Nessus Scan Report

General Scan Information

Scanner Version: Nessus 10.8.3

Scanner Build: 20010

Plugin Feed Version: 202501281217

Scanner Edition: Nessus Home

Scanner OS: Windows (win-x86-64)

Scan Type: Normal

Scan Name: My Basic Network Scan

Scan Policy Used: Basic Network Scan

Scanner IP: 192.168.126.108

Port Scanner Used: nessus_syn_scanner

Port Range Scanned: Default

Ping Round Trip Time (RTT): 11.696 ms

Thorough Tests: No

Experimental Tests: No

Scan for Unpatched Vulnerabilities: No

Plugin Debugging Enabled: No

Paranoia Level: 1

Report Verbosity: 1

Safe Checks: Yes

Optimize the Test: No

Credentialed Checks: No

Patch Management Checks: None

Display Superseded Patches: Yes

CGI Scanning: Disabled

Web Application Tests: Disabled

Maximum Hosts: 30

Maximum Checks: 4

Receive Timeout: 5

Backports: None

Allow Post-Scan Editing: Yes

Nessus Plugin Signature Checking: Enabled

Audit File Signature Checking: Disabled

Scan Start Date: 2025/01/28 21:55 IST

Scan Duration: 257 seconds

Scan for Malware: No

Detected Vulnerabilities & Information

1. ICMP Timestamp Request Remote Date Disclosure

Plugin ID: 10114

CVE: CVE-1999-0524

CVSS v2.0 Base Score: 2.1 (Low)

Risk Factor: Low

Host: 192.0.0.2

Protocol: ICMP

Port: 0

Synopsis:

- The remote host responds to ICMP timestamp requests, allowing an attacker to determine the system time.
- This information could assist in attacks against authentication protocols.

Solution:

- Filter out ICMP timestamp requests.

Plugin Output:

- The difference between the local and remote clocks is 1 second.

STIG Severity: N/A

CVSS v4.0 Base Score: 2.2

Risk Factor: Low

CWE: CWE-200 (Information Exposure)

Plugin Publication Date: 1999/08/01

Plugin Modification Date: 2024/10/07

2. Traceroute Information

Plugin ID: 10287

CVE: None

Risk Factor: N/A

Host: 192.0.0.2

Protocol: UDP

Port: 0

Description:

- It was possible to obtain traceroute information.

Plugin Output:

Traceroute from 192.168.126.108 to 192.0.0.2:

Hop Count: 1

Path: 192.168.126.108 to 192.0.0.2

3. Nessus Scan Information

Plugin ID: 19506

CVE: None

Risk Factor: N/A

Host: 192.0.0.2

Protocol: TCP

Port: 0

Description:

- This plugin provides details about the scan itself, including:
  - Plugin Version & Scanner Type
  - Nessus Version Used
  - Port Scanner(s) Used
  - Port Range Scanned

- Ping Round Trip Time
- Credentialed Checks Availability
- Date & Duration of the Scan
- Number of Hosts Scanned & Checks Done

Plugin Publication Date: 2005/08/26

Plugin Modification Date: 2024/12/31

Overall Risk Summary

Low-Risk Findings: 1 (ICMP Timestamp Disclosure)

Informational Findings: 2 (Traceroute Information, Nessus Scan Information)

This scan did not detect any critical or high vulnerabilities. However, it is recommended to disable ICMP timestamp responses to prevent potential reconnaissance attacks.