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.

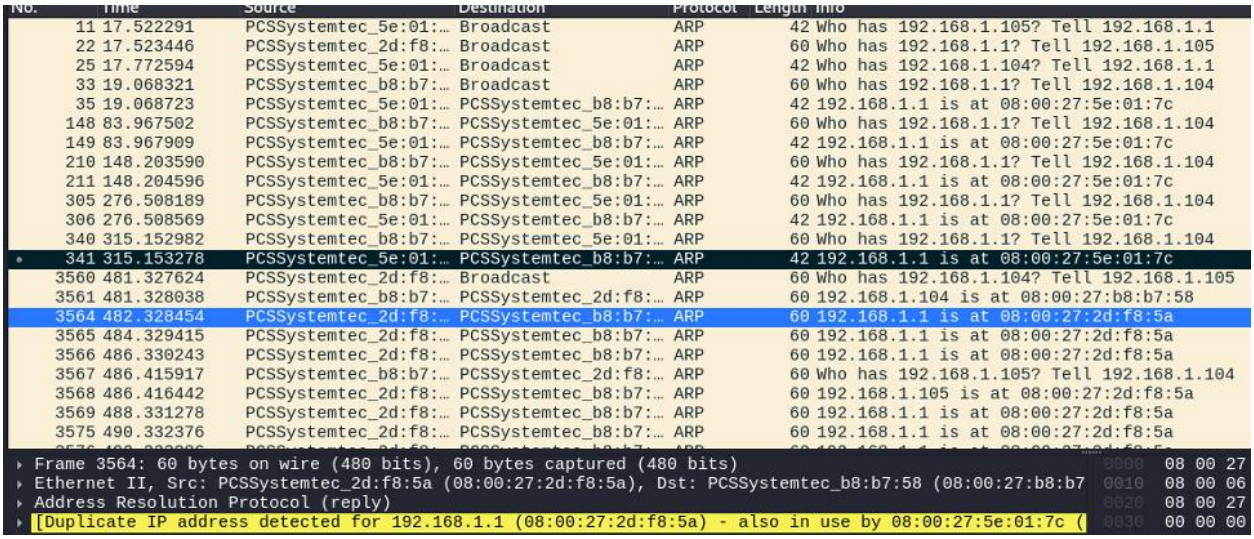
Step 2 — Identify Suspicious Frames

- 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.



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