### Network-Based Intrusion Detection System Using Suricata

### **Table of Contents**

### Introduction

### Prerequisites

### Installation

### Configuration

### Suricata

### Running the System

### Testing and Validation

### Introduction

### Project Overview

### This document outlines the setup of a Network-Based Intrusion Detection System (NIDS) using Suricata. The system is configured to detect suspicious network activity and visualize alerts using the ELK stack (Elasticsearch, Logstash, Kibana).

### Objectives

### Install and configure Suricata.

### Set up the ELK stack for data visualization.

### Create custom detection rules.

### Validate the system by generating and visualizing alerts.

### Prerequisites

### A server running Ubuntu 18.04 or later.

### Sudo privileges on the server.

### Basic understanding of networking and Linux command line.

### Installation

### Suricata on KALI Linux

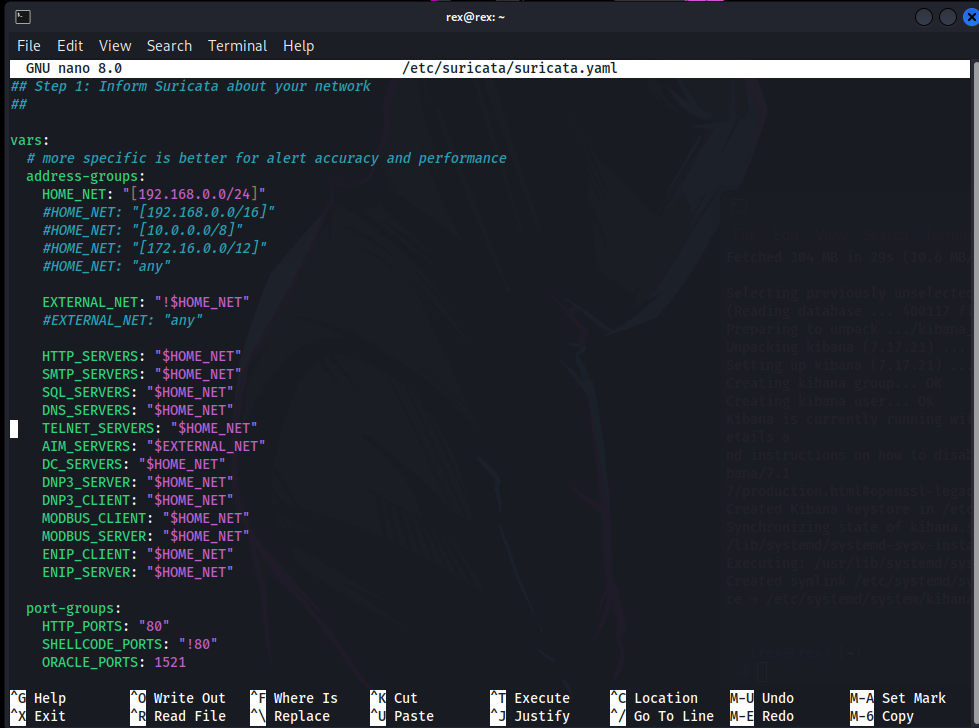
### sudo APt install Suricata

### Configuration

### Suricata

### Edit suricata.yaml

### Set network variables and rule paths:



Add Custom Rules

### Edit local.rules in suricata

### for example:

### alert http any any -> $HOME\_NET any (msg:"HTTP traffic detected"; sid:1000002; rev:1;)

### FTP Traffic

### alert tcp any any -> $HOME\_NET 21 (msg:"FTP traffic detected"; sid:1000003; rev:1;)

### Large ICMP

### alert icmp any any -> $HOME\_NET any (msg:"Large ICMP Echo Request detected"; itype:8; dsize:>1000; sid:1000017; rev:1;)

### 

### Running the System

### 

### Testing and Validation

