



RESULTADOS-INFORME-TECNICO

1.IFCONFIG

- ▶ **adaptador-red-auditor:**
eth0
- ▶ **direccion-ip-auditor:**
inet 192.168.1.10
- ▶ **mascara-de-subred:**
netmask 255.255.255.0
- ▶ **direccion-ip-difusion:**
broadcast 192.168.1.255
- ▶ **router:** 192.168.1.1

```
(kali@kali)~[~]  
ifconfig  
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.1.10 netmask 255.255.255.0 broadcast 192.168.1.255  
    inet6 fe80::f92b:3dd9:5aa2:4fca prefixlen 64 scopeid 0x20<link>  
    ether 08:00:27:63:b0:05 txqueuelen 1000 (Ethernet)  
    RX packets 718 bytes 44737 (43.6 KiB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 23 bytes 3150 (3.0 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 0x10<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
```

2. conocimiento de subnetting, vlsm y istema binario (partiendo del resultado anterior):

- ▶ **ip-id-red: 192.168.1.0**
- ▶ **prefijo-red: 24**
- ▶ **cantidad-ip-totales: 256**
- ▶ **cantidad-ip-asignables: 254**

3. (sudo arp-scan -I eth0 --localnet) o (sudo nmap -sn [direccion-ip-red/periferico-de-red]):

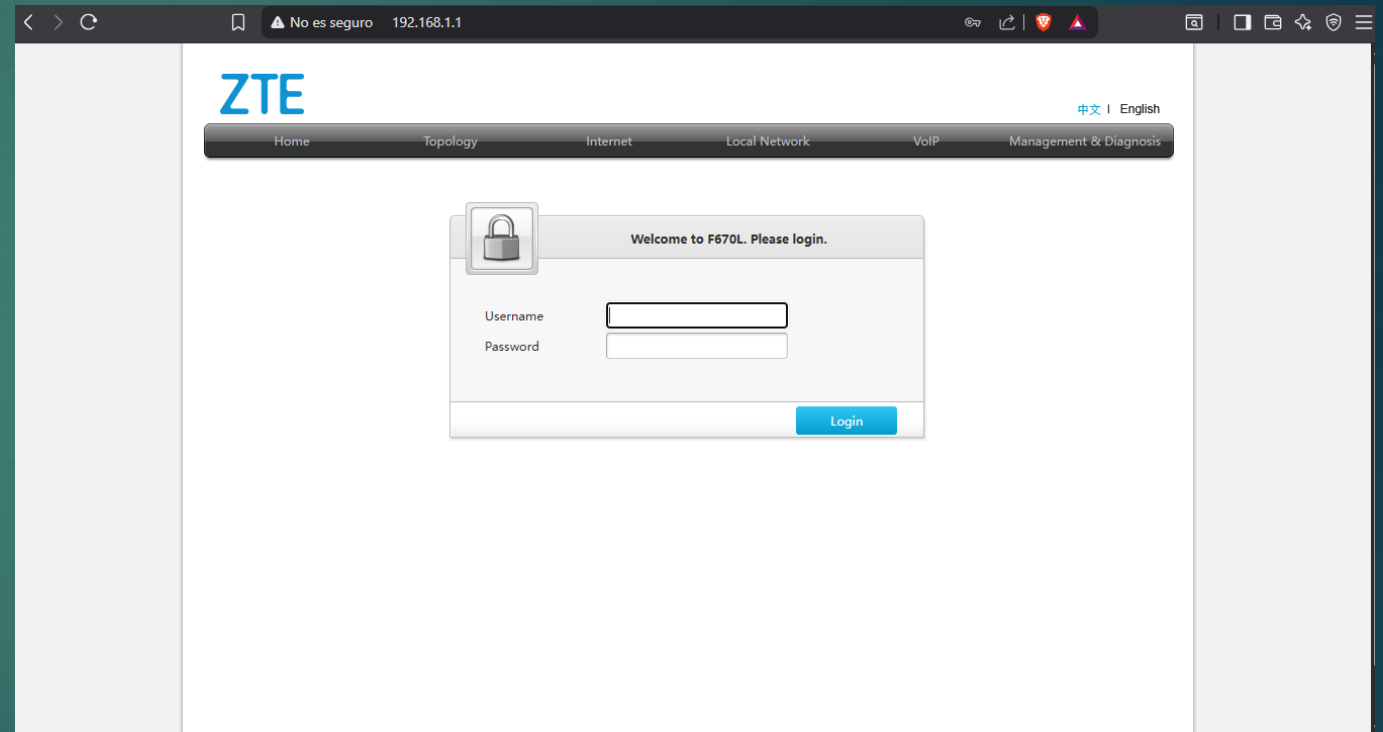
► **antidad-ip-activas: 8**

```
(kali@kali)-[~]
└─$ sudo arp-scan -I eth0 --localnet
[sudo] password for kali:
Interface: eth0, type: EN10MB, MAC: 08:00:27:63:b0:05, IPv4: 192.168.1.10
WARNING: Cannot open MAC/Vendor file ieee-oui.txt: Permission denied
WARNING: Cannot open MAC/Vendor file mac-vendor.txt: Permission denied
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
192.168.1.1      f8:73:1a:47:57:0e      (Unknown)
192.168.1.8      28:11:a8:21:a6:1a      (Unknown)
192.168.1.9      b4:45:06:7d:f7:9f      (Unknown)
192.168.1.6      fc:5b:8c:97:aa:ec      (Unknown)
192.168.1.4      48:01:c5:6f:1a:24      (Unknown)
192.168.1.3      e4:f8:be:06:57:47      (Unknown)
192.168.1.2      20:72:0d:39:51:53      (Unknown)
192.168.1.5      20:72:0d:39:51:4a      (Unknown)

8 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.840 seconds (139.13 hosts/sec). 8 responded
```

4. partiendo del resultado del comando anterior, abriendo en el navegador web la direccion ip seleccionada, sabras:

► **direccion-ip-rauter:192.168.1.1**



5.sudo nmap -p 445 --open -vvv 10.0.0.0/24:

- ▶ **cantidad-ip-vulnerables: 0**
- ▶ **cantidad-puertos-abiertos:0**
- ▶ **cantidad-servicios-vulnerables:0**
- ▶ **listado-ip-vulnerables:0**
- ▶ **listado-puertos-abiertos: 0**
- ▶ **listado-servicios-vulnerables:**

```
(kali@kali)~$ sudo nmap -p 445 --open -vvv 192.168.1.1/24
Starting Nmap 7.98 ( https://nmap.org ) at 2026-02-08 11:22 -0500
Initiating ARP Ping Scan at 11:22
Scanning 255 hosts [1 port/host]
Completed ARP Ping Scan at 11:22, 2.61s elapsed (255 total hosts)
Initiating Parallel DNS resolution of 8 hosts. at 11:22
Completed Parallel DNS resolution of 8 hosts. at 11:22, 3.02s elapsed
DNS resolution of 8 IPs took 3.02s. Mode: Async [#: 2, OK: 8, NX: 0, DR: 0, SF: 0, TR: 16, CN: 0]
Initiating Parallel DNS resolution of 1 host. at 11:22
Completed Parallel DNS resolution of 1 host. at 11:22, 2.01s elapsed
DNS resolution of 1 IPs took 2.01s. Mode: Async [#: 2, OK: 1, NX: 0, DR: 0, SF: 0, TR: 3, CN: 0]
Initiating SYN Stealth Scan at 11:22
Scanning 8 hosts [1 port/host]
Completed SYN Stealth Scan at 11:22, 0.22s elapsed (8 total ports)
Initiating SYN Stealth Scan at 11:22
Scanning 192.168.1.10 (192.168.1.10) [1 port]
Completed SYN Stealth Scan at 11:22, 2.01s elapsed (1 total ports)
Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (9 hosts up) scanned in 9.99 seconds
Raw packets sent: 521 (14.780KB) | Rcvd: 21 (692B)
```