Activity: Explore signatures and logs with Suricata

Introduction

In this lab activity, you'll explore the components of a rule using Suricata. You'll also have an opportunity to trigger a rule and examine the output in Suricata. You'll use the Bash shell to complete these steps.

What you'll do

You have multiple tasks in this lab:

- Examine a rule in Suricata
- Trigger a rule and review the alert logs
- Examine *eve.json* outputs

Lab instructions

i could setup a lab 4 u if u email inquiries@naruzkurai.com or Inquiries@baseshadow.maskmy.id

---

Revision #2
Created 2 November 2023 13:11:47 by naruzkurai
Updated 2 November 2023 13:20:08 by naruzkurai