Network Penetration Testing Summary

Home Automation Environment

1. Overview

This summary outlines the findings of a network penetration test performed on the home automation systems, including smart hubs, IoT devices, connected appliances, and supporting infrastructure.

2. Scope

- Smart speakers and assistants
- Wi-Fi connected lights and thermostats
- Home security cameras
- Smart door locks
- Wireless network infrastructure (Router, Access Points)

3. Methodology

- Passive and active network reconnaissance
- Vulnerability scanning of IoT endpoints
- Credential brute-force attempts (where permitted)
- Testing for default configurations and passwords
- Exploit attempts on outdated firmware

4. Key Findings

Risk Level	Finding	Recommendation
High	Default credentials found on multiple smart devices	Change all default usernames and passwords immediately
Medium	Outdated firmware on security cameras	Update firmware to the latest version
Medium	Open ports detected on home router	Disable unnecessary ports and services
Low	Non-encrypted communication detected with some devices	Enable encryption where supported

5. Recommendations

- Regularly review and update device firmware
- Change default access credentials for all devices
- Segment IoT devices on a separate network
- Review network access controls and disable unused services
- Implement strong Wi-Fi password and WPA3 encryption

6. Conclusion

The test revealed several common security issues within home automation systems. Addressing the above recommendations will greatly strengthen network security and device integrity.