

El host (bc:24:11:52:16:9a) está respondiendo "is-at" para varias IP (1,5,6,8,9).

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp.opcode == 2 && eth.src == bc:24:11:52:16:9a

No.	Time	Source	Destination	Protocol	Length	Info
160	35.144952	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.5 is at bc:24:11:52:16:9a
161	35.155042	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.1 is at bc:24:11:52:16:9a
162	35.205784	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.1 is at bc:24:11:52:16:9a
166	45.245829	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.9 is at bc:24:11:52:16:9a
167	45.296559	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.8 is at bc:24:11:52:16:9a
168	45.347150	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.5 is at bc:24:11:52:16:9a
169	45.397864	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.5 is at bc:24:11:52:16:9a
170	45.418212	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.9 is at bc:24:11:52:16:9a
171	45.428340	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.8 is at bc:24:11:52:16:9a
172	45.438519	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.6 is at bc:24:11:52:16:9a
173	45.448749	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.5 is at bc:24:11:52:16:9a
174	45.458934	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.1 is at bc:24:11:52:16:9a
175	45.509703	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.1 is at bc:24:11:52:16:9a
176	53.159100	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.9 is at 38:21:c7:cc:b2:c9
177	53.209666	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.8 is at e8:ed:d6:fc:14:18
178	53.260256	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.6 is at bc:24:11:ea:20:71
179	53.311037	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.5 is at bc:24:11:4a:e6:df
180	53.331292	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.9 is at 38:21:c7:cc:b2:c9
181	53.341308	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.8 is at e8:ed:d6:fc:14:18
182	53.351604	ProxmoxServe_52:16:9a	ProxmoxServe_ba:52:... ARP	ARP	60	192.168.127.6 is at bc:24:11:ea:20:71

```

Frame 172: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{33D71B1D-8C14-47B2-A948-94DB574F61DC}, 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)
  Destination: ProxmoxServe_ba:52:0e (bc:24:11:ba:52:0e)
  Source: ProxmoxServe_52:16:9a (bc:24:11:52:16:9a)
    Type: ARP (0x0806)
      [Stream index: 4]
        Padding: 000000000000000000000000000000000000
Address Resolution Protocol (reply)
Duplicate IP address detected for 192.168.127.6 (bc:24:11:52:16:9a) - also in use by bc:24:11:ea:20:71 (frame 75)
  
```

Por el TTL=64 consistente en primer salto y el patrón de ICMP sin data, el equipo atacante corre Linux.

[illegible]