TASK 4

Network Intrusion Detection System

To develop a network-based intrusion detection system (NIDS) using Snort or Suricata, we'll go through the following steps:

1. **Installation**: Install Snort or Suricata on a Linux system.
2. **Configuration**: Configure the NIDS to monitor network traffic.
3. **Rules and Alerts**: Set up rules to detect suspicious activities.
4. **Visualization**: Use tools to visualize the detected attacks.

Step 1: Installation

We'll use Suricata for this example. Suricata is a robust NIDS that can also function as an intrusion prevention system (IPS) and network security monitoring (NSM) tool.

Install Suricata on Ubuntu

```
sudo apt update
sudo apt install -y suricata
```

Step 2: Configuration

Configure Network Interface

Suricata needs to know which network interface to monitor. Edit the Suricata configuration file (`/etc/suricata/suricata.yaml`) and set the interface.

```
# /etc/suricata/suricata.yaml

af-packet:
  - interface: eth0
    threads: 4
    defrag: yes
    cluster-id: 99
    cluster-type: cluster_flow
    ring-size: 200000
```

Replace `eth0` with the appropriate network interface on your system.

Step 3: Rules and Alerts

Download and Update Rules

Suricata uses rules to detect suspicious activities. You can use the Emerging Threats rule set, which is widely used.

```
sudo apt install -y suricata-update
sudo suricata-update
```

Custom Rules

Create custom rules by adding them to the `local.rules` file.

```
sudo nano /etc/suricata/rules/local.rules
```

Example rules:

```
# Detect ICMP echo requests (ping)
alert icmp any any -> any any (msg:"ICMP Echo Request Detected"; itype:8;
sid:1000001; rev:1;)

# Detect TCP port scan
alert tcp any any -> any any (flags:S; msg:"TCP SYN Scan"; sid:1000002;
rev:1;)
```

Enable Logging

Ensure logging is enabled in the `suricata.yaml` configuration file.

```
# /etc/suricata/suricata.yaml

outputs:
  - fast:
      enabled: yes
      filename: fast.log
```

Step 4: Visualization

To visualize detected attacks, you can use Kibana with the ELK (Elasticsearch, Logstash, Kibana) stack.

Install ELK Stack

Follow the installation instructions for the ELK stack on your system. For example:

```
# Install Elasticsearch
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo
apt-key add -
sudo apt-get install apt-transport-https
echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo
tee -a /etc/apt/sources.list.d/elastic-7.x.list
sudo apt update
sudo apt install elasticsearch

# Install Logstash
sudo apt install logstash

# Install Kibana
sudo apt install kibana
```

Configure Logstash

Create a configuration file for Logstash to process Suricata logs.

```
sudo nano /etc/logstash/conf.d/suricata.conf
```

Example configuration:

```
input {
  file {
    path => "/var/log/suricata/fast.log"
    start_position => "beginning"
  }
}

filter {
  grok {
    match => { "message" => "%{TIMESTAMP_ISO8601:timestamp} %{IP:src_ip} ->
%{IP:dest_ip} %{WORD:protocol} %{DATA:payload}" }
  }
  date {
    match => [ "timestamp", "ISO8601" ]
  }
}
```

```
output {
  elasticsearch {
    hosts => ["localhost:9200"]
    index => "suricata-%{+YYYY.MM.dd}"
  }
  stdout { codec => rubydebug }
}
```

Start Services

Start the ELK stack services:

```
sudo systemctl start elasticsearch
sudo systemctl start logstash
sudo systemctl start kibana
```

Access Kibana

Open a web browser and navigate to `http://localhost:5601`. Set up an index pattern for Suricata logs.

Running Suricata

Start Suricata:

```
sudo systemctl start suricata
```

Suricata will now monitor network traffic, apply rules, and log suspicious activities to `fast.log`.

Visualizing in Kibana

In Kibana, go to the "Discover" section, select the Suricata index pattern, and visualize the logs. You can create dashboards to display metrics and alerts, helping you monitor network security visually.

Conclusion

By setting up Suricata with custom rules and integrating it with the ELK stack, you have a powerful NIDS capable of detecting and visualizing suspicious network activities. Regularly update your rules and configurations to ensure your network remains secure.