

## **Local Vulnerability Scan Report**

# **Vulnerability Scan Report**

Target: 192.168.1.0/24

Scanned at (UTC): 2025-11-25T07:16:34.270910Z

Generated at (UTC): 2025-11-25T07:22:41.829113

This report summarizes discovered hosts, open ports, detected services, and rule-based vulnerability alerts. Use this report strictly for devices you own or are authorized to test.

# Local Vulnerability Scan Report

## Severity Summary

Total Alerts Found: 4

Total Risk Score: 28

## Severity Breakdown



# Local Vulnerability Scan Report

## CVE Summary

Total CVEs Found: 0

## CVE Severity Breakdown



## Top Risk CVEs

No CVE data found.

# Local Vulnerability Scan Report

**Host: 192.168.1.1 (up)**

Port	Service	Version
22	ssh	
23	telnet	
53	domain	2.84rc2
80	http	1.30 26Oct2018
443	https	

## Alerts

- Telnet detected. Unencrypted access. (Severity: CRITICAL, Score: 10)

## Recommendations

- Disable Telnet. Use SSH instead.

# Local Vulnerability Scan Report

**Host: 192.168.1.2 (up)**

Port	Service	Version
135	msrpc	
139	netbios-ssn	
445	microsoft-ds	
3306	mysql	
5432	postgresql	
16992	http	14.1.70.2228

## Alerts

- SMB may expose SMBv1 vulnerability. (Severity: HIGH, Score: 8)
- MySQL exposed to the network. (Severity: MEDIUM, Score: 5)
- PostgreSQL exposed. Use IP restrictions and strong passwords. (Severity: MEDIUM, Score: 5)

## Recommendations

- Disable SMBv1 and apply security patches.
- Restrict MySQL usage to localhost or secure the port.

# Local Vulnerability Scan Report

**Host: 192.168.1.3 (up)**

Port	Service	Version

## Alerts

No critical alerts found.

## Recommendations

- No immediate recommendations for this host.

# **Local Vulnerability Scan Report**

## **Final Notes & Ethics**

This report is generated for educational and authorized use only. Never scan networks without explicit permission. High severity items should be addressed immediately. Medium and low severity items still pose risk and should be reviewed based on your environment.