# CyberSecurity (CSL6010)

## Lab Assignment 10 : IDS and IPS

Soumen Kumar
Roll No-B22ES006

# Objective

The objective of this lab is to install, configure, and test Snort as both an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS) on Kali Linux. Since I have two Kali Linux machines available, I have used one machine as the attacker and the other as the victim. The Snort IDS/IPS was configured on the victim machine to monitor and control the incoming traffic from the attacker machine.

# Understanding IDS and IPS

## Intrusion Detection System (IDS)

IDS is like a security camera for the network. It only monitors and detects suspicious activities or attacks but doesn't take any direct action to stop them. It simply alerts the administrator about the attack.

**Example:** In this lab, when I ran Snort in IDS mode, it detected ICMP (ping) packets and generated an alert but didn't block the traffic.

## Intrusion Prevention System (IPS)

IPS, on the other hand, is like a security guard. It not only detects the attack but also takes immediate action to block or drop the malicious traffic in real-time.

**Example:** In this lab, when I ran Snort in IPS mode, it detected ICMP packets and dropped them automatically, so the ping command failed to get a response.

## Summary of Difference

| **Feature** | **IDS** | **IPS** |
|---|---|---|
| Action | Detects only | Detects and Prevents |
| Response | Alert generation | Alerts + Blocks traffic |
| Working Mode | Passive | Active |
| Example in Lab | Alerted for ICMP | Dropped ICMP traffic |

# Task: Using Snort++ IDS/IPS

## Steps Performed:

- I started by installing Snort++ along with its necessary dependencies using the following commands:

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

```

  This ensured that all required packages and libraries for Snort++ were present.

- After installation, I set the DAQ (Data Acquisition Library) path environment variable so that Snort++ could locate the DAQ modules properly:

```
export SNORT_DAQ_PATH=/usr/local/lib/daq

```

- Then, I checked the available network interfaces on my machine to identify the correct interface to run Snort++:

```
ip link show

```

  In my case, the active interface was `eth0`.

- I ran Snort++ in IDS (Intrusion Detection System) mode to only detect and log the attacks without blocking them:

```
sudo snort -c /etc/snort/snort.lua -R /etc/snort/rules/local.rules -i eth0

```

- Later, I configured Snort++ in IPS (Intrusion Prevention System) mode to detect and prevent/block malicious traffic using inline DAQ mode:

```
sudo snort -c /etc/snort/snort.lua -R /etc/snort/rules/local.rules --daq pcap --daq-var device=eth0 -
    Q

```

- I also verified that Snort++ was operating correctly in inline mode:

```
sudo snort -c /etc/snort/snort.lua -R /etc/snort/rules/local.rules -i eth0 -Q

```

- Next, I created and configured custom rules inside `/etc/snort/rules/local.rules` file. For example, I wrote a rule to detect ICMP (Ping) packets:

```
alert icmp any any -> any any (msg:"ICMP Packet Detected"; sid:1000001;)

```

- For prevention, I used drop rules to block ICMP packets:

```
drop icmp any any -> any any (msg:"ICMP Packet Dropped"; sid:1000002;)

```

- Finally, I tested Snort++ by generating ICMP packets using `ping` command from another machine:

```
ping <victim-ip>

```

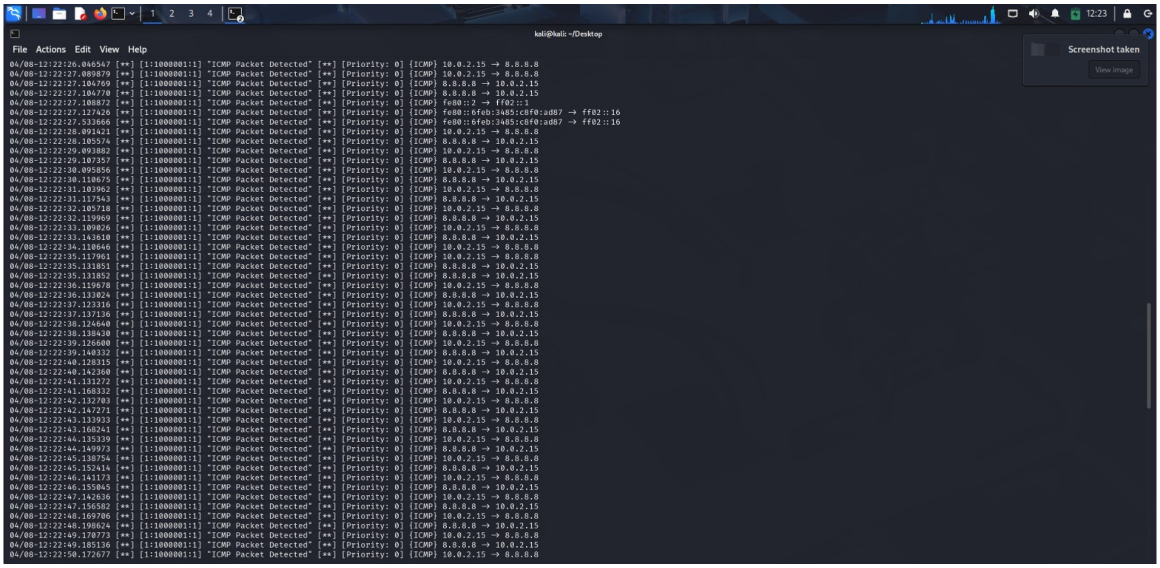
  I observed that in IDS mode, ICMP packets were detected but not blocked. In IPS mode, ICMP packets were immediately dropped, and no replies were sent back.

## Observations:

- Snort++ was successfully installed and configured in both IDS and IPS modes.
- In IDS mode, Snort++ was able to detect ICMP (ping) packets and log the alerts without blocking them. These alerts were stored in the default log file at `/var/log/snort/alert`.
- In IPS mode, after enabling drop rules, Snort++ was able to prevent ICMP packets effectively. The ping requests from the attacker machine failed, proving that the packets were dropped successfully.
- Custom rules worked as expected, and I was able to customize rules for different types of attacks like ICMP, TCP, and UDP easily.
- Snort++ generated detailed logs showing the timestamp, source IP, destination IP, and alert message for each detected or dropped packet.
- Overall, Snort++ provided flexible and powerful IDS/IPS functionalities with real-time detection and prevention capabilities.

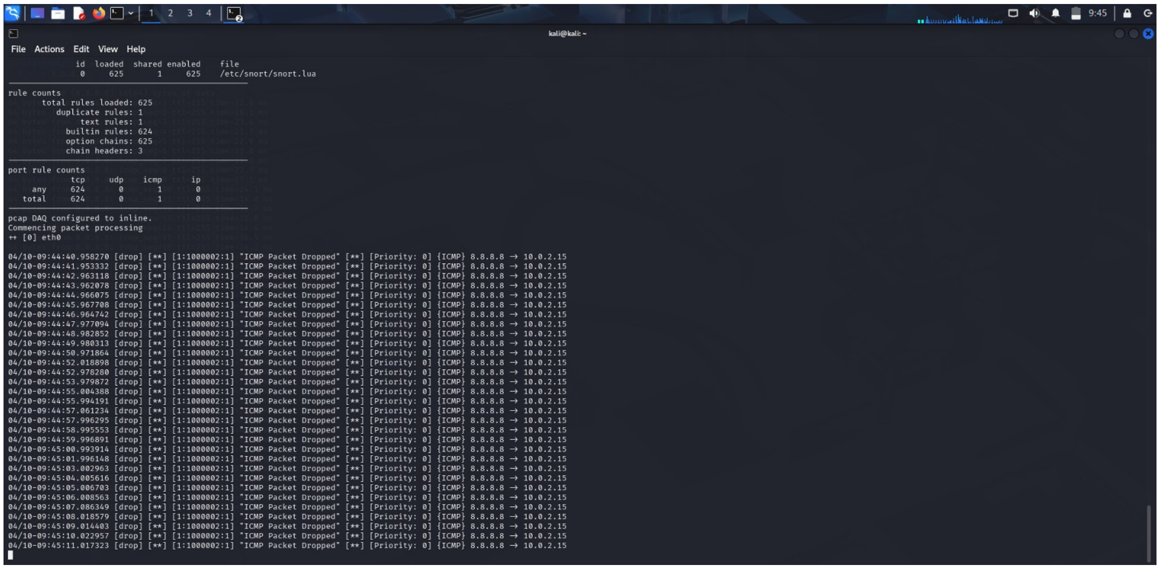
## Screenshots:

- ICMP Detection Alert in IDS Mode



```
04/08-12:22:26.046547 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:27.089879 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:27.104769 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:27.104770 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:27.108872 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} fe80::2 → ff02::1
04/08-12:22:27.127426 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} fe80::6feb:3485:c8f0:ad87 → ff02::16
04/08-12:22:27.533666 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} fe80::6feb:3485:c8f0:ad87 → ff02::16
04/08-12:22:28.091421 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:28.105574 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:29.093882 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:29.107357 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:30.095856 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:30.110675 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:31.103962 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:31.117543 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:32.105718 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:32.119969 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:33.109026 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:33.143610 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:34.110646 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:35.117961 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:35.131851 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:35.131852 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:36.119678 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:36.133024 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:37.123316 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:37.137136 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:38.124640 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:38.138430 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:39.126600 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:39.140332 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:40.128315 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:40.142360 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:41.131272 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:41.168332 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:42.132703 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:42.147271 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:43.133933 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:43.168241 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:44.135339 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:44.149973 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:45.138754 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:45.152414 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:46.141173 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:46.155045 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:47.142636 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:47.156582 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:48.169706 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:48.198624 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:49.170773 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
04/08-12:22:49.185136 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/08-12:22:50.172677 [**] [1:1000001:1] "ICMP Packet Detected" [**] [Priority: 0] {ICMP} 10.0.2.15 → 8.8.8.8
```

- ICMP Packet Dropped in IPS Mode



```
            id  loaded  shared enabled    file
             0     625       1     625    /etc/snort/snort.lua
--------------------------------------------------
rule counts
       total rules loaded: 625
          duplicate rules: 1
               text rules: 1
            builtin rules: 624
            option chains: 625
            chain headers: 3
--------------------------------------------------
port rule counts
             tcp     udp    icmp      ip
     any     624       0       1       0
   total     624       0       1       0
--------------------------------------------------
pcap DAQ configured to inline.
Commencing packet processing
++ [0] eth0

04/10-09:44:40.958270 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:41.953332 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:42.963118 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:43.962078 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:44.966075 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:45.967708 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:46.964742 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:47.977094 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:48.982852 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:49.980313 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:50.971864 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:52.018898 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:52.978280 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:53.979872 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:55.004388 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:55.994191 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:57.061234 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:57.996295 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:58.995553 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:44:59.996891 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:00.993914 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:01.996148 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:03.002963 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:04.005616 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:05.006703 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:06.008563 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:07.086349 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:08.018579 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:09.014403 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:10.022957 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
04/10-09:45:11.017323 [drop] [**] [1:1000002:1] "ICMP Packet Dropped" [**] [Priority: 0] {ICMP} 8.8.8.8 → 10.0.2.15
```

# Conclusion

This lab helped me to practically understand how Snort works in both IDS and IPS modes. Since I had two Kali Linux machines, I was able to generate ICMP traffic from one machine (attacker) and detect or block it on the other machine (victim) where Snort was installed. I learned how to write custom Snort rules for detecting specific traffic patterns, properly configure the `snort.conf` file, and use `iptables` for traffic redirection in IPS mode.