DETECTING SYN FLOOD ATTACK WITH SNORT IDS THROUGH SIGNATURE-BASED DETECTION AND ITS IMPACT ON NETWORK PERFORMANCE

ABDO SAIF ABDO DARGAN

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL: DETECTING SYN FLOOD ATTACK WITH SNORT IDS THROUGH SIGNATURE-BASED DETECTION AND ITS IMPACT ON NETWORK PERFORMANCE

SESI PENGAJIAN: 2022 / 2023

Saya: ABDO SAIF ABDO DARGAN

mengaku membenarkan tesis Projek Sarjana Muda ini disimpan di Perpustakaan Universiti Teknikal Malaysia Melaka dengan syarat-syarat kegunaan seperti berikut:

1. Tesis dan projek adalah hakmilik Universiti Teknikal Malaysia Melaka.
2. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan unituk tujuan pengajian sahaja.
3. Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. * Sila tandakan (✓)

______	SULIT	(Mengandungi maklumat yang berdarjah keselamatan atau kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972)
______	TERHAD	(Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi / badan di mana penyelidikan dijalankan)
___✓___	TIDAK TERHAD	

DR. ZAHEERA ZAINAL ABIDIN
Pensyarah Kanan
Fakulti Teknologi Maklumat Dan Komunikasi (FTMK)
Universiti Teknikal Malaysia Melaka (UTeM)

(TANDATANGAN PELAJAR)

(TANDATANGAN PENYELIA)

Alamat tetap: H-1-5, Taman Pelangi Apartment, Ayer Keroh, Melaka.

DR ZAHEERA BINTI ZAINAL ABIDIN
Nama Penyelia

Tarikh: 25 JUNE 2023

Tarikh: 18/09/2023

CATATAN: * Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

DETECTING SYN FLOOD ATTACK WITH SNORT IDS THROUGH SIGNATURE-BASED DETECTION AND ITS IMPACT ON NETWORK PERFORMANCE

ABDO SAIF ABDO DARGAN

This report is submitted in partial fulfilment of the requirements for the
Bachelor of Computer Science (Computer Security) with Honours.

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2023

DECLARATION

I hereby declare that this project report entitled

DETECTING SYN FLOOD ATTACK WITH SNORT IDS THROUGH SIGNATURE-BASED DETECTION AND ITS IMPACT ON NETWORK PERFORMANCE

is written by me and is my own effort and that no part has been plagiarized without citations.

STUDENT : Date : 25 JUNE 2023

(ABDO SAIF ABDO DARGAN)

I hereby declare that I have read this project report and found this project report is sufficient in term of the scope and quality for the award of Bachelor of Computer Science (Computer Security) with Honours.

SUPERVISOR : Date : 18/09/2023

(DR ZAHEERA BINTI ZAINAL ABIDIN)

DEDICATION

To my beloved parents, close friends, and encouraging family members, I want to thank everyone and dedicate my final project to you in this joyful moment. Your ongoing support and encouragement have been important to my achievement. To my parents, thank you for your love and sacrifices shaping me into who I am today. Your belief in my abilities has guided me throughout my academic journey.

To my friends, your unwavering faith in me has motivated me during challenging times. Your encouragement and shared experiences have made this journey memorable. To my relatives, thank you for your support and words of wisdom. Your belief in my potential has fueled my determination. This project reflects the love, support, and guidance I have received from each of you. I am grateful for your contributions to my success.

ACKNOWLEDGEMENTS

First and foremost, I express my deepest gratitude to Allah, the Most Merciful and the Most Gracious, for granting me strength, knowledge, and guidance throughout this journey. Alhamdulillah, all praise be to Allah for His blessings and for making this achievement possible.

I would also like to thank my dear supervisor, Dr. Zaheera Binti Zainal Abidin, for her enormous support, guidance, and supervision. Her knowledge, commitment, and support were invaluable in guiding my study process and deepening my knowledge of the project. I sincerely appreciate her encouragement and the faith she showed in me.

ABSTRACT

This project is known as Detecting SYN Flood Attack with Snort IDS Through Signature-Based Detection and Its Impact on Network Performance. As reported by cybersecurity news, the SYN flood attack has been one of the top 10 attacks in 2022. this project intends to Provide insight for network security practitioners in developing more robust and effective network security mechanisms that can detect and prevent SYN flood attacks, ensuring the stability and availability of network services. In this research, multiple tools have been used to serve the purpose of the research; the tools are hping3 in the Kali Linux to imitate the SYN flood attack, and the SNORT IDS was used to detect the presence of SYN flood attack in the network. Lastly, Wireshark has been used to analyze the impact of the SYN flood attack on the network performance. The primary purpose of this research is To detect the SYN flood attacks using Snort IDS signature-based detection, to analyze the impact of the SYN flood attack on the network performance, and to study the effectiveness of this approach in detecting the attack and analyzing the impact on network performance order to major the successfulness of the proposed research few matric measurements have been taking to consideration such as throughput, latency, package loss and bandwidth consumption.

ABSTRAK

Projek ini dikenali sebagai *Detecting SYN Flood Attack With Snort IDS Through Signature-Based Detection and Its Impact On Network Performance*. Seperti yang dilaporkan oleh berita keselamatan siber, serangan *SYN flood* merupakan salah satu daripada 10 serangan teratas pada tahun 2022. Projek ini bertujuan untuk memberikan panduan kepada para pengamal keselamatan rangkaian dalam membangunkan mekanisme keselamatan rangkaian yang lebih kukuh dan berkesan untuk mengesan dan mencegah serangan *SYN flood*, serta memastikan kestabilan dan ketersediaan perkhidmatan rangkaian. Dalam penyelidikan ini, beberapa alat telah digunakan untuk mencapai tujuan penyelidikan, iaitu hping3 dalam Kali Linux untuk meniru serangan *SYN flood*, SNORT IDS digunakan untuk mengesan kehadiran serangan *SYN flood* dalam rangkaian. Terakhir, Wireshark digunakan untuk menganalisis kesan serangan *SYN flood* terhadap prestasi rangkaian. Tujuan utama penyelidikan ini adalah untuk mengesan serangan *SYN flood* menggunakan pengesanan berdasarkan tandatangan Snort IDS, menganalisis kesan serangan *SYN flood* terhadap prestasi rangkaian, dan mengkaji keberkesanan pendekatan ini dalam mengesan serangan serta menganalisis kesan terhadap prestasi rangkaian. Untuk mengukur keberjayaan penyelidikan yang dicadangkan, beberapa metrik pengukuran telah diambil kira, seperti jumlah aliran data, waktu lewat, kehilangan pakej, dan penggunaan jalur lebar.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

IDS	-	Intrusion Detection System
IP	-	Internet Protocol
PC	-	Personal Computer
SYN	-	Synchronization
SFADBE	-	SYN Flood Attack Detection Based on Bayes Estimator
MANET	-	Mobile Ad-hoc Networks
PC	-	Advanced Encryption Standard
DOS	-	Denial of Services
HTTP	-	Hypertext Transfer Protocol
AR	-	Auto-Regressive
CH	-	Cluster Head
LSTM	-	Long-Short-Term-memory
MST	-	MeanSquare Error
IOT	-	Internet of Things
TCP	-	Transmission Control Protocol
MDFA	-	Multifractal Detrended Fluctuation Analysis
RMS	-	Root-Mean-Square
CLDAP	-	Connectionless Lightweight Directory Access Protocol

CHAPTER 1: INTRODUCTION

With the growing reliance on technology and the internet, network infrastructure security has emerged as a critical concern. Denial of service (DOS) attacks are among the most common threats to network security because they can make a server or network service unavailable to legitimate users by flooding it with requests. SYN floodattacks are particularly challenging to detect among the various DOS attacks.

As reported by cybersecuritynews.com, SYN flood attacks are among the top 10attacks likely to occur in 2023. The potential impact of these attacks can be severe, with the cost of downtime and lost productivity ranging from hundreds to millions of dollars. Therefore, it is crucial to have effective detection and analysis mechanisms inplace to mitigate the impact of SYN flood attacks.

This research project explores Snort IDS's real-time effectiveness in detecting SYN flood attacks and assessing their impact on network performance. The research will contribute to developing more robust and effective network security mechanisms that can detect and prevent SYN flood attacks, ensuring the stability and availability of network services.

1.1 Problem Statement

According to cybersecuritynews.com, the SYN flood attack is one of the top10 dangers likely to happen that can target any operation related to the internet (tushar subhra dutta, 2022)

Table 1.1: Summary of problem statement

PS	Problem statement
PS1	A common attack likely to occur is a SYN flood attack that disrupts legitimate traffic by consuming all server resources, rendering the server inaccessible.

1.2 Project Question

Project questions are specific, focused inquiries that help guide a projecttowards a successful outcome.

Table 1.2: Summary of project questions

PS	PQ	Project question
PS1	PQ1	How to detect the SYN flood attack?
	PQ2	What is the impact of the SYN flood attack on the network performance?
	PQ3	How effective is Snort IDS-real-time in detecting the SYN flood attack and towards the security of overall performance?

1.3 Project Objective

The following are the outcomes that will be produced and presented by the end of the project:

Table 1.3: Summary of project objectives

PS	PQ	PO	Project Objectives
PS1	PQ1	PO1	To detect the SYN flood attacks using Snort IDS real-time analysis.
	PQ2	PO2	To analyze the impact of the SYN flood attack on the network performance.
	PQ3	PO3	To study the effectiveness of this approach in detecting the attack and analyzing the impact on network performance.

1.4 Project Scope

The goals of this study are:

1.4.1 SYN Flood Attack

SYN flood attack has been one of the most dangerous attacks in 2022, according to cybersecuritynews.com. This attack is likely to happen where the attacker exploits the vulnerabilities of the open port, particularly port 80, which is used for Hypertext Transfer Protocol (HTTP). The attacker will send a large number of packets or a flood of SYN requests to the server in a period of time that finally leads to the disruption of services. In this research project, the further detection of the SYN flood attack approach is adopted through signature-based detection utilizing the SNORT IDS tools that will monitor the network traffic in real-time. Finally, the study of its impact on the network performance is also performed.

1.4.2 Snort IDS

Snort IDS is a free, open-source network intrusion detection system capable of real-time traffic analysis and packet logging. The Snort IDS define the malicious network activity based on rules. Besides that, it uses those rules to find the matches against them and generates alerts for users. The rules are customizable based on the requirements of the security policies. In this research project, the rule is set to detect the specific type of well-known SYN flood attack. Other than that, the effectiveness of the Snort IDS in detecting this specific attack is also evaluated.

1.4.3 Metric Measurement

In order to study the impact of SYN flood attack on network performance, several metric measurements have been selected, such as throughput, latency, packet loss and bandwidth consumption. The measurement of these metrics during the attack will be recorded and compared with the measurement before the attack. From this measurement, this impact on the network performance can be seen.

1.4.4 Simulation and Analysis

In this project, the SYN flood attack is simulated using HPing3 tools. The SNORT IDS will then detect the attack, where its rule has been customized and set to detect the presence of this attack. Once it is successfully detected, the Snort IDS will generate the alert and log the event in the log record as a future reference. The result gained from this attack simulation is then analyzed to study its impact on the network performance during the attack. The analysis that has been done will provide insight to the professional security practitioner in developing robust security mechanisms to mitigate this impact.

1.5 Project Contribution

By the time the project is completed, this analysis project will contribute to the following:

i. The accuracy in detecting the SYN flood attack.

By conducting the simulation and analyzing the collected data, the detection accuracy of SNORT IDS, false positive and false negative rates, and the response time of SNORT IDS are assessed in detecting the SYN flood attack and generating the alert in the event of an attack. This assessment contributes to identifying SNORT IDS's effectiveness in detecting SYN flood attacks.

ii. Provide insight for network security practitioners.

This project analysis contributes to developing more robust and effective network security mechanisms that can detect and prevent SYN flood attacks, ensuring the stability and availability of network services.

Table 1.4: Summary of project contribution

PS	PQ	PO	PC	Project Contributions
PS$_1$	PQ$_1$	PO$_1$	PC$_1$	The accuracy in detecting the SYN flood attack.
	PQ$_2$	PO$_2$	PC$_2$	Provide insight for network security practitioners in developing more robust and effective network security mechanisms that can detect and prevent SYN flood attacks, ensuring the stability and availability of network services.
	PQ$_3$	PO$_3$		

1.6 Report Organization

1.6.1 Chapter 1: Introduction

This chapter provided a quick overview of the project, project's background, problem statement, project questions, objectives, scopes, and contribution are all covered in this chapter.

1.6.2 Chapter 2: Literature Review

This chapter gives an overview of the literature review of previously published works on the domain of the research scope. It incorporates the findings of earlier studies. The data is collected from previously published articles, websites, and reports.

1.6.3 Chapter 3: Methodology

This chapter discusses the chosen project methodology, which is the agile model. Each of the phases from the model is well explained in detail. Next, the project milestone is also included as it is used to track progress toward the goals.

1.6.4 Chapter 4: Design

This chapter will describe the overall project, project architecture, network system architecture, logical and physical design, possible scenarios and metric measurement.

1.6.5 Chapter 5: Implementation

This chapter will install and set up the environment for testing and explain the parameters, variables, and assumptions used in the project.

1.6.6 Chapter 6: Testing

This chapter will describe the activity involved in the implementation phase of the simulation project.

1.6.7 Chapter 7: Conclusion

This chapter is going to Describe how the objective has been achieved. Introduction, summarization, contribution, project limitation, and futureworks.

1.7 Conclusion

In conclusion, SYN flood attacks are a significant threat to network security, and their potential impact on network performance can be severe. This research project explores the effectiveness of Snort IDS- real-time traffic analysis in detecting SYN flood attacks and assessing their impact on network performance. The project objectives include detecting SYN flood attacks, analyzing their impact on network performance, and evaluating the effectiveness of Snort IDS in real time. The project will collect network traffic data, stream it to Snort IDS, implement a SYNflood detection rule, and monitor network performance using Wireshark's monitoringtools. The project's contribution includes detecting SYN flood attacks and analyzing their impact on network performance, which can help network administrators and security professionals develop more robust defence strategies.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter will discuss the literature review and related work on this topic. Next, the list of related cases is also described in this chapter. Additionally, we will critically evaluate the strengths and weaknesses of the existing literature and highlight potential avenues for future research. This chapter serves as an essential foundation for the subsequent chapters of this research work.

2.2 Related Work

2.2.1 Snort IDS Application

Snort is a database that generates rules based on different suspicious attacks. Snort distribution uses a collection of rules that can include well-known attacks like buffer overflow and exploit dissemination. If Snort has flaws or deficiencies, they will be added to the rules in creating a Snort-based network detection and monitoring system. Snort distribution uses a set of rules that can detect and prevent threats. The Snort distribution is obtained by extracting a rule from the header assault and then collecting a rule that can close attacks or distribute exploits. Snort rules will be added to Snort if anything suspicious is discovered. The detection is compiled into rules and saved in a database Karmadenur and Raka Yusuf (2019a). Snort can be used to track the traffic entering and leaving a network. It willcontinuously monitor traffic and notify users when it finds potentially harmful packetsor threats on Internet Protocol (IP) networks.

2.2.2 Signature-based IDS

The Snort Intrusion Detection System (IDS) analyses network traffic using predefined rules known as "signatures" to detect possible attacks or suspicious activities. These signatures are simply data patterns or sequences that have been linked to specific attacks or security threats, and it is often stored in the form of rule files. On Linux systems, the rule files are default kept in the /etc/Snort/rules/directory.

When Snort receives network traffic, it examines the packet payload and header data for matches to its signature database. The signature database stores information regarding known attacks, such as network protocols, packet contents, and other characteristics associated with each attack. In this research project, the list of the rules file in Snort that has been used is as listed in the table below:

Table 2.1: Type of Snort rule files

Rule Files	Function
Snort.conf	This is the main configuration file for Snort that specifies the location of other rule files.
Snort.rules	This file contains a set of rules covering a wide range of known attacks and threats.
Local.rules	This file is meant for custom rules the user creates to address specific security requirements.

2.2.3 Real-time Monitoring

Real-time monitoring is the procedure of gathering, analyzing, and presenting data about a system or process as it occurs. It enables fast decision-making and reaction to change situations. Real-time monitoring systems use software tools to collect data from the monitored system or environment. The data collected is subsequently transferred, analyzed, and displayed in real-time to offer accurate information. Real-time monitoring can help in the early discovery of problems, preventing serious harm and downtime and saving time and money. Other than that, better decision-making: Real-time monitoring gives up-to-date information on the monitored system or process, allowing for improved operational decisions.