# 📚 Scanning Networks – Zero to Hero Master Notes

## What is Scanning?

Scanning means finding details about a target network after you've identified it in the footprinting stage. It's like checking all the doors and windows of a house to see which ones are open.

Scanning is a process of identifying network and service-related information by communicating with the target. Scanning helps in identifying IP/Hostnames, Ports, Services running on ports, Live hosts, Vulnerable services running on the target network

### Purpose:

- Find **live hosts** (computers/devices that are ON).
- Find **open ports** (doorways into a system).
- Find **services** running on those ports (e.g., web server, FTP, SSH).
- Find **vulnerable services** (weak points for attack).

## 2. Types of Scanning

### A. Network Scanning

- Finds live devices on the network.
- Tools: Angry IP Scanner, Netdiscover, Nmap, hping3.

Methods:

**Ping Sweep** – Sends ICMP packets to see which devices respond.
**ARP Scan** – Uses ARP requests to find devices in local network

### B. Port Scanning

- Checks which ports are open or closed.
- Finds the service running on each port.
- Tools: Nmap, SuperScan, Zenmap.

**Port Number Basics:**

- **0–1023** → Well-known ports (HTTP 80, HTTPS 443, FTP 21, SSH 22).
- **1024–49135** → Random/Registered ports.
- **49136–65535** → Experimental/private ports.

## 3. Live Host Discovery

**Goal:** Identify which machines are turned on.

**Techniques:**

1. **ICMP Ping** – Like saying “Hello, are you there?”
2. **ARP Requests** – Works within local networks.
3. **TCP/UDP Ping** – Using ports instead of ICMP.

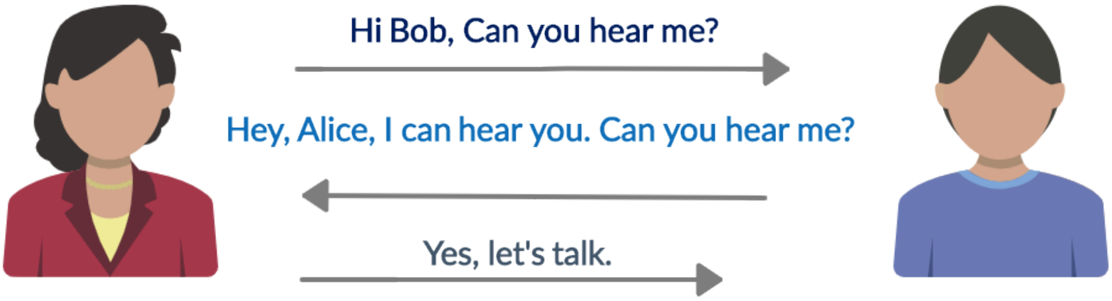
**Practical Tools & Commands:**

- **fping** → `fping -aqg 192.168.0.1/24`
- **Angry IP Scanner** → GUI tool, shows live hosts with a green dot.
- **netdiscover** → `sudo netdiscover -r 192.168.0.1/24`
- **arp-scan** → `sudo arp-scan 192.168.0.1/24`

## TCP & UDP Basics

### TCP (Transmission Control Protocol)

- Reliable, connection-based.
- Needs 3-way **handshake** before sending data:
  1. SYN → Start
  2. SYN-ACK → Acknowledge
  3. ACK → Confirm and start communication.



### UDP (User Datagram Protocol)

- Fast but unreliable, no handshake.
- Used for streaming, voice, video.

## 5. Port Scanning Techniques

### 1. TCP Connect Scan (Full Open)

```
nmap -sT <IP>
```

- Connects fully to the port.

- Easy to detect.

### 2. SYN Scan (Half-Open / Stealth)

```
sudo nmap -sS <IP>
```

- Sends SYN, waits for SYN-ACK, then drops connection.
- Harder to detect.

### 3. ACK Scan (Firewall Detection)

```
sudo nmap -sA <IP>
```

- Finds firewall rules, not open ports.

### 4. XMAS Scan

```
sudo nmap -sX <IP>
```

- Sends packets with FIN, PSH, URG flags.
- Used for bypassing filters.

### 5. FIN Scan

```
sudo nmap -sF <IP>
```

- Sends FIN to close a connection that was never open.

### 6. NULL Scan

```
sudo nmap -sN <IP>
```

- Sends packet with no flags set.

### 7. UDP Scan

```
sudo nmap -sU <IP>
```

- Finds open UDP ports.

### 8. Service Version Detection

```
sudo nmap -sV <IP>
```

- Shows service name & version.

### 9. OS Detection

```
sudo nmap -O <IP>
```

- Tries to guess the target OS.

### 10. Aggressive Scan

```
sudo nmap -A <IP>
```

- Combines OS detection, version detection, script scanning.

## Common Ports & Services

HTTP = 80

HTTPS = 443

FTP = 20,21

SSH = 22

DNS = 53

SMTP = 25

POP3 = 110

MYSQL = 3306

RDP = 3389

## Importance of Scanning

**Scanning will provide an exact outline of the network structure of the target workspace. It is beneficial for hacking target servers or individual computers. Scanning will provide a blueprint of entire network and details about devices running on the network, information related to network topology and helps in deciding what operating system is running on target computers.**

## Countermeasures

- **Block ICMP and UDP inbound.**
- **Disable unused ports with support of policy settings.**
- **Block internal IP addresses from coming inbound.**
- **Change system and application banners to counter software detection attacks.**
- **Always use a genuine operating system, update it frequently.**
- **Use IDS & IPS to detect and prevent attacks.**
- **Use “duckduckgo” or “StartPage” search engine to protect privacy**

# PRACTICALS

## Practical 1: Live Host Discovery with fping

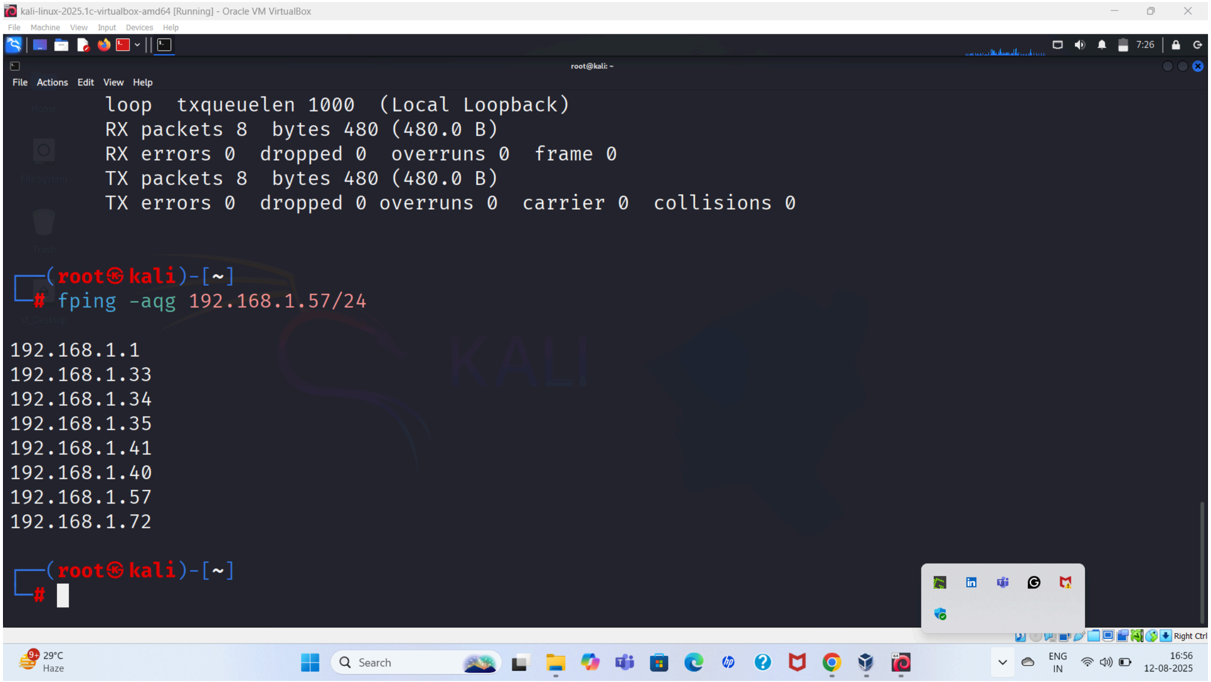
**Purpose:** Find which IP addresses in a network are active (alive).

**Command:**

fping -aqg 192.168.1.57/24

**Explanation:**

- `-a` → Show alive hosts only.
- `-q` → Quiet output (only shows results, no extra messages).
- `-g` → Generate IP range.
- `192.168.1.57/24` → Target network range.



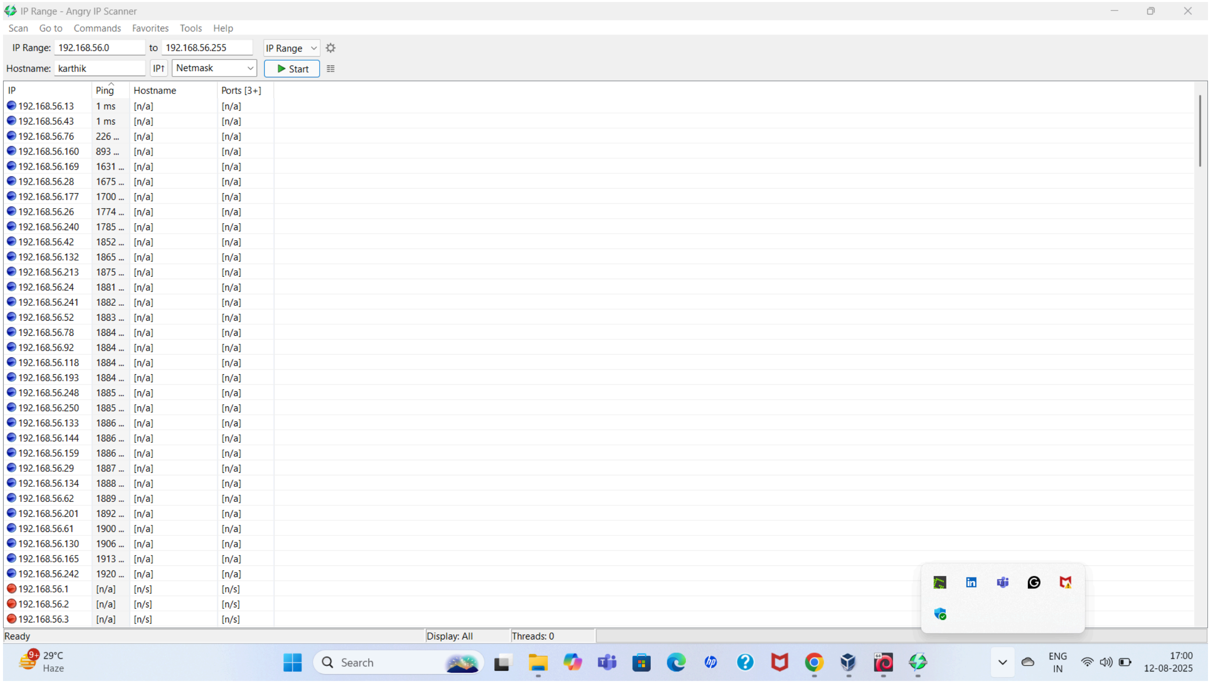
kali-linux-2025.1c-virtualbox-amd64 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
7:26
root@kali: ~
File Actions Edit View Help
Right Ctrl
29°C
Haze
Search
ENG
IN
16:56
12-08-2025

```
        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

┌──(root㉿kali)-[~]
└─# fping -aqg 192.168.1.57/24

192.168.1.1
192.168.1.33
192.168.1.34
192.168.1.35
192.168.1.41
192.168.1.40
192.168.1.57
192.168.1.72

┌──(root㉿kali)-[~]
└─# 
```

# Practical 2: Live Host Discovery with Angry IP Scanner

**Purpose:** Graphical tool to scan IP addresses and ports.

Download angry ip..



IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
Start
Display: All
Threads: 0
29°C
Haze
Search
ENG
IN
17:00
12-08-2025

IP Range: 192.168.56.0 to 192.168.56.255 IP Range

Hostname: karthik IP↑ Netmask

| IP | Ping | Hostname | Ports [3+] |
|---|---|---|---|
| ● 192.168.56.13 | 1 ms | [n/a] | [n/a] |
| ● 192.168.56.43 | 1 ms | [n/a] | [n/a] |
| ● 192.168.56.76 | 226 ... | [n/a] | [n/a] |
| ● 192.168.56.160 | 893 ... | [n/a] | [n/a] |
| ● 192.168.56.169 | 1631 ... | [n/a] | [n/a] |
| ● 192.168.56.28 | 1675 ... | [n/a] | [n/a] |
| ● 192.168.56.177 | 1700 ... | [n/a] | [n/a] |
| ● 192.168.56.26 | 1774 ... | [n/a] | [n/a] |
| ● 192.168.56.240 | 1785 ... | [n/a] | [n/a] |
| ● 192.168.56.42 | 1852 ... | [n/a] | [n/a] |
| ● 192.168.56.132 | 1865 ... | [n/a] | [n/a] |
| ● 192.168.56.213 | 1875 ... | [n/a] | [n/a] |
| ● 192.168.56.24 | 1881 ... | [n/a] | [n/a] |
| ● 192.168.56.241 | 1882 ... | [n/a] | [n/a] |
| ● 192.168.56.52 | 1883 ... | [n/a] | [n/a] |
| ● 192.168.56.78 | 1884 ... | [n/a] | [n/a] |
| ● 192.168.56.92 | 1884 ... | [n/a] | [n/a] |
| ● 192.168.56.118 | 1884 ... | [n/a] | [n/a] |
| ● 192.168.56.193 | 1884 ... | [n/a] | [n/a] |
| ● 192.168.56.248 | 1885 ... | [n/a] | [n/a] |
| ● 192.168.56.250 | 1885 ... | [n/a] | [n/a] |
| ● 192.168.56.133 | 1886 ... | [n/a] | [n/a] |
| ● 192.168.56.144 | 1886 ... | [n/a] | [n/a] |
| ● 192.168.56.159 | 1886 ... | [n/a] | [n/a] |
| ● 192.168.56.29 | 1887 ... | [n/a] | [n/a] |
| ● 192.168.56.134 | 1888 ... | [n/a] | [n/a] |
| ● 192.168.56.62 | 1889 ... | [n/a] | [n/a] |
| ● 192.168.56.201 | 1892 ... | [n/a] | [n/a] |
| ● 192.168.56.61 | 1900 ... | [n/a] | [n/a] |
| ● 192.168.56.130 | 1906 ... | [n/a] | [n/a] |
| ● 192.168.56.165 | 1913 ... | [n/a] | [n/a] |
| ● 192.168.56.242 | 1920 ... | [n/a] | [n/a] |
| ● 192.168.56.1 | [n/a] | [n/s] | [n/s] |
| ● 192.168.56.2 | [n/a] | [n/s] | [n/s] |
| ● 192.168.56.3 | [n/a] | [n/s] | [n/s] |

Ready

## Practical 4: Live Host Discovery with arp-scan

**Purpose:** Scan the local network using ARP requests.

**Command (CIDR format):**

bash

CopyEdit

```
sudo arp-scan 192.168.0.1/24
```

**Command (IP range):**

bash

CopyEdit

```
sudo arp-scan 192.168.0.1-192.168.0.255
```

---

## Practical 5: Nmap Port Scans

Nmap is a powerful network scanning tool.

---

### 1. TCP Connect Scan (Full Open)

bash

CopyEdit

```
nmap -sT 192.168.0.16
```

- Fully connects to the port → detectable.

---

### 2. SYN Scan (Half Open / Stealth)

bash

CopyEdit

```
sudo nmap -sS 192.168.0.16
```

- Sends SYN, waits for SYN-ACK, then closes connection → stealthy.

---

### 3. Version Detection Scan

bash

CopyEdit

```
sudo nmap -sV 192.168.0.16

sudo nmap -sV -p 80 192.168.0.16
```

- Shows service name and version.

---

### 4. OS Detection Scan

bash

CopyEdit

```
sudo nmap -O 192.168.0.16

sudo nmap -O -p80,443 192.168.0.16
```

- Tries to detect the target's operating system.

---

### 5. XMAS Scan

bash

CopyEdit

```
sudo nmap -sX 192.168.0.13
```

- Sends packet with **FIN, PSH, URG** flags.

---

### 6. UDP Scan

bash

CopyEdit

```
sudo nmap -sU 192.168.0.12
```

- Finds open UDP ports (slower than TCP scans).

---

### 7. Aggressive Scan

bash

CopyEdit

```
sudo nmap -A 192.168.0.13
```

- Combines OS detection, version detection, traceroute, and default scripts.

| Tool Name | Type | Main Use | Website |
|---|---|---|---|
| **Nmap** | CLI | Port scanning, service detection, OS detection | nmap.org |
| **Zenmap** | GUI | Graphical interface for Nmap | nmap.org/zenmap |
| **Angry IP Scanner** | GUI | Fast IP & port scanning | angryip.org |
| **Netdiscover** | CLI | ARP-based live host discovery | *(Pre-installed in Kali/Parrot)* |
| **arp-scan** | CLI | ARP-based host discovery on local network | linux.die.net/man/1/arp-scan |
| **fping** | CLI | Fast ping sweep for live host discovery | fping.org |
| **hping3** | CLI | Custom packet crafting & scanning | github.com/antirez/hping |