🔐 Security Scan Analysis Report

1. Introduction

This report presents the results of a security assessment performed using automated scanning tools. The objective of the scan was to identify open ports, running services, configuration issues, and potential vulnerabilities on the target system. The analysis includes findings from network scanning and vulnerability detection.

---

2. Scope of Assessment

- **Target Type:** Server / Host Machine
- **Method Used:** Network Scanning + Vulnerability Assessment
- **Tools Used:**
  - Port Scanning (e.g., Nmap)
  - Vulnerability Detection (e.g., OpenVAS/Nessus)
- **Goal:** Identify security risks and provide recommendations to improve system security.

---

3. Summary of Findings

Category	Status
Total Ports Scanned	1–65535
Open Ports Detected	✓ Identified
Vulnerabilities Found	✓ Multiple risk levels
High-Risk Issues	Present
Medium-Risk Issues	Present
Low-Risk/Informational	Present

Overall, the system contains **exposed services and misconfigurations** that may lead to unauthorized access or exploitation.

---

4. Detailed Scan Results

4.1 Open Ports & Services Identified

The scan detected the following open ports indicating active services:

- **Port xx/tcp** – Service Name (e.g., HTTP, SSH, FTP)
- **Port xx/tcp** – Service Name
- **Port xx/udp** – Service Name

These services increase the system's attack surface and should be restricted or monitored.

4.2 Vulnerability Analysis

Based on the scan, vulnerabilities were categorized into severity levels:

High Severity

- Critical service exposure
- Outdated software versions
- Weak authentication mechanisms
  Impact: High chances of unauthorized access, data leakage, or privilege escalation.

Medium Severity

- Misconfigured security policies
- Missing security patches
- Unsupported protocols
  Impact: Can be exploited with moderate effort.

Low Severity / Informational

- Banner disclosures
- Non-security-related warnings
  Impact: Low, but may help attackers during reconnaissance.

---

5. Risk Evaluation

The risk analysis shows that the system has **multiple exploitable attack points**. High severity vulnerabilities should be addressed immediately, especially those related to authentication and outdated services.

Risk scoring is based on:

- Exploitability
- Impact

- Exposure
- Business importance of the affected service

---

6. Recommendations

Immediate Actions

- Patch outdated software and services
- Disable or restrict unnecessary open ports
- Apply firewall rules to limit external access
- Enforce strong authentication (SSH keys, complex passwords)

Security Hardening

- Enable intrusion detection/prevention systems
- Regularly update OS and installed services
- Use secure protocols (HTTPS, SFTP, SSH v2)
- Disable version/banner disclosures

Long-Term Improvements

- Conduct periodic vulnerability scans
- Implement centralized logging and monitoring
- Enforce network segmentation
- Train personnel on security best practices

---

7. Conclusion

The scan highlights significant vulnerabilities that require immediate attention to avoid potential cyber threats. By implementing the recommended security measures, the organization can greatly enhance the overall security posture and reduce the risk of exploitation.