TASK 4: Network Intrusion Detection System (NIDS)

Objective

To deploy and configure a Network-Based Intrusion Detection System using Snort or Suricata, detect malicious network activity, and respond effectively to cyber threats.

1. NIDS Setup

- Installed Suricata (or Snort) on a Linux-based system (Ubuntu/Debian recommended).
- Enabled network interface in promiscuous mode to capture all traffic.
- Used pcap or live traffic monitoring for real-time packet inspection.
- Verified installation using test packets (ping, nmap, curl, etc.).

2. Rule Configuration and Alerts

- Loaded default rules from Emerging Threats (ET Open) or Snort rule sets.
- Created custom rules to detect:
  Port scans (e.g., nmap)
  Unauthorized SSH login attempts
  HTTP GET/POST anomalies
  Malware signatures
- Configured output options: fast.log, eve.json, syslog, and alert pop-ups.

Example Suricata Rule:

alert tcp any any -> any 22 (msg:"SSH Connection Detected"; sid:100001;)

3. Traffic Monitoring

- Enabled continuous monitoring using:
  suricata -c /etc/suricata/suricata.yaml -i eth0
  Live dashboards with Kibana + Elasticsearch + Filebeat
  Real-time logs reviewed using tail -f /var/log/suricata/fast.log

4. Intrusion Response Mechanisms

- Configured automatic alerts via email or Slack for critical threats.

- Integrated firewall rules (iptables) to block suspicious IPs.
- Implemented response script to isolate affected network segments.
- Maintained incident logs for forensic analysis and legal purposes.

5. Visualization of Attacks (Optional)

- Integrated Suricata with ELK Stack (Elasticsearch, Logstash, Kibana).
- Designed Kibana dashboards for:
  Top source IPs
  Attack types and frequency
  Time-series of alerts
- Used Grafana + Loki as an alternative lightweight setup.

Supporting Files (To Include)

- Suricata or Snort config (suricata.yaml or snort.conf)
- Sample alert logs (fast.log, eve.json)
- Screenshots of dashboards (Kibana/Grafana)
- Custom rule file examples

Conclusion

The deployed NIDS setup successfully monitored network traffic, detected intrusions, and generated real-time alerts. With visualization and automated responses in place, it offers an efficient mechanism to enhance the organizations cybersecurity posture.