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.

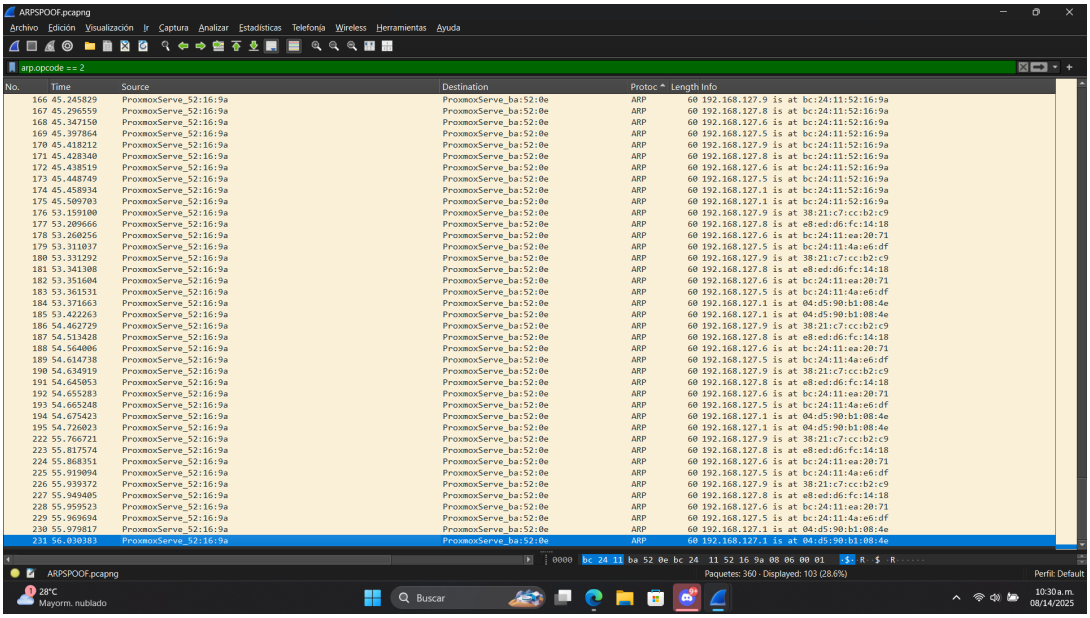

Figure 1: Evidencia de ARP Spoofing mostrando múltiples IPs asociadas al mismo MAC address

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

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

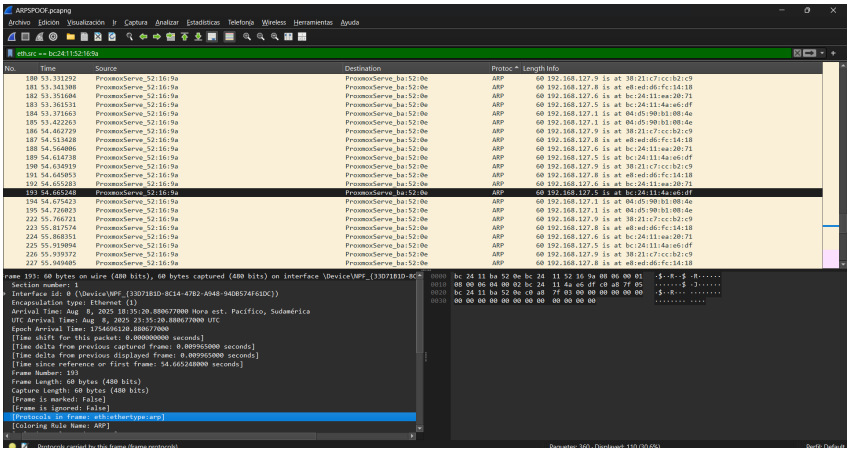

Figure 2: Análisis de paquetes mostrando TTL=64 (huella de Linux)