Task 3: Monitor Network Traffic

1. Start Suricata in live capture mode:

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

(Replace 'eth0' with your actual network interface)

2. Logs Location:

   /var/log/suricata/

   - fast.log -> alerts in real-time

   - eve.json -> structured JSON logs

   - stats.log -> performance stats

Check alerts:

   tail -f /var/log/suricata/fast.log