Home Network Security Assessment Report
Version: 1.0
Prepared by: Barjinder Singh
Date: 05/03/2025
Confidential – Internal Use Only

---

1. Introduction

1.1 Background

This document provides an in-depth security assessment of a residential home network, reflecting an increasingly common and critical attack surface in modern digital life. With the proliferation of IoT devices, remote work setups, and smart technologies, home networks are no longer low-priority targets for adversaries. This report aims to evaluate the network's resilience, uncover misconfigurations or flaws, and provide actionable recommendations based on industry frameworks such as **NIST SP 800-53** and **OWASP**.

1.2 Constraints and Disclaimer

The scope of this assessment was constrained to in-home, non-destructive, internal scanning and configuration analysis. While every effort was made to identify relevant vulnerabilities, this report is not exhaustive nor a guarantee against all risks. Findings should be interpreted within the context of continued monitoring and a defense-in-depth security posture.

1.3 Assessment Period and Personnel

The evaluation was conducted between 05/02/2025 and 05/02/2025 by Barjinder Singh, serving as the assessor and document author.

1.4 Risk Rating Methodology

The risk rating model in this report integrates:

- **CVSS v3.1 Base Scores** for technical severity
- **Likelihood & Impact** factors for contextual prioritization
- **NIST SP 800-30 Guidelines** for risk framing and control alignment
- **OWASP Risk Rating Methodology** for qualitative reinforcement

Each finding is presented with a technical CVSS score and a mapped NIST control for remediation guidance.

---

2. Scope and Methodology

2.1 In-Scope Assets

- **Home Router:** DHCP and Gateway device for internal LAN
- **Work Laptop:** Primary user endpoint for browsing and productivity
- **Smart TV:** Consumer IoT endpoint with web and media streaming
- **Guest Wi-Fi:** Isolated network segment for external users
- **Network Printer:** Wireless peripheral with embedded web services

2.2 Methodology

A structured black-box methodology was used, emulating an external threat actor without prior internal knowledge. Techniques included:

- Passive and active network reconnaissance
- Service fingerprinting
- Configuration and vulnerability inspection
- CVE-based firmware validation

2.3 Tools and Resources

Tool	Purpose
Nmap	Network mapping, port and version scanning
Shodan	Public IP intelligence and surface validation
Wireshark	DNS and plaintext traffic capture
Router UI	Manual configuration review
CVE Lookup	Vulnerability correlation (e.g., CVE-2021-20090)

2.4 Limitations

- WAN-side vulnerabilities not deeply tested (due to legal/ethical constraints)
- Firmware inspection limited to version and CVE match (no static analysis)
- Smart devices assessed via non-intrusive enumeration only

---

3. Network Architecture Overview

Component	IP Address	Role	Comments
Router	192.168.0.1	Gateway & DHCP Server	Manages LAN routing and NAT
Work Laptop	192.168.0.101	Primary Workstation	Connected daily to internal Wi-Fi

Component	IP Address	Role	Comments
Smart TV	192.168.0.110	Streaming Device (IoT)	Accesses media services online
Guest Wi-Fi	192.168.1.0/24	Guest Network Segment	No isolation from internal network
Printer	192.168.0.120	Wireless Peripheral	Accepts unauthenticated raw jobs

---

4. Executive Summary of Findings

The following table summarizes vulnerabilities identified, classified by severity and CVSS score:

ID	Title	Severity	CVSS	Status	Executive Summary
001	Default Router Login Enabled	High	8.8	Open	Default admin credentials expose the router’s configuration interface
002	No Guest Wi-Fi Isolation	Medium	6.0	Open	Guests can reach internal IP space, creating risk of lateral movement
003	Outdated Router Firmware	High	7.5	Open	Router firmware is over 2 years outdated with active exploits (CVE-2021-20090)
004	UPnP Enabled	Medium	5.3	Open	UPnP permits automatic port forwarding which can be abused by malware
005	Weak Wi-Fi Encryption (WPA)	High	9.0	Open	WPA protocol is obsolete and vulnerable to cracking attacks
006	Open Port 9100 on Printer	Low	4.0	Accepted	Jet Direct printing port left open with no IP restriction
007	No DNS over HTTPS (DoH)	Info	N/A	Open	DNS requests are plaintext, allowing for interception and spoofing

---

5. Detailed Technical Findings

Each issue is expanded with context, technical reasoning, impact, and specific recommendations.

5.1 Default Router Login Enabled

- **Risk Score:** 8.8 (Critical)
- **Description:** The router's web interface remains protected by factory-set credentials (`admin:admin`).
- **Impact:** Enables unauthorized users to reconfigure the entire network or install backdoors.
- **Mitigation:** Change credentials immediately. Disable remote admin access.
- **Mapped Control:** NIST AC-2 (Account Management), IA-2 (Identification and Authentication)

5.2 No Guest Wi-Fi Isolation

- **Risk Score:** 6.0 (Medium)
- **Description:** The guest wireless segment allows unrestricted access to devices in the internal LAN.
- **Impact:** Any guest could scan or attempt to exploit internal systems.
- **Mitigation:** Enforce AP isolation or implement VLANs to separate traffic.
- **Mapped Control:** NIST SC-7 (Boundary Protection)

5.3 Outdated Router Firmware

- **Risk Score:** 7.5 (High)
- **Description:** Firmware last updated over 24 months ago includes exploitable vulnerability.
- **CVE Reference:** CVE-2021-20090 – Path traversal & authentication bypass
- **Impact:** Exploitable by attackers to gain admin privileges remotely.
- **Mitigation:** Update to the latest stable firmware after backing up config.
- **Mapped Control:** NIST SI-2 (Flaw Remediation), CM-2 (Baseline Configuration)

5.4 UPnP Enabled

- **Risk Score:** 5.3 (Medium)
- **Description:** UPnP allows LAN devices to request public port mapping, increasing exposure.
- **Impact:** Malware-infected devices may silently open ports for C2 communication.
- **Mitigation:** Disable UPnP unless required by a known, trusted application.
- **Mapped Control:** NIST SC-7 (Boundary Protection), AC-4 (Information Flow Enforcement)

5.5 Weak Wi-Fi Encryption (WPA)

- **Risk Score:** 9.0 (High)
- **Description:** WPA protocol used without WPA2 or WPA3 fallback. Susceptible to handshake capture and dictionary attacks.
- **Impact:** Adversaries may decrypt traffic or impersonate access points.
- **Mitigation:** Upgrade to WPA2-Personal with a long, random passphrase, or WPA3 where supported.
- **Mapped Control:** NIST SC-12 (Cryptographic Key Establishment), SC-13 (Use of Approved Algorithms)

5.6 Open Port 9100 on Printer

- **Risk Score:** 4.0 (Low)
- **Description:** Printer exposes raw printing interface across the entire LAN.
- **Impact:** May lead to printing abuse or potential DoS with malformed jobs.
- **Mitigation:** Restrict access by IP or disable the port if unused.

- **Mapped Control:** NIST AC-6 (Least Privilege), SC-7 (Boundary)

5.7 No DNS over HTTPS (DoH)

- **Risk Score:** Informational
- **Description:** DNS lookups observed in plaintext using UDP/53, subject to interception.
- **Impact:** Privacy risks and potential for DNS spoofing.
- **Mitigation:** Enforce DoH via endpoint configuration or router-based DNS settings.
- **Mapped Control:** NIST SC-12, SC-28 (Protection of Information in Transit)

---

6. Aggregate Risk Score Summary

Severity	# of Findings
High	3
Medium	2
Low	1
Info	1

---

7. Strategic Recommendations

1. **Credential Hygiene:** Replace all default credentials on network hardware.
2. **Network Segmentation:** Isolate guest networks and restrict inter-VLAN routing.
3. **Firmware & Patch Management:** Establish a monthly check-in schedule for device updates.
4. **Service Minimization:** Disable all unused services, particularly auto port-mapping (UPnP).
5. **Cryptographic Hardening:** Enforce WPA2/WPA3; rotate keys annually.
6. **Privacy Enforcement:** Enable encrypted DNS resolvers across all client devices.
7. **Monitoring & Logging:** Deploy internal DNS logging (e.g., Pi-hole) to gain visibility into queries.

---

8. Conclusion

The evaluated home network displayed a combination of legacy configurations and security oversights typically in unmanaged residential setups. While no critical zero-day vulnerabilities were detected, the presence of outdated firmware, weak encryption, and misconfigured network segmentation significantly increased the risk exposure. Implementation of the above

recommendations will transition the environment into a more secure and resilient posture aligned with modern threat models.

Appendix A – Technical Tools & References

- **Nmap** – Network scanning and banner grabbing
- **Shodan** – Internet-wide exposure discovery
- **Wireshark** – Protocol-level traffic dissection
- **Router GUI** – Manual configuration validation
- **CVE Details / NIST NVD** – Firmware vulnerability correlation

---

Prepared by: Barjinder Singh
Date: 05/03/2025
Contact: barjindersingh1104@gmail.com
End of Report