SECURITY AUDIT

SECURITY AUDIT REPORT

Network & Infrastructure Assessment

Client:	Hospitality Client (Confidential)
Location:	Morocco
Date:	February 22, 2026
Auditor:	Independent Security Consultant
Classification:	PORTFOLIO VERSION - Redacted
Report Version:	1.0

PORTFOLIO VERSION: All identifying information redacted. This document demonstrates methodology and reporting capabilities. information about the security posture of the assessed network. Distribution is restricted to authorized personnel only.

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY

A comprehensive network security audit was conducted on the hostel's IT infrastructure on February 22, 2026. The assessment revealed multiple critical vulnerabilities that pose immediate risks to guest privacy, data security, and overall network integrity.

The most concerning findings include default credentials on critical infrastructure devices (router, security cameras, and WiFi extenders), complete lack of network segmentation between guests and administrative systems, and severely outdated firmware across all network devices.

Any guest connected to the hostel WiFi can currently access and control the security camera system, modify router settings, and intercept network traffic from other guests. These vulnerabilities require immediate remediation.

OVERALL RISK LEVEL	CRITICAL

2. SCOPE & METHODOLOGY

2.1 Scope

The audit covered the entire internal network of the hostel including the main router, WiFi access points, security camera system (DVR), and all connected devices. The assessment was performed as a black-box penetration test with no prior credentials or network information provided.

2.2 Methodology

The assessment followed the NIST Cybersecurity Framework and OWASP methodology. The process included: network discovery and enumeration, service and version detection, default credential testing, firmware version analysis, and network architecture review.

2.3 Authorization

Written authorization was obtained from the hostel owner prior to the assessment. All testing was performed within the agreed scope and timeframe.

3. RISK SUMMARY

Severity	Count	Description
CRITICAL	3	Default credentials on router, cameras, and WiFi extenders
HIGH	4	Outdated firmware, UPnP enabled, no network segmentation, exposed SSH
MEDIUM	2	Unmonitored network, unknown devices
LOW	1	Information disclosure in service banners

Total Findings: 10	Devices Scanned: 23	Open Ports Found: 9

4. CRITICAL FINDINGS

FINDING C-01: Router Default Credentials	CRITICAL
Device:	Consumer-grade WiFi Router
IP Address:	[REDACTED]
Ports Open:	22 (SSH), 53 (DNS), 80 (HTTP), 1900 (UPnP)
Credentials:	Factory default credentials (not changed)
Impact:	Full control of network infrastructure. An attacker can modify DNS settings to redirect all guest traffic, di
Evidence:	Successfully logged into router admin panel using manufacturer default credentials without any restricti

FINDING C-02: Security Camera System Default Credentials	CRITICAL
Device:	8-Channel DVR Security Camera System
IP Address:	[REDACTED]
Ports Open:	80 (HTTP), 554 (RTSP)
Credentials:	Common default credentials (not changed)
Firmware:	Version dated 2021 - nearly 5 years without updates
Serial Number:	[REDACTED]
Impact:	Any guest on the WiFi can view all 8 live camera feeds, access recorded footage, disable cameras, mo
Evidence:	Successfully authenticated to DVR web interface using common default credentials. Accessed live feed

FINDING C-03: WiFi Extenders - No Authentication	CRITICAL

Devices:	WiFi Range Extenders (3 units)
IP Addresses:	[REDACTED]
Web Server:	Embedded web server with known vulnerabilities
Credentials:	NO PASSWORD REQUIRED
Firmware:	Outdated - manufacturer update available
Impact:	Any guest can access the admin panel without any authentication, view and change WiFi passwords, m
Evidence:	Accessed WiFi extender admin panel without any login prompt. Full administrative access was immedia

5. HIGH SEVERITY FINDINGS

ID	Finding	Details
H-01	No Network Segmentation	Guests share the same network as cameras, router, and admin panels. A dedicated gu
H-02	Router SSH - Outdated Version	SSH service running version from 2014 with multiple known CVEs. This service should
H-03	UPnP Enabled (Port 1900)	Universal Plug and Play allows any device to automatically open ports on the router. Th
H-04	DVR Firmware Outdated	Firmware dated July 2, 2021 (nearly 5 years old). The system itself indicates a newer v

6. MEDIUM SEVERITY FINDINGS

ID	Finding	Details
M-01	Unmonitored Network	23 devices detected on network with no monitoring or alerting system in place. New dev
M-02	Unknown MAC Addresses	Multiple devices with randomized/unknown MAC addresses detected. While common fo

7. NETWORK INVENTORY

The following devices were identified during the network scan. A total of 23 active hosts were discovered.

Category	Device	IP (redacted)	Ports	Status
Router	Consumer Router	[REDACTED]	22,53,80,1900	VULNERABLE
DVR	8-Ch Camera System	[REDACTED]	80,554	VULNERABLE
WiFi AP	Extender #1	[REDACTED]	80,9000	VULNERABLE
WiFi AP	Extender #2	[REDACTED]	80	VULNERABLE
WiFi AP	Extender #3	[REDACTED]	filtered	UNKNOWN
Guest	Mobile Device	[REDACTED]	-	Guest
Guest	Mobile Device	[REDACTED]	-	Guest
Guest	13 Unknown	various	-	Guest
Auditor	Audit Equipment	[REDACTED]	-	Authorized
Auditor	Audit Equipment	[REDACTED]	-	Authorized

8. RECOMMENDATIONS

8.1 Immediate Actions (Within 24 Hours)

Priority	Action	Finding
1	Change router admin password to a strong, unique password (min. 16 characters)	C-01
2	Change Dahua DVR password to a strong, unique password	C-02
3	Set strong passwords on all Tenda WiFi extender admin panels	C-03
4	Enable Guest Network isolation on the router to separate guest WiFi from infrastructure	H-01

8.2 Short-Term Actions (Within 1 Week)

Priority	Action	Finding
5	Update Dahua DVR firmware to the latest version available	H-04
6	Update all Tenda WiFi extender firmware	H-04
7	Disable UPnP on the router	H-03
8	Disable or update SSH on the router (OpenSSH 6.6.0 is from 2014)	H-02

8.3 Long-Term Actions (Within 1 Month)

Priority	Action	Finding
9	Implement network monitoring solution to detect unauthorized devices	M-01
10	Restrict admin panel access to specific MAC addresses or a management VLAN	C-01,02,03
11	Establish a regular security review schedule (quarterly recommended)	All
12	Consider replacing the TP-Link router with a business-grade router with VLAN support	H-01

9. CONCLUSION

The security posture of the hostel's network infrastructure is currently at a critical risk level. The three most severe findings - default credentials on the router, security cameras, and WiFi extenders - mean that any guest connected to the WiFi has potential access to the entire network infrastructure, including live camera feeds of all 8 security cameras.

The lack of network segmentation compounds these issues, as there is no separation between guest devices and critical infrastructure. This is particularly concerning for a hospitality business where unknown individuals regularly connect to the network.

The positive news is that all critical and high severity findings can be remediated quickly and at minimal cost. Changing default passwords and enabling guest network isolation on the router can be completed within hours and will dramatically improve the security posture.

A follow-up assessment is recommended after remediation to verify that all vulnerabilities have been properly addressed.

10. TOOLS USED

Tool	Version	Purpose
Nmap	7.95	Network discovery and port scanning
Custom IR Toolkit	1.0	Automated security assessment and reporting
Custom Web Scanner	1.0	Security header analysis and directory enumeration
Custom Network Monitor	1.0	Real-time network device monitoring
Firefox DevTools	-	Web interface analysis
Kali Linux	2024.4	Security testing platform