

CONTENTS

Originality Statements

Agreement Page

ABSTRACT iv

UCAPAN TERIMA KASIH v

PREFACE vii

Contents viii

List of Figures x

List of Tables xi

1 INTRODUCTION 1

- 1.1 Background 1
- 1.2 Problem Formulation 2
- 1.3 Objectives 3
- 1.4 Scope of Work 3
- 1.5 Research Method 3
- 1.6 Bachelor's Thesis Organization 4

2 BASIC CONCEPT 6

- 2.1 Webserver 6
- 2.2 Transport Layer 6
 - 2.2.1 Transmission Control Protocol (TCP) 7
 - 2.2.2 User Datagram Protocol (UDP) 9
- 2.3 Denial of Service (DoS) and Distributed Denial of Service (DDoS) . 9
 - 2.3.1 SYN Flood Attack 11
 - 2.3.2 UDP Flood Attack 12
- 2.4 Snort 12
- 2.5 Wireshark 13
- 2.6 Zabbix 13

3	SYSTEM PLANNING	15
3.1	System Design	15
3.1.1	System Description	15
3.1.2	System Requirement	16
3.2	Installation of VMs on VMware	18
3.3	Configure Server's VM	19
3.3.1	Apache2 Installation	19
3.3.2	Zabbix Installation	20
3.3.3	Wireshark Installation	21
3.4	Configure Router's VM	22
3.5	Configure Client's VM	24
3.6	Research Scenario	24
3.6.1	Testing The Total Incoming Packets	25
3.6.2	Testing Using Snort	25
3.6.3	Testing Network Traffic	25
4	PERFORMANCE EVALUATION	27
4.1	Testing The Total Incoming Packets	27
4.1.1	Client Connection	27
4.1.2	Total Incoming Packet From Attackers	29
4.2	Testing Using Snort	32
4.2.1	Client Connection When Snort Active	32
4.2.2	Total Packet Dropped by HIPS Snort	33
4.3	Testing Network Traffic	34
5	CONCLUSIONS	36
5.1	Conclusion	36
5.2	Suggestion	37
	Bibliography	38