8. Related Work

A number of research studies have been conducted in the multi-stage attacks detection area. One of the studies [18] proposes a correlation framework that combines two engines, online and offline, and uses two mechanisms, high quality knowledge-based and statistical-based correlation. The proposed framework achieved a 92% multi-stage detection rate and 21.8% false positive rate during their lab experiments. This approach reduces the computation expenses by analysing only alerts received by IDS. However, the massive dependence on alerts received by IDS may lead to missing capturing attacks if alerts are not received.

Another study [19] proposed a system that follows the attack scenario construction approach. This approach is based on associating two security incidents, and it tries to find consequences of one incident and prerequisites for the incident that may occur later. The strong point of this approach is the ability to construct new attacks created by a mixture of known attacks that can be detected. On the other hand, attacks cannot be tracked without finding cause and effect of these attacks. Moreover, it requires a large consumption of computer resources.

Another study was based on using Hidden Markov Models (HMM) [20]. This study found that the HMM approach achieved greater classification accuracy, compared to other approaches. However, they reported that the accuracy obtained was at the expense of additional computations.

The proposed solution has an advantage over the above-mentioned solutions by checking the identity and the traffic contents rather than the traffic contents only. However, it may require more hardware resources as it has got two components. In addition, the complexity of the system is highly dependent in optimizing the number of models added to the system.

9. Conclusion and Future Work

The proposed approach in this paper to detecting multi-stage attacks is based on a hybrid approach that involves evaluating IP addresses participating in monitored network traffic using fuzzy logic. In addition, it involves using the PQS approach, which checks the traffic contents. The identity checker (IP info-based component) has been evaluated individually using a metrics-based approach. It has a medium score from the logistics perspective. On the other hand, it has a high score when looking from the design perspective. The last part of the evaluation looks at the system performance, and it was found that the system achieved a good performance with zero false positive and a high detection rate. However, it fails to detect multi-stage attacks if IP addresses participating in the traffic are not classified as malicious IP addresses. Such cases will be handled using the PQS approach.

It is planned to add more models to the PQS-based components then evaluating individually using the metrics-based approach. When adding more models, optimizing the number of models by combining similar models within one model will be considered in order to improve the performance of the system overall.

10. References

[1] D. Clark, “The Problem isn't Attribution; It's Multi-Stage Attacks” the Re-Architecting the Internet Workshop, 2010, Article No.11.

[2] J. Muila, A Novel Intrusion Detection System (IDS) Architecture, 2010.

[3] Tal Global. (2011) Operation Shady Rat – What It Really Means, and What You Can Learn From It? [Online] Available from: http://talglobal.com/operation-shady-rat-what-it-really-means-and-what-you-can-learn-from-it/. [Accessed: 19th Feb 2015]

[4] S. Rajasekaran, G.A. Pai, “Neural Networks, Fuzzy Logic and Genetic Algorithm: Synthesis and Applications” 2003, PHI Learning Pvt. Ltd.

[5]P. Alberto, A. Sala, and M. Olivares, “Fuzzy Logic Controllers. Methodology. Advantages and Drawbacks” [Online] Available from: http://www.softcomputing.es/estylf08/es/2000-X%20Congreso/01%20SESION%20INAUGURAL.pdf [Accessed: 19th April 2015]

[6]K. Pulo, “Fuzzy Logic vs Machine Learning” , [Online] Available from: http://www.kev.pulo.com.au/ai/ fuzzyml_report/ [Accessed: 20th April 2015]

[7]A. Chitrey, “prehensive Study of Social Engineering Based Attacks in India to Develop a Conceptual Model” IJINS ,2012. vol.1, n.4

[8]B. Hall, 2011 Countering Web Injection Attacks: A Proof of Concept, MSc thesis, University of Manchester UK.

[9]G. Cybenko, et al., "An overview of process query systems", Proc. SPIE 5403, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense III, 183 (September 15, 2004)

[10]G. Cybenko, and V. Berk (2007): “Process Query Systems”, IEEE Computer

[11]TP Group, Network Trace Files [Online] Available from: http://www.tp.org/jay/nwanalysis/traces/General%20Trace%20Files/ [Accessed: 24th Feb 2015]

[12]Mcafee. Operation Shady Rat – What It Really Means, and What You Can Learn From It? [Online] Available from:http://www.symantec.com/connect/blogs/truth-behind-shady-rat/ . [Accessed: 25th Feb 2015]

[13]Neutrino API [Online] Available from: https://www.neutrinoapi.com/. [Accessed: 25th Feb 2015]

[14]Fraudd Lab API [Online] Available from: https://www.fraudlabs.com . [Accessed: 25th Feb 2015]

[15]Mathworks Operation Shady Rat – What Is Mamdani-Type Fuzzy Inference? [Online] Available from: http://uk.mathworks.com/help/fuzzy/what-is-mamdani-type-fuzzy-inference.html. [Accessed: 26th April 2015]

[16]G. A. Fink, "A Metrics-Based Approach to Intrusion Detection System Evaluation for Distributed Real-Time Systems" Information TransferTechnology Group, 2002, Code B35, Naval Surface Warfare Center, Dahlgren Division

[17]I. Greogrio, et al.., "Detection of Complex Cyber Attacks" Proc. SPIE 6201, Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security and Homeland Defense V, 620106 (May 10,2006); doi:10.1117/12.670131

[18]F. Alserhani, M. Akhlaq, I. Awan, A. Cullen, and A. Mellor (2009): "Multi-Tier Evaluation of Network Intrusion Detection Systems" Journal for Information Assurance and Security (JIAS), 5 (4): 301-310.

[19]S. Templeton and K. Levit. A requires/provides model for computer attacks. In Proc. of New Security Paradigms Workshop, pages 31 – 38. September 2000.

[20] D. Ourston, S. Matzner,W. Stump, and B. Hopkins. Applications of hidden markov models to detecting multistage network attacks. In Proceedings of the 36th Hawaii International Conference on Systems Sciences, Los Alamitos, CA, USA, 2003 2003. IEEE Comput. Soc. 36th Hawaii International Conference on Systems Sciences, 6-9 January 2003, Big Island, HI, USA.

