2. Find your local IP range

```
┌──(kali㉿kali)-[~]
└─$ ip addr show
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state
UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc
fq_codel state UP group default qlen 1000
    link/ether 00:0c:29:e7:ac:ee brd ff:ff:ff:ff:ff:ff
    inet 192.168.171.128/24 brd 192.168.171.255 scope global dynamic
noprefixroute eth0
       valid_lft 1684sec preferred_lft 1684sec
    inet6 fe80::6aa2:5c5:6881:d577/64 scope link noprefixroute
       valid_lft forever preferred_lft forever

┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.168.171.128  netmask 255.255.255.0  broadcast 192.168.171.255
        inet6 fe80::6aa2:5c5:6881:d577  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:e7:ac:ee  txqueuelen 1000  (Ethernet)
        RX packets 8  bytes 928 (928.0 B)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 45  bytes 4836 (4.7 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
```

3. Perform TCP SYN Scan

```
┌──(kali㉿kali)-[~]
└─$ nmap -sS 192.168.171.128/24
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-20 06:40 EDT
Nmap scan report for 192.168.171.2
Host is up (0.00013s latency).
Not shown: 999 closed tcp ports (reset)
PORT   STATE    SERVICE
53/tcp filtered domain
MAC Address: 00:50:56:F3:9E:CA (VMware)

Nmap scan report for 192.168.171.254
Host is up (0.00013s latency).
All 1000 scanned ports on 192.168.171.254 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)
MAC Address: 00:50:56:F8:F7:66 (VMware)

Nmap scan report for 192.168.171.128
Host is up (0.0000040s latency).
All 1000 scanned ports on 192.168.171.128 are in ignored states.
Not shown: 1000 closed tcp ports (reset)
```

Nmap done: 256 IP addresses (3 hosts up) scanned in 6.23 seconds

4. Note down IP addresses and open ports found.

- 192.168.171.2
- 192.168.171.254
- 192.168.171.128

6. Research common services running on those ports.

192.168.171.2

- **What the scan shows:** Host is up. Port 53/tcp = filtered (Nmap couldn't confirm open or closed). Other 999 TCP ports showed reset (closed).
- **Likely meaning:** DNS service may be running but blocked by a firewall/packet filter or an intrusion-prevention device. Closed other ports => host responds to TCP (RST), so it's reachable and not completely stealthy.
- **Risk (short):** If DNS is actually running and accessible from attackers, it can be abused (DNS poisoning, zone transfers if misconfigured). If filtered, risk is mainly misconfiguration or exposed DNS when rules change.
- **Quick next check:** dig @192.168.171.2 any +tcp or nmap -sV -p 53

192.168.171.2 (service/version probe).

192.168.171.254

- **What the scan shows:** Host is up. All 1000 scanned TCP ports filtered (no-response).
- **Likely meaning:** Host is present but firewalled (drop/no-response) — often a gateway/router (address .254 commonly used for gateway) or a VM with host-based firewall set to drop probes.
- **Risk (short):** Hard to assess remotely — filtered hosts can still forward traffic or have management interfaces; if it's a gateway, misconfigurations could expose services externally.
- **Quick next check:** arp -a | grep 192.168.171.254 to confirm MAC/gateway role, or try ICMP ping ping -c3 192.168.171.254. If you have admin rights, check the gateway config.

192.168.171.128

- **What the scan shows:** Host is up. All 1000 scanned TCP ports closed (reset).
- **Likely meaning:** The host is reachable and actively rejecting TCP connections on scanned ports — no common TCP services on standard ports. Could still run UDP services or services on non-scanned ports.
- **Risk (short):** Low exposure over the scanned TCP ports. Still check UDP and non-standard ports; a closed port still reveals a live host (fingerprinting info).
- **Quick next check:** nmap -sU -p 53,123,161 192.168.171.128 (UDP common), or nmap -p- -sS -T4 192.168.171.128 if allowed (full TCP port sweep).

7.Identify potential security risks from open ports.

-> Port 53 (DNS) – If a DNS server is exposed:

- Attackers can perform DNS amplification (DDoS) or zone-transfer attacks.
- Misconfigured DNS may leak internal hostnames or IPs.
- If it's meant for internal use only, exposure to the LAN/internet is a configuration risk.

-> Filtered ports – A sign of a firewall; not a direct risk, but:

- If filtering is inconsistent, some rules may allow unauthorized access later.

-> Closed ports – Low risk now, but host still responds, confirming it's alive