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 Host Information

- Target: kali (192.168.1.67)
- Status: Up (0.000039s latency)

1.2 Open Ports and Services

1.2.1 Port 80/tcp

- 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 HTTP Methods: GET, POST, OPTIONS, HEAD

1.3 Operating System Information

- OS Detection: Not shown (Nmap couldn't determine the exact OS)
- TCP/IP Fingerprint:
- OS: SCAN(V=7.94SVN%E=4%D=12/17%OT=80%CT=1%CU=33179%PV=Y%DS=0%DC=L
  pc-linux-gnu)SEQ(SP=102%GCD=1%ISR=10F%TI=Z%CI=Z%II=I%TS=AOS:)OPS(O1=MFF
- OS Guess: x86_64-pc-linux-gnu

1.4 Uptime Estimate

- Estimated uptime: 5.451 days (since Thu Dec 12 06:05:38 2024)

1.5 Network Distance

- Network Distance: 0 hops

1.6 Vulnerability Information

Based on the provided scan results, there don't appear to be any specific vulnerabilities reported. However, the presence of an open web server (Apache httpd 2.4.62) on port 80/tcp could potentially expose the system to common web application vulnerabilities if proper security measures are not in place.

1.7 Additional Notes

- The host appears to have been up for approximately 5.451 days as of the scan date.
- Nmap was unable to determine the exact operating system running on this host.
- The TCP sequence prediction difficulty is rated as 258, which is considered good protection against basic sequence guessing attacks.

This report provides a summary of the nmap scan results, including open ports, service versions, operating system information, uptime estimate, network distance, and potential vulnerability considerations based on the available data.