2020

LAN security vulnerability analysis framework: case of National Irrigation Board

Wambugu, N. Muthoni
Faculty of Informatiopn Technology
Strathmore University

LAN Security Vulnerability Analysis Framework: Case of National Irrigation Board

WAMBUGU, NANCY MUTHONI

Submitted in partial fulfilment of the requirements for the Degree of Master of Science in Information Systems Security at Strathmore University

Faculty of Information Technology
Strathmore University
Nairobi, Kenya

June 2019

Declaration

I declare that this work has not been hitherto submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, this dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Wambugu, Nancy Muthoni

……

28th May 2019

Approval

The dissertation of Wambugu, Nancy Muthoni was reviewed and approved by the following:

Dr. Vincent Oteke Omwenga,
Senior Lecturer, Faculty of Information Technology,
Strathmore University.

Dr. Joseph Orero,
Dean, Faculty of Information Technology,
Strathmore University.

Prof. Ruth Kiraka,
Dean, School of Graduate Studies,
Strathmore University.

Abstract

In today's environment, many organisation like National Irrigation Board, have adopted open policies on the utilization of LAN where users may plug in unknown devices. Without the right network frameworks, it is difficult to manage network devices that are connected to the Local Area Network in an ad hoc manner. These LAN devices may have vulnerabilities that can expose entire network to security threats.

The study used case study research design and applied existing network exploration frameworks and security policies to collect data for analysis. Network exploration was carried out on the devices connected to the LAN of National Irrigation Board. Research findings showed the need for implementing a framework that checks the security vulnerability of devices connected to the LAN of National Irrigation Board. The framework was developed to allow a Network Administrator identify devices that are plugged into the LAN, analyse vulnerabilities and take remedial action based on the analysis outcome. This ensured that the devices connected to the LAN do not pose a security threat to the entire network.

The framework used policy-based network security metrics that were generated from an Institution's ICT Security Policy. Using the regression method, the metrics were quantified, weighted and applied on each computer on the LAN to generate the Security Score Index. Based on the outcome of the analysis, a decision was made on whether to allow or disconnect the LAN device from the network.

Keywords: LAN, Network, Vulnerabilities, Analysis, Security metrics

TABLE OF CONTENTS

List of Figures

List of Tables

List of Equation

List of Abbreviation / Acronyms

LAN	–	Local Area Network
NIB	–	National Irrigation Board
VPN	–	Virtual Private Network
ICT	–	Information and Communication Technology
GQM	–	Goal Question Method
CVSS	–	Common Vulnerability Scoring System

Acknowledgement

I would like to express my deepest appreciation to my supervisor, Dr Vincent Omwenga for his guidance and persistent help. I would also like to thank Strathmore University and @ilabAfrica for giving me the opportunity to partake my master's degree in their program. Thirdly, I express my special thanks to the management of National Irrigation Board for giving me the opportunity and financial support to purse my master's degree. Finally, special thanks to my mum (Mary Wambugu) and my sister (Beatrice Wangechi) my friends (Shadrack Wanyonyi and Edward Omwoyo) for their immense support and encouragement.

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

Network security means protecting information that is stored on or transmitted over a network against either unintentional or intentional unauthorized disclosure or alteration. The main goals of network security are to protect digital information assets by providing confidentiality, integrity and availability. Network security discussion now dominates in computer network related subjects (Akin, 2002). On a global perspective, a secure network should have integrity to ensure that any digital information kept therein is accurate and guarded from any accidental corruption as well as modifications. Subsequently, to ensure that digital information assets is accessible to users for whom the viewing is intended, confidentiality must be ensured. Finally, a secure network must ensure availability of digital information assets to authorised users when required without exclusion.

Security of a network also comprises of policies that are adopted by an organisation towards prevention of illegal access or alteration of computer systems (Pawar & Anuradha, 2015). Internet and other new technologies have made the world become more and more interconnected. This has resulted to an increase of computers and other related devices in the networking infrastructure. With the sprouts of interconnected computers, Local Area Networks, Wide Area Networks and devices connected to them are more open to network security vulnerabilities.

Recent incidents of network security attacks proves that security lapses in a network can lead to huge loss in terms of money, data confidentiality and reputation , to both public and private institutions ("US-CERT," 2018). These network securities comes from various entry points to the network, such remote access servers, removable medias, Internet gateways, Virtual Private Network (VPN), Email, Local Area Networks (LANs) devices, Mobile devices and internal employees.

Threats to LAN devices come in different forms. The most common one is a virus, a malware spread through a removable device used to transfer data from one computer to another. The main effect of a virus attack can be erratic operation of a computer, possible data loss, and the ability to spread to other networked users in an organization. Network based ransomware is another LAN device security threat. Ransomware is a self-propagating attack designed to destroy data and systems in LAN devices (Barens, 2018). To spread across the network, ransomware needs active and unpatched workstations. Security vulnerabilities in computers and other LAN devices can also lead to Distributed Denial of Service (DDoS) attacks. DDoS attack occurs when a malicious user sabotage a system by increasing volume of network traffic. This is achieved by use of zombie computers and can result to system or server shutdown (Barens, 2018).

Unknown LAN devices pose a great risk in the network. For instance, National Irrigation Board, a public entity in Kenya under the Ministry of Fisheries, Agriculture and Irrigation, does not have an inventory of all the ICT Assets connected into the LAN. A single attack on a network device within Local Area Network can wreak havoc into the entire organisation and the most worrisome is the fact that internal employees can initiate the attacks by plugging in unverified devices onto the organization's LAN.

Many organizational have developed standards and policies to evaluate the network security (Ahmed, Al-Shaer & Khan, 2008). Moreover, various researches on security policy evaluation and verification have been carried out. Atzeni et al. (2005) outlined the importance of using security metrics in evaluation of security policies. Ammann et al. (2002) described attack graph as another technique that can be used to assess network exploits vulnerabilities. Pamula et al. (2006) proposed a security metric based on the weakest adversary, which was the least amount of effort required to make an attack successful. Behi et al. (2016), proposed security metrics as a new approach to quantify network security.

1.2 Problem Statement

The likelihood of having devices that are unknown in a network continue to pose a security concern to many institutions that have adopted open policies on utilization of LAN. For instance, in empirical literature (Hess, 2013) where an open policy on the kind of devices hooked into the network is adopted, has been cited to be one way through which hackers may gain access to a network and cause disruptions. Shumate et al. (2014) found out that institution that have adopted an open policy on the BYOD are vulnerable to different types of attacks that can lead to breaches in confidentiality , integrity and availability of digital information assets.

When an employee attaches a personal device into an organizational network or machine (be it wired or wireless), it makes sense to worry about overall security. First, as soon as the LAN devices are attached, malware could migrate from the personal device into the company's machines and over the company's networks. Subsequently, sensitive data is likely to make its way onto the personal devices. As soon as information migrates to a device that the company does not control, the data is likewise no longer under control. Due to these challenges, there is a need to have a mechanism that identifies the LAN devices and analyses their vulnerabilities as they predominantly try to find existing threats and address how dangerous the exploits were on LAN devices. This study proposed a framework that uses security metrics to analyse, quantify vulnerabilities on LAN devices, and determine security score index for each device.

1.3 Research Objectives

1.3.1. General Objective

The study identified the parts that constituted a network security vulnerabilities analysis framework, techniques used in the existing network security vulnerabilities analysis framework, then developed a framework for analysing network security vulnerabilities on LAN devices.

1.3.2 Specific Objectives.

i. To analyse the network security policies for National Irrigation Board's LAN devices
ii. To examine the techniques used in the analysis of Network security vulnerabilities on Local Area Network devices
iii. To design and develop a network security vulnerabilities analysis framework
iv. To test the ability of the framework in flagging security vulnerabilities on the LAN

1.4 Research Questions

i. What are the network security policies that can be applied on National Irrigation Board LAN?
ii. What are the techniques used in the analysis of network security vulnerabilities on LAN?
iii. How can network security vulnerabilities analysis framework for LAN devices be developed?
iv. How can the functionality of network security vulnerabilities analysis framework for LAN be tested?

1.5 Justification of the Study

This research helped Network Administrator for National Irrigation Board in identification, analysis and reporting of potential security weaknesses on devices that were plugged into the Local Area Network. The information generated guided the management team in developing a substantial security protection plan to keep the network secure.

1.6 Scope of the Research

There exists various methods of analysing network security vulnerabilities on LAN. These includes host-based, wireless –based and application-based vulnerability assessments. This study focused on developing a framework that

analysed vulnerabilities on network hosts that were plugged into the NIB's LAN. In context of this study, the host were referred to as workstations.

CHAPTER TWO: LITERATURE REVIEW

2.1 Introduction

Literature review plays a critical role in any research. It helps and guides in understanding where, who and how research relevant to the analysis of network security vulnerabilities in LAN devices was carried out, how the network security and network security metrics were defined and measured, what were the findings of the earlier research and what are the gaps that exists between past research and present scenario.

2.2 Network Security

This section provides a review on network and network security with precise overview of network security at National Irrigation Board. The basics of network and network security were explained to give a hypothetical overview in this area. Network is defined as an interconnection of devices and systems for the purpose of sharing information and resources. The interconnection is done through a physical or a logical medium (Ahmad, 2010). There are various types of networks in use today namely; Local Area Network (LAN) which is an interconnection of devices within a building or several buildings within the same proximity; Wide Area Network (WAN) which refers to interconnection of two or more Local Area Network and Virtual Private Network (VPN) which allows users to access a private network through the internet.

Overreliance of interconnection has made security of networks more critical than ever. Network security is define as measures that organisation has put in place to ensure the safety of digital information in a network (Baral, 2010). Security of a network is measured by three elements namely; Integrity which refers to the ability to protect information from intentional or unintentional alteration; availability which refers to ensuring that authorised users have the ability to access the digital information when needed and confidentiality which refers to the ability of protecting digital information from unauthorised access.

Organisation have defined a security policy that describes mechanism of protecting digital information assets against security threats.

2.2.1 Network Security Management

The rapid growth of the threat designs, together with changes in network and security architectures, makes network security management more puzzling and complex than it was just a few years ago. Marin (2005) defined network monitoring frameworks, firewalls and intrusion detection system and traffic analysis as practical aspects of security networks. Flauzac et al. (2009) presented grid of security, a new approach for the implementation of distributed network security solution in a controlled and collaborative manner. In this approach, group of network devices ensures that a network device is trustworthy and interaction between them is done as per the security policies. Wuzheng et al. (2009) proposed use of Public Key Infrastructure (PKI)-based security framework as way of managing security in a wireless network. This framework defined various frameworks and treatment related to cryptography and network security. A firewall, a practical network security aspect as defined by Marin (2005), has been deployed on the Local Area Network for National Irrigation Board as a network security technique. It is the outermost layer of protection in a network that blocks network traffic with defined parameters. A set of rules has been configured on the hardware-based firewall to allow or restrict data transferred on a network. Another technique deployed on devices connected onto the LAN of this organisation is antivirus. The antivirus protects LAN devices from virus attacks. These techniques do not protect the Organisation's network from devices used and infected outside the corporate network, and then attached and used internally within the LAN.

2.2.2 Network Security Metrics

In this section, a review of the existing security metric was presented. According to National Institute of Standards and Technology (NIST, 2016) Computer Security Division, security metrics are standards of measurement that can be used

to measure the security level in an organization's network (Barker, 2007). Network security metrics are selected according to the organization security needs. It is the organizations' responsibility to develop and collect information in order to create good security metrics. Network security metrics are considered as reliable when they have consistently, ground truth, easy to collect, expressed numerically, have units of measure, are quantitative and have specific context (Jaquith , 2010).

Many organisations use qualitative methods to assess the security of their networks (Pamula , 2006). These methods are subjective and insights and therefore a network administrator cannot quantitatively identify which part of a network is the most secured. Other approaches to network security metrics have focused on individual network security vulnerabilities.

Network security metrics such as percentage of patched systems ignore interactions among network vulnerabilities. In this regard, there is a need of a general method to quantitatively assess network security. Several Researchers have developed security metrics for assessing network security. Philips et al. (1998) proposed Shortest Attack Path Metric that describes the minimum amount of effort an attacker needs to compromise a target. Pamula et al. (2006) proposed the Weakest Adversary Metric that assesses the strength of network security in terms of the attacker's ability to successfully penetrate a network. Ortalo et al. (1999) proposed the Number of Attack Path metric to assess the number of ways an attacker can compromise a target host. Li, Vaughn (2006) mention the Average Attack Path Length Metric.

2.2.3 Classification of Network Security Metrics

Few researches have been done on the classification of network security metrics. For instance, Vaughn et al. (2002) presented security metrics assessing the security capabilities of a system in a network. This metric was further classified into strength and weakness assessment. Pendleton et al. (2016) also developed four categories of security metrics that focused on the perspective between attackers and defenders in enterprise systems. These categories were; System

vulnerabilities security metrics for quantifying computer systems vulnerabilities through their user's password, software vulnerabilities, and the vulnerabilities of the cryptographic keys; Defence Security metrics quantifying the countermeasures deployed in an enterprise ; threats security metrics assessing the threats against an enterprise through the threat of zero-day attacks and Situations security metrics for assessing situations through security investments, security states and security incidents.

Other classifications were Network Security System Scoring and Ranking. These presented by industries such as the NIST (Barker, 2007) and were geared towards LAN device operations.

2.3 Network Security Vulnerabilities

Network Security vulnerabilities are weakness that can be exploited by a threat to do an illegal operation (Wiki, 2019). An attacker exploit a vulnerability through an application that links to a system weakness. These application runs on computer devices that are connected into the network. Protecting these devices from malicious activities reduces the chances of exploiting the vulnerabilities. A report for the year 2016 by Industrial Control System Cyber Emergency Response team (ICS-CERT) observed that a sharp increase of application vulnerabilities ("ICS-CER," 2016). 73.5% of these vulnerabilities had a Common Vulnerability Scoring System (CVSS) score of seven and above. A CVSS score of seven and above indicates that if the vulnerability is exploited, it can have a high impact. Majority of those vulnerabilities were associated with energy, manufacturing and water sectors applications. The most common vulnerability types includes cross scripting, buffer overflow and improper input validation vulnerabilities.

2.4 Network Vulnerabilities Analysis Techniques

This section focused on the review of the current frameworks and techniques in network exploration, detection of unauthorised network hosts and vulnerability assessment.

2.4.1 Network Exploration and Detection

Network exploration is a process of probing a network to generate network map that comprises network hosts such as servers, computers, printers and other nodes. The most common tool for network exploration is Network mapper (NMap). NMap is an open-source tool that explores a network by using raw Internet Protocol packets to determine the hosts available in a network. If the hosts do not respond to the data packets sent out by Nmap, it will conclude that no host or network device uses the scanned IP addresses. Nmap discover hosts, analyses and compares the host's signature with its database to determine the host's operating system, the services running on it and other characteristics that can attribute to differentiating a host from another network device (Lyon, 2008).

Xprobe2++ is another current network exploration tool and technique that scans a network to build host signature based on the collected information. The tool is able to identify all the details of an operating system running on a network host. Its host discovery modules are designed to perform host probing, firewall detection, and provide additional information to estimate the actual response time and identify packets propped by the detected host (Yarochkin, 2009).

LANsurveyor, another network exploration tool, uses multi-discovery techniques to discover active hosts in a network. The tool achieve this by sending out Simple Network Management Protocol (SNMP) pings and scans to Active Directory Domain Controllers that contains information about network services. LANsurveyor is able to monitor the network and dynamically update the network map with active new devices and rogue connection to the network. Once rogue connections are detected, they are automatically disabled from the network.

Another network exploration tool in the market is IPSonar. The tool works by scanning every host on a network to provide visibility of the connectivity between hosts/network devices and the underlying supporting networks, so that the administrators can analyse the potential security threats and attack patterns. IPSonar also has a capability to encompass identification of network bottlenecks

due to poor configurations and vulnerabilities exploitable by unknown devices (Lumeta, 2019).

From unauthorised network devices perspective, an attacker can gain entry into the network via unauthorised device. Detection of a network host can be achieved by using network exploration tool and techniques as discussed. These tools are able to give a comprehensive visibility of a network by automatically updating the network maps any time a change is detected in the network. The changes include network topology and unauthorized network host connection. However, these tools cannot determine the level of malicious activities and vulnerabilities in isolation without any vulnerability analysis techniques that are built-in or provided by another framework.

2.4.2 Vulnerability Assessment Tool

A number of existing vulnerability assessment tool has been design to determine specific vulnerabilities. For instance, Nessus is a well-known vulnerability assessment tool, designed to detect remote flaws, local flaws and missing patches of a host on the network (Wiki, 2018). Nessus uses the Nessus Attack Scripting Language (NASL), which allows network security experts to use a simple language to describe individual attacks. Nessus uses scanning, enumeration and vulnerability detection processes to determine the services that run on the network devices and checks for vulnerabilities based on known vulnerabilities. However, this tool has pre-defined parameters and therefore lack dynamism in dealing with user –define security metrics.

2.5 Proposed Network Security Vulnerability Analysis Framework

One of the major drawback of the approaches of the previous research was that they do not quantify vulnerability with some certainty. This study proposed the use of an integrated and quantifiable approach that provided proactive security mechanisms on LAN. Quantifying security variables involved identifying appropriate set of metrics based on vulnerabilities found in network devices by applying Goal- Question –Metric method (GQM). GQM is a three-step process that

get appropriate security metrics for the network devices. First, specific quantifiable goals that organisation hopes to achieve with regard to Network Security were defined. Subsequently, these questions were answered by identifying and developing appropriate security metrics. This method guaranteed that all the metrics identified were according to the goals of the organization. After an act of exploring the LAN according to the GQM method, security metrics were developed. The next phase was the analysis of vulnerabilities identified on the LAN devices. Based on the analysis results, the last phase was assigning of Security Score Index for each device and remedial action.

2.5.1 Proposed System Flow Diagram

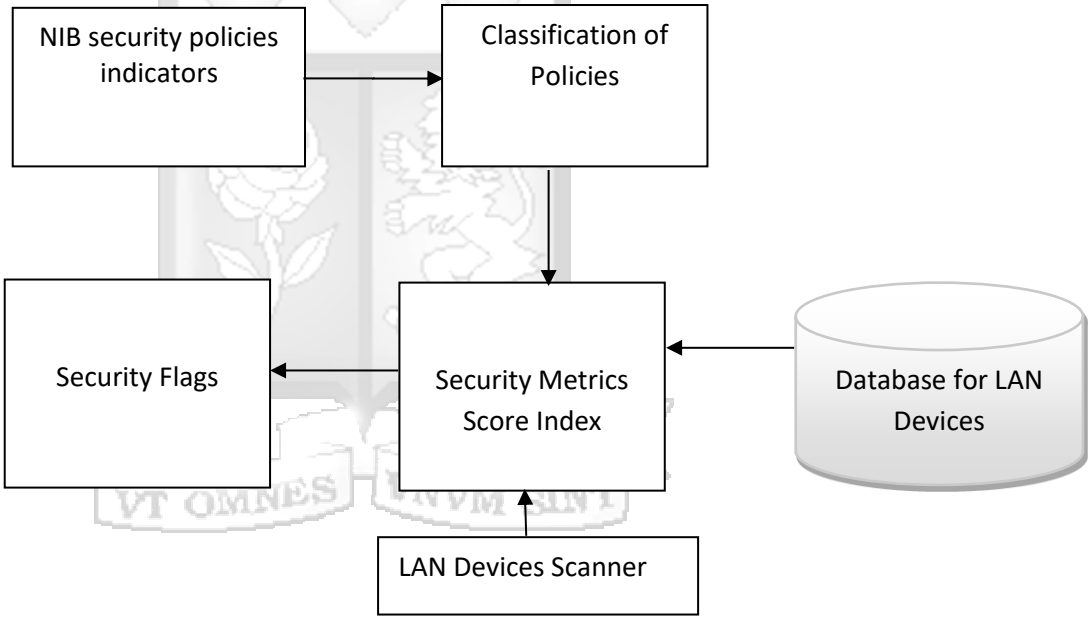


Figure 2. 1 Proposed Network Security Vulnerability Analysis Framework

The system flow diagram in figure 2.2 illustrate all components of the proposed framework. Using secondary data collection techniques, a list of rules were developed from the ICT policies of National Irrigation Board. The next phase involved classification of the data. The classified data was assigned a security metrics score index that was applied to LAN devices to flag and determine the level of vulnerabilities.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter outlined methods and techniques used in this study. It builds on theoretical viewpoints and empirical research techniques from network security to assemble a set of components to develop a Network Security Vulnerability Analysis Framework. Rist (1977) suggested that because research methodology is more than simply techniques for data gathering, selection of a methodology should focus at accessing the phenomena under observation, rather than the data itself. Methodology is a related set of assumptions that reflect how a researcher views are achieved. How this reality is articulated through research is dependent on choice of the method; choice of method is reflective of what the researcher wants to uncover. Moreover, the chapter also discussed, target population, sampling, data collection and data analysis procedures.

3.2 Research Design

Leedy (1997) defines research design as a strategy for a study, providing the overall framework for data collection. In this study, case study design was applied so that suitable research methods are used to ensure the attainment of the objectives set out in Chapter 1.

3.2.1 System Architecture

An integrated system architecture was adopted to ensure that the framework is working as expected. The first component of the system was a network scanner for identifying LAN devices connected to NIB's network. Second component was a logical quantifiable security metrics for analysing vulnerabilities on LAN devices and MySQL database as the third component.

3.2.2 System Analysis

Object-Oriented Analysis (OOA) is a system analysis procedure that identifies software requirements and developing software specification in terms of software system's object model. In this study, Object Oriented Analysis was realised through use of; Case diagram, applied to graphically represent system uses-cases, actors, relationships among the use cases and actors; System sequence diagram applied in a given use-case to show the activities of external actors while interacting directly with the system.

3.2.3 System Design

Object –Oriented Design (OOD) model was applied in this study to develop the framework as per the requirements identified in the system analysis phase. Approaches utilized to achieve the OOD are System design class diagram for conceptual modelling, detailed modelling and data modelling; Entity Relationship Diagram to illustrate the relationship between objects, people, concepts or events within the system. The software was also developed using Computer-aided software engineering (CASE) frameworks to ensure that it is of high-quality and reduce time and effort in software development ("Computer Aided Software Engineering, "2018). Case tool used in system development were Microsoft Visio for UML diagrams and Microsoft Project to assist in developing a plan, assigning resources to tasks, tracking progress, managing the budget, and analysing workloads.

3.2.4 System Development and Implementation

Rapid Application Development (RAD) was used to develop the prototype. Rapid Application Development (RAD) is a type of incremental model. Key objective is for fast development in the limited period and delivery of a high-quality system at a relatively investment cost. Project control involves prioritising development and defining delivery deadlines or "time boxes". If the project starts to slip, the emphasis is on reducing requirements to fit time box, not in increasing the deadline. It iteratively produces a production software. The RAD model

comprised of four stages: Requirements planning, User design, Construction, and Cutover. There is a continuous interaction between the user design and construction phases. RAD was built up to respond to the requirement of the fast system delivery. Due to the fast system delivery, the model produced a demonstrable outcome as fast as possible and refined that outcome at low cost (Powell-Morse, 2018).

The creation of the software was well-designed, robust, and maintainable software using object technologies and language such PHP. Programming was done in an Integrated Development Environment (IDE) that is suitable for meeting the objectives. Windows 10 Operating System, Xampp (Apache, PHP and MySQL) and PHP YII MVC framework were used. Secure software development techniques were applied in the development and the objects defined under design mapped into the code. The new system was implemented using a parallel approach, running along with the existing solution.

3.2.5 System Testing

During system implementation, testing was introduced at an early stage of System Development Life Cycle (SDLC) and therefore V-Model testing was employed. The model was validated through various test: Unit testing to ensure the smallest unit of code worked correctly when isolated from other codes; Integration test to ensure that different systems units are communicating correctly among them; System test to verify that both functional and non-functional requirements of the system were met and finally user acceptance test to ensure that use requirements were met and the system is working as expected.

3.3 Target Population

The research was carried out at National Irrigation Board. Secondary data was collected from the ICT Assets Inventory System as well as ICT policy documents.

3.4 Data Collection Procedure

ICT policy documents of NIB were examined with the key aim of extracting information about LAN security while ICT Asset Inventory System was reviewed to extract information about LAN devices.

3.5 Data Analysis Techniques

According to Carl & Louise (2003), data analysis is the procedure of looking at data and summarizing it with the intention of getting useful information. In this study, Content analysis method was used to analyse the data gathered from ICT Policy Documents for National Irrigation Board. Data gathered was categorized in themes and sub-themes, to be able to be comparable.

3.6 Ethical Consideration

During the entire process of this study, necessary measures were taken to ensure confidentiality and privacy of the collected data.

CHAPTER FOUR: SYSTEM ANALYSIS AND ARCHITECTURAL DESIGN

4.1 Introduction

This section describes processes and details that were undertaken toward development of the system for the purposes of automating and easing security analysis procedures on the network, and flagging of potential vulnerabilities thereof. Having data collected from the network in compliance with the network security policies, the system then became the core analysis framework by which the data was reduced into useful indexes or pointers for interpretation and enactment of network security measures. Finally was the development of a structured design of the proposed system by use of case diagrams, sequence diagrams, entity relation diagrams and security designs.

4.2 Data Analysis

The security of any network is firstly defined in the policies that govern it. Thus, it was important to review the policy documents at NIB in order to establish the broader aspects of network security. This was followed by classification of document contents into themes. Classification was significant in both creating familiarity with data and tracking what data has been collected and what needs to be collected. Next step was to develop subcategories and coding scheme using a comparative technique as prescribed by Glaser and Strauss (1967). The coding scheme was applied to generate a rough of set of key words and themes and eventual produce a thematic framework. In the next step, thematic framework was used to select the appropriate portion of data and the data was recorded in terms of themes. Themes were structured and categorised in terms of context, relationship and activities and as categories became saturated, significant themes were added to the thematic framework and the lesser significant ones discarded. Such aspects as Connectivity Software and Update Installation, and Device Access among other policies were distinctly drawn from this process. As such, the data that would be extracted from the LAN devices was grouped into any of those categories.

4.2.1 Data Analysis Results

4.2.1.1 Security Policies and Variables

Appreciating the above-mentioned groups of policies, precise measurable variables were developed in each category. These, in real sense, were the quantifiable properties of the workstations against which data would be drawn for the purposes of analysis. The input variables that were considered for security analysis and how they were classified are shown in table 4.1.

Table 4. 1 Input variables

Classification (Security Policy)	**Property (Input Variables)**	**Value**
Software and Update Installation Policies	i. Defence Update	No. of days since the last update was run
	ii. Operating system	No. of versions older than Windows 10. For instance, Windows 8 was denoted as 2 versions before windows 10.
	iii. Un-allowed software	No. of un-allowed software on the workstation
	iv. Un-updated software	No. of un-updated software on the workstation
Device Access Policies	i. Open unused ports	No. of open unused ports on the workstation
	ii. Local (user) accounts	No. of local accounts on the workstation
	ii. Administrator account on the Workstation	Admin account configured on the workstation 1, otherwise 0

Connection Policy	i. Firewall Status	Firewall configured and running on the workstation 0, otherwise 1
	ii. Anti-Virus	Anti-virus configured and running on the workstation 0, otherwise 1
	iii. AutoScan of External Storage media	Ability of workstation to run auto-scan on external media 0, otherwise 1
	iv. Last virus scan by user	No. of days since last virus scan invoked by user
	v. Prohibited Services running on the workstation.	No. of prohibited services running on the workstation

For the purpose of this research project, the security of a network was defined as reduced or minimal number or counts of vulnerabilities on the comprised workstations. Thus, the higher the vulnerability counts the less secure the network was considered to be, and the lower the number of vulnerabilities the more secure the network was considered to be. The Nessus Vulnerability Scanner was thus used to help establish the number of vulnerabilities on each workstation on the network.

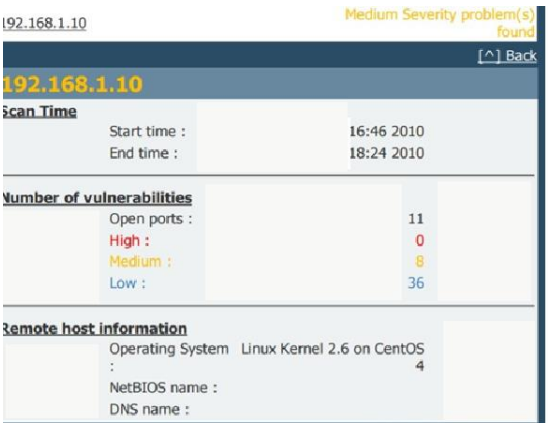


Figure 4. 1: Nessus Vulnerability Network Scanner Report (Hackertarget, 2019)

In the figure 4.1, for instance, the host (workstation with IP address 192.168.1.10) had 44 vulnerabilities, 8 of them medium-risk and 36 of them low-risk. There are no high-risk vulnerabilities.

4.2.1.2 Workstation Properties

Having established the input variables and accordingly classified them, various mechanisms were sought in order to collect necessary data and organize it for subsequent analysis. With help of the Nessus Vulnerability Scanner, values for a number of other variables were established including the version of operating systems running and the number of open ports on each workstation. For the variables for which such values could not be obtained from the scanner, reference was made to the organizational device inventory database or, as well, individual workstations were literally opened and investigated for system information among other details.

There were certain workstation properties, which were derived from the behaviours of the designated users or caretakers. For instance, for workstations that did not perform certain security tasks automatically, it was expected that the users regularly invoked such functions like scanning their devices regularly or external storage devices before using them on their workstations. Such data was thus inquired from the users.

4.2.1.3 Security Variable Weighting

Regression method was employed to get the weights for each of the security variables identified in the previous section. Regression referred to how each input variable (Independent variables) was found to affect the vulnerability count (Dependent variable). By way of aggregating the behaviours of the variables on the selected workstations, a mathematical rule would be obtained that would averagely define the combined effect of the security variables on each workstation to its security and well-being.

4.2.1.3.1 Regression Equation

Given a set of data with a number of independent variables and one dependent variable, the linear regression equation normally takes the form:

$$y = a + b_1x_1 + b_2x_2 + \cdots + b_kx_k$$

Equation 4. 1 Regression (statistics-how-to, 2019)

Where y = dependent variable, a = regression constant, x = independent variable, b = corresponding regression coefficient of x and k = number of independent variables.

Given a k independent variable case, the regression coefficients can then be computed thus:

$$b_i = \frac{\left(\sum x_{k-i}^{k}\right).\left(\sum x_i y\right) - \left(\sum x_i x_{k-i}\right).\left(\sum x_{k-i} y\right)}{\left(\sum x_{k-i}^{k}\right).\left(\sum x_i^{k}\right) - \left(\sum x_i x_{k-i}\right)^{k}}$$

Equation 4. 2 regression coefficient (statistics-how-to, 2019)

The symbols retain their initial meanings. X_{k-i}, however, means the product of independent variables excluding the one in the i^{th} position, i.e. $\frac{x_1 * x_2 * \ldots * x_k}{x_i}$.

Finally, the regression constant *a* is calculated thus:

$$a = \bar{y} - b_1\bar{x}_1 - b_2\bar{x}_2 - \cdots - b_k\bar{x}_k$$

Equation 4. 3 regression constant (statistics-how-to, 2019)

Where $\bar{y}$ = average of the independent variable, $\bar{x}_i$ = average of dependent variable in i^{th} position, b_i= corresponding correlation coefficient for x in i^{th} position.

All the regression coefficients and the regression constant computed, they are then correspondingly employed to define the regression equation thus:

$$\boldsymbol{y = a + b_1x_1 + b_2x_2 + \cdots + b_kx_k}$$ ***Equation 4. 4 Regression***

Where y = dependent variable, a = regression constant, x = independent variable, b = corresponding correlation coefficient of x and k = number of independent variables.

This regression equation essentially is a mathematical rule that maps the combined effect of the independent variables to the dependent variable.

Supplied with complete data sets about the workstations on the network, the system performed regression analysis on them and establishes a mathematical rule that was used to compute a security score index for each workstation. Referring to the regression process above, the regression equation (mathematical rule) was what entirely constituted the analysis framework.

4.2.1.3.2 Security Threshold

The security score index is a value that the analysis framework yields for the value of y, the dependent variable, upon applying its prediction rule on a workstation. Understanding that the dependent variable in this research refers to the number of vulnerabilities found on the workstation, the security score index thus directly relates to the vulnerability count. The higher the security score index obtained for a workstation the higher the anticipated security threats on it. The vice versa is also true.

4.2.1.3.3 Security Threshold

The core purpose for devising the Network security analysis framework, also called the Network Vulnerability analysis framework, is for it to be able to help flag potential vulnerability that could exist on the workstations or other devices on the Local Area Network. It was thus imperative to develop a means by which the derived security indexes for the workstations could be given full meaning by rating them as secure or not secure on the network. Given the dynamism that the network information characteristically presented itself with, it was found not wise to assign a static value by any means (percentage or amount) for the threshold. The system ought to, somehow, also dynamically, determine the threshold against which the security of a workstation would be regarded as safe or unsafe.

To achieve this, minimal acceptable values were declared and submitted against each independent variable during security variable definition. This could be thought as 'creation of a lowest ideal virtual workstation'. By applying the security rule on the 'virtual workstation', the system was able to establish the

threshold against which to rate the security of the other workstations on the network. Any workstation that obtained a security score index less than or equal to this threshold was regarded to be safe. A higher security index meant the corresponding workstation was unsafe and would be regarded to be a threat to the network. This process, then, of rating workstations as safe or unsafe according to their resultant security score indexes is subsequently referred to as ***flagging***.

4.3 Requirement Analysis

Specifying descriptions of services, features and limitations that should be addressed by the network security vulnerability analysis framework can be categorised into functional and non-functional requirements.

4.3.1 Functional Requirements

The functional capabilities of the system include the User registration (registration of users and management of their account privileges), Scanning (ability to fetch LAN devices information from an inventory system), Check vulnerabilities **(**for checking vulnerability by analysing the properties of the LAN devices and generate security index score, Flagging (achieved when the framework compares workstation security score index against this threshold index, the workstations were then automatically flagged as safe or unsafe) , Report generation (The system generate a report by showing the security indexes for each workstation with flags).

Other functional requirements include the ability to update the workstation properties, security variable details and threshold values right on the application interface. Any changes on the threshold values and workstation properties invokes automatic recalculation of the associated security indexes.

4.3.2. Non Functional Requirements

The system was a web -based application developed in an object-oriented, component-based Model View Controller (MVC) PHP web application framework called YII (Yes, It Is). This framework provides a simplified way for

development of complex systems by helping in code generation, simplified data validation approaches, convenient error reporting among others. Critical also is the conformity to MVC organization of code which allows the business logic of the system to be well laid out separately from the view pages, enhancing clarity of code and easy of execution. By breaking down the business logic into smaller units, the system was optimized for fast performance and minimal resource consumption. YII also comes with an excellent Cascade Styling Sheets(CSS) that constitutes an excellent user interface for relaxed visibility and minimal navigation between screens.

The database technology used for data storage is SQL MariaDB for its versatility, lightness, robustness, security and speed. All diligence was put forth to ensure integral interaction between the application frontend and the database in the backend in a secure way, and guarantee data integrity. Of this too involved optimal layout of the business logic, to ensure only minimal and very necessary calls to the database for data reading and writing purposes.

4.4. System Design

This section described the process of defining system architecture, system modules, and interfaces to satisfy specified requirements.

4.4.1 Proposed System Architecture

The developed solution has the following main actor: System User who runs the system and handles overall management of the system.

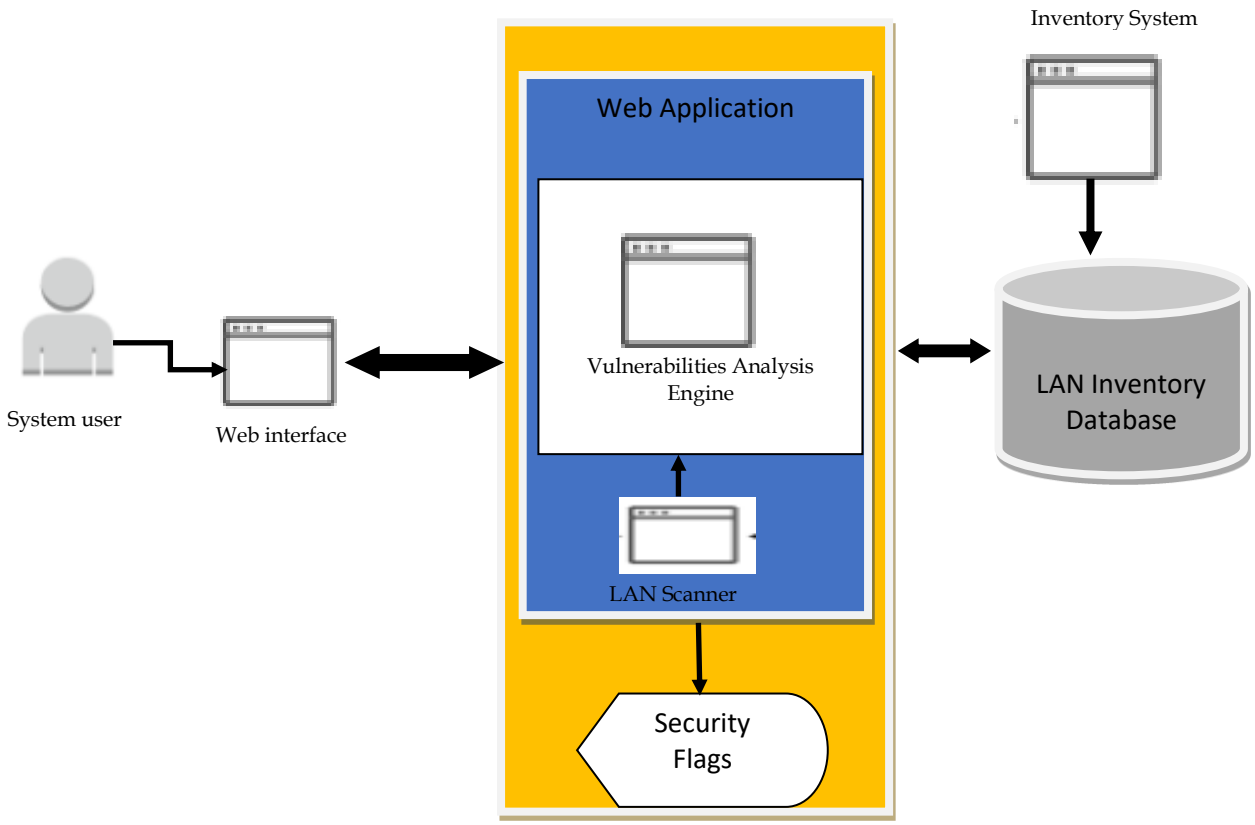


Figure 4. 2 System Architecture

Figure 4.2 demonstrates an architectural overview of how the system was designed to function and the flow of interactions for various processes. As illustrated above, the user (system user) starts the system through a web interface. A LAN scanner was triggered to check to give details of LAN devices connected to the network. Next phase is to subject the discovered devices through the vulnerability analysis engine where conformity to prescribed intuitional security policies is checked. Vulnerability analysis engine contains classified security policies to determine the level of vulnerability threat for LAN devices.

4.4.2 Use-case Diagram

Figure 4.3 shows the major interactions that took place between various modules and actors in the network security vulnerability analysis framework.

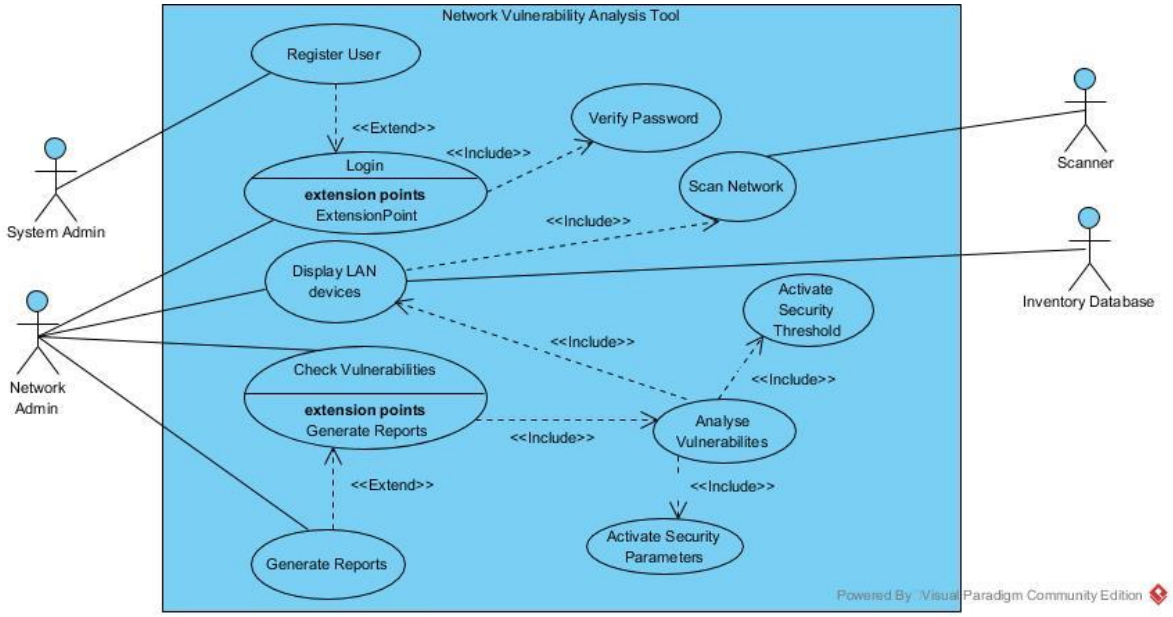


Figure 4. 3 Use case diagram

Various Use cases are discussed below:

4.4.2.1 Use Case: User registration

This use case description describes user registration is performed

Pre-conditions:

The user not previously registered.

Post Conditions:

User is registered and can now be allowed to access the system

Main success Scenario

1. System Admin opens the system through a web browser
2. Selects register user
3. Enters User details as required
4. System verifies user details do not exist
5. System records details and present results.

Alternative Flow: Duplication Error

At step 4, the system finds user details already exists

- User cancels registration
- User update details

Alternative Flow:

At step 5, the system fails to register user

- Replicate the process

4.4.2.2 Use Case: User Login

This use case describes how user login is performed

Pre-conditions:

Must be a registered user.

Post Conditions:

User logs into the system

Main success Scenario

1. User opens the system through a web browser
2. User selects sign in
3. User keys in logins credentials
4. System verifies user logins credentials
5. System records details and present results.

Alternative Flow: Login failure

At step 4, the system finds user credentials do not exist

- User cancels the sign in process
- User update details

4.4.2.3 Use-case: Display LAN devices

Preconditions

LAN devices database exists

Post-Condition

A list of LAN Devices is displayed

Main Success Scenario

1. User start the system
2. User logins successfully
3. User select display devices
4. System activates the scanner to get devices already plugged into the network
5. System updates the LAN device database

Alternative Flow: No devices found error

At step 2, system does not any display

- No data stored in the database.

4.4.2.4 Use case: check Vulnerabilities

Precondition

Connection between LAN devices and Security Metrics must exist

Post- condition

Each device is assigned security metrics score index

Main Success Scenario

1. User logins into the system successfully
2. Selects Checks vulnerabilities
3. The system retrieves LAN devices and analyse the vulnerabilities based by activating security parameters and security threshold respectively
4. System generates and display a list of network devices with associated vulnerabilities (if any) and security metrics score index

Alternative Flow: **Check Vulnerability Failure**

At step 3, system fails to check vulnerabilities

- Check the connection between devices database and security metrics database

4.4.2.5 Use case: Generate Reports

Precondition

User must have queried the service

Post- condition

User view the report

Main Success Scenario

1. User starts the framework
2. Select generate report

4.4.3 System Sequence Diagram

Sequence diagram in figure 4.4 models interaction between users, objects and systems of Network Security Vulnerability Analysis Framework for LAN devices.

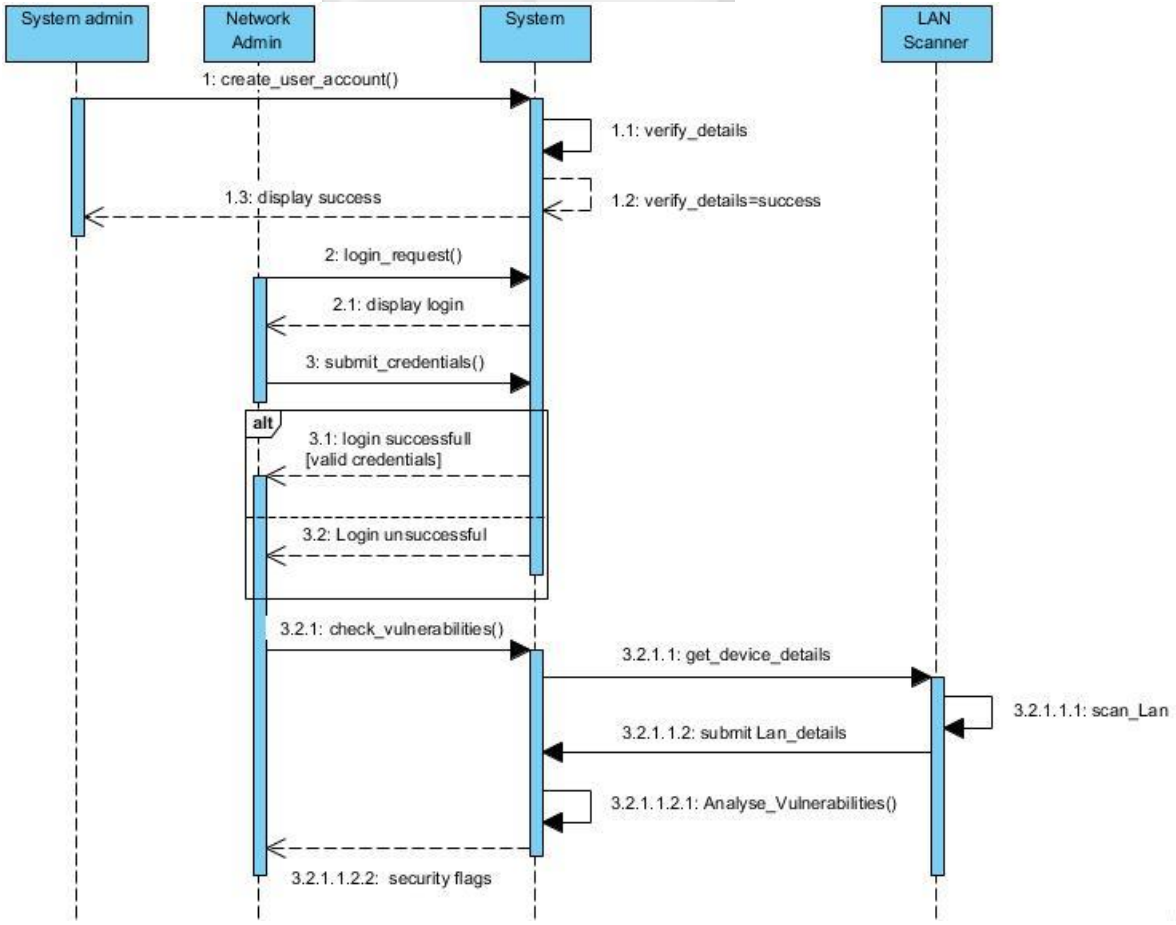


Figure 4. 4 Sequence diagram.

4.4.4 Entity Relationship Diagram.

Entity relationship diagram in figure 4.5 represent all the entities used in the database to save data that can be accessed from the system. Device details table stored inventory of LAN devices while device properties hold various properties for each device. Security Variable Table contained rules that should be met by LAN devices to allow them continue accessing services from the network. Classification table held details of the groups for security variables.

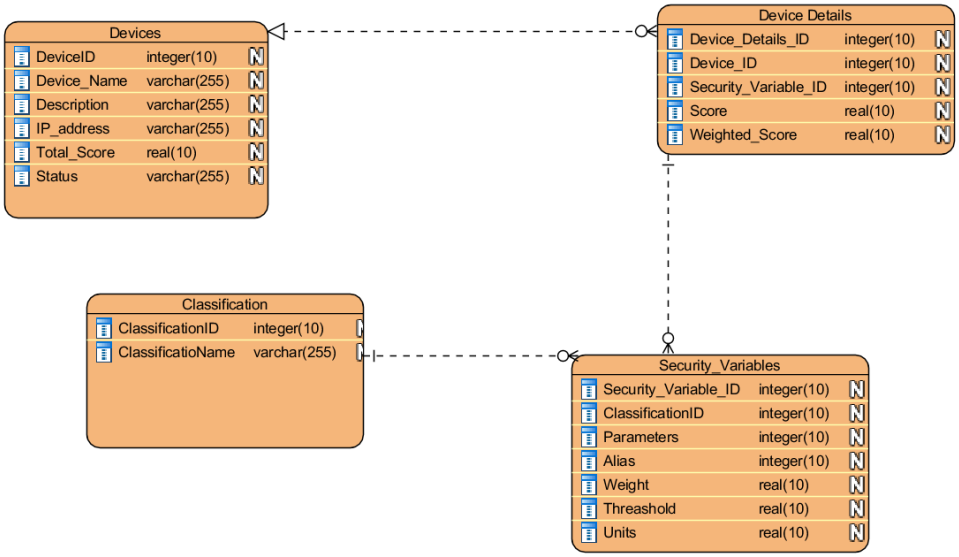


Figure 4. 5 Entity Relationship Diagram

4.5 Security Design

The system was designed in conformity with modern standards to assure security and most importantly, data integrity. The YII (Yes It Is) framework that was used to develop the system provided an excellent user authentication interface to ensure only valid users have access to the system functionalities. A second validation was also applied on all requests to filter and allow only verified request sources, otherwise, the requests were blocked and unattended. This was realized by use of CSRF (Cross Site Request Forgery) key which ensures, for instance, that form submission originated from the application and not elsewhere.

CHAPTER FIVE: SYSTEM IMPLEMENTATION AND TESTING

5.1 Introduction

This chapter described the implementation and testing of Network Security Vulnerability Analysis Framework for LAN devices. Implementation part explained different parts of the framework, how they were implemented and functioned. The testing section of this chapter focused on usability testing and functional testing to verify if the application attained the objectives of the proposed solution.

5.2 System Implementation

The algorithm that was used to develop the network vulnerability analysis framework applied the regression equation 4.2 discussed in Chapter 4. By applying the regression coefficients evaluation, the system was able to generate the coefficients for each of the security variables, called the weighting.

#	Classification	Variable	Alias	Weighting	Threshhold
1.	Access Policy	Open Unused Ports	Ports	5.98	0.00000 No.
2.		Local Accounts	Accounts	8.64	2.00000 No.
3.		Local Admin Account	Admin	2.72	1.00000 Yes/No
4.	Connection Policy	Anti-virus Installed	Antivirus	2.08	0.00000 Yes/No
5.		Firewall Configuration Status	Firewall	1.92	0.00000 Yes/No
6.		Auto-scan of External Storages	Auto Scan	2.43	1.00000 Yes/No
7.		Last Scan Invoked by User	Last Scan	17.81	0.00000 Days Ago
8.		Prohibited Services Running	Services	6.67	0.00000 No.
9.	Software and Update Policy	Operating System	OS	7.11	2.00000 Versions older
10.		Prohibited Softwares	Prohibited	6.91	0.00000 No.
11.		Stale Softwares	Stale	10.10	2.00000 No.
12.		Last Defense Update	Defense	18.03	1.00000 Days Ago
13.	Vulnerability	Vulnerability Count	Vulnerability	-163.00	40.00000 No.

Figure 5.0 security variable weights

As illustrated in figure 5.0 above, the highlighted dependent variable was also assigned a weight, which was the regression constant, Equation 4.1.

Thus, the Security rule, consequently, then was: $Vulnerability = -163.00 + 5.98Ports + 8.64Accounts + 2.72Admin + 2.08Antivirus + 1.92Firewall +$

$2.43AutoScan + 17.81LastScan + 6.67Services + 7.11OS + 6.91Prohibited + 10.10Stale + 18.03Defense$

Network Security Vulnerability Analysis Framework comprised of the frontend and the backend subsystems. They are explained below:

5.2.1 Front End Sub-System

This module is mainly a virtual program interface that depended on an external network LAN scanner in order to receive information about LAN devices. Figure 5.1 below shows the system gathering data from the network. This scanning process is not intrinsic in the system; hence the system got data about the workstations by reading from the scanner report file.

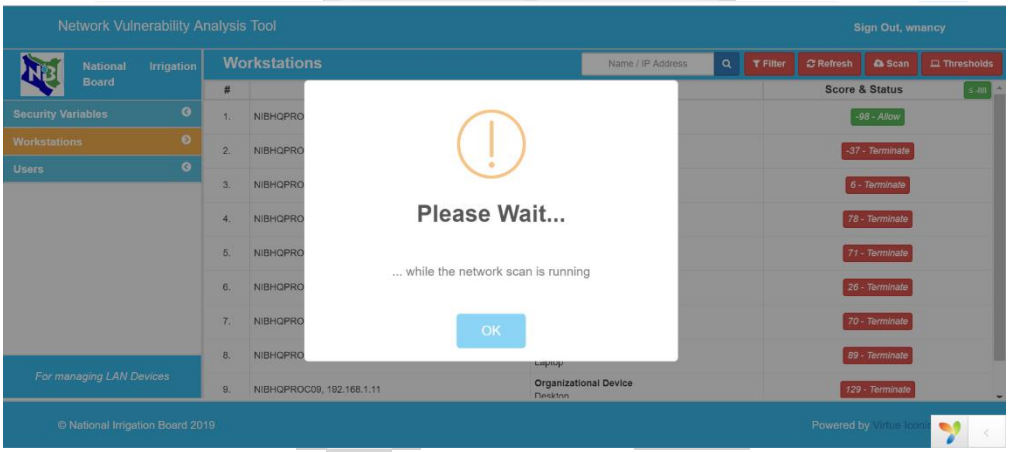


Figure 5. 1 Frontend Subsystem

The workstation properties (details) are returned such that are classified and pre-organized, so the system is able to perform the analysis without further instruction from the user.

5.2.2 Backend Sub-System

Upon completion of the data analysis, the system presented a number of screens on which the user gained an insight about the workstations.

a) The Security Variables

This screen is a report on the kind of details (variables) that were analysed by the scanner about each workstation on the network, accordingly classified. From the system's vulnerability analysis module, each security variable was dynamically assigned a weight as illustrated in figure 5.2.

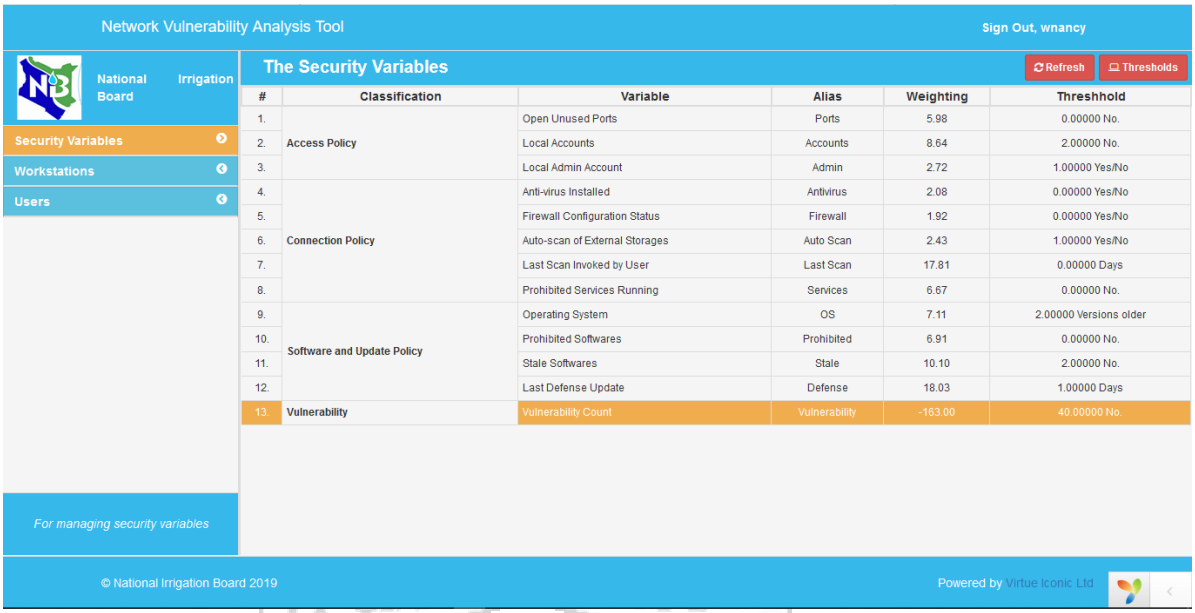


Figure 5. 2 Security variables

b) Security Thresholds

An important aspect of the variables that was also preconfigured in the system was the threshold. Figure 5.3 below shows the thresholds settings for the independent variables. The values implied the highest acceptable risk levels in each case. These values can also be adjusted from the application interface, and be applied on the workstations by clicking on the 'Apply & Close' button as illustrated on figure 5.4

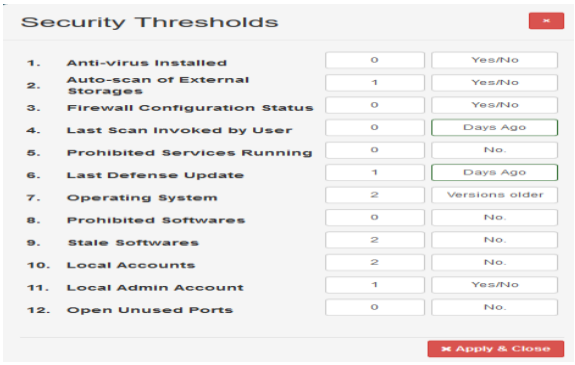


Figure 5. 3 Security Thresholds

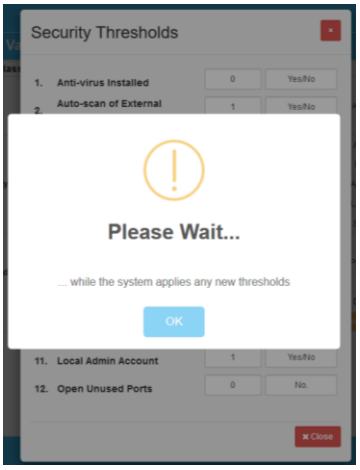


Figure 5. 4 Threshold Update

c) Workstation

Figure 5.5 illustrated the workstations screen with the list of workstations for which the network scanner retrieved data. For each, a security index was computed and security status appended for flagging. This rating changes automatically recomputed for a workstation whose details were adjusted from the system as shown in figure 5.6.

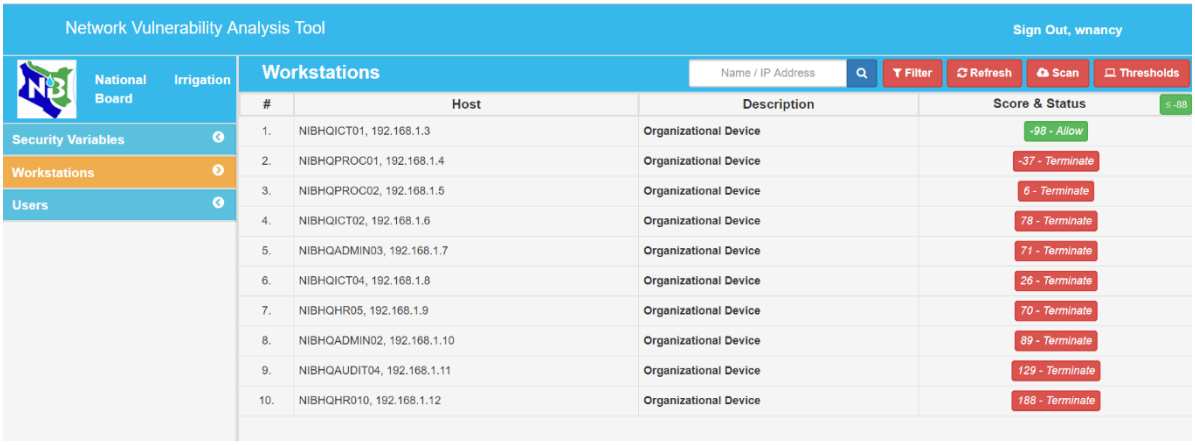


Figure 5. 5 workstation details

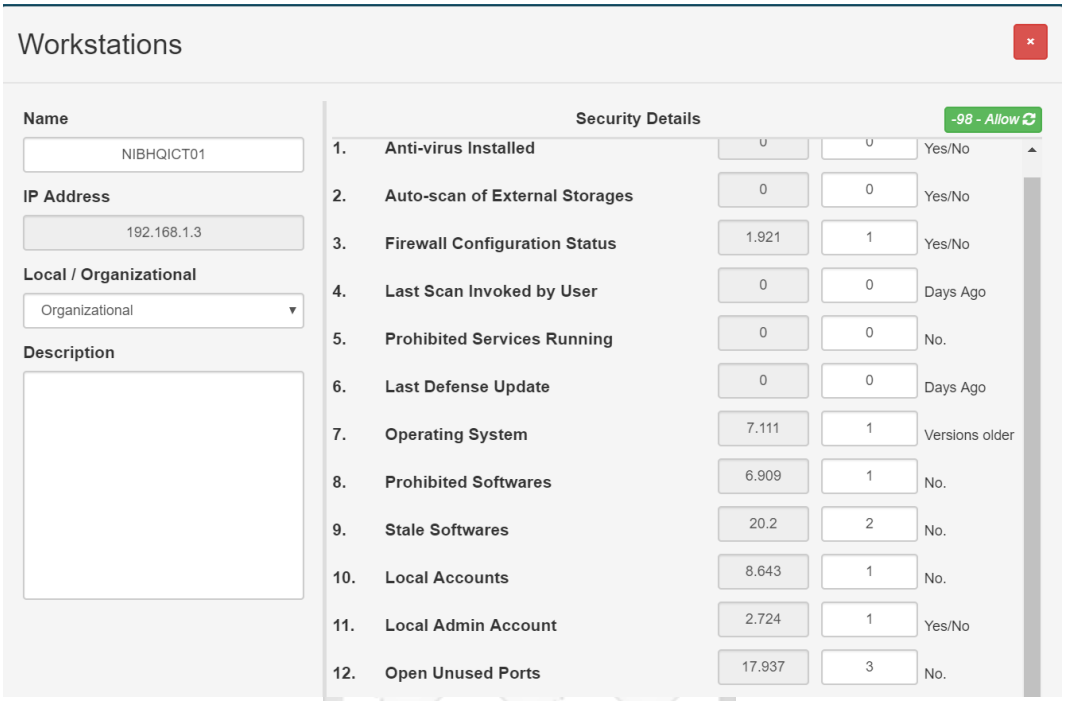


Figure 5. 6 workstation security variables

5.3 Testing

The testing section of this chapter focused on usability testing and system testing to verify if the application attains the objectives of the proposed solution.

5.3.1 System Testing

System testing focused on the functionality parts of the system, which are: user login, fetching LAN devices details from a scanner, checking vulnerabilities on LAN devices, flagging and report generation.

Table 5. 1 System Test Case

Module Name	Test Plan	Expected Behaviour
User login	Enter user credentials	Only registered users with correct credentials are allowed to login else an error message is displayed
Scan	The user click on the scan button	The system display the workstation and their details including their security score index else, The system

		should return an error message when the network scan report file was not available
Flagging	The user click on the scan button	The system display flags that are easily visually interpreted as red for unsafe, green for safe and security index scores were consistently interpreted by the system and accordingly color-coded for flagged else the security score index and colour code does not change

Figure 5.7 illustrates the response message received when user login was executed unsuccessfully.

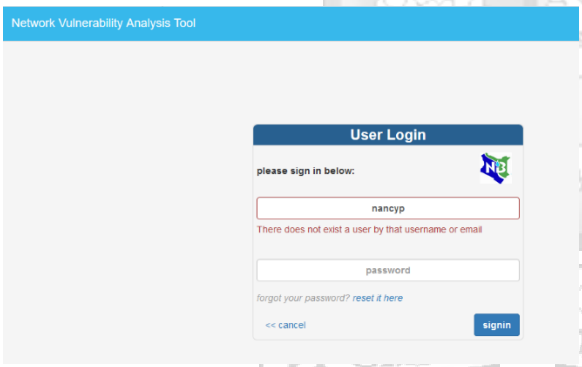


Figure 5. 7 Unsucessful login

Figure 5.8 depicts the output when scanning process is invoked by the user

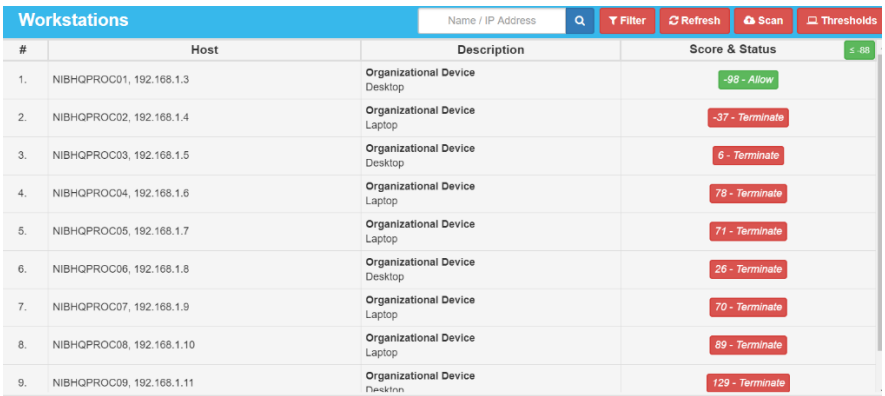


Figure 5. 8 Scan output screenshot

5.3.2 Usability Testing

Usability testing focused on the user interface, efficiency, usefulness and responsiveness. In this study, six (6) respondents were selected to carry out usability testing (Appendix A).

Usability results

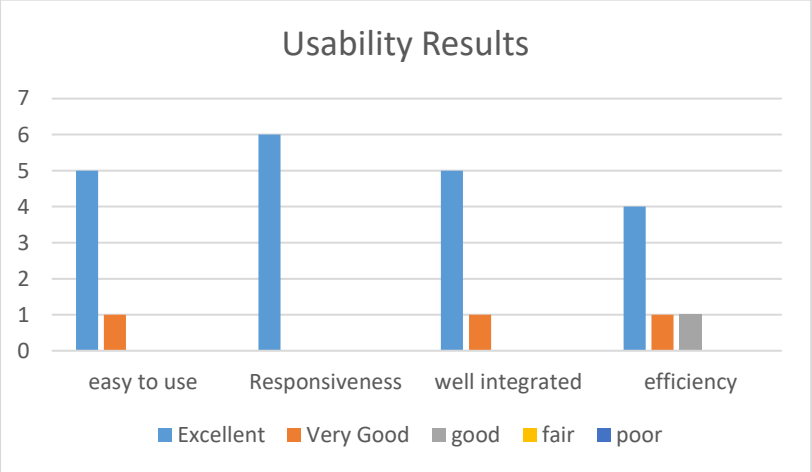


Figure 5. 9 usability results

As illustrated in figure 5.9, out of 6 respondent who tested in the system application of usability testing, 5 rated "easy to use" attribute excellent and 1 rated very good. On "responsiveness" attribute,all the 6 respondents rated excellence. On "well integrated" attribute, 5 rated excellent while 1 rated very good. On "efficiency attribute" 4 rated excellent, 1 rated very good and 1 rated good.

CHAPTER SIX: DISCUSSION OF RESULTS

6.1 Introduction

In this chapter, results obtained during the research formed the basis on which the Network Security Vulnerability Analysis Framework for LAN devices was developed. The framework was tested to evaluate its compliance with the specified requirements. Subsequently, the Chapter details the research findings of the study. This includes analysis of the results in relation to the research objectives.

6.2 Network Security Metrics

The first objective in Chapter 1 section 1.3 was to determine the network security metrics that are applicable to the LAN devices of National Irrigation Board. From the data analysis of this study, 11 security variables were identified as security metrics for National Irrigation Board's LAN Devices.

By devising methods of quantifying them in relation to the network security, and applying appropriate security analysis models, it was possible to evaluate the effect of each variable to the network security.

6.3 Network Security Vulnerabilities Analysis Techniques

The second objective was to investigate the techniques used in the analysis of network security vulnerabilities. The literature review discusses the current techniques used in the analysis of network vulnerabilities on LAN devices and their challenges, which is in harmony with the findings of this study.

6.4 Network Vulnerability Analyses Framework for LAN devices

The third objective was to develop a Network Security Vulnerability Analysis Framework for National Irrigation Board's LAN devices. Research findings show that since National Irrigation Board have adopted open policies on utilization of LAN, the network security vulnerability analysis framework was paramount in securing the network.

6.5 Network vulnerability analyses framework testing

The last objective was to test the Network Security Vulnerability Analysis Framework. System testing focused on the functionality parts of the system while usability questionnaire in appendix 1 was used to test the usability of the system. 6 respondents who tested in the system application of usability testing, 5 rated "easy to use" attribute excellent and 1 rated very good. On "responsiveness" attribute,all the 6 respondents rated excellence. On "well integrated" attribute, 5 rated excellent while 1 rated very good. On "efficiency attribute" 4 rated excellent, 1 rated very good and 1 rated good.

CHAPTER SEVEN: CONCLUSIONS, RECOMMENDATIONS AND FUTURE WORK

7.1 Introduction

This chapter provides conclusions of the research described in the dissertation. Recommendations and proposals for future work in the area of Network Security Vulnerability Analysis are suggested.

7.2 Conclusion

It is possible to automate security analysis and flagging for any given network. While the dynamics involved may continually pose challenges given the rapid technological advancements in this and other regards, but this study found that, any LAN administrator who would have a keen interest in monitoring the security of their network would apply such a strategy as suggested in this dissertation to keep their network in check.

Network security analysis remains an item of interest for all institutions that run a LAN. The art and science as to how threats find their way into a LANs may be well investigated and measures applied to bar. Indisputably, this strategy can only do so much. This study has delivered a prompt means by which pending vulnerability can be caught up with and remedied beforehand.

7.3 Recommendations

The use of the network security vulnerability analysis framework can be a convenient means of ensuring adequate compliance to the security policies by helping to effectively implement other security strategies on the network. However, from the findings of the dissertation, the researcher recommend the following:

(i) There is need to regularly review security policies to incorporate emerging trends in network security.

(ii) There is need for institution to prepare an adequate network vulnerabilities defence mechanism that will minimise the ever growing list of vulnerabilities

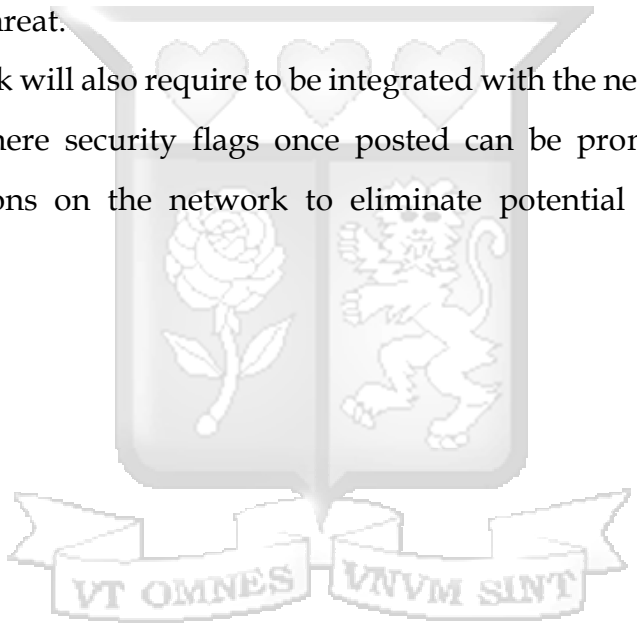
(iii) Use of an automated vulnerability remedial technology that can address vulnerabilities discovered by LAN scanners.

7.4 Future works

The Network Security Vulnerabilities Analysis Framework will need to be integrated with the network analyser or scanner for seamless real-time information from the network and prompt monitoring and flagging of potential threat holes on the network.

Alternatively, the framework can also be modified with the ability to perform network scanning and consequently acting on such data in a timely manner to flag areas of threat.

The framework will also require to be integrated with the network administration dashboard where security flags once posted can be promptly translated into remedial actions on the network to eliminate potential threat zones on the network.



REFERENCES

Ahmed, M., Al-Shaer, E., and Khan, L. (2008). *A novel quantitative approach for measuring network security* (pp. 1957 - 1965).

Akin, T. (2002). *Hardening Cisco Routers*. Retrieved January 24, 2019 from https://dl.acm.org/citation.cfm?id=572347

Alhazmi, H. and Malaiya, Y. (2006) Prediction capabilities of vulnerability discovery models. In Proc. Reliability and Maintainability Symposium, pages 86–91, Atzeni, Andrea, Lioy and Antonio. (2006). Why to adopt a security metric? A brief survey. Doi:10.1007/978-0-387-36584-8_1.

Ammann, A., Wijesekera, D., and Kaushik, S. (2002). *Scalable, graph-based network vulnerability analysis.* (pp. 217–224)

Atzeni, A., & Lioy, A. (2005). Retrieved from https://www.researchgate.net/publication/226387170_Why_to_adopt_a_security_metric_A_brief_survey

Azar, M., Dahar, A. and M. Jahani (2012). The assessment of computer network security by Honeypot technique in IDS & IPS systems"," journal of information technology era, pp. 78-84.

Baral, H.R., 2010. *AASA-A protocol for Network Security Assessment Methodology*. Chelmsford: Anglia Ruskin University.

Barens, S. (2018). "Six growing threats to network security". Retrieved 2 February 2019 from https://gcn.com/articles/2018/10/18/network-security-threats.aspx

Barker, C. (2007). *NIST Security Measurement NIST SP 800-55 Revision*. Retrieved January 31, 2019 from http://csrc.nist.gov/groups/SMA/ispab/documents/ minutes/2007-09/Barker ISPAB Sept2007-SP800-55R1.pdf

Behi, M., GhasemiGol, M., & Vahdat-Nejad, H. (2006). A new approach to quantify network security by ranking of security metrics and considering

their relationship. Retrieved January 25, 2019 from https://www.researchgate.net/publication/322195069

Carl F. Auerbach, L. (2003). *Qualitative Data: An Introduction to Coding and Analyzing*.

CyberCop Scanner (2012). Retrieved February 1, 2019 from www.nai.com/asp set/products/tns/ccscanner intro.asp

Dinh, T. N., Xuan, Y., Thai, M. T., Pardalos, P. M., and Znati, T. (2012). On New Approaches of Assessing Network Vulnerability: Hardness and Approximation. IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 20, NO. 2

Feng, C., ZHANG. Y, Jin-Shu, SU and Wen-Bao, H. (2010). Two Formal Analyses of Attack Graphs. Journal of Software, Vol.21, No.4, pp.8380y848

Flauzac, O., Nolot, F., Rabat, C. and Steffenel, L. (2009). Grid of security: a new approach of the network security. 3rd International Conference on Network. Retrieved February 2, 2019 from https://hal.archives-ouvertes.fr/hal-00510836/document

Gholi, F., Modiri, N. and Riahi, M. (2014). Providing a process for testing the security of webbased intranet applications," the National Conference on Advances in science, engineering and basic electronics, Tehran

Habib, K., and Ahmad, N. (2010) Analysis of Network Security Vulnerabilities and Vulnerabilities by Development & Implementation of a Security Network Monitoring Solution. Retrieved February 1, 2019 from https://www.diva-portal.org/smash/get/diva2:832701/FULLTEXT01.pdf

Hewett. R, and Kijsanayothin P, (2008). Host-Centric Model Checking for Network Vulnerability Analysis. Computer Security Applications Conference, 2008 Annual, pp 225-234.

Hess, K., (2013) "The top five trends in mobile and BYOD security," Retrieved January 30 , 2019 from http://www.zdnet.comlthe-top-five-trends-in-mobile-andbyod-security-70000 14226.

IBM (1994). Internet security systems System scanner. Retrieved February 2, 2019 from www.iss.ne

ICS/CERT,(2016). Retrieved February 2, 2019 from https://ics-cert.us-cert.gov/sites/default/files/Annual_Reports/NCCIC_ICS-CERT_2016_Annual_Vulnerability_Coordination_Report_S508C.pdf

Jaquith, A. (2010). *Security metrics*. Upper Saddle River, NJ: Addison-Wesley.

Javad, M., Kangavari M., and Fathi, S. (2013). To design and build the knowledge base of expert systems for network security test," Journal of electronic and cyber defense, pp. 43-51.

Li, W. and Vaughn, R. (2006). Security Research Involving the Modeling of Network Exploitations Graphs. In Proceedings of 6th IEEE International Symposium Cluster Computing and Grid Workshops (CCGRID). Retrieved January 30, 2019 from https://www.tib.eu/en/search/id/TIBKAT%3A597718539/

LiZhidong, Yang, W. Wang, and W. Man. (2012). Network Security threat situation evaluation based on spread analysis. Journal of Jilin University (Engineering and Technology Edition) Vol. 42

Lumeta (2019). Retrieved February 11 from http://www.lumeta.com/products/spectre/ipsonar.

Lyon, G. (2008). *Nmap Network Scanning*. Sunnywale: Insecure. Com LLC.

Manadhata, P. and Wing, J. An attack surface metric. In First Workshop on Security Metrics, Vancouver, BC, August 2006. Retrieved January 22, 2019 from https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=905450

Marin, G. (2005). *Network security basics*. In security & Privacy, IEEE, Issue 6, Vol. 3, pp. 68-72, 2005.

Murray,A. (2011). An overview of network vulnerability modeling approaches. GeoJournal. Retrieved February 2, 2019 from doi:10.1007/s10708-011-9412-z.

NIST (2009). United States Computer Emergency Readiness Team. Retrieved January 23, 2019 from http://www.us-cert.gov.

Noel. S, and Jajodia. S, (2004). Managing attack graph complexity through visual hierarchical aggregation[C]. Proceedings ACM CCS Workshop on Visualization and Data Mining for Computer Security, Fairfax, Virginia, ACM, pp.109-118., 2004

Pamula, J., Ammann, P., Jajodia, S. and Swarup, V (2006). A weakest-adversary security metric for network configuration security analysis. In ACM 2nd Workshop on Quality of Protection 2006. Retrieved January 28 , 2019 from https://dl.acm.org/citation.cfm?id=1179494

Pawar, M., & Anuradha, J. (2015). Retrieved January 28, 2019 from https://www.researchgate.net/publication/277723629_Network_Security_and_Types_of_Attacks_in_Network

Pendleton, M., Garcia-Lebron, R., and Xu, S.. (2016). A Survey on Security Metrics. Retrieved February 1, 2019 from doi: 10.1145/3005714

Phillips C. and Swiler P. (1998). A Graph-based System for Network Vulnerability Analysis. In Proceedings of the 1998 Workshop on New Security Paradigms (NSP-W), pages 71–79.

Rist, R. (1977). Retrieved Jan 30, 2019 from https://www.academia.edu/28347974/Approaches_to_Qualitative_Data_Analysis_Intuitive_Procedural_and_Intersubjective

Rogers, R., E. Fuller, G., Miles, M., Hoagberg, T., Schack, T. and Cunningham, B. (2005). Network Security Evaluation Using the NSA IEM. Retrieved January 23, 2019 from https://www.elsevier.com/books/network-security-evaluation-using-the-nsa-iem/rogers/978-1-59749-035-1

Sahinoglu, M. (2005). Security meter: A practical decision-tree model to quantify risk. In IEEE Security and Privacy. Retrieved Jan 30, 2019 from doi: 10.1109/MSP.2005.81

Savola, R. (2007). "Towards a security metrics taxonomy for the information and communication technology industry," in Proceedings of the International Conference on Software Engineering Advances, (Washington, DC: IEEE Computer Society), 60–60.

Shumate, T., & Ketel, M. (2014). Bring Your Own Device: Benefits, risks and control techniques. *Quality Of Protection*, 1-12. Retrieved Jan 30, 2019 from doi: 10.1007/978-0-387-36584-8_1

Solawinds (2013). LANsurveyor. Retrieved February 3, 2019 from https://www.solarwinds.com/lansurveyor-to-network-topology-mapper-2013.

Vaughn, R., Dampier,D. and Siraj, A. (2002). Information security system ranking and rating. Retrieved February 1, 2019 from https://www.researchgate.net/publication/221180192_Information_Assurance_Measures_and_Metrics_-_State_of_Practice_and_Proposed_Taxonomy.

Vizandan, A., Ghadri, A., and Sheykh, J.(2011) Passive defense in infrastructure communications networks with an emphasis on the security assessment of flow encryption algorithms," Journal of passive defense, pp. 47-52.

Wang, J., 2009. *Computer Network Security: Theory and Practice.* Higher Education Press https://en.wikipedia.org/wiki/Nmap

Wikipedia contributors. (2018, December 3). Nessus. In *Wikipedia, The Free Encyclopedia*. Retrieved February 22, 2019, from https://en.wikipedia.org/w/index.php?title=Nessus&oldid=871758109

Wuzheng, T., Maojiang, Y., Feng, Y. and Wei, R. (2009). A security framework for wireless network based on public key infrastructure. Computing,

Communication, Control, and Management, Vol. 2, pp. 567 – 570. Retrieved February 2, 2019 from https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5267848

Yun, Y., Xi-shan, X., Yan, J., Zhi-chang. Q, and Wen-Cong C.(2015) .Research on the risk adjacency matrix based on attack graphs. Journal on Communications

APPENDICES

Appendix A: Usability Testing Questionnaire

The questionnaire was used to gather information about the experience that the responders had when using the framework and performance of each module

1. Have you in the past used a network vulnerability framework?

[ ] Yes [ ] No

If yes, what was its name?

2. Did the application closed unexpectedly during testing?

[ ] Yes [ ] No

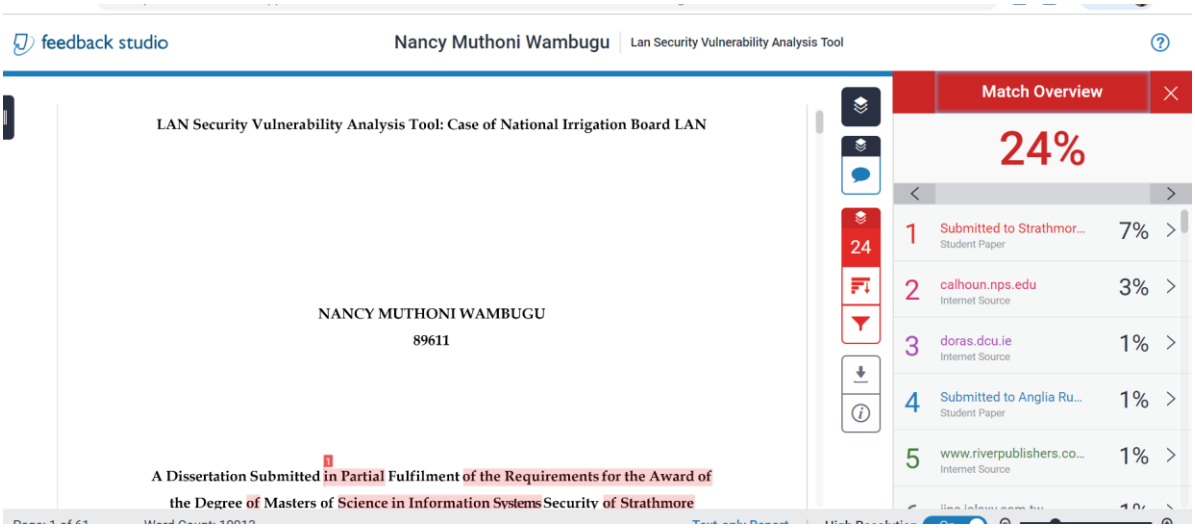
If yes , please expound on what happened.

3. How would you rate the whole application? Kindly tick where appropriate for each attribute

Attribute	Poor	Fair	Good	Very Good	Excellent
Easy to Use					
Responsiveness					
Well Integrated					
Efficiency					
Useful and Satisfying					

4. Anything else would like to comment about the usability of the system?

Appendix B: Turnitin Report



Declaration

I declare that this work has not been hitherto submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, this dissertation contains no material previously published or written by another person except where due reference is made in the dissertation itself.

Student Name Nancy Muthoni Wambugu
Student Number 89611
Signature .....
Date .....

Approval

This dissertation of Nancy Muthoni Wambugu was reviewed and approved by the