Vunerablity Tool Examination Paper

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

This paper examines the trials an tribulations of trying out 5 different vulnerability analysis tools in APA format.

Table of Contents

Table of Contents

[Abstract 2](#_Toc528183243)

[Table of Contents 3](#_Toc528183244)

[Tool #1: Nessus 6](#_Toc528183245)

[Description 6](#_Toc528183246)

[Screen Shot(s) 6](#_Toc528183247)

[Inputs & Outputs 6](#_Toc528183248)

[Summary of Tool 6](#_Toc528183249)

[Advantages & Disadvantages 7](#_Toc528183250)

[Logstash 8](#_Toc528183251)

[Description 8](#_Toc528183252)

[Screen Shot(s) 8](#_Toc528183253)

[Inputs & Outputs 8](#_Toc528183254)

[Summary of Tool 8](#_Toc528183255)

[Advantages & Disadvantages 8](#_Toc528183256)

[Elastic Search 9](#_Toc528183257)

[Description 9](#_Toc528183258)

[Screen Shot(s) 9](#_Toc528183259)

[Inputs & Outputs 9](#_Toc528183260)

[Summary of Tool 9](#_Toc528183261)

[Advantages & Disadvantages 9](#_Toc528183262)

[Kiabana 10](#_Toc528183263)

[Description 10](#_Toc528183264)

[Screen Shot(s) 10](#_Toc528183265)

[Inputs & Outputs 10](#_Toc528183266)

[Summary of Tool 10](#_Toc528183267)

[Advantages & Disadvantages 10](#_Toc528183268)

[Puppet 11](#_Toc528183269)

[Description 11](#_Toc528183270)

[Screen Shot(s) 11](#_Toc528183271)

[Inputs & Outputs 11](#_Toc528183272)

[Summary of Tool 11](#_Toc528183273)

[Advantages & Disadvantages 11](#_Toc528183274)

[Project Summary 12](#_Toc528183275)

[Future Implications 13](#_Toc528183276)

[End Notes / References 14](#_Toc528183277)

[Footnotes 15](#_Toc528183278)

[Tables 16](#_Toc528183279)

[Figures 17](#_Toc528183280)

Tool #1: Nessus

# Description

Nessus is a computer security tool. Specifically Nessus is a vulnerability scanner that appears to have the ability to enumerate remote services [i]. Nessus also looks for other vulnerabilities such as common misconfigurations; default or weak passwords; and susceptibility to Denial of Service (DOS) attacks [ii].

Table 1 Nessus Algorithms summarizes how Nessus works.

Table Nessus Algorithms

|  |  |
| --- | --- |
| Nessus Scan | How It Works / Algorithm [i, ii] |
| services / ports | scanning for open ports and probing them for running services |
| common misconfigurations | Proprietary algorithm |
| weak password: default, blank, common | Tries passwords on system accounts, can also use Hydra to launch a dictionary attack |
| Denial of Service (DOS) attacks | Using malformed TCP/IP packets against TCP/IP stack |

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.

[[1]](#endnote-1)[[2]](#endnote-2)

1. Rahil Arora. (2016). How does Nessus know which services are running in a host?. NY, NY: StackExchange. Retrieved October 24, 2018, from https://security.stackexchange.com/a/117219 [↑](#endnote-ref-1)
2. Wikipedia. Nessus (software). Wikipedia. Retrieved October 24, 2018, from https://en.wikipedia.org/wiki/Nessus\_(software) [↑](#endnote-ref-2)