

IP :

```
(jeevika@kali)-[~/intern]
$ ip a
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 08:00:27:72:36:ed brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.15/24 brd 10.0.2.255 scope global dynamic noprefixroute eth0
        valid_lft 83528sec preferred_lft 83528sec
    inet6 fd17:625c:f037:2:febc:6f01:b3a:1b15/64 scope global temporary dynamic
        valid_lft 86035sec preferred_lft 14035sec
    inet6 fd17:625c:f037:2:a00:27ff:fe72:36ed/64 scope global dynamic mngtmpaddr noprefixroute
        valid_lft 86035sec preferred_lft 14035sec
    inet6 fe80::a00:27ff:fe72:36ed/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

## 1.NMAP SCAN ON MY MACHINE

⇒ Starting a http server:

```
(jeevika@kali)-[~]
$ sudo python3 -m http.server 80
[sudo] password for jeevika:
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
Nmap scan report for 10.0.2.15 [host down]
Nmap scan report for 10.0.2.15 [host down]
```

⇒ Output :

```
(jeevika@kali)-[~/intern]
$ sudo nmap -sS 10.0.2.15 -Pn -T4 -v
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 11:34 IST
Initiating Parallel DNS resolution of 1 host. at 11:34
Completed Parallel DNS resolution of 1 host. at 11:34, 0.01s elapsed
Initiating SYN Stealth Scan at 11:34
Scanning 10.0.2.15 [1000 ports]
Discovered open port 80/tcp on 10.0.2.15
Completed SYN Stealth Scan at 11:34, 0.04s elapsed (1000 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Read data files from: /usr/share/nmap
Nmap done: 1 IP address (1 host up) scanned in 0.13 seconds
Raw packets sent: 1000 (44.000KB) | Rcvd: 2001 (84.044KB)
```

## 2.NMAP SCAN ON MY WHOLE NETWORK

```
(jeevika@kali)-[~/Intern]  
$ sudo nmap -sS 10.0.2.0/24 -Pn -T4 -v
```

⇒Output:

```

Initiating Parallel DNS resolution of 1 host. at 11:40
Completed Parallel DNS resolution of 1 host. at 11:40, 0.04s elapsed
Initiating SYN Stealth Scan at 11:40
Scanning 2 hosts [1000 ports/host]
Discovered open port 135/tcp on 10.0.2.2
Discovered open port 53/tcp on 10.0.2.3
Completed SYN Stealth Scan against 10.0.2.3 in 0.13s (1 host left)
Discovered open port 445/tcp on 10.0.2.2
Discovered open port 8089/tcp on 10.0.2.2
Discovered open port 8000/tcp on 10.0.2.2
Discovered open port 7778/tcp on 10.0.2.2
Discovered open port 1042/tcp on 10.0.2.2
Discovered open port 1043/tcp on 10.0.2.2
Completed SYN Stealth Scan at 11:41, 4.52s elapsed (2000 total ports)
Nmap scan report for 10.0.2.2
Host is up (0.0021s latency).
Not shown: 993 filtered tcp ports (no-response)
PORT      STATE SERVICE
135/tcp    open  msrpc
445/tcp    open  microsoft-ds
1042/tcp   open  afrog
1043/tcp   open  boinc
7778/tcp   open  interwise
8000/tcp   open  http-alt
8089/tcp   open  unknown
MAC Address: 52:55:0A:00:02:02 (Unknown)

Nmap scan report for 10.0.2.3
Host is up (0.0029s latency).
Not shown: 999 filtered tcp ports (net-unreach)
PORT      STATE SERVICE
53/tcp    open  domain
MAC Address: 52:55:0A:00:02:03 (Unknown)

Initiating SYN Stealth Scan at 11:41
Scanning 10.0.2.15 [1000 ports]
Discovered open port 80/tcp on 10.0.2.15
Completed SYN Stealth Scan at 11:41, 0.03s elapsed (1000 total ports)
Nmap scan report for 10.0.2.15
Host is up (0.0000010s latency).
Not shown: 999 closed tcp ports (reset)
PORT      STATE SERVICE
80/tcp    open  http

Read data files from: /usr/share/nmap
Nmap done: 256 IP addresses (3 hosts up) scanned in 6.75 seconds
Raw packets sent: 4510 (190.232KB) | Rcvd: 3646 (181.776KB)

```

### 3.UDP SCANNING

```
import socket
```

```
sock = socket.socket(socket.AF_INET, socket.SOCK_DGRAM)
```

```
sock.bind(("0.0.0.0", 9999))
print("✅ UDP Server running on port 9999...")
```

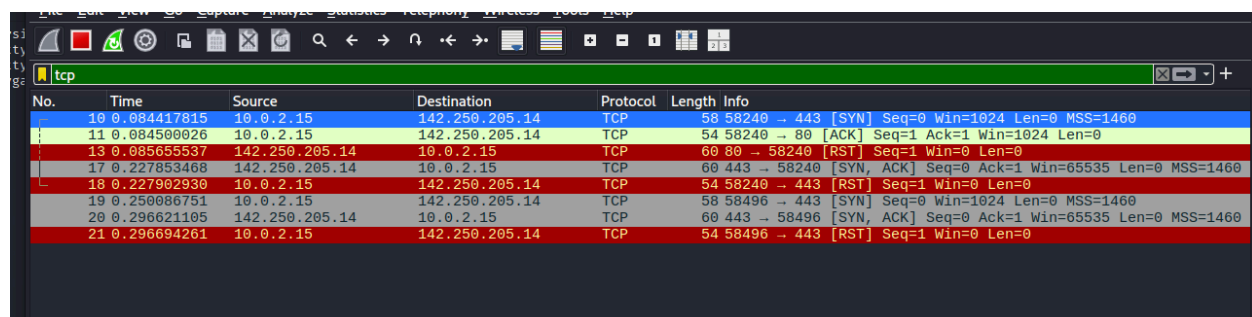
```
while True:
    data, addr = sock.recvfrom(1024)
    print(f"Received from {addr}: {data.decode()}")
    sock.sendto(b"ACK", addr)
```

```
(jeevika@kali)-[~/intern]
$ python3 udp_server.py
UDP Server running on port 9999 ...
Received from ('10.0.2.15', 33598):
```

```
(jeevika@kali)-[~]
$ sudo nmap -sU -p 9999 10.0.2.15 -Pn
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 12:03 IST
Nmap scan report for 10.0.2.15
Host is up (0.00044s latency).
Starting Nmap 7.95 ( https://nmap.org ) at 2025-06-23 11:59 IST
PORT      STATE SERVICE
9999/udp  open  distinct
```

## 4.WIRESHARK

```
(jeevika@kali)-[~]
$ sudo nmap -sS -p 443 google.com
```



No.	Time	Source	Destination	Protocol	Length	Info
10	0.084417815	10.0.2.15	142.250.205.14	TCP	58	58240 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
11	0.084500026	10.0.2.15	142.250.205.14	TCP	54	58240 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
13	0.085655537	142.250.205.14	10.0.2.15	TCP	60	80 → 58240 [RST] Seq=1 Win=0 Len=0
17	0.227853468	142.250.205.14	10.0.2.15	TCP	60	443 → 58240 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
18	0.227902930	10.0.2.15	142.250.205.14	TCP	54	58240 → 443 [RST] Seq=1 Win=0 Len=0
19	0.250086751	10.0.2.15	142.250.205.14	TCP	58	58496 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
20	0.296621105	142.250.205.14	10.0.2.15	TCP	60	443 → 58496 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
21	0.296694261	10.0.2.15	142.250.205.14	TCP	54	58496 → 443 [RST] Seq=1 Win=0 Len=0