Network Scan Report - Open Ports and Vulnerabilities

Generated by ShadowStrike

Table of Contents

Here's a detailed human-readable report generated from the nmap scan results:

1 Nmap Scan Report

1.1 Host Information

- IP Address: 192.168.1.67
- Hostname: kali
- Status: Up (0.000031s latency)

1.2 Open Ports

1.2.1 Port 80/tcp

- State: Open
- Service: http
- Version: Apache httpd 2.4.62 ((Debian))
- Description: Apache HTTP Server 2.4.62
- Additional Information:
- _http-title: ARP Spoofing Tool
- _http-server-header: Apache/2.4.62 (Debian)
- Supported Methods: GET POST OPTIONS HEAD

1.3 Operating System

- OS Detection: Not shown (N)
- TCP/IP Fingerprint:
- OS: SCAN(V=7.94SVN%E=4%D=12/17%OT=80%CT=1%CU=36621%PV=Y%DS=0%DC=L%
  pc-linux-gnu)
- OS Details: x86_64-pc-linux-gnu

1.4 Network Information

- Uptime Guess: 5.446 days (since Thu Dec 12 06:05:39 2024)
- Network Distance: 0 hops
- TCP Sequence Prediction Difficulty: 257 (Good luck!)
- IP ID Sequence Generation: All zeros

1.5 Additional Notes

- No exact OS matches were found.
- The host is running Apache HTTP Server 2.4.62 on port 80.

- The web server appears to have an ARP Spoofing Tool page.

1.6 Vulnerability Information

No specific vulnerabilities were detected in this scan. However, having Apache HTTP Server 2.4.62 exposed to the internet may pose security risks. It's recommended to keep the server updated and consider implementing additional security measures.

This report provides a comprehensive overview of the scanned host, highlighting open ports, services, and potential security concerns. Further investigation may be necessary to identify any specific vulnerabilities or misconfigurations.