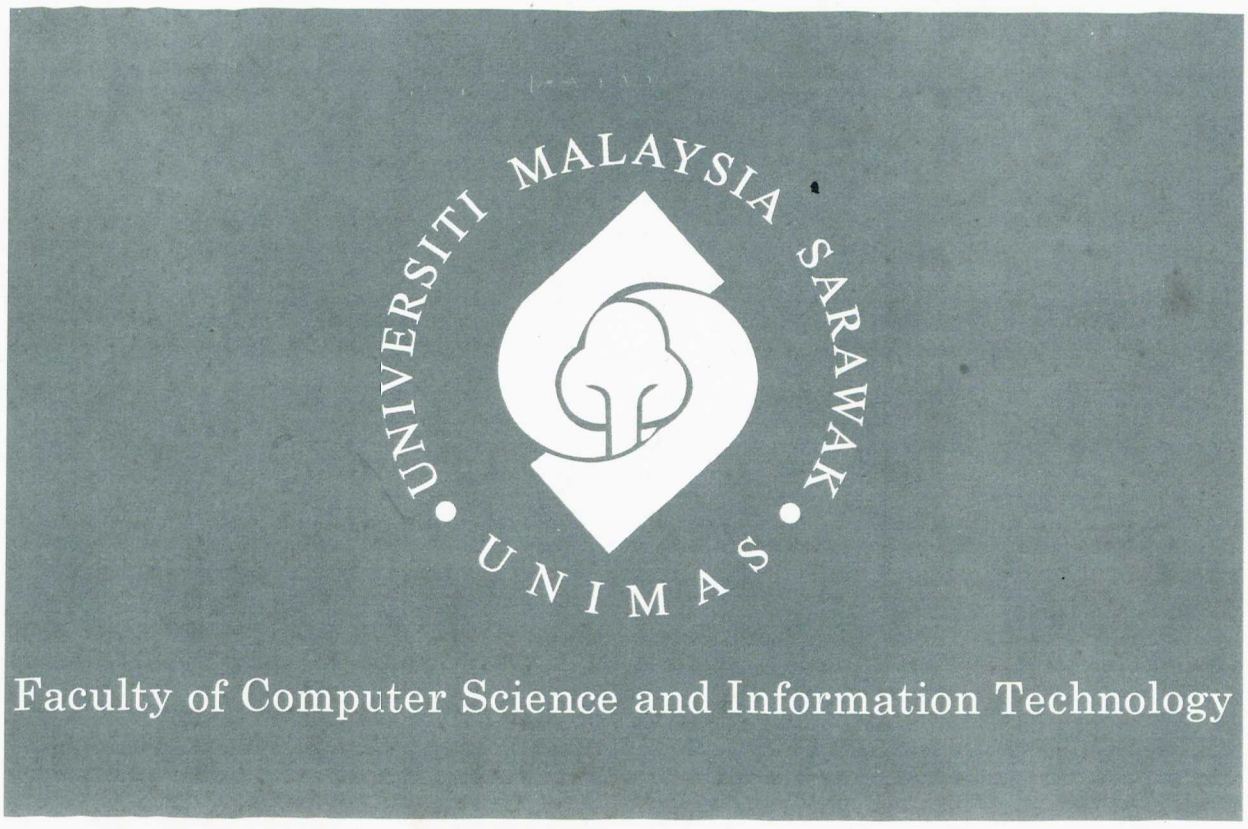

COMPARATIVE STUDY BETWEEN SIGNATURE-BASED AND ANOMALY-BASED NETWORK INTRUSION DETECTION SYSTEM (SBNIDS AND ABNIDS)

Chiadighikaobi Ikenna Rene

Bachelor of Computer Science with Honours
(Network Computing)
2015

COMPARATIVE STUDY BET[illegible]-BASED AND ANOMALY-BASED NETWORK [illegible]CTION SYSTEM

(SB[illegible])

CHIADIGHIKAOBI IKENNA RENE

This project is submitted in partial fulfilment of the
Requirements for the degree of
Bachelor of Computer Science with Honours
(Network Computing)

Faculty of Computer Science and Information Technology

UNIVERSITI MALAYSIA SARAWAK

2015

DECLARATION

I hereby declare that this project is my original work. I have not copied from any other student's work or from any other sources except where due reference or acknowledgement is not made explicitly in the text, nor has any part had been written for me by another person.

..... 09/03/015

(CHIADIGHIKAOBI IKENNA RENE) Date(m/d/y)

UNIVERSITI MALAYSIA SARAWAK

THESIS STATUS ENDORSEMENT FORM

TITLE **COMPARATIVE STUDY BETWEEN SIGNATURE-BASED AND ANOMALY-BASED NETWORK INTRUSION DETECTION (SBNIDS AND ABNIDS)**

ACADEMIC SESSION: 2014/015

(CAPITAL LETTERS)

hereby agree that this Thesis* shall be kept at the Centre for Academic Information Services, Universiti Malaysia Sarawak, subject to the following terms and conditions:

1. The Thesis is solely owned by Universiti Malaysia Sarawak
2. The Centre for Academic Information Services is given full rights to produce copies for educational purposes only
3. The Centre for Academic Information Services is given full rights to do digitization in order to develop local content database
4. The Centre for Academic Information Services is given full rights to produce copies of this Thesis as part of its exchange item program between Higher Learning Institutions [or for the purpose of interlibrary loan between HLI]
5. ** Please tick (√)

☐	CONFIDENTIAL	(Contains classified information bounded by the OFFICIAL SECRETS ACT 1972)
☐	RESTRICTED	(Contains restricted information as dictated by the body or organization where the research was conducted)
☑	UNRESTRICTED	

Validated by

(AUTHOR'S SIGNATURE)

(SUPERVISOR'S SIGNATURE)

Permanent Address
OBIDIKE UMUEZE ABA, ABIA STATE
NIGERIA.

Date: 07/03/015

Date: 3/7/15

Note * Thesis refers to PhD, Master, and Bachelor Degree
** For Confidential or Restricted materials, please attach relevant documents from relevant organizations / authorities

ACKNOWLEDGEMENT

I would like to express my greatest gratitude and appreciation to my supervisor Dr Johari Bin Abdullah for his leadership and instructions from the start of this project to the completion. Most importantly I will like to give very big thanks, love and God's blessings to my family, and to almighty God who saw me through and made me stand even in my weakness. To my friends and love ones I really appreciate you in one way or the other you rendered you help to me during this project.

June 25, 2015

Abstract

The rise in numbers of network intrusion is related to the growth and importance of the Internet in our daily live. In order to provide protection to organizations information / data, Intrusion Detection System (IDS) plays an important role in Network security. Signature-based intrusion detection focus on matching attack signature with the already stored signature in the database, it generates an alert if the incoming packets signature matches with the one in the database. Signature-based is vulnerable against newly emerging attacks, because the signature is not yet stored in the database, this leave this detection technique with the problem of false negative rate. On the other hand, Anomaly-based detection techniques which is a behaviour techniques, detects the abnormal behaviour in a computer systems and networks. The deviation of packets from normal behaviour is considered as attack. This leaves this technique with the problem of false positive rate. In this proposed project we will be making a comparative study of Signature-based and Anomaly-based IDS in order to select suitable comparison parameters between different approach in network intrusion detection, to evaluate suitable software/system for deploying Signature-based and Anomaly-based detection and to conduct experimental study to evaluate the differences in selected parameters in different approach in network intrusion detection. This project will provide a comparative analysis result between SBNIDS and ABNIDS after the evaluation study using DARPA dataset and we will be able to select a suitable techniques in the area of performance, efficiency in data size and non-functional parameters like CPU and Memory usage, which the result proposed that ABNIDS is better than SBNIDS and the conclusion was based on the evaluated parameters.

Contents

List of Tables

List of Figures

List of Tables

List of Figures

Chapter 1

Introduction

1.1 Introduction

Computer technology is now part of humans, as we get to be dependent on it. As the use of technology increases, so does the risk associated with technology increases. Network security is a challenge in the area of information system and management. According to [18], *"People are working in the field of network security, from 1987 when Dorothy Denning published an intrusion detection model"*, the published article was one of the first in the area of intrusion detection and this enabled a larger view of interest in this area. Though there is not yet a complete solution on detection system. Security threats for computer system over the network have increase immensely. According to [16] the 2014 Sophos-security threat report, botnets and malware based attacks has increased in recent years. Such as there are many various types of Security threats denial of service, vulnerability break-in and etc. While many security mechanisms have been introduced to undermine those attacks but none of them can completely prevent all attacks. Security mechanism can be perfect theoretically, but in the implementations stage there are always some compromises such as

miss configuration by admin, or malicious usage by a user. Based on the assumption that the system is not perfect, Intrusion Detection System (IDS) has been introduced to record all the threats and intrusions. Going through some research papers, it is clear that no perfect solution has been found for intrusion detection. SBNIDS identifies intrusion in a network by matching signature of incoming packets with existing one in the database, while ABNIDS uses behaviour techniques, it checks the behaviour of the incoming packets, it is abnormal SBNIDS generate alert. [11] This project focuses on understanding the way SBNIDS and ABNIDS works and analysing the abnormal connection that has been detected by IDS via Snort and comparing it with Anomaly-based detection technique which is done with PHAD (Packet Header Anomaly Detector), using the 1999 offline DARPA IDS evaluated data set [10] . IDS works as a network packet Sniffer, which based on comparison of packets content with known virus signatures encapsulated as rules, which can initiate action and record events and information related to them in a log file.[8] Snort is one of the known SBNIDS audits network packets and compare the signature with the existing signature with the one in database.

1.2 Problem Statement

Theoretically, firewall is the primary technique to filter any unauthorized user from gaining access and any unauthorized activity related to computer security manner. A firewall will fence around your network but still will not have the capability to detect anyone trying to break into the network system.[7] The firewall does not know who are penetrating it without permission. Firewall is defending the intrusion from outside the network but it does not defend the system from internal intrusion. It simply restricts access to the designated points. From the user point of view, firewall is a perfect defensive system but the reality is IDS system is a perfect defensive system. The IDS can capture all traffic and recognize attacks

against a network that a firewall are unable to detect. Here is an example that we extract from Robert [7].

"In April of 1999, many sites were hacked via a bug in Cold Fusion. These sites all had firewalls that restricted access only to the web server at port 80. However, it was the web server that was hacked. Thus, the firewall provides no defence. On the other hand, an intrusion detection system would have discovered the attack, because it matched the signature configured in the system and can compare the system behaviour."

Signature-based NIDS is vulnerable against newly emerging attacks. This is because before Signature-based techniques detect an intrusion, its signature should have been stored in the database and without storing the signature, it will be unable to be detected by Signature-based techniques. SBNIDS lags between a new threat discovery and its signature being applied to the IDS. During this time the IDS will be unable to identify the threat. Therefore, every new malicious traffic or attack need to be analysis and the signature of that malicious traffic identified before NIDS using signature detection can be able to detect and capture such a packet. Every signature requires an entry in the database and each packet needs to be compared with all the entries in the database, because every packet that will pass through the network, will be check for malicious attack, and compare with the database. This may potentially slow down the throughput of the system [8] .

Anomaly-based detection techniques which is a behaviour techniques, detects the abnormal behaviour in a computer systems and networks. The deviation of packets from normal behaviour is considered as attack. Anomaly IDSs strategy is to detect abnormal behaviour and it tries to model what is normal rather than what is anomalous. This detection technique generates an alarm whenever the deviation between a given observation at an instant and normal behaviour exceeds a predefined threshold. This leaves this technique with the problem of false positive rate. Anomaly based detects attacks by comparing the new traf-

fic with the already created profiles.[11][5] Analysis of Anomaly based approach is done in this proposed project with PHAD (Packet Header Anomaly Detector). PHAD is a simple time-based protocol anomaly detector for network packets.

1.3 Objective

The objective of this proposed project is to conduct comparative analysis between Signature-based and Anomaly-based intrusion detection system. This project aims at identifying the number of detection rate for each detection techniques and several other parameters.

Other objective includes:

1. To select suitable comparison parameters between different approach in network intrusion detection.

2. To evaluate suitable software/system for deploying Signature-based and Anomaly-based detection.

3. To conduct experimental study to evaluate the differences in selected parameters in (1).

1.4 Methodology

This defines how the works flow from the beginning until the end of the proposed project. The significant of this stage is for planning and controlling the proposed project to meet the objectives. The scope will cover all the processes which are directly or indirectly related to this proposed project in order to ensure that the proposed project is achieved. We made use of this research process in order to be guided in this proposed project. Refer to Figure 1.1, a research method from research methodology book [2].

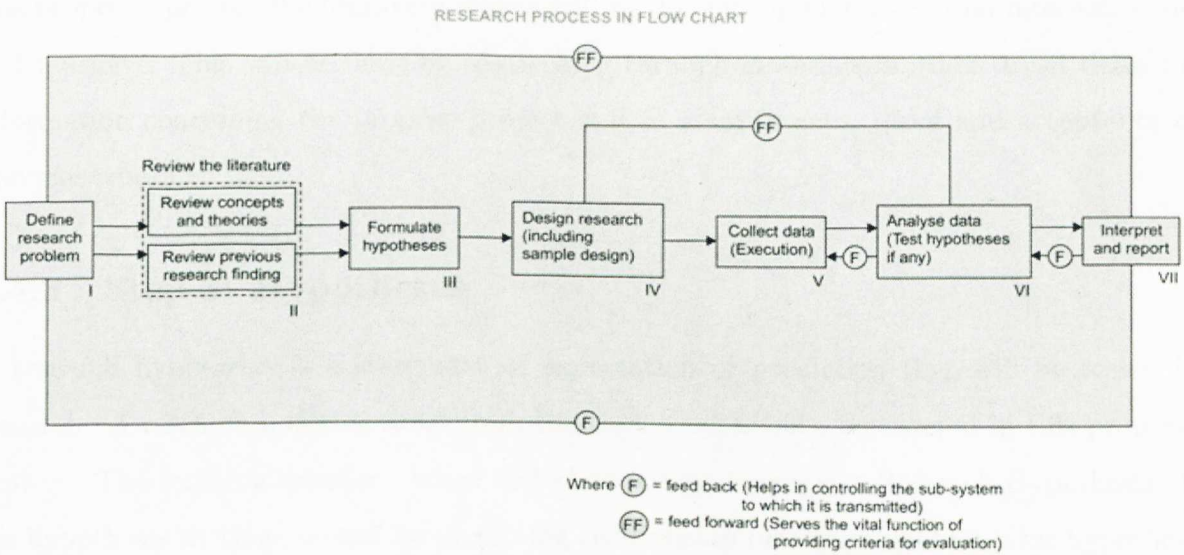

Figure 1.1: Research Process [2]

1.4.1 Step 1: Research problem

Identifying a research problem is one of the first steps in conducting a research. To start a research, there should be a pre-idea of the research that will generate into necessity for the research to be carried out. A research problem should be such in which the researcher may be deeply interested; it should express a relation between two or more variables. The problem should be within manageable limits, it should not be too comprehensive.

1.4.2 Step 2: Literature Review

A literature review discusses published information in the subject area, and some-times information in a subject area at a certain time. In Chapter two of this project, the literature review will be discuss, which will be use to give more clarification on this project topic. In