Task 4: Intrusion Response and Visualization

1. Intrusion Response (manual or automated):

   - Use fail2ban or iptables with script to block attackers

   - Parse eve.json for automatic blocking

2. Visualization with ELK (Optional):

   - Install ELK Stack (Elasticsearch, Logstash, Kibana)

   - Configure Suricata to forward logs to Logstash

   - Import Suricata dashboards into Kibana for attack graphs, stats, and maps

Alternative: Use Security Onion for a complete prebuilt setup.