

LABORATORIO

Analisis Forense con WireShark

Pregunta 1 : ¿Cual es la mac address del atacante?. Justifica con evidencia

Captura ARPSPOOF.pcapng

The screenshot shows the Wireshark interface with the capture file ARPSPOOF.pcapng loaded. The packet list pane displays several ARP packets. The packet details pane shows the details of an ARP reply (packet 179) from source MAC bc:24:11:52:16:9a to target MAC bc:24:11:52:16:9a. The packet bytes pane shows the raw data of the ARP reply.

No.	Time	Source	Destination	Protocol	Length	Info
164	39.948417	ProxmoxServe_4a:e6:df	Broadcast	ARP	60	Who has 192.168.127.11? Tell 192.168.127.5
165	40.972361	ProxmoxServe_4a:e6:df	Broadcast	ARP	60	Who has 192.168.127.11? Tell 192.168.127.5
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	53.159100	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	53.268256	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.6 is at bc:24:11:52:16:9a
179	53.311037	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:0e	ARP	60	192.168.127.5 is at bc:24:11:52:16:9a

Packet 179 details:

- Destination: ProxmoxServe_ba:52:0e (bc:24:11:52:16:9a)
- Source: ProxmoxServe_52:16:9a (bc:24:11:52:16:9a)
- Type: ARP (0x0806)
- [Stream index: 4]
- Padding: 00000000000000000000000000000000
- Address Resolution Protocol (reply)
- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: reply (2)
- Sender MAC address: ProxmoxServe_52:16:9a (bc:24:11:52:16:9a)
- Sender IP address: 192.168.127.9
- Target MAC address: ProxmoxServe_ba:52:0e (bc:24:11:52:16:9a)
- Target IP address: 192.168.127.3
- [Duplicate IP address detected for 192.168.127.9 (bc:24:11:52:16:9a) - also in use by 38:21:c7:cc:b2:c9]
- [Frame showing earlier use of IP address: 64]

Packet bytes:

```
0000 bc 24 11 ba 52 0e bc 24 11 52 16 9a 08 06 00 01 -.-R-.-R-.-
0010 08 00 06 04 00 02 bc 24 11 52 16 9a c0 a8 7f 09 -.-R-.-
0020 bc 24 11 ba 52 0e c0 a8 7f 03 00 00 00 00 00 -.-R-.-
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 -.-R-.-
```

R: La dirección MAC **bc:24:11:52:16:9a** puede ser identificada como la del atacante, ya que aparece en múltiples campos clave del tráfico de red, incluyendo el campo "**Source MAC Address**" y el campo "**Sender MAC Address**" en respuestas ARP. Además, la captura muestra una alerta de **conflicto de IP**, indicando que la IP **192.168.127.9** está siendo utilizada simultáneamente por dos direcciones MAC distintas: **bc:24:11:52:16:9a** y **38:21:c7:cc:b2:c9**. Este tipo de comportamiento es típico en ataques de **ARP poisoning**, donde un atacante intenta redirigir el tráfico de red hacia su dispositivo mediante la falsificación de respuestas ARP.

Pregunta 2 : ¿Cual es el sistema operativo del atacante?. Justifica con evidencia

IPSpooof.pcap.png

The screenshot shows a Wireshark capture of an IP spoofing attack. The packet list displays multiple ICMP Echo (ping) requests from source IP 8.8.8.8 to destination IP 192.168.127.3. The TTL (Time to Live) for all packets is 64. The packet details pane for packet 4 is expanded, showing the IP header fields: Version: 4, Differentiated Services Field: 0x00, Total Length: 28, Identification: 0x5ee1 (24289), Flags: 0x00, Fragment Offset: 0, Time to Live: 64, Protocol: ICMP (1), Header Checksum: 0xcc44, Source Address: 8.8.8.8, Destination Address: 192.168.127.3, and Stream index: 0.

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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
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 f...
18	0.000226	8.8.8.8	192.168.127.3	ICMP	60	Echo (ping) request id=0x1584, seq=62521/14836, ttl=64 (no response f...

Internet Protocol Version 4, Src: 8.8.8.8, Dst: 192.168.127.3

- 0100 = Version: 4
- 0101 = Header Length: 20 bytes (5)
- > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
- Total Length: 28
- Identification: 0x5ee1 (24289)
- > 0000 = Flags: 0x00
- ...0 0000 0000 0000 = Fragment Offset: 0
- Time to Live: 64
- Protocol: ICMP (1)
- Header Checksum: 0xcc44 [validation disabled]
- [Header checksum status: Unverified]
- Source Address: 8.8.8.8
- Destination Address: 192.168.127.3
- [Stream index: 0]

R: En este caso el TTL (**time to live de 64**) indica que se trata de un sistema operativo Linux