

Wireshark ARP Packet Analysis

Trenton Carter — COMP 305, Network Security

Date: 2/24/2025

Overview

This analysis inspects a provided packet capture (arpspoof.pcap) in **Wireshark** to identify ARP spoofing behavior and confirm man-in-the-middle (MITM) activity. The goals were to: isolate ARP frames, identify anomalous IP→MAC mappings, and document evidence showing an attacker impersonating the router. This exercise developed packet-level analysis skills and familiarity with ARP protocol behavior in hostile scenarios.

Tools & Environment

- **Wireshark** — packet capture and frame inspection
- **arpspoof.pcap** — provided packet capture file containing spoofed traffic
- **Lab environment** — simulated router, attacker, and victim VMs

Methodology

Step 1 — Load and Filter

- Open arpspoof.pcap in Wireshark.
- Apply the display filter: arp to isolate Address Resolution Protocol frames.

Step 2 — Identify Suspicious Frames

- Locate suspicious frames (example used here: **Frame 3564**).
- Inspect the **Packet List** and **Packet Details** panes to compare source MAC addresses and ARP reply contents.
- Record baseline mappings observed earlier in the capture for comparison:

Router: 192.168.1.1 → 08:00:27:5e:01:7c

Attacker: 192.168.1.105 → 08:00:27:2d:f8:5a

Victim: 192.168.1.104 → 08:00:27:b8:b7:58

Step 3 — Confirm Spoofing Pattern

- Verify that the router IP (192.168.1.1) appears in ARP replies mapping to the attacker MAC (08:00:27:2d:f8:5a) in suspicious frames (e.g., frames 3564 and 3568).
- Note Wireshark warnings such as “Duplicate IP address” and highlight mismatched Sender MAC fields.

No.	Time	Source	Destination	Protocol	Length	Info
11	17.522291	PCSSystemtec_5e:01:...	Broadcast	ARP	42	Who has 192.168.1.105? Tell 192.168.1.1
22	17.523446	PCSSystemtec_2d:f8:...	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.105
25	17.772594	PCSSystemtec_5e:01:...	Broadcast	ARP	42	Who has 192.168.1.104? Tell 192.168.1.1
33	19.068321	PCSSystemtec_b8:b7:...	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.104
35	19.068723	PCSSystemtec_5e:01:...	PCSSystemtec_b8:b7:...	ARP	42	192.168.1.1 is at 08:00:27:5e:01:7c
148	83.967502	PCSSystemtec_5e:01:...	PCSSystemtec_b8:b7:...	ARP	60	Who has 192.168.1.1? Tell 192.168.1.104
149	83.967909	PCSSystemtec_5e:01:...	PCSSystemtec_b8:b7:...	ARP	42	192.168.1.1 is at 08:00:27:5e:01:7c
210	148.203590	PCSSystemtec_b8:b7:...	PCSSystemtec_5e:01:...	ARP	60	Who has 192.168.1.1? Tell 192.168.1.104
211	148.204596	PCSSystemtec_b8:b7:...	PCSSystemtec_5e:01:...	ARP	42	192.168.1.1 is at 08:00:27:5e:01:7c
305	276.508189	PCSSystemtec_b8:b7:...	PCSSystemtec_5e:01:...	ARP	60	Who has 192.168.1.1? Tell 192.168.1.104
306	276.508569	PCSSystemtec_5e:01:...	PCSSystemtec_b8:b7:...	ARP	42	192.168.1.1 is at 08:00:27:5e:01:7c
340	315.152982	PCSSystemtec_b8:b7:...	PCSSystemtec_5e:01:...	ARP	60	Who has 192.168.1.1? Tell 192.168.1.104
*	341.315.153278	PCSSystemtec_5e:01:...	PCSSystemtec_b8:b7:...	ARP	42	192.168.1.1 is at 08:00:27:5e:01:7c
3560	481.327624	PCSSystemtec_2d:f8:...	Broadcast	ARP	60	Who has 192.168.1.104? Tell 192.168.1.105
3561	481.328038	PCSSystemtec_b8:b7:...	PCSSystemtec_2d:f8:...	ARP	60	192.168.1.104 is at 08:00:27:b8:b7:58
3564	482.328454	PCSSystemtec_2d:f8:...	PCSSystemtec_b8:b7:...	ARP	60	192.168.1.1 is at 08:00:27:2d:f8:5a
3565	484.329415	PCSSystemtec_2d:f8:...	PCSSystemtec_b8:b7:...	ARP	60	192.168.1.1 is at 08:00:27:2d:f8:5a
3566	486.330243	PCSSystemtec_b8:b7:...	PCSSystemtec_2d:f8:...	ARP	60	192.168.1.1 is at 08:00:27:2d:f8:5a
3567	486.415917	PCSSystemtec_b8:b7:...	PCSSystemtec_2d:f8:...	ARP	60	Who has 192.168.1.105? Tell 192.168.1.104
3568	486.416442	PCSSystemtec_2d:f8:...	PCSSystemtec_b8:b7:...	ARP	60	192.168.1.105 is at 08:00:27:2d:f8:5a
3569	488.331278	PCSSystemtec_2d:f8:...	PCSSystemtec_b8:b7:...	ARP	60	192.168.1.1 is at 08:00:27:2d:f8:5a
3575	490.332376	PCSSystemtec_2d:f8:...	PCSSystemtec_b8:b7:...	ARP	60	192.168.1.1 is at 08:00:27:2d:f8:5a
3576	490.332386	PCSSystemtec_b8:b7:...	PCSSystemtec_2d:f8:...	ARP	60	192.168.1.1 is at 08:00:27:2d:f8:5a
▶ Frame 3564: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) 0000 08 00 27						
Ethernet II, Src: PCSSystemtec_2d:f8:5a (08:00:27:2d:f8:5a), Dst: PCSSystemtec_b8:b7:58 (08:00:27:b8:b7:58) 0010 08 00 06						
▶ Address Resolution Protocol (reply)						
▶ [Duplicate IP address detected for 192.168.1.1 (08:00:27:2d:f8:5a) - also in use by 08:00:27:5e:01:7c (0030 00 00 00						

Findings & Results

- Detected ARP spoofing:** Wireshark shows duplicate-IP warnings and IP→MAC mismatches confirming ARP poisoning.
- Confirmed attacker mapping:** Attacker MAC (08:00:27:2d:f8:5a) replaces the router's legitimate MAC in multiple ARP replies.
- Impact:** The attacker-MAC mapping enables potential interception of traffic intended for the router (MITM), demonstrating confidentiality risk.

Skills Demonstrated

Network traffic analysis; ARP protocol inspection; Wireshark filtering & frame analysis; evidence capture; reporting.

Conclusion

Wireshark's frame-level inspection effectively reveals ARP spoofing indicators (duplicate IP warnings and MAC mismatches). Regular packet inspection and ARP integrity checks are valuable tactics for early detection and forensic validation of MITM attacks.

Appendix — Commands & Filters

Display only ARP frames:

arp

Example mappings to reference:

Router: 192.168.1.1 -> 08:00:27:5e:01:7c

Attacker: 192.168.1.105 -> 08:00:27:2d:f8:5a