

**RASPBERRY PI DOS ATTACK DETECTOR USING SIGNATURE  
BASED APPROACH FOR IPV6 TUNNELING SECURITY**



**UNIVERSITI TEKNIKAL MALAYSIA MELAKA**

**RASPBERRY PI DOS ATTACK DETECTOR USING SIGNATURE  
BASED APPROACH FOR IPV6 TUNNELING SECURITY**

**IMAM MUKHSINEEN BIN ABU ZAH**



اونيورسيتي تیکنیکل ملیسيا ملاک  
This report is submitted in partial fulfilment of the requirements for the Bachelor  
of Computer Science (Computer Network)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY  
UNIVERSITI TEKNIKAL MALAYSIA MELAKA 2017

**BORANG PENGESAHAN STATUS TESIS\***

JUDUL : RASPBERRY PI DOS ATTACK DETECTOR USING SIGNATURE BASED APPROACH FOR IPV6 TUNNELING SECURITY

SESI PENGAJIAN : 2016/2017

Saya IMAM MUKHSINEEN BIN ABU ZAH  
(HURUF BESAR)

Mengaku membenarkan tesis (PSM/Sarjana/Doktor Falsafah) ini disimpan di Perpustakaan Fakulti Teknologi Maklumat dan Komunikasi 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)

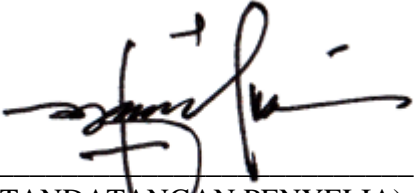
TERHAD (Mengandungi maklumat TERHAD yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan)

TIDAK TERHAD

*Imam Mukhsineen*

(TANDATANGAN PENULIS)

Alamat tetap: No 11, Jalan BB 20, Taman Bachang Baru, 75350, Batu Berendam, Melaka.



(TANDATANGAN PENYELIA)

Dr. NazrulAzhar Bahaman  
Nama Penyelia

Tarikh:

Tarikh: 31/08/2017

CATATAN: \* Tesis dimaksudkan sebagai Laporan Akhir Projek Sarjana Muda (PSM) \*\* Jika tesis ini SULIT atau TERHAD, sila lampirkan surat daripada pihak berkuasa.

## DECLARATION

I hereby declare that this project report entitled

### **RASPBERRY PI DOS ATTACK DETECTOR USING SIGNATURE BASED APPROACH FOR IPV6 TUNNELING SECURITY**

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

STUDENT: \_\_\_\_\_

(IMAM MUKHSINEEN BIN ABU ZAH)

Date: \_\_\_\_\_

31/08/2017

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 Networking) With Honours.

SUPERVISOR: \_\_\_\_\_

(DR. NAZRULAZHAR BAHAMAN)

Date: \_\_\_\_\_

31/08/2017

## DEDICATION

Dear Allah, I devoted my life for Allah and may life is within your guidance. Dear my parents thank you for your sacrifice and love. Dear supervisor thank you for all the knowledge and dear fellow friends especially to my supportive friends' thank you so much for assists and help.



## ACKNOWLEDGEMENTS

Primarily, I would like express full of my sincere gratitude to my supervisor, Dr. NazrulAzhar Bahaman for his guiding me throughout this project, patience and support throughout the year of my Degree study in Universiti Teknikal Malaysia Melaka (UTeM).Also, not forgetting my fellow friends Nuruljannah Binti Abdul Rasid, thank you for your time in guiding, sharing information with me throughout this project and help me constantly whenever I need it the most.Last but not least, I would also like to thank my beloved parents who have been giving me support and motivation throughout my project.



## ABSTRACT

IPv6 transition mechanism was introduced in order to permit hosts on an IPv4 network to communicate with hosts on an IPv6 network, and vice versa. There are vulnerabilities identified in this protocol suite and transition mechanism has been manipulated as a platform to perform threats that exploit those vulnerabilities. Present of attack that are hidden in the transition mechanism tunnel payload are unable to be detected. Hence, it is important to develop tool that can do attack detection through the transition mechanism. This project is about to detecting DoS attack by using Raspberry Pi with signature based approach on IPv6 Tunneling environment. IPv6 Transition Mechanism vulnerabilities currently exist, and as the popularity of the IPv6 protocol increases, so the number of threats does. IPv6 Transition Mechanism exploited as attack medium. This makes tunneling mechanism susceptible to be used in attacks such as DOS attack. The purpose of this project is to identify the possible threats in the transition mechanism. By using signature based approach, this project can show how the transition mechanism is exploited by attacker clearly. This project also produces a prototype that will scan all the network activity inside the transition mechanism to detect any presence of transition mechanism attack. Raspberry Pi is used in this project to send live alerts and notify upon occurrence of attacks. Build a testing method by simulating the attack to test the effectiveness of the proposed prototype in detecting the presence of threats. This project contains planning and analysis, design and implementation phases of the project, and testing. Planning and analysis phase includes the literature review to identify the current problem and make the best solution to overcome the problems. Next, a design and implementation phase of this project is developing a prototype Intrusion Detection System which can detect the attack by the rules that have been set. Lastly, perform the testing by simulate threat detection either successful or not.

## ABSTRAK

Mekanisme peralihan IPv6 diperkenalkan untuk membolehkan tuan rumah pada rangkaian IPv4 untuk berkomunikasi dengan tuan rumah pada rangkaian IPv6, dan sebaliknya. Terdapat kelemahan yang dikenal pasti dalam suite protokol ini dan mekanisme peralihan telah dimanipulasi sebagai platform untuk melaksanakan ancaman yang mengeksploitasi kerentanan tersebut. Hadir serangan yang tersembunyi dalam muatan terowong mekanikal peralihan tidak dapat dikesan. Oleh itu, adalah penting untuk membangunkan alat yang boleh melakukan pengesanan serangan melalui mekanisme peralihan. Projek ini akan mengesan serangan DoS dengan menggunakan Raspberry Pi dengan pendekatan berasaskan tandatangan pada persekitaran Tunneling IPv6. Kerentanan Mekanisme Peralihan IPv6 kini wujud, dan sebagai populariti protokol IPv6 meningkat, maka bilangan ancaman dilakukan. Mekanisme Peralihan IPv6 dieksploitasi sebagai medium serangan. Ini menjadikan mekanisme terowong mudah untuk digunakan dalam serangan seperti serangan DOS. Tujuan projek ini adalah untuk mengenal pasti kemungkinan ancaman dalam mekanisme peralihan. Dengan menggunakan pendekatan berasaskan tandatangan, projek ini dapat menunjukkan bagaimana mekanisme peralihan dimanfaatkan oleh penyerang dengan jelas. Projek ini juga menghasilkan prototaip yang akan mengimbas semua aktiviti rangkaian di dalam mekanisme peralihan untuk mengesan sebarang serangan mekanisme peralihan. Raspberry Pi digunakan dalam projek ini untuk menghantar makluman secara langsung dan memberitahu apabila berlakunya serangan. Bina kaedah ujian dengan mensimulasikan serangan untuk menguji keberkesanan prototaip yang dicadangkan dalam mengesan kehadiran ancaman. Projek ini mengandungi perancangan dan analisis, reka bentuk dan pelaksanaan fasa projek, dan ujian. Fasa perancangan dan analisis termasuk tinjauan literatur untuk mengenal pasti masalah semasa dan membuat penyelesaian terbaik untuk mengatasi masalah. Seterusnya, fasa reka bentuk dan pelaksanaan projek ini adalah membangun satu prototaip Sistem Pengesan Pencerobohan yang dapat mengesan serangan oleh peraturan yang telah ditetapkan. Akhir sekali, lakukan ujian dengan mensimulasikan pengesanan ancaman sama ada berjaya atau tidak.



## TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	i
	DEDICATION	ii
	ACKNOWLEDGEMENTS	iii
	ABSTRACT	iv
	ABSTRAK	v
	TABLE OF CONTENTS	vi
	LIST OF TABLES	x
	LIST OF FIGURES	xi
<b>CHAPTER I</b>	<b>INTRODUCTION</b>	
	1.1 Introduction	1
	1.2 Problem Statement	2
	1.3 Project Question	3
	1.4 Project Objective	4
	1.5 Project Scope	5
	1.6 Project Contribution	5
	1.7 Thesis Organization	6
	1.8 Conclusion	7

<b>CHAPTER II</b>	<b>LITERATURE REVIEW</b>	
2.1	Introduction	8
2.2	Related Work	9
	2.2.1 Internet Protocol Version 6 (IPV6)	9
	2.2.2 DOS Attack	11
	2.2.3 Network Intrusion Detection System (NIDS)	13
	2.2.4 Protocol 41	15
	2.2.5 Transition Mechanism	16
2.3	Critical Review	17
2.4	Proposed Solution	22
2.5	Conclusion	22
<b>CHAPTER III</b>	<b>PROJECT METHODOLOGY</b>	
3.1	Introduction	23
3.2	Project Methodology	23
	3.2.1 Planning Phase	24
	3.2.2 Analysis and Design Phase	25
	3.2.3 Implementation Phase	27
	3.2.4 Testing Phase	28
3.3	Project Milestones	29
	3.3.1 PSM 1 Milestone	29
	3.3.2 Gantt Chart	31
3.4	Conclusion	32
<b>CHAPTER IV</b>	<b>ANALYSIS AND DESIGN</b>	
4.1	Introduction	33
4.2	Problem Analysis	33
4.3	Requirement Analysis	34
	4.3.1 Data Requirement	34
	4.3.2 Functional Requirement	35
	4.3.3 Other Requirement	36

	4.3.3.1 Hardware Requirement	35
	4.3.3.2 Software Requirement	36
4.4	High-Level Design	38
	4.4.1 IPv6 Tested Architecture	38
	4.4.2 Physical and Logical Network Design	39
	4.4.3 Logical Design	40
4.5	Conclusion	40
<b>CHAPTER V</b>	<b>IMPLEMENTATION</b>	
5.1	Introduction	41
5.2	Environment Setup	42
5.3	Attack Signature Identification	44
5.4	Implementation Status	47
5.5	Result	48
5.6	Conclusion	52
<b>CHAPTER VI</b>	<b>TESTING</b>	
6.1	Introduction	53
6.2	Test Plan	53
	6.2.1 Test Organization	53
	6.2.2 Test Environment	54
6.3	Test Strategy	54
	6.3.1 Classes of test	55
6.4	Test Design	56
	6.4.1 Test Description	58
6.5	Conclusion	59
<b>CHAPTER VII</b>	<b>PROJECT CONCLUSION</b>	
7.1	Introduction	60
7.2	Project Summarization	60
7.3	Project Contribution	61
7.4	Project Limitation	61

7.4	Future Works	62
7.6	Conclusion	62

<b>REFERENCES</b>	<b>63</b>
-------------------	-----------



## LIST OF TABLES

<b>TABLE</b>	<b>TITLE</b>	<b>PAGE</b>
1.1	Problem Statement	2
1.2	Summary of Project Question	3
1.3	Summary of Research Objectives	4
1.4	Project Contribution	5
3.1	PSM 1 Milestone	29
3.2	Gantt Chart	31
6.1	Test Organization	54
6.2	Testbed connectivity test	56
6.3	Packet Capture Test	56
6.4	Signature Matching Test	57
6.5	Packet capture and decoding test result	58
6.7	Signature Matching Test Result	59

## LIST OF FIGURES

FIGURE	TITLE	PAGE
2.1	Comparison of IPv4 and IPv6 header	10
2.2	Denial of Service	12
2.3	Network Based IDS	14
2.4	Host Based IDS	15
2.5	Protocol 41 Packet	16
2.6	Tested for intrusion detection mechanism	21
3.1	Methodological Phase	24
4.1	Block Diagram of Attack Detector	34
4.2	Attack Detector Data Flow Diagram	35
4.3	Network System Architecture	38
4.4	Network Physical Design	39
4.5	Logical Network Design	40
5.1	Environment Setup	42
5.2	Environment Setup	42
5.3	Environment Setup Illustration	43
5.4	Denial6 Test Case 2 Packet Capture	44
5.5	Wireshark Snippet of Sendpees6 Attack	45
5.6	Wireshark Snippet During Thcsyn6 Attack	46
5.7	Output Produced by Attack Detector	48
5.8	Output Produced by Attack Detector	49
5.9	Output Produced by Attack Detector	49
5.10	Attack Notification using LED	50

5.11	Attack Notification using LED	50
5.12	Attack Notification using LED	51
5.13	Attack Notification using LED	51
6.1	Black box testing	55



## CHAPTER I

### INTRODUCTION

#### 1.1 Introduction

IPv6 is a short for “Internet Protocol Version 6”, that is the latest version of the Internet Protocol (IP), designed to replace the current IPv4 or known as “Internet Protocol Version 4” due to overcome the shortfall of IPv4 protocol in meeting the demand of growing number of user in the global internet. More users and devices are allowed to communicate on the Internet through this IPv6 by using bigger numbers to create IP addresses. Unfortunately, IPv6 and IPv4 are two completely separate protocols and it is not backward compatible with the existing IPv4 protocol. IPv6 transition mechanism was introduced in order to permit hosts on an IPv4 network to communicate with hosts on an IPv6 network, and vice versa. There are vulnerabilities identified in this protocol suite and transition mechanism has been manipulated as a platform to perform threats that exploit those vulnerabilities. Present of attack that are hidden in the transition mechanism tunnel payload are unable to be detected. Hence, it is important to develop tool that can do attack detection through the transition mechanism.

One of the possible countermeasures for this issue is by using improved intrusion detection system that is capable of encapsulating the tunnel header and checks the packet in the payload. Python is the programming language that can be used to develop the intrusion detection system. Scapy, a packet manipulation utility



for Python helps to process the packets. The deployment of this improved intrusion detection system enable attacks in the tunnel can be detected and necessary actions can be taken.

## 1.2 Problem Statement

The problem that has been identified is summarized in Table 1.1 below

**Table 1.1: Problem Statement**

<b>PS</b>	<b>Problem Statement</b>
<b>PS 1</b>	IPv6 Transition Mechanism has been manipulated as a platform to perform threats that exploit these vulnerabilities

IPv6 Transition Mechanism has been manipulated as a platform to perform threats that exploit these vulnerabilities due to the present of attack that are hidden in the transition mechanism tunnel payload that unable to be detected.

### 1.3 Project Question

The three Project Question (PQ) is constructed based on the problem statement that needs to be answered in this project. The summary of project question is shown in Table 1.2.

**Table 1.2: Summary of Project Questions**

PS	PQ	Project Question
PS1	PQ1	What are the possible threats in the transition mechanism?
	PQ2	How attack detection alert can be notified directly, quickly and urgently?
	PQ3	How to detect the threat effectively?

**PQ1: What are the possible threats in the transition mechanism?**

Identify the characteristics and the signature of the threats that could possibly occur through the implementation of IPv6 transition mechanism.

**PQ2: How attack detection alert can be notified directly, quickly and urgently?**

The method or type of tools to be used to detect the presence of threats or attack.

**PQ3: How to detect the threat effectively?**

The effectiveness of the solution whether it will able to detect the threats during attack with minimal false positive and false negative.

## 1.4 Project Objective

Based on the project questions formulated in previous section, appropriate project objectives (PO) are developed as follows: The Project Objective (PO) is summarized into Table 1.3.

**Table 1.3: Summary of research objectives**

PS	PQ	PO	Project Objective
PS1	PQ1	PO1	To identify the possible threats in the transition mechanism.
	PQ2	PO2	To develop a prototype of NIDS that can live alerts and notify upon occurrence of attacks.
	PQ3	PO3	To test and verify the effectiveness of the prototype

**PO1: To identify the possible threats in the transition mechanism.**

Study on how to identify the signature of the attack and how the transition mechanism is exploited by attacker.

**PO2: To develop a prototype of NIDS that can live alerts and notify upon occurrence of attacks.**

Produce a prototype that will scan all the network activity inside the transition mechanism to detect any presence of transition mechanism attack.

**PO3: To test and verify the effectiveness of the prototype.**

Build a testing method by simulating the attack to test the effectiveness of the prototype in detecting the presence of threats.

## 1.5 Project Scope

The Scope of this research paper will be focusing on the aspects stated below:

1. Threats that exploits in transition mechanism.
2. Intrusion Detection System that detect the presence of threat in IPv6 transition mechanism.
3. Test bed to test the effectiveness of the Intrusion Detection System.

## 1.6 Project Contribution

**Table 1.4: Project Contribution**

PS	PQ	PO	PC	Project Objective
PS1	PQ1	PO1	PC1	Identification of threats and attack in IPv6 transition mechanism.
	PQ2	PO2	PC2	Propose a prototype that will act as a test bed and it is capable to detect attacks.
	PQ3	PO3	PC3	Propose feature selection match that is capable to detect DOS attacks.

## 1.7 Thesis Organization

This report consists of six chapter namely Chapter 1: Background, Chapter 2: Literature Review, Chapter 3: Methodology, Chapter 4: Design and Implementation, Chapter 5: Testing and Result Analysis and Chapter 6: Conclusion.

### Chapter 1: Introduction

This chapter will discuss about introduction, project background, research problem, research question, research objective, scope, project significant and report organization.

### Chapter 2: Literature Review

This chapter will explain related work of this recommendation system, such as standards, type of attacks and transition mechanisms.

### Chapter 3: Methodology

This chapter will explain the methodology used to carry out the project and description of activities carried out during each phase of the methodology.

### Chapter 4: Analysis and Design

This chapter discusses on the analysis on the problem and requirement. Besides this chapter covers the high-level design, user interface design and the system architecture.

## **Chapter 5: Implementation**

This chapter covers the activity involved in the implementation phase, the software development environment setup, software configuration management and the implementation status.

## **Chapter 6: Testing**

This chapter discusses on the activity involved in the testing phase, the test plan includes test environment, test schedule and test strategy and also the test result analysis.

## **Chapter 7: Conclusion**

This chapter summarizes the project and discusses on how the objective has been achieved, the strength and weakness of the project and what the contributions of this project are.

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

### **1.8 Conclusion**

In this chapter, problem statement, objective, scope, project significant and expected output of the projects are clearly identified. The next chapter, Chapter 2 will discuss the related work of this project.

## CHAPTER II

### LITERATURE REVIEW

#### 2.1 Introduction

A literature review is an evaluative report of information found in the previous literature related to the project. The review should describe summaries, evaluate and clarify this literature. All works included in the review must be evaluated and analyzed. The literature review also focuses on knowledge and ideas established in the topic as well as their strengths and weaknesses.

Back to the topic, the exponential growth of number of computer and other smart devices causes depletion of IPv4 address. IPv6, that is the improved version of network layer protocol has been introduced to overcome the shortfall of IPv4 protocol in meeting the demand of growing number of user in the global internet. IPv6 was developed with the intention of replacing IPv4 protocol. However, IPv6 is not interoperable directly with IPv4. Thus, transition mechanism is used to smooth out the transition to the latest internet protocol. The implementation of transition mechanism raised security concerns as it allows cybercriminal to launch attacks namely denial-of-service attack. Many researches have been done to discover the defense against attacks on transition mechanism. Intrusion detection system is a form of countermeasure identified as a defense layer against the attacks.

In this chapter, published information regarding topics related in this project is reviewed and discussed. Besides, the problems related to this research is studied and analyzed. Previous research in the area of this topic is studied and the possible solution to the problem is proposed.

## 2.2 Related Work

This section explains in detail the subjects or knowledge area related to this project which includes the network layer protocols, transition mechanism and intrusion detection system.

### 2.2.1 Internet Protocol Version 6 (IPV6)

Internet Protocol (IP) is the protocol where the data is sent from one host to another on the Internet where each host has at least one IP address that which allow it to uniquely identifies it from all other computers on the Internet. Internet Protocol Version 6 or known as IPV6 is the most recent version of the Internet Protocol (IP) that can support a very large number of nodes compare to Internet Protocol Version 4 (IPV4). This latest version is developed to address the shortfall of IPV4 that have a very limited address space and it is facing exhaustion. In IPV6, the addressing space has been increase from 32 bits in IPV4 to 128 bits which supports up to 340 undecillions addresses or  $3.4 * 10^{38}$  addresses. IPV6 also increase the addressing capabilities by supporting increased levels of addressing hierarchy, stateless address auto-configuration and introduction of a new type of address known as any cast address that is used to send a packet to group of nodes (RFC2460, 1998). Besides, IPV6 simplifies the header of the packet by eliminates fields that useless and adds field that provide better support for real-time traffic. The improvement of the security by authentication and privacy capably also has been improved.