Network Scan Report - Open Ports and Vulnerabilities

Generated by ShadowStrike

Table of Contents

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

1 Nmap Scan Report

1.1 Target Information

- Host: kali (192.168.1.67)
- Status: Up
- Latency: 0.000049s

1.2 Open Ports

1.2.1 Port 80/tcp

- Service: http
- Version: Apache httpd 2.4.62 ((Debian))
- Description:
- Supported HTTP methods: GET, POST, OPTIONS, HEAD
- Server header: Apache/2.4.62 (Debian)

1.3 Vulnerabilities

Unfortunately, the provided scan results don't contain specific vulnerability information. However, based on the detected services, we can identify potential security concerns:

1. Outdated Apache version: The Apache server is running version 2.4.62, which may have known vulnerabilities.
2. Default or weak configuration: The presence of default pages or misconfigured settings could expose sensitive information.
3. Unencrypted traffic: HTTP (port 80) is used instead of HTTPS, potentially exposing data in transit.

1.4 Additional Information

- OS Detection: No exact match found, but the system appears to be Linux-based (x86_64-pc-linux-gnu)
- Uptime: Estimated 5.462 days (since Thu Dec 12 06:05:38 2024)

1.5 Recommendations

1. Update Apache to the latest stable version to address potential security issues.
2. Implement HTTPS for secure communication.
3. Conduct a thorough web application security audit.
4. Review and harden the Apache configuration.
5. Consider using a Web Application Firewall (WAF) for additional protection.

This report provides a high-level overview of the detected services and potential security concerns based on the nmap scan results. For a comprehensive security assessment, additional tools and techniques may be necessary.