Practical: 9

SIEM Practical Documentation: ELK Stack + IDS/IPS Integration

Overview

This guide walks through deploying the ELK Stack as a SIEM and integrating it with an Intrusion Detection/Prevention System (IDS/IPS) such as Suricata for comprehensive, real-time security event monitoring and analytics.[2][1]

Step 1: Prepare the Environment

- Deploy or provision servers for ELK Stack services (Elasticsearch, Logstash, Kibana) on Linux (Ubuntu recommended).
- Deploy a separate machine, VM, or container for Suricata IDS/IPS and ensure network connectivity between Suricata and ELK servers.[3]
- Install Java (required for Logstash):

```
sudo apt-get update
sudo apt-get install openjdk-11-jdk
```

Step 2: Install and Configure ELK Stack

- **Install Elasticsearch:**

```
wget https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-8.x.x-amd64.deb
sudo dpkg -i elasticsearch-8.x.x-amd64.deb
```

  - Start and enable service.

- **Install Logstash:**

```
wget https://artifacts.elastic.co/downloads/logstash/logstash-8.x.x-amd64.deb
sudo dpkg -i logstash-8.x.x-amd64.deb
```

  - Start and enable service.

- **Install Kibana:**

```
wget https://artifacts.elastic.co/downloads/kibana/kibana-8.x.x-amd64.deb
sudo dpkg -i kibana-8.x.x-amd64.deb
```

  - Start and enable service.

- Access Kibana via browser at http://localhost:5601 to confirm correct setup.[4]

Step 3: Install and Configure Suricata IDS/IPS

- Install Suricata on a security monitoring server:

```
sudo apt-get install suricata
```

- Confirm Suricata generates log events using the EVE JSON output format (in /var/log/suricata/eve.json).[3]

Step 4: Forward IDS/IPS Alerts to ELK Stack

- Install Filebeat on Suricata server:

```
sudo apt-get install filebeat
```

- Configure Filebeat to forward Suricata logs:

    - Edit /etc/filebeat/filebeat.yml

    ```
    filebeat.inputs:
      - type: log
        enabled:true
        paths:
          - /var/log/suricata/eve.json

    output.elasticsearch:
      hosts: ["http://elasticsearch_server:9200"]
    ```

    - Enable and start Filebeat:

    ```
    sudo systemctl enable filebeat
    sudo systemctl start filebeat
    ```

- Alternatively, configure Logstash to ingest Suricata logs:

    - Logstash pipeline config /etc/logstash/conf.d/suricata.conf:

    ```
    input {
      file {
        path => "/var/log/suricata/eve.json"
        codec => "json"
      }
    }
    output {
      elasticsearch {
        hosts => ["http://localhost:9200"]
        index => "suricata-logs"
      }
    }
    ```

Step 5: Visualization & Alerting in Kibana

- In Kibana, define index patterns for Suricata/IDS logs.
- Build dashboards visualizing IDS/IPS alerts, suspicious events, traffic anomalies.
- Configure alerting and detection rules in Elastic Security:

  - Navigate to “Detection rules (SIEM)” and “Create new rule” for specific threat conditions (SSH brute-force, port scans, etc.).[5][6]

Step 6: Testing & Verification

- Generate test attacks (e.g., Nmap or Hydra brute-force) on monitored network.
- Confirm Suricata logs alerts to EVE JSON and ELK dashboards reflect detected events in real-time.[2]
- Review and fine-tune dashboards, detection rules, alerting configurations.

Additional Enhancements

- Integrate with other detection sources (firewall logs, endpoint logs).
- Enable machine learning features for anomaly and pattern-based detection.
- Expand alerting to email, Slack, or SIEM orchestration platforms.[1]