

INSIDER THREAT DETECTION USING SNORT IDS

MOHAMAD BAHARUDDIN BIN MOHD ZULKIFLI

This report is submitted in partial fulfilment of the requirements for the Bachelor of
Computer Science (Computer Security)

FACULTY OF INFORMATION AND COMMUNICATION TECHNOLOGY

UNIVERSITI TEKNIKAL MALAYSIA MELAKA

2019

TABLE OF CONTENTS

DECLARATION.....	2
DEDICATION.....	3
ACKNOWLEDGEMENT.....	4
ABSTRACT.....	5
ABSTRAK.....	6
TABLE OF CONTENTS.....	7
LIST OF TABLES.....	10
LIST OF FIGURES.....	11
LIST OF ABBREVIATIONS.....	13
CHAPTER 1:INTRODUCTION.....	14
1.1 Introduction.....	14
1.2 Problem Statement.....	14
1.3 Project Objective.....	15
1.4 Project Scope.....	15
1.5 Project Contribution.....	15
1.6 Thesis Organization.....	16
1.7 Conclusion.....	17
CHAPTER 2:LITERATURE REVIEW.....	18
2.1 Introduction.....	18
2.2 Insider Threat.....	18
2.2.1 Definition of Insider Threat.....	18

2.2.2	Categories of Insider Threat.....	18
2.3	Intrusion Detection System (IDS).....	20
2.3.1	Definition of Intrusion Detection System.....	20
2.3.2	Type of Intrusion Detection System.....	21
2.3.3	Intrusion Detection System Tools for Insider Threat.....	21
2.3.4	Snort as IDS.....	23
2.3.5	Advantage and Disadvantage Using Snort.....	25
2.4	Remote Attack.....	25
2.4.1	Definition of Remote Attack.....	25
2.4.2	Remote Attack with Authorized.....	25
CHAPTER 3: METHODOLOGY.....		27
3.1	Introduction.....	27
3.2	Information Searching.....	27
3.2.1	Collect Information about Common Insider Threat Activity.....	27
3.2.2	Analysis of the Activity.....	27
3.3	Identify Pattern of Insider Threat.....	28
3.3.1	Unauthorized Remote Access.....	28
3.3.2	Misuse Resources and Application.....	30
3.4	Design Method of Implementation.....	31
CHAPTER 4: IMPLEMENTATION.....		33
4.1	Introduction.....	33
4.2	Installation Snort.....	33
4.3	Running Snort.....	34
4.4	Setting up Rules.....	37

4.5	Activities Insider Threat.....	38
4.5.1	Port Scanning.....	38
4.5.2	Denial of Services (DoS) Attack.....	38
4.5.3	Secure Shell (SSH) Connection Attempt.....	38
4.5.4	File Transfer Protocol (FTP) Attempt.....	39
4.5.5	TeamViewer Connection.....	39
CHAPTER 5: FINDING AND RESULT.....		40
5.1	Introduction.....	40
5.2	Threat Activities Detail.....	40
5.2.1	Scanning Target.....	40
5.2.2	Connection Attempt on SSH Service.....	43
5.2.3	FTP Service Attempt.....	48
5.2.4	TeamViewer Connection.....	52
5.2.5	Web Access Detection.....	56
5.2.6	Denial of Service (DoS) Attack.....	58
CHAPTER 6: PROJECT CONCLUSION.....		62
6.1	Introduction.....	62
6.2	Project Summarization.....	62
6.3	Project Limitation.....	63
6.4	Future Work.....	63
REFERENCE.....		64

REFERENCES

- Homoliak, I., Toffalini, F., Guarnizo, J., Elovici, Y. and Ochoa, M., (2018). "Insight into Insiders: A Survey of Insider Threat Taxonomies, Analysis, Modeling, and Countermeasures".
- Elmrabit, N., Yang, Shuang-Hua., Yang, L., (2015). "Insider Threat in Information Security: Categories and Approaches".
- Center, C.I.T, (2011). "Insider Threat Control: Using a SIEM signature to detect potential precursors to IT sabotage"
- F. L. Greitzer, J. Strozer, S. Cohen, J. Bergey, J. Cowley, A. Moore, and D. Mundie, (2014), "Unintentional Insider Threat: Contributing Factors, Observables, and Mitigation Strategies,"
- Waters, M. D. (2016). "Identifying and Preventing Insider Threats", Eastern Kentucky University.
- Choi, B. and Cho, K., 2012. Detection of Insider Attacks to the Web Server. JoWUA, 3(4), pp.35-45.
- Mehra, P., 2012. A brief study and comparison of snort and bro open source network intrusion detection systems. International Journal of Advanced Research in Computer and Communication Engineering, 1(6), pp.383-386.
- R. Chi, (2014), "Intrusion Detection System Based on Snort", Chap82, pp. 657-664
- Kumar, V. and Sangwan, O.P., 2012. Signature based intrusion detection system using SNORT. International Journal of Computer Applications & Information Technology, 1(3), pp.35-41.
- Pir, R.M., 2014. Intrusion detection techniques and open source intrusion detection (IDS) tools. International Journal of Engineering Development and Research, 2(3), pp.3290-3295.

Scott, C., Wolfe, P. and Hayes, B., 2004. Snort? For Dummies

Rajesh, K., 2009, accessed 28 April 2019, <<https://www.excitingip.com/636/snort-open-source-intrusion-detection-system/>>

Paliwal, S. and Gupta, R., 2012. Denial-of-service, probing & remote to user (R2L) attack detection using genetic algorithm. International Journal of Computer Applications, 60(19), pp.57-62.