# Network Scan Report - Open Ports and Vulnerabilities

**Generated by ShadowStrike**

## Table of Contents

Based on the provided nmap scan results, I'll generate a detailed human-readable report including open ports and vulnerabilities:

# 1 Nmap Scan Report

## 1.1 Target Information

- Host: kali (192.168.1.67)
- Status: Up
- Latency: 0.000030s

## 1.2 Open Ports

### 1.2.1 Port 80/tcp

- Service: http
- Version: Apache httpd 2.4.62 (Debian)
- Description:
- Supported Methods: GET, POST, OPTIONS, HEAD
- Server Header: Apache/2.4.62 (Debian)
- Title: ARP Spoofing Tool

## 1.3 OS Detection

The host does not match any known operating system. However, the TCP/IP fingerprint suggests it may be running on an x86_64-pc-linux-gnu platform.

## 1.4 Uptime Estimate

Estimated uptime: 5.465 days (since Thu Dec 12 06:05:38 2024)

## 1.5 Network Distance

0 hops away

## 1.6 Vulnerabilities

Based on the limited information provided, there are no explicit vulnerabilities reported. However, some potential concerns:

1. Apache httpd 2.4.62 may have known vulnerabilities. It's recommended to check for any available security patches or upgrades.

2. The presence of an ARP Spoofing Tool suggests the server may be used for network analysis or attack simulation purposes. Ensure proper security measures are in place if this is not intended.
3. The host is running for approximately 5.465 days, which could indicate a long-running service. Consider reviewing its necessity and security implications.

## 1.7 Additional Information

- TCP Sequence Prediction Difficulty: 257 (Good luck!)
- IP ID Sequence Generation: All zeros
- Raw packets sent/received: 1110 / 2211

## 1.8 Recommendations

1. Update Apache httpd to the latest stable version to address any known vulnerabilities.
2. Implement proper authentication mechanisms for the web server.
3. Regularly monitor and update the system to prevent exploitation of known vulnerabilities.
4. If the ARP Spoofing Tool is not intentionally deployed, consider removing it to minimize potential risks.
5. Review the necessity of the long-running service and implement appropriate security measures.

This report provides a summary of the nmap scan results, highlighting open ports, potential vulnerabilities, and recommendations for improvement. For a comprehensive security assessment, further investigation and testing would be necessary.