Vulnerability Scan Report

Tenable Nessus Essentials

Generated for: kala08@gmail.com

Scan Date: June 26, 2025, 11:13 AM IST

Scan Duration: 21 minutes

Executive Summary

- Generating detailed analysis identifying vulnerabilities on host 192.168.230.128.
- Highlighting critical, high, medium, low, and informational issues detected.
- Providing recommendations for remediation to enhance security posture.

Chapter 1

Vulnerability Details

1.1 Scan Overview

- Policy: Advanced Scan
- Status: Completed
- Scanner: Nessus Scanner
- Start: Today at 11:13 AM
- End: Today at 11:34 AM
- Elapsed: 21 minutes

1.2 Vulnerability Breakdown

Severity	Count	CVSS	VPR	EPS
Critical	11	10.0	7.4	0.716
High	27	7.5	6.7	0.792
Medium	9	5.0	4.0	0.504
Low	4	2.5	2.0	0.251
Info	83	0.0	0.0	0.000

1.3 Detailed Vulnerabilities

Severity	Name	CVSS	VPR	EPS	Description
Critical	CVSS: 10.0 - Canonical Ubuntu Linux 18.04 (Bionic)	10.0	7.4	0.716	Multiple vulnerabilities detected
Critical	VNC Server Password	10.0	7.4	0.716	Weak password configuration
Critical	SSL Version 2 and Protocol Detection	9.8	7.0	0.692	Outdated SSL protocol
High	Apache Tomcat (Multiple Issues)	7.5	6.7	0.792	Multiple security issues

Severity	Name	CVSS	VPR	EPS	Description
High	Samba Backdoor Vulnerability	7.5	6.7	0.792	Potential backdoor detected
Medium	Unencrypted Telnet Server	5.0	4.0	0.504	Telnet without encryption
Low	TLS Diffie-Hellman Modulus $<$ 1024 Bits (Logjam)	2.5	2.0	0.251	Weak encryption modulus

Chapter 2

Recommendations

- Addressing critical vulnerabilities by updating Canonical Ubuntu Linux to the latest patch.
- Strengthening VNC Server security with strong passwords and encryption.
- Upgrading SSL protocols to modern standards (e.g., TLS 1.2 or higher).
- Applying patches for Apache Tomcat and Samba vulnerabilities.
- Disabling unencrypted Telnet and switching to SSH.
- Enhancing TLS configurations to mitigate Logjam vulnerabilities.