

1

Introduction

Cyber security stands as a cornerstone to the stability and safety of technology. In the coming years, growth surrounding the use and transaction of individual data is set to become rampant, with more extensive data collection approaches stemming from the introduction of new online applications and technologies [1]. Ensuring the secure collection and storage of this data is vital, with guidance materials such as the DPA 2018 and GDPR 2016 enforcing strict measures protecting the handling of individual data.

This project aimed to highlight the shortcomings of many network infrastructures, showcasing the weaknesses and vulnerabilities of systems across the digital world. The inclusion of a real-time network infrastructure will provide a genuine insight into how vulnerability assessments function, and their effect on an active infrastructure, something that is lacking within the field of study.

2

Aim

The aim of this project was to investigate and analyse a real-time network within an organisation, assessing its vulnerabilities and proposing mitigation strategies.

3

Objectives

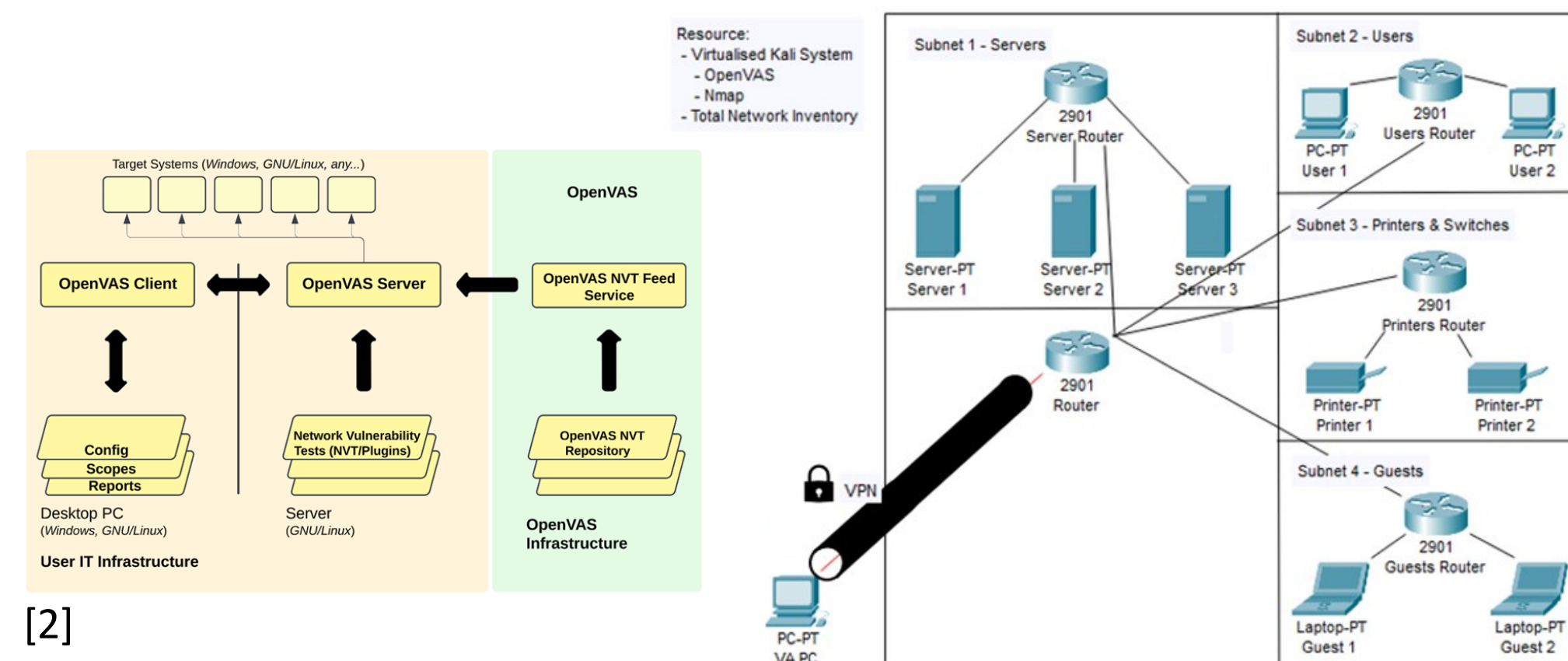
- Review current work done on an existing real-time network to identify the importance of vulnerability assessment on securing a network infrastructure.
- Explore existing literatures to identify the effectiveness, cost, accuracy, user-friendly interface, and detailed reports of various vulnerability assessment tools.
- Choose an appropriate research method for investigating and analysing the real-time network's security posture.
- Plan a vulnerability assessment using appropriate tools on the real-time network.
- Analyse and compare the outcomes gathered from vulnerability assessments in the real-time network with the existing assessments.
- Design and implement high threat vulnerabilities to demonstrate their impact within a simulated environment.
- Propose appropriate mitigation measures to aid in the remediation of the NGO network based on the vulnerability assessment conducted.

4

Methodology & Design

Subject to approval by the NGO involved, the external vulnerability assessment was conducted using a secure VPN connection provided by the network. The encrypted tunnel enabled a thorough assessment of the target network and its infrastructure without hindering the research project.

The data collected was crucial for analysing the effectiveness of infrastructure security enhancements and for advancing the understanding of vulnerability assessments in securing a network.



5

Findings

