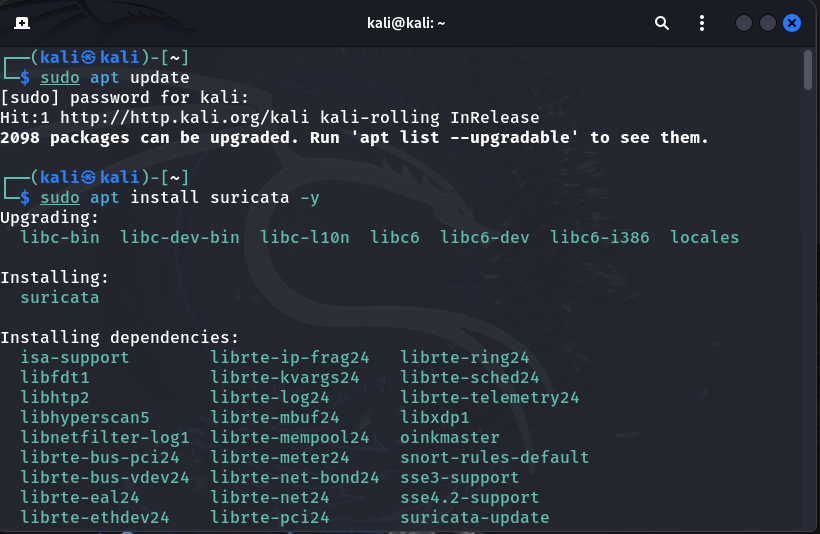
**Name: Aalaa Mahmoud Zahran**

**Id:** **2106136**

**Proactive project**

**Suricata**

**Suricata** is an open-source tool designed for **network intrusion detection**, **prevention**, and **monitoring**. It provides real-time analysis of network traffic, helping detect malicious activities and threats. Suricata works by analyzing packets and matching them against pre-configured rules or custom rules, making it a valuable tool in identifying threats like the **Zeus Banking Trojan**.In this project, Suricata is used to monitor and analyze the network traffic generated by the Zeus Trojan. By leveraging its ability to detect suspicious patterns and generate alerts, Suricata helps identify malicious behaviors such as **command-and-control (C2) communications**, data exfiltration, or other network anomalies. Additionally, its integration with tools like Splunk enhances visibility and provides a comprehensive analysis of malicious activity.

**In the screenshot, you performed the following steps:**

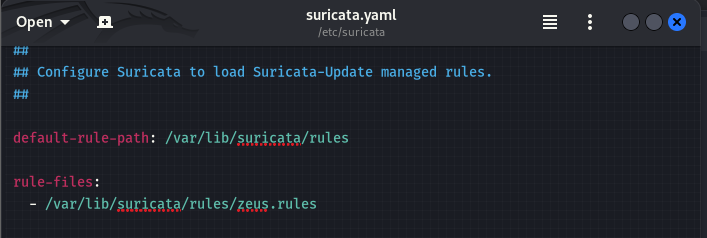
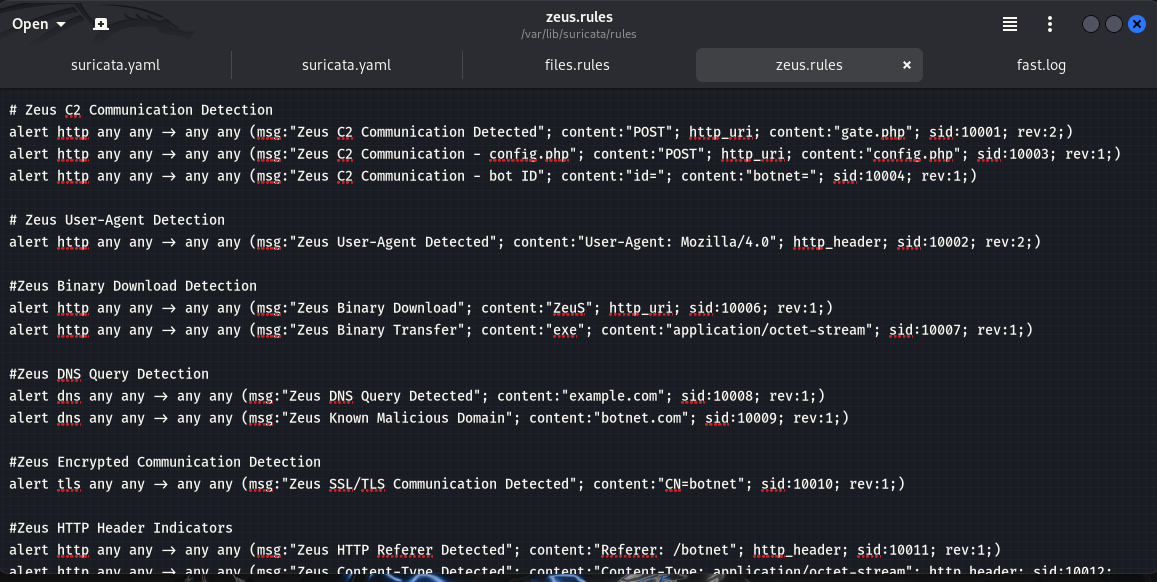
1. **Updated the Package List**:
   1. Used sudo apt update to refresh the list of available software packages from the Kali Linux repositories.
2. **Installed Suricata**:
   1. Used sudo apt install suricata -y to install Suricata along with its required dependencies.
   2. The -y flag automated the installation process by confirming prompts.

A screenshot of a computer

Description automatically generated**In this screen, the following actions occurred:**

1. **Processed Installation Triggers:**
   1. After installing Suricata, the system completed setup tasks for dependencies (e.g., libc-bin, systemd, man-db). These are required for Suricata to function correctly.
2. **Displayed Network Interface Information:**
   1. The command ip a was executed to display information about the system's network interfaces:
      1. **Interface lo (Loopback):**
         1. Used for internal communication within the system.
         2. IP address: 127.0.0.1.
      2. **Interface eth0:**
         1. The primary network interface connected to the network.
         2. Assigned the IP address 192.168.247.128/24.
         3. Shows the MAC address (00:0c:29:cf:9c:35) and additional details such as broadcast and IPv6 addresses.

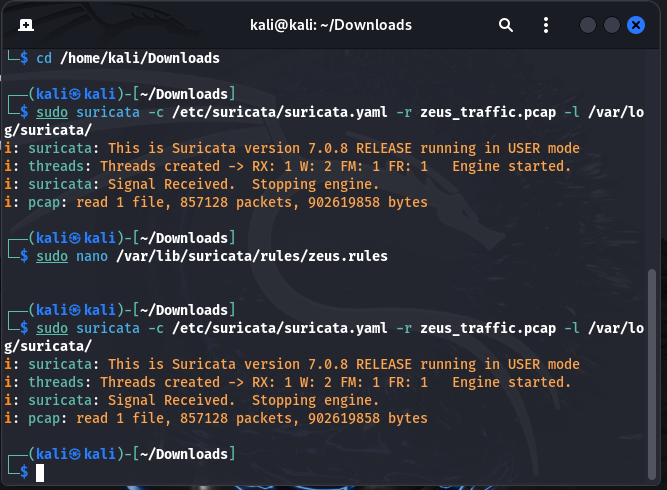
A computer screen shot of a computer code

Description automatically generated**The actions across the three screens were as follows:**

1. **Creating and Editing Zeus Rules**:
   1. Used nano to create and edit the file /etc/suricata/rules/zeus.rules.
   2. Added custom Suricata rules to detect Zeus-related activities, such as:
      1. **C2 Communication** (e.g., specific POST requests).
      2. **User-Agent Strings** linked to Zeus.
      3. **Binary Downloads**, **DNS Queries**, and **Encrypted Communications**.
2. **Configuring Suricata to Use Zeus Rules**:
   1. Edited the suricata.yaml configuration file using nano to include the newly created zeus.rules.
   2. Updated the rule-files section in the YAML file to load the zeus.rules file during Suricata's execution.

### A screen shot of a computer Description automatically generated**Summary of What Happened:**

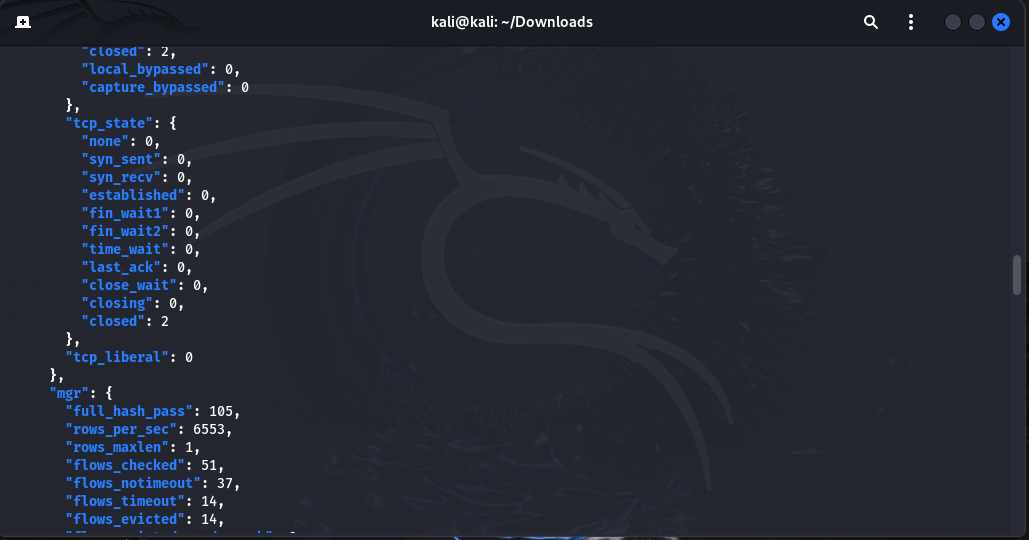
* **Command Explanation:**
  + -T: Tests the Suricata configuration file without starting the service.
  + -c /etc/suricata/suricata.yaml: Specifies the configuration file (suricata.yaml) to validate.
* **Outcome:**
  + Suricata successfully verified the configuration file and loaded it without errors.
  + The message confirms that Suricata is configured correctly and ready to run using the specified configuration.

**This screen:**

1. **Analyzed PCAP File:**
   1. Ran Suricata to analyze zeus\_traffic.pcap using the specified configuration file and logged results in /var/log/suricata/.
2. **Updated Rules:**
   1. Edited the zeus.rules file to fine-tune Zeus-specific detection.
3. **Reprocessed PCAP:**
   1. Re-ran Suricata to apply updated rules and reanalyze the PCAP file.

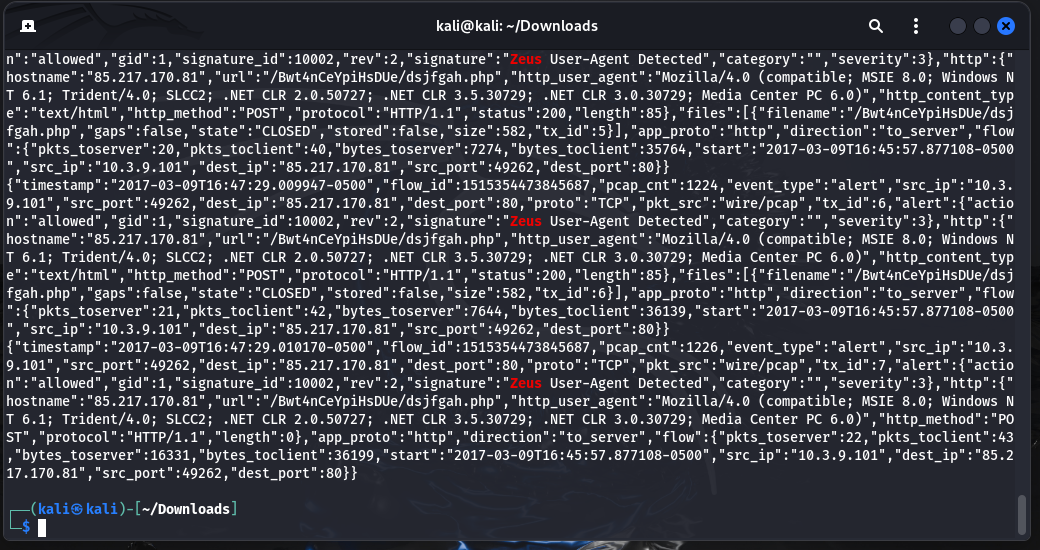
This process ensured effective detection of Zeus-related activity based on the latest rule updates.

A screenshot of a computer

Description automatically generated**This screen:**

**Viewed Logs**:

* 1. Used the cat command to display the contents of eve.json, which contains detailed information about the analyzed traffic, including statistics and any detected events.

**This screen:**

* **Zeus Detected:** Suricata identified Zeus-related activity in the analyzed zeus\_traffic.pcap file.
* **Key Findings:**
  + Detected events include **Zeus User-Agent** patterns, such as HTTP requests containing the User-Agent string "Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1)".
  + Alerts point to communication between the source IP (10.3.9.101) and destination IP (85.217.170.81) on port 80.
* **Outcome:**
  + Logs confirm the detection of Zeus behavior based on custom Suricata rules.
  + The generated alerts provide evidence of suspicious traffic for further investigation.