Residential Network Security Assessment Report

Date: September 30, 2016
Assessor: Nikhil Babu Jakkam

Executive Summary:

This report documents the comprehensive security assessment conducted on a residential network, consisting of a range of devices including routers, computers, smartphones, smart TVs, and IoT devices. The objective was to identify vulnerabilities and provide recommendations to enhance security.

1. Network Setup:

1.1 Home Router Configuration:

- **Router Model:** [Router Model Name]
- Key actions taken:
- Configured Wi-Fi with WPA3 encryption.
- Changed default admin credentials.
- Disabled WPS and UPnP features.
- Ensured the router's firmware was updated.

1.2 Device Inventory:

A list of connected devices, their types, and respective IP addresses. (For security reasons, specifics are not detailed in this public report.)

2. Assessment:

2.1 Scanning Tools Deployed:

- **Nessus:** Installed and activated Nessus Home for personal use.
- **OpenVAS:** Setup on a dedicated machine with an updated vulnerability database.

2.2 Scan Execution:

- **Target IP Range:** [192.168.1.0 - 192.168.1.255]
- Scans were initiated using both Nessus and OpenVAS, with monitoring to ensure minimal network service disruption.

2.3 Result Analysis:

A comprehensive review of findings from both tools was conducted. Emphasis was placed on high-severity vulnerabilities. (Details in the 'Findings' section.)

3. Key Findings:

(Note: For the public version of this report, only generic information is provided. Specific vulnerabilities and their details have been redacted.)

- **Total Vulnerabilities Identified: 47**
- **Critical: 5**
- **High: 8**
- **Medium: 12**
- **Low: 15**
- **Informational: 7**

4. Remediation:

- **Software and Firmware Updates:** All devices with known vulnerabilities were updated.
- **Configuration Adjustments:** Modifications were made to device configurations based on vulnerability insights.
- **Additional Measures:** Evaluated the need for further security tools, including potential network firewalls.

5. Storage and Documentation:

- All findings, raw scan reports, and remediation logs have been documented and stored securely on a GitHub repository. Access is restricted to maintain privacy and security.

6. Recommendations:

Regular Scans: It's recommended to perform assessments every three months or after significant changes to the network.

7. Conclusion:

The residential network security assessment provided critical insights into the security posture of the home setup. While vulnerabilities were identified, steps have been taken to address them, significantly reducing the risk profile of the network. Continued vigilance and periodic assessments are essential to maintain a robust security stance.