

LIST OF FIGURES

2.1	OSI Model and TCP/IP Model	7
2.2	TCP Handshaking	8
2.3	TCP Segmentation	8
2.4	UDP Workflow	9
2.5	Denial of Service (DoS)	10
2.6	Distributed Denial of Service (DDoS)	10
2.7	SYN Flood Attack	11
2.8	UDP Flood Attack	12
3.1	System design block diagram	16
3.2	Research Flowchart	18
3.3	VMs are installed	19
3.4	Apache2 is installed	20
3.5	Zabbix is installed	21
3.6	Wireshark is installed and ready to use	22
4.1	Impact DoS and DDoS to the client connection	29
4.2	Average packet from attackers	30
4.3	Snort result for DDoS UDP collision packets evidence	30
4.4	Snort result for DDoS UDP collision packets evidence	31
4.5	Snort result for DDoS UDP collision packets evidence	31
4.6	Client connection when Snort active	32
4.7	Total Packet Dropped by HIPS Snort	33
4.8	Total Packet Dropped by HIPS Snort	34
4.9	Comparison network traffic during test	35