Capstone Interim Project Report

Digital Forensics & Incident Response over a Remote Network

|  |  |
| --- | --- |
| Team Name: Polaris Sight |  |
| Owen Charters | N8962375 |
| Curtis Dooley | N9152237 |
|  |  |
|  |  |

# Introduction

## Client

The project that we are developing was conceived by our client, Dr Ernest Foo.

The client explained that the idea for the project stems from his time working with a large government organisation who lamented a lack of live forensic analysis software. In particular, the ability to assess an ongoing attack, and to determine the actions and aim of the hacker as well as the extent to which the system was compromised. Learning what the hackers are doing also helps to protect against future attacks.

The system is to be deployed on critical infrastructure. It should be scalable to a large network, and this should be simulated through virtual machines. It should also be suitable for small businesses, and interpretable by a layman. The primary goal is detection and analysis while maintaining forensic readiness.

## Domain

The project consists of elements belonging to several discrete domains. Key amongst these are:

Incident Response

Incident Response is the discipline of detecting and managing the response to security events. This can include data logging, scans, malware analysis and other tasks as well as the procedure of coordinating systems and staff in order to achieve the best result.

Digital Forensics

Digital Forensics is the practice of investigating devices that have undergone some kind of criminal influence, intrusion, damage or other incident resulting in the Confidentiality, Integrity or Availability of data. In the context of our project, this could include things such as brute force authentication attempts, file theft or manipulation or malicious registry keys. Forensic readiness is then the practice of being able to detect and log such events, as well as taking steps to mitigate or restore damage.

Networking

Networks are connected computers that exchange data. This can include a connection to the internet or simply a local network. In the case of our project, we aim to replicate the environment of a small business by connecting several computers of varying operating systems and states.

## Technical Description

The project aims to unify multiple open source security software products into one centralised incident response system. Key security software products comprising this are:

Google Rapid Response (GRR)

Google Rapid Response, an effective digital forensics tool that can perform forensic tasks such as file and registry searches, memory analysis and overall client device monitoring. It is versatile and compatible with client computers that may have operating systems such as Windows, Linux or Mac.

It allows for an administrator to set up a front-end server that can be accessed via an authenticated web login. The necessary binaries are stored for the various operating systems that the administrator may encounter.

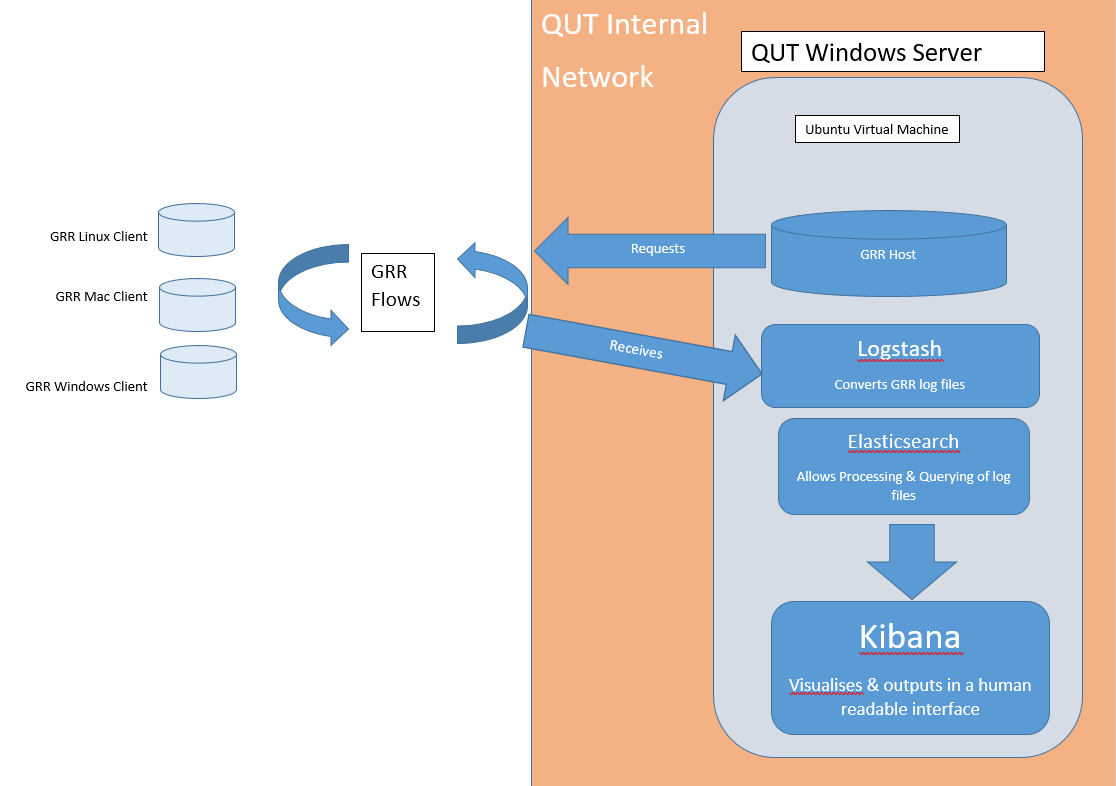
These can be installed on their client’s computers allowing for communication with GRR using a HTTP POST request. From the GUI (Graphical User Interface) within the GRR front-end server, the administrator can initiate flows and hunts that will perform previously stated forensic tasks. The output of these is in the form of security logs such as YAML files.

ELK Stack (Elasticsearch, Logstash and Kibana)

ELK Stack, a platform that combines three security software products into one to provide better capabilities in events that require incident response. ELK Stack achieves this through effective searches and filters provided by Elasticsearch, efficient storage and categorisation of security event logs provided by Logstash and ease of use via visualisation provided by Kibana.

While tools such as GRR will aim to achieve efficiency and usability in its operations, Logstash will still reduce the strain on an incident response system regarding the many security event logs it will receive. Furthermore, GRR lacks the ability to create searches within the security event logs which Elasticsearch allows.

These are automated and the administrator can tell it to monitor for key terms and types within the log files as well produce metrics relating to the logs. Finally, from these results with the use of Kibana the security logs can be visualised into various graphs, maps and tables. This is especially helpful to the laymen due to the complexity of YAML files making it hard to interpret the data within the file.



Literature Review - Live Forensics and Incident Response system

# Introduction

The cyber security environment nowadays is complex, and has never been simple. 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. Forensic readiness requires enterprises who want to protect their data from attack to set up a live forensics and 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 (Rouse, 2017). Ultimately, the goal is to effectively manage the incident or attack so that the damage can be limited as well as 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 and prevent further attacks.

Live forensics and incident system can be implemented by combining several tools. In this review, the comparison of different tools and how those tools relate to live forensics and incident response system will be discussed. Following this, the key features and benefits of some selected tools including Google Rapid Response (GRR) live forensic tool, Elasticsearch, Logstash, Kibana (ELK Stack) analytics and visualization tool and OSSEC endpoint protection tools, will then be outlined.

# Discussion

The tools that can be used to develop incident response system are multitudinous; with the development and maturity of computer and software technology, the functions of software and tools are becoming more powerful and complicated. Different tools with different features can be combined to achieve the functions of live forensics and incident response system. If the tools are sorted by functions, it can be broadly divided into five categories, which include evidence collection tools, incident management tools, log analysis tools, memory analysis tools and all in one tools (Wahnon, 2015).

In the past several years, as incident response tools have advanced, a single tool with several functions may achieve automation in security controls and processes, and the viable options for incident response automation are various. There are five top open source incident response automation tools chosen by Cyberbit’s incident response experts, which are CimSweep, GRR Rapid Response, TheHive, osquery and MIG, to improve incident response process, and assess incident response automation needs (Ashman, 2017). CimSweep is a suite of CIM/WMI-based tools which are able to perform incident response and threat hunting remotely on all versions of Windows. GRR Rapid Response is an agent-based cross-platform framework, and various data collection tasks such as memory analysis, file and registry search, and client device monitoring can be performed through on it. TheHive is a scalable open source and free security incident response platform, it is designed for SOCs, CSIRTs, CERTs and any information security practitioner to deal with security incidents that need to be investigated and acted upon swiftly more easily. osquery is an operating system instrumentation framework and it exposes an operating system as a high-performance relational database to allow developers to write SQL-based queries to explore operating system data. MIG is an agent-based investigation platform that allows real-time querying and investigation of endpoints. The endpoint data returned by platform can be used for file, network and memory inspection.

These tools are all able to achieve multiple functions like collecting data or dealing with security incidents. In a 2015 report, forensic expert Alissa Torres stated that automation of any incident response process should focus on three major phases: continuous data collection, aggregating and applying threat intelligence and streamlining live response capabilities (Shackleford, 2016). In implementing automated continuous data collection strategies, security teams can gain deeper insight into historical system state, event logs and network traffic. The automated collection can allow security teams to know what normal system and user behavior looks like and recognize anomalous activity when it occurs. By centralizing continuous network data collection, powerful correlations can be drawn with regards to threat activity, attack and reconnaissance techniques and threat actors. Streamlining of the IR process and reduction of inefficiencies is a critical element of an effective automated plan. The need for automation and efficiency of process and procedure exists no matter what type of incident an organization encounters (Torres, 2015).

Many of the tools have the capabilities of ongoing data collection such as CIRTKit, but only partial functions of the live forensics and incident system can be realized; they may not be capable of remote live forensics or scalable for enterprise. So it is important to choose appropriate tools to be combined to build the live forensics and incident response system.

There are three different tools mentioned in the project outline to be used to build live forensics and incident response system, which represent three different functions: live forensic analysis, visualization and endpoint protection. GRR is designed to be scalable, opening the door for continuous enterprise wide forensic analysis (Cohen, Bilby & Caronni, 2011). Analysts can use GRR to quickly classify attacks and execute remote analysis and this helps analysts collect and process data from numerous machines effectively. Various forensic tasks can be performed on the client machine in GRR client after the server and agent are deployed, such as analyzing the memory, searching various settings and managing configuration options (Morgenstern, 2016).

Kibana is one of the components in ELK Stack, it provides the platform of analytics and visualization to give a better understanding of the data. By using it, the analysts can customize the dashboards so that the most critical information, such as intrusion detection logs or connection logs, are immediately available for review.

OSSEC is a free open source HIDS (host-based intrusion detection system) and LIDS (log-based intrusion detection) system (Sigmon, 2016).It provides real-time alerting using log analysis signatures, and has an active response feature that allows automated execution of scripts. There are many benefits to using OSSEC in this system. The main benefit would be that it automates the incident response process of blocking attacks. By automating this process, it will save analysts time from chasing down these attacks and manually blocking them on the firewall. While the OSSEC is not very customizable, to change this, it is better to integrate with the ELK Stack giving users more freedom to customize dashboards and find the data they needed faster.

# Conclusion

In conclusion, choosing appropriate tools in a large scope of tools with different functions to build live forensics and incident response system can greatly increase the efficiency of the system as well as reduce the time spent on manually blocking common attacks. GRR Rapid Response provides the functionality to build a live forensics and incident response system. The scalability provided by GRR extends to other components of an incident response system to enable wider analysis. It helps lower the cost of response and increase the quality of evidence obtained. Although GRR is still in early stages of development, it is clear that the tool is useful for managing large scale investigations in the enterprise. Also, implementing the OSSEC will provide a central location to view all log data and correlate security events from all log sources, as well as provide more accurate attack information from the host-level.

**References**

Ashman, O. (2017). *Top 5 Open Source Incident Response Automation Tools.* Retrieved from <https://www.cyberbit.com/blog/security-operations/top-5-open-source-incident-response-automation-tools/>

Cohen, M.I., Bilby, D., & Caronni, G. (2011). Distributed forensics and incident response in the enterprise. *Digital Investigation,* 8(13), 101-110. doi: 10.1016/j.diin.2011.05.012

Morgenstern, T. (2016). *5 Open Source Malware Tools You Should Have in Your Arsenal.* Retrieved from <https://www.cyberbit.com/blog/endpoint-security/open-source-malware-analysis-tools/>

Rouse, M. (2017). *What is incident response?* Retrieved from <https://searchsecurity.techtarget.com/definition/incident-response>

Shackleford, D. (2016). *Incident response tools can help automate your security.* Retrieved from <https://searchsecurity.techtarget.com/feature/Incident-response-tools-can-help-automate-your-security>

Sigmon, B.A. (2016). Automating Incident Response Using OSSEC.

Torres, A. (2015). Automation in the Incident Response Process: Creating an Effective Long-Term Plan.

Wahnon, M. (2015). *A curated list of tools for incident response.* Retrieved April 14, 2018, from https://github.com/meirwah/awesome-incident-response