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

IMAM MUKHSINEEN BIN ABU ZAH

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

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

IMAM MUKHSINEEN BIN ABU ZAH

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.

Tarikh:

____
(TANDATANGAN PENYELIA)
Dr. NazrulAzhar Bahaman
Nama Penyelia

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 Date:

(IMAM MUKHSINEEN BIN ABU ZAH) 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: ____________________ Date:

(DR. NAZRULAZHAR BAHAMAN) 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

LIST OF TABLES

LIST OF FIGURES

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

PS	Problem Statement
PS 1	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 IPv6transition 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.

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.

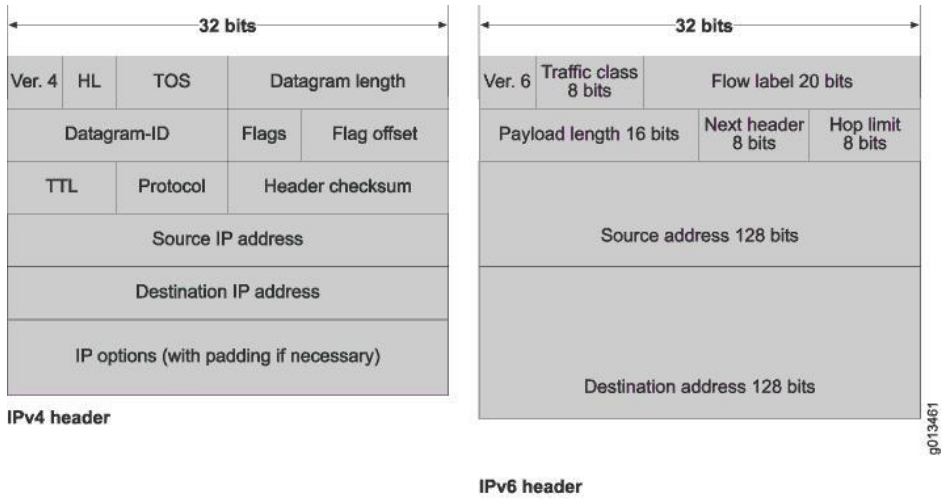


Figure 2.1: Comparison of IPv4 and IPv6 header

Figure 2.1 above shows the difference in header field between IPV4 and IPV6. IPV6 header is simpler than IPV4 header. Next, because of IPV6 address size is bigger of 128 bit binary numbers compare to IPV4 that has 32 bit binary numbers, the size of IPV6 header is bigger. The traffic class operates same as IPV4 Type of Service Field which support for the marking of traffic based on differentiated services code point. Besides, Hop Limit is similar to IP version 4 Time to Live field which limit the number of maximum number of hops the packet allowed to travel. The 16 bit payload length indicates how long in octets the payload and extension header of the packet.

In IPV6, multicast, unicast and any cast were introduced to replace broadcast and is and integrated and necessary function in IP network. In IPV6 multicast, the transmission of a packet to multiple destinations is in a single operation. Certain protocol was eliminated because of some changes and improvements that have been made. Unlike unicast, multicast address identifies multiple. With the appropriate multicast routing topology, packet addresses to a multicast address are delivered to all interfaces that are identified by the address.

IPsec, is a framework that define policies for secure communication in network and also define how to enforce these policies. It was assigned in the IPV6 protocol specification to allow IPV6 packet authentication and payload encryption via the Extension Headers. IPsec in IPV6 is implemented using AH authentication header and the ESP extension header. Without changing some of network and application, the IPsec IPV6 advanced security can be deployed by IT administrators immediately. However, IPsec must be configured and used with a security key exchange because it was not automatically implemented.

2.2.2 DOS Attack

Denial of Service (DoS) attack is one of the main threats that the network is facing. DoS attack makes use of many hosts to send a lot of useless packets to the target in short time of invalid access which will consume the targets resources and causes outage of server operations (Monika Malik et al, 2015). An attacker that is performing DOS attack will 'flood' the victim or target with false request thus reducing the target bandwidth and available system resource, prevent access to a service or disrupt service to legitimate system or user.

Dos attack also can come from more than one source at the same time that known as a Distributed Denial of Service, DDoS attack. DDoS attack is a large-scale, coordinated attack on the provision of services of a victim system or network resources that launched indirectly through a large number of compromised computer agents on the internet (K.Munivara Prasad et al, 2014). Attacker use DDoS attack to controls infected computers remotely and commands them to send false request to the target system, service or host. Figure 2.9 below shows the difference between denial of service and distributed denial of service.

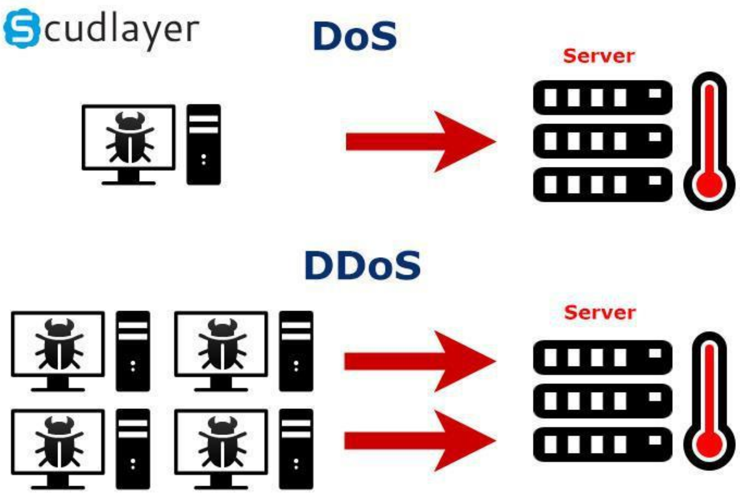


Figure 2.2: Denial of Service

ICMP flooding is one of the simplest method used by attacker to perform denial of service attack. This form of attack uses ICMP request and response packets that is used to test connectivity between hosts. The attacker send huge amount of request packet to the victim causing the victim to utilize all of its resources to respond to the request. Since computer nowadays has huge computing resources, this form of attack is less successful. Smurf attack is an amplified version of ICMP flooding and it is a form of DDoS attack (Kumar et al, 2007).

During Smurf attack, the attacker send ping packet to broadcast IP addresses with the source IP address is spoofed with the victim IP address. Each single host in the broadcast domain responds to request by sending ICMP response packet to the victim causing resource exhaustion of the victim computer or even the entire network. Besides, DOS attack is also carried out using SYN flood. The attacker sends large amount SYN request to the target causing the target to send SYN/ACK packet and wait for the final ACK to complete the three-way handshake process of TCP. The target will wait for the ACK until unable to accept other legitimate incoming connection (Lau, et al., 2000).

An intrusion detection system (IDS) is one of the countermeasures of denial of service attack. It is capable to detect the presence of DOS attack through the signature of the attack and notify the administrator for further action. Besides, it is crucial for host computer and server is up to date with the latest security patches to guard against DOS attack. Moreover, IP broadcast used by flood and Smurf attack should be disabled so that it can't be used as amplifier. The router can be effective in defeating DOS attack by configuring security features such as Ingress and Egress filtering rules and TCP Intercept and Committed Access Rate (CAR) (Piskozub et al, 2002).

2.2.3 Network Intrusion Detection System (NIDS)

An Intrusion Detection System or IDS meant to be a software application which monitors the network or system activities and finds if any malicious operations occur (S. Vijayarani et al, 2015). IDS are implemented in the network to detect the presence of intruders especially those that manage or trying to bypass the security defense layer such as a firewall, anti-virus and access control so that preventive measures can be taken. IDS are used in network related activities, medical applications, credit card frauds, Insurance agency.

The logical components of an IDS are sensors, analyzers and user interface. The sensors are responsible to sniff and collect data. The data collected will then be analyst by the analyzer to detect malicious activities. The common detection methodology of IDS is signature-based and anomaly-based (Whitman et al, 2008). Signature-based detect attack by observing and identifying events and patterns which match with the signature of the attack. An attack signature is known as the event that required to perform the attack, and the order in which they must be performed. This detection method are easy to develop if the network behavior can be identify. On the other hand, anomaly-based detection IDS compare observed event with a baseline or activity that is considered normal to identify significant deviations (Mell et al, 2007).

It detects unknown attacks, due to the rapid development of malware. By using this anomaly-based to identify attack traffic, it must be taught to identify normal system activity.

There are two phases of anomaly detection system that is training phase where a profile of normal behaviors is built and testing phase that is about where current traffic is compared with the profile created in the training phase. Anomalies can be detected in several ways, one of that is by using artificial intelligence type techniques.

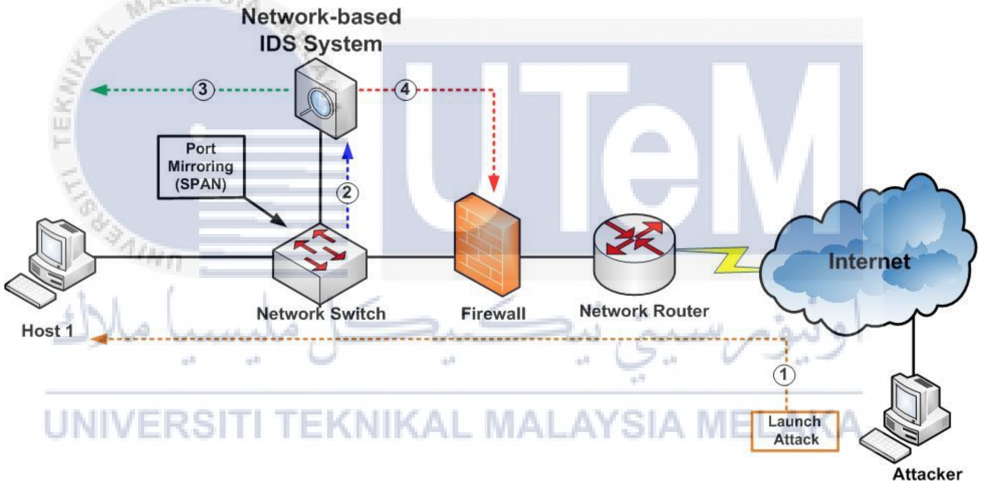


Figure 2.3: Network Based IDS

There are most two common classifications of IDS that is Network Intrusion Detection System (NIDS) and Host Intrusion Detection System (HIDS). NIDS is functioning to identify the unwanted or illegal behavior on network traffic. Figure 2.3 above is an illustration of network based IDS where the system is placed in the network. It monitors traffic at selected points in the network. The network based IDS uses an interface in promiscuous mode to sniff all the traffic. The interface is connected to the monitored network segment. Most NIDS are pattern based, which means that they require signature to alert an attack happen, or a set pattern in the payload. The accuracy of this method depends on the level to which the NIDS are fine-tuned. Network based IDS is easier to deploy compared to host based IDS.

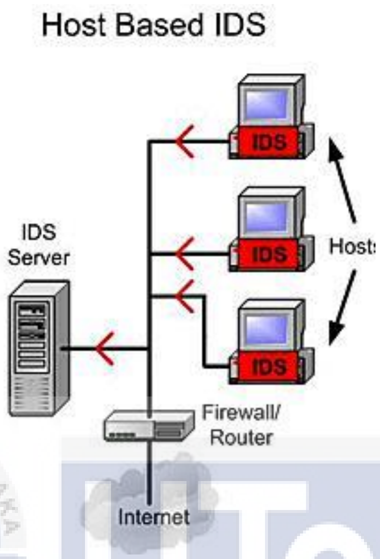


Figure 2.4: Host Based IDS

In the meantime, HIDS identify unwanted or unauthorized and anomalous behavior on a specific device. Figure 2.4 shows how host-based IDS is deployed. The HIDS scans the log files for operating system, application or DBMS for activity traces. This makes it completely dependent on the contents of the log files. As a result, if the log-files data is corrupt or in the worst case, these systems will not be able to detect the presence of the attack.

2.2.4 Protocol 41

There is an 8-bit header field in IPv4 packet that identify the next level protocol (RFC791, 1981). The equivalent header field in IPv6 packet is called Next Header (RFC2460, 1998). The protocol number known as Assigned Internet Protocol Numbers is handled by Internet Assigned Numbers Authority (IANA). Protocol number 41 assigned by IANA denotes that the payload of the packet is

IPv6 encapsulation (Internet Assigned Number Authority, 2016). IPv6 encapsulation is a mechanism in which a packet is encapsulated and transmitted as a payload within another packet (RFC2473 , 1998).

This is known as tunneling. Source node at the tunnel entry-point encapsulates a packet and channels it through the tunnel and the opposite end of the tunnel known as the tunnel exit-point, the packet is de-capsulated.

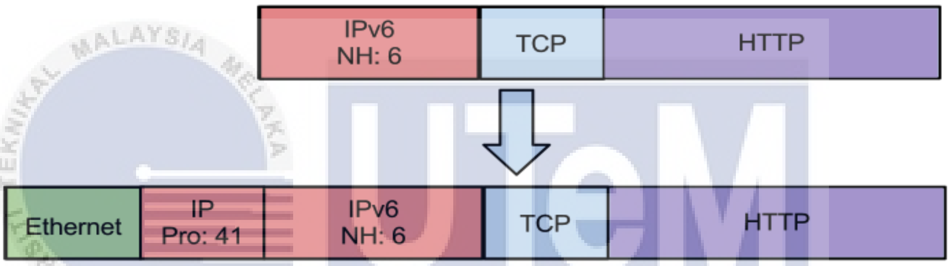


Figure 2.5: Protocol 41 Packet

Figure 2.5 above shows an example of HTTP protocol data unit (PDU) using IPv6 network protocol. The IPv6 packet is encapsulated into the payload of protocol 41 packets thus becoming an IPv4 packet.

2.2.5 Transition Mechanism

IPv6 adoption rate in the network is still low despite having huge address space and has many improvements such as streamlined protocol header over the widely used IPv4 protocol (Hagen, 2014). The factor hindering the deployment of IPv6 is its incompatibility with IPv4. IPv6 would not be able to communicate directly with IPv4. This would be a major issue as most host and router in the network around the globe still uses IPv4 (Lawton, 2001). IPv6 transition mechanism is introduced to overcome the issue and to facilitate the transition to IPv6. IPv6 designed to allow IPv6 nodes to maintain complete compatibility with IPv4, which should greatly simplify the deployment of IPv6 in the Internet, and facilitate the eventual transition of the entire Internet to IPv6. (RFC2893, 2000). IPv6 transition mechanism include dual stack in which both IPv4 and IPv6 are implemented in the host as well as at the router

2.3 Critical Review

Critical review is a writing task from the summarization and evaluation of a text. It can be from a book, a journal article or other medium. People need to read the selected text in detail in order to present a fair and reasonable evaluation of the selected text. The material must be clearly understood so that, the analyzation and evaluation of that material will be done perfectly using appropriate criteria. Therefore, there are several journals that were to be used as guidelines for this project. Among them are as follows:

Research Title: Study on Intrusion IPv6 Detection System on Linux

Intrusion detection system (IDS) can complement firewall as firewall only capable of protecting network from outside threat and unable to prevent internal intrusion. Common Intrusion Detection Framework is one of the models for IDS. This model consists of event generators, event analyzers, and response unit and event database.

The study made by the researcher focus on methods of using Linux platform to detect intrusions in coexisting IPv4 and IPv6 network environment. The method in designing IPv6 intrusion detection centers on four aspect; capturing and understanding IPv6 packet and research and implementation on packet pre-processing, extraction of intrusion features, fast detection and matching of intrusion attack (Yu et al, 2009). Since IPv6 has new structure of packet with different header fields and extension header, the IDS have to be capable to understand the whole packet. The intrusion detection engine is based on rule set. The controls to the whole function is done using web-based visual console.

The placement of Intrusion detection system in a high-speed network may cause the IDS to be saturated with traffic and causes packet to be dropped. The method suggested in the research is using multiple node processing system. The functions of the IDS are split where a node capture packets and another node processes the packets. Information system security assurance is achieved by protection, detection, reaction and recovery. The implementation of IDS can provide detection so that reaction and recovery can be done to secure the information system.

Research Title: Ipv6 Security Threats and Possible Solutions

A study has been conducted on IPv6 security threats and the possible solutions. According to the research, despite the introduction of IPv6 security mechanism, their evasion and misuse is still possible. Besides, transition mechanism provides new, previously unknown possibilities of intrusion and misuse of computer system (Zagar et al, 2006).

The security threats to IPv6 are reconnaissance attack where the attacker perform scanning and data mining usually using the IPv6 multicast address to gain information about the target network for further attacks. Besides, routing header can be misused to bypass access control. Access control can also be bypassed by using fragmentation as security mechanism does not reassemble.

Besides ICMPv6 and multicast is misused to cause multiple response targeted to the victim to perform denial-of-service attack. ICMPv6 message such as Router Advertisement and Neighbors Discovery can be exploited to perform attack. In transition mechanism, IPv4 or IPv6 address can be spoofed to perform denial-of-service attack to target IPv6 node, IPv4 node or other 6to4 node (Zagar et al, 2006). Moreover, the tunneling facilitates attacker to avoid filtering checks.

One of the solutions to the threats is by implementing firewall as it is the most essential defense mechanism. Firewall must be able to support IPv6 because of the different structure of IPv6 packet. Firewall filters traffic based on the separately predefined rules for IPv6 and IPv4. The filtering rules must be separated between IPv4 and IPv6 because the difference in the network layer mechanism. For example, ICMPv6 cannot be filtered by the firewall because it is crucial for proper IPv6 functioning.

It is recommended by this research to implement Host-based IDS on every host and Network based ids on each network segment. Intrusion Detection System implemented must support IPv6 due to the new header format. IDS is recommended to check the extension header and drop undefined “Next Header” and irregular or duplicate options such as hop-by-hop and destination. Furthermore, IDS should also be able to recognize IPv6 tunneled in IPv4. IPv6 tunnel end point should be before the firewall and IDS is placed at network entry point behind the firewall.

Testbed designed in the study using 5 dual boot computers with Linux and Windows as well as supporting dual-stack with IPv6 connected in a LAN. The LAN is connected to Croatian Academic Research Network version 6 (CAR6Net). NMap application has been used to perform TCP connect scan, SYN scan, Xmas tree scan (FIN,URG,PUSH), ICMP scan and UDP scan. All the scan is used to identify opened ports on the target machine. All the scan failed to bypass Linux firewall but some managed to pass through Windows firewall. IDS placed in front of firewall can detect intrusion attempt and behind firewall can detect intrusion that manage to bypass.

Since IPv6 supporting IDS was not present at the time of research, Ethereal application is used to detect intrusion and it successfully capture reconnaissance attack in the experiment as different port is attempted during short period of time. The finding of this study is that it is recommended to implement packet filtering and intrusion detection to safeguard against IPv6 threat. Besides it is suggested to filter all unnecessary services, discard fragment less than 1280 except the last fragment, and selectively filter ICMPv6 and use dual-stack or static tunnel instead of dynamic tunnel.

Research Title: Implementation of IPv6 Network Testbed: Intrusion Detection System on Transition Mechanism

There are a couple of researches done on intrusion detection system on IPv6. One of the research designed a testbed which can be used for experiments to learn the activity of intruder and attacker on transition mechanism (Bahaman, et al., 2011). The testbed includes native IPv6 network, IPv4 network as well as IPv4/IPv6. IPv6 over IPv4 tunnel is used to interconnect IPv6 network to IPv6/IPv4 network over a IPv4 network.

IDS and packet analyzer to is placed at the 6to4 tunnel. The traffic from attacker to the victim was observed. The testbed architecture is shown in the Figure 2.5 below. ICMPv6 flood attack is used as sample attack in the experiment. The data taken from the experiment is the connectivity, hop count, round trip time, throughput, threat and intrusion detection and packet flow.

The researchers found out that the testbed is effective and the hardware and software used is capable of performing its intended function.

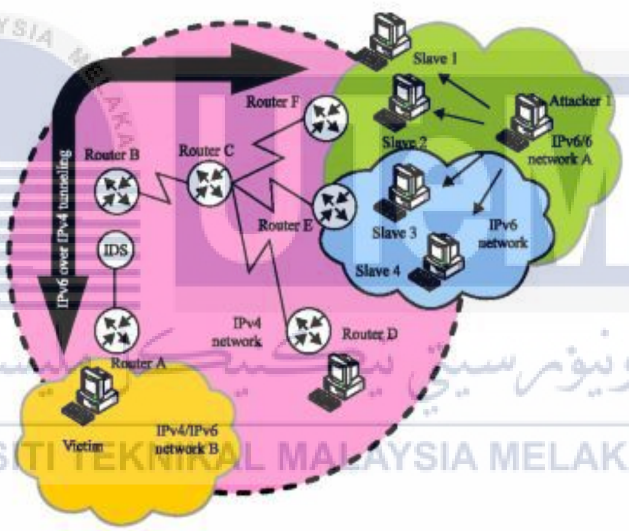


Figure 2.5 Testbed for intrusion detection mechanism on transition mechanism.

2.4 Proposed Solution

Based on the previous solution, there is various techniques for intrusion detection in order to detect the present of the threat. The proposed solution for security threats on IPv6 transition mechanism is to implement a Network Intrusion Detection System (NIDS) prototype that can live alert and notify upon occurrence of attacks. The testbed designed in (Bahaman, et al., 2011) will be used as a reference to test the effectiveness of the IDS implemented.

2.5 Conclusion

IPv6 is the future of IP network that has huge address space and much more efficient than IPv4. While waiting for the rest of the world to fully adopt the latest protocol, transition mechanism is needed to maintain interoperability with the widely used IPv4 protocol. However, the usage of transition mechanism might expose the network from security threats. Thus, it is crucial to take necessary action to secure the network while the transition from IPv4 to IPv6 is in progress.

CHAPTER III

PROJECT METHODOLOGY

3.1 Introduction

A methodology is a documented series of systematic methods for dealing with a complex job or task such as solving problems or developing a system (Dewitz, 1996). Selecting a methodology that is suitable to the project is important because it can ensure the optimum cost and time in carrying out the project. This chapter covers the selected methodology that will be used in this project. The project will be carried out in phases and the activities in each phase will be explained in this chapter. The milestone of each phase is listed out in the form of Gantt chart.

3.2 Project Methodology

Rapid Application Development (RAD) has been chosen as a methodology for the project to ensure the objective of the project can be fulfilled. RAD dictates that a preliminary version of the end product is developed and tested. Changes and improvements are incorporated to produce a better version iteratively until requirement fulfilling version is achieved. This methodology is suitable to this project because it allows a prototype to be developed with known requirement and improvements are made to the prototype when there are changes to the requirement.

The five main phases in this project are planning, analysis, design, implementation and testing. The project flow is illustrated in the block diagram below:

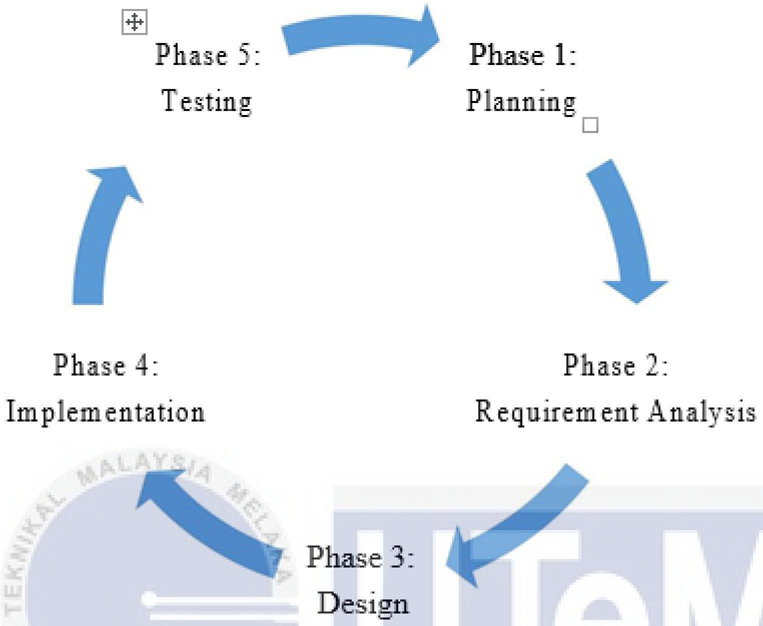


Figure 3.1 Methodological Phase

3.2.1 Planning Phase

This is the first phase of this project. Plans are created on how this project will be carried out till completion. The activity carried out in this phase are as below:

- Proposal

The problem that lead to the commencement of this project is identified. The problem statement, objective and scope of this project is derived from the problem. The project scheduling is created and the milestone for each phase are identified.

3.2.2 Analysis and Design Phase

The requirements of the project are defined in this phase. The problem is analysed to obtain a well-defined requirement that will determine the direction of the project. The activity carried out in this phase are as below:

- Perform literature review

Previous and related work of this project is reviewed. The methodology, techniques, hardware and software used and parameter of the previous work is studied to serve as a guide to this project.

- Simulate and analyse the transition mechanism attack

The attacks on transition mechanism is analysed to figure out the pattern or signature of the attack. The pattern or the signature will be used to develop the countermeasure in the form of signature based intrusion detection system.

- Perform requirement analysis

During this activity, the data, functional and non-functional requirement is determined. The data requirement indicates what data is input to the system and what output does the system should produce. Functional requirement includes the functions of the system and how it perform its operation. Non function requirement covers the performance and quality aspects of the system.

- Hardware and software analysis

The hardware and software to be used in this project is determine during this activity. Various options of hardware and software is evaluated to identify the one which best suits this project.

In design phase, the requirement from previous phase is translated into design. The activities involved in this project are listed below:

- Architecture / Test bed design

The placement of host devices, routers, connections are determined in this design. How the devices are interconnected are designed during this activity. The architecture in this design will be used to perform attack as well as detection of attacks.

- Software design

The function of detecting an attack and producing alert of the IDS is designed during this activity. The design of the IDS is illustrated using Data Flow Diagram (DFD). Besides, program specifications which includes description, input/output and are created during this activity.

3.2.3 Implementation phase

The end product of this project starts to take shape during this phase. The design from the previous phase is implemented during this phase. Activities during this phase are as below:

- Setting up the architecture / test bed

The test bed design is set up physically during this activity. The network as well as the transition mechanism is configured. The OS of the host devices is installed. The connectivity is tested to ensure the devices are working as intended.

- Develop the intrusion detection system

The software design is developed into a working system. The IDS developed is ran on the monitoring host device.

3.2.4 Testing phase

This is the crucial phase of the project. This phase determine the effectiveness of this project. The activities involved in this phase includes test plan, test design and test results analysis.

- Test plan

During this activity, the personnel involved during testing, testing environment, test schedule and testing strategy is determined. Testing environment is the environment or location the testing is carried out. Test schedule indicate how many times the test is repeated and the duration of the test.

- Test design

In this activity, the attack simulation is designed to test the effectiveness of the IDS.

- Test result analysis

The test is carried out during this activity and the data and result is collected. The result is analyzed and compared with the expected result. The failed test case is studied and documented.

Changes were made at the design and implementation phase to solve the failed test case.

3.3 Project Schedule and Milestones

3.3.1 PSM 1 Milestone

The project schedule is created to ensure efficient time management and to ensure the project can be completed within the stipulated period. Table 3.1 below shows the scheduling of this project.

Table 3.1: PSM 1 Milestone

Week/ Dates	Milestones/Project Activities	Description
1 13 - 17 Feb	Submit & Present PSM Proposal	Deliverable – **Proposal** Action – Student
		Deliverable – **Proposal Presentation** Action – Student
	Evaluation and verification of proposal Upload approved proposal to e-Repository System	Action – Supervisor, Evaluator
2 20 - 24 Feb	Correction / Enhancement Proposal Chapter 1	Action – Student
	Supervisor list/PSM Title	Action – AJK PSM/PD
3 2 - 3 Mar	Chapter 1 (System Development Begins)	Deliverable – **Chapter 1** Action – Student, Supervisor
4 6-10 Mar	Chapter 1 & 2	Action – Student
5 13 - 17 Mar	Chapter 2	Action – Student
6 20 -24 Mar	Chapter 2 & 3	Deliverable – **Chapter 2 Progress Presentation 1** Action – Student, Supervisor
	Determination of Status Students Students borrow equipment for development stage	Action – AJK PSM/PD, Supervisor

7 27 – 31 Mar	Demo Chapter 3, Chapter 4	Action – Student
8 3 - 7 Apr	Mid Semester Break	
9 10 - 14 April	Demo Chapter 4	Deliverable – Chapter 3 Action – Student, Supervisor
10 17- 21 April	Demo Chapter 4	Deliverable – Progress Presentation 2 Action – Student, Supervisor
	Student Status	Action – AJK PSM/PD, Supervisor Warning Letter 2
11 24 - 28 April	Demo PSM Report	Action-Student
	Determination of student status(Continue/Withdraw)	Action –PSM/PD Committee, Supervisor(submit student status to AJK)
12 1 – 5 May	Demo PSM Report	Action – Student, Supervisor, Evaluator
13 8 -12 May	Table Presentation	AJK PSM/PD
	Demo PSM Report	Deliverable PSM Report Action – Student, Supervisor
14 15 - 19 May	Project Demo & PSM Report	Deliverable – PSM Report Action – Student, Supervisor
15 22 -26 May	Final Presentation	Action – Student, Supervisor, Evaluator
16 29 May - 2 June	STUDY WEEK Correction draft report based on supervisor’s and evaluator’s comments during the final presentation session. Submission overall marks to PSM/PD committee.	Action – Student, Supervisor, Evaluator AJK PSM/PD

The table above shows the milestone for PSM 1. The PSM 1 covered from week 1 until week 28. The activity included the proposal submission, Chapter 1, 2, 3, and 4 submissions and the project demonstration and final report presentation. The activity listed out together with the period of the project demonstration and the report presentation.

3.3.2 Gantt Chart

Table 2.2: Gantt Chart

Research Activities & Milestones	2017						Sem Khas			2017					
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Research Process															
Literature Review	■	■													
Analysis			■	■											
Create Forms - Enrolment					■	■									
Forms Prototype						■	■	■							
Evaluation/Matching							■	■	■						
Propose Prototype								■	■	■					
Milestones															
Project kick start	■														
Project Meeting	■	■	■	■	■	■	■	■	■	■	■	■			
Progress Report Submission				■				■				■			
Conference Paper				■							■				
Journal				■								■			
PSM Final Report												■	■	■	
Report Writing															
Introduction	■	■	■	■											
Literature Review		■	■	■	■	■	■	■							
Methodology					■	■	■	■							
Analysis and Discussion									■	■	■	■			
Conclusion									■	■	■	■			
Demo / Presentation															
Demo I							■								
Demo II									■						
Demo III										■					
Demo IV											■				
Demo V												■			
Demo VI													■		
Project Demo & PSM Report														■	
Final Presentation															■

3.4 Conclusion

As the conclusion, the methodology describes the steps and processes involved in conducting this project from beginning till the completion which assist in delivering the outcome expected in this project. Thus proper methodology is crucial and it ensures that the project is executed in a systematic way. The subsequent chapter will discuss in detail on the analysis, design, implementation and testing phase mentioned above.

CHAPTER IV

ANALYSIS AND DESIGN

4.1 Introduction

Analysis and design is the crucial stage during development. It helps to define a clear idea on the product being developed. In this chapter, the analysis and design of IPv6 transition mechanism is discussed in detail. The analysis phase involves gathering requirements for the system. Once requirement is defined, the design phase commences. The design phase includes designing the network architecture as well as the software design.

4.2 Problem Analysis

IPv6 is an improved version of IPv4 that provide features such as stateless auto-configuration and faster routing. Growing number of organizations adopted IPv6 into their network. However, IPv6 and ICMPv6 has inherent protocol weaknesses that can be exploited and expose the network to threats. Toolkit to attack the weakness of mentioned protocol is widely available on the internet. The Hacker Choice-IPv6 or known as THC-IPv6 is an example of attack toolkit.

Conventional security mechanism such as Intrusion Detection System supposedly would be able to detect these attacks. In order to avoid detection, attacker launch attack through the IPv6 transition mechanism tunnel. For example, in 6to4 tunneling, the attack is placed in the packet inside the payload which allows it to pass the IDS undetected. Intrusion detection system should be improved to be able to detect attack inside the transition mechanism**.**

4.3 Requirement Analysis

4.3.1 Data Requirement

The data or input that will be received by the attack detector is the mirrored traffic or packets from the tunnel. The packets will be analyzed by the attack detector and it will generate alert notification if an attack occurred. Figure 4.1 is the block diagram of the attack detector.

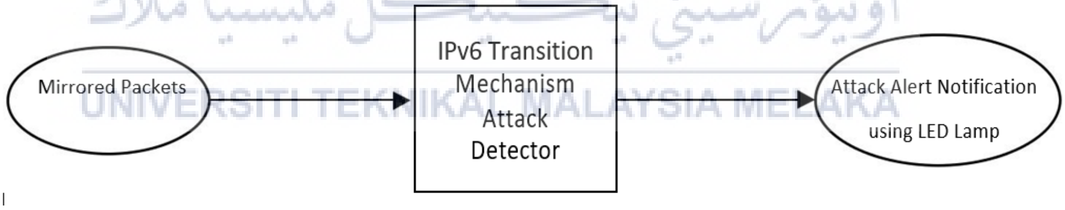

Mirrored Packets
IPv6 Transition Mechanism Attack Detector
Attack Alert Notification using LED Lamp

Figure 4.1: Block Diagram of Attack Detector

4.3.2 Functional Requirement

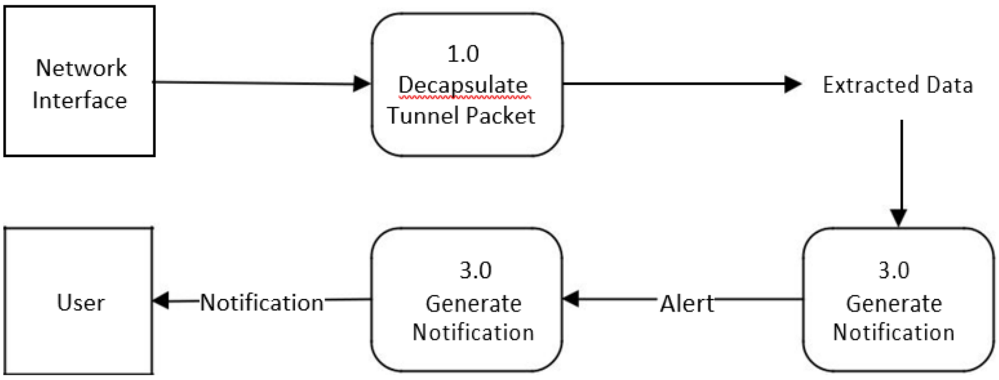

Network Interface
1.0 Decapsulate Tunnel Packet
Extracted Data
3.0 Generate Notification
Alert
3.0 Generate Notification
Notification
User

Figure 4.2: Attack Detector Data Flow Diagram

The IPv6 Transition Mechanism detector operates by receiving packets from the network interface. Since it receives packet from a tunnel, the packet is decapsulated to obtain the payload packet. The payload packet will be analysed by comparing it to attack signature. If an attack is detected, an alert is generated to notify user.

4.3.3 Other Requirement

4.3.3.1 Hardware Requirement

- **Router**

Router is a layer 3 networking device that route packets across computer networks.

Routers interconnect multiple networks. Routers forward packet using IP protocols. Routers are used in this research to simulate IPv4 cloud. Besides, router is used to create IPv6 transition mechanism 6to4 tunnel that interconnects two IPv6 island over IPv4. The model of the router used is Cisco 2800 series router.

- **Switch**

Switch is a layer 2 networking device that is used to connect multiple networking

device together. It receives, process and forward data frame towards the destination using frame switching. Switch is used in this research to replicate the traffic in the tunnel by using port mirroring function of the switch. The attack detector will be connected to the mirror port. Switch model used is Cisco 2960 series.

- **Computer**

Computer running Ubuntu Linux operating system is used in this project.

Penetration tools provided in Kali Linux operating system is used to launch the attack. Another computer is used to run the attack detector and sniff for attacks are using Raspberry Pi 3 Model B. The third computer is the target computer.

- **Breadboard with LED Lamp**

A number of LED has been installed on the breadboard that connected to the Raspberry PI. This LED will give a signal to the user once when the attack occurred inside the tunneling.

4.3.3.2 Software Requirement

- **Python**

Python is an open source programming language. Python can be run on almost any platform. Python is also fast making it suitable for this research. Besides, Python provide high number of third party package that can be implemented. Python is used to program the attack detector.

- **Scapy**

Scapy is an open source packet manipulation program. It is used in this research to decode captured packets.

- **PuTTY**

PuTTY is an open source secure shell client application. The application is used in this research to access the router using console cable as well as accessing it remotely using secure shell. Configuration of the router is done through this application. It is also used to remotely accessed another computer in the test bed.

4.4 High Level Design

4.4.1 IPv6 Testbed Architecture

This section describes the setup and the configuration of the network environment that will be used as testbed to test the effectiveness of the IDS in detecting attacks.

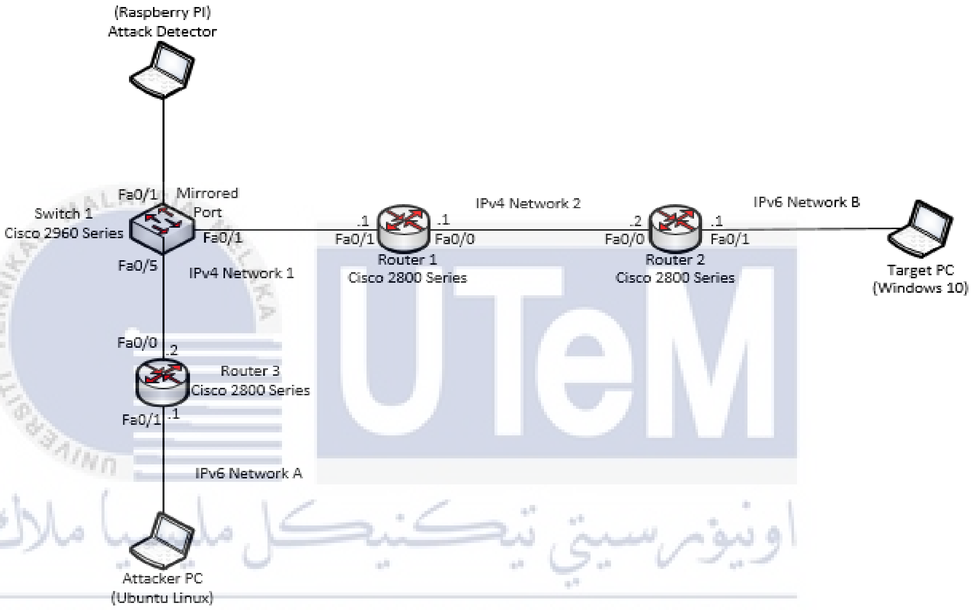


Figure 4.3: Network System Architecture

Figure 4.3 above shows the overall design of the network architecture. In the architecture, IPv6 network A and IPv6 network B are isolated by IPv4 only networks. The connection between Router 3 and Router 2 only support IPv4. Thus, to enable connection between the two IPv6 island, 6to4 tunnelling method of transition mechanism is created to connect Router 3 to Router 2. Router 1 is the intermediary router used to mimic an IPv4 cloud that forwards tunnelled packet towards its destination. A switch is placed in between Router 3 and Router 1 and the traffic in between the router is mirrored to the IDS. Attack will be done from attacker PC running Ubuntu Linux operating system in IPv6 network A to target PC in IPv6 network B through the 6to4 tunnel.

4.4.2 Physical and Logical Network Design

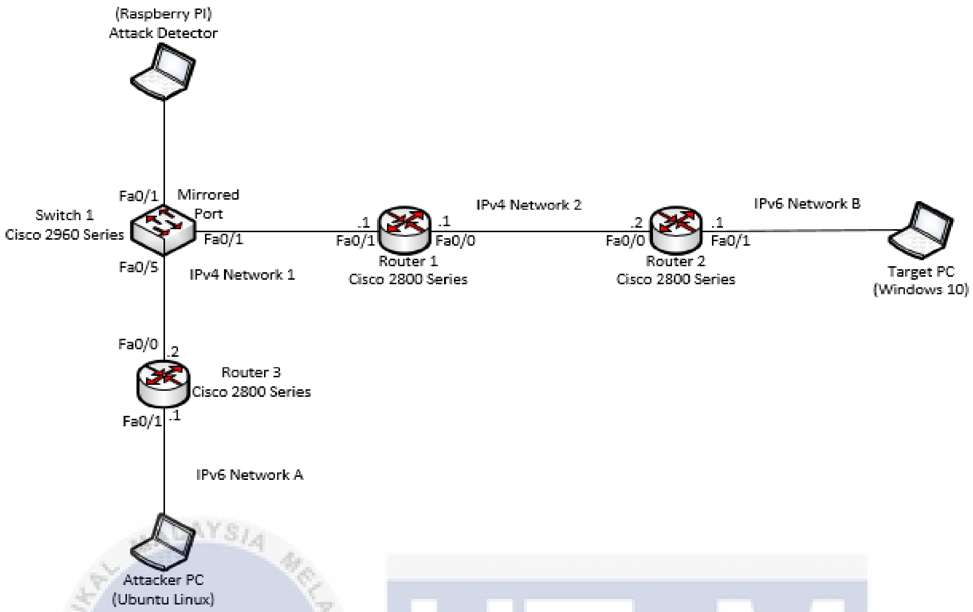


Figure 4.4:Network Physical Design

Figure 4.4 above illustrates the physical setup of the network. The network is made up of 3 routers with each router having 2 Fast Ethernet interfaces. The router used in this research is Cisco 2800 series router and the switch used is Cisco 2960 series. All network connection is done using Ethernet UTP Cat5e cable. In IPv6 Network A, a pc is connected to the Fa0/1 of the router 3. Similar setup is done at IPv6 Network B. Router 1 is connected to Switch port Fa0/1 and Router 3 is connected to Switch port Fa0/5. Port Fa0/1 is configured as mirrored port of port Fa0/3. The mirrored port is connected to the PC running IDS application.

4.4.3 Logical Design

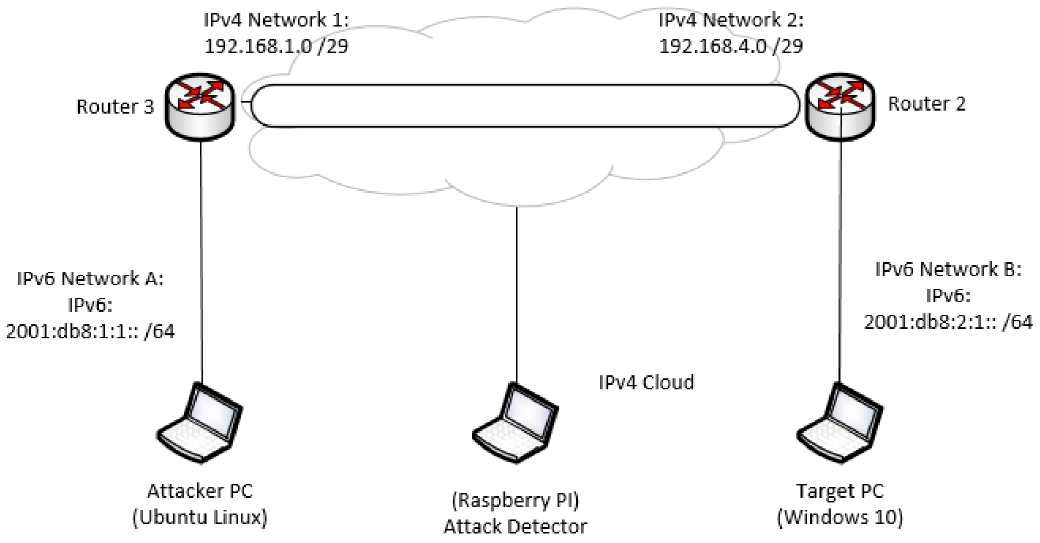


Figure 4.5: Logical Network Design

Figure 4.5 above shows the logical design of the network. Since the network between Router 3 and Router 2 only supports IPv4, IPv6 traffic between IPv6 network A and IPv6 network B is tunnelled in 6to4 tunnelling. The IPv6 packet is encapsulated in IPv4 packet as it exits Router 3 towards Router 2. The tunnel uses 6to4 prefix 2002::/16. The IP address of cloud facing interface of 192.168.1.2 and it is the tunnel source. Thus the tunnel IPv6 address of Router 3 is derived from the IPv4 address and the address is 2002:COA8:102::/64. The IP address of the cloud facing interface of Router 2 is 192.168.4.2 and the tunnel IPv6 address is 2002:COA8:102::/64. The IPv6 network address of IPv6 network A is 2001:db8:1:1:: /64 while the network address for IPv6 network B is 2001:db8:2:1:: /64.

4.5 Conclusion

The thorough problem analysis facilitates the data, functional, hardware and software requirements gathering. A well-defined requirement can ensure the development is on the right track to achieve its objective. The software and architecture design facilitates the implementation process. The implementation phase and activity will be discussed in the next chapter.

CHAPTER V

IMPLEMENTATION

5.1 Introduction

This chapter elaborates on the implementation of this IPv6 Transition Mechanism DOS Attack Detector. The analysis and design made in the previous chapter is applied and implemented in this chapter. The environment setup and implementation status for each component is described in this chapter. It will only contain information on how the design became and how this was complete. There will be used some diagrams, tables and figures to explain flows and some logical examples.

There has been some small changes made throughout the project, these changes were been made to enhance the project. In this chapter it will be explained what has been done and how it became so.

5.2 Environment Setup

The environment setup of the testbed in this project is as below:

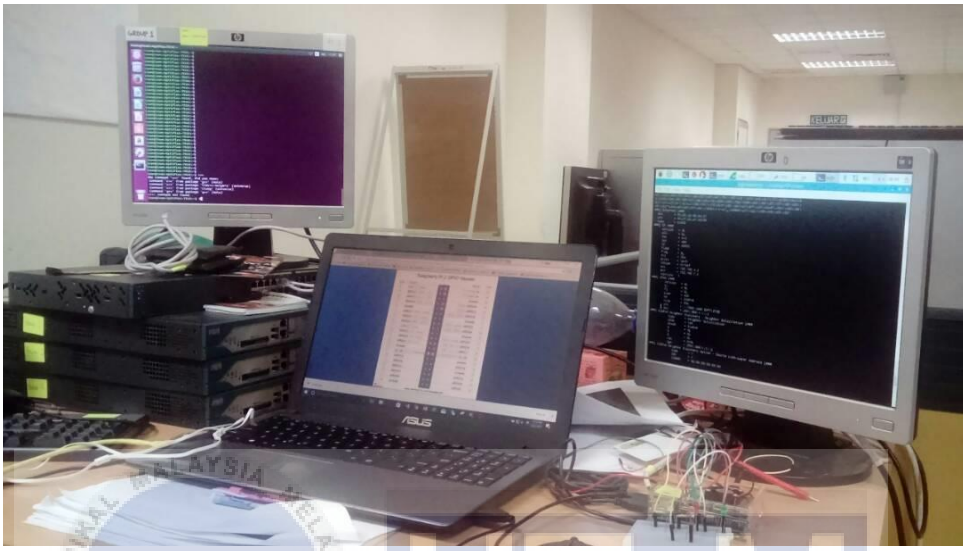


Figure 5.1: Environment Setup

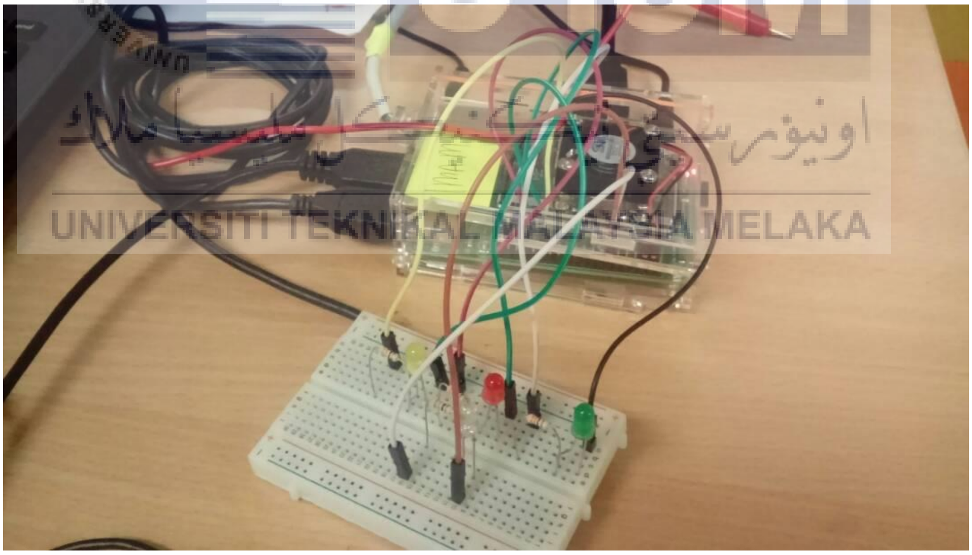


Figure 5.2: Environment Setup

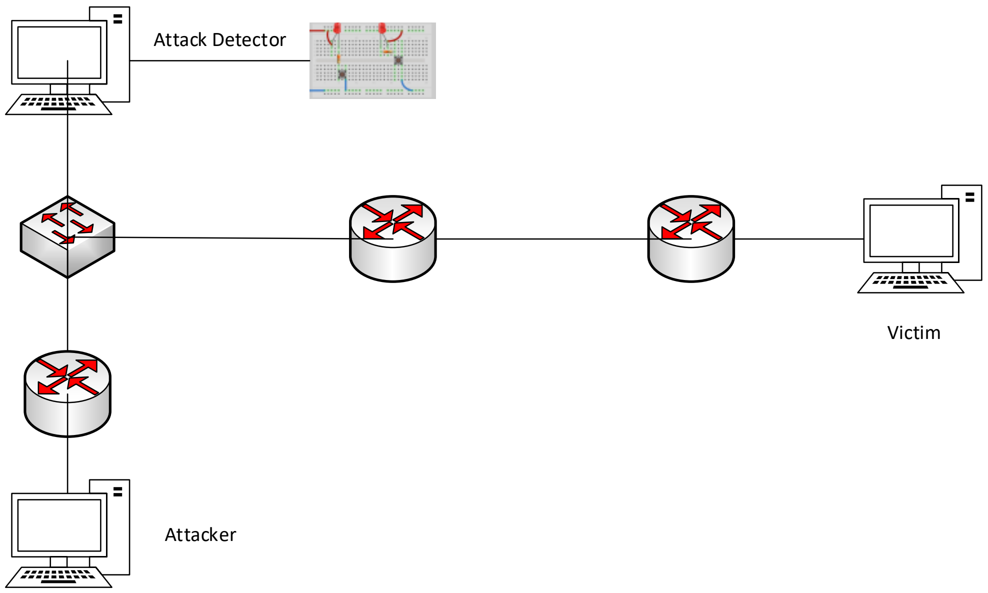


Figure 5.3: Environment Setup Illustration

Figure 5.3 above shows the setup and placement of hardware in this project. The routers are connected together to form an IPv4 cloud with the border router as the 6to4 tunnel endpoint. The network configuration is as Figure 4.6 Logical Network Design from the previous chapter. The Attacker PC is used to launch attack to the Target PC. The 6to4 tunnel traffic is mirrored to the computer running the IPv6 Transition Mechanism DOS Attack Detector to detect the presence of attack.

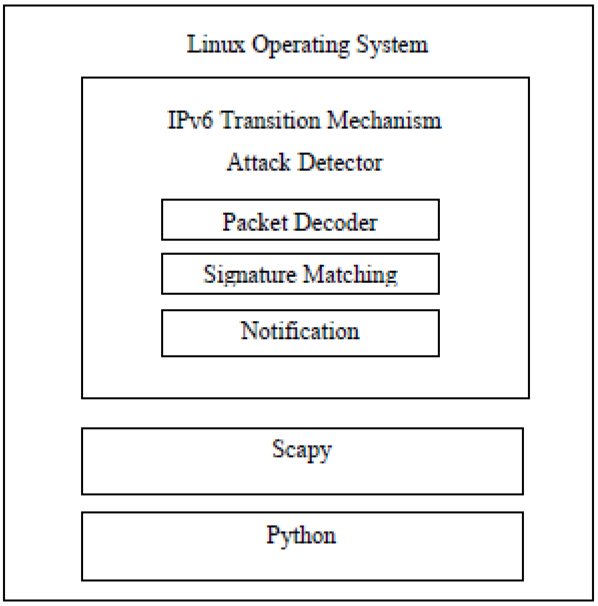


Figure 5.4: Software Environment

Figure 5.4 shows the software environment of the IPv6 Transition Mechanism DOS Attack Detector software. The software will run inside a Linux Ubuntu operating system. The software is compiled and run using python. Scapy provides a portable framework for low level network monitoring. It is used to capture the packets in the network.

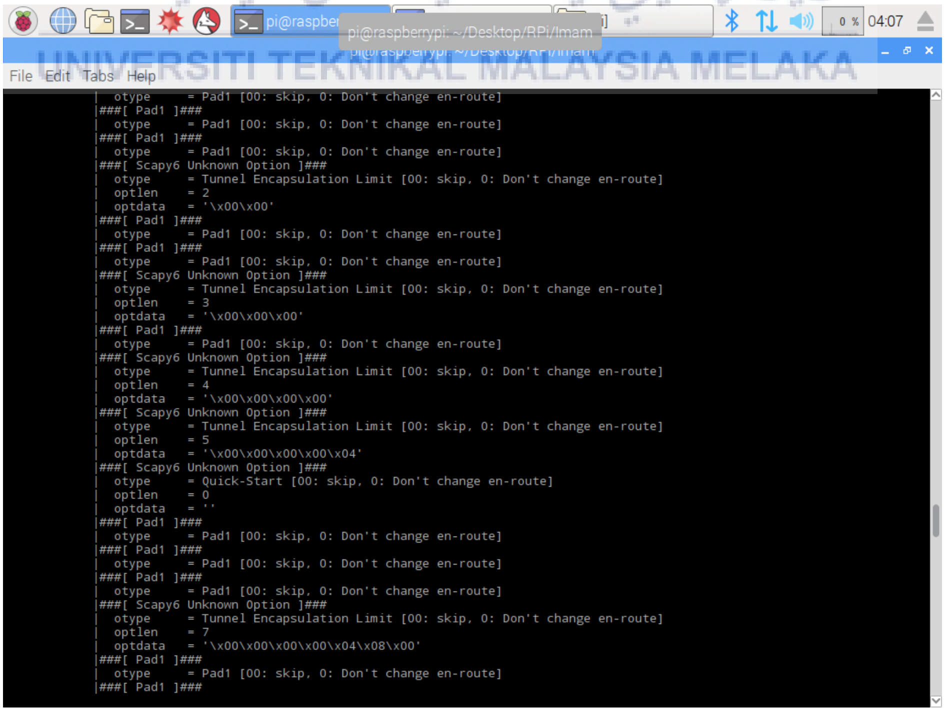
5.3 Attack Signature Identification

This section discusses the signature of the attacks that is involved in this project. The attacks selected in this project are denial6, sendpees6 and thcsyn6.

Denial6

Denial6 is a form of Denial-of-Service attack from the *THC-IPv6* attack toolkit. The attack is showed below:

- Denial6 Test case 2: Large destination header filled with unknown option



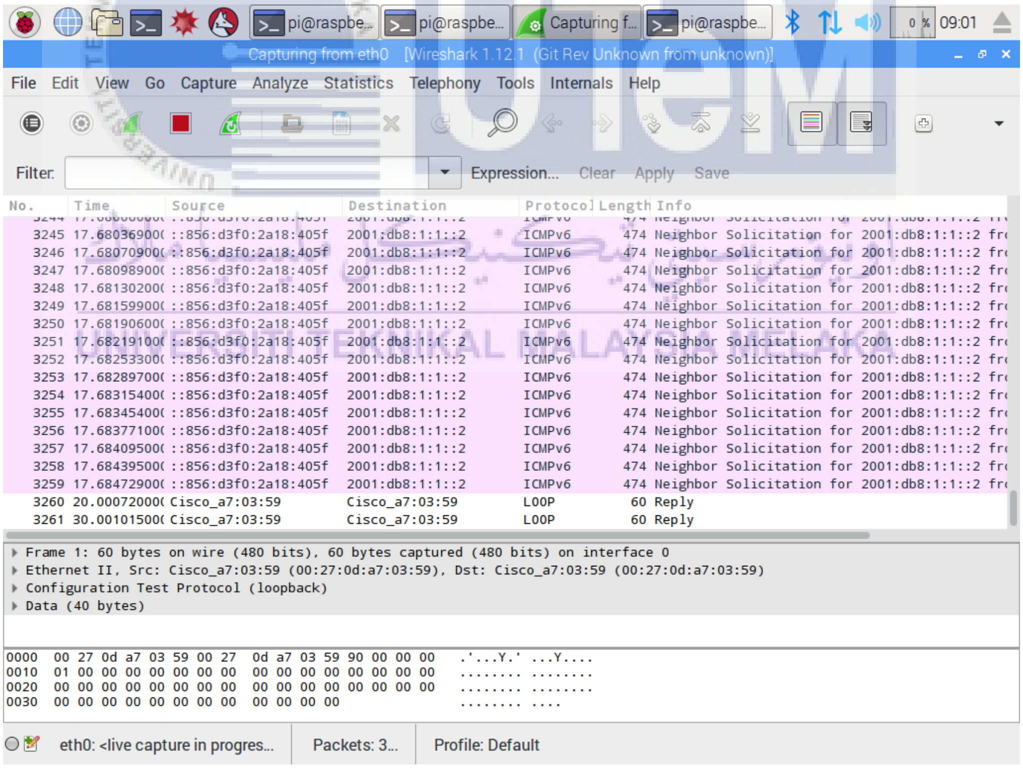
```
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Scapy6 Unknown Option ]###
  |  otype     = Tunnel Encapsulation Limit [00: skip, 0: Don't change en-route]
  |  optlen    = 2
  |  optdata   = '\x00\x00'
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Scapy6 Unknown Option ]###
  |  otype     = Tunnel Encapsulation Limit [00: skip, 0: Don't change en-route]
  |  optlen    = 3
  |  optdata   = '\x00\x00\x00'
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Scapy6 Unknown Option ]###
  |  otype     = Tunnel Encapsulation Limit [00: skip, 0: Don't change en-route]
  |  optlen    = 4
  |  optdata   = '\x00\x00\x00\x00'
  |###[ Scapy6 Unknown Option ]###
  |  otype     = Tunnel Encapsulation Limit [00: skip, 0: Don't change en-route]
  |  optlen    = 5
  |  optdata   = '\x00\x00\x00\x00\x04'
  |###[ Scapy6 Unknown Option ]###
  |  otype     = Quick-Start [00: skip, 0: Don't change en-route]
  |  optlen    = 0
  |  optdata   = ''
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Scapy6 Unknown Option ]###
  |  otype     = Tunnel Encapsulation Limit [00: skip, 0: Don't change en-route]
  |  optlen    = 7
  |  optdata   = '\x00\x00\x00\x00\x04\x08\x00'
  |###[ Pad1 ]###
  |  otype     = Pad1 [00: skip, 0: Don't change en-route]
  |###[ Pad1 ]###
```

Figure 5.4: Denial6 Test Case 2 Packet Capture

Figure 5.4 shows the destination header of captured denial6 test case 2 packet. As shown in figure, the destination header is filled with unknown option and padding with the aim of wasting processing resource of the victim and cause Denial of Service under heavy load. This attack is identified by the unknown options in the destination header.

Sendpees6

Sendpees6 is a form of Denial-of-Service attack from the THC-IPv6 that exploits the Secure Neighbour Discovery Protocol (SeND). SeND secure the vulnerable Network Discovery Protocol (NDP) by using Cryptographically Generated Address. Sendpees6 make the victim to verify large number CGA thus causing Denial of Service.


pi@raspbe...
pi@raspbe...
Capturing f...
pi@raspbe...
0 %
09:01
Capturing from eth0 [Wireshark 1.12.1 (Git Rev Unknown from unknown)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Filter:
Expression... Clear Apply Save

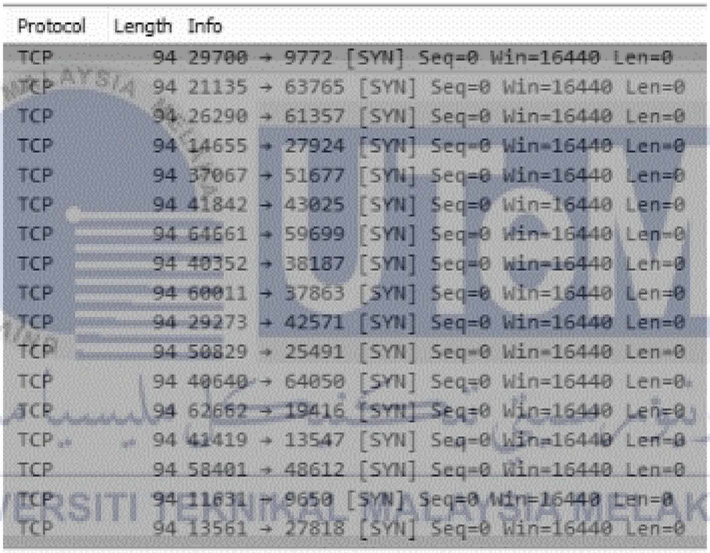
```
No.   Time        Source                  Destination        Protocol Length Info
 3245 17.68036900( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3246 17.68070900( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3247 17.68098900( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3248 17.68130200( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3249 17.68159900( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3250 17.68190600( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3251 17.68219100( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3252 17.68253300( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3253 17.68289700( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3254 17.68315400( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3255 17.68345400( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3256 17.68377100( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3257 17.68409500( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3258 17.68439500( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3259 17.68472900( ::856:d3f0:2a18:405f   2001:db8:1:1::2    ICMPv6    474 Neighbor Solicitation for 2001:db8:1:1::2 fr
 3260 20.00072000( Cisco_a7:03:59         Cisco_a7:03:59     LOOP       60 Reply
 3261 30.00101500( Cisco_a7:03:59         Cisco_a7:03:59     LOOP       60 Reply

▸ Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0
▸ Ethernet II, Src: Cisco_a7:03:59 (00:27:0d:a7:03:59), Dst: Cisco_a7:03:59 (00:27:0d:a7:03:59)
▸ Configuration Test Protocol (loopback)
▸ Data (40 bytes)

0000  00 27 0d a7 03 59 00 27  0d a7 03 59 90 00 00 00   .'...Y.' ...Y....
0010  01 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0020  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0030  00 00 00 00 00 00 00 00  00 00 00 00              ........ ....

eth0: <live capture in progres...   Packets: 3...   Profile: Default
```

Figure 5.5: Wireshark Snippet of Sendpees6 Attack

Figure 5.5 above shows the Wireshark capture of the tunnel during the Sendpees6. Sendpees6 attack floods the victim with SeND neighbour solicitation message using the link-layer address 58:58:58:58:58:58. The attack uses the same link layer address each time and there is no option to change the address. Thus, this attack can be detected by high rate of neighbour solicitation packet from the link layer address 58:58:58:58:58:58.

Thcsyn6

Thcsyn6 is a form of Denial of Service attack from the THC-IPv6 that does SYN flooding. This attack exploits the TCP three-way handshake connection establishment process. When a host receive a SYN flagged packet, it has to respond with SYN ACK or SYN NACK packet. This exhaust the victim resource and affect legitimate traffic.



```
Protocol  Length Info
TCP           94 29700 → 9772 [SYN] Seq=0 Win=16440 Len=0
TCP           94 21135 → 63765 [SYN] Seq=0 Win=16440 Len=0
TCP           94 26290 → 61357 [SYN] Seq=0 Win=16440 Len=0
TCP           94 14655 → 27924 [SYN] Seq=0 Win=16440 Len=0
TCP           94 37067 → 51677 [SYN] Seq=0 Win=16440 Len=0
TCP           94 41842 → 43025 [SYN] Seq=0 Win=16440 Len=0
TCP           94 64661 → 59699 [SYN] Seq=0 Win=16440 Len=0
TCP           94 40352 → 38187 [SYN] Seq=0 Win=16440 Len=0
TCP           94 60011 → 37863 [SYN] Seq=0 Win=16440 Len=0
TCP           94 29273 → 42571 [SYN] Seq=0 Win=16440 Len=0
TCP           94 50829 → 25491 [SYN] Seq=0 Win=16440 Len=0
TCP           94 40640 → 64050 [SYN] Seq=0 Win=16440 Len=0
TCP           94 62662 → 19416 [SYN] Seq=0 Win=16440 Len=0
TCP           94 41419 → 13547 [SYN] Seq=0 Win=16440 Len=0
TCP           94 58401 → 48612 [SYN] Seq=0 Win=16440 Len=0
TCP           94 11631 → 9650 [SYN] Seq=0 Win=16440 Len=0
TCP           94 13561 → 27818 [SYN] Seq=0 Win=16440 Len=0
```

Figure 5.6: Wireshark Snippet During Thcsyn6 Attack

Figure 5.6: shows the flooding of TCP SYN packet during Thcsyn6 attack. Thus, this attack can be detected if there is high rate of TCP SYN in the network.

5.4 Implementation Status

The development status of each for each of the components or the module of the IPv6 Transition Mechanism DOS Attack Detector is described below:

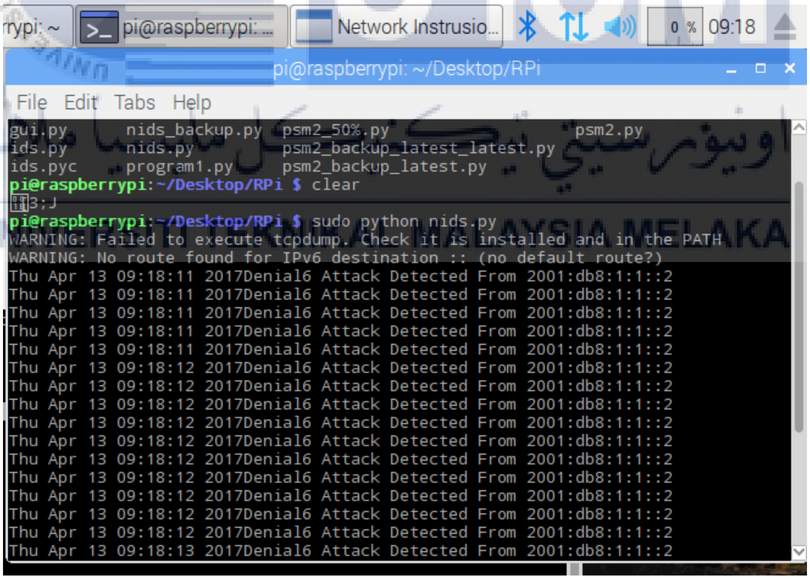
Component 1	:	De-capsulation of tunnel packet
Descriptions	:	The application receives mirrored tunnel traffic. The IPv6 packet is encapsulated in IPv4 packet. The attack is in the IPv6 packet. In order to perform inspection, the tunneled packet is de-capsulated and decoded.
Duration to complete	:	3 weeks
Completion Date	:	24 / 7 / 2017

Component 2	:	Compare to attack signature
Descriptions	:	The IDS type implemented is signature based. The characteristic or the signature of the attack is stored in the application. The captured traffic is compared to the signature.
Duration to complete	:	2 weeks
Completion Date	:	6 / 8 / 2017

Component 3	:	Generate Notification
Descriptions	:	This module generate notification to the user once attack has been detected
Duration to complete	:	1 weeks
Completion Date	:	13 / 8 / 2017

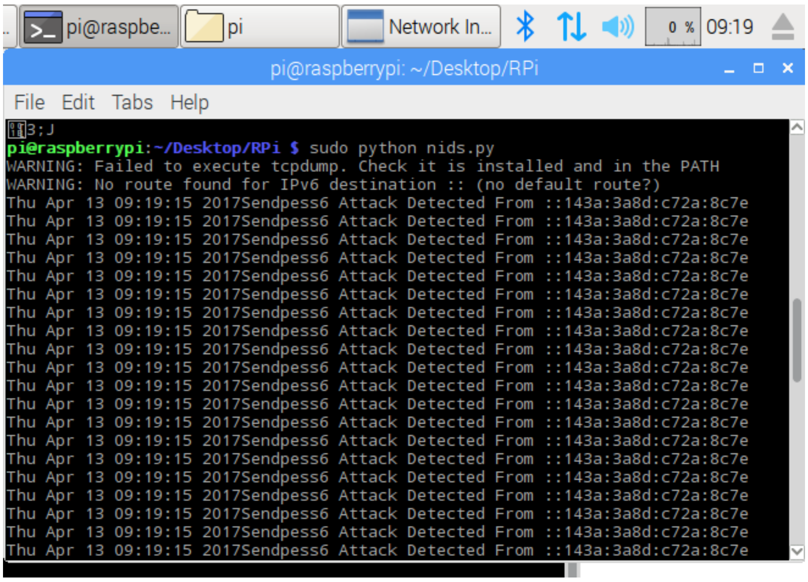
5.5 Result

This section discusses the output of the implementation phase. Figure 5.7 below shows the detection of attack by the IPv6 Transition Mechanism Attack Detector.



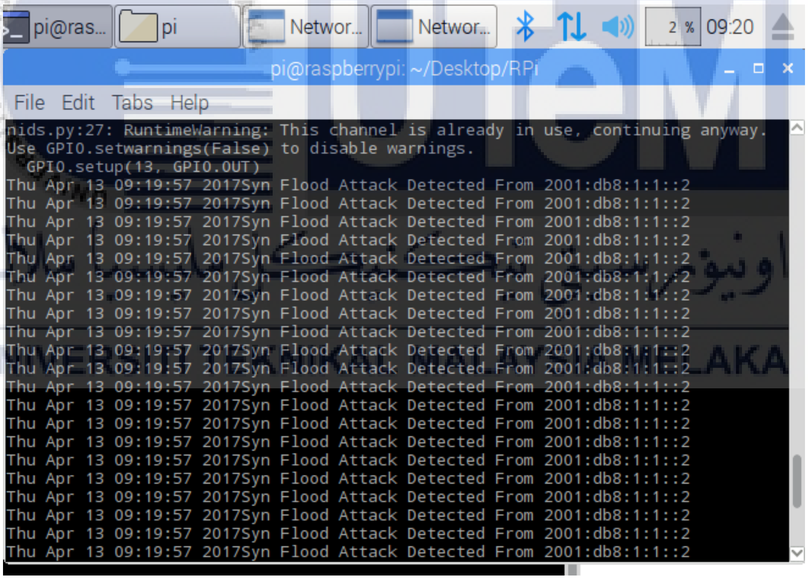
```
gui.py      nids_backup.py  psm2_50%.py               psm2.py
ids.py      nids.py         psm2_backup_latest_latest.py
ids.pyc     program1.py     psm2_backup_latest.py
pi@raspberrypi:~/Desktop/RPi $ clear
▯3;J
pi@raspberrypi:~/Desktop/RPi $ sudo python nids.py
WARNING: Failed to execute tcpdump. Check it is installed and in the PATH
WARNING: No route found for IPv6 destination :: (no default route?)
Thu Apr 13 09:18:11 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:11 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:11 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:11 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:11 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:12 2017Denial6 Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:18:13 2017Denial6 Attack Detected From 2001:db8:1:1::2
```

Figure 5.7: Output Produced by Attack Detector



```
3;J
pi@raspberrypi:~/Desktop/RPi $ sudo python nids.py
WARNING: Failed to execute tcpdump. Check it is installed and in the PATH
WARNING: No route found for IPv6 destination :: (no default route?)
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
Thu Apr 13 09:19:15 2017Sendpess6 Attack Detected From ::143a:3a8d:c72a:8c7e
```

Figure 5.8: Output Produced by Attack Detector



```
nids.py:27: RuntimeWarning: This channel is already in use, continuing anyway.
Use GPIO.setwarnings(False) to disable warnings.
  GPIO.setup(13, GPIO.OUT)
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
Thu Apr 13 09:19:57 2017Syn Flood Attack Detected From 2001:db8:1:1::2
```

Figure 5.9: Output Produced by Attack Detector

Figure 5.7, 5.8 and 5.9 above shows that IPv6 Transition Mechanism Attack Detector able to detect multiple different attacks at the same time.

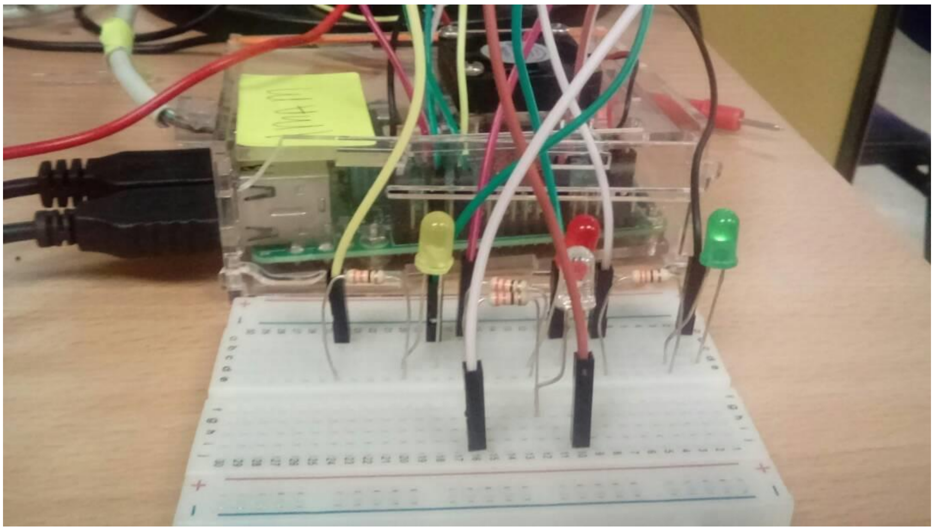


Figure 5.10: Attack Notification using LED

Figure 5.10 above shows the Green LED will turn on after the NIDS system has been turn on.

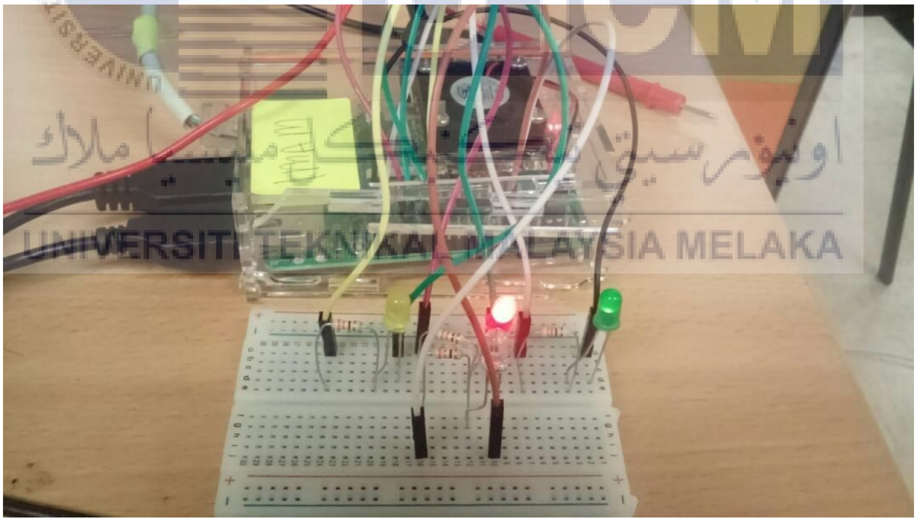


Figure 5.11 Attack Notification using LED

Figure 5.11 above shows the Red LED will turn on after the system has detect the SENDPEES6 attack.

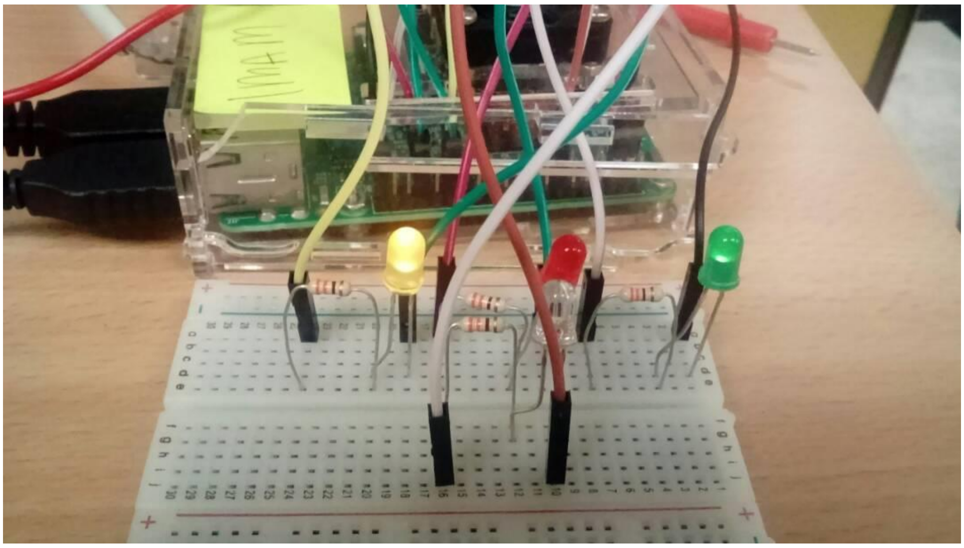


Figure 5.12: Attack Notification using LED

Figure 5.12 above shows the Yellow LED will turn on after the system has detect the DENIAL6 attack.

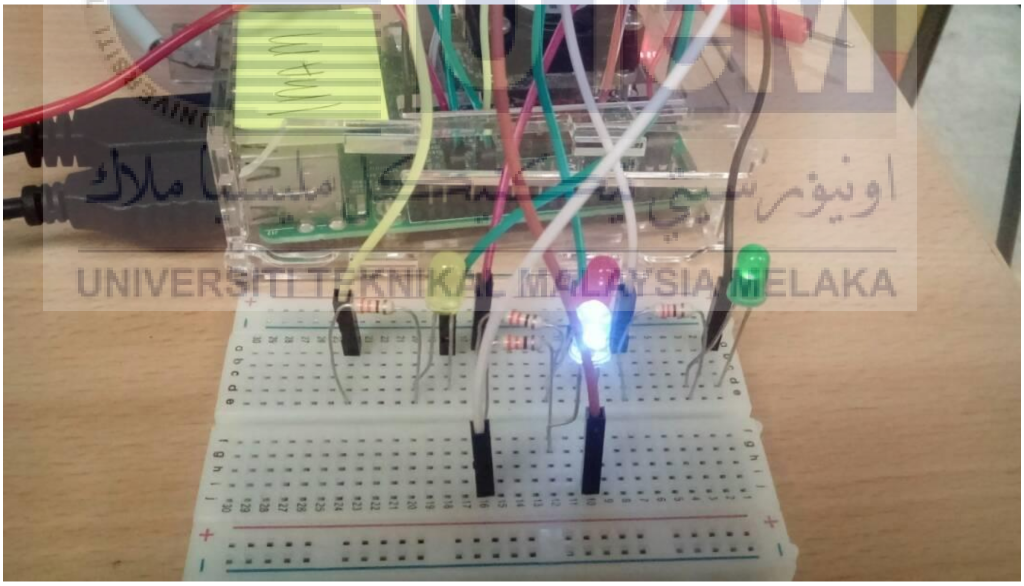


Figure 5.13 Attack Notification using LED

Figure 5.13 above shows the Silver LED will turn on after the system has detect the THCSYN6 attack.

5.6 Conclusion

As a conclusion, this chapter actually carries out a clear idea on how to develop the project, method needed, and proper management techniques. The activity in the implementation phase transforms the output of analysis and design phase into a product that is the IPv6 Transition Mechanism DOS Attack Detector. The environment setup and software environment is based on the testbed design and software design respectively. The next chapter will discuss further on the testing process done to ensure the product meets its requirement and function as intended.

CHAPTER VI

TESTING

6.1 Introduction

In this chapter, all of the results from the testing will presented. This chapter discusses on the testing of IPv6 Transition Mechanism DOS Attack Detector. Testing is carried out to evaluate the developed product with the intent of finding whether the satisfies its objective. Beside, testing helps to identify the errors or defects software. The test strategy employed is black box testing. This chapter covers the test plan, test strategy, test design and the results.

6.2 Test Plan

This section describes the planning on how the testing will be carried out in this project.

6.2.1 Test Organization

Test organization involves deciding on the personnel involved in the testing process and the assignment of responsibilities to each personnel. Test organization ensures systematic delegation of task. Table 6.1 below shows the test organization.

Table 6.1: Test Organization

Tester ID	Title / Position	Responsibilities
Tester 1	System Developer	Develop, document, manage and testing the system. He/she will ensure the system will run smoothly and systematically based on the requirement before delivered the system to the end user.
Tester 2	Project Supervisor	Act as end user for staff and administrator of the system and give their feedback. All the responses will be a guide to enhance the system.

6.2.2 Test Environment

Test environment is the location or the environment of the testing carried out. The testbed designed in Figure 4.4 Network System Architecture during analysis and design phase is used as the testing environment.

6.3 Test strategy

Test strategy defines the method of testing that will be employed in this project. The test strategy selected in this project is black box testing. Black box testing is a testing method used to examine the functionality of the developed software without the need to know about the code structure. Black box testing determines whether the developed software able to produce the required output. This testing strategy is selected because it ensures the development meets its requirement. Figure 6.1 below shows the overview of black box testing.

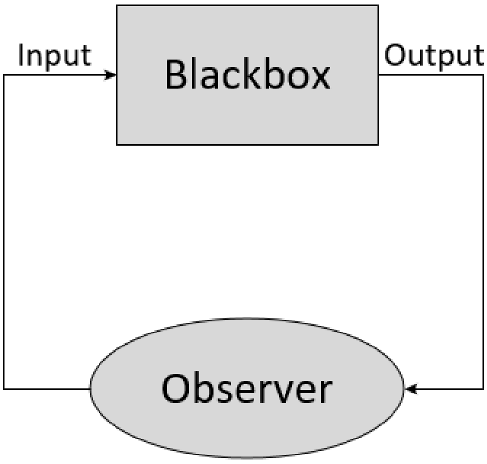


Figure 6.1: Black box testing

6.3.1 Classes of test

There are 2 classes of testing that will carried out namely unit test and functionality test:

i. Unit test

Unit test is the test carried out on individual component of the software by the developer. This test requires understanding of the program code. The aim of the test is to ensure the component is working fine.

ii. Functionality test

Functionality test is carried out to test the functions of the program and determine whether the output produced by the function meets the requirement or doesn't.

6.4 Test Design

This section describes the design of the test being carried in the form of test cases and the expected results.

6.4.1 Test Descriptions

Table 6.2: Testbed connectivity test

Test	Testbed Connectivity Test
Test Case ID	TC01
Test Purpose	Verify design and configuration of the testbed by ensuring there is connectivity between the devices
Test Procedure	Perform ping6 from the attacker to the target network
Expected Result	Successful ping from the attacker to the target network

Table 6.3: Packet Capture Test

Test	Packet capture and decoding test
Test Case ID	TC02
Test Purpose	Verify that the packet capture and decoding component of the program is able to capture packets and decode the packet.
Test Procedure	1. Temporarily code the program to display all the packet received 2. Use ping6 utility to send ICMPv6 packet towards the target network. 3. Use thc-ipv6 tool to send thcsyn6, sendpees6 and denial6 packet towards

	target network 4. Perform multiple attack 5. View the interface and led for the output of captured packet and its decoded contents
Expected Result	All the captured packet and the decoded content is shown in the terminal.

Table 6.4: Signature Matching Test

Test	Signature Matching Test
Test Case ID	TC03
Test Purpose	Verify the developed program able to detect attack launched
Test Procedure	1. Use THC-IPv6 toolkit in the attacker PC to launch DOS attack using thcsyn6 2. Use THC-IPv6 toolkit in the attacker PC to launch DOS attack using sendpees6 3. Use THC-IPv6 toolkit in the attacker PC to launch DOS attack using denial6 4. Check whether the program able to detect the attacks by monitoring output.
Expected Result	Program generate notification when the attack is being carried out detailing the attack and led lamp will turn on based on the attack.

6.5 Test Results and Analysis

This section documents the results of the test cases carried out during the testing phase.

Table 6.5: Testbed Connectivity Test Result

Test	Testbed Connectivity Test
Test Case ID	TC01
Tester	System Developer
Expected Result	Successful ping from the attacker to the target network
Test Results	Success

The successful ping from the attacker shows that the network configurations are correct. ICMPv6 packet were able to traverse the network from the attacker through the IPv4 network cloud using 6to4 tunnel to the target and return. This verifies the operation of 6to4 tunnel.

Table 6.6: Packet capture and decoding test result

Test	Packet capture and decoding test
Test Case ID	TC02
Tester	System Developer
Expected Result	All the captured packet and the decoded content is shown in the terminal
Test Result	Success

The test result shows that the program able to capture the packets from the interface and decode the packet. This test is crucial to ensure that the program able to capture packet and reduce false negative from the attack detector.

Table 6.7: Signature Matching Test Result

Test	Signature Matching Test	
Test Case ID	TC03	
Tester	System Developer / Supervisor	
Expected Result	Program generate notification when the attack is being carried out detailing the attack.	
Result	thcsyn6	Success
	denial6 (2)	Success
	sendpees6	Success
	multiple attack	Success

This test is critical as this is the core function of the IPv6 Attack Detector. The success of this test determines the overall success of this program as it requires each component to work properly.

6.6 Conclusion

In this chapter, testing is demeanour to ensure that the project function fully as mention in objectives and scope. If all the expected output is achieve, the project will be a perfect system that will meet user satisfaction. Overall, process testing shown that the system is running smoothly. Testing is a very important phase as it verifies that the development and setup done during the implementation phase meets the requirement and objective. The functionality of testbed and each component of the attack detector is tested and documented. The next chapter will discuss the conclusion of the project.

CHAPTER VII

PROJECT CONCLUSION

7.1 Introduction

This chapter discusses and conclude overall of this project. This is in fact the last phase of the project where to see if the project fulfils project objectives. The project is summarized by stating its objective and how the objective is achieved. Besides, the contribution of this project and to whom is examined as well as the limitation of the project. Those are all significant to be discuss in order to help improve and contribute in the study and researches of later constructed analysis.

7.2 Project Summarization

IPv6 Transition Mechanism can be exploited to perform attack. Thus the objective of this project is to identify the signature of the possible threats in the transition mechanism. The threats are identified by launching the attack and study the pattern to identify the signature.

Once the attacks signature identified, the second objective which is to develop a tool that can detect the presence of the threat achieved by developing the IPv6 Transition Mechanism DOS Attack Detector. A test bed is designed to meet the third objective which is to test the effectiveness of the tool created.

The strength of this project is that it is capable to detect attacks hidden in the tunnel. The tool able to inspect the IPv6 packet in the payload of IPv4 packet for attack signatures. The weakness of this project is limited number of attack signatures. Besides, the does not have graphical user interface that able to report the detection.

7.3 Project Contribution

The project work made the following main contributions:

i. The project helps organization to minimize the security risk associated by implementing 6to4 IPv6 transition mechanism. The implementation of attack detector prevents attacks to be carried out through the tunnels bypass security layer and go unnoticed by the administrator.

ii. The test bed designed in this project can be used for further development of security mechanism such as improved IDS or firewall. The test bed can be used to simulate real life environment and test the effectiveness of the development.

7.4 Project Limitation

There were some constraints and limitations discussed in the approach about privileges and other minor constraints that may have an effect on the project. The IPv6 attack detector performs its operation by scanning all the traffic that passes through the network at strategically location.

Since the number of packets can be very high and the attack detector need to scan each of the packet, large amount of processing resources is required. The host PC running the attack detector must have enough processing power to cope the demand of the attack detector. Besides the code has to be efficient to ensure it does not consume too much resource.

7.5 Future Works

There are still plenty room for improvement for the IPv6 Transition Mechanism DOS Attack Detector. One of the area of improvement is the user interface to be more user friendly for novice user. The improved user interface should be able to perform analysis on detection and displays the results to the user.

Besides, another improvement that can be make is the better attack notification alert to the user. The improved alert should be able to make user notify attack as fast as possible. It should be done by using combination of current application such as telegram or email.

Furthermore, the detection mechanism of the attack detector can be improved further by combining the current signature based detection with anomaly based detection. The hybrid of signature and anomaly based detection will be able to detect both known and new attacks.

7.6 Conclusion

Finally, the project successfully meets all the objective by the development of the IPv6 Transition Mechanism DOS Attack Detector as well as the design of a test bed. Improvement can be made in the future to make the IPv6 Transition Mechanism more robust and effective. The attack detector can contribute as a security layer when transition mechanism is being implemented while awaiting the rest of the internet to fully migrate to IPv6.

REFERENCES

Bahaman, N., Prabuwono, A. S., & Mas'ud, M. (2011). Implementation of IPv6 Network Testbed. *Journal of Applies Sciences, 11*(1), 118-124.

Çalışkan, E. (2014). *IPv6 Transition and Security Threat Report.* Talinn: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE).

Carpenter, B. (2011). RFC 6343: Advisory Guidelines for 6to4 Deployment. Internet Engineering Task Force.

Carpenter, B., & Moore, K. (2001). RFC 3056: Connection of IPv6 Domains via IPv4 Clouds. Internet Engineering Task Force.

Chown, T., & Venaas, S. (2011). RFC6104: Rogue IPv6 Router Advertisement Problem Statement. Internet Engineering Task Force.

Conta, A., & Deering , S. (1998). RFC 2473: Generic Packet Tunneling in IPv6. Internet Engineering Task Force.

Deering, S., & Hinden, R. (1998). RFC 2460: Internet Protocol, Version 6 (IPv6) Specification. Internet Engineering Task Force.

Dewitz, S. (1996). *Systems Analysis and Design and The Transition to Objects.* New York: McGraw-Hill.

Gilligan, R., & Nordmark, E. (2000). RFC2893: Transition Mechanisms for IPv6 Hosts and Routers. Internet Engineering Task Force.

Hagen, S. (2014). *IPv6 Essentials* (3rd ed.). California: O'Reilly Media.

Hei, Y., & Yamazaki, K. (2004). Traffic analysis and worldwide operation of open 6to4 relays for IPv6 deployment. Tokyo: IEEE Conference Publication.

Huitema, C. (2001). RFC3068: An Anycast Prefix for 6to4 Relay Routers. Internet Engineering Task Force.

Information Sciences Institute, University of Southern California. (1981). RFC 791 : DARPA Internet Program Protocol Specification . Virginia: Internet Engineering Task Force.

Internet Assigned Number Authority. (2016). *Assigned Internet Protocol Numbers*. Retrieved from http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml

Kumar, S. (2007). Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. San Jose: Second International Conference on Internet Monitoring and Protection.

Lau, F., Rubin, S. H., Smith, M. H., & Trajkovic, L. (2000). Distributed Denial of Service Attacks. *IEEE International Conference on Systems, Man and Cybernatics.* Nashville: IEEE.

Lawton, G. (August, 2001). Is IPv6 finally gaining ground? *Computer*, pp. 11-15.

Li, Z., Das, A., & Zhou, J. (2005). Theoretical basis for intrusion detection. New York: IEEE Conference Publication.

Naidu, S., & Patcha, A. (2013). IPv6: Threats Posed By Multicast Packets, Extension Headers. *IOSR Journal of Computer Engineering , 15*(2), 66-75.

Narten, T., Nordmark, E., Simpson, W., & Soliman , H. (2007). RFC4861: Neighbor Discovery for IP version 6 (IPv6). Internet Engineering Task Force.

Perkins, C. (October, 1996). RFC2003: IP Encapsulation within IP.

Piskozub, A. (2002). Denial of service and distributed denial of service attacks. Lviv-Slavsko: IEEE Conference Publication.

Redwan, M., Ramadass, S., & Manickam, S. (2013). Intrusion Detection System in IPv6 Network Based on Data Mining Techniques - Survey. Kuala Lumpur: Institute of Research Engineers and Doctors.

Roesch. (1999). Snort - lightweight intrusion detection for networks. Seattle: USENIX LISA.

Whitman, M., & Mattord, H. (2008). *Principles of Information Security* (3rd ed.). Cengage Learning.

Yu, Z. (2009). Study on Intrusion IPv6 Detection System

Zagar, D., & Grgic, K. (2006). IPv6 Security Threats and Possible Solusions. Budapest: World Automation Congress.

Zulkiflee, M., Robiah, Y., Abu, N., & Shahrin, S. (2012). Improvising Intrusion Detection for Malware Activities on Dual-Stack Network Environment. *World Academy of Science, Engineering and Technology*, *67*, 642-649.