Task 3: Suricata NIDS Setup Report

# 1. Introduction

This document provides a detailed guide on setting up Suricata, a Network Intrusion Detection System (NIDS), on your system. It explains the installation steps, configuration, and validation to ensure Suricata is properly monitoring and analyzing network traffic for suspicious activities.

# 2. System Requirements

Before starting the setup, make sure the system meets the following requirements:  
- A Linux machine (Kali Linux)  
- Python 3.x installed (for script-based tasks)  
- Suricata 7.0.10 or newer version installed  
- A network interface to monitor (e.g., eth0)

# 3. Installation

Follow the steps below to install Suricata on your machine.  
  
Step 1: Update the system:  
 - sudo apt-get update  
  
Step 2: Install Suricata:  
 - sudo apt-get install suricata  
  
Step 3: Verify installation:  
 - suricata --version  
 Ensure the installed version is Suricata 7.0.10 or newer.

# 4. Configuration

After installation, you need to configure Suricata for monitoring your network traffic. Follow these steps:  
  
Step 1: Locate the Suricata configuration file:  
 - /etc/suricata/suricata.yaml  
  
Step 2: Modify the configuration file to enable the necessary settings for monitoring traffic.  
Ensure the network interface is correctly defined (e.g., eth0 or enp3s0).  
  
Step 3: Start Suricata with the following command:  
 - sudo systemctl start suricata  
  
Step 4: Check Suricata status to ensure it's running properly:  
 - sudo systemctl status suricata

# 5. Traffic Generation and Testing

Once Suricata is running, you can generate network traffic to test its functionality.  
  
Step 1: Generate traffic using the following tools:  
- ping -f <Suricata-IP>  
- nmap -sS <Suricata-IP>  
  
Step 2: Check Suricata logs to verify it has detected the suspicious traffic:  
 - tail -f /var/log/suricata/fast.log

# 6. Troubleshooting

If Suricata isn't detecting traffic as expected, follow these troubleshooting steps:  
  
- Ensure Suricata is bound to the correct network interface.  
- Update Suricata rules with the following command:  
 - sudo suricata-update  
- Verify that traffic is reaching the correct interface and that Suricata is configured to monitor it.

# 7. Conclusion

After following the above steps, Suricata should be actively monitoring your network traffic for suspicious activity. Make sure to regularly update the rule sets to keep Suricata effective against new threats.