INTRUSION DETECTION SYSTEM ALERTING SYSTEM USING RASPBERRY PI

SITI NOR DIANA BINTI MAISITA

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGESAHAN STATUS LAPORAN

JUDUL:INTRUSION DETECTION SYSTEM ALERTING SYSTEM USING RASPBERRY PI

SESI PENGAJIAN: 2020/ 2021

Saya: SITI NOR DIANA BINTI MAISITA

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 untuk 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

(TANDATANGAN PELAJAR)

Alamat tetap: No 30 Blok F1 Felda Jengka 7, 26410 Bandar Jengka, Pahang

Tarikh: 15 September 2021

(TANDATANGAN PENYELIA)

DR NUR FADZILAH BINTI OTHMAN

Nama Penyelia

Tarikh: 15 September 2021

INTRUSION DETECTION SYSTEM ALERTING SYSTEM USING RASPBERRY PI

SITI NOR DIANA BINTI MAISITA

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

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2021

DECLARATION

I hereby declare that this project report entitled

INTRUSION DETECTION SYSTEM ALERTING SYSTEM USING RASPBERRY PI

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

STUDENT : SITI NOR DIANA BINTI MAISITA Date : 15 September 2021

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 : Dr. NUR FADZILAH BINTI OTHMAN Date : 15 September 2021

DEDICATION

One and only one,
Thank you to our Almighty god Allah s.w.t to give me strength and idea on doing this project.

To my soul Mom and Dad,
Thank you always be there for me, fulfill my needs and always pray my best in this journey.
Thank you for believing me to go through this meaningful journey.
I hope both of you would proud of me.
I hope this will give meaningful gift as my successful battle in this journey.

To my lovely Supervisor,
Thank you for guide and encourage me to finish my final year project.
Thank you for spending your precious time and energy to give me the direction to finish this project.

Last but not least,
To all my friend who are with me on doing this project,
Thank you for giving me some idea when I am stuck and give some motivation when I lack spirit.
I hope we can achieve our dream together.

Thank you, I really appreciate it.
Love.

ACKNOWLEDGEMENTS

Most importantly, I might want to say thank a ton to our Almighty god Allah S.W.T that consistently with me when I was glad and battle. I truly appreciate for strength that given to finish and complete my last year project. Other than that, Thank Allah S.W.T show the way to aiding me a long excursion in my life as understudy.

An extraordinary appreciation will be given to my lovely supervisor Dr Fadzilah who has been giving a lot of direction in carrying out this task. Dr Fadzilah likewise gave me direction, consolation, and coordination all through my last task. I am grateful that Dr Fadzilah will forfeit time and energy in controlling me during the trouble of finishing this undertaking and giving advice and comment to make improvement in this ideal report.

I might want to thank all my lovely friends and lecturer who have never been debilitate and upheld as long as I am in UTeM. Furthermore, mother and father consistently care about me by giving all my adapting needs even though they are getting more established. I am the youngest child attempting to achieve their hope where they want to see their child succeed graduate as a degree student.

Finally, I want to thank the University of Technology Malaysia Melaka (UTeM) which gives a stage to creating and improving my abilities in the web climate of innovation. Also, remember to the personnel at the Faculty of Information Technology (FTMK) who sharpened their understudies' abilities without griping. I implore that Allah S.W.T will favour the prescribed procedures they have committed and make UTeM a focal point of greatness for Graduate.

ABSTRACT

Due to worldwide proliferation and rapid progress in Information Technology (IT), networking is the crucial state where everybody is using the network including the small business, office or home also affected. Statistic of cybersecurity cases has been rising to 82.5% during the MCO. 82% cases have been receiving reported from the home user and other. This a big value compared to the last year. This is because due to increasing use of technology during the Covid-19 pandemic. So, they need to secure their network to make sure all the data that has been stored in their personal computer are fully safe from any threat especially port scanning threat. This purpose of study to minimize risk getting attack by detecting port scanning threat. In this project, Snort, Barnyard2, and Telegram has been implemented. Raspberry Pi 3 Model B has been used for developing this system. If home user implementing this project, it can minimize chances getting network breach since all the alerts will be send to the user mobile phone in real time. User can take fast action to prevent the network. Moreover, user also can monitor the current packet incoming by viewing in the webpage. They can analyze number of packets. Hopefully, this project will give a better future although it does not eliminate all the cybercrime cases, but it will minimize the risk getting attack.

ABSTRAK

Oleh kerana penyebaran di seluruh dunia dan kemajuan pesat dalam Teknologi Maklumat (IT), jaringan adalah keadaan penting di mana semua orang menggunakan rangkaian termasuk perniagaan kecil, pejabat atau rumah juga terjejas. Statistik kes keselamatan siber meningkat kepada 82.5% semasa MCO. 82% kes telah diterima dilaporkan dari pengguna rumah dan lain-lain. Ini nilai yang besar berbanding tahun lalu. Ini kerana peningkatan penggunaan teknologi semasa pandemi Covid-19. Oleh itu, mereka perlu mengamankan rangkaian mereka untuk memastikan semua data yang telah disimpan di komputer peribadi mereka selamat sepenuhnya dari sebarang ancaman terutama ancaman pengimbasan port. Tujuan kajian ini untuk meminimumkan risiko mendapat serangan dengan mengesan ancaman pengimbasan pelabuhan. Dalam projek ini, Snort, Barnyard2, dan Telegram telah dilaksanakan. Raspberry Pi 3 Model B telah digunakan untuk mengembangkan sistem ini. Sekiranya pengguna rumah melaksanakan projek ini, ia dapat meminimumkan kemungkinan terjadinya pelanggaran rangkaian kerana semua makluman akan dikirimkan ke ponsel pengguna secara real time. Pengguna boleh mengambil tindakan pantas untuk mengelakkan rangkaian. Selain itu, pengguna juga dapat memantau kemasukan paket semasa dengan melihat di laman web. Mereka dapat menganalisis bilangan paket. Mudah-mudahan, projek ini memberi masa depan yang lebih baik walaupun tidak menghapuskan semua kes jenayah siber, tetapi akan mengurangkan risiko diserang.

TABLE OF CONTENTS

PAGE

DECLARATION ..... **II**

DEDICATION ..... **III**

ACKNOWLEDGEMENTS ..... **IV**

ABSTRACT ..... **V**

ABSTRAK ..... **VI**

TABLE OF CONTENTS ..... **VII**

LIST OF TABLES ..... **XII**

LIST OF FIGURES ..... **XIII**

LIST OF ABBREVIATIONS ..... **XV**

CHAPTER 1: INTRODUCTION **16**

1.1 Introduction 16

1.2 Problem Statement (PS) 18

1.3 Research Question (RQ) 19

1.4 Research Objective (RO) 20

1.5 Project Scope 21

1.6 Project Contribution 21

1.7 Report Organization 22

1.8 Conclusion 23

CHAPTER 2: LITERATURE REVIEW **24**

2.1 Introduction 24

2.2 Theory and Technical Background 25

2.2.1 Intrusion Detection System 25

2.2.1.1 Intrusion Detection Architectural Model 26

2.2.2 Snort 30

2.2.2.1 Snort rules 31

2.2.3 Port scanning 32

2.2.4 Raspberry Pi 32

2.3 Comparison of the Raspberry Pi 34

2.4 Comparison with the existing system 35

2.5 Project Solution 38

2.6 Conclusion 38

CHAPTER 3: PROJECT METHODOLOGY 39

3.1 Introduction 39

3.2 Project Methodology 40

3.3 Project Milestones 43

3.4 Conclusion 45

CHAPTER 4: DESIGN 46

4.1 Introduction 46

4.2 Problem Analysis 47

4.3 Analysis Requirement 48

4.3.1 Data Requirement 48

4.4 Software Requirement 49

4.4.1 Snort 49

4.4.2 Telegram 49
4.4.3 Barnyard2 50
4.5 Hardware Requirement 51
4.5.1 Raspberry Pi 51
4.5.2 Switch 52
4.6 Model Design 52
4.7 Conclusion 54
CHAPTER 5: IMPLEMENTATION 55
5.1 Introduction 55
5.2 Software Development Environment Setup 56
5.2.1 Package Dependent Libraries 56
5.2.2 Data Acquisition (DAQ) 57
5.2.3 Snort 58
5.2.4 Rules 59
5.2.5 Barnyard2 59
5.2.6 Database 59
5.2.7 Telegram 60
5.2.8 Webpage 61
5.3 Implementation Status 63
5.4 Conclusion 64
CHAPTER 6: TESTING 65
6.1 Introduction 65
6.2 Test Plan 66
6.2.1 Test Organization 66
6.2.1.1 Attacker 66

6.2.1.2 User and Administrator 66

6.2.1.3 Network Engineer & System Developer 66

6.2.2 Test Environment 67

6.2.3 Test Schedule 67

6.3 Test Strategy 68

6.3.1 Classes of Test 68

6.3.1.1 Functional Test 68

6.4 Test Design 68

6.4.1 Test Description 69

6.5 Test Result and Analysis 75

6.5.1 Raspberry Pi 3 And Mirroring Switch Connectivity 75

6.5.1.1 Attacker Side 75

6.5.1.2 Server Side 76

6.5.2 Alert To Database Testing 77

6.5.3 System Testing 78

6.5.3.1 Login Testing 78

6.5.3.2 Dashboard Testing 79

6.5.3.3 Add New User Testing 80

6.5.3.4 Threat Show Counter Testing 81

6.5.3.5 Logout Testing 82

6.5.4 Telegram Notification Testing 83

6.5.5 Analysis of Ram Usage When Execute All the Script Needed 84

6.6 Conclusion 85

CHAPTER 7: PROJECT CONCLUSION 86

7.1 Introduction 86

7.2 Project Summarization 87

7.3 Project Contribution 87

7.4 Project Limitation 88

7.5 Future Works 88

7.6 Conclusion 89

REFERENCES 90

APPENDIX A 91

LIST OF TABLES

PAGE

Table 1.1 Problem Statement **18**
Table 1.2 Research Question **19**
Table 1.3 Research Objective **20**
Table 2.1 Comparison between Raspberry Pi **34**
Table 2.2 Comparison Previous Project **35**
Table 5.1 Implementation status **63**
Table 6.1 RPi 3 and Mirroring Switch Connectivity **69**
Table 6.2 System Login Testing **70**
Table 6.3 Add New User Testing **71**
Table 6.4 Logout Testing **72**
Table 6.5 Web Panel **73**
Table 6.6 Telegram Alert **74**

LIST OF FIGURES

PAGE

Figure 2.1 Functions of IDS 26
Figure 2.2 Selective phase in identifying anomaly activities 27
Figure 2.3 Classification of intrusion detection system 28
Figure 2.4 Raspberry Pi 3 Model B 33
Figure 3.1 Flowchart of the project 42
Figure 4.1 Flow System Architecture 47
Figure 4.2 Data Flow of the Project 48
Figure 4.3 Snort Logo 49
Figure 4.4 Bot Father Logo 50
Figure 4.5 Illustration function of Barnyard2 50
Figure 4.6 Raspberry Pi Model 3B 51
Figure 4.7 Tenda Switch 52
Figure 4.8 Design Architecture of the Project 53
Figure 4.9 Real Design 53
Figure 5.1 Software Flow 56
Figure 5.3 Dependency for MySQL Server 56
Figure 5.4 Dependency for library MySQL Client 56
Figure 5.5 Install Auto configure 57
Figure 5.6 Install MySQL client 57
Figure 5.7 Install libraries 57
Figure 5.8 Securing the Database 57
Figure 5.9 Install dependency for database 57
Figure 5.10 Install dependency for database 57
Figure 5.11 Install dependency for database 57
Figure 5.12 Install dependency for database 57
Figure 5.13 DAQ installation 57
Figure 5.14 Missing Dependencies 58

Figure 5.15 Missing Dependencies **58**
Figure 5.16 Snort Missing Dependencies **58**
Figure 5.17 Snort Missing Dependencies **58**
Figure 5.18 Snort Missing Dependencies **58**
Figure 5.19 Dependencies LuaJit **58**
Figure 5.20 Snort configure by enabling sourcefire **58**
Figure 5.21 Snort installation **59**
Figure 5.22 sid message map **59**
Figure 5.23 Barnyard with MySQL **59**
Figure 5.24 Barnyard with snort **59**
Figure 5.25 Database configuration **60**
Figure 5.26 Log count **60**
Figure 5.27 Telegram Identification **61**
Figure 5.28 Webpage Script **62**
Figure 5.29 Database Script **62**
Figure 6.1 Illustrated the test environment **67**
Figure 6.2 Port Scanning **75**
Figure 6.3 Snort Alert Testing **76**
Figure 6.4 Database Testing **77**
Figure 6.5 System Testing **78**
Figure 6.6 Login Testing **78**
Figure 6.7 Dashboard **79**
Figure 6.8 Add New User **80**
Figure 6.9 Successfully Adding New User **81**
Figure 6.10 Threat Show Counter Testing **81**
Figure 6.11 Logout Testing **82**
Figure 6.12 Telegram Alert **83**
Figure 6.13 Size of RAM Without Any Process **84**
Figure 6.14 Size of RAM With Process **84**
Figure 6.15 RAM Usage Comparison **84**

LIST OF ABBREVIATIONS

FYP	-	**Final Year Project**
IDS	-	**Intrusion Detection System**
RPi	-	**Raspberry Pi**
IP address	-	**Internet Protocol Address**
NIDS	-	**Network Intrusion Detection System**
HIDS	-	**Host Intrusion Detection System**
IT	-	**Information Technology**
URL	-	**Uniform Resource Locator**
TCP	-	**Transmission Control Protocol**

CHAPTER 1: INTRODUCTION

1.1 Introduction

Due to worldwide proliferation and rapid progress in Information Technology (IT), networking is the crucial state where everybody is using the network including the small business, office or home also affected. In addition, nowadays, worldwide has been hit with the pandemic Coronavirus or known as Covid19. As the outbreak of coronavirus at the end of 2019 which required humankind to practice a social distancing as a part of prevention step in containing the virus from spreading. As regards to that matter, the government has announced a mandatory lockdown to the entire nation to break the chain of the virus where it prohibits travel in or out from the affected area. Hence, halt the business operation of most of the companies throughout the country. For the sake of business continuity, the management had decided to adopt the concept of telecommuting which enables the worker to work remotely from home. Thus, all the people need to work fully using their own internet. With the rapid proliferation of computer usage and network, security aspect bcame very critical. Especially in network vulnerability such as port scanning is the most common vulnerability in the network. Port scanning is the first step that attacker will take before launch the attack. As an example, the attacker will scan the IP address to check whether that host are alive or not, then the attacker will scan port that has been opened to breach the user's network or do other attack. Port scanning is a method for discovering hosts' flaws by sending port inquiries. An intrusion detection system (IDS) is one of the popular methods that can detect any suspicious activity within a network. Intrusion detection system (IDS) will be functioning as monitoring any traffic that seems suspicious and unusual activities. In other words, it will analyze the behaviors that has

been breach the access control policy that has been set up by administrator. Meanwhile, the user needs to be always aware about the network status either in a safe mode or being threaten. By using alert system, it can help user to minimize the risk.

Currently, the increasing number of attackers make the network became more unsecure for everyone. Nowadays, everybody has a smart phone, computer, laptop, and other gadget that connected to the internet to do the work and social such as using Facebook, WhatsApp, and other application to connected with each other. Internet are very essential to every people nowadays for each level including kids and senior citizens that surely do not have a good knowledge about the security. People will simply use the internet without thinking any destruction that maybe happen. People also will simply put the easy guess password that attacker can easily breach to the network. Then, the innovative people need to solve this kind of problem to minimize the cyber security cases.

1.2 Problem Statement (PS)

Internet has become the highest essential tools in this modern era. Computer networking become more attractive because of the application such as Local Area Network (LAN), Wireless Local Area Network (WLAN) and Wide Area Network (WAN) that is have been uses in various enterprises, security service, health care and other emergency services. Hence, exposure to intrusion activities has been incremented proportionally because of the increasing number of Internet users worldwide. Because of that, some users are willing to spend money to protect the network form a certain threat such as port scanning, however, there always have several people that do not have an enough or a lot of budgets but want to secure the network also. Since the statistic of cybersecurity cases has been rising to 82.5% during the MCO and more than have percent cases have been receiving reported from the home user and other reported by The Star news. Thus, to setup a network detector is costly. Moreover, nowadays many people lose their jobs and have some payroll deductions that make people hard to spend money to this network equipment. Next, most of the people are not have a good knowledge in IT especially in network and command prompt version with other type of OS such Linux OS. Furthermore, the status of the network is unknown because do not have any alert that can send to the user inform about the current status either in safe environments or has been attack. Table 1.1 shows the summarize of the problem statement.

Table 1.1 Problem Statement

PS	Problem Statement
PS1	Costly to setup a network detector to identify port scanning threat.
PS2	Snort log file are non-user friendly to understand.
PS3	Users are not aware that their network has been attack.

1.3 Research Question (RQ)

To solve the problem statement, it needs to come out with research question. The question arose when further intending to get know more about the research. In this development, we need to answer the question before can proceed the progress. The main problem in this project is about the cost, so that how this project could be solved to this problem. Then, how the user who does not have a good knowledge in IT to understand the snort log file, understand what ingoing in their network are. The last question in this study is about the user knowledge if there someone that are tyring to port scanning to their network. This study carries out as the attempt to answer the research questions as follows in Table 1.2.

Table 1.2 Research Question

PS	RQ	Research Question
PS1	RQ1	How to minimize cost to detect the port scanning threat?
PS2	RQ2	How to understand the snort log file?
PS3	RQ3	How user know if their network has been threatened?

This development will be built based on the questions stated above. These questions are valuable in order to develop this project effectively. The questions arise will also be used to accomplish the objectives of this project.

1.4 Research Objective (RO)

Discussing to the project question mentioned previously, there are three objectives that will be used in answering all available questions. The objective will be to make sure that the project is extra structured as proposed. The objective of this project is to implement IDS on raspberry pi since the raspberry pi is affordable. Second objective is user can monitor the number of packets that has been send into their network by monitoring on the website which is user-friendly where user can easily understand. The last objective to achieve is to send the notification alert in Telegram to the user if the rules has been fulfilled. Table 1.3 shows that the summary of research objectives.

Table 1.3 Research Objective

PS	RQ	RO	Project Objective
PS1	RQ1	RO1	Implement IDS on raspberry pi.
PS2	RQ2	RO2	User can monitor and analyze the number of packets that incoming and outgoing into the network by using website.
PS3	RQ3	RO3	User will be receiving the notification in the real time if someone that are trying to port scanning (TCP port) into their network by using Telegram.

1.5 Project Scope

The targeted user for this project will be focused on basic to intermediate level of home user. The project will be driven by Raspberry Pi in making this project and Tenda switch to function as a port mirroring. On a network switch, port mirroring is used to send a duplicate of network packets viewed on one switch port or an entire VLAN to a network monitoring connection on another switch port. It assists administrators in keeping a close check on network performance and notifies them when problems arise. Moreover, Raspbian OS has been used to functioning in this project. Raspberry Pi 3 Model B with 32 GB memory will be use in this project. This project is working by detecting 3 devices and lasting forever if still in the same network. This project also will be detecting for TCP port scanning only.

1.6 Project Contribution

Nowadays, Internet is a complex entity consist of different users, resources, and networks. Today in the mission to ensure all people safe and in a trusted communication in daily usage was very crucial, it is because it need to maintain an intermediary level of security, especially during this pandemic. By implementing this project, it will give the benefit to the basic and intermediate home user. It is because user can easily understand if their network has been attacked because user can monitor by using the website. Moreover, user will be receiving an alert using Telegram. So that user can take any action to prevent their network. User can protect their network with low-cost.

As an attacker the first step to launch any attack they need to know which port are open or the vulnerability from that network. From that, the attacker will start to launch attack to breach the network information. Thus, providing a secure place to every environment in the network is a huge challenging issue. It has become critical since the attackers or intruders are very active to accessing our information over the network.

1.7 Report Organization

Chapter 1: Introduction

In this chapter, it has been discussing about the first planning in doing this project which are project objective, problem statement and project questions. Basically, this is our general information toward this project. Moreover, this chapter also the guide in pointing the main or important information that need to be mark as prior for this project.

Chapter 2: Literature Review

In this chapter, it will be focusing on discovering the previous study or researcher that has been done the similar project, in order to get the useful information on conduct this project. This section also discussing on the general fact that this project will be going. Thus, this section are explaining a first point to this project.

Chapter 3: Project Methodology

This section focuses on the how the methodology or process of the project. It also generally provides the Gantt Chart as the planning to finish this project.

Chapter 4: Design

This part may focus on analyzing the whole discussion over this project assessment with the structural design that was utilized for this project with the help of the need for computer hardware and computer software during the duration of this project.

Chapter 5: Implementation

The test technique will be discussed in detail in Chapter 5 in order to obtain the precision result. The results of this research will be collected to validate that it is comprehensive, and the results will be recorded to generate an assessment, which will then be equated to other methods. Characterize the software nature setup, software