Installing and Executing Suricata with Custom Rules for IDS

Step 1: Install Suricata

Run the following commands to install Suricata on Ubuntu:

```
sudo add-apt-repository ppa:oisf/suricata-stable -y
sudo apt update
sudo apt install suricata -y
```

Step 2: Verify Installation

Check the installed Suricata version:

```
suricata --build-info
```

Step 3: Configure Suricata

Edit the Suricata configuration file to enable IDS mode:

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

Ensure **AF_PACKET** or **NFQUEUE** is enabled for live packet analysis.

Set **rule-files** to include your custom rules file:

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

Save and exit the file.

Step 4: Add Custom Rules

Create a new rules file for your attacks:

```
sudo nano /etc/suricata/rules/custom-rules.rules
```

Copy and paste the Suricata rules for **De-Authentication Attack** or other attacks.

Save and exit the file.

Step 5: Test Rule Syntax

Before running Suricata, validate your rule syntax:

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

Step 6: Run Suricata in IDS Mode

Start Suricata with the custom rules in IDS mode:

```
sudo suricata -c /etc/suricata/suricata.yaml -i eth0
```

Replace eth0 with your active network interface (ip link show to find it).

Step 7: Monitor Alerts

View generated alerts in real-time:

```
sudo tail -f /var/log/suricata/fast.log    (or)
sudo tail -f /var/log/suricata/alerts.log
```

Step 8: Enable Suricata as a Service (Optional)

To run Suricata automatically on boot:

```
sudo systemctl enable --now suricata
```

Now, Suricata will actively monitor for **Attacks** and log any detections. Let me know if you need additional configurations!