Network Intrusion Prevention System Based on Enhanced Snort Rules to Protect Network Resources from DoS & DDoS Attacks (An Empirical Approach)

G.R.C. Kumara

139193P

Dissertation submitted to the Faculty of Information Technology,
The University of Moratuwa, Sri Lanka for the partial fulfilment of the requirements of the Degree of Master of Science in Information Technology.

March 2021

Declaration

I declare that this dissertation is my work and has not been submitted in any form for another degree or diploma at any university or other institution of tertiary education. Information derived from the published or unpublished work of others has been acknowledged in the text and a list of references is given.

Name of Student

Signature of Student (s)

Date:

Supervised by

Name of Supervisor (s)

Signature of Supervisor (s)

Date:

Dedicated to

my parents, my teachers

Acknowledgement

I would like to thank and gratitude the individuals for their contribution and motivation in various ways to make this research project a success.

First of all, I would like to express my gratitude to Dr C.R.J. Amalraj, my Supervisor, for his guidance, encouragement, tact, guidance, mature and intelligent advice, suggestions, positive thoughts and optimistic encouragement to continue to make this project a success. The supervisor also helped me to succeed in my future career as well as academics by encouraging me to overcome difficulties. I was lucky enough to do this research project under his supervision.

As well I am deeply grateful to senior lecturers Mr Saminda C. Premarathna and Mr Chaman P. Wijesiriwardhana for their support and continuous help to succeed in this endeavour.

Further, I would like to offer my special thanks to the senior lecturer of the faculty Mr B.H. Sudantha for his continuous support of the success of the project work.

I gratefully acknowledge Dr Lochandaka Ranatunga for initiating a research project and giving a more effective start on the path to success.

Again, I am also in debt too to the evaluators of the interim presentation of this project, Mr D.K. Withanage, Mr S.C. Premarathne, and Mr B.H. Sudantha for their valuable advice and comments to improve my work.

I am indebted to Mr D.K. Withanage, Mr S.C. Premaratne and Mr B.H. Sudantha, the Interim Project Evaluators, for their advice and suggestions on how to drive the research a success.

Also, I am once again indebted to the final evaluator's Dr C.R.J Amalraj, Mr B.H Sudantha and Dr T. G. I. Fernando of the project for their valuable advice in making the dissertation successful and correcting the shortcomings of the research project.

I would like to offer my special thanks to Professor Asoka Karunanada who taught us the "Research Methodology" subject for this master program on behalf of his guidance and motivations to research thinking and handling.

Furthermore, I would like to extend my sincere thanks to other academic staff, academic support and none academic staff members, those who support me in many ways in the IT faculty, UoM.

Again, I should grateful for Prof. Asoka Karunananda our teacher in "*Literature review & Thesis Writing"* who guided us for better researching and dissertation writing.

I would specially thank Mr Saminda Premaratne the course coordinator, MScIT, UoM for his encouragement and advice on this project.

Furthermore, I would like to extend my sincere thanks to my former director-general Prof. Kapila C.K. Perera who directed me to this M.Sc. program in the Faculty of IT, University of Moratuwa and my present director-general Dr W. Hilary E. Silva for always encouraging academic staff towards the research culture in Sri Lanka Institute of Advanced Technological Education (SLIATE). Further, I would be thankful to the director -Eng. Mr N.K.A. Rupasinghe, staff members and students in my institute, ATI Galle for being patient on my busy schedule. In addition, I would like to specially acknowledge the financial assistance offered by the HETC Project, Ministry of Higher Education.

I am grateful to my wife Manoja for her unwavering support in this endeavour and her patience and support and for the loving son Manula, who lost my attention and love during this period. Moreover, I would like to thank my friends and colleagues in the master program who encouraged me with their ideas and experiences to complete the project.

Finally, I would like to express my gratitude to the authors of the most important scholarly works that have been adopted for this research project. Here, Prof Buchanan B., Flandrin F., Richard Macfarlane, Dr Jamie Graves from Edinburgh Napier University are majors for utilizing their methodology to evaluate rate-based IPS in this research work and I am much graceful to them for their contribution to academia.

Finally, in the face of this scientifically significant research project and dissertation, I thank and thank all the gods who have given me unwavering courage, strength, and guidance.

Abstract

Virtual computers from anywhere in the world are designed to enable any user to access the computer resources contained in the cloud computing (CC) environment. The flour resources in the cloud environment, which pose a great threat to security, are shared so that they can be accessed by users anywhere in the world. Denial of service and denial of distributed services is one of the leading challenges posed by attackers who pose a serious threat to CC's security. Next Generation Invasion Prevention Systems (NGIPS), also known as non-traditional invasion prevention systems or next-generation invasion prevention systems, is being introduced as a tactic to overcome these offensive challenges. Thus, the author intends to find research results on the technological strategies used in NIPS and their evaluation and to find solutions to the challenges of cloud computing (CC).

The author has used a very systematic literature review to explore and identify the latest NIPS techniques using Inspec, IEEE, ACM Digital Library, Wiley, Scopus and Google scholar library databases. Articles are selected based on the acceptance and rejection formula when selecting for literature review. This experimental methodology has been selected as a research methodology for experimental comparison of the source and destination approaches of Snort NIGPS. The experimental bed is designed and deployed using Snort filtering techniques deployed in a virtual machine through a virtual switch in a virtual environment.

In this research, the author involves in finding the answers to the research problems and the first problem was the use of next-generation IPS technologies to protect the cloud computing surrounding from DoS and DDoS attacks. The second and third research questions are identifying different types of measurements to assess the performance of NIPS, and the third is the find the performance skill among both source and destination approaches of Snort Intrusion prevention systems.

Network engineers, network administrators and academia has been considered as users of the research scope. The hypothesis in this research is the filter will never work if the attack is launched on a large number of source IP addresses, and Snort will not be able to distinguish between legal and non-legal packets, even if the filter is functional. Finally, the null hypothesis used is the Snort does not show any difference between both source and destination approaches.

TCP, UDP, HTTP and mixture of the protocols used as attack input using LOIC attack tool and legitimate traffic inputs to the system generated using JMeter tool and Further, TCPreplay has been used to regenerate the same amount of both attack and normal traffic to maintain the justification and all those considered as independent variables. The dependent variables considered as the output of the research results are load on the CPU results, Utilization of the memory, availability of the Bandwidth, Delay (Latency), percentage (rate) of loss of packets.

In this research, the processes are the generating of both normal and attack traffics, detecting and preventing malicious traffic using Snort rate filtering rules. In the source approach, packet-based identification and filtering of packets are done by scanning the source IP address and enabling Snort to activate the filter if a specific packet rate is reached. Destination detection and filtering of packets are done by ordering Snort to swipe packets to the destination IP address and to enable filtering when a predetermined packet rate is reached.

NIPS strategic algorithms can be evaluated using classical metrics such as Load of the CPU, Utilization of Memory, Bandwidth availability, Delay (Latency), Rate of packet loss (both “false positives” and “false negatives”) and Accuracy. This experiment also found that when accessing parameters such as Load of the CPU, Utilization of Memory, Bandwidth availability, Delay (Latency) and Rate of packet loss, destination access was more efficient than source access. That is, the filtration rate system of the destination approach is more efficient.

Most of the NIPS technologies used in the Cloud Computing environment to protect from DoS and DDoS attacks are concluded as similar and interrelated. Furthermore, the author concludes that there is a difference in performance appraisal in the cloud computing environment between Snort's source and destination approaches.

Table of Contents

List of Figures

List of Tables

ACRONYMS

CC : Cloud Computing

PaaS : Platform as a service

SaaS : Software as a Service

IaaS : Infrastructure as a Service

DoS : Denial of Service

DDoS : Distributed Denial of Service

IPS : Intrusion Prevention Systems

IDPS : Intrusion Detection Prevention Systems

NGIPS : Non-Traditional Intrusion Prevention Systems

TIPS : Traditional Intrusion Prevention Systems

CSP : Cloud service providers

DC : Data Center

MITM : Man in The Middle Attack

NGIPS : Next-Generation Intrusion Prevention Systems

ICMP : Internet Control Message Protocol

TCP : Transmission Control Protocol

UDP : User Datagram Protocol

HTTP : Hypertext Transfer Protocol

LOIC : Low Orbit Ion Canon

GUI : Graphical User Interface

RTT : Round Trip Time

PRS : Packet Resonance Strategy