Network Scanner Tool Using Python

A technical project focused on identifying active hosts and exposed services within network infrastructure

Core Scanning Approach & Design

Host Discovery

- ICMP echo requests for initial detection
- Primary method for identifying live systems
- Fast and efficient network sweep

TCP Fallback Detection

- Identifies systems with ICMP restrictions
- TCP response analysis for validation
- Ensures comprehensive host coverage

Service Enumeration

- Scans commonly used TCP ports
- Detects exposed network services
- Maps potential attack surface

This multi-layered approach provides foundational network reconnaissance capabilities essential for security assessments and vulnerability identification.

Key Results from Implementation & Testing

Host Detection

- Successfully identified live hosts within specified IP ranges
- Accurate differentiation between ICMP-reachable and TCP-responsive systems
- Consistent performance across various network configurations

Port Scanning

- Identified open ports on responsive hosts
- Detected commonly exposed services including HTTP, SSH, and FTP
- Generated actionable data for security analysis

Project Screenshot

```
PS F:\Projects\network-scanner-tool> python main.py 192.168.0.1 192.168.0.225
[+] Host reachable (ICMP): 192.168.0.101
[-] Host appears down: 192.168.0.3
[-] Host appears down: 192.168.0.2
[-] Host appears down: 192.168.0.6
[-] Host appears down: 192.168.0.12
[-] Host appears down: 192.168.0.8
[-] Host appears down: 192.168.0.16
[-] Host appears down: 192.168.0.11
[-] Host appears down: 192.168.0.15
[-] Host appears down: 192.168.0.10
[-] Host appears down: 192.168.0.4
[-] Host appears down: 192.168.0.9
[-] Host appears down: 192.168.0.13
[-] Host appears down: 192.168.0.7
[-] Host appears down: 192.168.0.14
[-] Host appears down: 192.168.0.19
[-] Host appears down: 192.168.0.5
[-] Host appears down: 192.168.0.1
[-] Host appears down: 192.168.0.20
[-] Host appears down: 192.168.0.18
[-] Host appears down: 192.168.0.23
[-] Host appears down: 192.168.0.31
[-] Host appears down: 192.168.0.30
[-] Host appears down: 192.168.0.21
[-] Host appears down: 192.168.0.28
[-] Host appears down: 192.168.0.17
[-] Host appears down: 192.168.0.26
[-] Host appears down: 192.168.0.35
[-] Host appears down: 192.168.0.27
```

Next Steps & Project Ownership

01

Custom Port Range Support

Extend scanner to accept user-defined port ranges for targeted service discovery

02

Export Functionality

Add result export to CSV and JSON formats for integration with reporting tools

03

Performance Optimization

Implement multi-threading for faster scanning of large network segments

---

Project Owner: Akash Motghare

Responsibilities: Complete design, implementation, testing, and documentation of network scanning tool