IMPROVING THE THREAT DETECTION PERFORMANCE OF A NETWORK INTRUSION DETECTION SYSTEM USING A 3-TIER FRAMEWORK

Samira Dinusha Wickrama Senanayake

(179350H)

Dissertation submitted in partial fulfilment of the requirements for the degree Master of Science in Computer Science specializing in Security Engineering.

Department of Computer Science and Engineering

University of Moratuwa

Sri Lanka

May 2021

DECLARATION OF THE CANDIDATE & SUPERVISOR

I declare that this is my own work, and this dissertation does not incorporate without acknowledgement any material previously submitted for a Degree or Diploma in any other University or institute of higher learning and to the best of my knowledge and belief it does not contain any material previously published or written by another person except where the acknowledgement is made in the text.

Also, I hereby grant to University of Moratuwa the non-exclusive right to reproduce and distribute my thesis/dissertation, in whole or in part in print, electronic or other medium. I retain the right to use this content in whole or part in future works (such as articles or books).

Signature: UOM Verified Signature Date: 24-03-2021

The above candidate has carried out research for the Masters Dissertation under my supervision.

Name of the supervisor: Dr C.D. Gamage

Signature of the supervisor: Date: 24-03-2021

Abstract

Information security is becoming more and more critical for data and information. Network security plays a major role in securing the data and systems from Cyber adversaries. It is crucial to detect the dangers actively and implement defences to protect network infrastructure from Cyber-attackers. In this project, we have introduced a way to optimise the threat detection capabilities using Zeek Network Security Monitor and Weka machine learning application. In fact, we have performed a comprehensive study on the evolution of Intrusion Detection Systems (IDS) using the past literature and identified the factors that contributed to both improved performance and limitations in threat detection. We have designed and developed a Network Security Monitoring (NSM) system prototype using Zeek NSM, Elasticsearch, Filebeat and Kibana Stack(EFK stack) and Weka application.

Moreover, our prototype actively performs network surveillance and alerts the user in an event of intrusion. Finally, we have performed a passive machine learning analysis using Random Forrest, K-Nearest Neighbors and Naïve Bayes classifiers on Denial of Service, Reconnaissance and Worm attacks. We have used a sample set of data from the UNSW-NB15 data set for the machine learning analysis activities.

Installation and configuration of open-source applications are not always straightforward, and they could be swamped with cumbersome processes. We have provided foolproof, stepwise guidance to perform the installation and configure of the Zeek and EFK stack at the end of this thesis.

The authors main objective is to design and develop user-friendly security solutions for threat detection using open-source applications. This project is the initial step to achieve that objective.

Keywords: Network Security, NIDS, Zeek NSM, Weka

DEDICATION

I dedicate this work to all my teachers, lecturers and mentors who taught me not to give up when life is challenging and encourage me to be at my best. May they live a long and healthy life!

ACKNOWLEDGEMENTS

I would like to express my sincere gratitude to all those who contributed to carry out this study and make this project a success.

Firstly, I would like to thank my research supervisor Dr C.D. Gamage for giving me valuable advice, guidance, and suggestions to carry out this study.

Secondly, I would like to thank my parents, Ms Vindya Munaweera, Mr Duleep Nakandala, Mr Damsenevi Gurudeniya and my MSc. batchmate Mr Pansilu Pitigalaarachchi who encouraged me and supported me in numerous ways for the whole duration of this project to make this study a reality.

Next, I would like to thank my office colleagues at HSBC Data Processing Lanka (Pvt.) Ltd for all the support and advice given to me to accomplish this project. I would like to mention Mr Kasun Attanayake, Mr Chathura Yatawatte, Mr Lasantha Dasanayaka, Mr Yashodharan Sinnathamby, Mr Hamada Packeer, Mr Richard Baines, Mr Gavin Hawkins, and Mr Colin Fawkes for supporting me in my higher educational activities.

Finally, I would like to thank the Zeek open-source community for being the helping-hand when I needed it the most. I should mention and thank Dr Vern Paxson, Mr Yacin Nadji and Mr Pierre Gaulon for all the advice they provided me through the virtual space.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS

DoS	Denial-of-service
EFK	Elasticsearch, Filebeat, Kibana
ELK	Elasticsearch, Logstash, Kibana
HIDS	Host-based Intrusion Detection System
IDS	Intrusion Detection System
IP	Internet Protocol
KNN	K-Nearest Neighbor Algorithm
ML	Machine Learning
NIDS	Network-based Intrusion Detection System
NSM	Network Security Monitor
TCP	Transmission Control Protocol
TSV	Tab-separated Values
WEKA	Waikato Environment for Knowledge Analysis
.arff	Attribute-Relation File Format
.csv	Comma-separated values Format
.pcap	Packet Capture Format

LIST OF APPENDICES