*“Student complex”*

**Security Report**



**Date:** 13-01-2025

**Group:** Aminatou

**Version:** Version 1

**Project plan:** “Student complex”

Table of content

[Requirements 3](#_Toc184301126)

[What should the system be able to do? 3](#_Toc184301127)

[- Functional Requirements 3](#_Toc184301128)

[- Non-Functional Requirements 3](#_Toc184301129)

[- Prioritization 3](#_Toc184301130)

[System setup 3](#_Toc184301131)

[Architecture Description 3](#_Toc184301132)

[Network Configuration 3](#_Toc184301133)

[Network diagram 4](#_Toc184301134)

[Description of the services 4](#_Toc184301135)

[GUI Design 5](#_Toc184301136)

[Website Wireframe 5](#_Toc184301137)

[References 7](#_Toc184301138)

# Introduction

The Student Complex Infrastructure project aims to design and implement a secure network environment for a newly constructed student housing complex comprising 10 apartments, each housing at least 3 ICT students. As part of this initiative, our group has been tasked with conducting a comprehensive security assessment of the implemented infrastructure.The scope of this security report encompasses:

* Individual LANs for each apartment, connected via routers
* Representative webservers hosting tenant information and available services
* Advertisement blockers implemented in each apartment
* Inter-apartment connectivity for website access
* Shared internet connection for the entire complex
* Real-time electricity consumption monitoring systems

Our primary objectives for this security assessment are to:

1. Identify potential vulnerabilities within the network architecture
2. Evaluate the effectiveness of current security measures
3. Assess risks associated with the identified vulnerabilities
4. Provide actionable recommendations to enhance the overall security posture

This report will detail our findings from rigorous testing using industry-standard tools such as Suricata, Security Onion, and Snort. We will present a thorough analysis of the network's current state, highlighting any security gaps and proposing mitigation strategies to ensure a robust and secure environment for the student residents.

# Network Architecture

Description of the network setup

* + Each apartment has a router connected to a centrally managed switch that utilizes LANs to isolate each apartment's network. The main router provides internet access to all flats through this switch, allowing residents to connect to their apartment's network via Ethernet or Wi-Fi. This setup ensures privacy and security while sharing a single internet connection, combining convenience with robust network isolation. Our apartment hosts a simple website on a representative web server. This website contains tenant information and details about all available services in their network. The apartment has implemented an advertisement blocker, allowing students to browse without advertisements. To increase awareness of energy consumption, our apartment monitors electricity consumption in real time. This is implemented as an IoT service for tracking and displaying energy usage data. We also have implemented Philips Hue light bulbs that the tenant can control remotely.

## Diagram illustrating the network topology

## Devices included in the network

* Wireless Router
* Ethernet cable
* Arduino Device
* Philips Hue light bulbs
* Raspberry Pie 4
* Pi-hole
* Web server

# Testing Methodology

## Overview of tools used (Suricata, Security Onion, Snort)

## Description of testing procedures:

### Vulnerability scanning

### Network traffic analysis

### Penetration testing

# Findings and Vulnerabilities

## Detailed list of vulnerabilities discovered

## Categorization of vulnerabilities by severity

## Potential impact on the network and website

# Risk Assessment

## Evaluation of identified risks

## Likelihood and impact analysis

## Prioritization of risks based on potential consequences

# Recommendations

## Specific actions to address each vulnerability

## Prioritized list of security improvements

## Suggested timeline for implementing changes

# Conclusion

## Summary of key findings

## Overall assessment of the network's security posture

## Importance of ongoing security monitoring and updates