

Task 1: Scan Your Local Network for Open Ports

- **Find your local IP range (e.g., 192.168.1.0/24):**

```

root@kaliinux:/home# charge
Session Session Edit View Help
--(charge) kaliinux[~]
$ sudo su
[rooe] password for charge:
--(root@kaliinux:/home)# charge
$ ip s
1: lo: <LOOPBACK,UP,>LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1 scope host
        valid_lft forever preferred_lft forever
    inet6 ::1::1 scope host noprefroute
        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 08:00:27:f1:c3:a3 brd ff:ff:ff:ff:ff:ff
    inet 192.168.43.10 scope global dynamic noprefroute eth0
        valid_lft 3045sec preferred_lft 3045sec
    inet6 fe80::c00:27ff:fe1:349:4 scope link noprefroute
        valid_lft forever preferred_lft forever
    inet6 fc00::f0e1:scopel scope global temporary dynamic
        valid_lft 3081sec preferred_lft 3081sec
    inet6 fc00::f0e1:scopel scope global dynamic mngtppaddr nopre
        valid_lft 3081sec preferred_lft 3081sec
    inet6 fe80::c00:27ff:fe1:349:4 scope link noprefroute
        valid_lft forever preferred_lft forever
[rooe] kaliinux/home# charge
$ nmap -sS 192.168.43.10
Nmap scan report for kaliinux (192.168.43.10)
Host is up (0.0000000s latency).
At least one scanned port on kaliinux (1
Not shown: 1000 closed tcp ports (reset)
3.15) are in ignored states.

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
[rooe] kaliinux/home# charge

```

- **Run: `nmap -sS 192.168.1.0/24` to perform TCP SYN scan and note down IP addresses and open ports found:**

```

Session Actions Edit View Help
5 Captured ARP Req/Rep packets, from 3 hosts. Total size: 300

IP At MAC Address Count Len MAC Vendor / Hostname
2 120 Xiaomi Communications Co Ltd
2 120 AzureWave Technology Inc.
1 60 Unknown vendor

ssh: suspended netdiscover

root@kali:~/home/charge
└─arp-scan -i
Interface: eth0, type: EN10MB
WARNING: Cannot open MAC/Vendor file ieee-cui.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)
(Unknown)
(Unknown)
(Unknown: locally administered)

19 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.879 seconds (136.24 hosts/sec), 3 responded

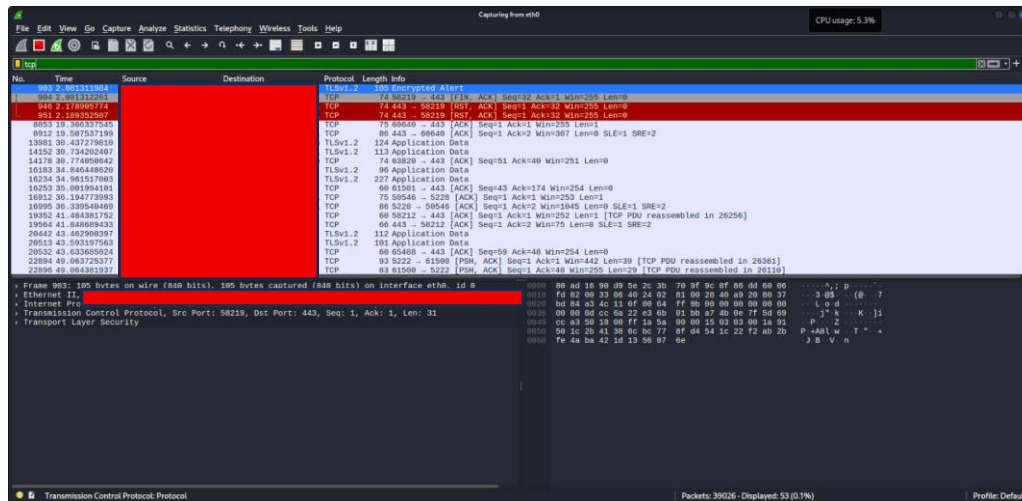
root@kali:~/home/charge
└─hmap -s 192.168.43.1
Starting Nmap 7.95 (https://nmap.org) 15-10-20 12:15:17
sendto in send_ip_packet_sd: sendto(5, ..., 44, 0, 192.168.43.1, 56) => Operation not permitted
Offending packet: TCP 192.168.43.15:49829 > 192.168.43.1:4455 win=0 len=28596 [plen=44 seq=1892670711 win=1024 <ms 1460>
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 192.168.43.1, 56) => Operation not permitted
Offending packet: TCP 192.168.43.15:49829 > 192.168.43.1:54 id=42202 [plen=44 seq=1892670711 win=1024 <ms 1460>
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 192.168.43.1, 56) => Operation not permitted
Offending packet: TCP 192.168.43.15:49831 > 192.168.43.1:39 id=2753 [plen=44 seq=1892539037 win=1024 <ms 1460>
sendto in send_ip_packet_sd: sendto(5, packet, 44, 0, 192.168.43.1, 56) => Operation not permitted
Offending packet: TCP 192.168.43.15:49831 > 192.168.43.1:4455 id=24474 [plen=44 seq=1892539037 win=1024 <ms 1460>
hmap scan report for 192.168.43.1
Host is up (0.078s latency).
Not shown: 297 closed tcp ports (reset)
PORT STATE SERVICE
53/tcp open domain
159/tcp filtered netbios-ssn
445/tcp filtered microsoft-ds
MAC Address: 82:AD:96:90:D9:5E (Xiaomi Communications)

Nmap done: 1 IP address (1 host up) scanned in 1.53 seconds

root@kali:~/home/charge
└─

```

➤ Optionally analyze packet capture with Wireshark:



➤ Research common services running on those ports:

- **Zone transfer:** TCP is required for full zone transfers between authoritative servers or from a master to a slave.
- **Authoritative DNS server:** answers queries for zones it is authoritative
- **Recursive Queries:** Resolve names reliably for clients

⇒ These are the some of services that runs on 53/tcp port.

➤ Identify potential security risks from open ports:

⇒ TCP/UDP 53 (DNS) - Zone transfer leak:

- attacker can retrieve full DNS zone, like all hostnames/IPs.
- Version/feature disclosure: reveals vulnerable software/version (helps exploit).
- Cache poisoning / DNS spoofing: redirect users to malicious sites.

⇒ TCP 139:

- Null sessions - unauthenticated info disclosure (users, shares).
- Authentication bypass or relay attacks.

⇒ TCP 445 (SMB over TCP):

- Remote code execution / worm propagation.
- Unauthorized file/share access.
- Ransomware/malware spread.