

CONTENTS

APPROVAL PAGE	i
SELF DECLARATION AGAINST PLAGIARISM.....	ii
ABSTRACT	iii
DEDICATION.....	iv
ACKNOWLEDGMENTS.....	v
CONTENTS.....	vi
LIST OF FIGURES.....	viii
LIST OF TABLES.....	x
LIST OF ABBREVIATION	xi
CHAPTER 1.....	1
THE PROBLEM	1
1.1 Rationale	1
1.2 Theoretical Framework.....	3
1.3 Conceptual Framework/Paradigm.....	5
1.4 Statement of the Problem.....	6
1.5 Hypothesis.....	6
1.6 Assumption	7
1.7 Scope and Delimitation.....	8
1.8 Importance of the Study	9
CHAPTER 2.....	11
REVIEW OF LITERATURE AND STUDIES	11
2.1 Intrusion Prevention System (IPS) with Suricata.....	11
2.2 SQL Injection, Cross-Site Scripting (XSS) and Command Injection	12
2.3 ELK Stack	14
CHAPTER 3.....	16
RESEARCH METHODOLOGY.....	16

3.1	Research Methods	16
3.2	System Model.....	19
3.3	Intrusion Prevention System with Suricata	20
3.4	Suricata Configuration	21
3.5	ELK Stack	30
3.6	Testing Scenarios and Parameters	32
CHAPTER 4.....		35
DATA PRESENTATION AND ANALYSIS		35
4.1	Detection and Traffic Blocking Test Based on Signatures in Suricata.....	35
4.2	Validation of Suricata JSON Logs with Elasticsearch Logs	36
4.3	Validation of Log Visualization in Discover on Elasticsearch.....	39
4.4	Intrusion Prevention System (IPS) Suricata on Damn Vulnerable Web Application (DVWA).....	41
4.5	Analysis of Flow Bytes and Response Time on SQL Injection, XSS and Command Injection Payloads in DVWA.....	59
4.6	Evaluation of Network Traffic Performance and IPS Effectiveness in Mitigating Slow HTTP Attacks	77
4.7	Performance Comparison of CPU and Memory Utilization	80
CHAPTER 5.....		82
CONCLUSIONS AND RECOMMENDATIONS		82
5.1	Conclusions	82
5.2	Recommendations	83
REFERENCES.....		85