

Instituto Tecnológico de Cancún.

PoC sniffing de Bettercap.

Daniel Pérez Vélez.

Fundamentos de telecomunicaciones.

Ismael Jiménez Sánchez.

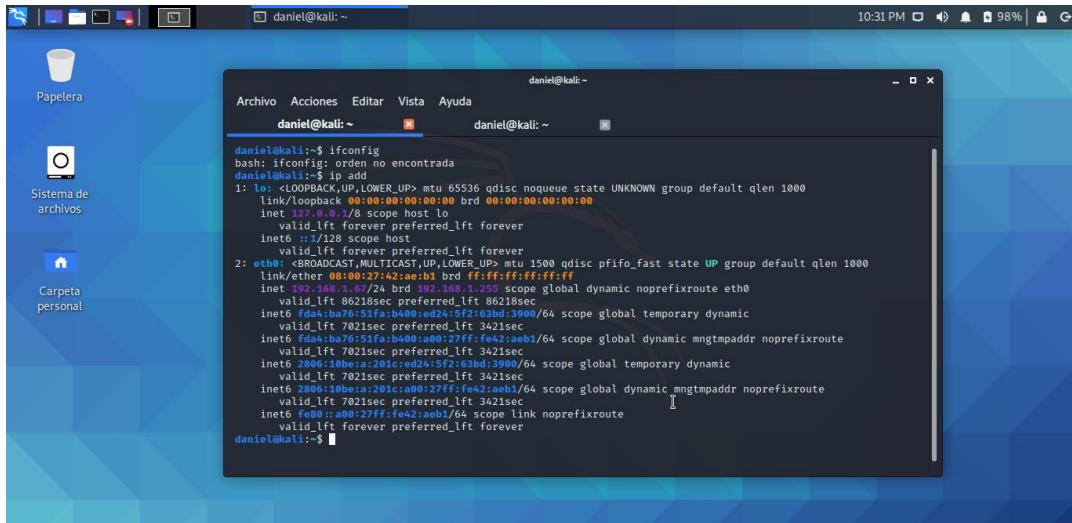
Noviembre 2020.

# Introducción.

La prueba de concepto que realicé es un sniffing dentro de mi propia red. El sistema operativo que elegí fue Kali Linux desde Virtualbox.

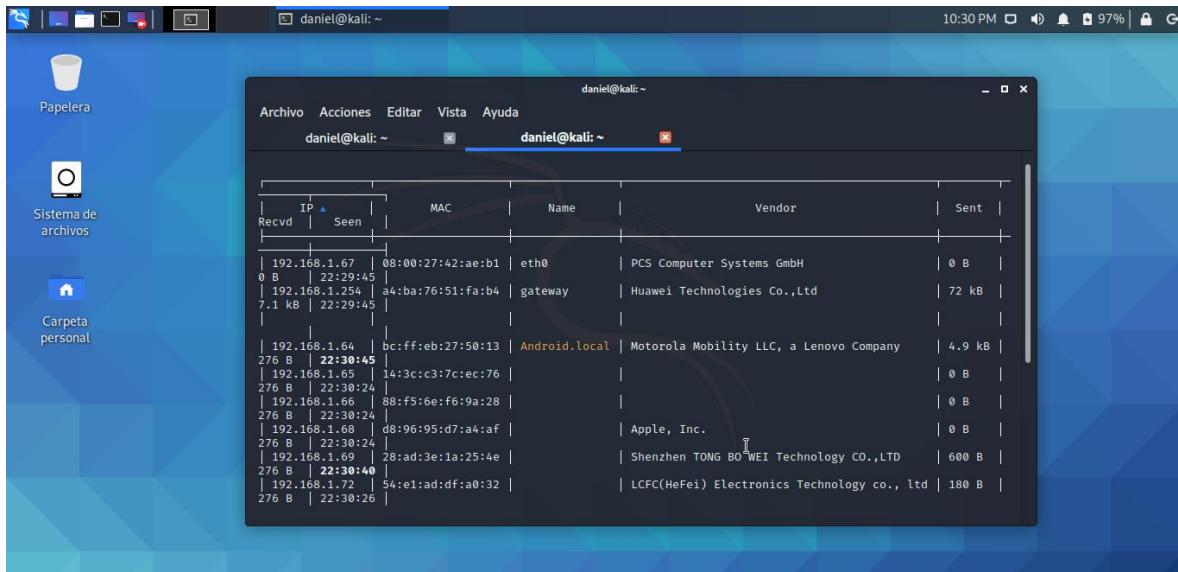
## Desarrollo.

Primero revisamos nuestra dirección IP para descartar un objetivo de sniffing.



```
daniel@kali:~$ ifconfig
bash: ifconfig: orden no encontrada
daniel@kali:~$ ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback brd 00:00:00:00:00:00
    inet 127.0.0.1/8 brd 127.0.0.1 scope host loopback
        valid_lft forever preferred_lft forever
        link/loopback brd 00:00:00:00:00:00
        inet6 ::1/128 brd :: scope host loopback
            valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 08:00:27:42:aeb1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.1.67/24 brd 192.168.1.255 scope global dynamic noprefixroute eth0
        valid_lft 86218sec preferred_lft 86218sec
        inet6 fda4:ba76:51fa:b400:d24:5f2:3bd:3900/64 scope global temporary dynamic
            valid_lft 7021sec preferred_lft 3421sec
        inet6 2806:10be:a1:20c:7a5f:5f7a:3bd:3900/64 scope global temporary dynamic
            valid_lft 7021sec preferred_lft 3421sec
        inet6 2806:10be:a1:20c:7a5f:5f7a:3bd:3900/64 scope global dynamic mngtmpaddr noprefixroute
            valid_lft 7021sec preferred_lft 3421sec
        inet6 fe80::a00:27ff:fe42:aeb1/64 scope link noprefixroute
            valid_lft forever preferred_lft forever
daniel@kali:~$
```

Acto seguido se ejecuta el comando “net.probe on” y “ticker on” para ver una tabla de direcciones que se encuentran dentro de la red.



IP	MAC	Name	Vendor	Sent
Recv	Seen			
192.168.1.67 0 B   22:29:45	08:00:27:42:ae:b1	eth0	PCS Computer Systems GmbH	0 B
192.168.1.254 7.1 kB   22:29:45	a4:ba:76:51:fa:b4	gateway	Huawei Technologies Co.,Ltd	72 kB
192.168.1.64 276 B   22:30:45	bc:ff:eb:27:50:13	Android.local	Motorola Mobility LLC, a Lenovo Company	4.9 kB
192.168.1.65 276 B   22:30:24	14:3c:c3:7c:ec:76			0 B
192.168.1.66 276 B   22:30:24	88:f5:6e:f6:9a:28			0 B
192.168.1.68 276 B   22:30:24	d8:96:95:d7:a4:af		Apple, Inc.	0 B
192.168.1.69 276 B   22:30:40	28:ad:3e:1a:25:4e		Shenzhen TONG BO WEI Technology CO.,LTD	600 B
192.168.1.72 276 B   22:30:26	54:e1:ad:df:a0:32		LCFC(HeFei) Electronics Technology co., ltd	180 B

El objetivo será el celular Motorola 192.168.1.64 y lo establecemos con "set arp.spoof.targets x.x.x.x".

```
daniel@kali:~
```

```
Archivo Acciones Editar Vista Ayuda
```

```
daniel@kali:~ daniel@kali:~
```

192.168.1.68	1.4 kB	22:30:24	1.4 kB	22:32:18	1.4 kB	22:30:26
d8:96:95:d7:a4:af	28:ad:3e:1a:25:4e	54:e1:ad:df:a0:32	Apple, Inc.	Shenzhen TONG BO WEI Technology CO.,LTD	LCFC(HeFei) Electronics Technology co., ltd	0 B
						1.9 kB
						180 B

```
↑ 202 kB / ↓ 869 kB / 12938 pkts
```

```
[192.168.1.68/24 > 192.168.1.67] » [22:30:24] [sys.log] [inf] net_probe starting net.recon as a requirement for net.probe
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.65 detected as 14:3c:c3:7c:ec:76.
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.69 detected as 28:ad:3e:1a:25:4e (Shenzhen TONG BO WEI Technolog
```

```
y CO.,LTD).
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.68 detected as d8:96:95:d7:a4:af (Apple, Inc.).
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.72 detected as 54:e1:ad:df:a0:32 (LCFC(HeFei) Electronics Techno
```

```
logy co., ltd).
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.66 detected as 88:f5:6e:f6:9a:28.
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.64 (Android.local) detected as bc:ff:eb:27:50:13 (Motorola Mobil
```

```
ity LLC, a Lenovo Company).
```

```
[22:30:26] [sys.log] [inf] ticker running with period 1s
```

```
[22:32:16] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
```

```
[192.168.1.68/24 > 192.168.1.67] »
```

Activamos el spooff y el sniff. Después se comienza a generar actividad desde el celular, por ejemplo, entrar a Chrome/Amazon, Facebook y Youtube.

```
daniel@kali:~
```

```
Archivo Acciones Editar Vista Ayuda
```

```
daniel@kali:~ daniel@kali:~
```

3.0 kB	22:34:36
--------	----------

```
↑ 453 kB / ↓ 1.8 MB / 28014 pkts
```

```
[192.168.1.68/24 > 192.168.1.67] » [22:30:24] [sys.log] [inf] net_probe starting net.recon as a requirement for net.probe
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.65 detected as 14:3c:c3:7c:ec:76,
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.69 detected as 28:ad:3e:1a:25:4e (Shenzhen TONG BO WEI Technolog
```

```
y CO.,LTD).
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.68 detected as d8:96:95:d7:a4:af (Apple, Inc.).
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.72 detected as 54:e1:ad:df:a0:32 (LCFC(HeFei) Electronics Techno
```

```
logy co., ltd).
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.66 detected as 88:f5:6e:f6:9a:28.
```

```
[22:30:24] [endpoint.new] endpoint 192.168.1.64 (Android.local) detected as bc:ff:eb:27:50:13 (Motorola Mobil
```

```
ity LLC, a Lenovo Company).
```

```
[22:30:26] [sys.log] [inf] ticker running with period 1s
```

```
[22:32:16] [sys.log] [inf] arp.spoof arp spoofer started, probing 1 targets.
```

```
[22:33:00] [net.sniff.ndns] ndns Android.local : PTR query for _233637D6_sub._googlecast._tcp.local
```

```
[22:33:00] [net.sniff.ndns] ndns Android.local : PTR query for _googlecast._tcp.local
```

```
[22:33:03] [net.sniff.ndns] ndns Android.local : PTR query for _fb._tcp.local
```

```
[22:34:34] [net.sniff.ndns] ndns Android.local : PTR query for fb._tcp.local
```

```
[22:34:38] [net.sniff.ndns] ndns Android.local : PTR query for _fb._tcp.local
```

```
[192.168.1.68/24 > 192.168.1.67] »
```

