

# ■ Vulnerability Scan Report

Tool Used:	Nessus Essentials
Scan Date:	2025-08-07
Target:	192.168.0.101
Scan Type:	Basic Network Scan

## ■ Summary:

Total Vulnerabilities	14
Critical	2
High	4
Medium	5
Low	3

## ■■ Sample Issues Found:

Vulnerability	Severity	Description	Recommendation
SMBv1 Enabled	High	Outdated and insecure SMB protocol	Disable SMBv1
OpenSSH 7.4	Medium	Version with known vulnerabilities	Update OpenSSH to latest
SSL Self-Signed Cert	Low	Untrusted SSL certificate	Use valid SSL certs
Apache 2.4.29	Critical	Multiple CVEs detected	Upgrade to latest version
FTP Anonymous Access	High	FTP server allows anonymous login	Disable anonymous FTP access