Basic Search Vulnerability Assessment Report

1. Introduction

This report provides an analysis of basic vulnerabilities identified on the host 10.153.242.222. The information is based on extracted scan logs. The goal is to highlight potential weaknesses and provide mitigation recommendations.

2. Summary of Key Findings

- High-risk open ports (SMB, RPC, ephemeral ports)
- SMB service exposure
- Multiple DCE-RPC services
- Unresponsive/misconfigured web services
- SSL certificate chain issues
- Insecure SNMP configuration
- Large number of listening ports

3. Detailed Vulnerability Findings

3.1 SMB Service Exposure (Ports 445 & 139)

Risk: High

SMB is exploitable for lateral movement and ransomware attacks.

Recommendation: Disable SMBv1, restrict access, enforce NTLMv2.

3.2 DCE-RPC & Ephemeral Ports Exposure

Risk: Medium

Large RPC surfaces can enable enumeration or remote execution.

Recommendation: Restrict RPC access, firewall unused ports.

3.3 Web Service Misconfigurations

Risk: Low–Medium

Unresponsive HTTP/HTTPS services may be misconfigured.

Recommendation: Disable unused services.

3.4 SSL Certificate Chain Issues

Risk: Medium

A broken CA chain may lead to MITM attacks.

Recommendation: Install full certificate chain.

3.5 SNMP Default Community String

Risk: High

SNMP with 'public' community leaks sensitive device info.

Recommendation: Disable SNMP or upgrade to SNMPv3.

3.6 Excessive Listening Ports

Risk: Medium

More open ports increase attack surface.

Recommendation: Harden system and close unused services.

4. Overall Risk Rating

- SMB Exposure: High

- RPC Surface: Medium

- SSL Issues: Medium

- SNMP Weaknesses: High

- Overall System Security: Medium–High

5. Recommendations Summary

- Harden SMB

- Reduce RPC exposure

- Fix SSL/TLS configuration

- Secure or disable SNMP

- Reduce unnecessary services

6. Conclusion

The host shows multiple vulnerabilities that should be addressed to strengthen security posture.

Applying the recommended remediations will significantly reduce potential attack vectors.