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.

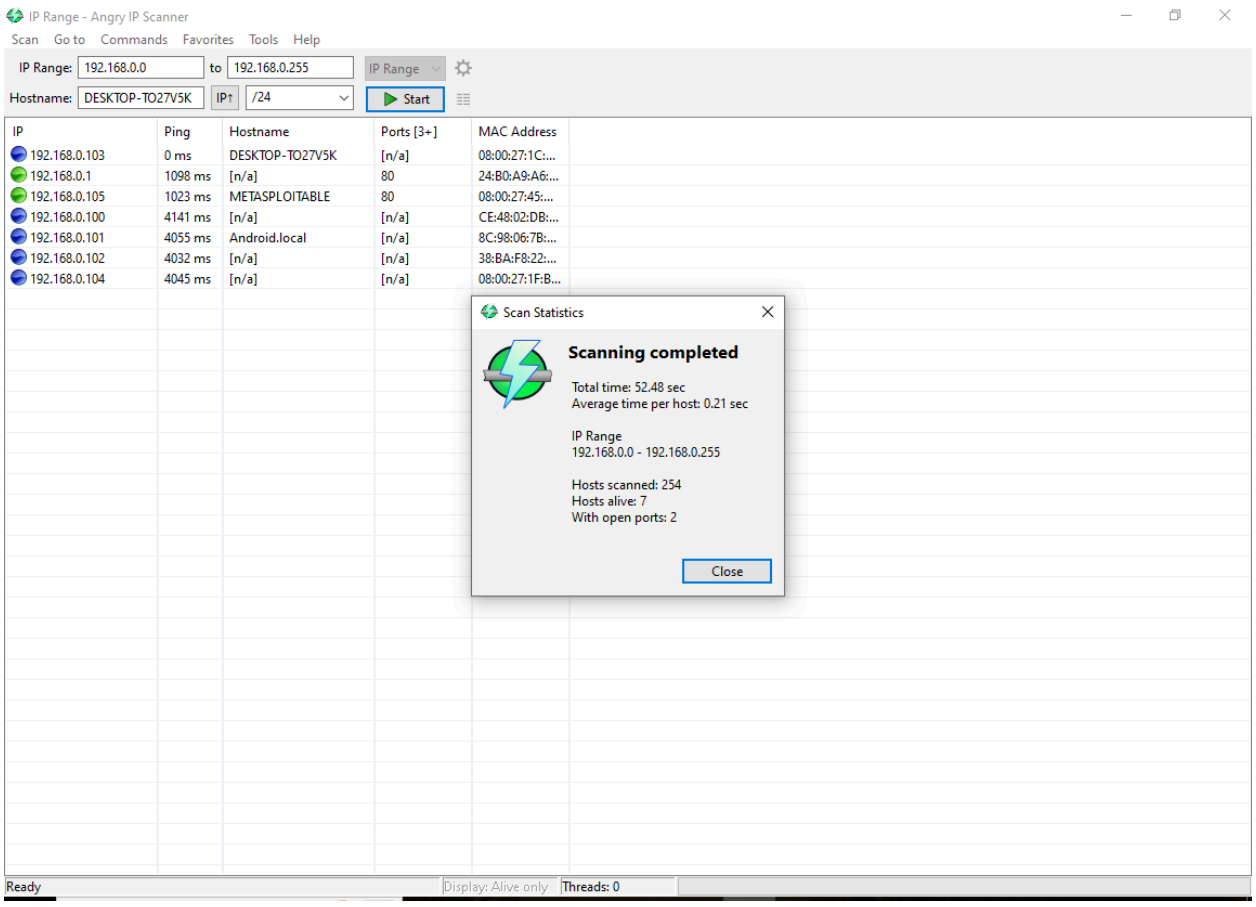
Tool 1: Angry IP Scanner

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.

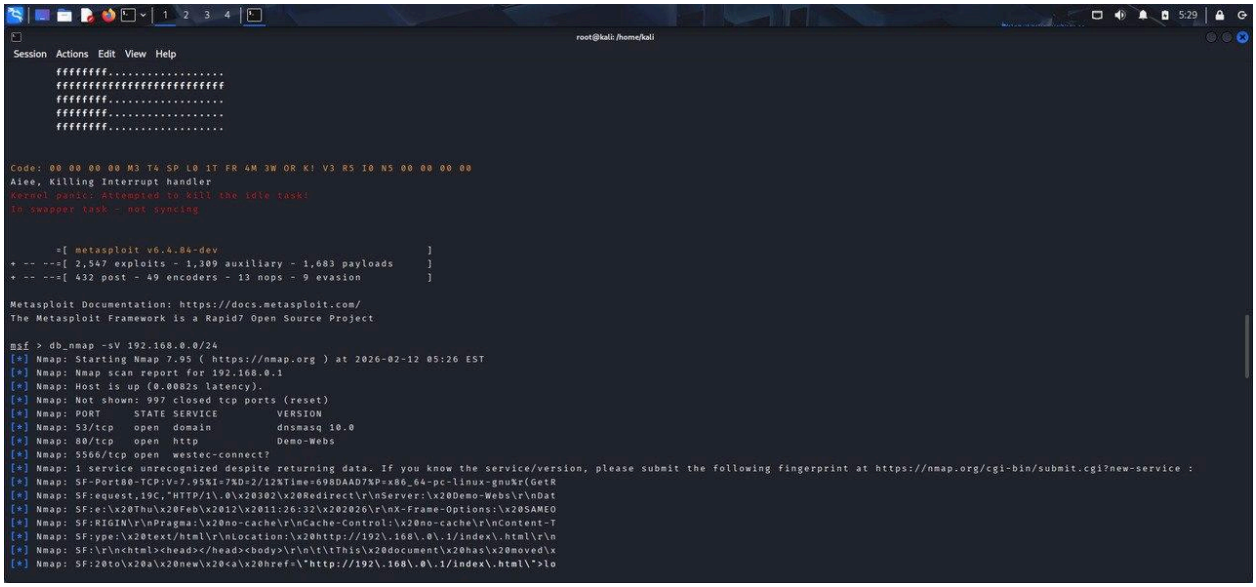
Tool 2: Metasploit Framework (msfconsole)

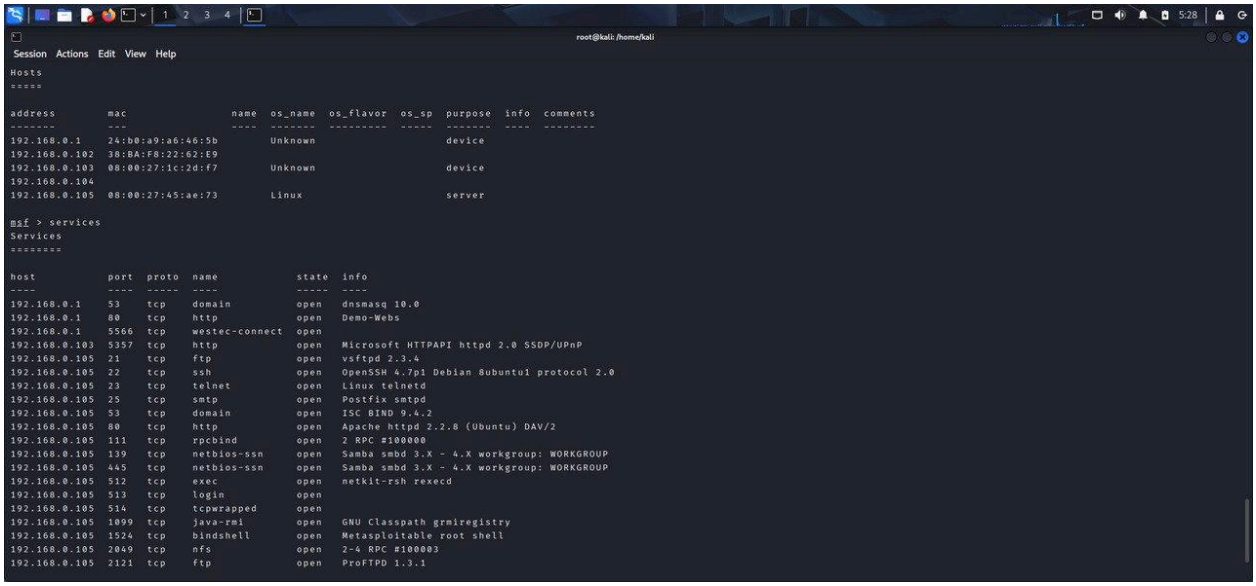
Methods Used

- 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





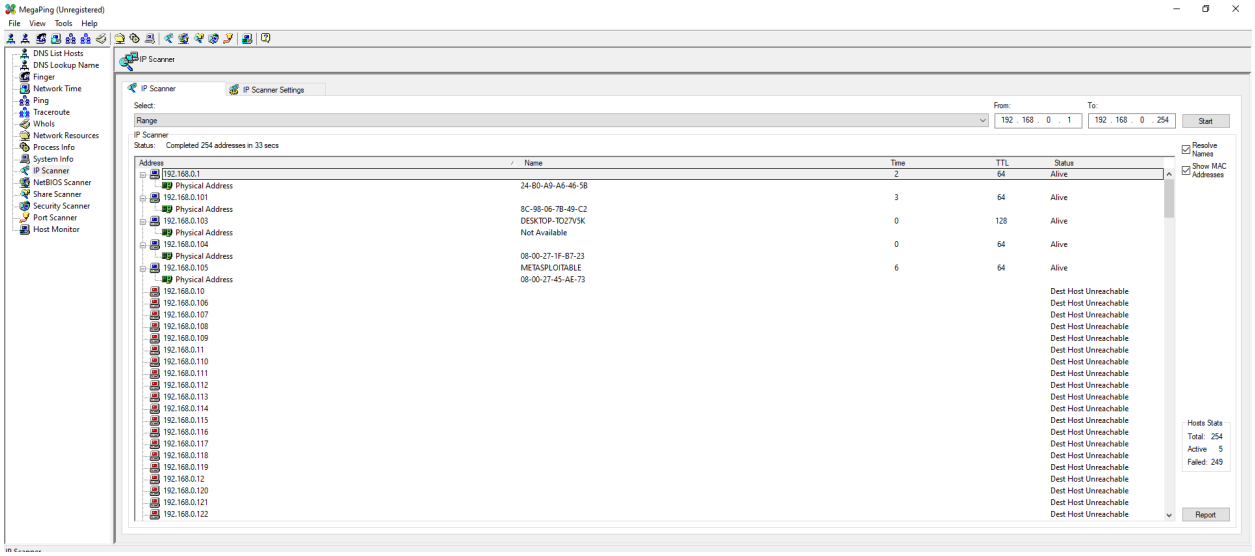
Observation

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

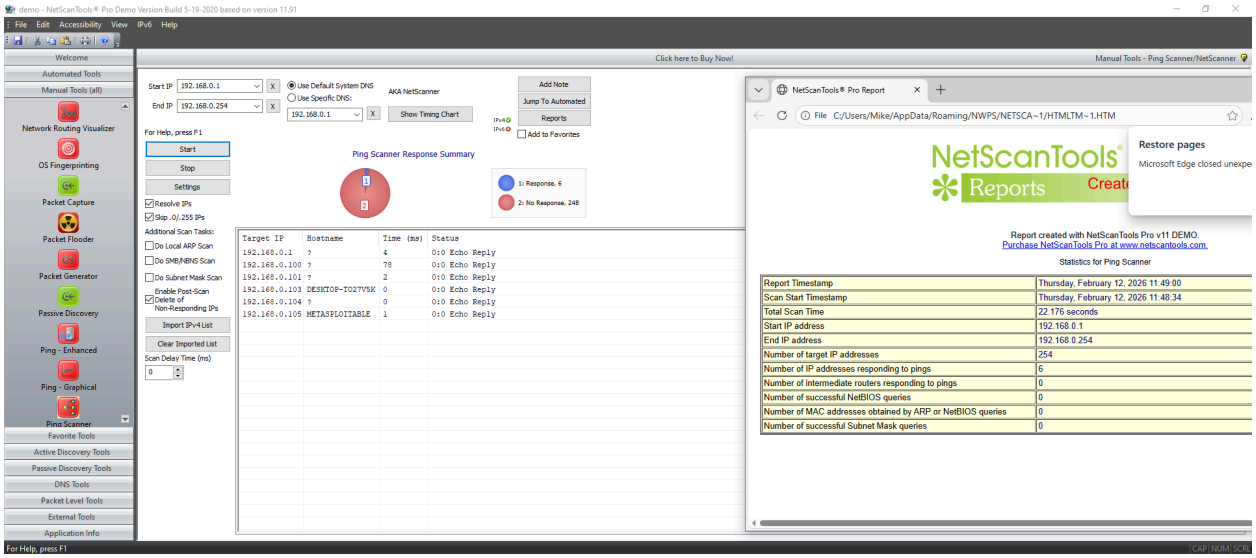
- Successfully resolved hostnames
- Retrieved physical (MAC) addresses
- Detected Metasploitable test machine

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

Tool 4: NetScan Tools Pro

A. Ping Scanner

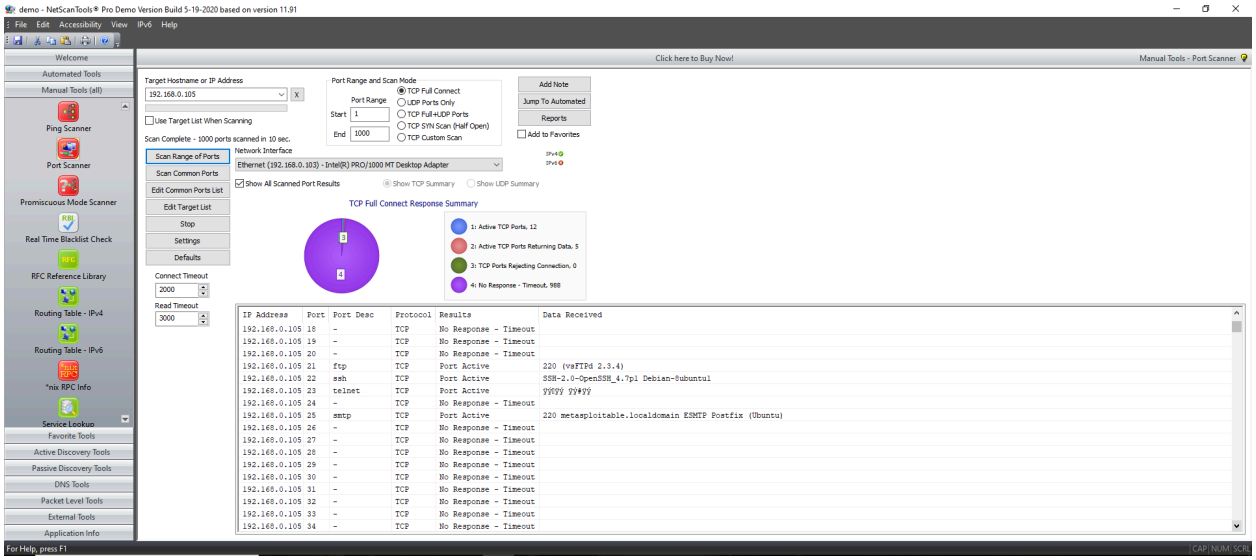
- Total IP addresses scanned: 254
- Responding hosts: 6
- Non-responding: 248
- Scan time: ~22 seconds



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.