BORANG PENGESAHAN STATUS TESIS

JUDUL: IDENTIFY WORM(BLASTER.T)ATTACK PATTERN

SESI PENGAJIAN: SESI 2011/2012

Saya DIANA SHAZELIN BINTI MOHD NASIR 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 Kolej Universiti Teknikal Kebangsaan Malaysia.
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

diyana

(TANDATANGAN PENULIS)

Alamat tetap :Lot 121, Kampung Gemang,
17700 Ayer Lanas, Jeli
Kelantan, Malaysia
Tarikh : 30/8/2012

DR ROBIAH YUSOF
Pensyarah Kanan
Fakulti Teknologi Maklumat Dan Komunikasi
Universiti Teknikal Malaysia Melaka
Hang Tuah Jaya,76100
Durian Tunggal. Melaka

(TANDATANGAN PENYELIA)

Dr.RobiahYusof
Nama Penyelia
Tarikh: 30/8/2012

BLASTER.T ATTACK PATTERN GENERALIZATION

DIANA SHAZELIN BINTI MOHD NASIR

This report is submitted in partial fulfillment of the requirement for the Bachelor of Computer Science (Computer Networking)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY
UNIVERSITI TEKNIKAL MALAYSIA MELAKA
2012

DECLARATION

I hereby declare that this project report entitled

BLASTER.T ATTACK PATTERN GENERALIZATION

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

STUDENT : diyana Date: 30/8/2012

(DIANA SHAZELIN BINTI MOHD NASIR)

SUPERVISOR : Date: 30/8/2012

(DR. ROBIAH BINTI YUSOF)

DR ROBIAH YUSOF
Pensyarah Kanan
Fakulti Teknologi Maklumat Dan Komunikasi
Universiti Teknikal Malaysia Melaka
Hang Tuah Jaya,76100
Durian Tunggal, Melaka

DEDICATION

Dear Allah

Giving me the ideas, strengths, knowledge and healthy that helps me to finish this project as schedule.

Dear Beloved Parents

Thank you because always supports me with their love and gives the motivations to finish this project.

Dear Lecturers and Supervisor

Thank you for all the guidance, patience, encouragement and supervision to make me finish this project.

Dear Friends

Thank you for all the knowledge, support and encouragement.

ACKNOWLEDGEMENTS

First of all, I would like to thank Allah for giving me the ideas, strengths, knowledge and healthy that helps me to finish this project as schedule.

I would like to thanks to my beloved supervisor Dr.Robiah Yusof for her guidance, patience, excellent support,motivation, constant patience, and continuous understanding throughout the semester of my Final Year Project in UniversitiTeknikal Malaysia Melaka (UTeM).

I would also like to dedicate my appreciation to my beloved parents Mohd Nasir (My father) and Marhaini (my mother) and also my siblings that always supports me with their love and gives the motivations to finish this project. throughout the year of my studies in UTeM.

Lastly, I am thankful to all colleagues and friends for their understanding, suggestions and comments throughout my project, which made my final years memorable in UTeM.

ABSTRACT

The number of malware variants is still persistent. The infection appears to have successfully transitioned to new hosts as the original systems are cleaned or shut off. The current approach had used Intrusion Detection System (IDS) as a technique to detect this worm but it still not comprehensive enough because IDS can generate huge amounts of data. In this project, network traffic is explored to establish the attack pattern in order to reveal the true attacker or victim of Blaster.T and identify the traces leave on the attacker and victim. This project will only concentrate on malware network intrusion and traditional worm namely Blaster worm variants. This project will trace pattern in attacker's and victim's perspective.Thus, the objectives of this project are to identify the features or attributes of malware in perspective of victim and attacker, to generate attack pattern for malware in perspective of victim and attacker and to generalize the attack pattern in perspective of victim and attacker.

ABSTRAK

Bilangan variasi malware masih berterusan.Jangkitan itu ternyata telah berjaya beralih kepada tuan rumah baru sebagai sistem asal dibersihkan atau dimatikan.Pendekatan yang digunakan kini telah menggunakan Sistem Pengesanan Pencerobohan (IDS) sebagai satu teknik untuk mengesan cacing ini tetapi ia masih tidak cukup komprehensif kerana IDS boleh menjana jumlah data yang besar. Dalam projek ini, trafik rangkaian diterokai untuk menubuhkan corak serangan untuk mendedahkan penyerang benar atau mangsa Blaster.T dan mengenal pasti kesan meninggalkan kepada penyerang dan mangsa. Projek ini hanya akan menumpukan perhatian kepada pencerobohan rangkaian malware dan cacing tradisional iaitu variasi cecacing Blaster. Projek ini akan mengesan corak dalam perspektif penyerang dan mangsa. Oleh itu, objectif projek ini adalah untuk mengenal pasti ciri-ciri atau sifat-sifat malware dalam perspektif mangsa dan penyerang, untuk menjana corak serangan malware dalam perspektif mangsa dan penyerang dan umum corak serangan dalam perspektif mangsa dan penyerang.

TABLE OF CONTENTS

CHAPTER	SUBJECT	PAGE
	DECLARATION	**i**
	DEDICATION	**ii**
	ACKNOWLEDGMENT	**iii**
	ABSTRACT	**iv**
	ABSTRAK	**v**
	TABLE OF CONTENTS	**vi**
	LIST OF TABLES	**x**
	LIST OF FIGURES	**xii**
1	**INTRODUCTION**	
	1.1 Project Background	1
	1.2 Problem Statement	3
	1.3 Research Question	3
	1.4 Research Objectives	4
	1.5 Scopes	5
	1.6 Project Significance	5
	1.7 Conclusion	5

2 LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction 6
2.2 Fact and Finding (Malware) 8
2.2.1 Overview of Malware Issues 8
2.2.1.1 Malware Definition 8
2.2.1.2 Malware Classification 9
2.2.1.3 Malware Families 11
2.2.2 Worm 12
2.2.2.1 Worm Definition 12
2.2.2.2 Worm History 12
2.2.2.3 Worm Classification 13
2.2.2.4 Type Of Worm 18
2.2.2.5 Blaster Worm 15
2.2.2.6 Blaster.T Pattern 16
2.2.3 Attack Pattern 17
2.2.4 Network Traffic 17
2.3 Project Methodology 23
2.4 Project Requirements 25
2.4.1 Software Requirement 25
2.4.2 Hardware Requirement 25
2.4.3 Other Requirement 25
2.5 Project Schedule and Milestones 25
2.6 Conclusion 28

3 ANALYSIS

3.1 Introduction 29
3.2 Problem Analysis 30
3.3 Requirement Analysis 32
3.3.1 Data Requirements 33

3.3.2 Software Requirements 52

3.3.3 Hardware Requirements 53

3.3.4 Summary of Selecting Features 53

3.4 Conclusion 54

4 **DESIGN** 55

4.1 Introduction 55

4.2 Process Flow Blaster.T in Perspective Of Attacker and Victim 57

4.3 Attack Pattern Design 59

4.3.1 Basic Attack Model 59

4.3.2 Attack Pattern of Blaster.T 60

4.3.3 Generalized Attack Pattern of Worm (Blaster.A, Blaster.T and Sasser.B) 62

4.3.4 Scripting Design 63

4.4 Conclusion 65

5 **IMPLEMENTATION** 66

5.1 Introduction 66

5.2 Software Configuration Management 67

5.2.1 Configuration Environment Setup 67

5.2.1.1 Java Programming Language 67

5.2.1.2 Jpcap 68

5.2.1.3 Netbeans (Version 7.1.2) 69

5.2.1.4 Wireshark 69

5.2.2 Software Configuration Management 70

5.3 Hardware Configuration Management 70

5.3.1 Hardware Setup 71

	5.4	Development Status	71
	5.5	Conclusion	73
6	TESTING		74
	5.1	Introduction	74
	6.2	Test Plan	75
		6.2.1 Test Organization	75
		6.2.2 Test Environment	75
		6.2.3 Test Schedule	76
	6.3	Test Strategy	81
		6.3.1 Classes of Test	81
	6.4	Test Design	81
		6.4.1 Test Description	82
		6.4.2 Test Data	82
	6.5	Test Result and Analysis	83
	6.6	Conclusion	95
7	CONCLUSION		96
	7.1	Observation on Weaknesses and Strengths	96
		7.1.1 Project Strengths	96
		7.1.2 Project Weakness	97
	7.2	Proposition for Improvement	97
	7.3	Contribution	98
	7.4	Conclusion	98
	REFERENCES		
	APPEDICES		

LIST OF TABLES

TABLE	TITLE	PAGE
1.1	Summary of problem statement	3
1.2	Summary of research question	3
1.3	Summary of research objectives	4
2.1	Task, tools and technique for fighting malware [7]	9
2.2	Classifications of Malware	10
2.3	Type of virus worm [12]	14
2.4	Overview of Blaster variants (15)	16
2.5	TCP Flags Fields	20
2.6	Summary of IP Header	20
2.7	Summary of TCP Header	21
2.8	Selected Features	21
2.9	Software Requirement	25
2.10	Hardware Specification	26
2.11	Milestone and Schedule	27
3.1	Summary of attacker's pattern [1] (Attributes found=√, attributes not found=×, nil)	30
3.2	Summary of Victim's pattern (Attributes found=√, attributes not found=×) [1]	30
3.3	Selected Features	53
5.1	Hardware Setup	71
6.1	Tester Name	75
6.2	Software Requirements	75
6.3	Hardware Requirements	76
6.4	Testing Schedule Using Blaster T (i)	76
6.5	Testing Schedule Using Blaster T (ii)	77

6.6 Testing Schedule Using Blaster T (iii) 77

6.7 Testing Schedule Using Blaster A (i) 78

6.8 Testing Schedule Using Blaster A (ii) 78

6.9 Testing Schedule Using Blaster A (iii) 79

6.10 Testing Schedule Using Sasser B (i) 79

6.11 Testing Schedule Using Sasser B (ii) 80

6.12 Testing Schedule Using Sasser B (iii) 80

6.13 Data to be tested 82

6.14 Data to verification 83

6.15 Output Comparison Blaster T (i) 84

6.16 Output Comparison Blaster T (ii) 86

6.17 Output Comparison Blaster T (iii) 87

6.18 Output Comparison Blaster A (i) 88

6.19 Output Comparison Blaster A (ii) 89

6.20 Output Comparison Blaster A (iii) 92

6.21 Output Comparison Sasser B (i) 93

6.22 Output Comparison Sasser B (ii) 94

6.23 Output Comparison Blaster T (iii) 95

LIST OF FIGURES

FIGURE	TITLE	PAGE
1.1	Number of new malware programs per year since 2005 And in half of 2010 [5]	2
2.1	Literiture Review Phase	7
2.2	Classification of worm (Robiah Yusof, 2010)	13
2.3	IP Header	18
2.4	TCP Header	19
2.5	Capture packet with ip address [19]	22
2.6	Captured packet with ip and port number [19]	22
2.7	Captured packet with timestamps [19]	23
2.8	Project Methodology	23
3.1	Process to select features	32
3.2	Connection on 135 port with protocol TPC	33
3.3	Connection on 135 port using DCERPC protocol	34
3.4	Connection on 135 port with TCP protocol	35
3.5	Connection on port 4444 with TCP protocol (i)	35
3.6	Connection on port 4444 with service krb524 using TCP protocol (ii)	36
3.7	Connection on port 4444 with service krb524 using TCP protocol (iii)	36
3.8	Connection on port 4444 with service krb524 using TCP protocol (iv)	37
3.9	Connection on port 4444 with service krb524 using TCP protocol (v)	37

3.10 Connection on port 4444 with service krb524 using TCP protocol (vi) 38
3.11 Connection on port 4444 with service krb524 using TCP protocol (vii) 38
3.12 Connection on port 69 with tftp protocol 39
3.13 Connection on port 3xxx with tftp protocol 39
3.14 Continue Connection on port 4444 with TCP protocol (viii) 40
3.15 Continue Connection on port 4444 using tcp protocol (ix) 40
3.16 Continue Connection on port 4444 using tcp protocol (x) 41
3.17 Continue Connection on port 4444 with tcp protocol (xi) 41
3.18 Continue Connection on port 4444 with tcp protocol (xii) 42
3.19 Continue Connection on port 4444 with tcp protocol (xiii) 42
3.20 Continue Connection on port 4444 with tcp protocol (xiv) 43
3.21 Continue Connection on port 4444 with tcp protocol (xv) 43
3.22 Continue Connection on port 4444 with tcp protocol (xvi) 43
3.23 Continue Connection on port 4444 with tcp protocol (xvii) 44
3.24 Continue Connection on port 4444 with tcp protocol (xviii) 44
3.25 Continue Connection on port 4444 with tcp protocol (xix) 45
3.26 Connection Finish 45
3.27 Blaster.T attack in scenario A 46
3.28 Blaster.T attack in scenario B 47
3.29 Blaster.T attack in scenario C 48
3.30 Percentages of First Data Set 49
3.31 Percentages of Second Data Set 50
3.32 Percentages of Third Data Set 51
4.1 Process flow of scripting design 56
4.2 Blaster.T attacker process flow 57
4.3 Blaster.T victim process flow 58
4.4 Basic Attack Model 59

4.5	Blaster.T attack pattern design on attacker perspective	60
4.6	Blaster.T attack pattern design on victim perspective	61
4.7	Generalized attacker's attack pattern	62
4.8	Generalized victim's attack pattern	63
4.9	General Script Design	64
4.10	Script Design	65
5.1	Code fragment for reading pcap file	70
5.2	Select file	71
5.3	File Browser	72
5.4	Output (i)	72
5.5	Output (ii)	73
5.6	Output (iii)	73
6.1	Classes of test	81
6.2	Testing Output Blaster T (1)	83
6.3	Testing Output Blaster T (2)	84
6.4	Testing Output Blaster T (3)	85
6.5	Testing Output Blaster T (4)	85
6.6	Testing Output Blaster T (5)	86
6.7	Testing Output Blaster T (6)	87
6.8	Testing Output Blaster A (1)	88
6.9	Testing Output Blaster A (2)	89
6.10	Testing Output Blaster A (3)	90
6.11	Testing Output Blaster A (4)	90
6.12	Testing Output Blaster A (5)	91
6.13	Testing Output Blaster A (6)	91
6.14	Testing Output Sasser B (1)	92
6.15	Testing Output Sasser B (2)	93
6.16	Testing Output Sasser B (3)	94

CHAPTER I

INTRODUCTION

1.1 Project Background

Malware is malicious software that designed to disrupt computer operation. It is not generally directly observable. Even if it has destructive consequences, it is not a "bug" or a defect in a legitimate software program. The malware implies malice of forethought by malware inventor with the intention to disrupt or damage a system. [1].

There are many types of malware such as virus, Trojan horse, worm, spyware, adware and other malicious software. It is good to aware that there are malicious software programmer with bad intentions out there.[3].

The network environment of this project consists of Windows and Linux operating system workstations with IDS. Generally, the network environment will be purposely infected with any type of malware, but this research will only focus on worm (Blaster.T) pattern.

Blaster.T is a worm that exploits the DCOM RPC (Distributed Component Object Remote Procedure Call) vulnerability using TCP port 135. This worm attempts to download the msblast.exe file to the "%WinDir%\system32" directory and then execute it. Then, using network traffic, the data will be collect and analyze the order to generate specific worm attack pattern from attacker and victim perspective [2].

In this research network traffic is captured using tcpdump. Tcpdump is one of the original packet capture (or "sniffing") tools that provide these analysis capabilities, and even though it now shares the field with many other utilities, it remains one of the most powerful and flexible [3].

Even since malware activities are indentified, it usually can infiltrate the most of modern computer system. It has threatened the network activity and can cause bad impact on finance prospect especially [4]. Malware activities that had been recognized in facts and figure are shown below:

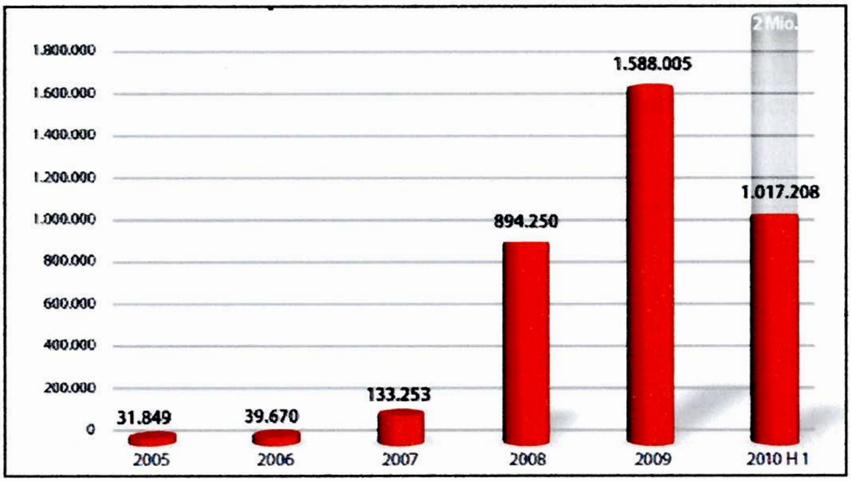

Figure 1.1: Number of new malware programs per year since 2005 and in first half of 2010. [5]

According to Figure 1.1,it represent a new record with the 1,017 ,208 new malicious computer programs1 are detected, exceeding the previous half year by around 10%.

In comparison with the same period last year [5], the number was up by more than 50%. More new malicious programs have surfaced in the first half of 2010.The number of new malicious programs is likely break through the two million levels by the end of the year.

1.2 Problem Statement

The research problem had been found in this project. It is known that malware behaviors are difficult to predict and it is always attacks and it can give impact to some of data. Table 1.1 shows the research problems are occurring.

Table 1.1: Summary of Research Problems

No	Research Problems
RP 1	Malware is an epidemic lead to difficulty of identifying the behavior of the malware.

1.3 Research Question

Research Question1 (RQ1) are found based on research problem1 (RP1). One research question (RQ1) is constructed to identify the research problem as described in Table 1.2.

Table 1.2: Summary of Research Question

RP	RQ	Research Question
1	1	How can we identify the behavior of the malware?

1.4 Research Objective

There are three research objective identified for this project which are listed as below and Table 1.4 summarize the objective that can be achieve at the end of this project

RO 1: To identify the features or attributes of malware in perspective of victim and attacker.

The purpose of this research is to identify the features or attributes of this pattern of Malware in perspective of victim and attackers. So it can help user to determine whether their computer in safe environment or not.

RO2: To generate attack pattern for malware in perspective of victim and attacker.

This research used network analyzer to generate the attack pattern for malware in perspective of victim and attacker. So, it helps to identify this kind of malware if it occurs.

RO3: To generalize the attack pattern in perspective of victim and attacker.

Based on research question1 and research problem 1, we also can generalize the attack pattern of this malware in perspective of victim and attacker.

Table 1.3: Summary of Research Objectives.

<table>
<tr><td rowspan="4">RP</td><td rowspan="4">RQ</td><th>RO</th><th>Research Objective</th></tr>
<tr><td>1</td><td>To identify the features to attributes of malware in perspective of victim and attacker.</td></tr>
<tr><td>2</td><td>To generate attack pattern for malware in perspective of victim and attacker.</td></tr>
<tr><td>3</td><td>To generalize the attack pattern in perspective of victim and attacker.</td></tr>
</table>

The scope for this project will describe in next section.

1.5 Scope

The scope of this research will focus on some issues as stated below:

1. This research just only focuses on one type of traditional worm which is Blaster.T
2. This research focuses on attack pattern in perspective of victim and attackers.
3. For this research, we use network traffic data (tcpdump) for identifying the pattern of this malware and later on generate the pattern in perspective of victim and attacker.

1.6 Project Significances

To determine the pattern of the malware from the data that we have and can generates attack pattern. Then, we can also know the attributes of this malware in perspective of victim and attackers.

1.7 Conclusion

This chapter helps to understand what the project background, scope of the project and problem statement clearly before started this project. Malware programs can cause your computer to become unbearably slow and unstable in addition to all the other havoc they wreak [6]. Blaster.T is one of them. In the next chapter, will explain about literature review and project methodology.

CHAPTER II

LITERATURE REVIEW AND PROJECT METHODOLOGY

2.1 Introduction

In this chapter, the study tries to understand about malware and the pattern of it. Some literature reviews on malware issue, current approach used in detecting malware and others related issue are reviews and analyze to achieve intention above. The findings from literature reviews especially information about malware in perspective of victim and attacker will help to achieve the research question (RQ1) and research objective (RO1) that had been mention in Chapter 1.

The fact and finding that researcher get from journal, book or website and the project requirement including the software, hardware also will described in this chapter. This chapter also describe about project methodology that used in this project. Project methodology is a combination of step-by-step methods and techniques for successful planning of projects. For develop this project, it combines many of disciplines, project analysis, design and development, implementation, testing and evaluate in order to complete this project.

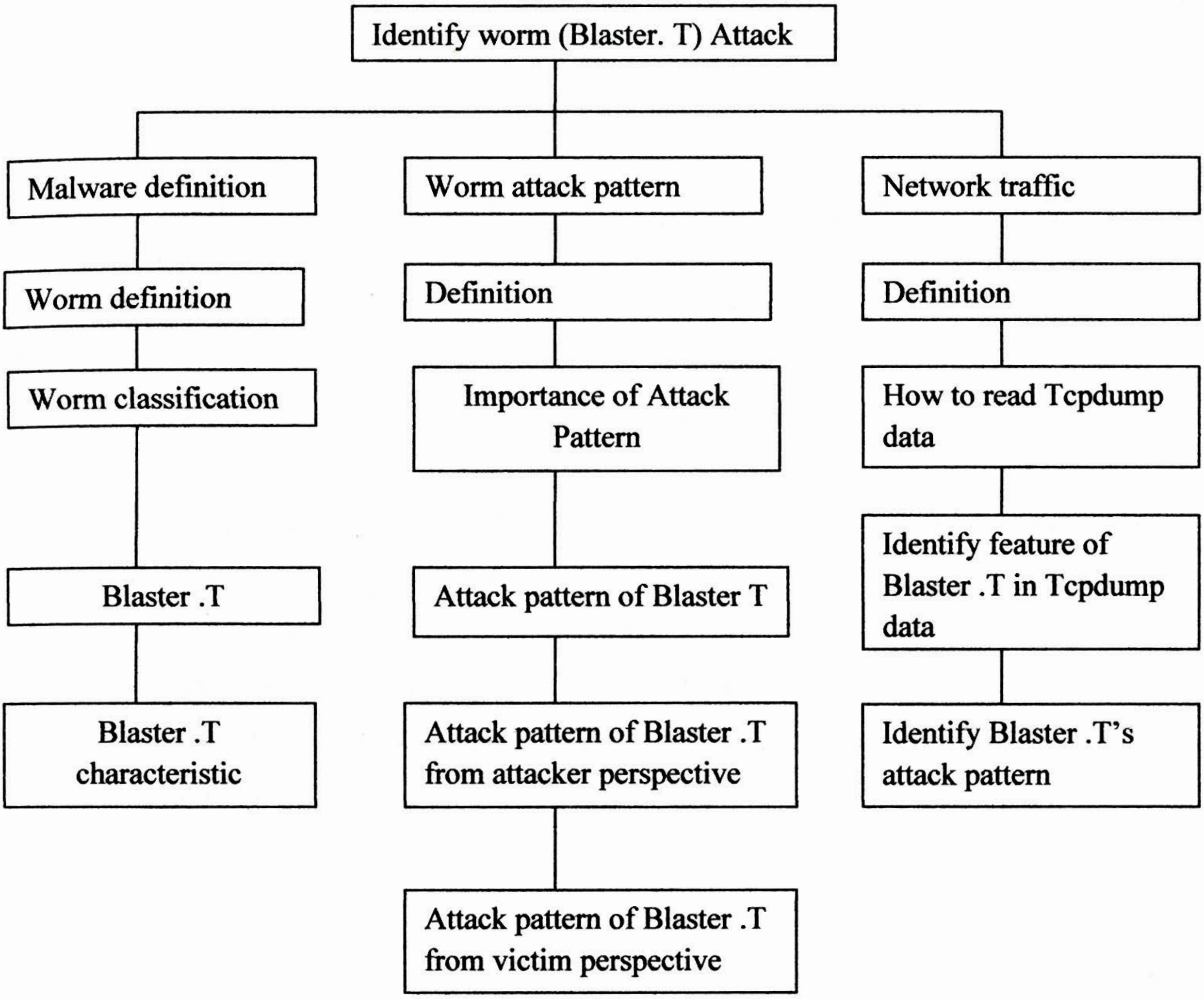
Identify worm (Blaster. T) Attack
Malware definition
Worm definition
Worm classification
Blaster .T
Blaster .T characteristic
Worm attack pattern
Definition
Importance of Attack Pattern
Attack pattern of Blaster T
Attack pattern of Blaster .T from attacker perspective
Attack pattern of Blaster .T from victim perspective
Network traffic
Definition
How to read Tcpdump data
Identify feature of Blaster .T in Tcpdump data
Identify Blaster .T's attack pattern

Figure 2.1: Literature Review Phase

Figure 2.1 is a detail phase about malware. This project will focus on identify worm (Blaster.T).

2.2 Malware

Malware is a one of malicious software that design to gather sensitive information and also to disrupt computer operation. Other information about malware is providing in next section.

2.2.1 Overview of Malware Issue

Since then and now, attack of malware still the issues that always give impact to computer system whether to individuals or organizations.

According to [4], Security for modern computer systems is relatively weak due to malware activities. Malware is one of the major security threats in computer and network environment. In order to learn and understand the malwares, behavior-based technique that applied dynamic approach is the possible solution for identification, classification and clustering the malwares [9].

Many of the most visible and serious problems facing the Internet today depend on a vast ecosystem of malicious software and tools. Spam, phishing, denial of service attacks, botnets, and worms largely depend on some form of malicious code, commonly referred to as malware. Malware is often used to infect the computers of unsuspecting victims by exploiting software vulnerabilities or tricking users into running malicious code [8].

2.2.1.1 Malware Definition

A lot of research has been done in order to clarify the definition of malware. According to [7], malware is a malicious software .The malicious intention is not generally directly observable. Even if it has destructive consequences, Malware is not a "bug" or a defect in a legitimate software program. The malware implies malice of forethought by malware inventor with the intention to disrupt or damage a system [1].

The task, tools and technique for fighting malware is identified. The Task, tools and techniques for fighting malware is shown in Table 2.1.