Task 2: Configure Rules and Alerts

1. Edit Suricata rules file: /etc/suricata/rules/local.rules

Example rule (ICMP detection):

```
alert icmp any any -> any any (msg:"ICMP Ping detected"; sid:1000001; rev:1;)
```

2. Ensure rule file is loaded in /etc/suricata/suricata.yaml:

```
default-rule-path: /etc/suricata/rules
rule-files:
  - local.rules
```