

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.

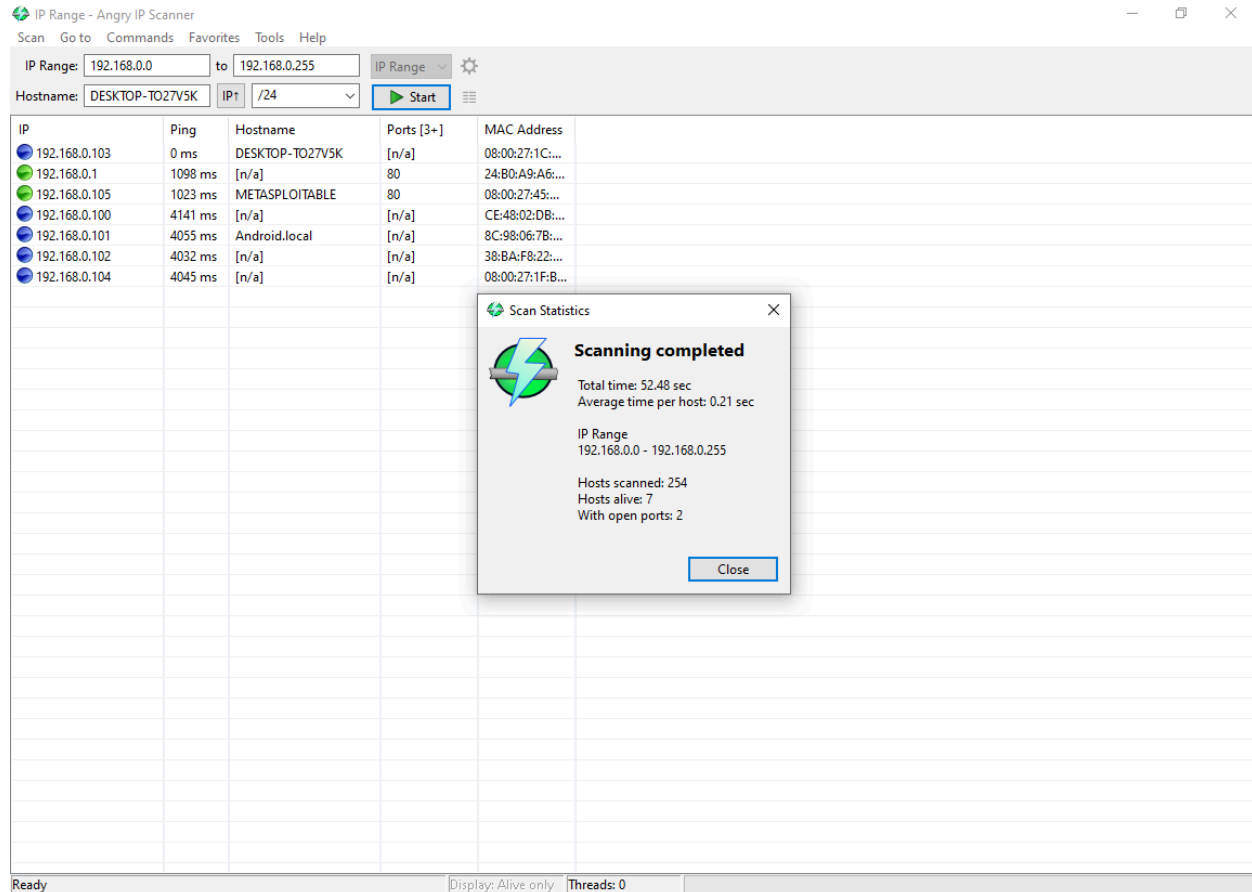
Tool 1: Angry IP Scanner

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



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.

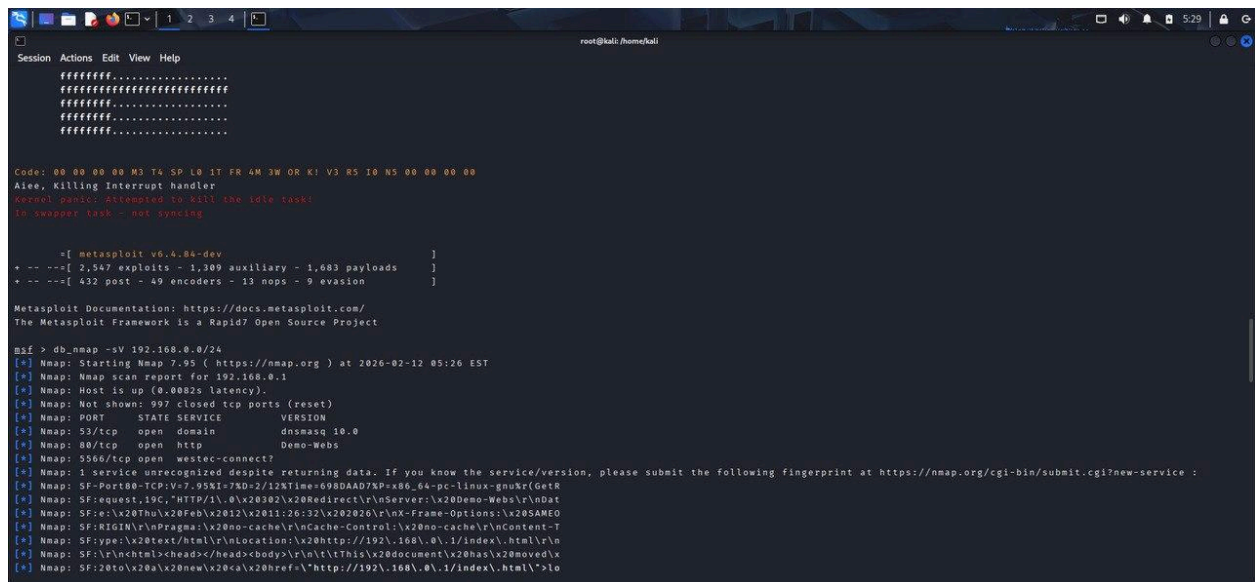
Tool 2: Metasploit Framework (msfconsole)

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



```
root@kali: /home/kali

Session Actions Edit View Help

#####
#####
#####
#####
#####

Code: 00 00 00 00 M3 T4 SP L0 IT FR 4W 3W OR K1 V3 R5 I0 N5 00 00 00 00
Aieee, Killing Interrupt Handler
Kernel panic: Attempted to kill the idle task!
In 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 192.168.0.0/24
[*] 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 (0.0082s 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  westec-connect?
[*] Nmap: 1 service unrecognized 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:V=7.95XI=7XD=2/12XTime=698DAAD7XP=x86_64-pc-linux-gnuKr(GetR
[*] Nmap: SF:request,19C,"HTTP/1.1.0"x20302x20Redirect\r\nServer:x20Demo-Webs\r\nDat
[*] Nmap: SF:e-x20Thu\x20Feb\x2012\x2012:26:21x202020\r\nx-frame-Options:x20SAMEO
[*] Nmap: SF:RIGIN\r\nPragma:x20no-cache\r\nCache-Control:x20no-cache\r\nContent-T
[*] Nmap: SF:Type:x20text/html\r\nLocation:x20http://192.168.0.1/index.html\r\n
[*] Nmap: SF:\r\nhtml<head></head><body>\r\n\t\tThis x20document x20has x20moved x
[*] Nmap: SF:20to x20a x20new x20a x20href="http://192.168.0.1/index.html">lo
```

```
root@kali: /home/kali
Session Actions Edit View Help
Hosts
-----
address      mac          name  os_name  os_flavor  os_cp  purpose  info  comments
-----
192.168.0.1   24:b0:a9:a6:46:5b   Unknown   Unknown   device
192.168.0.102 38:8A:F8:22:62:E9   Unknown   Unknown   device
192.168.0.103 08:00:27:1c:2d:f7   Linux     server
192.168.0.104 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
192.168.0.105 21    tcp    ftp           open   vsftpd 2.3.4
192.168.0.105 22    tcp    ssh           open   OpenSSH 4.7p1 Debian Subuntui 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 BIND 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 gmiiregistry
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
```

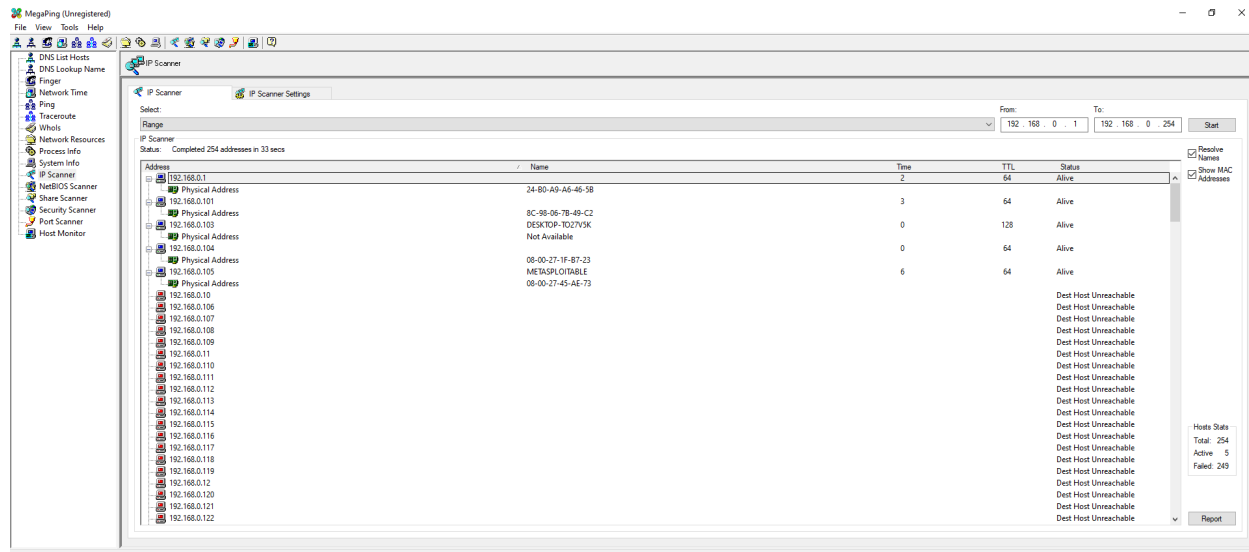
Observation

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

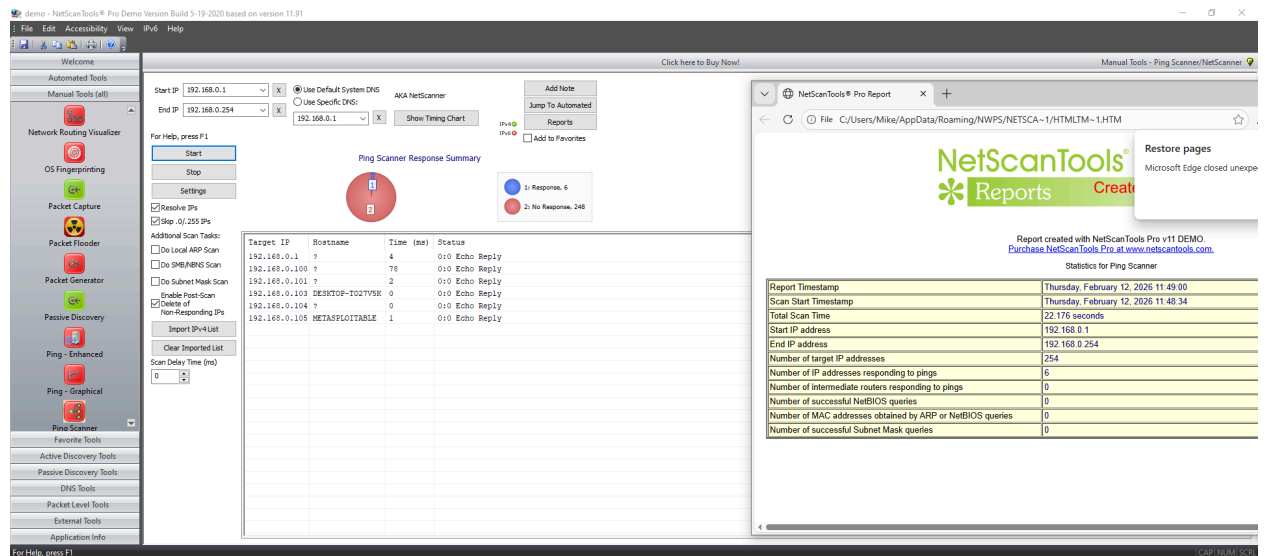
- Successfully resolved hostnames
- Retrieved physical (MAC) addresses
- Detected Metasploitable test machine

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

Tool 4: NetScan Tools Pro

A. Ping Scanner

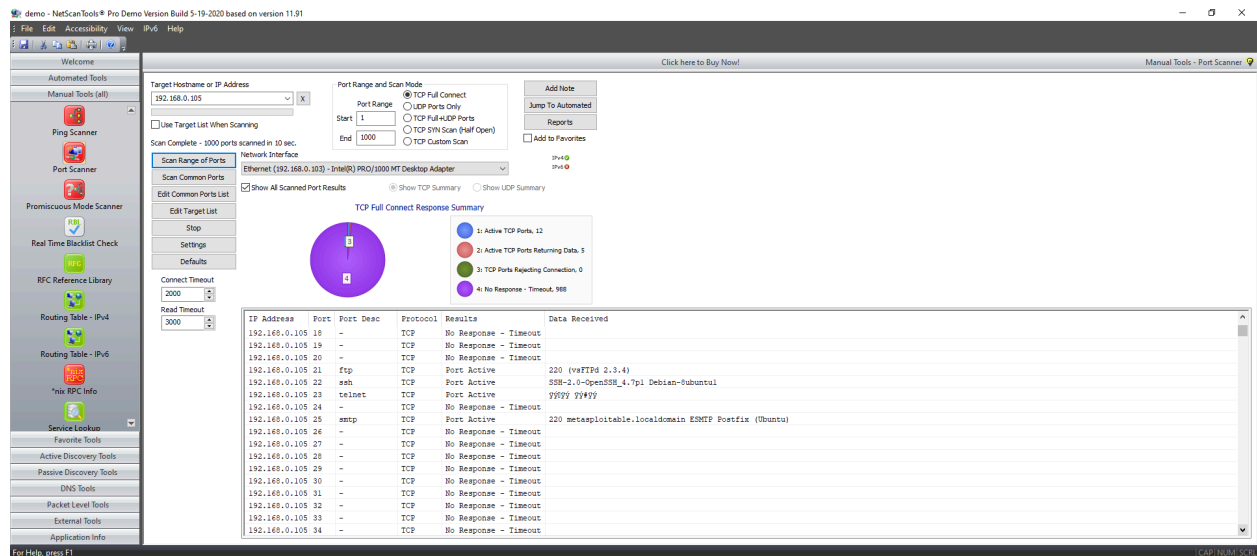
- Total IP addresses scanned: 254
- Responding hosts: 6
- Non-responding: 248
- Scan time: ~22 seconds



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 Detection	Ease of Use
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.