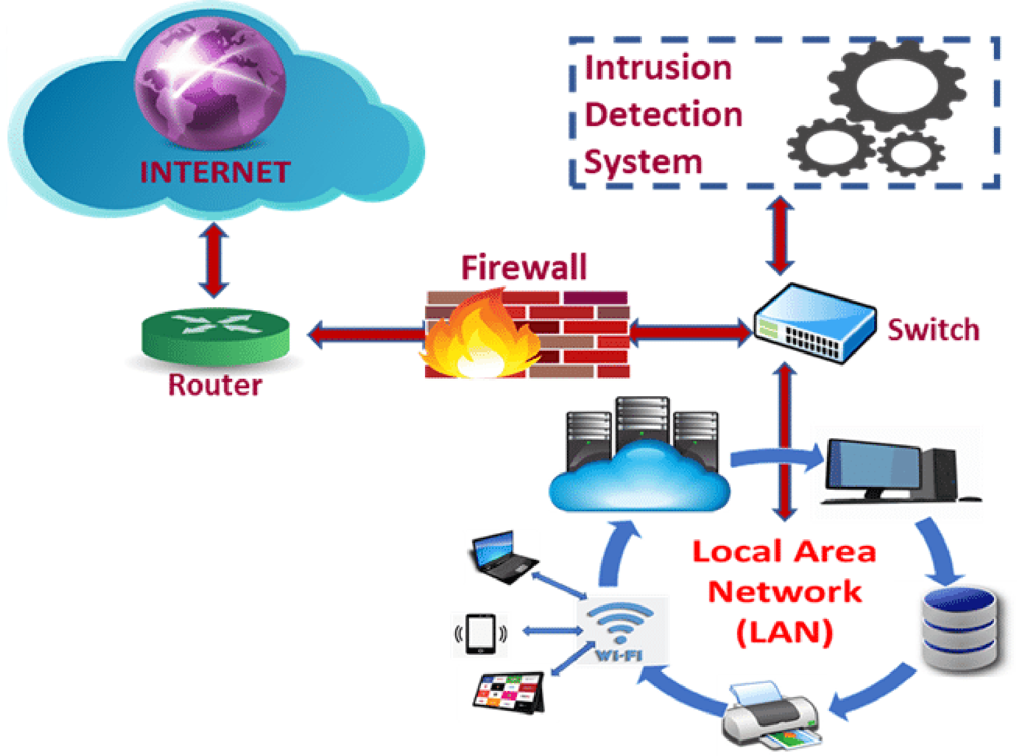
# EXPERIMENT – 10

***AIM:*** Demonstrate Intrusion Detection System (ids) using any tool eg. Snort or any other s/w.

## ***DESCRIPTION:***

An **Intrusion Detection System (IDS)** is a security tool that monitors network traffic and system activities for malicious actions or policy violations. One popular open-source IDS tool is Snort, which works by analyzing network packets in real time and comparing them against predefined rules to detect potential intrusions. To demonstrate Snort, first, install it on a Linux-based system such as Ubuntu. You need to configure the network interface in promiscuous mode to capture all network traffic. Next, create or modify Snort rules that define specific patterns to detect threats like port scanning, denial-of-service (DoS) attacks, or malware traffic. Snort operates in different modes: sniffer mode (monitoring traffic), packet logging mode (logging network packets), and network intrusion detection mode (real-time monitoring and alerting based on rules). Once Snort is running, it examines every packet traversing the network, looking for suspicious activity based on the rules. If a match is found, Snort triggers an alert, which is logged for further investigation. This allows network administrators to detect, analyze, and respond to potential security breaches, making IDS a critical component of network defence. The logs can also be integrated with other security systems for comprehensive analysis and reporting.



**Snort Setup and ICMP Ping Detection**

**Prerequisites:**

Ensure Snort is installed on your Linux system. If it's not, you can install it by running:

```
sudo apt-get update
sudo apt-get install snort
```

**Step 1: Configure Network Interface in Promiscuous Mode**

To capture all network traffic, set your network interface to promiscuous mode:

```
sudo ip link set eth0 promisc on
```

Replace eth0 with the correct network interface name (use ip a to find the interface if needed).

**Step 2: Create a Basic Snort Rule**

You'll create a rule to detect ICMP ping requests, which can be indicative of a ping sweep.

1. Open the Snort rules file, typically found at:
   ```
   sudo nano /etc/snort/rules/local.rules
   ```
2. Add this rule to detect ICMP ping requests:
   ```
   alert icmp any any -> any any (msg:"ICMP Ping detected"; itype:8; sid:1000001; rev:1;)
   ```

**Explanation:**

- alert: Triggers an alert action when this rule matches.
- icmp: Sets the rule to inspect ICMP traffic.
- any any -> any any: Matches traffic from any IP/port to any IP/port.
- msg:"ICMP Ping detected": Custom message displayed when the rule matches.
- itype:8: Filters ICMP packets for echo requests (ping requests).
- sid:1000001: Assigns a unique ID to this rule.
- rev:1: Specifies the rule version.

After editing, save the file and exit the editor.

**Step 3: Run Snort in Network Intrusion Detection System (NIDS) Mode**

To activate Snort and monitor for alerts in the console:

```
sudo snort -A console -q -c /etc/snort/snort.conf -i eth0
```

**Explanation of Options:**

- -A console: Outputs alerts directly to the console.
- -q: Runs Snort in quiet mode, reducing non-essential output.
- -c: Specifies the Snort configuration file to use.
- -i eth0: Sets the network interface Snort will monitor (replace eth0 if needed).

**Step 4: Test the IDS**

Initiate an ICMP ping request from a different device to test the rule:

```
ping <target-ip>
```

Replace <target-ip> with the IP of the machine running Snort.

**Example Output:**

If the rule works, Snort will output an alert similar to:

```
[**] [1:1000001:1] ICMP Ping detected [**]
```

This indicates that Snort successfully detected and alerted on the ICMP ping request based on the rule.

***OUTPUT ANALYSIS:***

In the output, Snort logs an alert when the ICMP Ping rule is triggered. The message [**] [1:1000001:1] ICMP Ping detected [**] indicates that a network packet matching the rule was detected. The numbers [1:1000001:1] represent the Generator ID, Signature ID(sid), and Revision ID, respectively. These help in uniquely identifying the rule and tracking its version. Snort captures the packet metadata, including the source and destination IP addresses, time, and protocol details. This output allows network administrators to monitor suspicious traffic and take appropriate security measures based on the alerts generated.