Penetration Test Report

Small Business WiFi Network

ASSESSMENT TYPE	DATE	TESTER	CLIENT	CLASSIFICATION
Internal Network Pentest	March 2026	Matthew Nebiyou	[Redacted]	Public (redacted)

Note: *This is a redacted version of the full report. Business name, location, specific IP addresses, device model numbers, SSID names and credentials have been removed. This test was conducted with the full knowledge and explicit consent of the business owners.*

1. Executive Summary

A penetration test was conducted against a small cafe's WiFi network infrastructure at the request of the business owners. The engagement was fully authorized and performed on-site.

The assessment identified a **critical vulnerability**: the security camera system was accessible from the customer-facing WiFi network and had not had its factory-default credentials changed. Any guest connected to the WiFi network could have accessed live and recorded footage from all on-site cameras using just a web browser.

Two additional findings were identified relating to flat network architecture and default credentials on network management equipment. Following the engagement, a comprehensive network redesign was carried out — a custom router/firewall appliance was built and deployed and the network was segmented into isolated VLANs. All findings were fully remediated.

SEVERITY	COUNT	STATUS
Critical	1	**Resolved**
High	0	—
Medium	1	**Resolved**
Low	1	**Resolved**

2. Scope & Methodology

In Scope

– Customer-facing and staff WiFi network
– IP security camera system
– Router and switching infrastructure
– Network-attached devices visible from guest or staff networks

Out of Scope

– Point-of-sale (POS) systems
– Third-party cloud services
– Physical intrusion testing

Methodology

Testing followed a **grey-box** approach — no prior knowledge of internal network topology, IP ranges, or device configurations. A responsible disclosure model was used: the critical finding was reported to the owners immediately upon discovery, before the report was finalised.

Tools used: Nmap, Nikto, Gobuster, arp-scan, web browser / curl, OPNsense built-in diagnostics.

3. Findings

Finding 1 — Security Cameras Accessible from Guest Network — CRITICAL · RESOLVED

Description	The security camera system's web administration interface was reachable from the customer WiFi network on its default port. The cameras retained factory-default credentials (publicly documented by the manufacturer), allowing any cafe customer to log in, view all live feeds, modify camera settings, and download recordings.
Impact	Any customer on the WiFi could access live and recorded footage without authorisation, with no specialist knowledge required. This is a significant privacy risk to staff and customers, and could facilitate physical security incidents.
Remediation	The camera system was moved to a dedicated IoT VLAN with no inbound access from guest or staff networks. Firewall rules block all traffic from the IoT VLAN to other segments. Default credentials were changed on all camera units. Remote access is now only possible via authenticated VPN.

Finding 2 — No Network Segmentation — MEDIUM · RESOLVED

Description	All devices — customer laptops, staff computers, IoT devices, and security cameras — shared a single flat network with no segmentation. Devices on the guest WiFi could reach any other device on the network without restriction.
Impact	Lateral movement between any device on the network was unrestricted. A bad actor could have attempted to access staff systems, network equipment management interfaces, or other internal resources.
Remediation	Network redesigned with three isolated VLANs (Guest, Staff, IoT) with strict inter-VLAN firewall rules. Client isolation enabled on the guest WiFi so customers cannot communicate with each other.

Finding 3 — Consumer Router with Default Management Password — LOW · RESOLVED

Description	The previous router's web management interface was accessible from the LAN, and the admin password had not been changed from the ISP default — visible on the label of the router.
Impact	Simply being on the network allowed visibility of the router via Nmap scan. Brief physical access or line-of-sight to the label would have been sufficient to access the router admin panel and modify network settings, DNS configuration, or port forwarding rules.
Remediation	Router replaced with a custom OPNsense appliance. Management interface restricted to the staff VLAN only, HTTPS enforced, and a strong unique password set.

4. Remediation & Network Redesign

The all-in-one TP-Link mesh system was decommissioned and replaced with a custom-built appliance, managed switch, and wireless access points. The router/firewall is a repurposed Dell Optiplex desktop running **OPNsense** — an open-source enterprise-grade firewall and routing platform.

VLAN	DEVICES	POLICY
Guest	Customer laptops & phones	Internet only · No access to Staff or IoT · Client isolation on
Staff	Staff computers, POS system	Internet access · No inbound from Guest or IoT
IoT	IP cameras, smart devices	No internet · Isolated from all segments · All inbound blocked

Additional Hardening

– Default credentials changed on all networked devices
– OPNsense management HTTPS-only, restricted to staff VLAN
– Strong WPA3/WPA2 passwords on all SSIDs
– Guest WiFi client isolation enabled
– Automatic firmware update notifications enabled
– Firewall logging enabled for inter-VLAN rule matches

5. Conclusion

The penetration test identified significant weaknesses in the original network configuration, with the most serious being the exposure of the security camera system to guest WiFi devices. All findings were remediated on the day of the engagement.

The new OPNsense-based architecture with VLAN segmentation is well-suited to the environment and substantially reduces the attack surface. Future recommendations include annual password rotation, prompt firmware updates, and a follow-up assessment in 12–18 months.

All testing was conducted with the express written consent of the business owners. This redacted report has been published for educational and portfolio purposes only.