**Name - Gaurang A Raorane Roll No - 49**

**Class - D15A Batch - C**

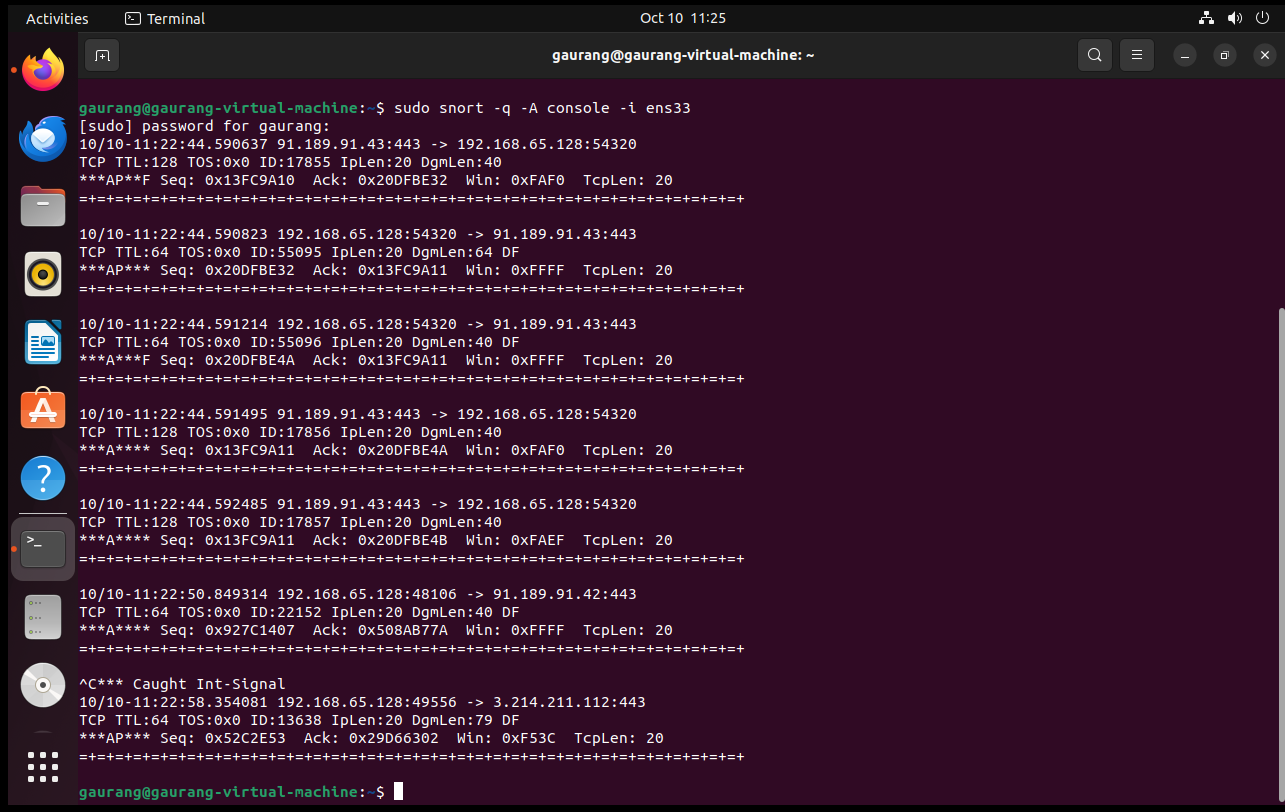
**EXPERIMENT 9**

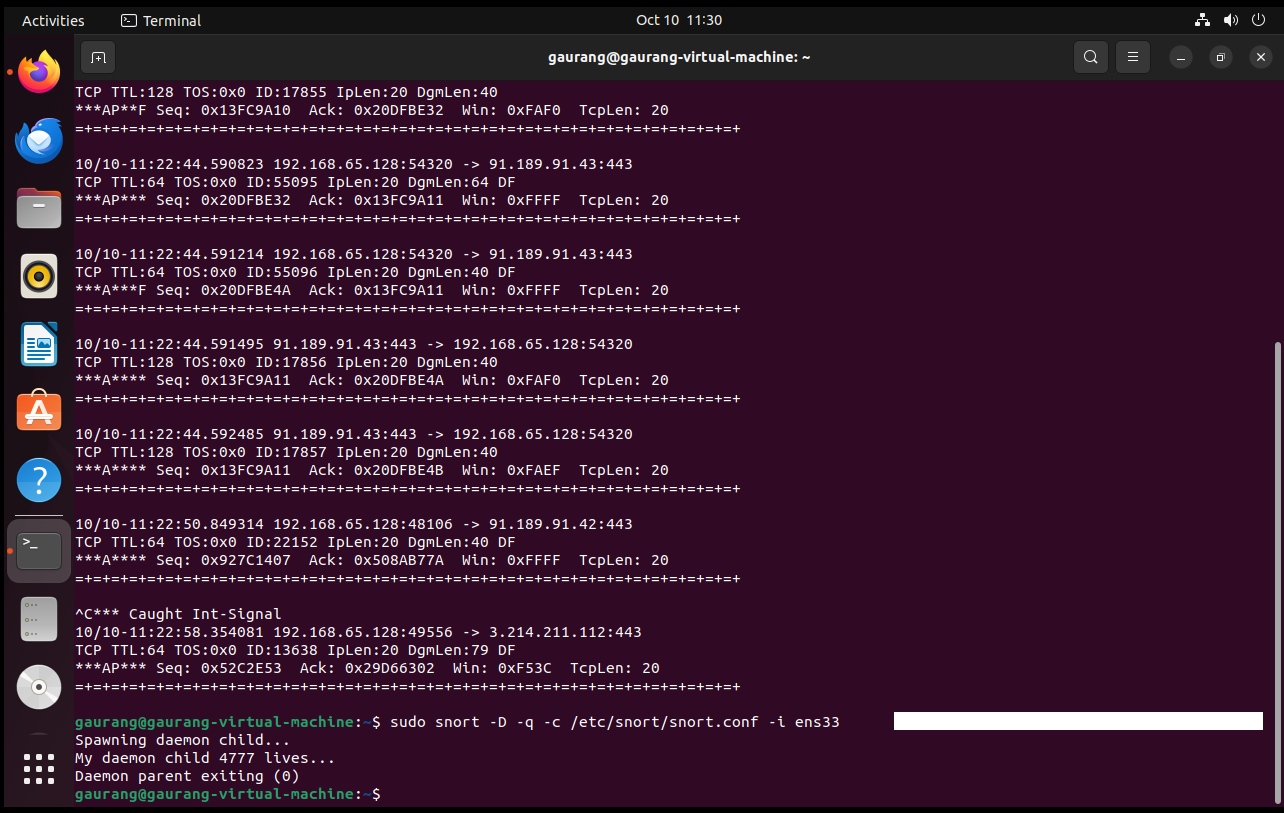
**Aim:-** Study of Network security : Set up Snort and study the logs

**Theory:-**

In today's interconnected world, network security is of paramount importance. Intrusion Detection Systems (IDS) play a crucial role in safeguarding networks by monitoring traffic for suspicious activities or known attack patterns. Snort, an open-source IDS, is a widely-used tool for this purpose. This lab aims to provide hands-on experience in setting up Snort and analyzing its generated logs.

* **Intrusion Detection System (IDS):** IDS is a critical component of network security, designed to monitor network traffic for suspicious activities and potential security threats. Snort is utilized in this lab as an IDS.
* **Snort Rules:** Snort employs rules to specify the conditions for generating alerts. Rules are written in a simple language and define the patterns or behaviors that Snort should watch for.
* **Sniffer Mode vs. Inline Mode:** Snort can function in either a sniffer mode (passive) or an inline mode (active). In sniffer mode, it observes network traffic without direct intervention, while in inline mode, it has the capability to block or modify traffic.
* **Logging:** Snort generates log files that contain vital information about network traffic and detected security events. These logs are essential for security analysts to identify and respond to potential threats.





**Conclusion :-** Snort is set up successfully and logs are studied.