

## **Resultados-informes-técnicos: CIBE**

Primero hacemos un ifconfig para saber las diferentes IP de auditor y difuncion y la mascara de subred:

```
kali㉿kali: ~
Session Actions Edit View Help
└─(kali㉿kali)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.0.159 netmask 255.255.255.0 broadcast 10.0.0.255
        inet6 fe80::d2c4:d6f7:3f8b:3214 prefixlen 64 scopeid 0x20<link>
        inet6 2001:1308:2039:bf00:c6f:c374:a325:1b39 prefixlen 64 scopeid 0
    brd 10.0.0.255
    link layer ... (physical address) ...
    RX: 0 bytes 0 packets (0 bytes/sec, 0 pkts/sec)
    TX: 0 bytes 0 packets (0 bytes/sec, 0 pkts/sec)
```

Luego hacemos el calculo de los binarios para obtener el resultado de: ROUTER, IP DE RED, PREFIJO DE RED CANTIDAD DE IP TOTALES Y ASIGNABLES Y CANTIDAD DE IP ACTIVAS.

Dirección-IP-Auditor: 10. [REDACTED]  
mascara-de-subred: 255.255.255.0  
dirección-ip-difusión: 10. [REDACTED]  
  
router: 10.0.0.1  
ip-id-red: 10.0.0.0  
prefijo-red: /24  
  
cantidad-ip-totales: 256 totales  
cantidad-ip-asignables: 254 ip asignables  
cantidad-ip-activas: 43

Ahora hacemos un sudo nmap -p- --open -vvv 10.0.0.0/24 para saber cuáles están vulnerables:

```
(kali㉿kali)-[~]
$ sudo nmap -p 445 -open -vvv 10.0.0.0/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-03 09:06 -0500
Initiating ARP Ping Scan at 09:06
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 09:06, 2.34s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 26 hosts. at 09:06
Completed Parallel DNS resolution of 26 hosts. at 09:06, 7.37s elapsed
DNS resolution of 26 IPs took 7.37s. Mode: Async [#: 2, OK: 1, NX: 25, DR: 0,
SF: 0, TR: 38, CN: 0]
Initiating Parallel DNS resolution of 1 host. at 09:06
Completed Parallel DNS resolution of 1 host. at 09:06, 1.51s elapsed
DNS resolution of 1 IPs took 1.51s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, S
F: 0, TR: 2, CN: 0]
Initiating SYN Stealth Scan at 09:06
Scanning 26 hosts [1 port/host]
Discovered open port 445/tcp on 10.0.0.129
Discovered open port 445/tcp on 10.0.0.121
Discovered open port 445/tcp on 10.0.0.149
Completed SYN Stealth Scan at 09:06, 1.35s elapsed (26 total ports)
Nmap scan report for 10.0.0.121
Host is up, received arp-response (0.074s latency).
Scanned at 2026-02-03 09:06:39 EST for 0s

PORT      STATE SERVICE      REASON
445/tcp    open  microsoft-ds syn-ack ttl 128
MAC Address: [REDACTED] (Intel Corporate)
```

```
445/tcp open  microsoft-ds syn-ack ttl 128
MAC Address: [REDACTED] (Intel Corporate)

Nmap scan report for 10.0.0.129
Host is up, received arp-response (0.090s latency).
Scanned at 2026-02-03 09:06:39 EST for 0s

PORT      STATE SERVICE      REASON
445/tcp    open  microsoft-ds syn-ack ttl 128
MAC Address: [REDACTED] (Intel Corporate)

Nmap scan report for 10.0.0.149
Host is up, received arp-response (0.076s latency).
Scanned at 2026-02-03 09:06:39 EST for 0s

PORT      STATE SERVICE      REASON
445/tcp    open  microsoft-ds syn-ack ttl 128
MAC Address: [REDACTED] (Intel Corporate)

Initiating SYN Stealth Scan at 09:06
Scanning 10.0.0.159 [1 port]
Completed SYN Stealth Scan at 09:06, 2.03s elapsed (1 total ports)
Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (27 hosts up) scanned in 14.74 seconds
Raw packets sent: 524 (15.232KB) | Rcvd: 55 (1.924KB)
```

cantidad-ip-vulnerables: 1

cantidad-puertos-abiertos: 1

cantidad-servicios-vulnerables: 15

listado-ip-vulnerables:

1. 10.0.0.129
2. 10.0.0.121
3. 10.0.0.149

listado-puertos-abiertos:

1. 445/tcp

listado-servicios-vulnerables

- 1.