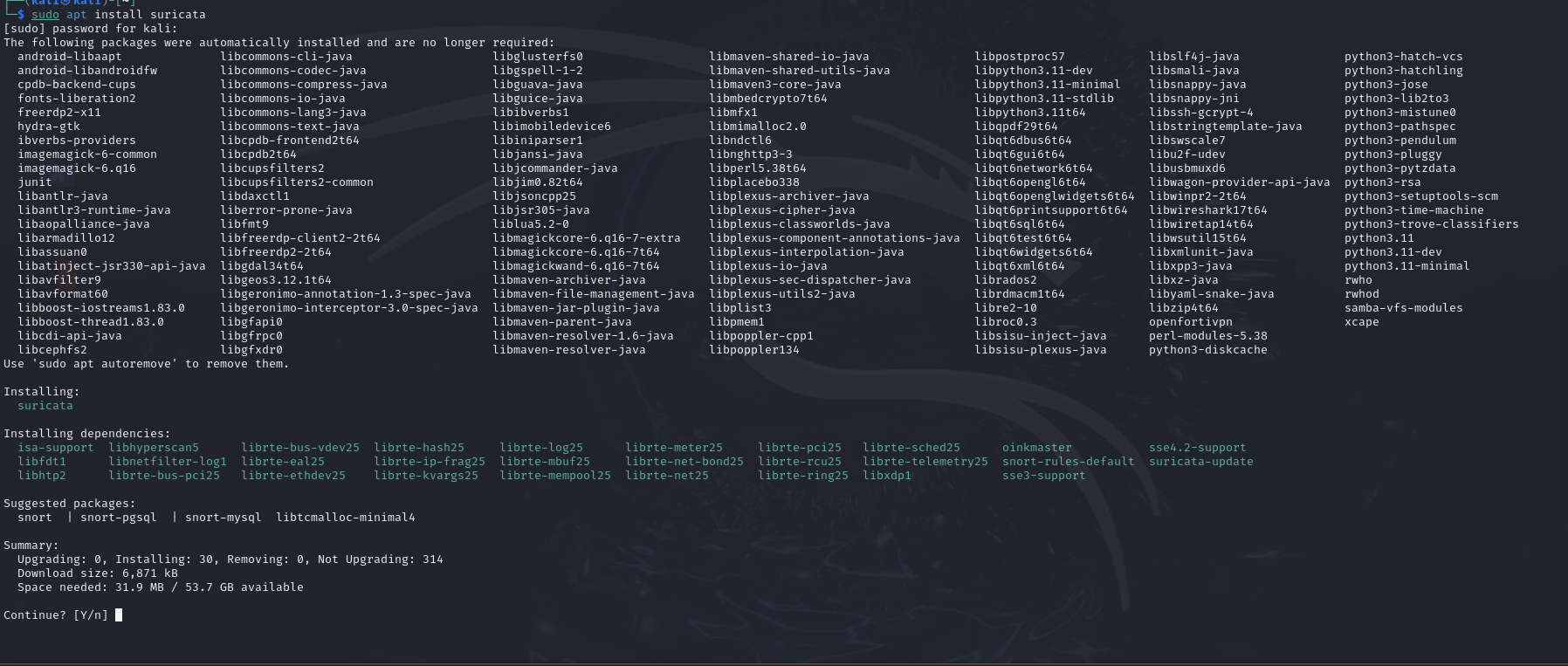
Install Suricata in Kali, Download Rulesets and Generate a Custom Alert

Suricata is an open-source network security monitoring tool that functions as a **network intrusion detection system (NIDS)**, **network intrusion prevention system (NIPS)**, and **network security monitoring tool**. It is widely used to monitor and protect networks against malicious traffic and cyber threats.

We don’t have it installed so the first step is to install it.

sudo apt install suricata

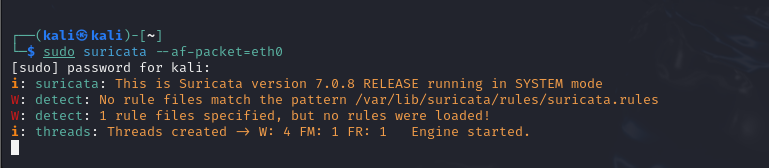


When we run Suricata from the command line with no arguments it gives us the help page with all the options that we can use.



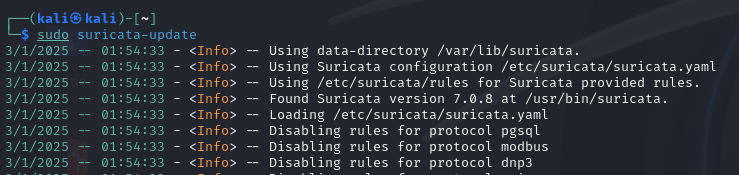
For this exercise we will run Suricata with the <–af-packet> mode option with the interface <eth0>.

AF\_PACKET (Advanced Packet Socket) is a socket type in Linux that provides a way for applications to receive (in our case) or send raw packets directly from or to the NIC. It allows the capture and analysis of packets at a low level.

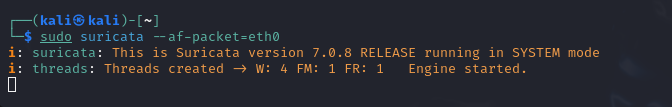


Suricata is running. Looking above we can see that no rules files were loaded so we better download some rules.

An easy way to download open source rules is using the built in utility <suricata-update>

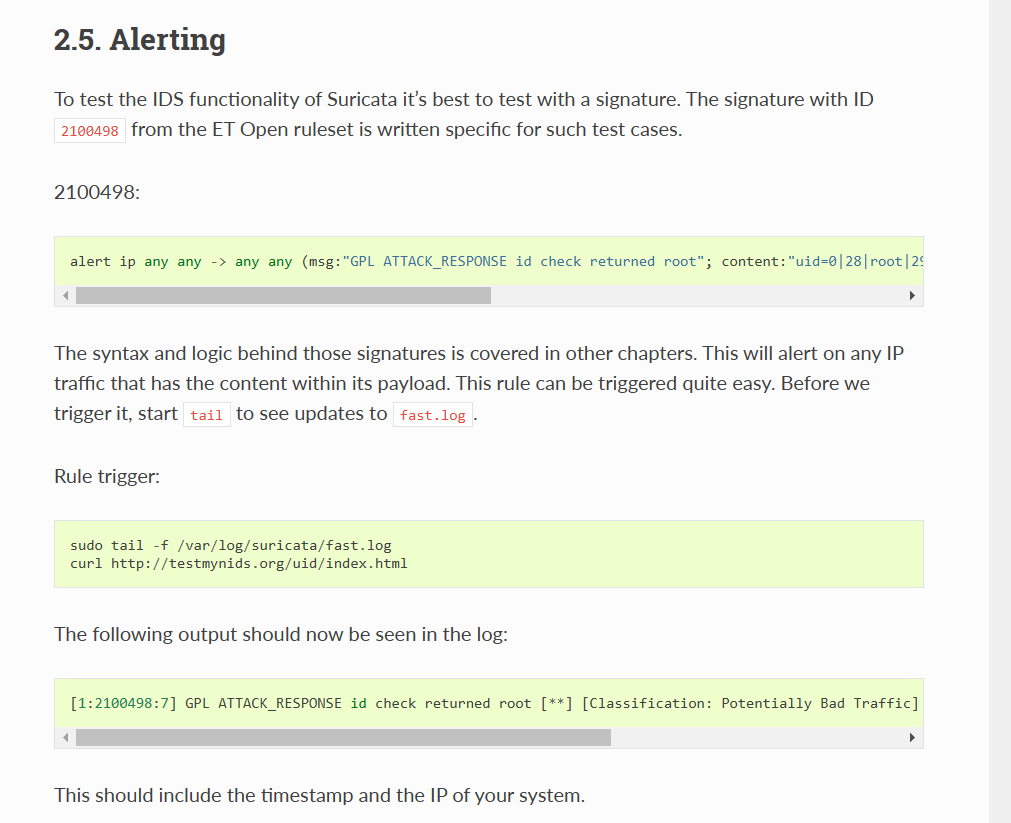


Once we have updated our rules try to run Suricata again with af-packet.



Now Suricata is running with no errors or warnings.

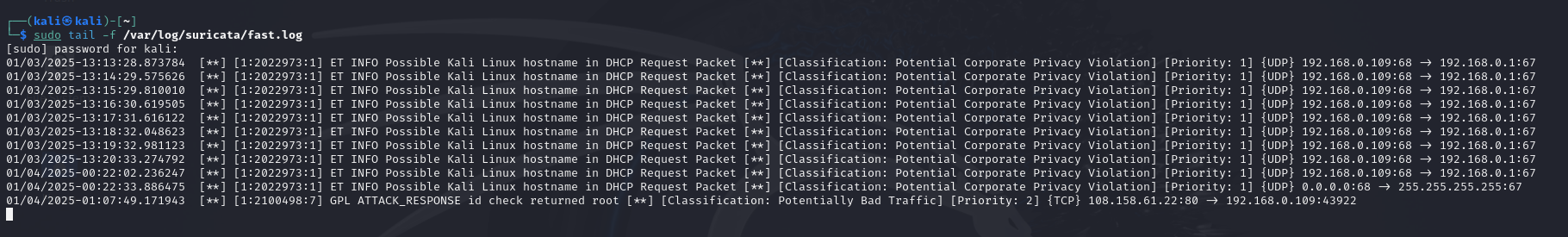
To test Suricata alerts we can use the method mentioned in the [Suricata Quick Start documentation 2.5 Alerting](https://docs.suricata.io/en/suricata-6.0.9/quickstart.html#alerting). This involves triggering the rule with sid: 2100498. You may notice that the documentation uses <tail -f> to view the log. The -f flag appends new data as the file grows and is what should be used when you want to dynamically view the log file for example during testing.



As we can see above to trigger the rule we curl the following URL.



When we view the log file again we see the expected alert in the log.



Now let’s move on to creating our own custom signature.

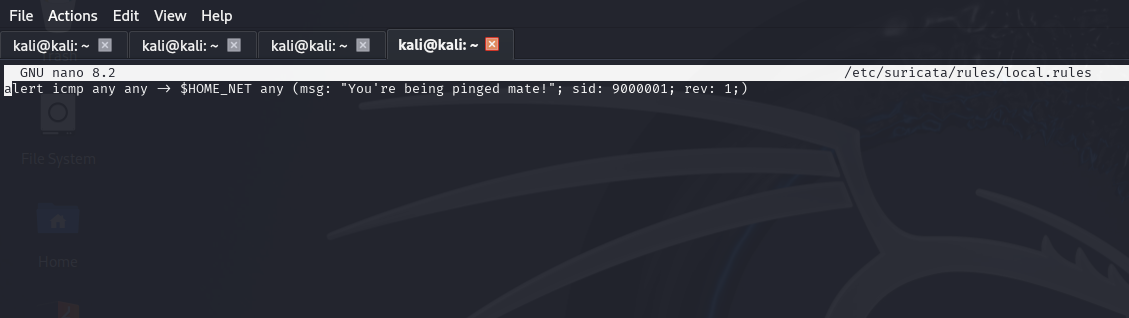
## Creating a custom rule

Now that we have created our signature, we must create the custom rules file.



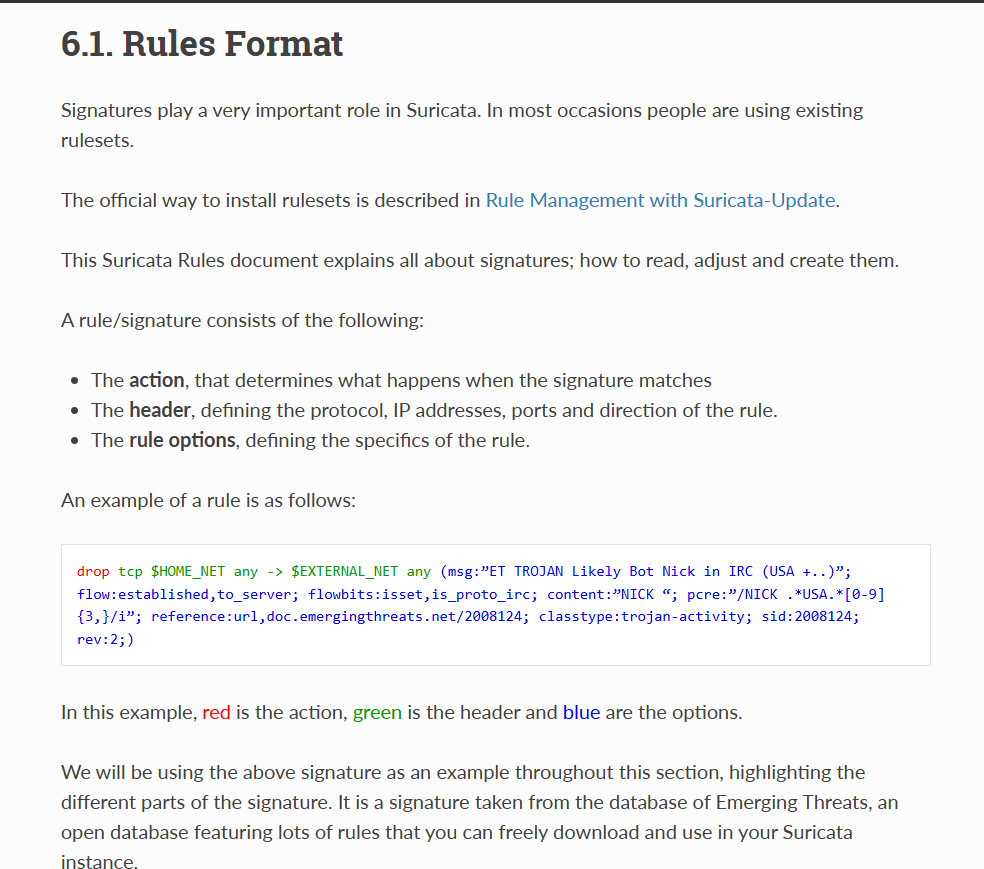
Next open the file with your favourite text editor and type in the signature. I’m using nano.

sudo nano /etc/suricata/rules/local.rules



When writing our custom rule, we can go back to the manual section on rules and use it as a reference:

<https://docs.suricata.io/en/suricata-6.0.0/rules/intro.html>



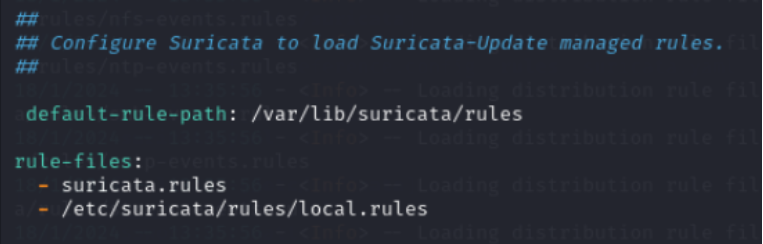
For our example we will create a rule that generates an alert when the home network is pinged with an ICMP packet.

alert icmp any any -> $HOME\_NET any (msg: "You're being pinged mate!"; sid: 9000001; rev: 1;)

### **Explanation**

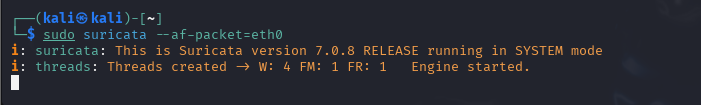
1. **alert**:
   * Specifies the action to take when the rule matches.
   * In this case, it generates an alert.
2. **icmp**:
   * The protocol this rule applies to.
   * ICMP is commonly used for network diagnostics (e.g., ping).
3. **any any**:
   * any for source IP: Matches any source IP address.
   * any for source port: Since ICMP doesn’t use ports, this is ignored.
4. **->**:
   * Directional operator, indicating traffic flowing **from** the source to the destination.
5. **$HOME\_NET**:
   * A variable typically defined in the Suricata configuration file (e.g., suricata.yaml).
   * It represents the network(s) you want to monitor or protect.
   * This could be a specific range of IP addresses, like 192.168.0.0/24.
6. **any**:
   * Matches any destination port. Again, for ICMP, this is ignored.
7. **(msg: "You're being pinged mate!"; sid: 9000001; rev: 1;)**:
   * **msg**: The message to display in the alert.
     + Here, it’s "You're being pinged mate!".
   * **sid**: Unique **Suricata ID** for the rule.
     + 9000001 is a custom ID chosen to avoid conflicts with pre-defined rules.
     + Custom rule IDs typically start at 9000000.
   * **rev**: Revision number of the rule.
     + Used to track updates or changes to the rule. The current revision is 1.

take a look at the configuration file <suricata.yaml> found in /etc/suricata/. Here we navigate to the default rule path and rule files and add a file to have our custom rule in. This is located at the very bottom of the config file

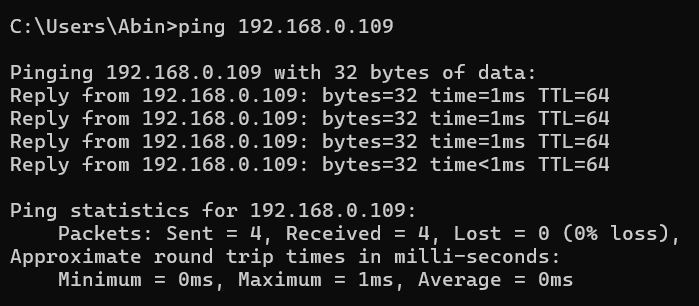
We insert /etc/suricata/rules/local.rules under rule-files:, which is the absolute path to our custom rule file.

## Testing our custom rule and alert

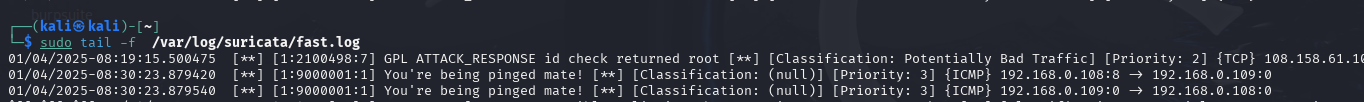
To test if our custom rule works let’s get Suricata searching again.



Then let’s ping it from another machine on the network.

****

And finally let’s check the alerts log again.



Here at the bottom of the log we can see the most recent two alerts are for our pings!