Security Log Analysis with ELK Stack and Puppet

Ronald A. Neely

Rowan University, ASRC Federal Mission Solutions

Term Project Assignment, Outline Due 2018.09.30

Advanced Cyber Security Principles and Applications

Instructor: Mike Davies, Fall 2018

Abstract

Computer system intrusions are becoming more prevalent and difficult to detect. Log analysis can provide a means to detect an intrusion occurred. However, current methods of manually analyzing logs take time and specialized knowledge. The person analyzing logs must know how to use tools that can find relevant log entries, and how to piece those entries together to determine whether and intrusion occurred. Even then the analysis effort may not be successful. And, if the analysis is successful it can take up to 18 months to detect an intrusion or anomaly.

This paper seeks to provide an exploration of the possibilities five tools provide in aiding automation of log analysis for intrusion or anomaly detection as well as configuring operational data to be logged. Four tools aid in automating log analysis. These tools comprise the ELK stack: 1) Elastic Search, 2) Logstash, 3) Kibana, and 4) Beats. Additionally, the feasibility of 5) Puppet is examined regarding its ability to configure and enable gathering of operational metrics data such as logging of metrics data application performance monitoring data.

This paper does not seek to establish or change any organizational policies or procedures regarding incident handling of an intrusion incident. Rather it focuses on whether or not any of the abovementioned tools can aid in intrusion detection, and if so, how.

Keywords: #ELK Stack #Log #Metric #Intrusion #Detection #Elastic Search # Logstash #Kibana #Beats #Puppet

Table of Contents

Table of Contents

[Abstract 2](#_Toc526100928)

[Table of Contents 3](#_Toc526100929)

[Security Log Analysis with ELK Stack and Puppet: Why? & What? 6](#_Toc526100930)

[Beats 7](#_Toc526100931)

[Description 7](#_Toc526100932)

[Screen Shot(s) 7](#_Toc526100933)

[Inputs & Outputs 7](#_Toc526100934)

[Summary of Tool 7](#_Toc526100935)

[Advantages & Disadvantages 7](#_Toc526100936)

[Logstash 8](#_Toc526100937)

[Description 8](#_Toc526100938)

[Screen Shot(s) 8](#_Toc526100939)

[Inputs & Outputs 8](#_Toc526100940)

[Summary of Tool 8](#_Toc526100941)

[Advantages & Disadvantages 8](#_Toc526100942)

[Elastic Search 9](#_Toc526100943)

[Description 9](#_Toc526100944)

[Screen Shot(s) 9](#_Toc526100945)

[Inputs & Outputs 9](#_Toc526100946)

[Summary of Tool 9](#_Toc526100947)

[Advantages & Disadvantages 9](#_Toc526100948)

[Kiabana 10](#_Toc526100949)

[Description 10](#_Toc526100950)

[Screen Shot(s) 10](#_Toc526100951)

[Inputs & Outputs 10](#_Toc526100952)

[Summary of Tool 10](#_Toc526100953)

[Advantages & Disadvantages 10](#_Toc526100954)

[Puppet 11](#_Toc526100955)

[Description 11](#_Toc526100956)

[Screen Shot(s) 11](#_Toc526100957)

[Inputs & Outputs 11](#_Toc526100958)

[Summary of Tool 11](#_Toc526100959)

[Advantages & Disadvantages 11](#_Toc526100960)

[Project Summary 12](#_Toc526100961)

[Future Implications 13](#_Toc526100962)

[End Notes / References 14](#_Toc526100963)

[Footnotes 15](#_Toc526100964)

[Tables 16](#_Toc526100965)

[Figures 17](#_Toc526100966)

Security Log Analysis with ELK Stack and Puppet: Why? & What?

[The body of your paper uses a half-inch first line indent and is double-spaced. APA style provides for up to five heading levels, shown in the paragraphs that follow. Note that the word Introduction should not be used as an initial heading, as it’s assumed that your paper begins with an introduction.]

<Include picture of ELK Stack Here> Picture will contain:

|  |  |
| --- | --- |
| Solutions | application search, site search, enterprise search, logging, metrics, APM, business analytics, security analytics |
| Visualization, Management | Kibana |
| Storage, Search, Analysis | Elasticsearch |
| Ingest | Beats, Logstash |

<Include picture of ELK Dev Ops Instantiated by Puppet Here> Picture will contain:

Puppet instantiating configuration of ELK samples dev ops stack

Beats

# Description

Description of tool #1, how it works, algorithm(s), method(s), where obtained, author / company, size, platform / os it runs on, does it integrate with other software for added functionality (if so (if so list it). Details of how to use the tool would be nice.

# Screen Shot(s)

Color would be nice here!

# Inputs & Outputs

What comes into the tool?

What goest out of the tool?

# Summary of Tool

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

# Advantages & Disadvantages

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

Logstash

# Description

Description of tool #1, how it works, algorithm(s), method(s), where obtained, author / company, size, platform / os it runs on, does it integrate with other software for added functionality (if so (if so list it). Details of how to use the tool would be nice.

# Screen Shot(s)

Color would be nice here!

# Inputs & Outputs

What comes into the tool?

What goest out of the tool?

# Summary of Tool

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

# Advantages & Disadvantages

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

Elastic Search

# Description

Description of tool #1, how it works, algorithm(s), method(s), where obtained, author / company, size, platform / os it runs on, does it integrate with other software for added functionality (if so (if so list it). Details of how to use the tool would be nice.

# Screen Shot(s)

Color would be nice here!

# Inputs & Outputs

What comes into the tool?

What goest out of the tool?

# Summary of Tool

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

# Advantages & Disadvantages

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

Kiabana

# Description

Description of tool #1, how it works, algorithm(s), method(s), where obtained, author / company, size, platform / os it runs on, does it integrate with other software for added functionality (if so (if so list it). Details of how to use the tool would be nice.

# Screen Shot(s)

Color would be nice here!

# Inputs & Outputs

What comes into the tool?

What goest out of the tool?

# Summary of Tool

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

# Advantages & Disadvantages

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

Puppet

# Description

Description of tool #1, how it works, algorithm(s), method(s), where obtained, author / company, size, platform / os it runs on, does it integrate with other software for added functionality (if so (if so list it). Details of how to use the tool would be nice.

# Screen Shot(s)

Color would be nice here!

# Inputs & Outputs

What comes into the tool?

What goest out of the tool?

# Summary of Tool

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

# Advantages & Disadvantages

Summary of tool #1, does it work, is it difficult to use, easy to use, was it fast or processor intensive?

Project Summary

what did you learn from all of this, what is you favorite Security Audit tool, least

favorite Security Audit tool? Why?

Future Implications

Write a few paragraphs on how Security Audit Tools could solve some

of the problems IT Security professionals face every day.

End Notes / References

Federal Agent Byron S. Collie (Australian Federal Police) Directorate of Information Warfare Headquarters Air Command, Royal Australian Air Force, (2006) *INTRUSION INVESTIGATION AND POST-INTRUSION COMPUTER FORENSIC ANALYSIS.* <https://www.mirrorservice.org/sites/ftp.wiretapped.net/pub/security/info/papers/law-enforcement/intrusion-investigation-and-post-intrusion-forensic-analysis.pdf>*.*

Dand Roscigno and Jamie Smith (2018). An Introduction to the ELK Stack for Logs and Metrics. *Elastic.co*. <https://www.elastic.co/webinars/introduction-elk-stack>.

Self.Devops. (2017) Advice on setting up Jenkins to test puppet code. *Reddit.* <https://www.reddit.com/r/devops/comments/4kee5r/advice_on_setting_up_jenkins_to_test_puppet_code>.

Koen van Gilst (2017) API testing with Jest <https://hackernoon.com/api-testing-with-jest-d1ab74005c0a>.

Footnotes

1[Add footnotes, if any, on their own page following references. The body of a footnote, such as this example, uses the Normal text style. (Note: If you delete this sample footnote, don’t forget to delete its in-text reference as well. That’s at the end of the sample Heading 2 paragraph on the first page of body content in this template.)]

Tables

Table 1

[Table Title]

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Column Head | Column Head | Column Head | Column Head | Column Head |
| Row Head | 123 | 123 | 123 | 123 |
| Row Head | 456 | 456 | 456 | 456 |
| Row Head | 789 | 789 | 789 | 789 |
| Row Head | 123 | 123 | 123 | 123 |
| Row Head | 456 | 456 | 456 | 456 |
| Row Head | 789 | 789 | 789 | 789 |

Note: [Place all tables for your paper in a tables section, following references (and, if applicable, footnotes). Start a new page for each table, include a table number and table title for each, as shown on this page. All explanatory text appears in a table note that follows the table, such as this one. Use the Table/Figure style, available on the Home tab, in the Styles gallery, to get the spacing between table and note. Tables in APA format can use single or 1.5 line spacing. Include a heading for every row and column, even if the content seems obvious. A table style has been setup for this template that fits APA guidelines. To insert a table, on the Insert tab, click Table.]

Figures



Figure 1. [Include all figures in their own section, following references (and footnotes and tables, if applicable). Include a numbered caption for each figure. Use the Table/Figure style for easy spacing between figure and caption.]

For more information about all elements of APA formatting, please consult the APA Style Manual, 6th Edition.