ANALYSIS DENIAL OF SERVICE (FLOOD ATTACK) ON IPV6 NETWORK

MUHAMMAD NAJMI BIN JAMIL

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

BORANG PENGSAHAN STATUS TESIS*

JUDUL: ANALYSIS DENIAL OF SERVICE (FLOOD ATTACK) ON IPV6 NETWORK

SESI PENGAJIAN: **2015/2016**

Saya **MUHAMMAD NAJMI BIN JAMIL**

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 tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
3. ** Sila tandakan (/)

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

(TANDATANGAN PENULIS)	(TANDATANGAN PENYELIA)
Muhammad Najmi Bin Jamil No. 10 Jalan Semangat, Kg Bukit Cerakah 40170, Shah Alam Selangor	En Zulkiflee Bin Muslim
Tarikh: 25 AUGUST 2016	Tarikh: 25 AUGUST 2016

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

ANALYSIS DENIAL OF SERVICE (FLOOD ATTACK)

ON IPV6 NETWORK

MUHAMMAD NAJMI BIN JAMIL

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

FACULTY OF INFORMATION AND COMMUNCATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2016

DECLARATION

I hereby declare that this project research entitled

ANALYSIS DENIAL OF SERVICE (FLOOD ATTACK)

ON IPV6 NETWORK

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

STUDENT : ______________________________ Date: 25 August 2016

(MUHAMMAD NAJMI BIN JAMIL)

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: 25 August 2016

(EN ZULKIFLEE BIN MUSLIM)

DEDICATION

This thesis is dedicated to my parents Jamil Bin Abdul Rahman and Halimah Bintti Lokman. That has risen me since I was young until now. Also to all my siblings that will support me in everything I do Natrah Binti Jamil, Muhammad Nazri Bin Jamil, Najiha Binti Jamil, Najib Bin Jamil, Najuwa Binti Jamil and Nadzirah Binti jamil. Lastly to myself that has been working so hard to finish this thesis.

ACKNOWLEDGEMENTS

Firstly I would like to express my thankful to Almighty God, Allah (S.W.T) only with his will, I'll able to complete this research successfully. I believe all the difficulty has only make me stronger and matured to overcome it in the future. My greatest gratitude to my parents and family that always support me physically and mentally. Always bring me up whenever I'm feeling down. Next, I would like to give infinite of thank you to my supervisor, En Zulkiflee Bin Muslim for all his effort in guiding me to complete this research. He always there to give a help whenever I'm at lost to go on with this project. Also, not forgetting all my lecturer in this university that has taught me so much about networking which is very helpful knowledge for me to use in this research.

ABSTRACT

With the evolution of our technology and widely use of internet, IPv6 was introduce as the internet next-generation protocol that has been design to replace current Internet Protocol which is IPv4. As the nature of our network environment nowadays, there is so many threat occur with the motive of harming the internet. We can call it as network attack. With the various attack that can be done to the IPv4, it seemly the same thing to be occur to IPv6. Therefore, it is important for us o study and get knowledge of those activities so that we will be able to used IPv6 confidently. There is so many network attack that can be listed and one of those is Denial of Service (DoS) attack. This project will focus on DoS attack on IPv6 network by studying the attack patern and packet characteristic. This kind of activities will improve our knowledge about both IPv6 network and network attack so that we can always countermeasure it whenever it occur to our network environment

ABSTRAK

Dengan perkembangan teknologi dan penggunaan internet yang sangat meluas, IPv6 telah diperkenalkan sebagai internet protokol generasi seterusnya bagi menggantikan internet protokol yang digunakan masa kini iaitu IPv4. Lumarah persekitaran rangkain internet masa kini, terlalu banyak ancaman berlaku denagn tujuan merosakkan internet. Perkara ini boleh digelarkan sebagai serangan rangkaian. Dengan pelbagai serangan boleh dilakukan kepada IPv4, perkara sama juga boleh berlaku kepasa IPv6. Oleh sebab itu, adalah penting untuk kita belajar dan memperoleh pengetahuan dalam perkara tersebut agar kita dapat menggunakan IPv6 dengan lebih yakin. Terdapat banyak serangan rangkaian yang di ketahui salah satu daripadanya adalah serangan yg dipanggil Denial of Service (DoS). Projek ini akan mengupas lanjut mengenai serangan DoS degan cara menganalisa corak serangan dan ciri-ciri paket serangan tersebut. aktiviti seperti ini dapat meningkatkan pengetahuan mengenai kedua-dua rangkaian IPv6 dan serangan terhadap rangkaian agar kita dapat melawannya apabila ia berlaku.

TABLE OF CONTENT

CHAPTER **SUBJECT** **PAGE**

DECLARATION **I**

DEDICATION **II**

ACKNOWLEDGEMENT **III**

ABSTRACT **IV**

ABSTRAK **V**

TABLE OF CONTENT **V1**

CHAPTER I: INTRODUCTION

1.1 Introduction 1

1.2 Problem Statement 2

1.3 Research Question 3

1.4 Research Objective 4

1.5 Project Scope 5

1.6 Project Contribution 5

1.7 Thesis Organization 5

1.8 Summary 7

CHAPTER II: LITERATURE REVIEW

2.1 Introduction 8

2.2 Related work 9

2.2.1 IPv6 9

2.2.1.1 IPv6 Addressing Format 10

2.2.1.2 Type of IPv6 Address 10

2.2.1.3 Goals of IPv6 10

2.2.1.4 IPv6 header 11

2.2.1.5 IPv6 Vulnerability 12

2.2.1.6 IPv6 Threat 13

2.2.2 Protocol 14

2.2.2.1 ICMPv6 14

2.2.2.2 TCP 14

2.2.2.2 UDP 14

2.2.3 Network Attack Taxonomy 15

2.2.4 Type of Network Attack 16

2.2.4.1 Denial of Service (DoS) Attack 16

2.2.4.2 Distributed Denial of Services (DDoS) 17

2.2.4.3 Man-In-The-Middle 18

2.2.4.4 Attack under DoS 19

2.2.5 Other DoS attack 20

2.2.6 Previous Research 21

2.3 Justification 21

2.4 Proposed Solution 22

2.4.1 Hardware 22

2.4.2 Software 23

2.5 Summary 23

CHAPTER III: PROJECT METHODOLOGY

3.1 Introduction 24

3.2 Project Methodology 26

3.3 Milestone 27

3.4 Project Gant Chart 29

3.5 Summary 29

CHAPTER IV: DESIGN

4.1 Introduction 30

4.2 Network System Architecture 31

4.3 Physical and Logical Design 32

4.3.1 Logical Design 33

4.3.2 Physical Design 34

4.4 Possible Scenario 34

4.4.1 First Scenario 35

4.4.2 Second Scenario 35

4.4.3 Third scenario 36

4.5 Metric Measurement 36

4.6 Summary 36

CHAPTER V: IMPLEMENTATION

5.1 Introduction 37

5.2 Environment Setup 38

5.2.1 Phase I: Obtaining Dataset 38

5.2.2 Phase II: Organize Data 39

5.2.3 Phase III: Differentiate and Analysis Data 42

5.3 Destination Address Graph 43

5.3.1 Normal Traffic 43

5.3.2 ICMP flood attack (smurf6) Traffic 44

5.3.3 TCP Flood Attack (Alive6) traffic 45

5.3.4 UDP Flood Attack (Alive6) Traffic 46

5.4 Graph of Protocol Type 47

5.4.1 Normal Traffic 47

5.4.2 ICMP flood attack (smurf6) Traffic 48

5.4.3 TCP Flood Attack (Alive6) Traffic 49

5.4.4 UDP Flood Attack (Alive6) Traffic 50

CHAPTER IV: TESTING AND ANALYSIS

6.1 Introduction 51

6.2 Results and Analysis 52

6.2.1 Measurement 1: Number of Packet 53

6.2.2 Measurement II: Protocol Type 54

6.2.3 Measurement III: Packet Frequency on Destination Address 56

6.2.4 Measurement IV: Frequency and Number of Packets 58

6.3 Analysis 60

CHAPTER IIV: CONCLUSION

7.1 Introduction 61

7.2 Project Summarization 61

7.3 Project Contribution 62

7.4 Project limitation 63

7.5 Future Work 63

7.6 Conclusion 63

REFERENCES 64

LIST OF FIGURE

Figure 2.1: IPv6 Header Structure 11

Figure 2.2: Network Attack Taxonomy 15

Figure 2.3: How DoS Attack Work 16

Figure 2.4: DDoS Attack Concept 17

Figure 2.5: Man-In-The-Middle Concept 18

Figure2.6: Smurf Attack Concept 19

Figure 3.1: Methodology Phase Flow 25

Figure 3.2: Project Gant Chart 29

Figure 4.1: Network Design 31

Figure 4.2: Logical Design 33

Figure 4.3: Physical Design 34

Figure 5.1: Obtaining data Flow Chart 38

Figure 5.2: Wireshark Captured of Normal Traffic 39

Figure 5.3: Data Collection Flow Chart 40

Figure 5.4: Data Convert to Excel 41

Figure 5.5: Differentiate and Analysis Data Flow Chart 42

Figure 5.6: Normal traffic graph by destination 43

Figure 5.7: Smurf6 traffic graph by destination 44

Figure 5.8: TCP flood traffic graph by destination 45

Figure 5.9: UDP flood traffic graph by destination 46

Figure 5.10: Normal traffic graph by destination 47

Figure 5.11: Graph for Smurf attack by Protocol 48

Figure 5.12: Graph for TCP flood attack by Protocol 49

Figure 5.13: Graph for Smurf attack by Protocol 50

Figure 6.1: Graph No. of Packets per Traffic by Specific Duration 53

Figure 6.2: Graph No of Packets by Protocol 55

Figure 6.3: Graph Normal, TCP and UDP by Destination 56

Figure 6.4: Smurf6 Graph by Destination 57

Figure 6.5: Graph Packet Frequency by No. of Packets 58

Figure 6.6: Graph Comparison Packet Frequency by No. of Packets 59

LIST OF TABLE

Table 1.1: Problem Statement 2

Table 1.2: Research Question 3

Table 1.3: Research Objective 4

Table 1.4: Project Contribution 5

Table 3.1: Milestone 27

Table 6.1: Data Taken for Analysis Process 52

Table 6.2: Number of Packets for different traffic 53

Table 6.3: Type of protocol 54

Table: 6.4 Analysis Table 60

CHAPTER I

INTRODUCTION

1.1 Introduction

With the evolution of our technology and widely use of internet, IPv6 was introduce as the internet next-generation protocol that has been design to replace current Internet Protocol which is IPv4. As the IPv6 has not been fully implement on the internet, there are hugely activities run by network professionals to analyze and detect the vulneberity of the new version so that it can always be improve from time to time.

One of the most important to be analyze is the security aspect. With the various attack that can be done to the IPv4, it seemly the same thing to be occur to IPv6. Therefore, it is need for us to study those kind of activities so that we will be able to used IPv6 confidently. There are many types network attack now adays such as reconnaissance attack, Denial of Service attack (DoS), men-in-the-middle attack and a many more. The type of attack that will be focused in this project is Flood Denial of Service attack

Denial of service was considered as the most famous network attack. It has been occur so many times and causing huge trouble in an IPv4 network. However, DoS attack still not new to IPv6, there is been activities of DoS attack in IPv6 network that has been spotted even though it not as much as in IPv4. With those being said, it is believe to be only the matter of time before it is become so huge like what happen to the version of IPv4.

There is many type of attack that can be done under Denial of Service such as UDP flood attack, ping flood attack, smurf attack, fraggle attack, Syn flood attack, and many more. There will be three selected DoS attack that will be used in this project which is based on Flooding attack. First is ICMP flood, UDP flood and TCP flood

1.2 Problem Statement

Table 1.1: Problem Statement

No	Problem Statement
PS1	Feeling unsecure to use IPv6 network because of increasing number of attack to harm and threat the vulnerability of IPv6
PS2	Lack of knowledge about IPv6 network attack cause the detection rate is ineffective

PS1: Feeling unsecure to use IPv6 network because of increasing number of attack to harm and threat the vulnerability of IPv6

There are few problem statement in this project which is first, Feeling unsecure to use IPv6 network because of increasing number of attack to harm and threat the vulnerability of IPv6. There are many hacker trying to manipulate the vulnerability of IPv6 with the bad purposes.

PS2: Lack of knowledge about IPv6 network attack cause the detection rate is ineffective

Second problem statement is Lack of knowledge about IPv6 network attack cause the detection rate is ineffective. There is so many type and categories of network attack, so it is important to have knowledge about it.

1.3 Research Question

There are few research question in this project. First, what technique or method used by attacker to DoS attack IPv6 network? Second, what is pattern and behaviour of each DoS attack that been used? Lastly, what is the different on the traffic between each of DoS attack and normal traffic?

Table 1.2: Research Question

PS	PQ	Project Question
PS1	PQ1	What type of attack that can be done to IPv6 network?
PS2	PQ2	What is pattern and behavior of each Flood DoS attack
	PQ3	What is the different on the traffic between each of Flood DoS attack and normal traffic?

1.4 Research Objective

Research objective were determined by referring to the research question. In this project, there will be three research objective. First,

Table 1.3: Research Objective

PS	PQ	PO	Project Objective
PS1	PQ1	PO1	To study technique and method used to attack IPv6 network
PS2	PQ2	PO2	To analyze the pattern and behaviour of each flood DoS attack
	PQ3	PO3	To differentiate flood dos attack traffic and normal traffic

PO1: To study technique and method used to attack IPv6 network

To analyze pattern of flood DoS attack, it is important to know the method and technique to attack first.

PO2: To analyse the pattern and behaviour of each flood DoS attack

Analysing based on the traffic and packet to determine the pattern and behaviour of the attack

PO3: To differentiate flood DoS attack traffic and normal traffic

After analysing the attack packet and normal packet. Make a comparison between them to see the differences.

1.5 Project Scope

The scope in this research project will focusing on these issue:

- This research will only using IPv6 network environment with no involvement of IPv4 network
- Research will focusing on Denial of Service attack only
- Few tools provided by The hacker's choice were used to launch the attack
- Tcpdump and Wireshark were used as sniffer tools

1.6 Project Contribution

This project research should have it contribution that can be used for future research.

Table 1.4: Project Contribution

PS	PQ	PO	PC	Project Contribution
PS1	PQ1	PO1	PC1	Classification type of DoS attack on the network
PS2	PQ2	PO2	PC2	Proposed a characteristic about DoS attack on IPv6 network.
	PQ3	PO3	PC3	Give a technique to be used to detect DoS attack in IPv6 network

1.7 Thesis Organization

Chapter I: Introduction

This chapter explain about overall important aspect in this research project including problem statement, research question, research objective, research scope, project contribution, thesis organization and lastly conclusion.

Chapter II: Literature Review

In this chapter, summarization about all the related work and previous research about ipv6 and network are stated and being review. Other than that, the way of this research will be handle and proposed solution about project will be explained

Chapter III: Project Methodology

In this chapter, summary about project methodology that will be used in this project will be explained. All the phase that involved in completing this project will each be explained briefly.

Chapter IV: Design

In this chapter, summary about design that will be used in this project will be explained. All the network and system architecture in this project including hardware and software used will be justified. Other than that, all the possible scenario related to the project will also be explained in this chapter.

Chapter V: Implementation

This chapter will be explained about the setup of the real network environment based on design that has been completed in the previous chapter.

Chapter VI: Testing and Analysis

In this chapter, project will be on implement the attack to the network environment that has been created. The data will be collected and analyse based on requirement of the research objective to get the final result.

Chapter VII: Project Conclusion

In this chapter researcher will explain about overall result that were gained by doing this research and give their perspective view whether this project are meet the project objective.

1.8 Summary

In this chapter, all the information needed for this project are being clearly identified and explained. In the next chapter, it will be on literature review of the project and related work for the project

CHAPTER II

LITERATURE REVIEW

2.1 Introduction

In chapter 2, we will discuss about literature review of the project about overall network attack on IPv6 generally and focusing on IPv6 vulnerability, threat and attack alongside the tools to be used in this project. The end result of literature review will be used as a guideline to setup the network environment to carry out the project and fulfilled the research objective which is to study technique and method used to attack IPv6 network. Second, to analyse the pattern and behaviour of flood DoS attack and lastly to differentiate flood DoS attack and normal attack.

2.2 Related work

2.2.1 IPv6

IPv6 stand for Internet Protocol Version 6, is the most recent version of the internet protocol after the previous version IPv4. It was developed and introduced by The Internet Engineering Task Force (IETF), the organization that is responsible to handle about the Internet Protocol standards. With the rapid growth of the Internet after being commercialize in the 1990s, it become clear that even the large number of IPv4 are still not enough to patch the capacities of the growing internet and more IP addresses is needed to connect with new devices in the future.

Main features in IPv6 is, it is an internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP network. IPv6 has large addressing space which is 128 bits compared to only 32 bits in IPv4. This means IPv6 has total of 18,446,744,073,709,551,616 IP addresses in a single /64 allocation while IPv4 has 4,294,967,296 IP addresses (Hurricane Electric).

IPv6 accessibility relies on upon your Service Provider, either at home or for work. In a dual stack environment, IPv4 and IPv6 coincide along the same association and don't require any uncommon sort of connection. In the event that dual stack is not accessible, you may wind up utilizing an IP tunnelling item or administration to convey IPv6 availability to you. Despite the fact that IPv4 exhaustion has happened at IANA, IPv4 won't just vanish off the substance of the Internet, yet proceeded with hazardous development requiring more one of a kind IP address assignments will mean utilizing increasingly of the bottomless IPv6 address space.

2.2.1.1 IPv6 Addressing Format

2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456

- 16-bit numbers of hexadecimal
- The numbers separated by (:) symbols
- The hexadecimal numbers are not case sensitive

Example:

2001:0DBB:AC10:FE01:0000:0000:0000:0000

(Zero can be omitted)

2001:0DBB:AC10:FE01::

2.2.1.2 Type of IPv6 Address

i. Unicast Address

- Single interfaces. A packet is delivered to one interfaces.

ii. Multicast Address

- Set of interfaces. A packet is delivered to multiple interfaces.

iii. Anycast Address

- Set of interfaces. A packet delivered to the nearest of multiple interfaces.

2.2.1.3 Goals of IPv6

- Enough IP address for the next decades
- Auto configuration of IP address and networking
- Hierarchical address structure
- Integrated security features

2.2.1.4 IPv6 header

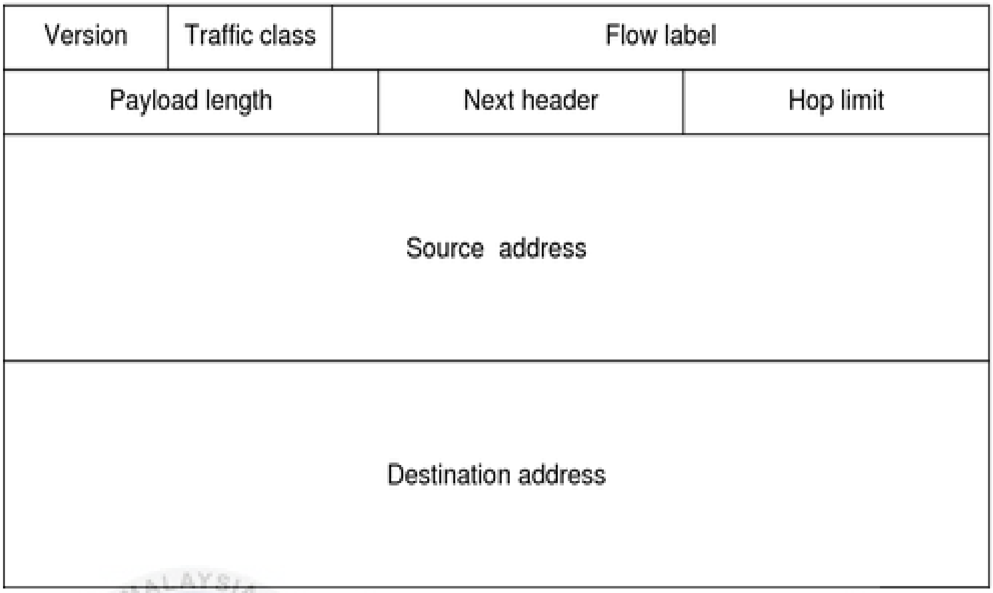


Figure 2.1: IPv6 Header Structure

Description

Version (4 bits) represent the version number of internet protocol**. Traffic Cla**ss (8 bits) divided into two parts. 6 bits were used for Type of Service to inform router what services should be provided for the packet. The other 2 bits are used for Explicit Congestion Notification (ECN).

Flow Label (20 bits) used to maintain sequence flow of packets that belong to a communication. This will help router to recognize the packet belongs to specific flow of information**. Payload Length** (16 bits) function to tell routers how much information a packet contains in its payload

Next Header (8 bits) used to point out the type of extension header. If the Extension Header des not present then it will point to the **Upper Layer** PDU.Hop Limit (8 bits) function to stop loop of packet from happen in the network endlessly. Source Address (128 bits) provides the address sender of the packet. Lastly, **Destination Address** (128 bits) indicates the address of the intended receiver of the packet

2.2.1.5 IPv6 Vulnerability

IPv6 was created in the mid-90s in which at the time IPv4 still being used without a concern of exhausted like what happen today. At that time many security vulnerability of IPv4 still not fully identified and fixed. Even IPv6 known as next generation of IP address, it's still function pretty much the same as IPv4. In that fact it is believe the same attack on IPv4 can still be used to IPv6 network with a little adjustment of the attack.

IPv6 often being considered more secure than IPv4 because of the inclusion of IPsec in IPv6 specification (Kent and Atkinson 1998). That fact was agreed by John Spence, of Nephos6 in his statement that "Much of the early thinking that IPv6 security was better than IPv4 based on the Request for Comment (RFC) requirement that IPv6 stacks include IPsec support, but that is clearly too simple as a reason.

Although IPv6 has improvement in security aspect, it is still vulnerable in the network environment because it is considered immature compared to IPv4. IPv6 was called immature because of the fact that it was not fully used as main Internet Protocol so the security has not yet been tested and confirmed. Compared to IPv4 that has been used so many years, we know the limitation of its security and vulnerability. We wouldn't know our real capability if we not fully know our weaknesses. That is the case to the IPv6, there will always be some unsure and unsecure until we really sure the limitation of its security. That is something that can be achieved by researching and testing and as we know for that purposes, many security and networking expert either personal or organizations has been working out for so many years.

Throughout the advancement of the new Internet Protocol variant, changes in and supplements to usefulness were made. These upgrades, be that as it may, yield diverse conduct Furthermore, in this manner regularly bring about novel security vulnerabilities. There is few Vulnerabilities of IPv6 that can be list out. Johanna Ullrich and her co-member of SBA Research has state in their research about security vulnerability of IPv6 that are listed below (Johanna Ullrich. IPv6 Security: Attacks and Countermeasures in a Nutshell)

List of IPv6 vulnerability

- Extension Headers
- Fragmentation
- Mandatory IPv6 Header Fields
- Neighbor Discovery
- Multicast Listener Discovery
- Tunneling
- Address Space Size
- Mobile IPv6

2.2.1.6 IPv6 Threat

As we know, the immature of IPv6 security. The gateways are vulnerable because of the amount of information and data they holding. Internet of Things (IoT) will present hackable devices to the scene. All things considered, it is an absolute reason for us to be worry (IPv6 and the growing DDoS, Danger Rene Paap, February 2015)

In the first quarter of 2015 of its Internet security report, Akamai Technologies has state that they have found that DDoS attack were up generally. To make things worse, it is up dramatically. The firm observed that attack were twice compared to quarter of the year-back and rose 35 percent contrasted with the past year.

2.2.2 PROTOCOL

2.2.2.1 ICMPv6

The Internet Control Message Protocol (ICMP) is a protocol used as a helper. It support Internet Protocol (IP) for simple queries and error reporting.

2.2.2.2 TCP

The Transmission Control Protocol is a core or main protocol in the internet protocol suite. It is connection oriented that's make it reliable through three way hand-shake process.

2.2.2.3 UDP

User Datagram Protocol (UDP) is also one of core protocol in internet protocol suite. It is connectionless type of connection that make faster but quite unreliable

2.2.3 Network Attack Taxonomy

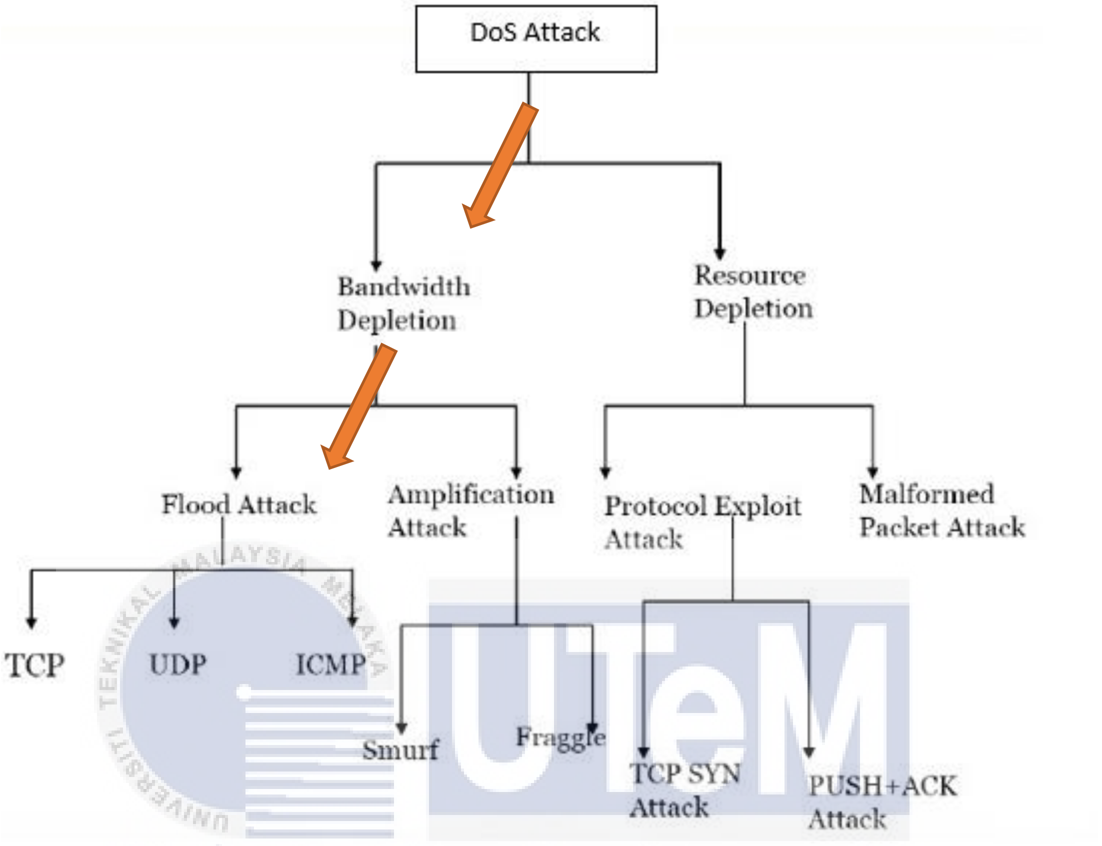


Figure 2.2: network Attack Taxonomy

Taxonomy Description

Figure 2.2 shows DoS Network attack taxonomy, DH Nong Lam TP.HCM (2008). Based on taxonomy that has been stated, this research will follow covered Flood attack which is under Bandwidth Depletion type attack. In flooding attack there is three type of attack that can be done which is TCP flood, UDP flood and ICMP flood.

2.2.4 Type of Network Attack

When we talk about attack on the network environment, there is hundreds if not thousand type of network attack that has been occurred. At the very high level, network attack can be divided into two categories which is: host-based attack and traffic flow based attack. Host-based is alludes to any device that depends on the host PC (that is, the PC the device is connected to) to handle or control a few operations.

The focus of IPv6 attack in this writing is on traffic flow based attack because it is more related to the research. There is many types of network attack on flow based traffic such as reconnaissance attack, denial of service attack, network worm attack, man-in-the middle and many more. (Muhammad Fermi Pasha1, (2001). IPv6 Traffic Flow Security Threats and Trend Analysis: Towards Combined Intelligent Detection Approach)

2.2.4.1 Denial of Service (DoS) Attack

Victim Machine

Figure 2.3: How Dos Attack Work

Denial-of service (DoS) attack is an attack to make a computer machine or network resources not function as supposedly by its intended user. It will make the system or computer interrupt or suspend services temporarily until it is terminated or stopped. DoS attack are one of the most used attack in the internet nowadays because it is easy to execute but it is difficult to destroy or eliminate. DoS attack nature is it was a simple attack with a only a few command to launch it but it is attack that target the system or network resources usually by sending huge fake request for the system to respond resulting a system or network to be hang or down.

2.2.4.2 Distributed Denial of Services (DDoS)

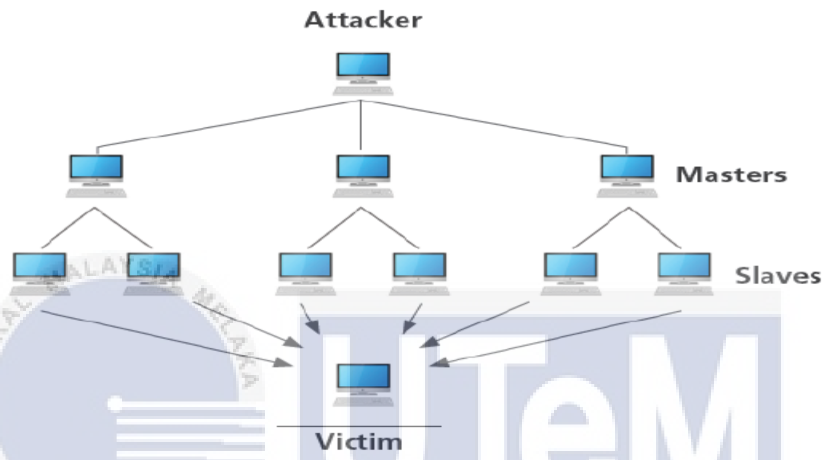


Figure 2.4: DDoS Attack Concept

A distributed-denial-of-service (DDoS) is extended/ new form of DOS in which the source of the attack is more than one and possibly thousands of different IP address. Therefore even the type of attack were same but the result and effect are so much worse than normal DoS attack.

In a DDoS attack, a hacker has remote control of hundreds of computers over a large geographical area and commands them to send false requests to a Internet device such as Web browser

2.2.4.3 Man-In-The-Middle

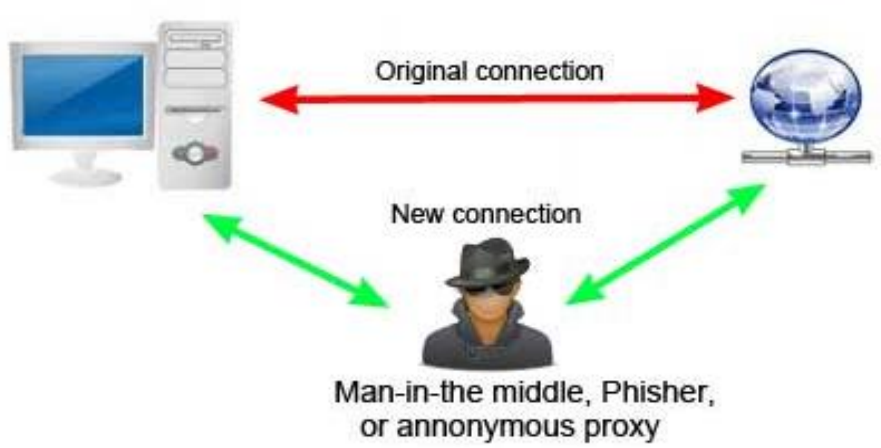


Figure 2.5: Man-In-The-Middle Concept

Man-in-the-middle-attack is an attack where a hacker gets between the sender and receiver of information and sniff any information being sent. The data may be encrypted or unencrypted. If it is encrypted data, hackers need to unencrypt the data first before it can be able to read.

- A type of intrusion involves the theft of network data
- If hackers find a working user ID and password, they can sign onto the network and appear as a legitimate user
- Hackers also try to intercept data (e-mail, files, chat dialogs and data packages) as it is transmitted across the LAN, an attack known as main in the middle.

2.2.4.4 Attack under DoS

Smurf Attack

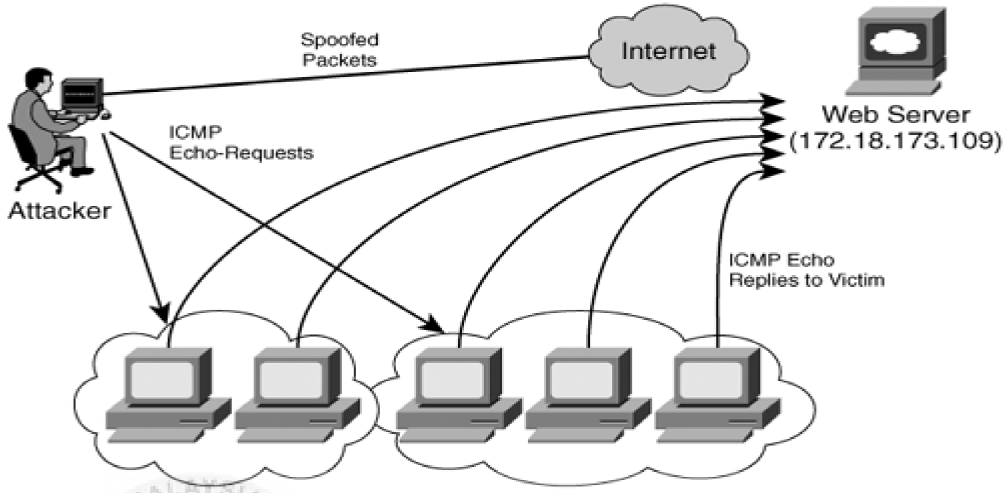


Figure2.6: Smurf Attack Concept

Smurf attack is categories as Denial of Service attack, it function by broadcasting fake ICMP echo request to a network using the IP address from of the victim. This behaviour will cause all computer device in the same network to reply the request to the source address which is the victim address. Victim machine will be overwhelming with ICMP echo reply from all the computer and make the victim machine to become slow or hang or even shutdown because if it can handle the process.

Flood Attack

By Protocol

Flood attack work by sending large amount of packet to the network or specific target. It is very easy to execute but has big impact. In the large amount of packet that are sending to the network, we can specify to flood the network by protocol such as ICMP packet, TCP packet or UDP packet.

On Router

Flood router is an attack that are created and design to exploit a vulnerability of IPv6 network. It is type of attack that sending large amount of router advertisement (RA) to the overall network or selected host. This attack were using an Internet Control Message Protocol version 6 (ICMPv6) protocol

2.2.5 Other DoS attack

Ping of Death

Ping of dead is a variation of ping flooding. It uses the ping protocol to send a abnormal packet that is larger than 65,536 bytes allowed by the IP protocol. Some or most computer device or system are unable to effectively handle a ping packet that are larger than the normal maximum size of the packet. When the victim receive the packet, it will become overflow and can cause the pc to hang or crash.

SYN Flooding

In SYN flood attack, it function by exploiting TCP three way handshakes. Attacker will send multiple request by false or invalid IP which actually cannot be access to the target server. This handshake process will not complete because the host will never reply or respond to the ACK. If this process continue the server will finally runs out of it resources and eventually cannot respond the ACK when the valid host send a request.

2.2.6 Previous Research

This section will explain about the previous work that are related to IPv6 attack that has been done such as technique that they use, hardware and software.

In the previous work that I found, they are doing the research by using technique. Simulation and can be setting as real environment situation**.** This technique are beneficial for the research without having to harming or effect the real network in order to launch the attack and gathering the data. It is also saving more cost compared to have to buy expensive hardware to setup private network for research purposes.

For the hardware, simulation only needed one computer device to make it work. They need a few software to be install to the computer in order to setup the simulation. The software that were used such as Virtual machine. Virtual machine were used to install multiple Operating system in one device. Other than that, they need software like packet tracer or GNS3 to setup a network environment. Sniffing software used to captured data and packet such as Wireshark and TCPdump.

For the type of attack, the researcher using one of DoS attack which is flood router and comparing them with normal data.

2.3 Justification

Based on previous research, this project will also do DoS attack which is flooding attack. Instead of only one type of attack on previous research which is flood router, this research project will do three type of attack which is ICMP flood, TCP flood and UDP flood.

The type of attack that the previous research select is attack that attacking the network itself but for this research project the type of attack selected is attacking the host and not network. And lastly, the previous research are using simulation to get the data. Instead of that, this project will using real network environment that is setup inly for this purposed and will not harming other network

2.4 Proposed Solution

This section will explained about technique that will be used for this project. Technique that are used maybe different from the previous research.

The technique that will be used in this project is by using real network environment. Network will be setup using required hardware and software and then the scenario will be run to the environment.

2.4.1 Hardware

Router

This project will be using two Cisco router to be implement to the network in order to connect between two network

Switch

Two Cisco switch will be used to connect multiple pc in two different network. This switch then will be connected to the router to complete the network environment.

2.4.2 Software

THC IPv6 Toolkit

THC is stand for The Hacker’s Choice. It is a non-commercial group of international security researchers and hackers that provide tools to test a network. THC provide various type of tools for different type of attack especially for testing IPv6 network.

Kali Linux

Kali linux is an operating system, it is one of Debian-based linux that are mainly purposes of security and panetration testing. Kali linux contain hundreds of tools inside it for variety security task.

2.5 Summary

As the conclusion, the literature review topic discuss about all the information that are related to the project research. IPv6 vulnerability, IPv6 threat, type of network attack and all important information were found from previous work. This is important especially for the researcher to carry on the project using all the information gathered in this chapter.

CHAPTER III

PROJECT METHODOLOGY

3.1 Introduction

In this chapter detail about methodology used in this project will be explained. The purpose of project methodology is to make sure research of the project can be done in the proper way and correct sequence. This is important so that the conducted project can be completed successfully on time. There is total of 6 phases that will be explained in this project methodology which is literature review (Phase 1), analysis (Phase 2), design and development (Phase 3), implementation (Phase 4) and lastly testing and evaluation (Phase 5).

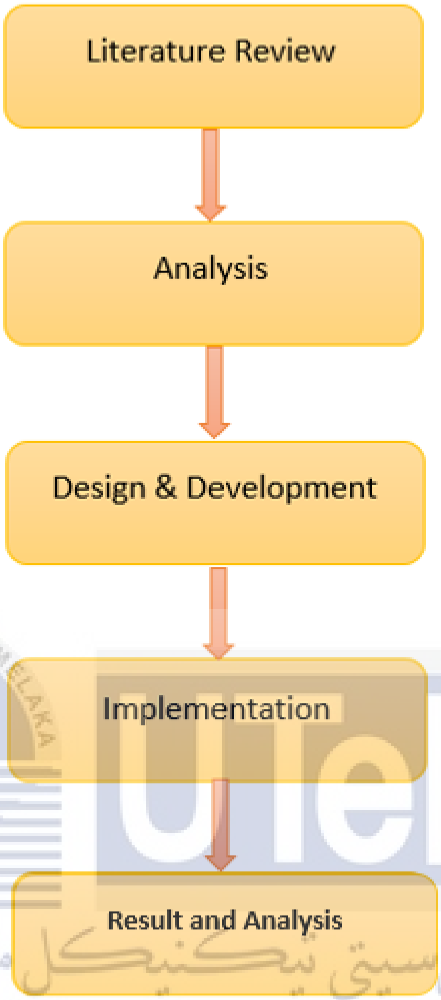


Figure 3.2: Methodology Phase Flow

3.2 Project Methodology

Phase 2: Literature Review

In literature review, all information and related work needed to do the research need to be finish. Detail about IPv6 network such as IPv6 architecture, IPv6 vulnerability, type of IPv6 address and many more. Also information and related work about network attack such as, type of attack and tools that will be used will be explained. All of the information in this phases was needed to carry on the next phase, analysis phase.

Phase 2: Requirement Analysis

In requirement analysis, detail of software and hardware that are used for the research purposed were listed. This phase important to make sure that all the process to get data or information for the research can be done successfully. Requirement analysis also important and related to the next phase, design and development

Phase 3: Design and Development

In this phase, network design such as physical design and logical design will be introduced. The design must be appropriate to easier the process of implementation later. Example of network design are shown below.

Phase 4: Implementation

In implementation phase, the design that has been done in the previous phase will be used and implement it in the real environment using all hardware and software needed.

Phase 5: Testing and Evaluation

In this phase, a 3 series of attack will be launch to see and find the effect of each attack to the IPv6 network. All the packet and data will be captured using specific software. All collected data will be analysed and the result will be documented and be evaluate. Submission of full report will be done showing that the project has been completed

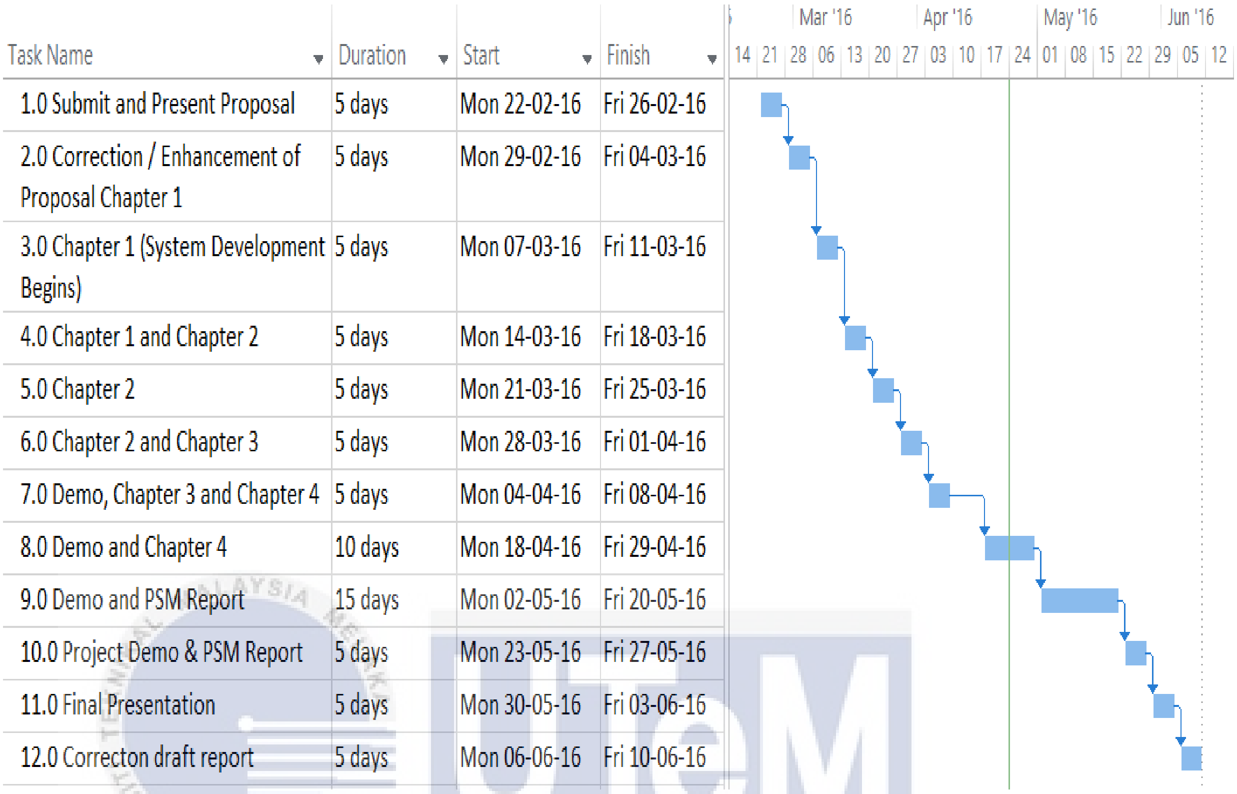
3.3 Milestone

Table 3.1: Milestone

Week	Activity
1 22-26 Feb	Proposal PSM: Submission & Presentation
	Proposal assessment and verification
2 29 Feb- 4 Mar	Proposal Correction/Improvement Chapter 1
	List of supervisor
3 7-11 Mar	Chapter 1 (System Development Begins)

4 14-18 Mar	Chapter 1 & Chapter 2
5 21 – 25 Mar	Chapter 2
6 28 Mar – 1 April	Chapter 2 Chapter 3
	Student Status
7 4-8 April	Project Demo & Chapter 3 Chapter 4
8 18 -22 April	Project Demo & Chapter 4
9 25-29 April	Project Demo & Chapter 4
10 2-6 May	Project Demo
11 9-13 May	Project Demo & PSM Report
12 16 – 20 May	Project Demo & PSM Report
	Presentation Schedule
13 23 – 27 May	Project Demo & PSM Report
14 30 May – 3 June	FINAL PRESENTATION (PA)

g3.4 Project Gant Chart



Task Name	Duration	Start	Finish
1.0 Submit and Present Proposal	5 days	Mon 22-02-16	Fri 26-02-16
2.0 Correction / Enhancement of Proposal Chapter 1	5 days	Mon 29-02-16	Fri 04-03-16
3.0 Chapter 1 (System Development Begins)	5 days	Mon 07-03-16	Fri 11-03-16
4.0 Chapter 1 and Chapter 2	5 days	Mon 14-03-16	Fri 18-03-16
5.0 Chapter 2	5 days	Mon 21-03-16	Fri 25-03-16
6.0 Chapter 2 and Chapter 3	5 days	Mon 28-03-16	Fri 01-04-16
7.0 Demo, Chapter 3 and Chapter 4	5 days	Mon 04-04-16	Fri 08-04-16
8.0 Demo and Chapter 4	10 days	Mon 18-04-16	Fri 29-04-16
9.0 Demo and PSM Report	15 days	Mon 02-05-16	Fri 20-05-16
10.0 Project Demo & PSM Report	5 days	Mon 23-05-16	Fri 27-05-16
11.0 Final Presentation	5 days	Mon 30-05-16	Fri 03-06-16
12.0 Correcton draft report	5 days	Mon 06-06-16	Fri 10-06-16

Figure 3.2: Project Gant Chart

3.5 Summary

As the conclusion, in this chapter project methodology, discussion and clarification about all the phases to complete this project is done. The phase that are stated must be relevant and appropriate in considering all the aspect including software and hardware requirement. Most important is to follow project milestone and project gant chart so that the project will be completed as planned in the schedule.

CHAPTER IV

DESIGN

4.1 Introduction

In this chapter, details about design of the project will be shown and explained. As we need to build a real environment of network to launch attack and collect data to fulfil project objective, design are very important so that process of creating the real environment are easier. Furthermore, in this chapter requirement analysis also will be explained. Requirement analysis was needed for the purposed of selecting the right equipment that are suitable to be used in the project. Hardware and software requirement are important factor that need to be check so that all the equipment can work and function properly according to the design.

4.2 Network System Architecture

For this project's system architecture, 3 PC will be used along with 2 router and 2 switch. Few types of cable also will be used to connect all the device and forming a complete network. 7 straight-through cable are used to connect between PC to switch and switch to router and one cross-over cable were used to connect between two routers. There is also a laptop that will be used as a client. All of this hardware will be used to setup only an IPv6 network which means there is no IPv4 configuration at all. In the environment that are created, there will be two different network which is inside network and outside network

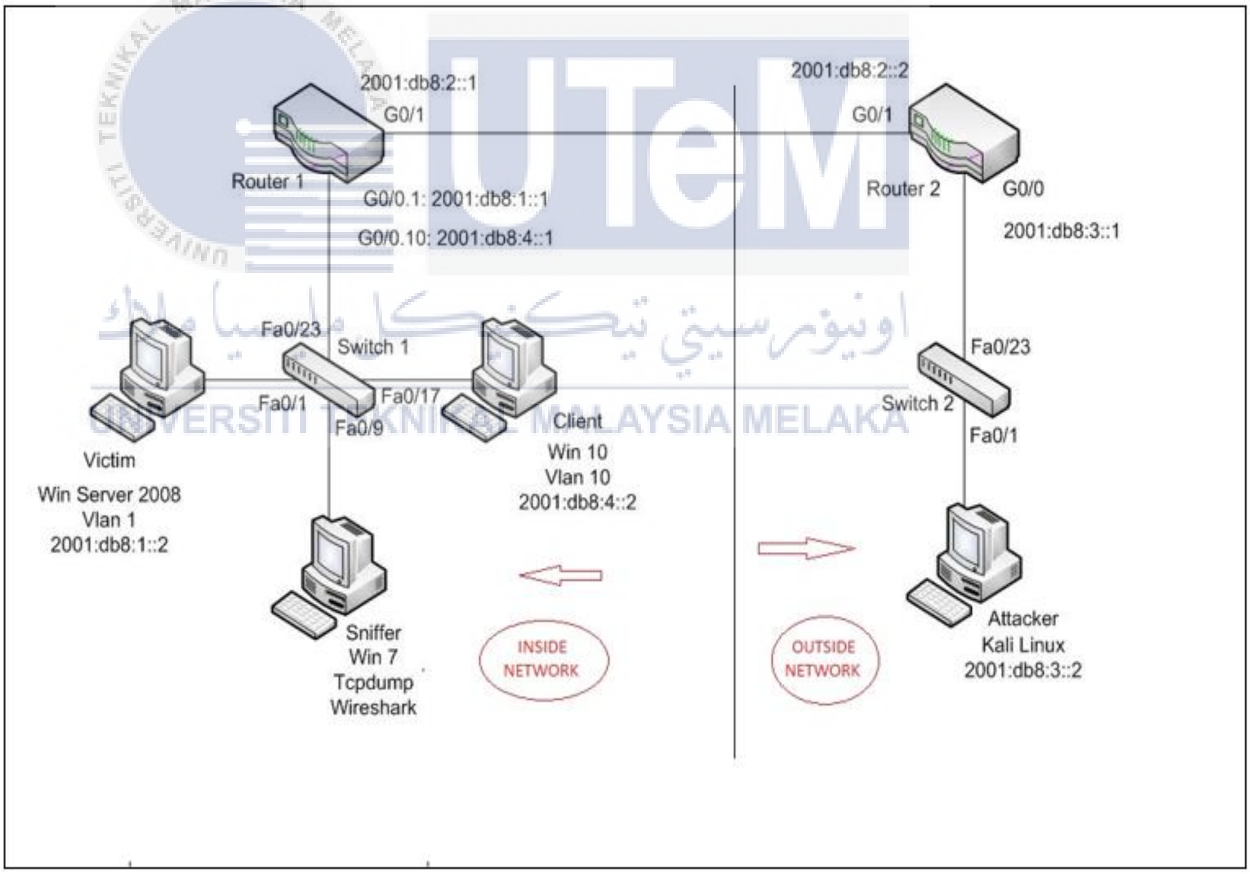


Figure 4.1: Network Design

As for the function, each PC has their own task. For inside network, one PC will be the server and have a few service in it such as DNS, FTP and Web Server. This PC will also be the victim for the attack. This PC will connect to port Fa0/1 and will have an IPv6 of 2001:db8:1::2/64. One PC will function as a sniffer where port mirroring have been configured and assign it to port Fa0/23 in which this PC connect to that port. Software that will be install to this PC is Wireshark and Tcpdump. It will monitor and capture all the data that go through the network. This PC will have an IPv6 of 2001:db8:1::3/64. Lastly for the network, we will use an extra laptop that will act as client to the network. The IP that will be used is random from the range of available IPv6 address of the network

For inside network, there will only be one PC. This PC will function as a attacker that will launch few attack to the inside network. This PC connected to port Fa0/1 and have an IPv6 address of 2001:db8:3::2/64. This PC will be using Kali Linux Operating System(OS) as it is an OS that have many tools inside it that are will be used in this project.

4.3 Physical and Logical Design

Physical design and logical design that are related to the project will be explained in this section. Explanation will be in form of picture that will be attached below.

4.3.1 Logical Design

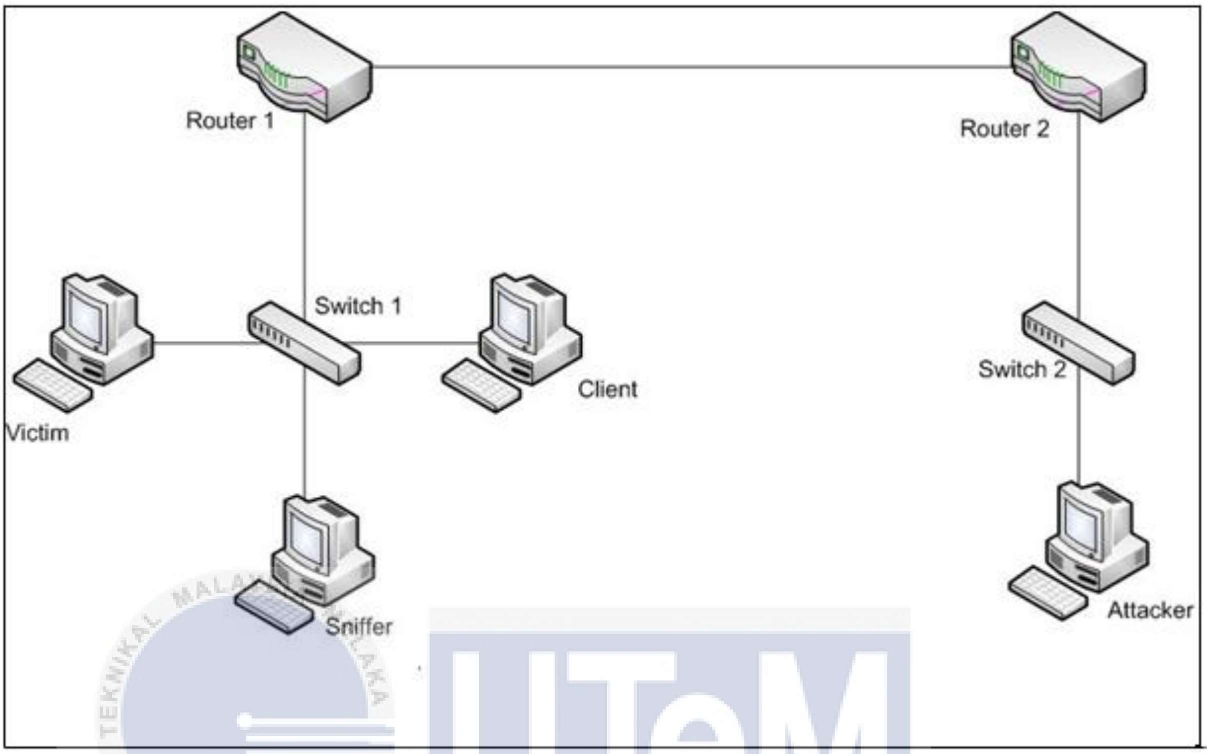


Figure 4.2: Logical Design

Logical design used to display graphical view of network consist of hardware and overall positioning of it before it being implement to the real environment. In other word, logical design is the model of the real or actual system

4.3.2 Physical Design

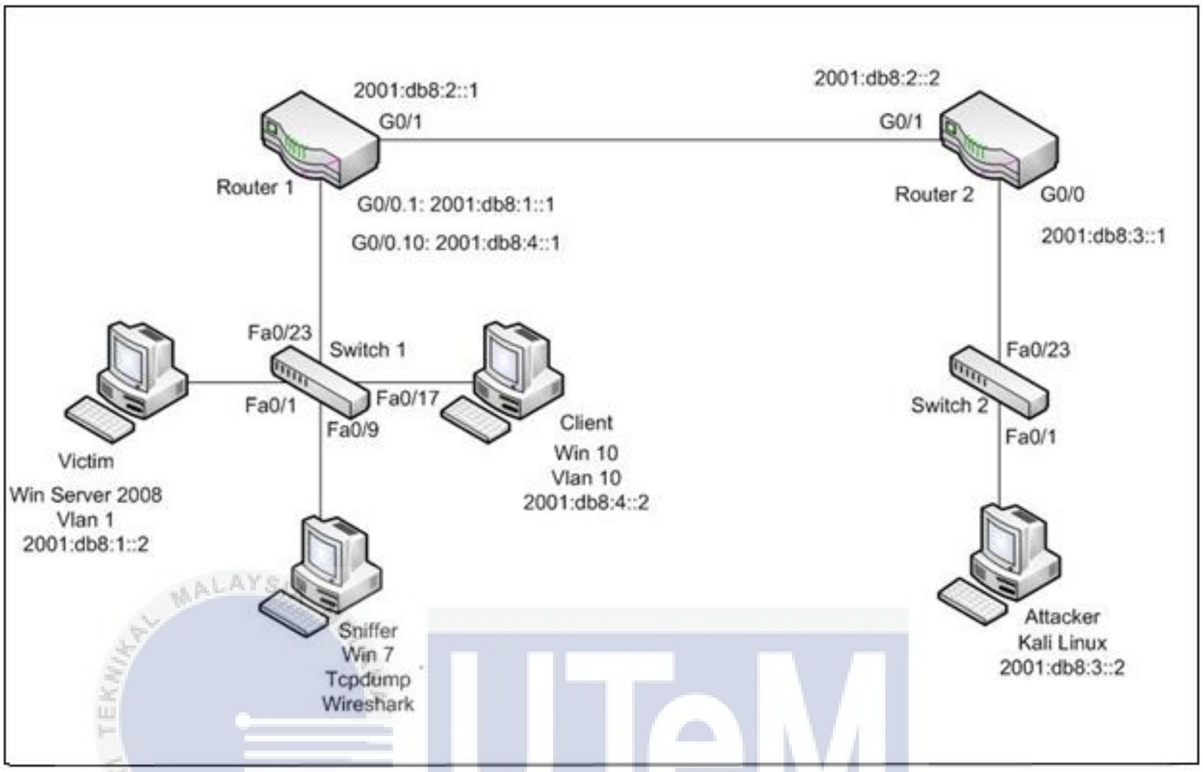


Figure 4.3: Physical Design

In Physical design, it will used the same graphical image as the logical design. But with more information of it. Which port that are using for each device, subnetting and IP structure will be present and vlan will also be shown if there is any.

4.4 Possible Scenario

In this section, every possible scenario related to the project will be explained. Scenario are very important because it will be used to obtain the objective of this project

4.4.1 First Scenario

On the first scenario of the research, first flood DoS attack which is Smurf (ICMP flood) attack will be launch to the IPv6 network environment. Then the attack flow and packet will be captured and recorded. Smurf6 is the IPv6 attacking tools provided by THC which is will be used to launch the attack. In this scenario, 4 computers will involve to make the attack work. First computer is Kali Linux and it will be used as the attacker. Second computer is using window server and it act as the server in this network. This server will be the target and victim of the attack. Third computers is using window 7 and it will function as a sniffer to capture packet and data from the attack. And last computer will be act as client

4.4.2 Second Scenario

In this scenario, second flood DoS attack will be launch to the IPv6 network. In this attack I will try to flood the local network with router advertisement. The tools that will be used is alive6 (TCP flood), it is tool that provided by THC. The environment that will be used in this attack is same with scenario one which is using four computer. First computer is kali linux and it will be used as the attacker. Second computer is using window server and it act as the server in this network. This server will be the target and victim of the attack. Third computers is using window 7 and it will function as a sniffer to capture packet and data from the attack. And last computer will be act as client on the network and will use it to see whether it will have any effect from the attack.

4.4.3 Third scenario

On the third scenario, last flood DoS attack will be launch to the network. This attack function by flooding the network with UDP protocol packet. Tools that will be used is Alive6. It is also the tools provided by THC. The environment that will be used in this attack is same with scenario one

4.5 Metric Measurement

Metric measurement that will be used in this project is the packet characteristic based on number of packet, destination address, protocol used and packet frequency

4.6 Summary

To conclude about this chapter, all architecture and design related to the project has been determined and explained. This chapter is important as a guide to be used for the next chapter, Implementation.

Next chapter is implementation, which is it will focusing to implement the project based on design to the real environment. The test will be conducted and data collected will be analyse.

CHAPTER V

IMPLEMENTATION

5.1 Introduction

In this chapter, real network environment will be set up based on design that has been done in the previous chapter. Activity involved to get the data will briefly describe and explain in form of data flow and graph. The collected data then will be used and analyze in the last chapter which is result and finding

5.2 Environment Setup

This section will explain detail about each phases taken starting from setting up the equipment until the process of collecting data from the network.

5.2.1 Phase I: Obtaining Dataset

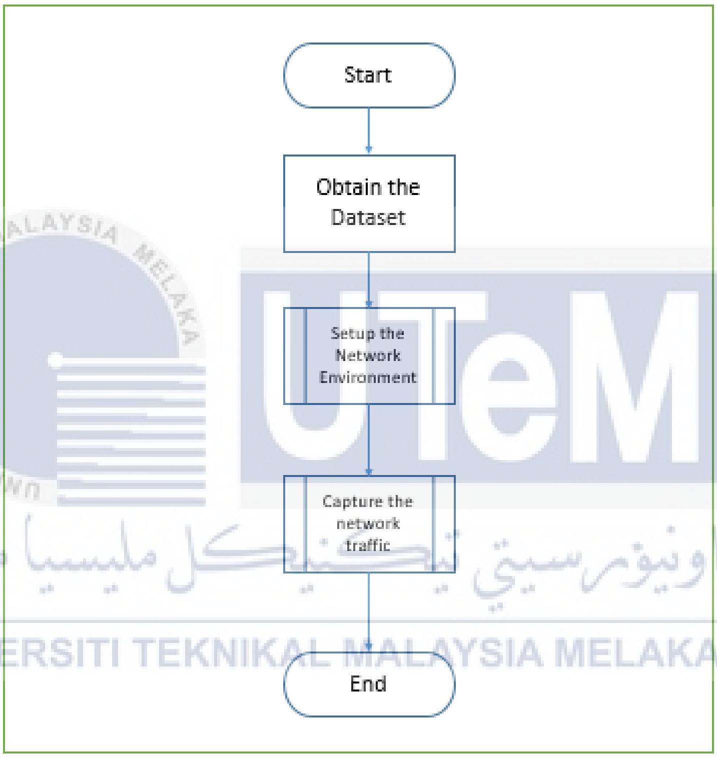


Figure 5.1: Obtaining data Flow Chart

Flow Chart Description

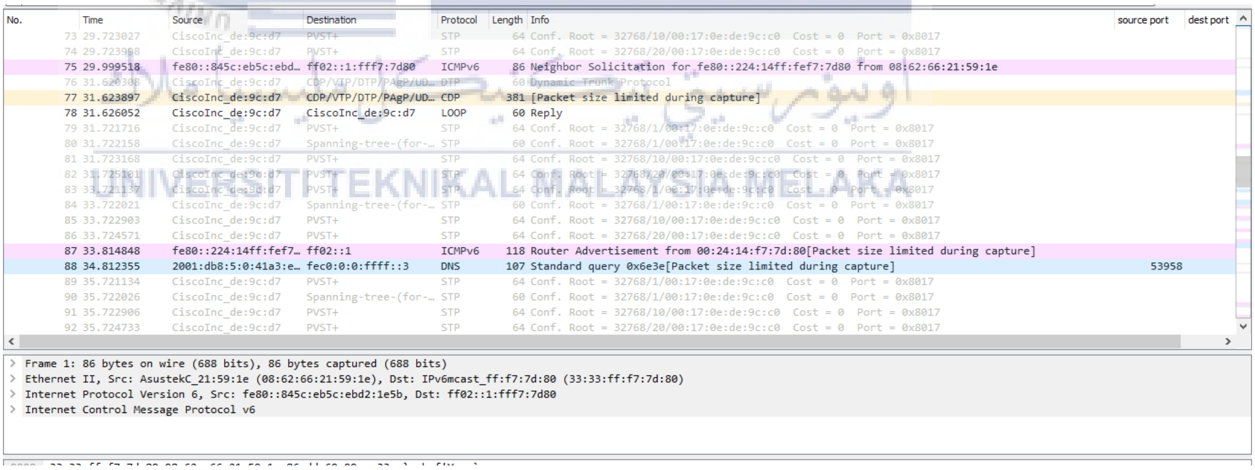
Setup Network Environment.

Network environment is set up for the purpose of obtaining data. The environment will be set up based on network design that has been done in previous chapter. The network will be configured with IPv6 network only. There will be four type of data that will be obtain which is normal traffic, ICMP flood traffic, TCP flood traffic and UDP flood traffic.

Capture the Network Traffic

For capturing process, first we have to install required software to the sniffer PC which is Wireshark and TCPdump. After that, launching the attack involved which is Smurf6 and Alive6 to the target and capturing the packet using TCPdump tools. The captured packet then was viewing using Wireshark.

Below is all the packet captured for normal traffic and attacks traffic using wireshark. Noted that all shown pictured is only a part of the full captured packet.



```
No.   Time       Source                 Destination             Protocol Length Info                                                                          source port  dest port
   73 29.723027  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/10/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   74 29.723998  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/20/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   75 29.999518  fe80::845c:eb5c:ebd…   ff02::1:fff7:7d80       ICMPv6    86 Neighbor Solicitation for fe80::224:14ff:fef7:7d80 from 08:62:66:21:59:1e
   76 31.620308  CiscoInc_de:9c:d7      CDP/VTP/DTP/PAgP/UD…    DTP       60 Dynamic Trunk Protocol
   77 31.623897  CiscoInc_de:9c:d7      CDP/VTP/DTP/PAgP/UD…    CDP      381 [Packet size limited during capture]
   78 31.626052  CiscoInc_de:9c:d7      CiscoInc_de:9c:d7       LOOP      60 Reply
   79 31.721716  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/1/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   80 31.722158  CiscoInc_de:9c:d7      Spanning-tree-(for-…    STP       60 Conf. Root = 32768/1/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   81 31.723168  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/10/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   82 31.725101  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/20/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   83 33.721137  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/1/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   84 33.722021  CiscoInc_de:9c:d7      Spanning-tree-(for-…    STP       60 Conf. Root = 32768/1/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   85 33.722903  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/10/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   86 33.724571  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/20/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   87 33.814848  fe80::224:14ff:fef7…   ff02::1                 ICMPv6   118 Router Advertisement from 00:24:14:f7:7d:80[Packet size limited during capture]
   88 34.812355  2001:db8:5:0:41a3:e…   fec0:0:0:ffff::3        DNS      107 Standard query 0x6e3e[Packet size limited during capture]                  53958
   89 35.721134  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/1/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   90 35.722026  CiscoInc_de:9c:d7      Spanning-tree-(for-…    STP       60 Conf. Root = 32768/1/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   91 35.722906  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/10/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017
   92 35.724733  CiscoInc_de:9c:d7      PVST+                   STP       64 Conf. Root = 32768/20/00:17:0e:de:9c:c0  Cost = 0  Port = 0x8017

> Frame 1: 86 bytes on wire (688 bits), 86 bytes captured (688 bits)
> Ethernet II, Src: AsustekC_21:59:1e (08:62:66:21:59:1e), Dst: IPv6mcast_ff:f7:7d:80 (33:33:ff:f7:7d:80)
> Internet Protocol Version 6, Src: fe80::845c:eb5c:ebd2:1e5b, Dst: ff02::1:fff7:7d80
> Internet Control Message Protocol v6
```

Figure 5.2: Wireshark Captured of Normal Traffic

Figure 5.2 show how traffic view from Wireshark, from there we can see information such as number of packet, source address, destination address, port number and many more. All the information from here will be used for data analysing process.

5.2.2 Phase II: Organize Data

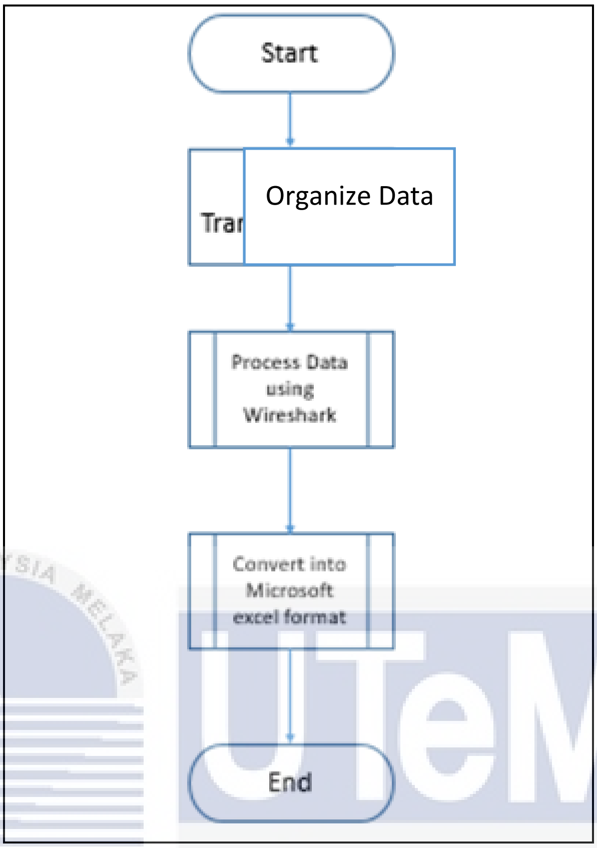

Start
Trar
Organize Data
Process Data using Wireshark
Convert into Microsoft excel format
End

Figure 5.3: Data Collection Flow Chart

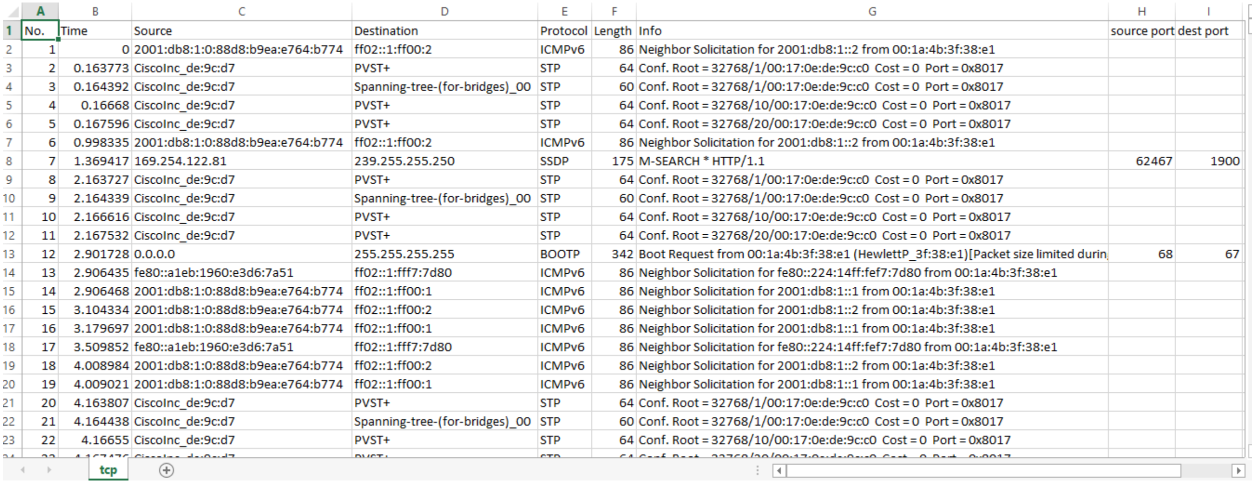
Flow Chart Description

Process of organizing the data can be start when all the related data has been captured after the attack has been launch to the target on the network.

Process Data Using Wireshark

For this process, the data that has been captured will be managed and split based on selected time. This process will done to all traffic involved which is normal traffic, attack Smurf6 traffic, Alive6 TCP traffic and Alive6 UDP traffic.

Convert Into Excel Format



No.	Time	Source	Destination	Protocol	Length	Info	source port	dest port
1	0	2001:db8:1:0:88d8:b9ea:e764:b774	ff02::1:ff00:2	ICMPv6	86	Neighbor Solicitation for 2001:db8:1::2 from 00:1a:4b:3f:38:e1		
2	0.163773	CiscoInc_de:9c:d7	PVST+	STP	64	Conf. Root = 32768/1/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
3	0.164392	CiscoInc_de:9c:d7	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
4	0.16668	CiscoInc_de:9c:d7	PVST+	STP	64	Conf. Root = 32768/10/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
5	0.167596	CiscoInc_de:9c:d7	PVST+	STP	64	Conf. Root = 32768/20/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
6	0.998335	2001:db8:1:0:88d8:b9ea:e764:b774	ff02::1:ff00:2	ICMPv6	86	Neighbor Solicitation for 2001:db8:1::2 from 00:1a:4b:3f:38:e1		
7	1.369417	169.254.122.81	239.255.255.250	SSDP	175	M-SEARCH * HTTP/1.1	62467	1900
8	2.163727	CiscoInc_de:9c:d7	PVST+	STP	64	Conf. Root = 32768/1/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
9	2.164339	CiscoInc_de:9c:d7	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
10	2.166616	CiscoInc_de:9c:d7	PVST+	STP	64	Conf. Root = 32768/10/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
11	2.167532	CiscoInc_de:9c:d7	PVST+	STP	64	Conf. Root = 32768/20/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
12	2.901728	0.0.0.0	255.255.255.255	BOOTP	342	Boot Request from 00:1a:4b:3f:38:e1 (HewlettP_3f:38:e1)[Packet size limited durin	68	67
13	2.906435	fe80::a1eb:1960:e3d6:7a51	ff02::1:fff7:7d80	ICMPv6	86	Neighbor Solicitation for fe80::224:14ff:fef7:7d80 from 00:1a:4b:3f:38:e1		
14	2.906468	2001:db8:1:0:88d8:b9ea:e764:b774	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001:db8:1::1 from 00:1a:4b:3f:38:e1		
15	3.104334	2001:db8:1:0:88d8:b9ea:e764:b774	ff02::1:ff00:2	ICMPv6	86	Neighbor Solicitation for 2001:db8:1::2 from 00:1a:4b:3f:38:e1		
16	3.179697	2001:db8:1:0:88d8:b9ea:e764:b774	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001:db8:1::1 from 00:1a:4b:3f:38:e1		
17	3.509852	fe80::a1eb:1960:e3d6:7a51	ff02::1:fff7:7d80	ICMPv6	86	Neighbor Solicitation for fe80::224:14ff:fef7:7d80 from 00:1a:4b:3f:38:e1		
18	4.008984	2001:db8:1:0:88d8:b9ea:e764:b774	ff02::1:ff00:2	ICMPv6	86	Neighbor Solicitation for 2001:db8:1::2 from 00:1a:4b:3f:38:e1		
19	4.009021	2001:db8:1:0:88d8:b9ea:e764:b774	ff02::1:ff00:1	ICMPv6	86	Neighbor Solicitation for 2001:db8:1::1 from 00:1a:4b:3f:38:e1		
20	4.163807	CiscoInc_de:9c:d7	PVST+	STP	64	Conf. Root = 32768/1/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
21	4.164438	CiscoInc_de:9c:d7	Spanning-tree-(for-bridges)_00	STP	60	Conf. Root = 32768/1/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		
22	4.16655	CiscoInc_de:9c:d7	PVST+	STP	64	Conf. Root = 32768/10/00:17:0e:de:9c:c0 Cost = 0 Port = 0x8017		

Figure 5.4: Data Convert to Excel

Figure 5.7 Show example of packet capture using wireshark has been converted and view in Microsoft excel. Noted that figured shown is only part of the full data. Every traffic was filtered and split to 60 seconds each.

5.2.3 Phase III: Differentiate and Analysis Data

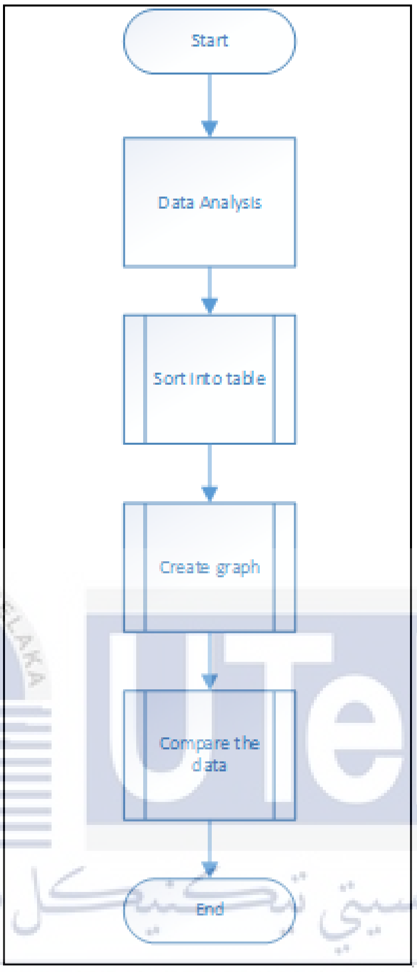


Figure 5.5: Differentiate and Analysis Data Flow Chart

Flow Chart Description

In this process, data that has been transferred to Excel will be sort out in form of table according to the matrix measurement that has been decided for this project.

After all the data has been sorted in form of table, then Process of creating the graph can take place. Several graph will be created based on the table. Graph will be used to analyze data separately and then comparing with each of the data based on specific information. The graph will be shown below

5.3 Destination Address Graph

5.3.1 Normal Traffic

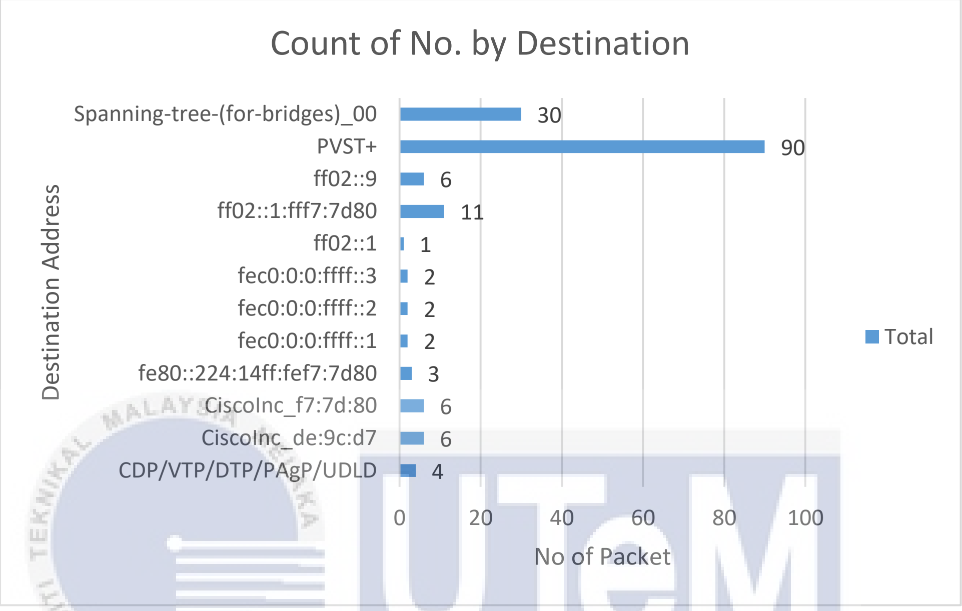


Figure 5.6: Normal traffic graph by destination

From the graph that has been created and analyized, we can see for normal packet traffic, the highest number of packet by destination is at Per Vlan Spanning Tree Plus (PVST+) which is 90 packets.

5.3.2 CMP flood attack (smurf6) Traffic

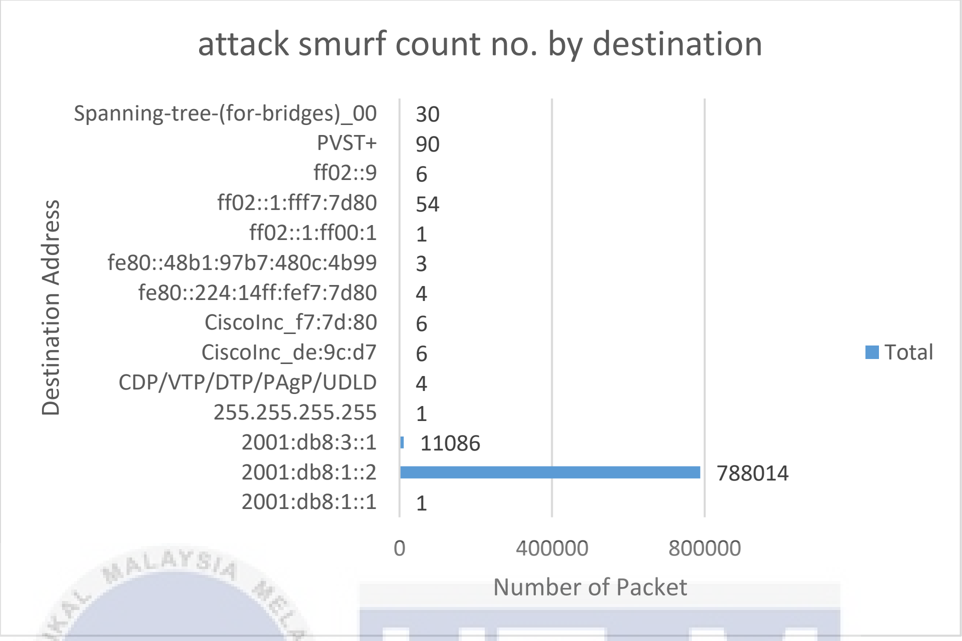


Figure 5.7: Smurf6 traffic graph by destination

From the graph that has been created and analysed, we can see that for smurf6 packet traffic, the highest number of packet by destination is at 2001:db8:1::2 address which is 788014 packets. This is because 2001:db8:1::2 is the victim address of the attack. Analysis and comparison of the graph will be shown in the next chapter

5.3.3 TCP Flood Attack (Alive6) traffic

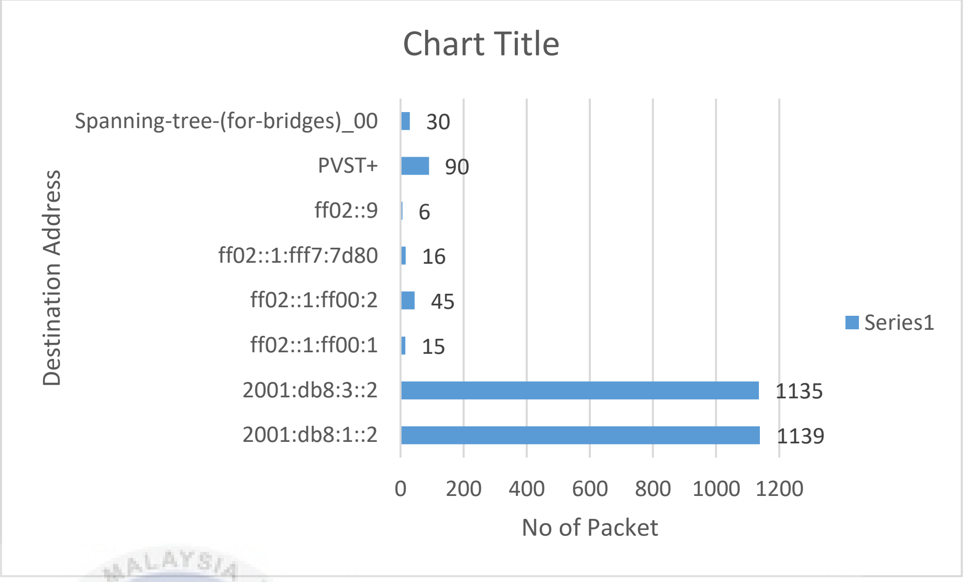


Figure 5.8: TCP flood traffic graph by destination

From the graph that has been created and analysed we can see for TCP flood packet traffic, the highest number of packet by destination is at 2001:db8:1::2 address which is 1139 packets. Further analysis and comparison will be shown in next chapter.

5.3.4 UDP Flood Attack (Alive6) Traffic

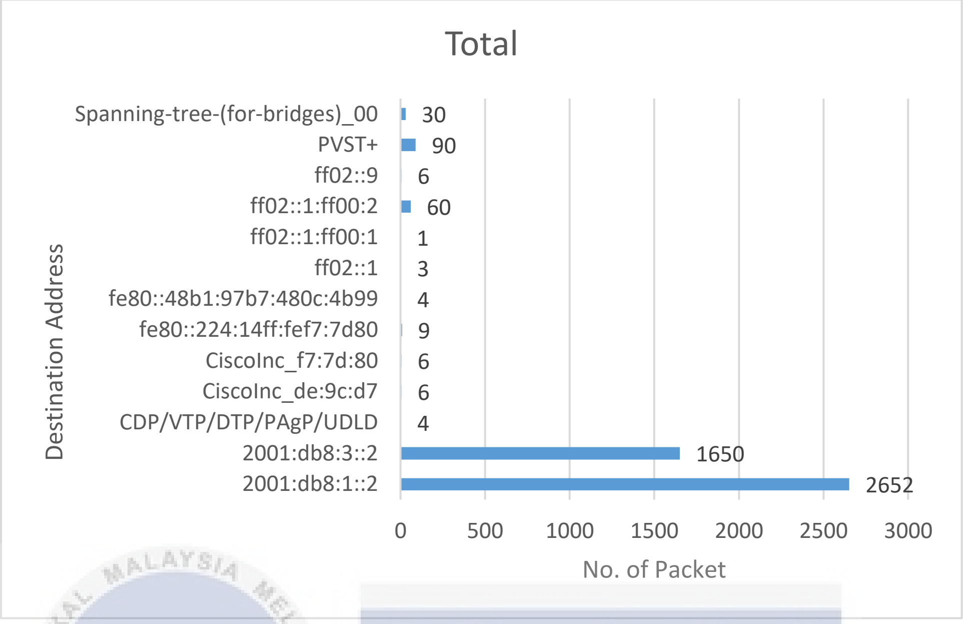


Figure 5.9: UDP flood traffic graph by destination

From the graph that has been created and analysed we can see for UDP flood packet traffic, the highest number of packet by destination is at 2001:db8:1::2 address which is 2652 packets.

5.4 Graph of Protocol Type

5.4.1 Normal Traffic

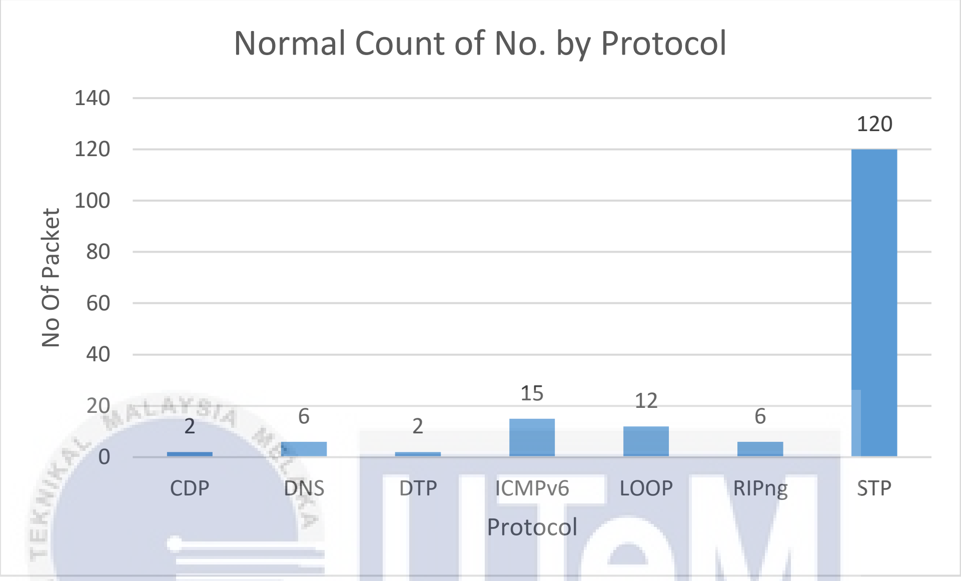


Figure 5.10: Normal traffic graph by destination

From the graph that has been created and analysed, we can see for normal packet traffic, the highest number of protocol is Spanning Tree Protocol (STP) which is 120 packets. While all other packet is distribute normally between other protocols. Further explanation will be given in the next chapter

5.4.2 ICMPv6 flood attack (smurf6) Traffic

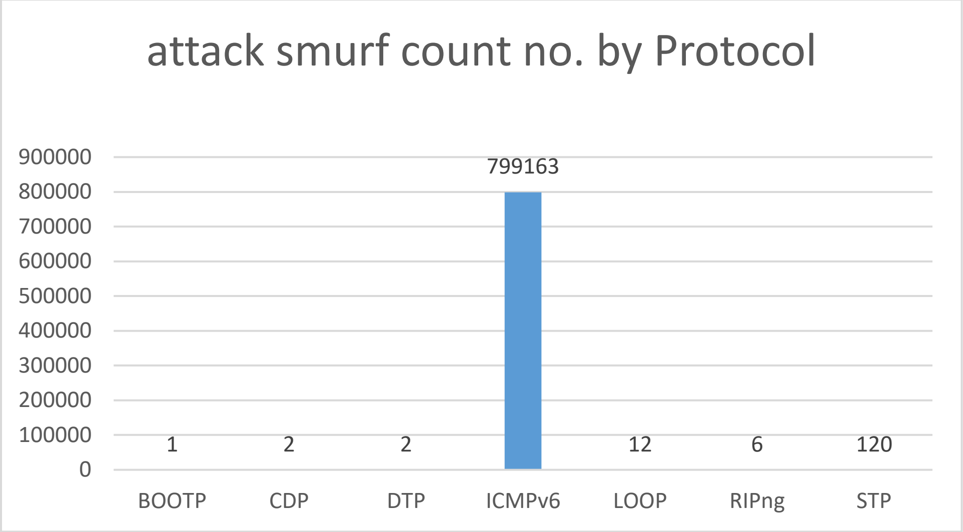


Figure 5.11: Graph for Smurf6 attack by Protocol

From the graph that has been created and analysed we can see for smurf6 packet traffic, the highest number of protocol is ICMPv6 which is 799163 packets. We can see from this information there is clearly unusual behaviour has occur to this traffic. Further analysis will be shown in the next chapter, Testing and Analysis

5.4.3 TCP Flood Attack (Alive6) Traffic

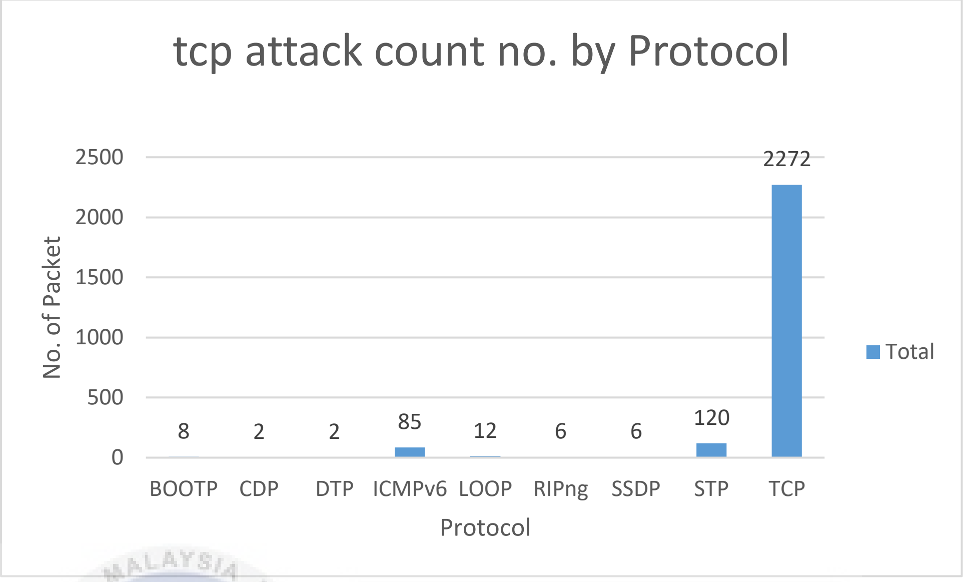


Figure 5.12: Graph for TCP flood attack by Protocol

From the graph that has been created and analysed we can see for Alive6 TCP packet traffic, the highest number of protocol is TCP which is 2272 packets.. We can see from this information there is clearly unusual behaviour has occur to this traffic. Further analysis will be shown in the next chapter, Testing and Analysis

5.4.4 UDP Flood Attack (Alive6) Traffic

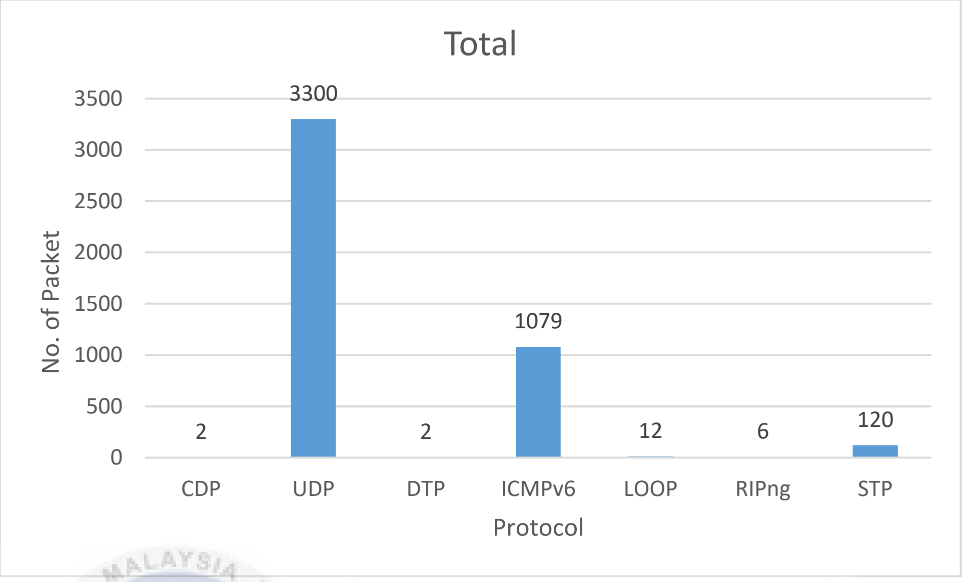


Figure 5.16: Graph for Alive6 UDP attack by Protocol

From the graph that has been created and analysed we can see for Alive6 UDP packet traffic, the highest number of protocol is UDP which is 3300 packets. We can see from this information there is clearly unusual behaviour has occur to this traffic involving UDP protocol. Further analysis will be shown in the next chapter, Testing and Analysis

CHAPTER IV

TESTING AND ANALYSIS

6.1 Introduction

Testing and Analysis are the last Chapter for this project. It will determine whether the objective were achieve through few process of collecting data and analysis of the collected data. Four type of collected data will be analyze which is one normal packet, and three flooding attack packet from ICMPv6 flood attack, TCP flood attack and UDP flood attack. Graph will be used to provide needed information for analyzing process.

6.2 Results and Analysis

For this section one normal attack and three flooding attack that has been captured and graphed in previous chapter will be used. Analysis will be based on information such as destination address, number of packet, protocol and packet frequency.

For this project, every traffic data was collected for 30 minutes. The collected data then will be selected and analyze for three separate minute each of one minute. Below are the table for analysis process.

Table 6.1: Data Taken for Analysis Process

Type of Traffic Data	Total Time of Traffic Data	Time of Data To be Analyze		
Normal Data	30 Minutes	1 minute (0s-60s)	1 minute (Random)	1minute (Random)
Attack data (ICMPv6 flood, TCP flood, UDP flood)	30 Minutes	1 minute (0s-60s)	1 minute (Random)	1minute (Random)

Based on the table, the data will be analyzed based on specific criteria.

6.2.1 Measurement 1: Number of Packet

Table 6.2: Number of Packets for different traffic

Type of Traffic Data	Total Time of Traffic Data	Number Of Packet for Specific Duration		
		1 minute (0 sec – 60 sec)	1 minute (random time)	1 minute (random time)
Normal Data	**30 Minutes**	**163**	**178**	**389**
ICMPv6 flood Data (Smurf6)	**30 Minutes**	**799306**	**851281**	**999752**
TCP Flood Data (Alive6)	**30 Minutes**	**2523**	**3606**	**3508**
UDP Flood Data (Alive6)	**30 Minutes**	**3633**	**4521**	**4512**

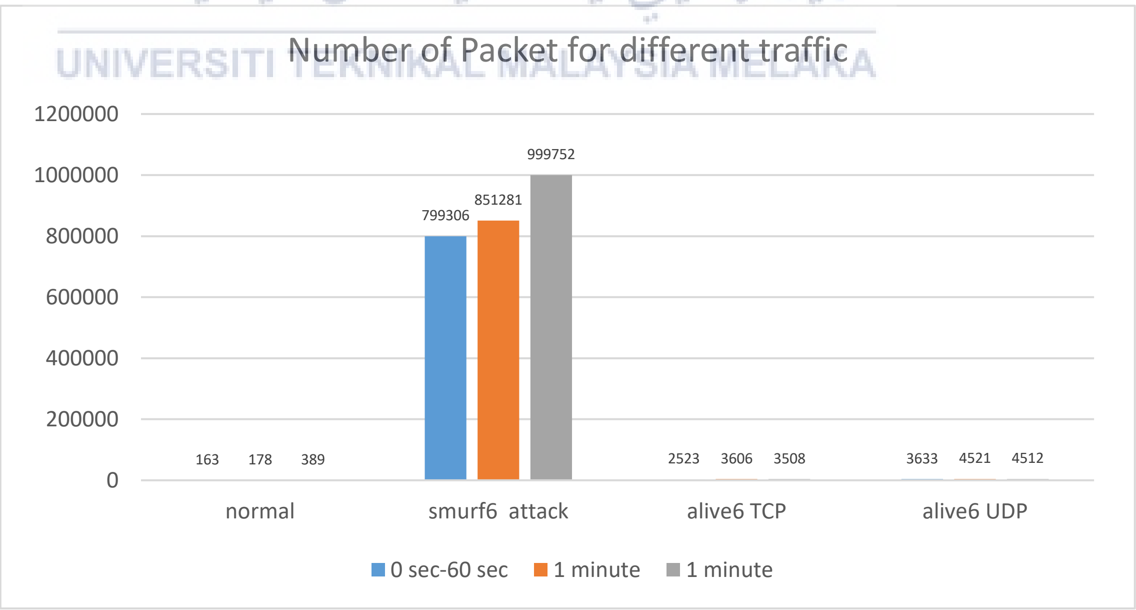


Figure 6.1: Graph No. of Packets per Traffic by Specific Duration

From the graph we can see that for normal traffic, only hundreds of packet occur during 1 minute duration. The average packet is between 100 to 400 packets per minute. For TCP, UDP and ICMPv6 flood attack, the number of packet per minute is more than normal traffic in which average traffic for TCP flood attack is between 2000 – 4000 packets per minute while for UDP flood attack is between 3000 – 5000 packets per minute.

For ICMPv6 flood attack the number of packet was much huge with the average packet per minutes is between 700,000 to 1 million packets per minute. This is because for ICMPv6 flood, the attack used smurf6 which is by default send packet simultaneously after being apply. While for Alive6 attack, it use looping script to run the command.

6.2.2 Measurement II: Protocol Type

Table 6.3: Type of protocol

Protocol	**Traffic Type**			
	Normal	**Alive6 TCP**	**Alive6 UDP**	**Smurf6**
CDP	2	2	2	2
DTP	2	2	2	2
ICMPv6	15	85	864	799163
LOOP	12	12	12	12
UDP	6	0	2623	0
TCP	0	2272	0	0
RIPng	6	6	9	6
STP	120	120	120	120

Table 6.3 shows protocol involved in the traffic that has been captured. There are few protocol that can be seen which is Cisco Discovery Protocol (CDP), Dynamic Trunking Protocol (DTP), Internet Control Message Protocol Version 6 (ICMPv6), LOOP, User Datagram Protocol (UDP), Transmission Control Protocol (TCP), RIPng, Spanning Tree Protocol (STP).

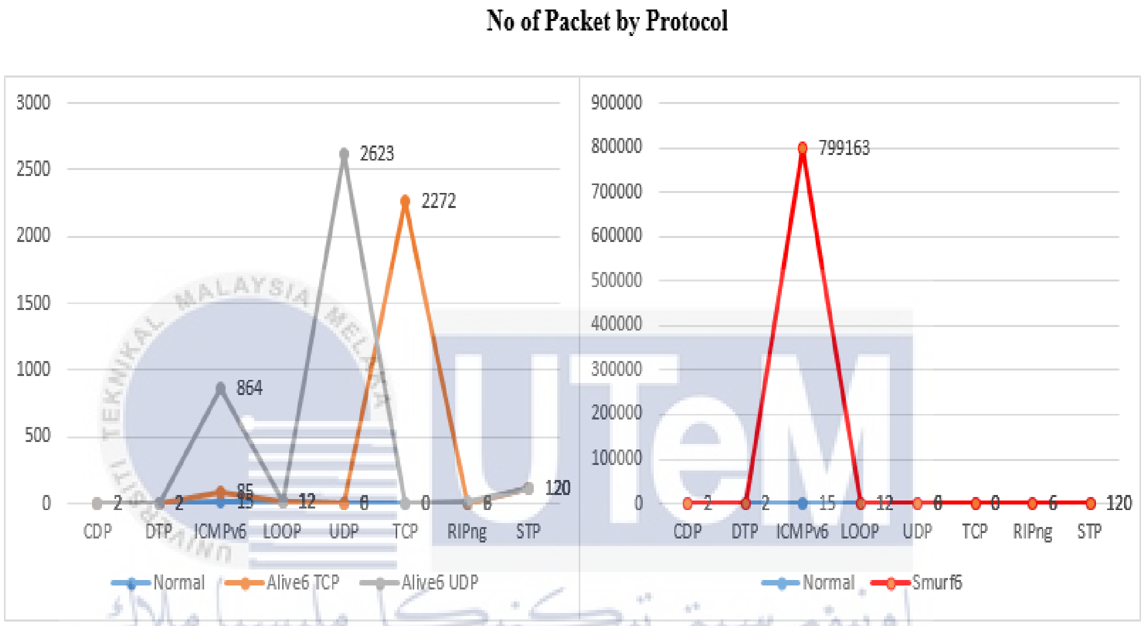


Figure 6.2: Graph No of Packets by Protocol

Analysis has been done to the captured packet by its protocol. Based on the graph we can see normal packet has stable amount of packet in every protocol with highest packet is on STP protocol by 120 packets per minute.

For attack packet, we can see each are different from normal traffic. In Alive6 TCP attack there is large number of packet on TCP protocol which is 2272 packets in one minute while in Alive6 UDP attack we can see most of the packet is on UDP protocol which is 2623 total number of packets per minute. Lastly for smurf6 attack there is stable number in all protocol except in ICMPv6 protocol where we can see a large number of packet captured on ICMPv6 protocol just in one minute which is 799163 number of packets.

6.2.3 Measurement III: Packet Frequency on Destination Address.

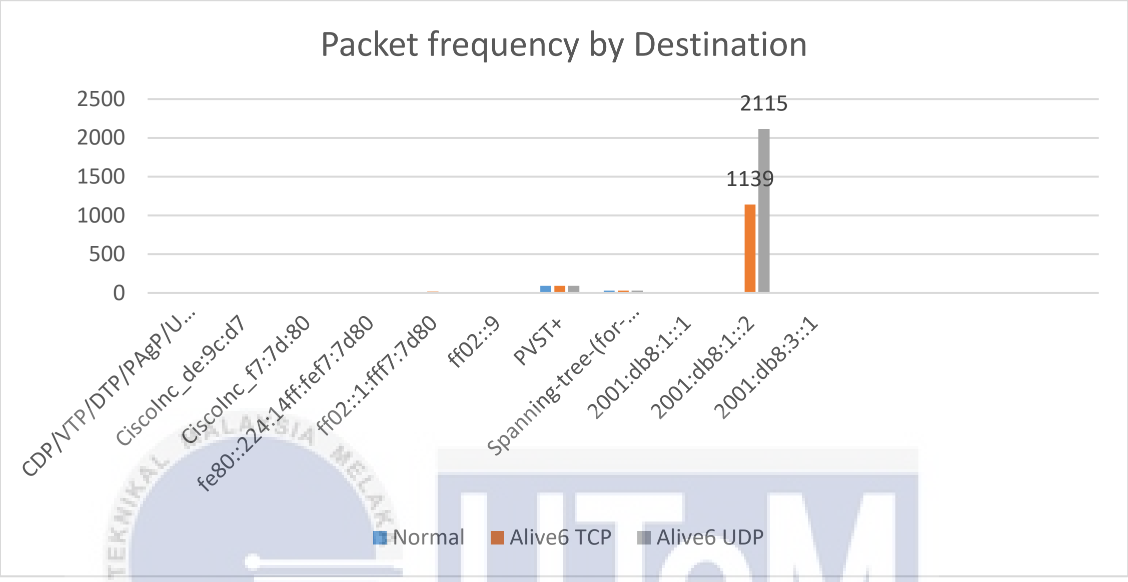


Figure 6.3: Graph Normal, TCP and UDP by Destination

From the graph we can see that in normal traffic has consistent packet to every destination. For Alive6 TCP the packet frequency is high at the 2001:db8:1::2. This is also happen to packet frequency of Alive6 UDP traffic.

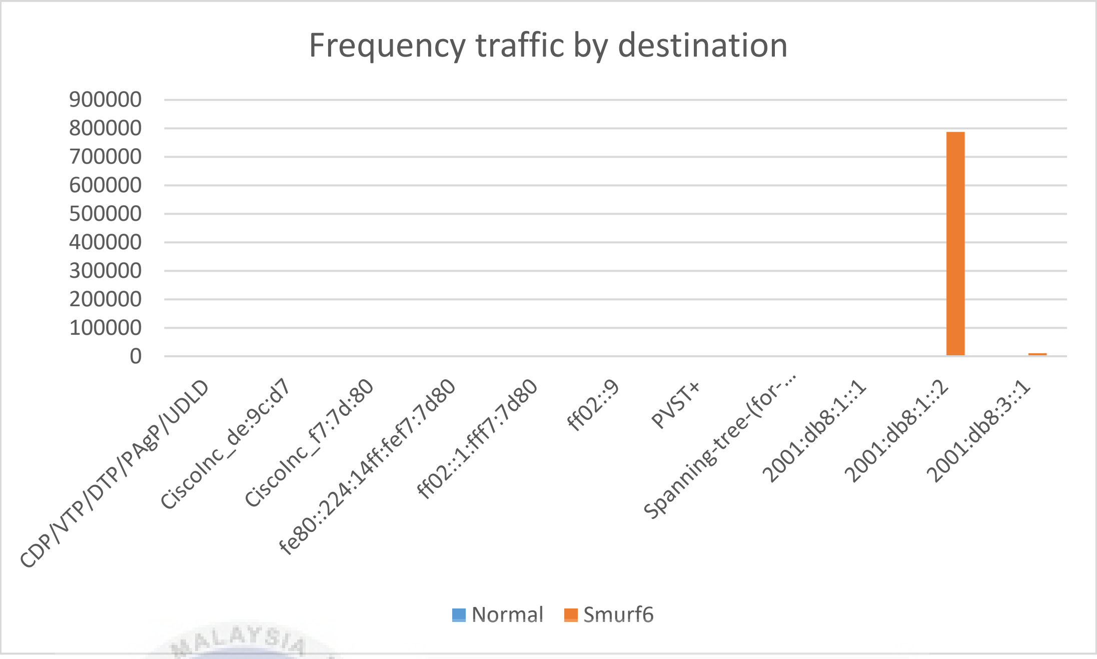


Figure 6.4: Smurf6 Graph by Destination

From the graph we can see that in normal traffic has consistent packet to every destination, but none to the 2001:db8:1:: and 2001:db8:3:: network. For smurf6 traffic there is very high packet frequency at 2001:db8:1::2 address. This is because 2001:db8:1::2 is the taret victim of the attack. This is the same happen to all attack traffic.

6.2.4 Measurement IV: Frequency and Number of Packets

For this measurement, frequency based on number of packets per seconds will be determine.

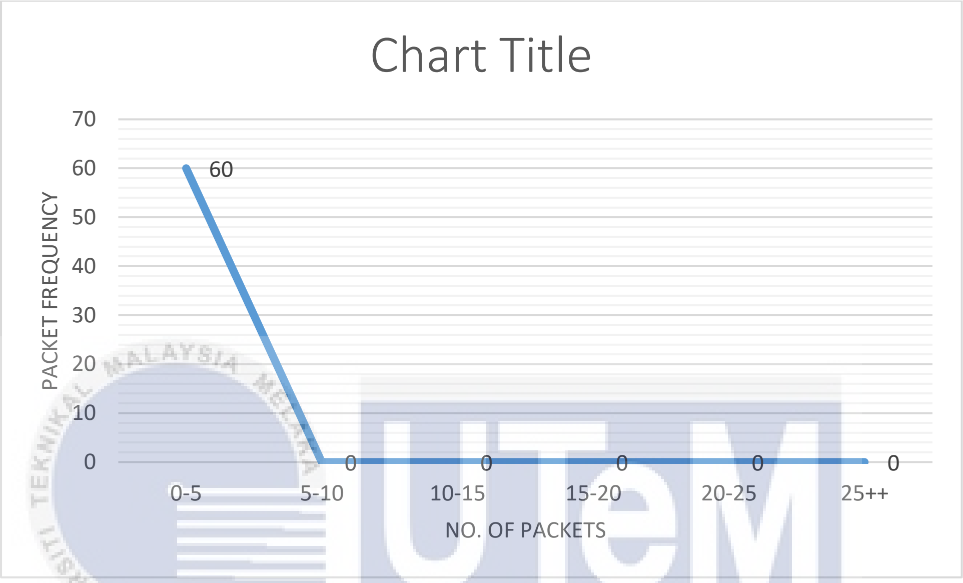


Figure 6.5: Graph Packet Frequency by No. of Packets

Figure 6.5 is based on normal traffic frequency and number of packets that has been analyze. From the graph we can see that most of number of packet per second is between 0-5 with frequency of 53. While Number of packet between 5-10 is only 7 times and the remaining is zero.

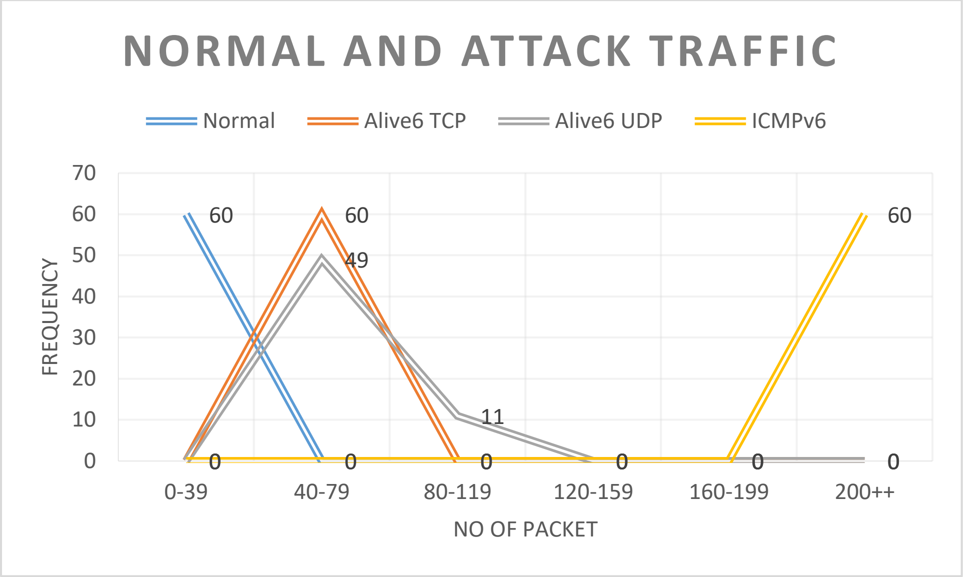


Figure 6.6: Graph Comparison Packet Frequency by No. of Packets

Figure 6.5 was based on all traffic from Alive6 TCP, Alive6 UDP, Smurf6 attack and normal packet. From the graph we can see that for Alive6 TCP traffic, the number of packet per second is between 40-79 packets with maximum frequency which is 60.

For Alive6 UDP attack traffic, the no of packet per second also between 40-79 packet with frequency of 49 and another 11 is between 80-119 packets. Lastly for Smurf6 attack traffic, the number of packet is more than 200 no of packets and for the exact amount is between 14000-15000 packets per second.

6.3 Analysis

These are analysis that can be conclude after obtaining the result. The analysis (A) has been presented in the table below.

Table: 6.4 Analysis Table

A	**Problem Statement**
A1	Based on the result of Flooding attack and normal attack, we can see that the no of packet for normal traffic is small. But when we see the number of packet on the attack packet all the Smurf6, Alive6 TCP and Alive6 UDP packet has enormous amount of packet captured. We can conclude that this is the sign of flooding attack on the network.
A2	By looking at the destination packet result. We can see that normal attack has stable amount of packet sent to every destination in the network. But for the attack traffic, all attack the Smurf6, Alive6 TCP and Alive6 UDP has large amount of packet sent to certain destination. This indicate unusual behavior has occur to that specific address and possible of becoming the attack victim. We can avoid that by creating policy to block certain amount of packet to the destination host
A3	As for the frequency and protocol result, we can see that normal traffic only sending maximum of 8 packets per second consist of various protocol. As for the attack packet, we can see that each attack Smurf6, Alive6 TCP and Alive6 UDP sending way more than that and mostly by specific protocol. From here if flooding attack happen we can know the type of flooding by looking at the protocol. We can make solution for this by making policy that accept maximum 8 ICMPv6, TCP or UDP packet per second and assume as an attack if more than that.

CHAPTER IIV

CONCLUSION

7.1 Introduction

In this chapter, overall conclusion about this research project will be made whether this project have meet the objective that has been stated. Other than that, project limitations and contribution along with future works will also be included in this chapter.

7.2 Project Summarization

There is three objective in this research project which is to study technique and method used to attack IPv6 network. Second, to analyze the pattern and behaviour of flood DoS attack and lastly to differentiate flood DoS attack traffic and normal traffic.

The first objective of the project is to study technique and method used to attack IPv6 network. This objective were achieve by reading and studying about IPv6 network structure and about overall network attack.

Second objective is to analyze the pattern and behaviour of flood DoS attack. This objective were achieve by collecting the data from each attack and then the behaviour of each attack were analyzed by using table and graph method.

Lastly to differentiate flood DoS attack traffic and normal traffic. This objective were achieve by collecting traffic attack and normal traffic. Both traffic then was analyze using method table and graph and comparing them.

7.3 Project Contribution

There were few contribution for this research project which is provided reading platform for knowledge about IPv6 network and network attack. Providing information about DoS attack in IPv6 network through readable data and graph. Lastly as small source of references for future study or research.

7.4 Project limitation

This project only focus on attack on IPv6 network and only flooding DoS attack was covered in this research. As we know there is many more type of attack that can be done to the network, so this project can’t be used if it is involving other type of network attack.

7.5 Future Work

As been stated on the title of this project, it only covered on flooding DoS attack. However, there is more attack that can be done under DoS attack and more tools to be used. Not forgetting about all other type of network attack such as Men-In-The-Middle attack, reconnaissance attack and many more. Should the project to be continued in the future, all of those mentioned should be considered to put in the scope research so that the output will be more knowledgeable and useful.

7.6 Conclusion

This Chapter determined whether this project were successful to meet the objective. We can conclude that this research project was successfully achieve the objective which is to study technique and method used to attack IPv6 network, to analyze the pattern and behaviour of flood DoS attack and lastly to differentiate flood DoS attack traffic and normal traffic.

REFERENCES

1. James Small. IPv6 Attack And Countermeasure retrieve on April 2016 from http://www.rmv6tf.org/wp-content/uploads/2013/04/5-IPv6-Attacks-and-Countermeasures-v1.2.pdf

2. Harith A. Dwood (2011). IPv6 Security Vulnerabilities. I.T. Department, British Royal University for Science and Technology, Erbil, IRAQ.Retrieve on April 2016

3. Atik Pilihanto (2011). A Complete Guide on IPv6 Attack and Defense. GIAC (GSEC) Gold certification. Available at: https://www.sans.org/reading-room/whitepapers/detection/complete-guide-ipv6-attack-defense-33904

4. Muhammad Fermi Pasha1, Mustafa Abdat2, Mandava Rajeswari1 (2013). IPv6 Traffic Flow Security Threats and Trend Analysis: Towards Combined Intelligent Detection Approach

5. Farhan Sajjad (2011). Denial of Service – The Smurf Attack. School of Computer Science University of Windsor

6. Johanna Ullrich, Katharina Krombholz, Heidelinde Hobel, Adrian Dabrowski, Edgar Weippl (2010). IPv6 Security: Attacks and Countermeasures in a Nutshell.

7. Kavita Choudhary , Meenakshi, Shilpa (2011). Smurf Attacks: Attack using ICMP

8. Janos Mohascsi (2005). IPv6 Security: Threats and solutions. Available at: http://www2.garr.it/conf_05_slides/j_mohacsi-IPv6_sec.pdf

9. Muraleedharan N (2011). Flow Based Traffic Analysis. Available at: http://docplayer.net/11858897-Flow-based-traffic-analysis.html

10. Van Hauser (2005). Attacking the IPv6 Protocol Suite. The Hacker's Choice. Available at : https://pacsec.jp/psj05/psj05-vanhauser-en.pdf

11. Emin Caliskan (2014). IPv6 Transition and Security Threat Report. Available at: https://ccdcoe.org/publications/articles/IPv6-Report.pdf

12. Rene Paap (2015). IPv6 and the Growing DDoS Danger. Available at: http://www.darkreading.com/attacks-breaches/ipv6-and-the-growing-ddos-danger/a/d-id/1322942

13. Carl Weinschenk (2015). Prepare for the IPv6 DDoS Attack Challenge. Available at: http://www.itbusinessedge.com/blogs/data-and-telecom/prepare-for-the-ipv6-ddos-attack-challenge.html

14. Antonios Atlasis (2011). Attacking IPv6 Implementation Using Fragmentation. Available at: https://media.blackhat.com/bh-eu-12/Atlasis/bh-eu-12-Atlasis-Attacking_IPv6-WP.pdf

15. LIN Zhao-wen (2005). Possible Attacks based on IPv6 Features and Its Detection. Available at: http://master.apan.net/meetings/xian2007/publication/031_lin.pdf