1. Suricata Setup (Wazuh Agent - Target Ubuntu VM)

Suricata is an open-source intrusion detection system (IDS) that monitors network traffic for suspicious activities. In the SOC Co-Pilot project, Suricata is deployed on a target Ubuntu virtual machine (VM3), which also functions as a Wazuh agent. This setup allows for real-time threat detection at the network level.

Prerequisites

- An Ubuntu VM (VM3) with two network adapters:
  - **NAT**: For internet access.
  - **Custom vmnet0 (Host-only)**: For communication within your isolated lab environment.

Installation

1. **Install Suricata**:

   ```
   bash sudo apt update sudo apt install suricata -y
   ```

Configuration

1. **Configure `suricata.yaml`**:

   Open the Suricata configuration file:

   ```
   bash sudo nano /etc/suricata/suricata.yaml
   ```

   Set the `HOME_NET` variable to your internal network range (e.g., `192.168.1.0/24`):

   ```
   yaml HOME_NET: "[your_network_range]"
   ```

2. **Create Custom Rules**:

   Create a custom rules file:

   ```
   bash sudo nano /var/lib/suricata/rules/custom.rules
   ```

Add your custom rules. For example:

```
suricata alert tcp any any -> $HOME_NET 22 (msg:"SURICATA SSH brute-force attempt"; flow:to_server,established; threshold:type threshold, track by_src, count 5, seconds 10; sid:100001; rev:1;) alert tcp any any -> $HOME_NET 3389 (msg:"SURICATA RDP brute-force detected"; flow:to_server,established; threshold:type threshold, track by_src, count 5, seconds 10; sid:100002; rev:1;)
```

3. **Load Custom Rules**:

   In `suricata.yaml`, ensure your custom rules file is included:

   ```
   yaml rule-files: - custom.rules
   ```

Testing and Activation

1. **Test Configuration**:

   ```
   bash sudo suricata -T -c /etc/suricata/suricata.yaml
   ```

2. **Start Suricata**:

   ```
   bash sudo suricata -c /etc/suricata/suricata.yaml -i [your_network_interface]
   ```

   Replace `[your_network_interface]` with your host-only network interface (e.g., `ens37`).

3. **Restart Suricata**:

   To apply changes, restart the Suricata service:

   ```
   bash sudo systemctl restart suricata
   ```

[Reference: `steps(1).txt`, `steps(2).txt`]