

ARC '18

مؤتمر مؤسسة قطر
السنوي للبحوث

QATAR FOUNDATION
ANNUAL RESEARCH CONFERENCE

البحث والتطوير: التركيز على
الأولويات، وإحداث الأثر

R&D: FOCUSING ON PRIORITIES,
DELIVERING IMPACT

20-19 مارس
19-20 MARCH



مؤسسة قطر
Qatar Foundation

إطلاق قدرات الإنسان.
Unlocking human potential.

Computing & Information Technology - Poster Display

<http://doi.org/10.5339/qfarc.2018.ICTPD914>

Framework for Visualizing Browsing Patterns Captured in Computer Logs

Noora Fetais*, Rachael Fernandez

KINDI Center for Computing Research, Qatar University
* n.almarri@qu.edu.qa


Research Problem An Intrusion Detection System (IDS) is used for preventing security breaches by monitoring and analyzing the data recorded in log files. An IDS analyst is responsible for detecting intrusions in a system by manually investigating the vast amounts of textual information captured in these logs. The activities that are performed by the analyst can be split into 3 phases, namely: i) Monitoring ii) Analysis and iii) Response [1]. The analyst starts by monitoring the system, application and network logs to find attacks against the system. If an abnormality is observed, the analyst moves to the analysis phase in which he tries to diagnose the attacks by analyzing the users' activity pattern. After the reason has been diagnosed, appropriate steps are taken to resolve the attacks in the response phase. The analyst's job is time-consuming and inevitably prone to errors due to the large amount of textual information that has to be analyzed [2]. Though there have been various frameworks for visualizing information, there hasn't been much research aimed at visualizing the events that are captured in the log files. Komlodi et al. (2004) proposed a popular framework which is enriched with a good set of requirements for visualizing the intrusions in an IDS. However, they do not provide any details for handling the data in the logs which is essentially the source of data for an IDS, nor do they provide any tasks for predicting an attack. It has also been identified that current IV systems tend to place more importance on the monitoring phase over the other two equally important phases. Hence, a framework that can tackle this problem should be developed. **Proposed Framework** We propose a framework for developing an IDS which works by monitoring the log files. The framework provides users with a set of parameters that have to be decided before developing the

© 2018 The Author(s), licensee HBKU Press. This is an open access article distributed under the terms of the Creative Commons Attribution license CC BY 4.0, which permits unrestricted use, distribution and reproduction in any medium, provided the original work is properly cited.

دار جامعة حمد بن خليفة للنشر
HAMAD BIN KHALIFA UNIVERSITY PRESS



Cite this article as: Fetais N and Fernandez R. (2018). Framework for Visualizing Browsing Patterns Captured in Computer Logs. Qatar Foundation Annual Research Conference Proceedings 2018: ICTPD914 <http://doi.org/10.5339/qfarc.2018.ICTPD914>.



IDS and supports the classification of activities in the network into 3 types, namely: Attack, Suspicious and Not Attack. It also provides phase-specific visualization tasks, and other tasks that are required for extracting information from log files and those that limit the size of the logs. We also outline the working of a Log Agent that is responsible for collecting information from different log files and then summarizing them into one master log file [3]. The proposed framework is applied on a simple file portal system that keeps track of users who access/delete/modify an existing file or add new files. The master log file captures the browsing patterns of the users that use the file portal. This data is then visualized to monitor every activity in the network. Each activity is visualized as a pixel whose attributes describe whether it is an authorized activity or an illegal attempt to access the system. In the analysis phase, tasks that help to determine a potential attack and the reasoning behind the classification of an activity as Suspicious or Attack are provided. Finally, in the response phase, tasks that can resolve the attack and tasks for reporting the details of the attack for future analysis are provided.

References

- [1] A. Komlodi, J. Goodall, and W. Lutters, "131 An information visualization framework for intrusion detection," CHI'04 Extended Abstracts on . . . , pp. 1743- 1746, 2004. [Online]. Available: <http://dl.acm.org/citation.cfm?id=1062935>
- [2] R. Fernandez and N. Fetais, "Framework for Visualizing Browsing Patterns Captured in Computer Logs Using Data Mining Techniques," International Journal of Computing & Information Sciences, vol. 12, no. 1, pp. 83-87, 2016.
- [3] H. Kato, H. Hiraishi, and F. Mizoguchi, "Log summarizing agent for web access data using data mining techniques 2 . Approach for web access log mining 3 Analysis of web access log 4 . Design of Log Analysis System," Analysis, vol. 00, no. C, pp. 2642-2647.