|  |
| --- |
| Graphical user interface, text, application  Description automatically generated |
| **Lab Report** |
| COURSE: Cyber 262  LAB: SNORT Lab  Submitted BY: Jack Morgan  Date: 03/26/2022  Instructor: Hozza |
| *By submitting this report, I certify that this is my work and was not copied from other sources. Any use of public materials is cited.* |

Table of Contents

[INTRODUCTION 3](#_Toc50470226)

[SCREEN CAPTURES 3](#_Toc50470227)

[REFLECTION 7](#_Toc50470228)

# INTRODUCTION

During this lab, we will be learning how to use Snort to detect foreign alerts and signal system users to existing alerts and threats. In addition, we will be implementing five or so given rules implemented from github and creating our own rule to add as well. Lastly, we will be using Kibana to detect malicious activity such as the Ping-of-Death we will attempt to issue. While these rules we add to our system are basic, we are learning what it is like to manage alerts on a system and properly detect intruders in our systems.

# SCREEN CAPTURES

***Figure (1.1): Take a screen shot of Snort logging at least one of the ping (ICMP) attempts.***

Graphical user interface, text, application, email

Description automatically generated

*This screenshot shows multiple ICMP attempts towards the PLabOnion server using snort.*

***Figure (2.1): Take a screen shot of Snort showing that “Snort successfully validated the configuration”***

Graphical user interface, text, application, email

Description automatically generated

*This screenshot shows the successful validation of the new snort rules that we improted from GitHub to the servers desktop.*

***Figure (2.2): Include a screen shot similar to above that shows the “Fly Piggy Fly” results of a successful rule update.***

Graphical user interface, text, application

Description automatically generated

*Screenshot displays the successful update of the snort rules we implemented to the server with the “Fly Piggy Fly” result.*

***Figure (3.1): Re issue your ping attack but with parameters that made it a Ping of Death, do some research. Submit a screen showing snort displaying your Ping of Death Alerts with your ID.***

Graphical user interface, text, application

Description automatically generated

***Figure (3.2): Three Screen Shots***

1. ***Your new Rule***
2. ***The attack command you ran from Kali***
3. ***The alert being generated in Snort (Must show description of activity and your PSUID***

*Spent a lot of time trying to figure out how to add a unique rule and ended up running out of time with other deadlines and non-school related work. I will submit a lab re-do request for this lab at the end of the semester if I need to redo the lab for a better grade.*

***Figure (4.1) Post a screen of Kibana showing info that is relevant to the Snort alerts that came across through the ELK stack. This could include a graph of peaked alerts or details of NIDS alerts. Be creative. Explain your logic under the screen shot.***

Graphical user interface

Description automatically generated

This screenshot shows the overall number of misc activities recorded during the last couple minutes of performing this lab. I recorded a mix of 35 ping attempts using the ping of death command and 35 regular ping attempts. Unfortunately, when attempting to retrieve a more accurate screenshot, I accidentally dragged the graph and upon reentering Kibana, the graph would not allow me to update it to show all alerts.

# REFLECTION

During this lab we learned how to write rules to our snort system and detect intruder activity and attacks such as the ping-of-death attack we used on the plabonion system. By using the command ping 192.168.0.2 -s 65550, we were able to issue a ping that triggered the Snort system to respond to the ping with an alert. This is just one example of the many types of alerts we can create for our snort system, and these are crucial for analysts to know how to import in order to properly manage their systems. As we spend more time learning about prevention and detection systems, snort will become increasingly more important as it plays a crucial role in the detection of foreign actors and attacks as we demonstrated during this lab.