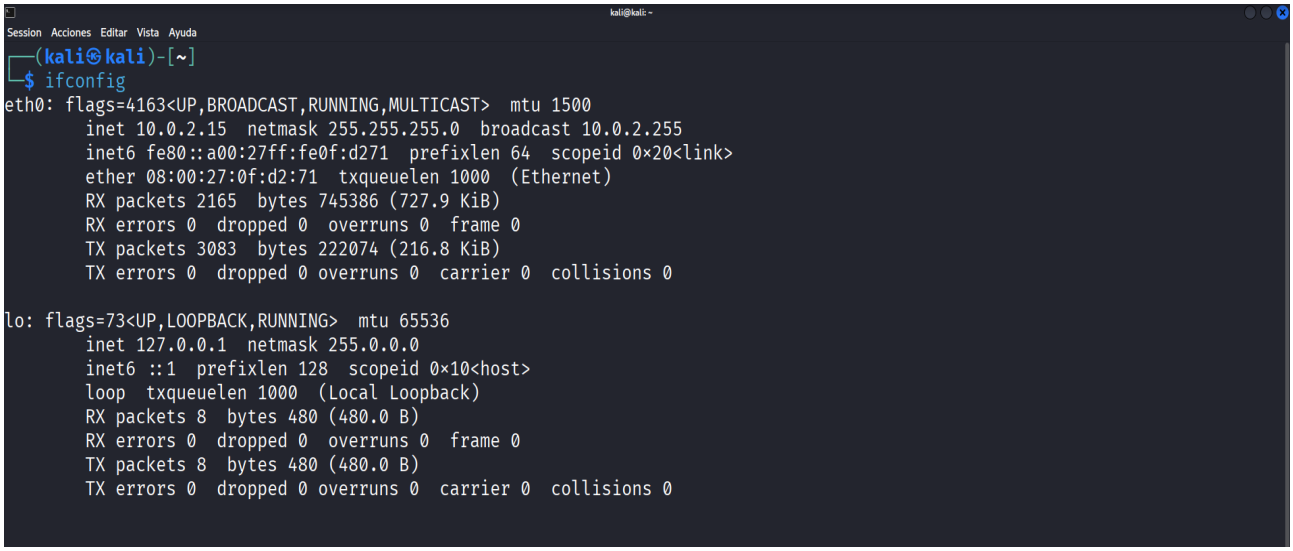
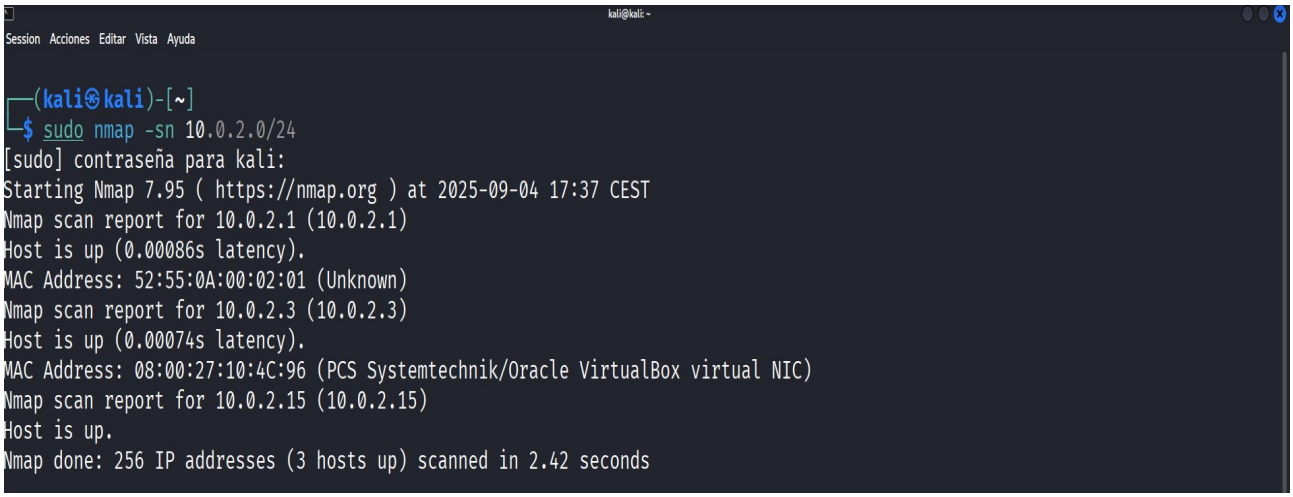
Martin
Dalla Pozza

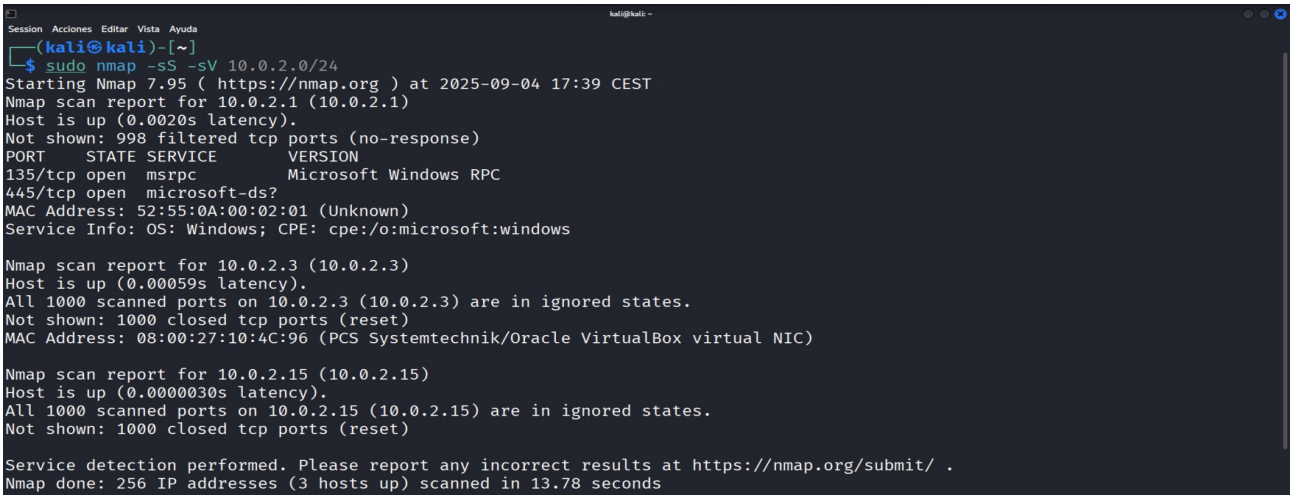
Analisis de puertos y vulnerabilididades

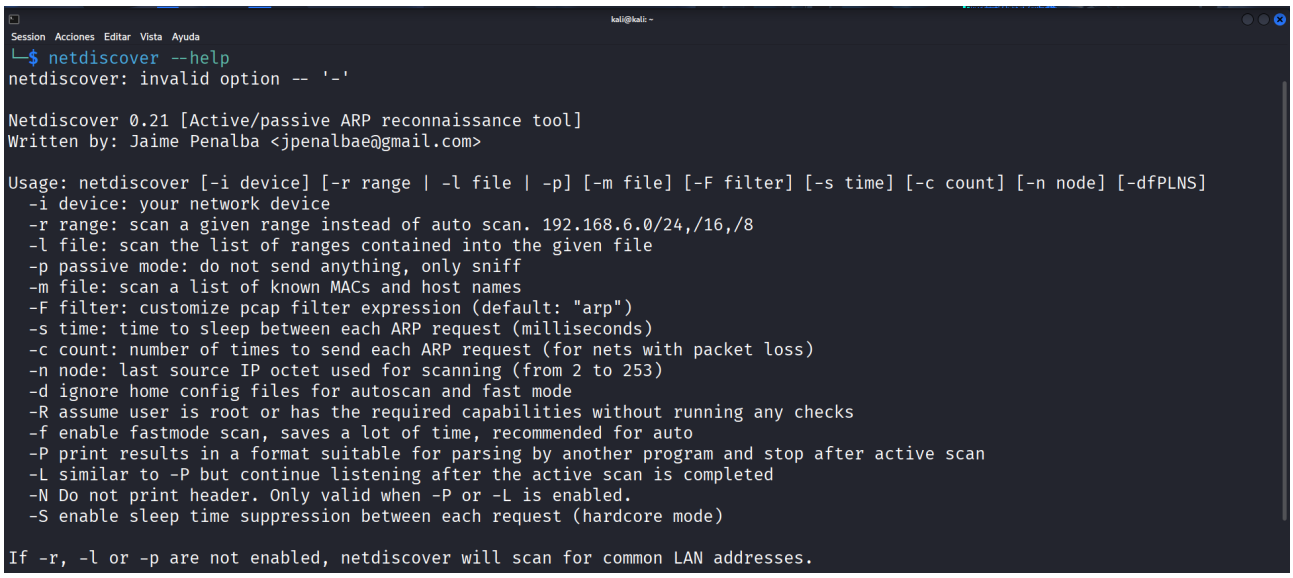
Ejercicio 1

Ejecutar nmap -sn y netdiscover

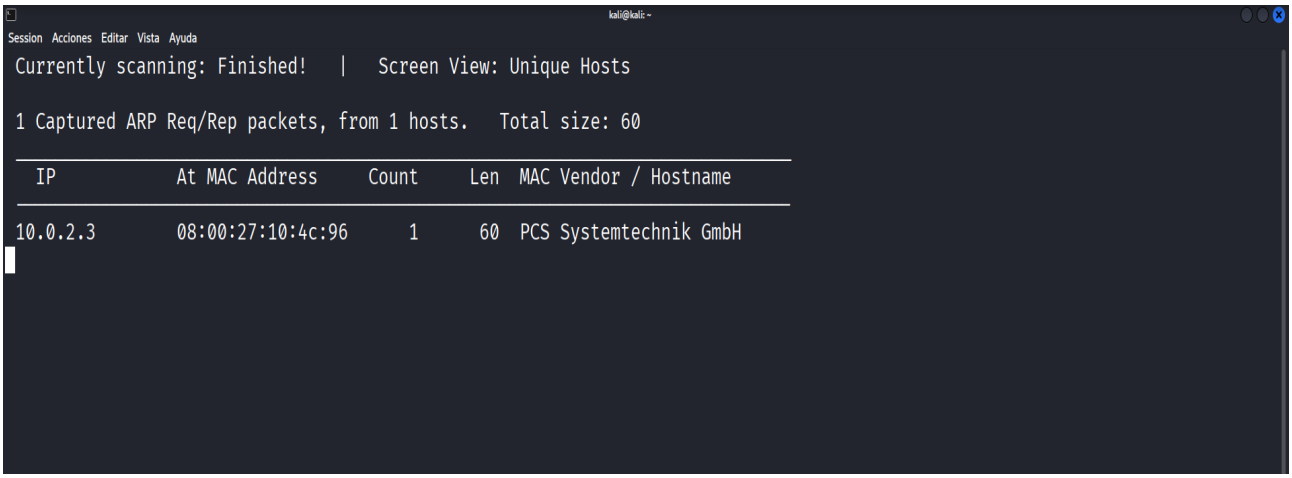

kali@kali: ~
Session Acciones Editar Vista Ayuda
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
inet6 fe80::a00:27ff:fe0f:d271 prefixlen 64 scopeid 0×20<link>
ether 08:00:27:0f:d2:71 txqueuelen 1000 (Ethernet)
RX packets 2165 bytes 745386 (727.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 3083 bytes 222074 (216.8 KiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
inet 127.0.0.1 netmask 255.0.0.0
inet6 ::1 prefixlen 128 scopeid 0×10<host>
loop txqueuelen 1000 (Local Loopback)
RX packets 8 bytes 480 (480.0 B)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 8 bytes 480 (480.0 B)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0


kali@kali: ~
Session Acciones Editar Vista Ayuda
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sn 10.0.2.0/24
[sudo] contraseña para kali:
Starting Nmap 7.95 (https://nmap.org) at 2025-09-04 17:37 CEST
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.00086s latency).
MAC Address: 52:55:0A:00:02:01 (Unknown)
Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.00074s latency).
MAC Address: 08:00:27:10:4C:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up.
Nmap done: 256 IP addresses (3 hosts up) scanned in 2.42 seconds


kali@kali: ~
Session Acciones Editar Vista Ayuda
┌──(kali㉿kali)-[~]
└─$ sudo nmap -sS -sV 10.0.2.0/24
Starting Nmap 7.95 (https://nmap.org) at 2025-09-04 17:39 CEST
Nmap scan report for 10.0.2.1 (10.0.2.1)
Host is up (0.0020s latency).
Not shown: 998 filtered tcp ports (no-response)
PORT   STATE SERVICE   VERSION
135/tcp open msrpc   Microsoft Windows RPC
445/tcp open microsoft-ds?
MAC Address: 52:55:0A:00:02:01 (Unknown)
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Nmap scan report for 10.0.2.3 (10.0.2.3)
Host is up (0.00059s latency).
All 1000 scanned ports on 10.0.2.3 (10.0.2.3) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
MAC Address: 08:00:27:10:4C:96 (PCS Systemtechnik/Oracle VirtualBox virtual NIC)
Nmap scan report for 10.0.2.15 (10.0.2.15)
Host is up (0.0000030s latency).
All 1000 scanned ports on 10.0.2.15 (10.0.2.15) are in ignored states.
Not shown: 1000 closed tcp ports (reset)
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (3 hosts up) scanned in 13.78 seconds


kali@kali: ~
Session Acciones Editar Vista Ayuda
└─$ netdiscover --help
netdiscover: invalid option -- '-'
Netdiscover 0.21 [Active/passive ARP reconnaissance tool]
Written by: Jaime Penalba <jpenalbae@gmail.com>
Usage: netdiscover [-i device] [-r range | -l file | -p] [-m file] [-F filter] [-s time] [-c count] [-n node] [-dfPLNS]
-i device: your network device
-r range: scan a given range instead of auto scan. 192.168.6.0/24,/16,/8
-l file: scan the list of ranges contained into the given file
-p passive mode: do not send anything, only sniff
-m file: scan a list of known MACs and host names
-F filter: customize pcap filter expression (default: "arp")
-s time: time to sleep between each ARP request (milliseconds)
-c count: number of times to send each ARP request (for nets with packet loss)
-n node: last source IP octet used for scanning (from 2 to 253)
-d ignore home config files for autoscan and fast mode
-R assume user is root or has the required capabilities without running any checks
-f enable fastmode scan, saves a lot of time, recommended for auto
-P print results in a format suitable for parsing by another program and stop after active scan
-L similar to -P but continue listening after the active scan is completed
-N Do not print header. Only valid when -P or -L is enabled.
-S enable sleep time suppression between each request (hardcore mode)
If -r, -l or -p are not enabled, netdiscover will scan for common LAN addresses.


kali@kali: ~
Session Acciones Editar Vista Ayuda
┌──(kali㉿kali)-[~]
└─$ sudo netdiscover -i eth0 -r 10.0.2.0/24


kali@kali: ~
Session Acciones Editar Vista Ayuda
Currently scanning: Finished! | Screen View: Unique Hosts
1 Captured ARP Req/Rep packets, from 1 hosts. Total size: 60
IP At MAC Address Count Len MAC Vendor / Hostname
10.0.2.3 08:00:27:10:4c:96 1 60 PCS Systemtechnik GmbH