Literature Review - Live Forensics and Incident Response system

The cyber security environment nowadays is complicated and it has never been simple. And because attacks evolve every day as attackers become more inventive, it is critical to properly define cyber security and identify what constitutes good cyber security. This requires enterprises who want to protect their data from attack to set up an incident response system to collect and analyze data during an attack. Incident response is an organized approach to addressing and managing the effects or consequences of a cyberattack. Ultimately, the goal is to effectively manage the incident so that the damage is limited and reduce recovery time and costs at a minimum way. However, the incident may still be in progress while collecting data, so it is important to continually collect forensic data to protect the system under attack. Live forensics and incident system can be implemented by combining several tools. In this review, the key features and benefits of some secreted will be outlined, which include Google Rapid Response (GRR) live forensic tool, Elasticsearch, Logstash, Kibana (ELK Stack) analytics and visualization tool and OSSEC endpoint protection tools. Following this, the comparison of different tools and how those tools relate to incident live forensics and incident system, will then be discussed.

There are three different tools which are recommended to be used to build live forensics and incident response system. Google Rapid Response is an incident response framework focused on remote live forensics. The goal of GRR is to support forensics and investigations in a fast, scalable manner to allow analysts to quickly triage attacks and perform analysis remotely. GRR was built to run at scale so that analysts are capable of effectively collecting and processing data from large numbers of machines and it consists of two parts, client and server. GRR client is a cross-platform support for Linux, OS X and Windows clients and has powerful search and download capabilities for files and the Windows registry. It also provides OS-level and raw file system access and functions like secure communication infrastructure designed for internet deployment and detailed monitoring of client CPU, memory, IO usage and self-imposed limits. Meanwhile, GRR server has fully fledged response capabilities handling most incident response and forensics tasks and provides enterprise hunting support as well as fast and simple collection of hundreds of digital forensic artifacts. The GRR sever is also able to support variety of formats and output plugins with powerful data export features and provide fully scalable back-end capable of handling large deployments and automated scheduling for recurring tasks. Its asynchronous design allowing future task scheduling for clients and designed to work with a large fleet of laptops.

The ELK Stack is comprised of three components, which are Elasticsearch, Logstash and kibana. Elasticsearch is a log searching tool that allows for near real-time searching of log data. Logstash is the mechanism that handles the intake of log files from the sources across the network, process log entries, and finally, allows for their output through a visualization platform. There are several benefits as well as common pitfalls of using ELK stack. But it is very useful for analyzing data and dealing with logs and visibility is the key here. Kibana serves as the visual interface or dashboard of the ELK Stack. This platform allows analysts to gain insight into the data through the use of dashboards. Kibana also allows analysts to drill down into specific key data points for detailed analysis. Incident response analysts can customize the dashboards so that the most critical information, such as intrusion detection logs or connection logs, are immediately available for review. While there are also some limitations of Kibana. Kibana cannot perform aggregations across fields that contain nested objects. It also cannot search on nested objects when Lucene Query Syntax is used in the query bar. Incident response analysts who are involved in parsing and examining log files would be best served by evaluating, and possibly deploying, the ELK Stack in their environment if there is currently no solution in place that allows for the aggregation and deep mining of log files for incident investigations.

OSSEC is a platform to monitor and control systems. It mixes together all the aspects of HIDS (host-based intrusion detection), log monitoring, and Security Incident Management (SIM)/Security Information and Event Management (SIEM) together in a simple, powerful, and open source solution. It performs log analysis, integrity checking, Windows registry monitoring. The key benefits of OSSEC are compatible with multiple platforms, integration with current infrastructure and real-time and configurable alerts. It also can check the integrity of files to alert user when attack happens. The function of active response allows OSSEC to take immediate action when specified alerts are triggered. This may prevent an incident from spreading before an administrator can take action. Although OSSEC offers an open-source web user interface (Web UI), that is very basic and not very customizable. To change this, companies started to integrate with Elasticsearch, Logstash, and Kibana (ELK Stack) giving users more freedom to customize dashboards and find the data they needed faster.

Cohen, M.I., Bilby, D., & Caronni, G. (2011). Distributed forensics and incident response in the enterprise.

Meyer, R. (2008). Challenges of Managing an Intrusion Detection System

(IDS) in the Enterprise.

Sigmon, B.A. (2016).AUTOMATING INCIDENT RESPONSE USING OSSEC.

https://www.fireeye.com/current-threats/what-is-cyber-security.html

https://www.coe.int/en/web/octopus/blog/-/blogs/live-data-forensics-or-why-volatile-data-can-be-crucial-for-your-cases

http://grr-doc.readthedocs.io/en/v3.2.0/what-is-grr.html

https://practicalassurance.com/blog/ossec-elk-stack-integration/

https://www.elastic.co/guide/en/kibana/current/nested-objects.html

https://www.safaribooksonline.com/library/view/digital-forensics-and/9781787288683/57b5d81a-367a-47b6-973d-2a939050baca.xhtml

https://ossec-docs.readthedocs.io/en/latest/manual/non-technical-overview.html