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

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.