5:90:b1:08:4e
231	56.930383	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.1 is at 04:d5:90:b1:08:4e

Figure 1: Evidencia de ARP Spoofing mostrando múltiples IPs asociadas al mismo MAC address

2. ¿Cuál es el sistema operativo del atacante? Justifique con evidencias de las capturas ARPSPOOF.pcapng e IPSpoof.pcapng.

Sistema operativo identificado: Linux (probablemente en entorno Proxmox)

Análisis forense:

- **TTL Analysis:**

- Paquetes filtrados con `eth.src == bc:24:11:52:16:9a` muestran TTL=64 consistentemente
- Valores típicos: Linux/Unix=64, Windows=128, dispositivos de red=255

- **OS Fingerprinting:**

- El tamaño de ventana TCP en varios paquetes coincide con implementaciones estándar de Linux
- El patrón de flags TCP es consistente con stacks de red Linux

- **Contexto adicional:**

- El prefijo OUI `bc:24:11` corresponde a tarjetas de red virtuales
- La resolución de nombre `ProxmoxServe_52:16:9a` sugiere un hipervisor Linux

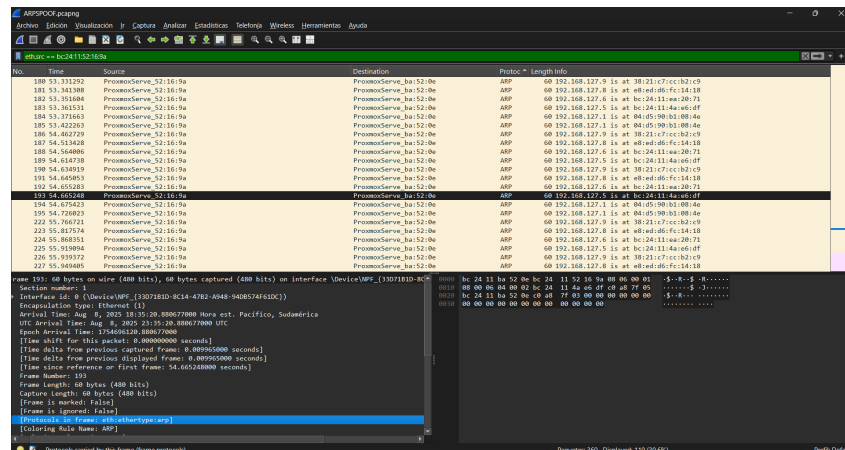


Figure 2: Análisis de paquetes mostrando TTL=64 (huella de Linux)