ALSHY TECH

WHERE TECHNOLOGY MEETS TRUST

NETWORK SECURITY AUDIT REPORT

📅 **Date:** 18/03/2025

📝 **Author:** Alen P Shyju

🔍 **Scope:** Internal Network Security Audit

🎯 **Objective:** Identify vulnerabilities in the network, assess risks, and provide security recommendations.

EXECUTIVE SUMMARY

The Network Security Audit Report conducted by ALSHY TECH for CyberShield Solutions highlights multiple security risks within their internal network. The audit involved port scanning, vulnerability assessment, and packet analysis to identify potential weaknesses. Key findings include open ports exposing critical services, outdated software with known vulnerabilities, weak authentication mechanisms, and unencrypted data transmission. High-risk issues such as Telnet usage (unencrypted access), outdated Apache and MySQL versions, SMBv1 enabled (vulnerable to Eternal Blue attacks), and RDP access without Multi-Factor Authentication (MFA) pose serious threats. Additionally, Wireshark analysis detected cleartext login credentials, ARP spoofing, and unusual traffic spikes, suggesting a possible rogue device. If left unaddressed, these vulnerabilities could lead to unauthorized access, data breaches, malware infections, and service disruptions. The report recommends immediate remediation measures, including disabling insecure protocols, applying security patches, enforcing strong authentication policies, encrypting communications, and implementing network monitoring tools like IDS and SIEM. ALSHY TECH advises CyberShield Solutions to take urgent action within seven days to mitigate risks and conduct a follow-up assessment to ensure compliance with security best practices. Proactively addressing these issues will significantly enhance the overall security posture of CyberShield Solutions.

1 INTRODUCTION

This report documents the findings from a network security audit conducted on a sample network environment. The assessment involved port scanning, vulnerability scanning, and packet analysis to detect potential security weaknesses.

---

2 AUDIT SCOPE & METHODOLOGY

- **Scope**
  - Target: Internal Network (e.g., 192.168.1.0/24)
  - Devices: Workstations, routers, firewalls, and servers
  - Tools Used:
    - **Nmap** (Network scanning)
    - **Wireshark** (Packet analysis)
    - **OpenVAS** (Vulnerability scanning)
    - **Metasploit** (Exploitation testing)
- **Methodology**
  1. **Reconnaissance:** Scanned network for active hosts & services.
  2. **Vulnerability Assessment:** Identified outdated software & weak configurations.
  3. **Packet Analysis:** Captured & analysed network traffic.
  4. **Report Findings:** Documented risks & provided recommendations.

---

3 FINDINGS & RISK ANALYSIS

- **3.1 Open Ports & Services**

Scan Result (Nmap Output):

sh

nmap -sS -p- 192.168.1.1-254

IP Address	Open Ports	Services Detected	Risk Level
192.168.1.10	22(SSH), 80 (HTTP), 3306 (MySQL)	Outdated Apache Server	⚠ High
192.168.1.20	445 (SMB), 3389 (RDP)	RDP enabled without MFA	⚠ High
192.168.1.30	23 (Telnet)	Insecure Protocol in Use	⚠ Critical

Risk Summary

- Telnet service found → Unencrypted communication
- SMB/RDP enabled → Potential for brute force attacks
- Apache outdated → Exploitable vulnerabilities (CVE-XXXX-XXXX)

🔹 3.2 VULNERABILITY ASSESSMENT

Scan Result (OpenVAS Report Extract):

Sh

openvas-cli --target 192.168.1.10

Vulnerability	Affected System	CVSS Score	Recommendation
SMB v1 Enabled	192.168.1.20	9.3 (Critical)	Disable SMBv1, use SMBv2+
Weak MySQL Passwords	192.168.1.10	8.5 (High)	Enforce strong authentication
Apache 2.2.15 (EOL)	192.168.1.10	7.5 (High)	Upgrade to latest version

Risk Summary:

- Outdated Apache and MySQL installations → High risk of remote code execution
- SMBv1 detected → Vulnerable to EternalBlue exploit
- Weak passwords → Susceptible to brute-force attacks

🔹 3.3 PACKET ANALYSIS & TRAFFIC INSPECTION

Analysis using Wireshark:

- Captured traffic shows unencrypted login credentials being sent over HTTP.
- ARP spoofing detected, indicating a potential MITM attack.
- Excessive broadcast traffic from IP 192.168.1.50 (possible rogue device).

Risk Summary:

- Cleartext passwords must be encrypted (HTTPS, SSH)
- Unusual traffic spikes → Possible malware or misconfigured device
- Rogue device detected → Requires network isolation

---

4 RECOMMENDATIONS & SECURITY HARDENING

✅ Network Hardening

- Close unnecessary ports (Block Telnet, SMB, and RDP externally).
- Apply firewall rules to restrict access based on IP.

✅ Update & Patch Systems

- Upgrade Apache, MySQL, and remove end-of-life software.
- Disable SMBv1 and enforce multi-factor authentication (MFA) for RDP.

✅ Improve Authentication & Encryption

- Enforce strong passwords & account lockout policies.

- Switch from HTTP to HTTPS (SSL/TLS).

✅ **Monitoring & Incident Response**

- Enable intrusion detection (Snort, Suricata).
- Configure SIEM (Splunk/ELK) for log analysis.

---

5 CONCLUSION

This audit revealed several high-risk vulnerabilities, including outdated software, weak authentication, and unencrypted communication. Immediate action is recommended to patch critical security gaps and enforce stronger access controls.

6 IMMEDIATE ACTION PLAN

To mitigate the identified vulnerabilities and strengthen network security, ALSHY TECH recommends implementing the following measures **within the next 7 days:**

✅ **Phase 1: Critical Fixes (Within 24-48 Hours)**

- Disable Telnet and enforce SSH for secure remote access.
- Upgrade Apache, MySQL, and other outdated software to the latest versions.
- Disable SMBv1 and enforce SMBv2+ to prevent exploitation (EternalBlue).
- Enforce Multi-Factor Authentication (MFA) for RDP access.
- Encrypt all sensitive communications (force HTTPS, SSH, and VPN usage).

✅ **Phase 2: Security Hardening (Within 3-5 Days)**

- Implement firewall rules to restrict external access to critical services.
- Apply strong password policies (minimum length, complexity, and expiration).
- Enable account lockout policies to prevent brute-force attacks.
- Monitor network traffic for anomalies using IDS/IPS (Snort, Suricata).

✅ **Phase 3: Ongoing Monitoring & Compliance (Within 7 Days & Beyond)**

- Deploy SIEM (Splunk/ELK) for centralized log monitoring and threat detection.

- Conduct security awareness training for employees on phishing & social engineering.
- Perform a follow-up security audit to validate implemented fixes.
- Establish an incident response plan (IRP) for future security incidents.

🔍 **Final Review & Compliance Check:**

- ALSHY TECH will conduct a re-assessment post-remediation to ensure compliance with security best practices.

Prepared By:
📝 **Alen P Shyju**
🔗 *GitHub: github.com/alenshyju*
📧 *Contact: ALSHY TECH alenshyju27@gmail.com.com*