

# Network Scanning and Enumeration Report

**Course:** Network Security Fundamentals

**Student:** Michael Olayiwola

**Tools Used:**

- Angry IP Scanner
- Metasploit Framework (msfconsole)
- MegaPing
- NetScan Tools Pro

**Network Scope:** 192.168.0.0/24

## Objective

The objective of this exercise was to perform network reconnaissance on a local wireless network using multiple scanning tools in order to:

- Identify active hosts
- Detect open ports
- Retrieve hostnames and MAC addresses
- Compare scanning results across different tools

All scans were conducted within a controlled local environment.

## Tool 1: Angry IP Scanner

### Scan Configuration

- IP Range: 192.168.0.0 – 192.168.0.255
- Total Hosts Scanned: 254

## Results

- Active Hosts Discovered: 7
- Hosts with Open Ports: 2

The screenshot shows the Angry IP Scanner interface. At the top, the IP range is set from 192.168.0.0 to 192.168.0.255, with a subnet mask of /24. The 'Start' button is highlighted. Below the table, a 'Scan Statistics' dialog box is open, showing the following details:

IP	Ping	Hostname	Ports [3+]	MAC Address
192.168.0.103	0 ms	DESKTOP-T027V5K	[n/a]	08:00:27:1C....
192.168.0.1	1098 ms	[n/a]	80	24:B0:A9:A6....
192.168.0.105	1023 ms	METASPLOITABLE	80	08:00:27:45....
192.168.0.100	4141 ms	[n/a]	[n/a]	CE:48:02:DB....
192.168.0.101	4055 ms	Android.local	[n/a]	8C:98:06:7B....
192.168.0.102	4032 ms	[n/a]	[n/a]	38:BA:F8:22:....
192.168.0.104	4045 ms	[n/a]	[n/a]	08:00:27:1F:B...

**Scan Statistics**

- Scanning completed
- Total time: 52.48 sec
- Average time per host: 0.21 sec
- IP Range: 192.168.0.0 - 192.168.0.255
- Hosts scanned: 254
- Hosts alive: 7
- With open ports: 2

At the bottom, there are buttons for 'Display: Alive only' and 'Threads: 0'.

## Key Findings

- Hostnames identified (e.g., DESKTOP-T02V75K, METASPLOITABLE)
- MAC addresses successfully retrieved
- Port 80 (HTTP) identified on two hosts

## Observation

Angry IP Scanner efficiently identified live systems and provided quick visibility into exposed services. It is lightweight and effective for fast host discovery.

# Tool 2: Metasploit Framework (msfconsole)

## Methods Used

- ARP Sweep (auxiliary/scanner/discovery/arp\_sweep)
  - TCP Port Scan (auxiliary/scanner/portscan/tcp)
  - db nmap integration

## Results

- Live hosts successfully enumerated
  - Open ports identified on selected targets
  - Service versions detected using nmap integration

```
Session Actions Edit View Help
        ..fffff...
        ..fffff...
        ..fffff...
        ..fffff...
        ..fffff...

Code: 00 00 00 00 M3 T4 SP L0 IT FR 4M 3W OR K! V3 R5 I8 N5 00 00 00 00 00
Aiee, Killing Interrupt handler
Kernel panic: Attempted to kill the idle task!
10 swapper task - not syncing

      =[ metasploit v6.4.84-dev                      ]
+ -- ==[ 2,547 exploits - 1,309 auxiliary - 1,683 payloads      ]
+ -- ==[ 432 post - 49 encoders - 13 nops - 9 evasion       ]

Metasploit Documentation: https://docs.metasploit.com/
The Metasploit Framework is a Rapid7 Open Source Project

MSF > db_nmap -sv 192.168.0.24
[*] Nmap: Starting Nmap 7.95 ( https://nmap.org ) at 2026-02-12 05:26 EST
[*] Nmap: Nmap scan report for 192.168.0.1
[*] Nmap: Host is up (0.0002s latency).
[*] Nmap: Not shown: 997 closed tcp ports (reset)
[*] Nmap: PORT      STATE SERVICE      VERSION
[*] Nmap: 53/tcp    open  domain      dnsmasq 10.0
[*] Nmap: 80/tcp    open  http        Demo-Webs
[*] Nmap: 5566/tcp open  westelic-connect?
[*] Nmap: I service detection failed despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-service :
[*] Nmap: SF:port80-TCP|http|7.95X|NID-2|12|NTIME|690BAA075P|x86_64-pe-linu...gnux(Get)
[*] Nmap: SF:port80-TCP|http|7.95X|NID-2|12|NTIME|690BAA075P|x86_64-pe-linu...gnux(Get)
[*] Nmap: SF:port80-TCP|http|7.95X|NID-2|12|NTIME|690BAA075P|x86_64-pe-linu...gnux(Get)
[*] Nmap: SF:<x>207Thu</x>20Feb),x28Feb),x2823,(x2011:26:32(x207025),x)nx-Fr...x20SAM5D
[*] Nmap: SF:RIGTGNV\r\n\r\nPragm...x20no-cache\r\nCache-Control:\r\nx20no-cache\r\nContent-T
[*] Nmap: SF:ype\>x20text/html\r\nLocation:x20http://192.168.0.1/index.html\r\nx
[*] Nmap: SF:\r\nhtml\>head\>(head\>body\>)x1mt\>(this\>x20document\>x20has\>x20move...x
[*] Nmap: SF:x20/x20new(x20s\x20ref=\r\n"ht...//192.168.0.1/index.html"\>10
```

```

root@kali: /home/kali
Session Actions Edit View Help
Hosts
=====
address      mac          name  os_name  os_flavor  os_sp  purpose  info  comments
-----  -----
192.168.0.1  24:b0:a9:a6:46:5b  Unknown        device
192.168.0.102 38:BA:F8:22:62:E9
192.168.0.103 08:00:27:1c:3d:f7  Unknown        device
192.168.0.104
192.168.0.105 08:00:27:45:ae:73  Linux         server

Msf > services
Services
=====
host      port  proto  name      state  info
-----  -----
192.168.0.1  53    tcp    domain   open   dnsmasq 10.0
192.168.0.1  80    tcp    http     open   Demo-Webs
192.168.0.1  5566  tcp    westec-connect  open
192.168.0.103 5357  tcp    http     open   Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.0.103 5357  tcp    http     open
192.168.0.105 21    tcp    ftp      open   vsftpd 2.3.4
192.168.0.105 22    tcp    ssh      open   OpenSSH 4.7p1 Debian Subuntu protocol 2.0
192.168.0.105 23    tcp    telnet   open   Linux telnetd
192.168.0.105 25    tcp    smtp    open   Postfix smtpd
192.168.0.105 53    tcp    domain   open   ISC DIND 9.4.2
192.168.0.105 80    tcp    http     open   Apache httpd 2.2.8 (Ubuntu) DAV/2
192.168.0.105 111   tcp    rpcbind  open   2 RPC #100000
192.168.0.105 139   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.0.105 445   tcp    netbios-ssn  open   Samba smbd 3.X - 4.X workgroup: WORKGROUP
192.168.0.105 512   tcp    exec    open   netkit-rsh rexecd
192.168.0.105 513   tcp    login   open
192.168.0.105 514   tcp    tcpwrapped  open
192.168.0.105 1099  tcp    java-rmi  open   GNU Classpath grmiregistry
192.168.0.105 1524  tcp    bindshell  open   Metasploitable root shell
192.168.0.105 2049  tcp    nfs     open   2-4 RPC #100003
192.168.0.105 2121  tcp    ftp      open   ProFTPD 1.3.1

```

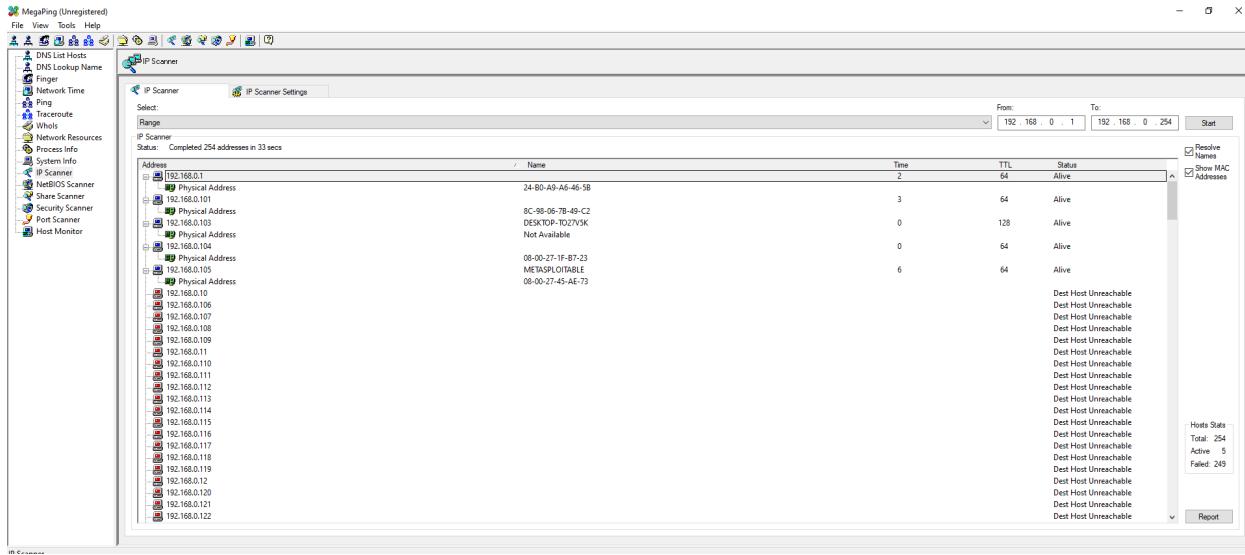
## Observation

Metasploit provides deeper integration for reconnaissance and exploitation. Unlike basic scanners, results can be stored in a database for further analysis.

## Tool 3: MegaPing

### IP Scanner Results

- Range: 192.168.0.1 – 192.168.0.254
- Active Hosts: 5
- Failed/Unreachable: 249



## Observations

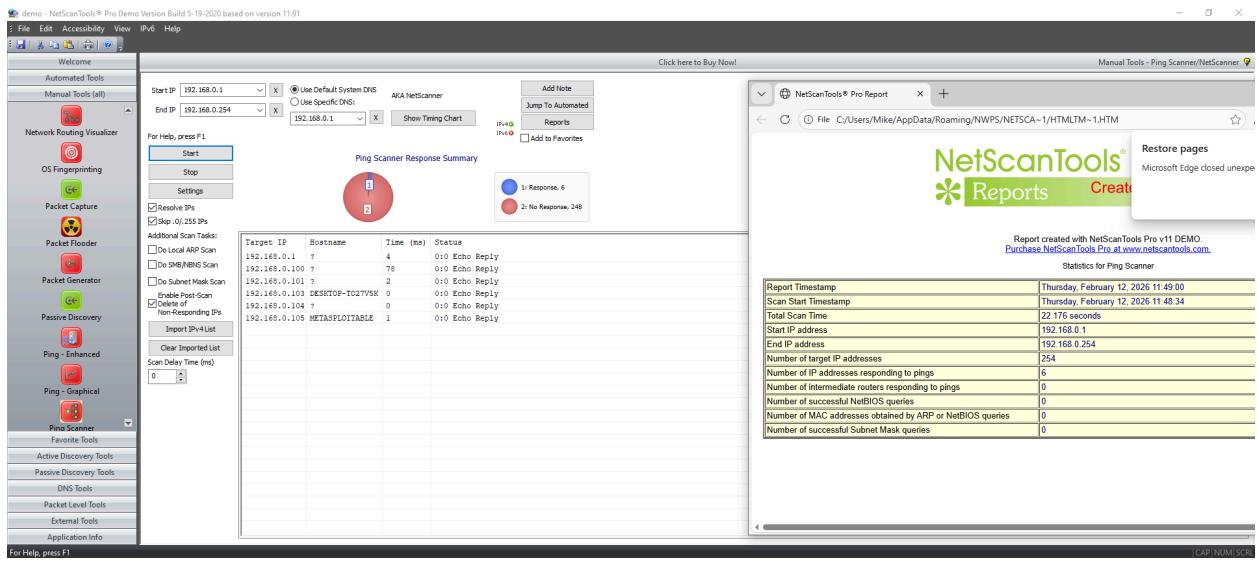
- Successfully resolved hostnames
- Retrieved physical (MAC) addresses
- Detected Metasploitable test machine

MegaPing provided clear visibility into reachable systems but offered less depth compared to Metasploit.

## Tool 4: NetScan Tools Pro

### A. Ping Scanner

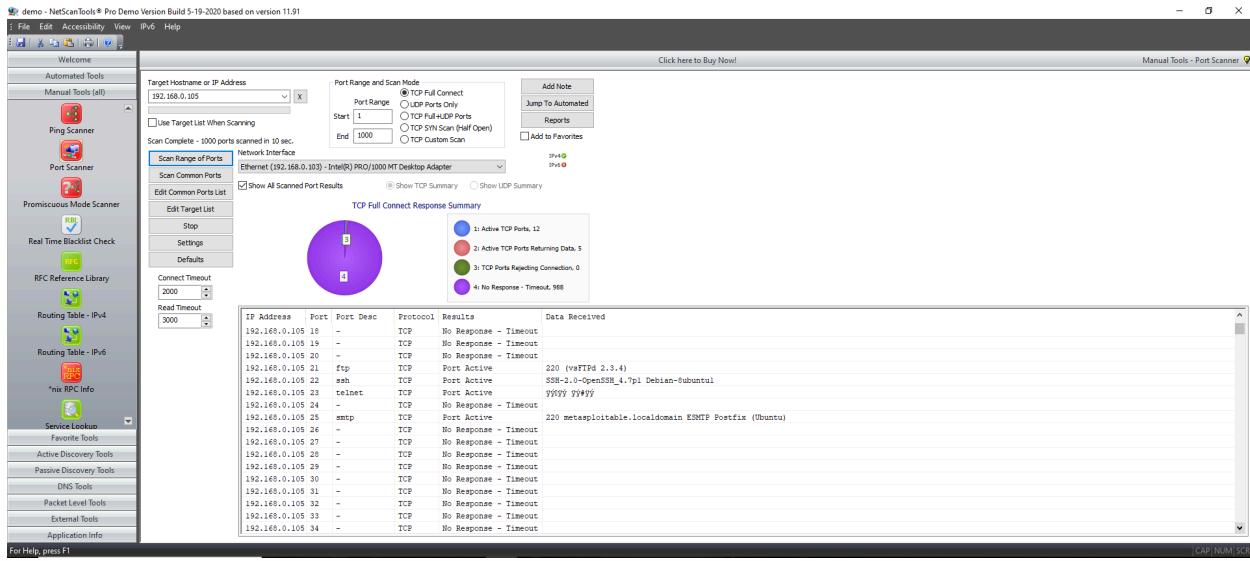
- Total IP addresses scanned: 254
- Responding hosts: 6
- Non-responding: 248
- Scan time: ~22 seconds



## B. Port Scanner (Target: 192.168.0.105 – Metasploitable)

### Open Ports Identified:

Port	Service	Version
21	FTP	vsFTPD 2.3.4
22	SSH	Open SSH 4.7p1
23	Telnet	Active
25	SMTP	Postfix (Ubuntu)



## Observations

The Metasploitable machine exposed multiple services, demonstrating a large attack surface. This is consistent with its purpose as a vulnerable testing machine.

## Comparative Analysis

Tool	Host Discovery	Port Scan	Service	Ease of Use
			Detection	
Angry IP Scanner	Yes	Basic	Limited	Easy
Metasploit	Yes	Advanced	Yes	Intermediate
MegaPing	Yes	Basic	Limited	Easy
NetScan Tools Pro	Yes	Advanced	Partial	Intermediate

## Security Implications

This exercise demonstrates that:

- Open ports represent potential attack vectors
- Legacy services (FTP, Telnet) increase risk exposure

- Network reconnaissance is the first stage of penetration testing
- Different tools provide varying levels of depth and analysis

Understanding exposed services allows defenders to:

- Disable unnecessary services
- Harden configurations
- Reduce attack surface

## Conclusion

This practical exercise successfully demonstrated:

- Host discovery techniques
- Port enumeration methodologies
- Service identification
- Tool comparison in network reconnaissance

The results highlight the importance of continuous network monitoring and service hardening to reduce vulnerabilities within a local network.