Man in the Middle Attack in a LAN using ARP Cache Poisoning

Siam Habib
1605083

1 Steps Of Attack

1. Determine pair of nodes whose communication will be sniffed.
2. Continuously send ARP reply packets with the attacker mac and spoofed IP to the victims nodes.
3. Since the IPs have been sniffed, all communication will between the nodes will come the attacker who relays them to the appropriate destination (after making any modification that the attacker seems fit or storing them). This will require us to:
    - Receive all ethernet frames using IP packets
    - Change Ethernet mac address
    - Recompute checksums if kernel doesn't fill them (and hardware overwrites the actual checksum)

2 Result of Experiment

The attack was successful in both poisoning the arp cache of the targeted nodes and sniffing packets and relaying them.

3 Observed Outputs

3.1 ARP cache Poisoning

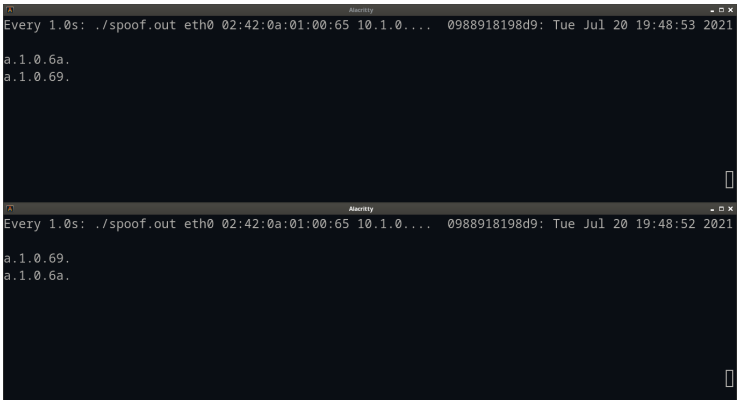

Figure 1: Attacker running spoof.out from two terminals. The top one is sending arp replies pretending to be 10.1.0.106 to 10.1.0.105 and the bottom one is sending the opposite

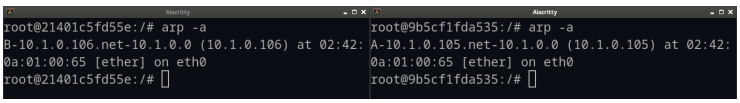

Figure 2: ARP caches of the two victims. 10.1.0.105 is in the left.

3.2 Sniffing Packets (Man in the Middle)

3.2.1 ICMP

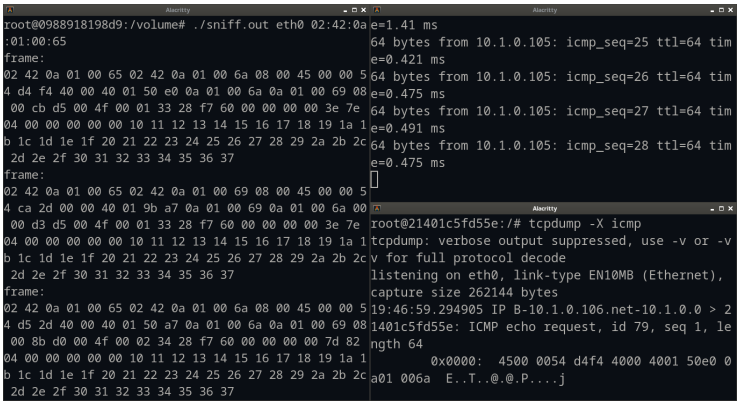

Figure 3: 10.1.0.106 (top right) is pinging 10.1.0.105 (bottom right). Attacker is sniffing their frames (left)

3.2.2 netcat via TCP

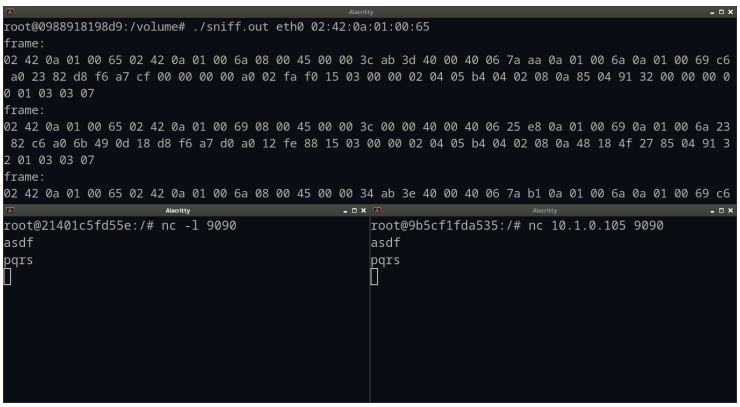

Figure 4: 10.1.0.106 (bottom right) is connecting to 10.1.0.105 (bottom left) using netcat (tcp) on port 9090. Attacker is sniffing their frames (top)

3.3 netcat via UDP

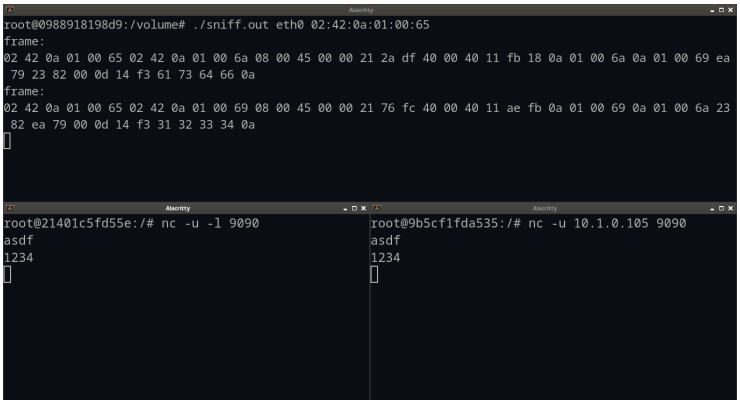

Figure 5: 10.1.0.106 (bottom right) is connecting to 10.1.0.105 (bottom left) using netcat (udp) on port 9090. Attacker is sniffing their frames (top)

3.3.1 Telnet (via TCP)

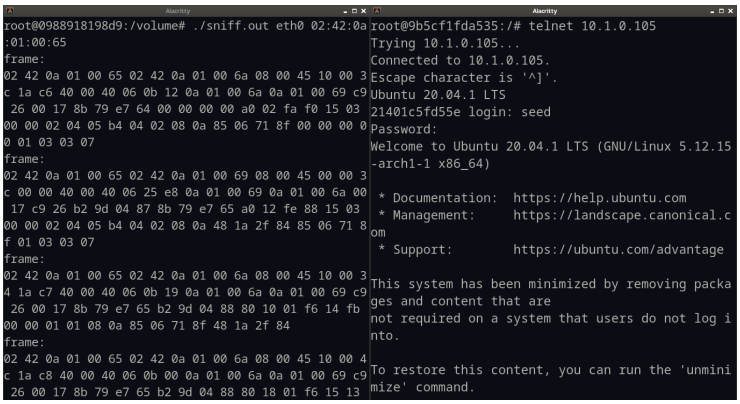

Figure 6: 10.1.0.106 (right) is connecting to 10.1.0.105 (bottom left) using telnet. Attacker is sniffing their frames (left)

4 Counter measures

No counter measures were designed, how ever the following methods can be used:

- Using static arp table

- Detect any device that has multiple IPs for the same MAC address
- Do not accept Gratuitous ARP packets