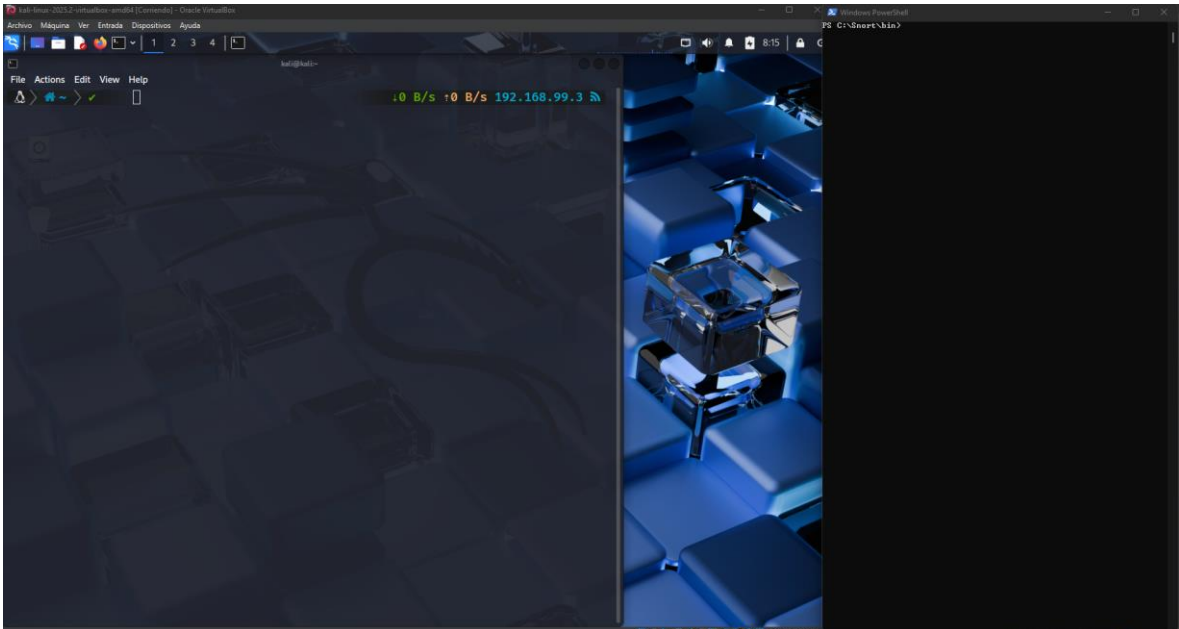


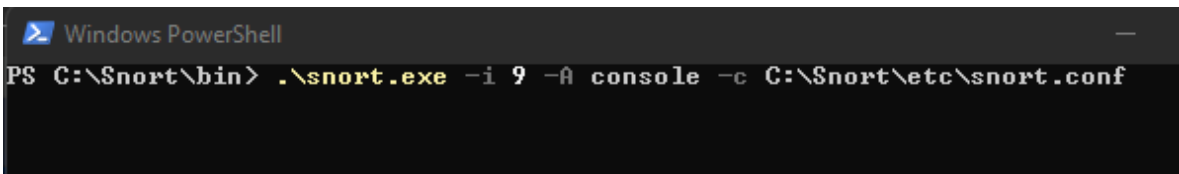


RECONOCIMIENTO DE HOST A NIVEL ORGANIZACIONAL

1. Escenario a utilizar

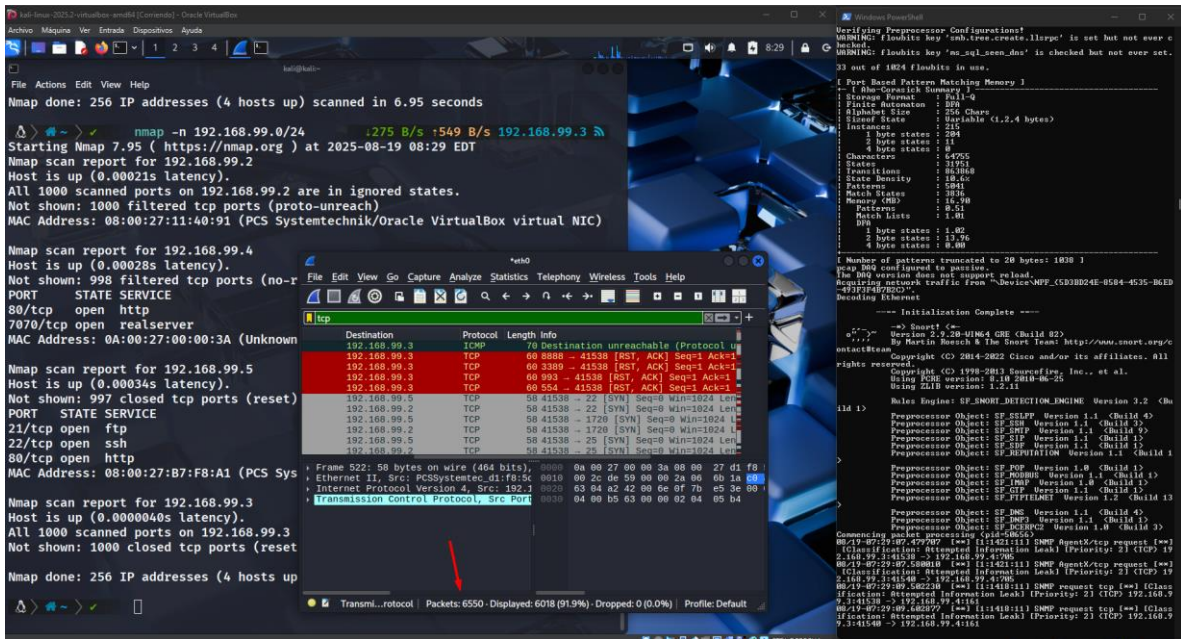
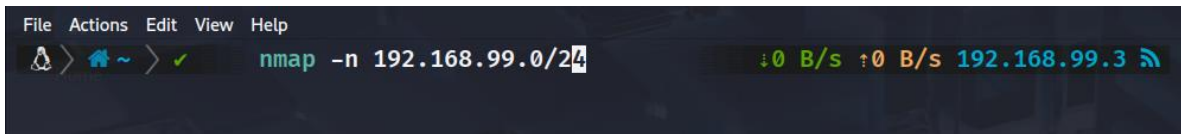


2. Utilizar snort para que empiece a monitorizar todo lo que se lleve a cabo en la infraestructura de red

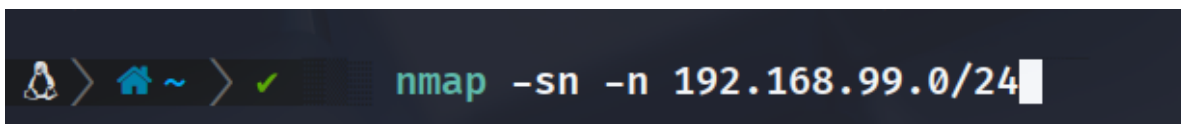


Lanzar un nmap básico

```
nmap -n 192.168.99.0/24
```



Ir a la literatura de nmap y buscar el sn que no hace escaneo de puertos





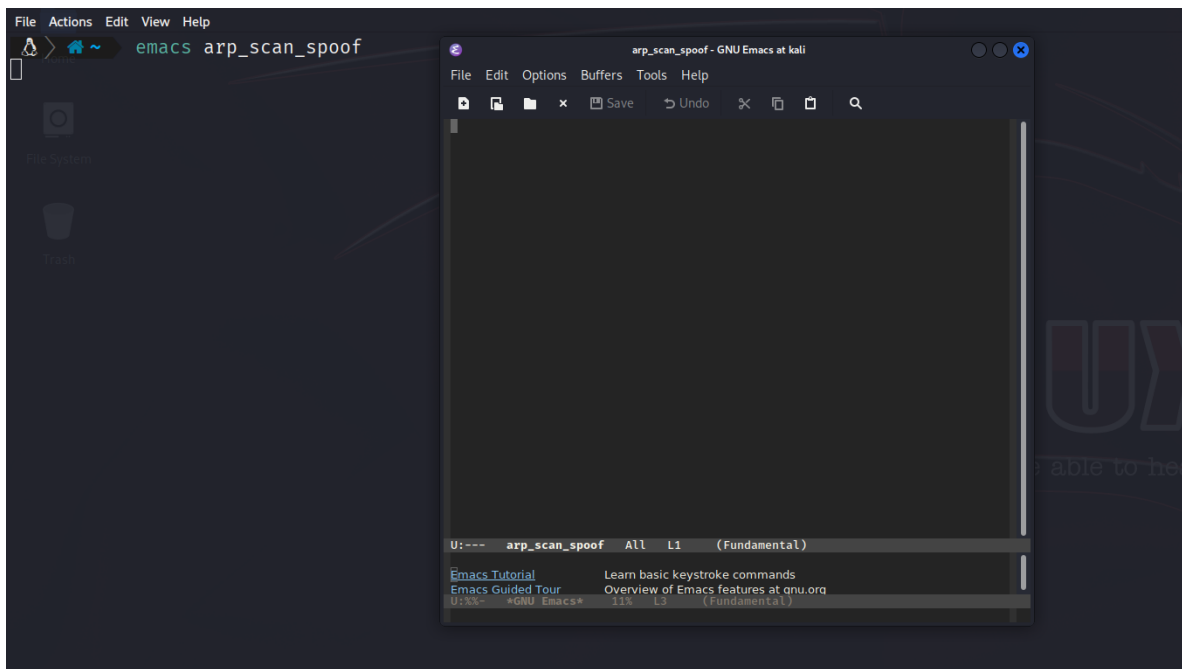
Terminal window showing Nmap scan results for 192.168.99.5 and 192.168.99.3. The scan for 192.168.99.5 shows ports 21/tcp (ftp), 22/tcp (ssh), and 80/tcp (http) open. The scan for 192.168.99.3 shows all 1000 scanned ports closed.

Wireshark packet capture showing ARP requests and responses. The packet list shows several ARP requests from 192.168.99.5 to 192.168.99.3 and responses from 192.168.99.3 to 192.168.99.5.

Wireshark packet details showing the ARP request and response structure. The packet details show the Ethernet II, Internet Protocol Version 4, User Datagram Protocol, and ARP fields.

Wireshark packet bytes showing the raw data of the ARP request and response. The packet bytes show the hexadecimal representation of the ARP request and response.

emacs arp_scan_spoof



M-x

alt

Python-mode

Vamos que scapy importe todo

```
from scapy.all import *
```

Se pón a scapy a hacer sniffing por el filtro ARP y si es así que llame a una función llamada handle_packet



```
arp_scan_spoof - GNU Emacs at kali
File Edit Options Buffers Tools Python Help
Save Undo
from scapy.all import *

sniff(filter="arp", prn=handle_packet)

U:**- arp_scan_spoof All L3 (Python ElDoc)
Welcome to GNU Emacs, one component of the GNU/Linux operating system.
Emacs Tutorial Learn basic keystroke commands
Emacs Guided Tour Overview of Emacs features at gnu.org
View Emacs Manual View the Emacs manual using Info
Absence of Warranty GNU Emacs comes with ABSOLUTELY NO WARRANTY
U:%- *GNU Emacs* Top L3 (Fundamental)
```

Ahora se deberá configurar para que crea que es otra función



```
arp_scan_spoof - GNU Emacs at kali
File Edit Options Buffers Tools Python Help
+ Save Undo
from scapy.all import *
def handle_packet(packet):
    if packet[ARP].op == 1:
        if packet.pdst == "192.168.99.11":
            print("sending ARP response")
sniff(filter="arp", prn=handle_packet)
```

ip falsa que quiero que se muestre

```
U:***- arp_scan_spoof All L7 (Python ElDoc)
Welcome to GNU Emacs, one component of the GNU/Linux operating system.
Emacs Tutorial Learn basic keystroke commands
Emacs Guided Tour Overview of Emacs features at gnu.org
View Emacs Manual View the Emacs manual using Info
Absence of Warranty GNU Emacs comes with ABSOLUTELY NO WARRANTY
U:%%- *GNU Emacs* Top L3 (Fundamental)
```

Ahora formar el paquete ARP porque ya será la respuesta vamos a ir a wire



```
arp_scan_spoof - GNU Emacs at kali
File Edit Options Buffers Tools Python Help
+ Save Undo % Copy Paste Search
from scapy.all import *

def handle_packet(packet):
    if packet[ARP].op == 1:
        if packet.pdst == "192.168.99.11":
            print("sending ARP response")
            reply = ARP(op=2,
                        hwsrc="00:0C:29:3D:1D:6F",
                        psrc="192.168.99.11",
                        hwdst="08:00:27:d1:f8:5d",
                        pdst="192.168.99.255")

sniff(filter="arp", prn=handle_packet)

U:*** arp_scan_spoof All L12 (Python ElDoc)
Welcome to GNU Emacs, one component of the GNU/Linux operating system.
Emacs Tutorial Learn basic keystroke commands
Emacs Guided Tour Overview of Emacs features at gnu.org
View Emacs Manual View the Emacs manual using Info
Absence of Warranty GNU Emacs comes with ABSOLUTELY NO WARRANTY
U:%%~ *GNU Emacs* Top L3 (Fundamental)
```

Y copiamos el destino que le responde para eso



arp.opcode == 2						
No.	Time	Source	Destination	Protocol	Length	Info
12	1.719375071	0a:00:27:00:00:3a	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.4 is at 0a:00:27:00:00:3a
13	1.719375312	PCSSystemtec_11:40:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.2 is at 08:00:27:11:40:91
14	1.719518705	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
54	2.021795987	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
178	2.325075183	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
272	2.820196091	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
306	3.122782028	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
435	3.420038488	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1

Frame 435: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec_b7:f8:a1 (08:00:27:b7:f8:a1), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)

Address Resolution Protocol (reply)

Hardware type: Ethernet (1)

Protocol type: IPv4 (0x0800)

Hardware size: 6

Protocol size: 4

Opcode: reply (2)

Sender MAC address: PCSSystemtec_b7:f8:a1 (08:00:27:b7:f8:a1)

Sender IP address: 192.168.99.5

Target MAC address: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)

Target IP address: 192.168.99.3



arp ==

No.	Time	Protocol	Length	Info
501	3.43649	ARP	42	who has 192.168.99.250? Tell
502	3.43650	ARP	42	who has 192.168.99.251? Tell
503	3.43663	ARP	42	who has 192.168.99.252? Tell
504	3.43665	ARP	42	who has 192.168.99.253? Tell
505	3.43666	ARP	42	who has 192.168.99.254? Tell
506	3.43666	ARP	42	who has 192.168.99.255? Tell
507	3.52617	ARP	42	who has 192.168.99.150? Tell
508	3.52619	ARP	42	who has 192.168.99.151? Tell
509	3.52620	ARP	42	who has 192.168.99.158? Tell
510	3.52621	ARP	42	who has 192.168.99.159? Tell
511	3.52621	ARP	42	who has 192.168.99.176? Tell
512	3.53124	ARP	42	who has 192.168.99.196? Tell
513	3.53128	ARP	42	who has 192.168.99.197? Tell
514	3.53128	ARP	42	who has 192.168.99.199? Tell
515	3.53129	ARP	42	who has 192.168.99.200? Tell
516	3.53129	ARP	42	who has 192.168.99.206? Tell
517	3.53416	ARP	42	who has 192.168.99.148? Tell
518	3.53420	ARP	42	who has 192.168.99.177? Tell
519	3.53420	ARP	42	who has 192.168.99.207? Tell
520	3.53421	ARP	42	who has 192.168.99.243? Tell
521	3.53422	ARP	42	who has 192.168.99.244? Tell

Expand Subtrees
Collapse Subtrees
Expand All
Collapse All
Apply as Column Ctrl+Shift+I
Apply as Filter
Prepare as Filter
Conversation Filter
Colorize with Filter
Follow
I/O Graph
Copy
Show Packet Bytes... Ctrl+Shift+O
Export Packet Bytes... Ctrl+Shift+X
Wiki Protocol Page
Filter Field Reference
Protocol Preferences
Decode As... Ctrl+Shift+U
Go to Linked Packet
Show Linked Packet in New Window

Selected
Not Selected
...and Selected
...or Selected
...and not Selected
...or not Selected

Frame 509: 42
Ethernet II, Src: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
Address Resolution Protocol (ARP) Request (Opcode: request (1))
Sender MAC address: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)
Sender IP address: 192.168.99.3
Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
Target IP address: 192.168.99.158

Opcode (arp.opcode) 2 bytes



kali-linux-2025.2-virtualbox-amd64 [Corriendo] - Oracle VirtualBox

Archivo Máquina Ver Entrada Dispositivos Ayuda

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

arp.opcode == 2

No.	Time	Source	Destination	Protocol	Length	Info
12	1.719375071	0a:00:27:00:00:3a	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.4 is at 0a:00:27:00:00:3a
13	1.719375312	PCSSystemtec_11:40:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.2 is at 08:00:27:11:40:91
14	1.719518705	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
54	2.021795987	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
178	2.325075183	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
272	2.820196091	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
306	3.122782028	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1
435	3.426038488	PCSSystemtec_b7:f8:...	PCSSystemtec_d1:f8:...	ARP	60	192.168.99.5 is at 08:00:27:b7:f8:a1

Frame 272: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface eth0, id 0

Ethernet II, Src: PCSSystemtec_b7:f8:a1 (08:00:27:b7:f8:a1), Dst: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)

Destination: PCSSystemtec_d1:f8:5d (08:00:27:d1:f8:5d)

.....0. = LG bit: Globally unique address (factory default)

.....0. = IG bit: Individual address (unicast)

Source: PCSSystemtec_b7:f8:a1 (08:00:27:b7:f8:a1)

Type: ARP (0x0806)

[Stream index: 4]

Padding: 00000000000000000000000000000000

Address Resolution Protocol (reply)

Opcode (arp.opcode), 2 bytes

Por último crear la capa ethernet con el destino mac original y el source es el inventado



```
arp_scan_spoof - GNU Emacs at kali
File Edit Options Buffers Tools Python Help
+ Save Undo
from scapy.all import *
def handle_packet(packet):
    if packet[ARP].op == 1:
        if packet.pdst == "192.168.99.11":
            print("sending ARP response")
            reply = ARP(op=2,
                        hwsrc="00:0C:29:3D:1D:6F",
                        psrc="192.168.99.11",
                        hwdst="08:00:27:d1:f8:5d",
                        pdst="192.168.99.255")
            pkt = Ether(dst="08:00:27:d1:f8:5d", src="00:0C:29:3D:1D:6F") / reply
            sendp(pkt)

sniff(filter="arp", prn=handle_packet)

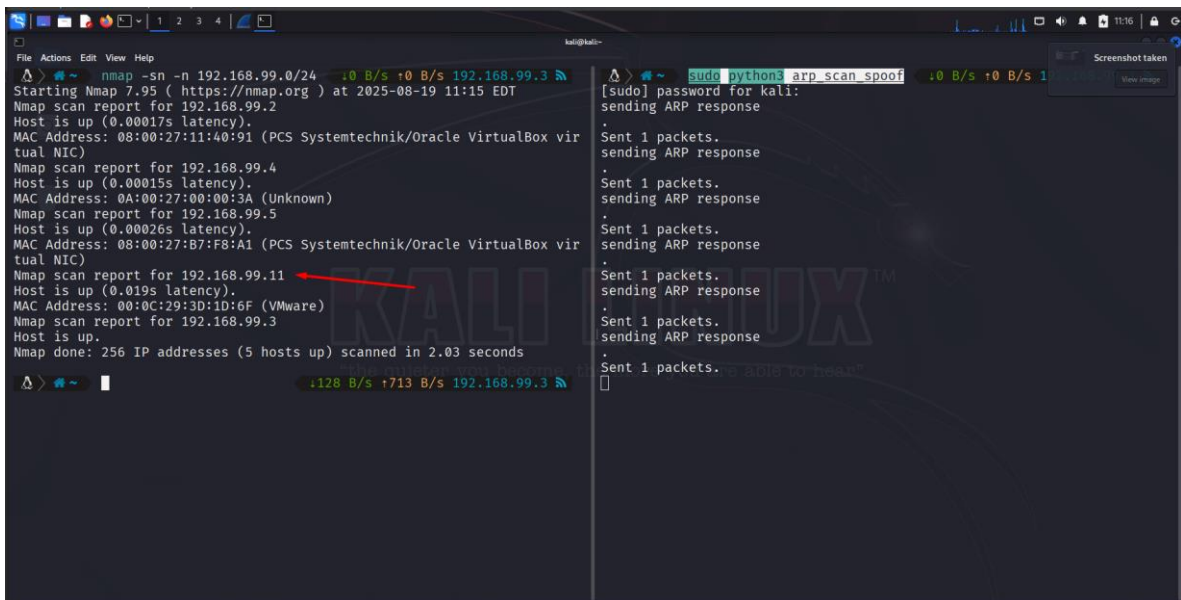
U:--- arp_scan_spoof All L12 (Python ElDoc)
Welcome to GNU Emacs, one component of the GNU/Linux operating system.
Emacs Tutorial Learn basic keystroke commands
Emacs Guided Tour Overview of Emacs features at gnu.org
View Emacs Manual View the Emacs manual using Info
Absence of Warranty GNU Emacs comes with ABSOLUTELY NO WARRANTY
U:%%- *GNU Emacs* Top L3 (Fundamental)
Undo
```

Se guarda se pone en terminal y a probar

```
sudo python3 arp_scan_spoof
```



nmap -sn -n 192.168.99.0/24



ESCANEEO AVANZADO DE PUERTOS

```
nmap -n -PS 192.168.99.0/24
```

[illegible]