



# **An Open-Source Solution for Corporates to Implement Scenario based Intrusion Detection for Incident Response**

**D.S Kithulgoda**

Reg. No. MS20907198

**M.Sc. in IT**

**Specialized in Cyber Security**

Supervisor : Mr. Amila Nuwan Senarathne

December 2021

Dissertation submitted in partial fulfillment of requirements for the  
Degree of Master of Science in Information Technology - Specialized  
in Cyber Security

**Faculty of Graduate Studies and Research  
Sri Lanka Institute of Information Technology**

# Table of Contents

Table of Contents.....	2
List of Figures .....	3
List of Tables .....	4
Declaration.....	5
Acknowledgement .....	6
Abstract.....	7
Chapter 1 Introduction .....	8
1.1 Context and Background.....	8
1.2 Problem Statement.....	11
1.3 Research Objectives and Questions.....	13
Chapter 2 Literature Review .....	15
Chapter 3 Research Methodology .....	24
3.1 NIDS and SIEM Configuration .....	29
3.2 Attack Types Coverable by the Detection Engine.....	38
3.2.1 Playbook : Malicious Network Behavior .....	39
3.2.2 Playbook : Ransomware Attack .....	42
3.2.3 Playbook : Phishing Scam / Fraud.....	44
3.2.4 Playbook : Distributed Denial of Service (DDoS).....	47
3.2.5 Playbook : Worm Infection .....	50
3.2.6 Playbook : Windows Intrusion .....	52
3.2.7 Playbook : Unix (Linux) Intrusion .....	55
3.3 Addition : Threat Hunting Platform .....	57
3.4 Addition : Open Source Intelligence (OSINT).....	58
Chapter 4 Results .....	59
4.1 How to add the entries to the TOC.....	59
Chapter 5 Conclusion .....	60
5.1 How to add the entries to the TOC.....	60
References (Bibliography).....	61
Chapter 6 Formatting Basics .....	65
6.1 How to add the entries to the TOC.....	65
Appendix .....	66
Appendix 1: NIDS and SIEM Configuration .....	66
Appendix 2: Ruleset .....	76

# List of Figures

Figure 1: Positioning of Network Intrusion Prevention System (NIPS).....	10
Figure 2: Growth of Reported Incidents [5].....	11
Figure 3: Variations of Reported Incidents [5].....	12
Figure 4: Establishing Security Relationships.....	13
Figure 5: Metrics Evaluation Process.....	17
Figure 6: Unique Functions Added.....	18
Figure 7: Realistic Scenario.....	19
Figure 8: Variance with Operating Systems [19].....	20
Figure 9: Results for Scenarios.....	21
Figure 10: Conceptual Framework.....	25
Figure 11: Switch-Span Setup.....	26
Figure 12: Network Tap/Hub Setup.....	27
Figure 13: Key Deliverables.....	28
Figure 14: Alerts in JSON Format.....	33
Figure 15: Sample JSON Alert Logs.....	37
Figure 16: LxssManager for WSL Ubuntu (Host).....	66
Figure 17: apt and dist upgrades.....	66
Figure 18: Time Zone Setup (Critical for Incident Timeline Generation).....	67
Figure 19: Snort 3 Pre-requisite Installation.....	67
Figure 20: safec for Runtime Bounds Check.....	68
Figure 21: Perl Compatible Regular Expressions.....	68
Figure 22: gperftools for performance profiling and memory checking.....	69
Figure 23: Ragel Machine Compiler and Parser Generator.....	69
Figure 24: Boost C++ Libraries.....	70
Figure 25: Hyperscan Pattern Matching Tool.....	70
Figure 26: Flatbuffers Serialization Library.....	70
Figure 27: Data Acquisition Library (DAQ).....	71
Figure 28: Snort v3.1.6.0.....	71
Figure 29: Ethtool Configuration.....	71
Figure 30: Rules Creation.....	72
Figure 31: Local Test Rule for ICMP Traffic.....	72
Figure 32: Snort lua Configuration.....	73
Figure 33: PulledPork Ruleset Downloader.....	73
Figure 34: PulledPork Configuration.....	73
Figure 35: PulledPork Rules.....	74
Figure 36: ethtool Service systemd Script.....	74
Figure 37: Snort Detection Mode.....	75
Figure 38: ICMP Rule.....	76
Figure 39: ICMP Rule Testing.....	76

## List of Tables

Table 1: Research Questions, Sub and Optional Objectives .....	14
Table 2: Independent and Dependent Variables .....	25

## Declaration

I hereby declare that this work is my original research and formally acknowledge that this MSc. Thesis contains no material that has been previously submitted to another university or higher education institution for the purpose of earning a degree or diploma and, to the best of my knowledge and belief, contains no previously published or written material by another person, except where the author's name is acknowledged in the document. Additionally, I grant Sri Lanka Institute of Information Technology the non-exclusive right to reproduce and redistribute my dissertation, in whole or in part, in print and other media for the purpose of future works, with the understanding that this right will be revoked. I reserve the right to use this material in its entirety or in part in any manner I deem appropriate (such as any book or ongoing article).

.....

.....

D.S Kithulgoda (MS20907198)

Date

The above candidate has carried out the research for the MSc. under my supervision.

.....

.....

Mr. Amila Nuwan Senarathne

Date

## Acknowledgement

Without the assistance from several individuals, the core of this research would not have been possible. I would like to express my humble appreciation to everyone who has aided me in any way with this project. My thesis supervisor, Mr. Amila Nuwan Senarathne, has provided me with exceptional guidance, encouragement, and support throughout the work and I really appreciate his assistance. I am grateful to my parents and all friends for their unflinching love and support received during my master's degree journey, as well as for everyone else who assisted me in many situations during the dissertation writing. I owe my university a debt of gratitude for providing timely and valuable course modules in the field of cybersecurity and also for guiding me in a multitude of ways to continue developing my theoretical and practical knowledge in this field while also advancing my professional career in a smooth yet revealing parallel timeline.

## Abstract

Detecting potential security compromises to aid in formulating a proactive response strategy is still a relatively new field in the local network security arena. Even managed security service providers who support these corporates on different digital security tiers face difficulties when using practical implementations that have the capability to detect and escalate to relevant parties for mitigation. This research discusses how a third-tier detection strategy can be developed with open-source toolkits like the Snort intrusion detection system as the second line of defense to support network teams. The necessity of auxiliary packages to work along with Snort must be stressed upon because the demands are higher in corporate environment settings. Some examples include Zeek and Security Onion. The placement of an IDS to perform as expected requires careful planning after a thorough examination of the relevant network diagrams. For this, the recommendation is to use dedicated hardware composed of all tools mentioned on an ad-hoc basis with a switch-span setup. It is also commonly known as port mirroring, so that an exact copy of the traffic that flows can be fed for investigation. To suit the Sri Lankan context, a stripped-down version of the MITRE ATT&CK + SHIELD Active Defense Matrix will be used to choose the applied malicious datasets and for designing the security playbooks.