**Cryptography & Network Security Lab**

**PRN/ Roll No: 2019BTECS00004**

**Full name: Yash Babasaheb Nale**

**Batch: B1**

**Assignment No. 15**

**<https://www.sunnyvalley.io/docs/linux-tutorials/how-to-install-and-configure-snort-on-ubuntu-linux>**

**Title: Snort Intrusion Detection System (IDS)**

**Aim: To install and configure Snort Intrusion Detection System (IDS)**

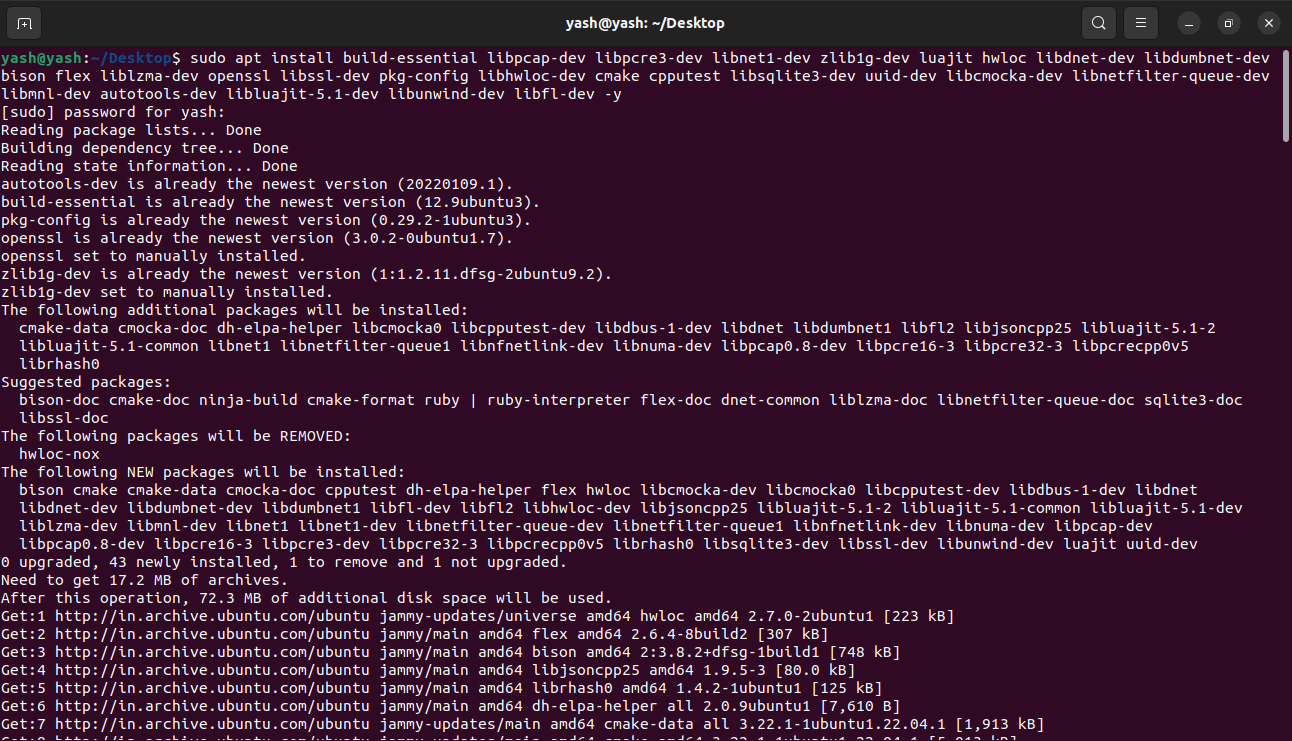
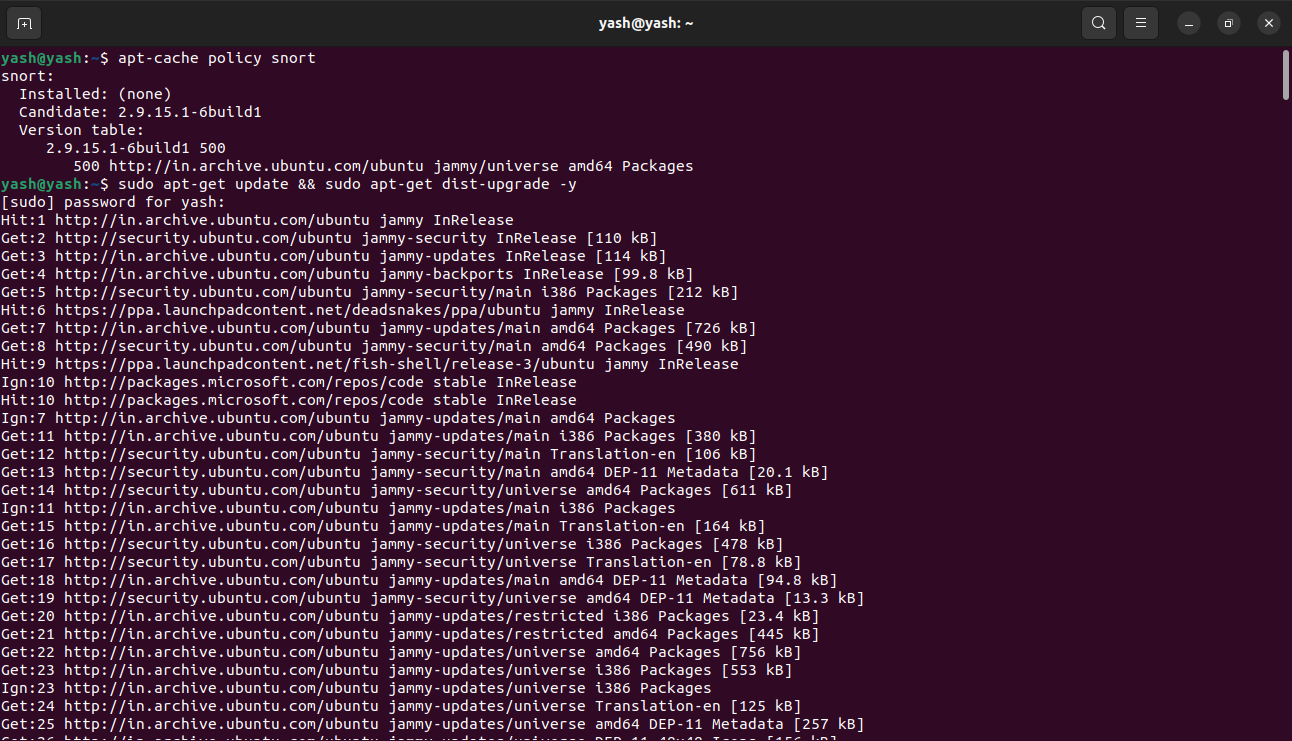
**Theory:**

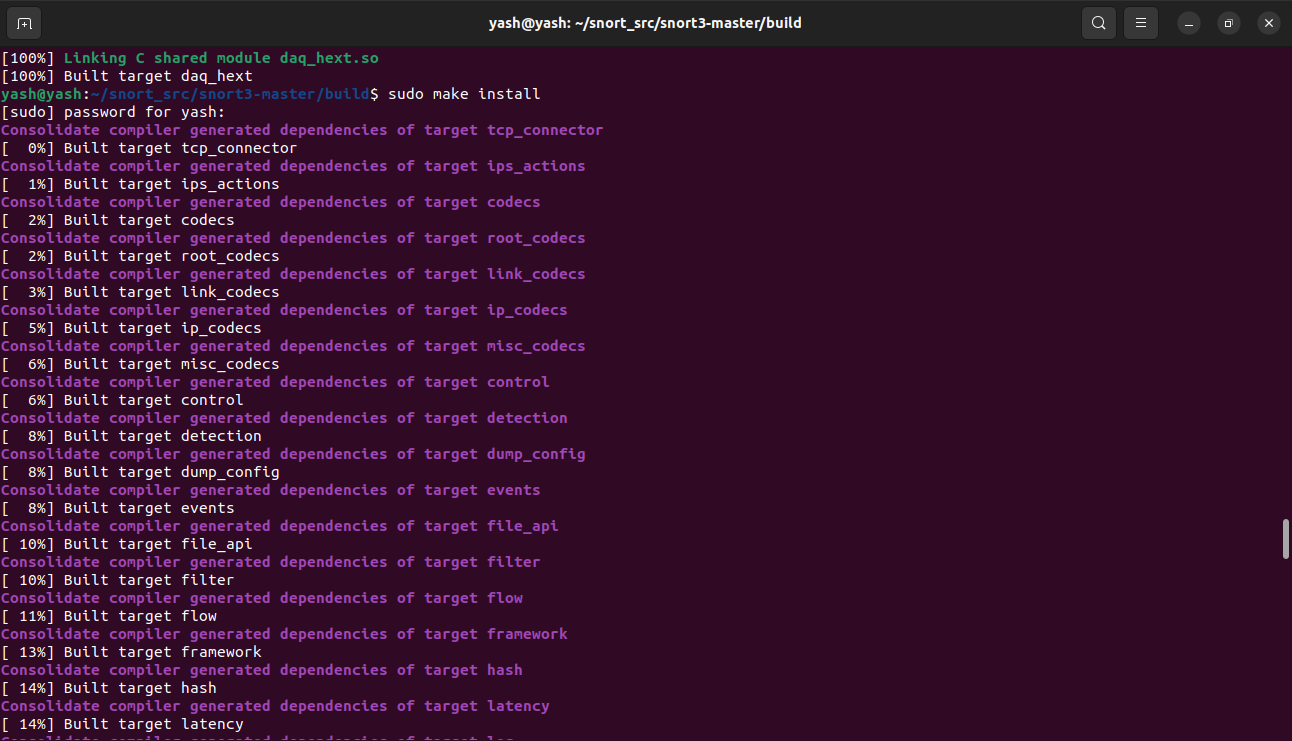
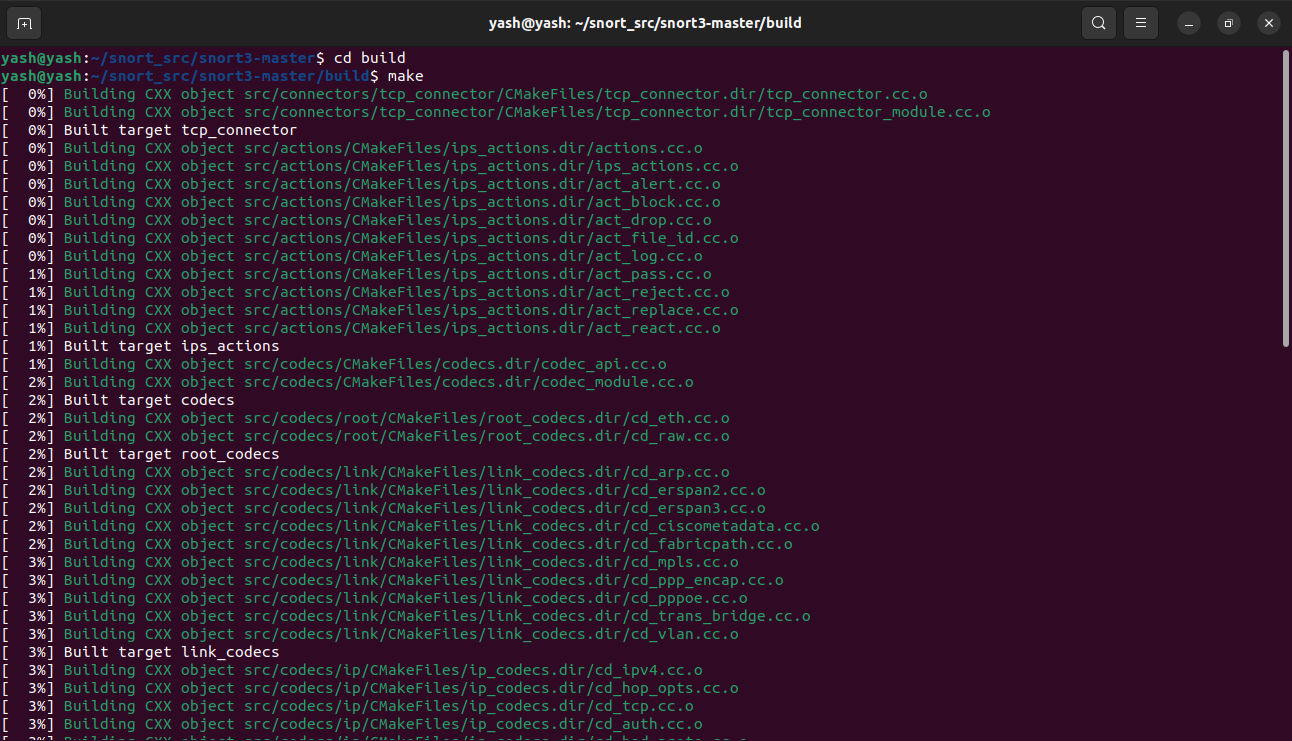
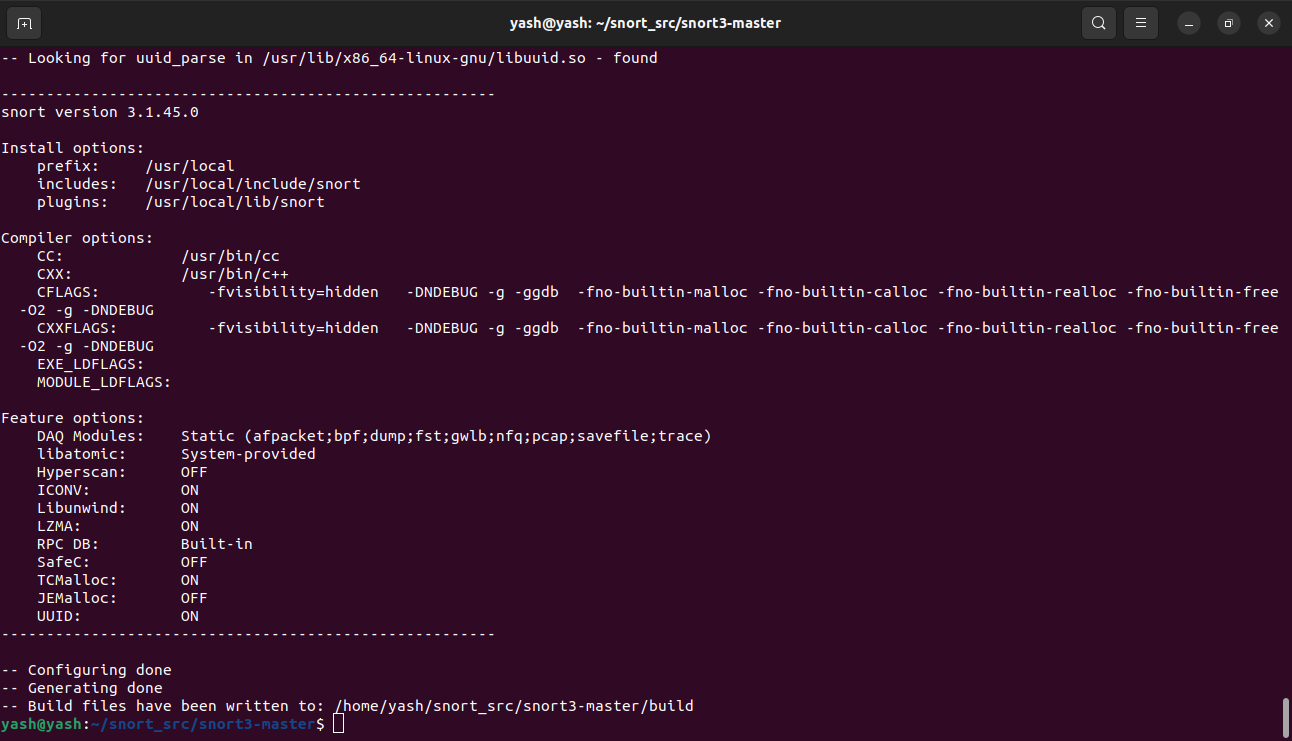
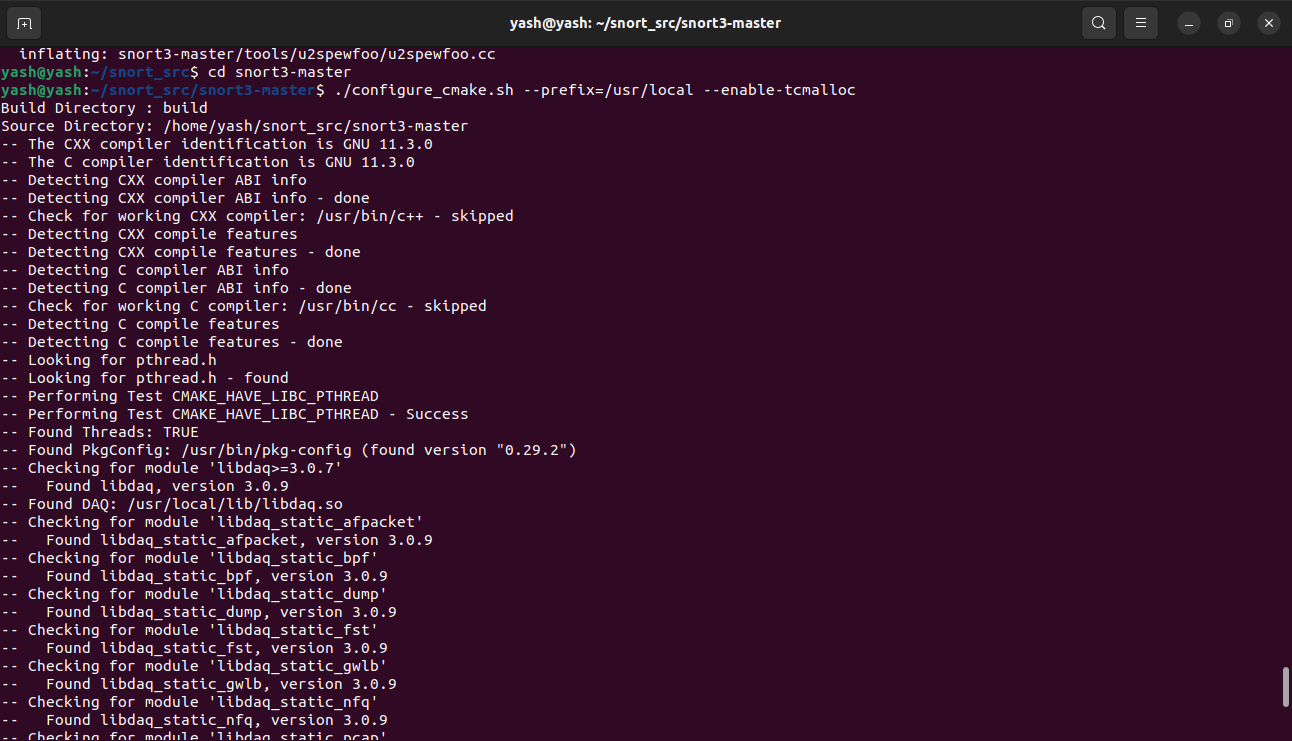
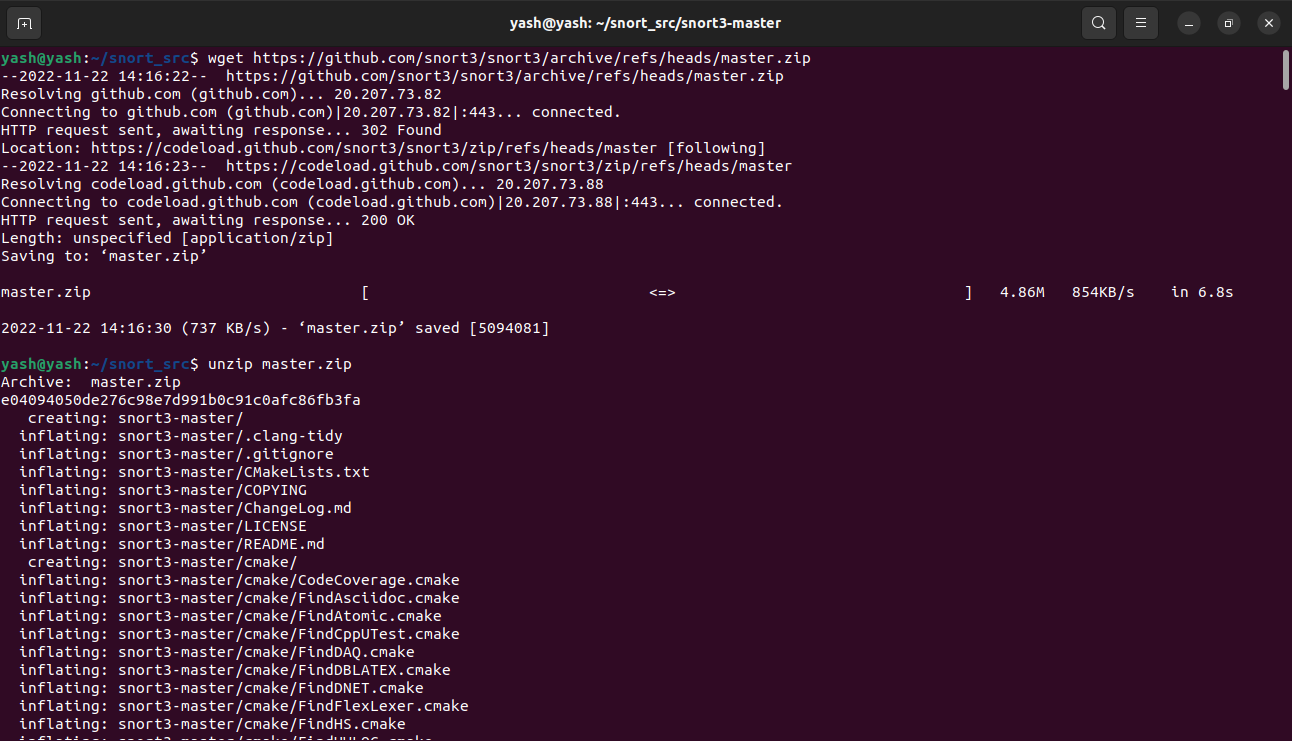
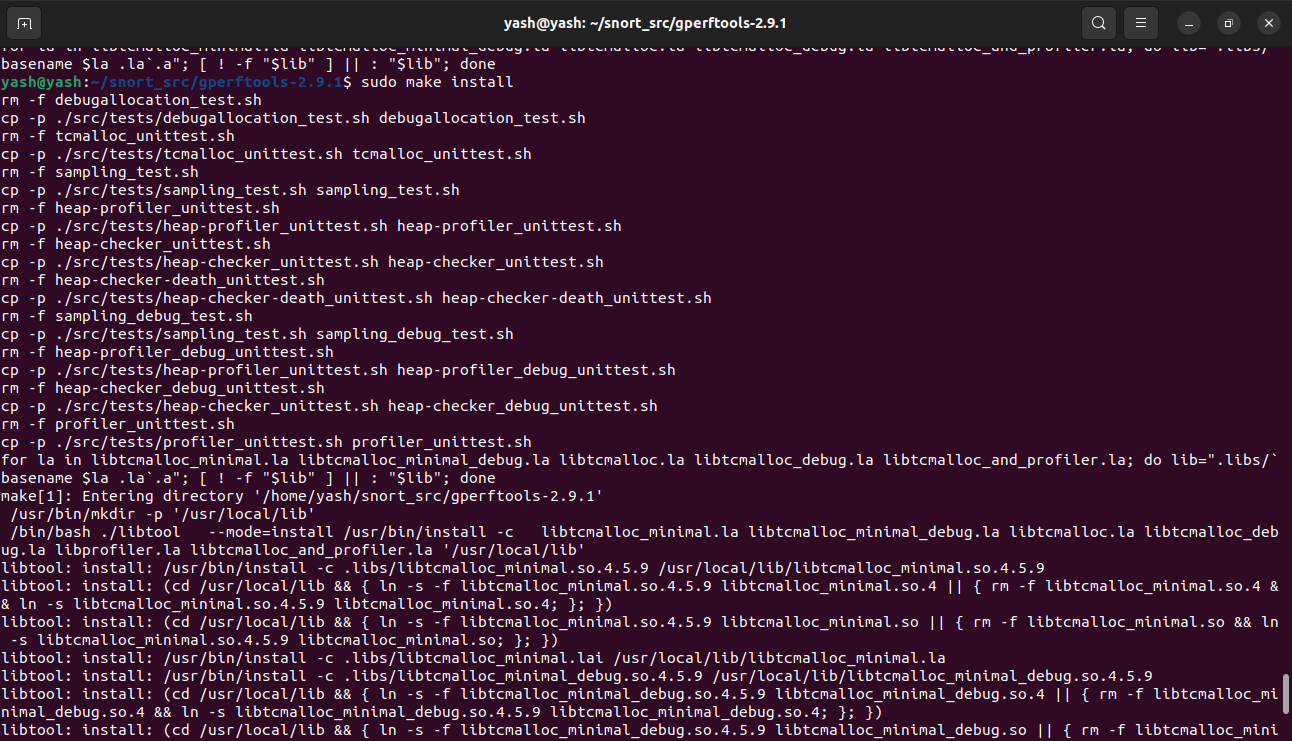
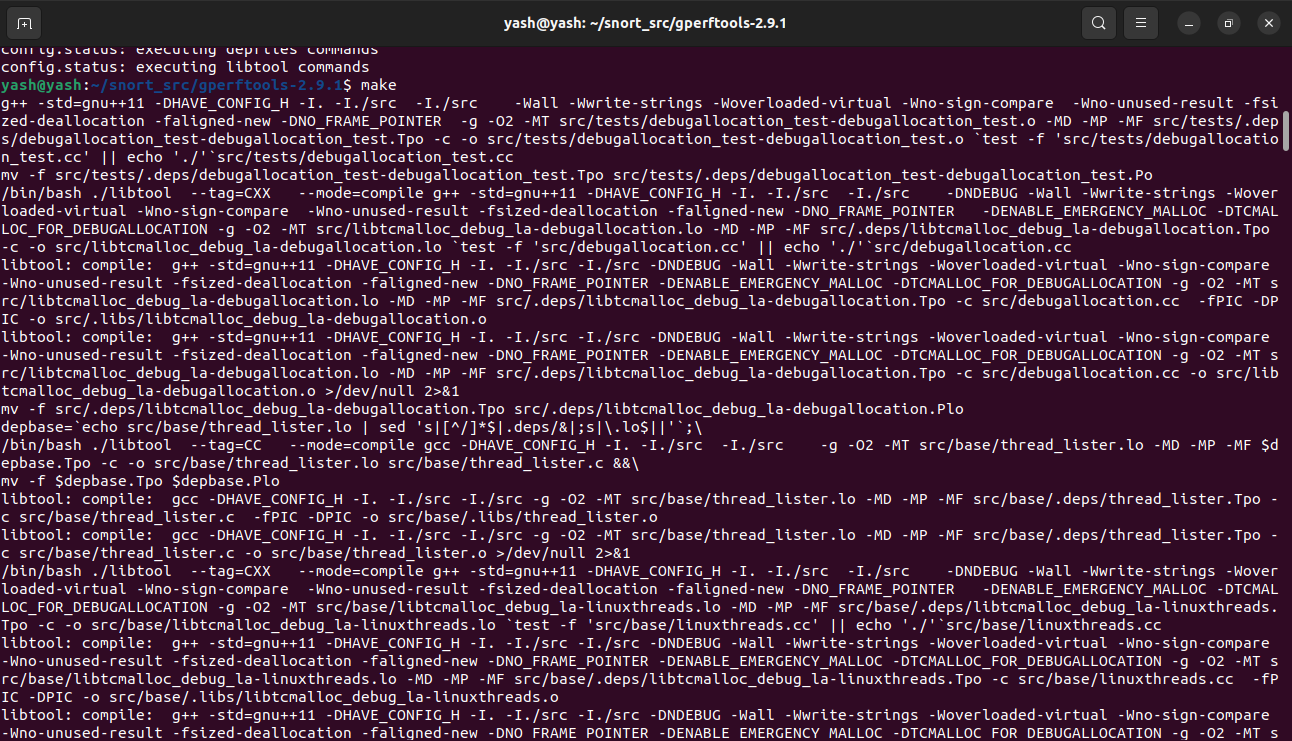
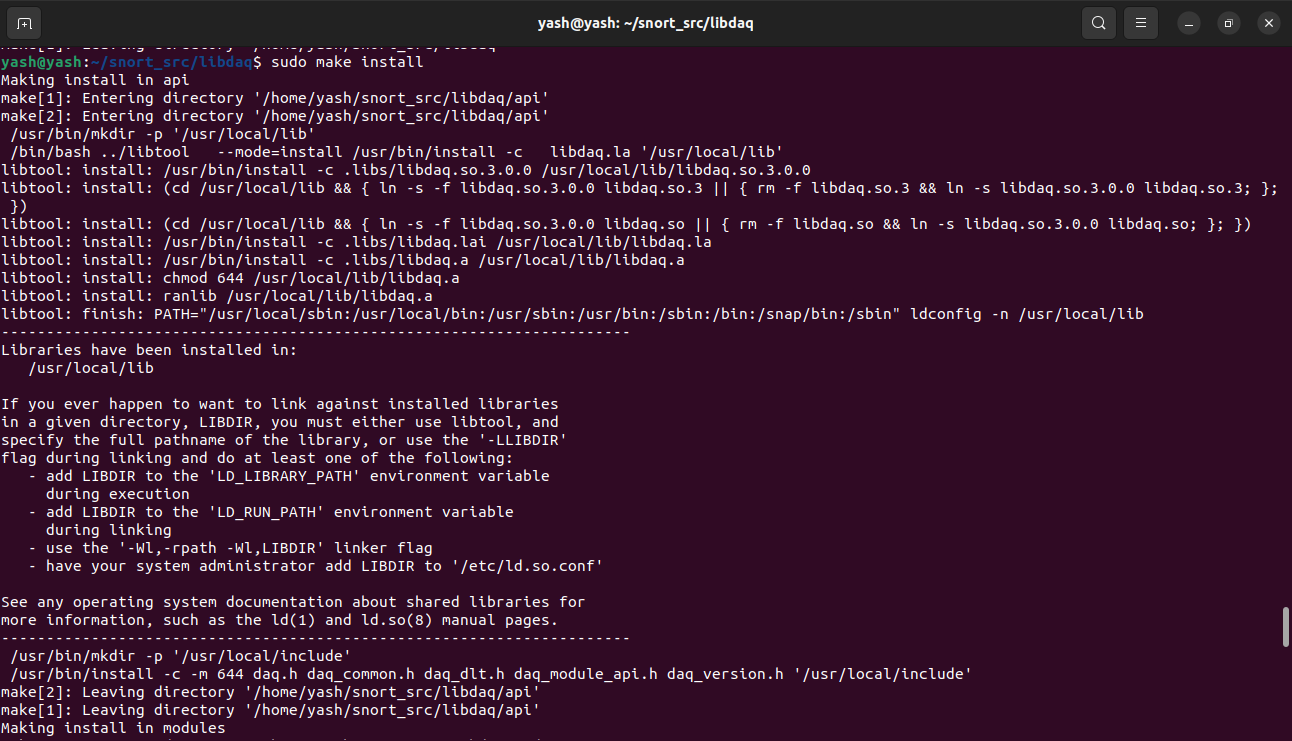
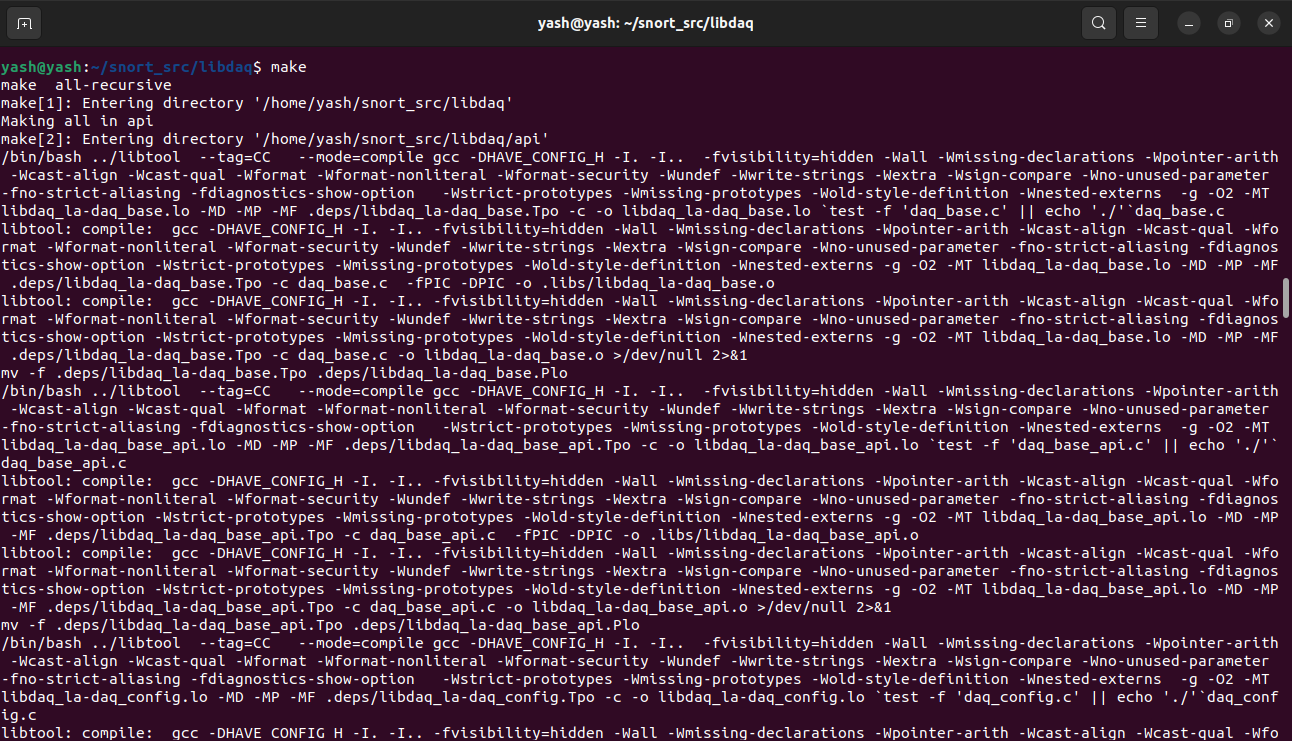
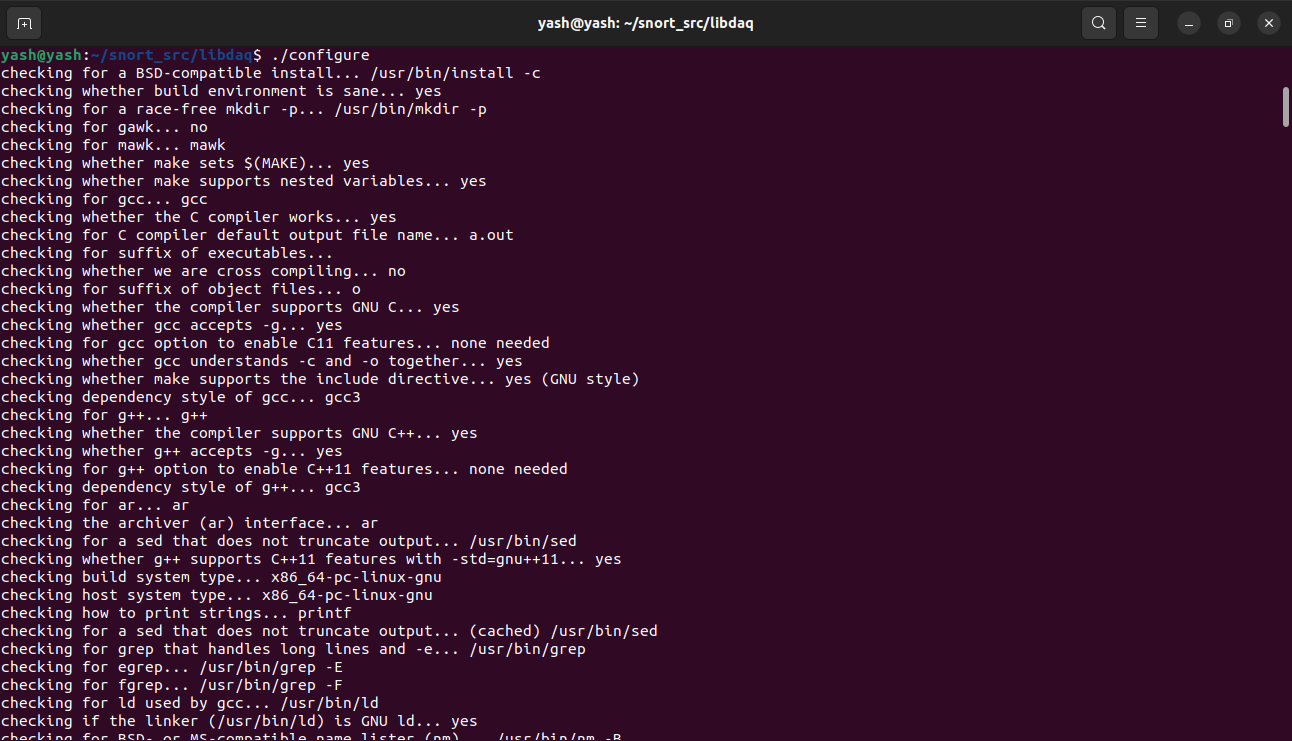
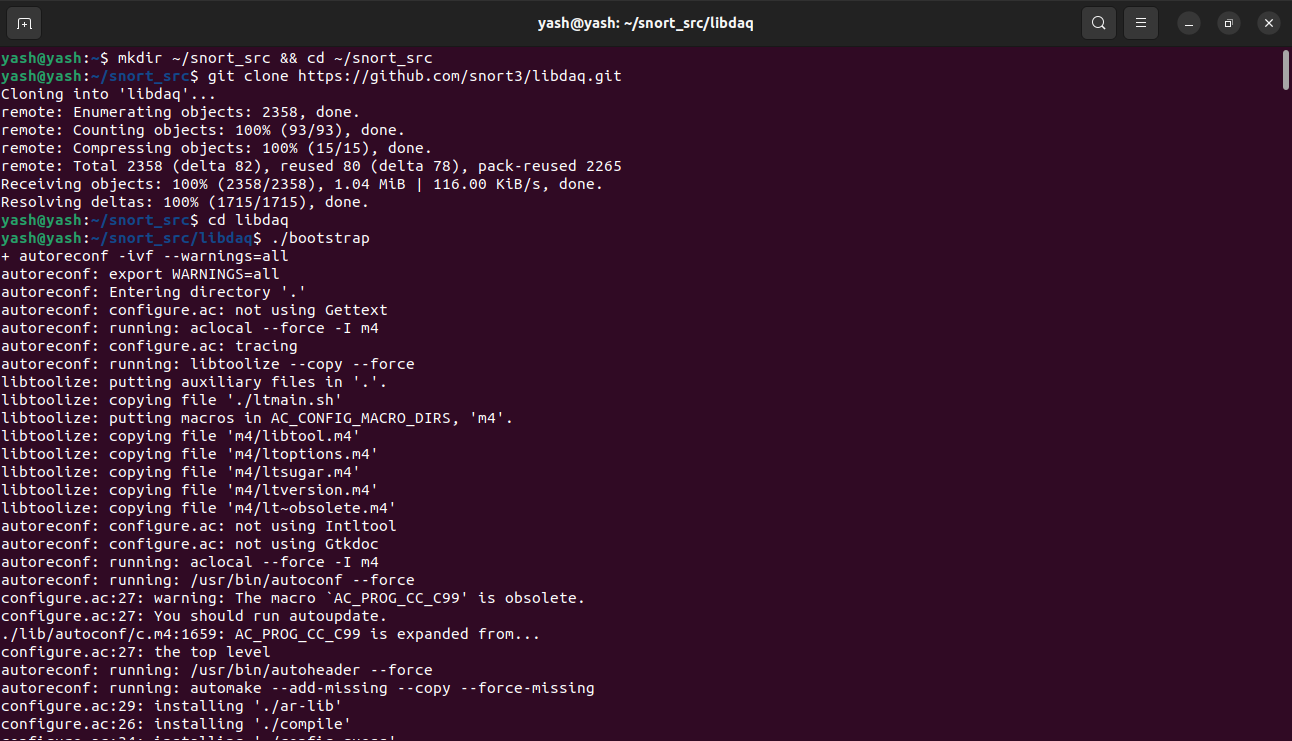
**Snort is referred to as a packet sniffer that monitors network traffic, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies. It’s an intrusion prevention and detection tool.**

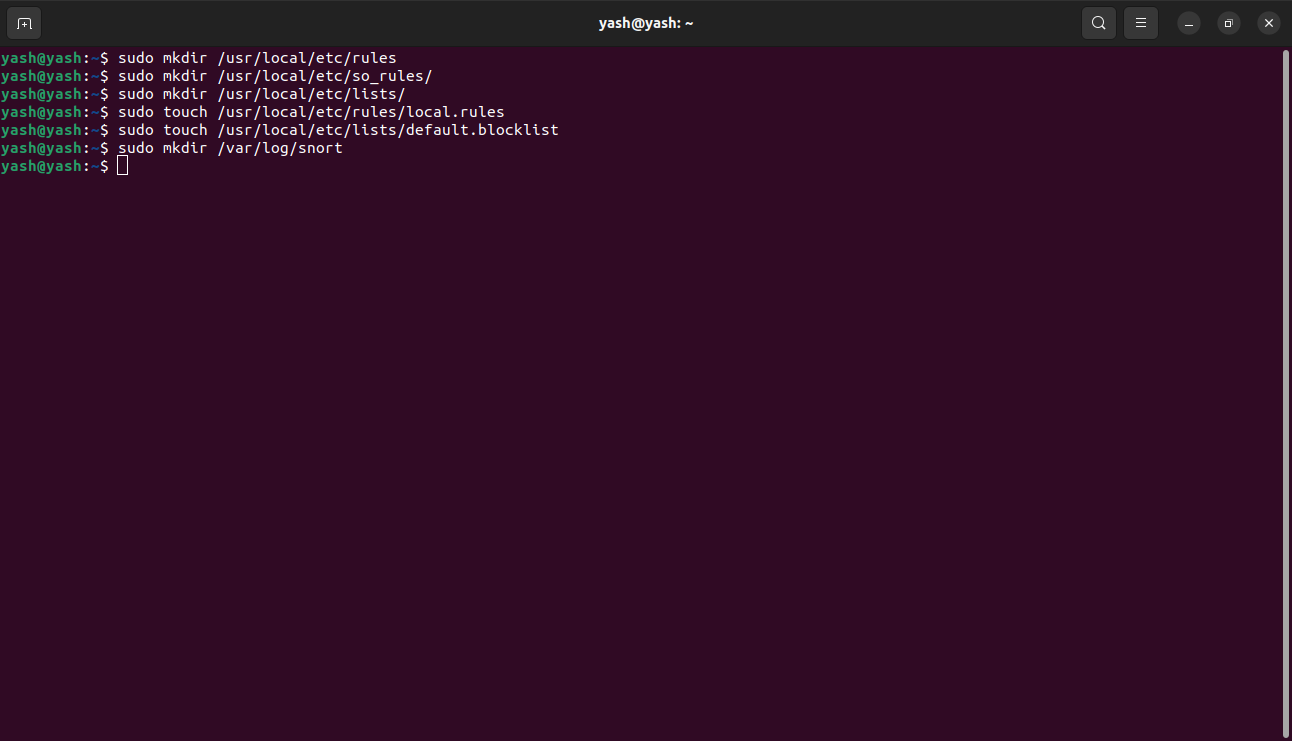
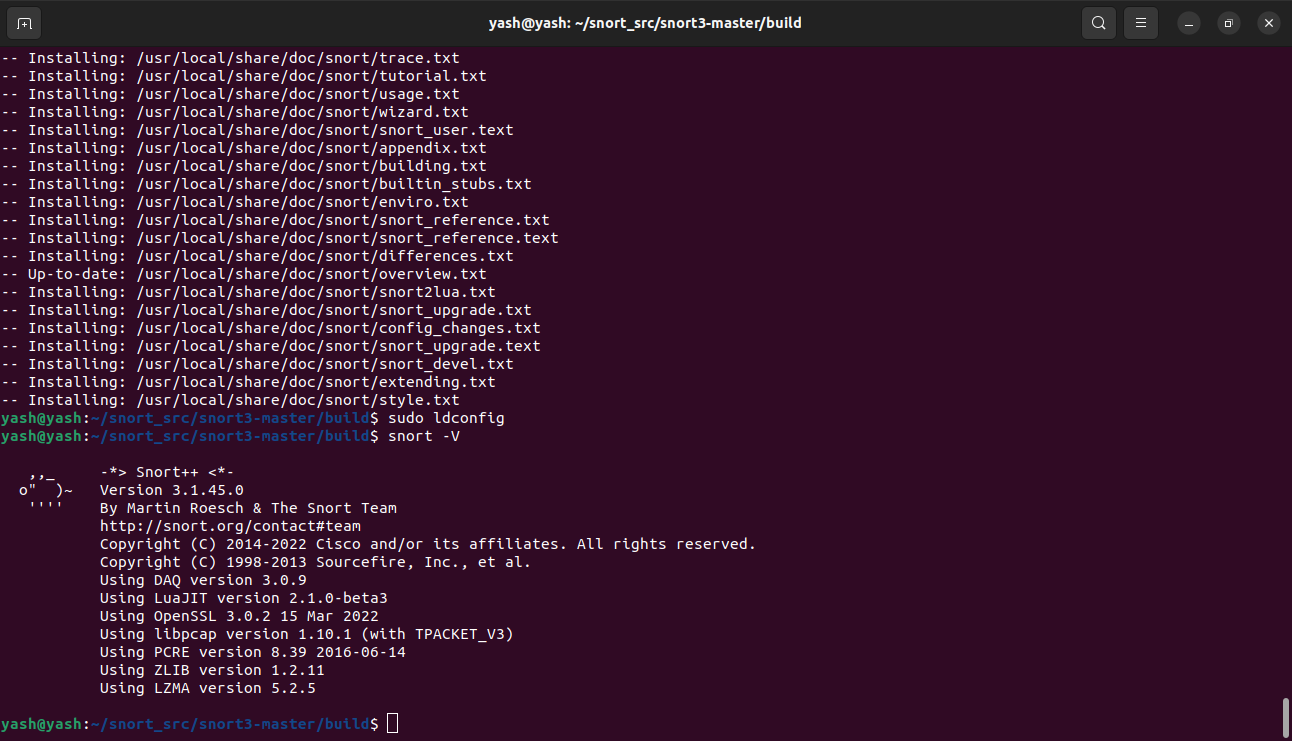
**Screenshots:**

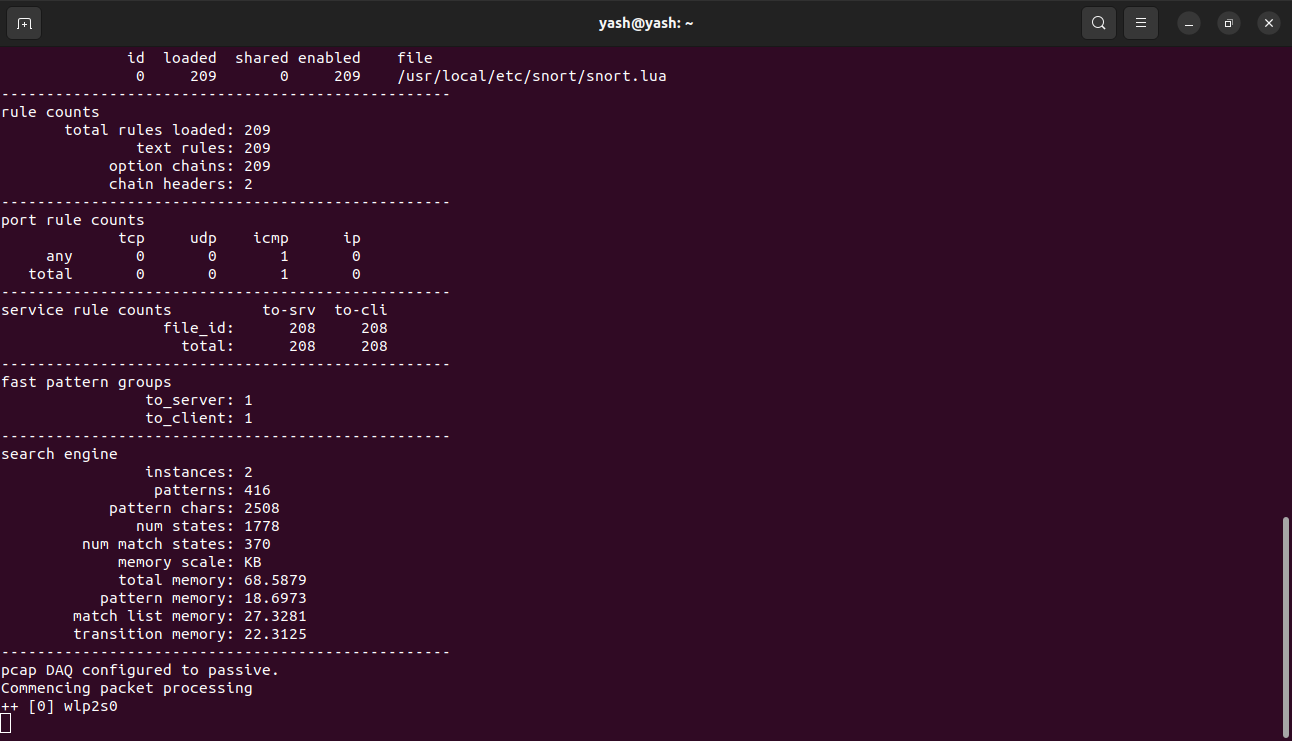
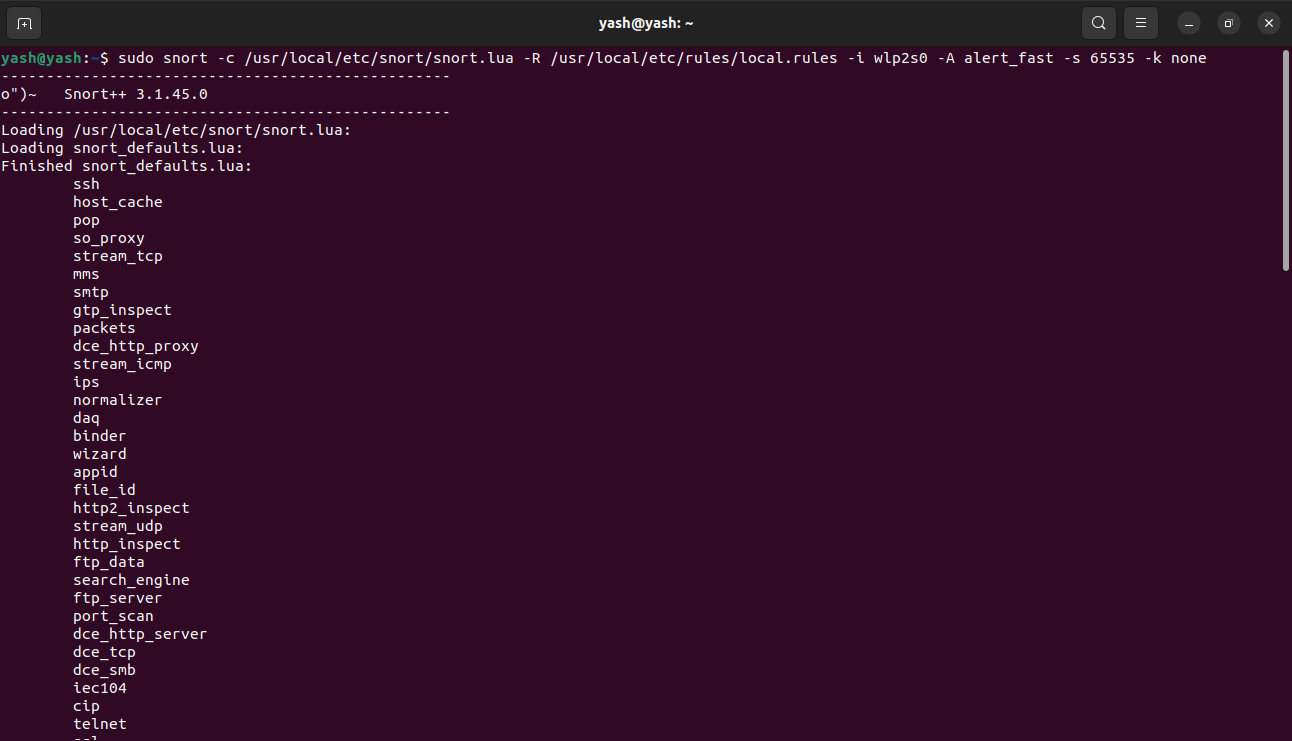
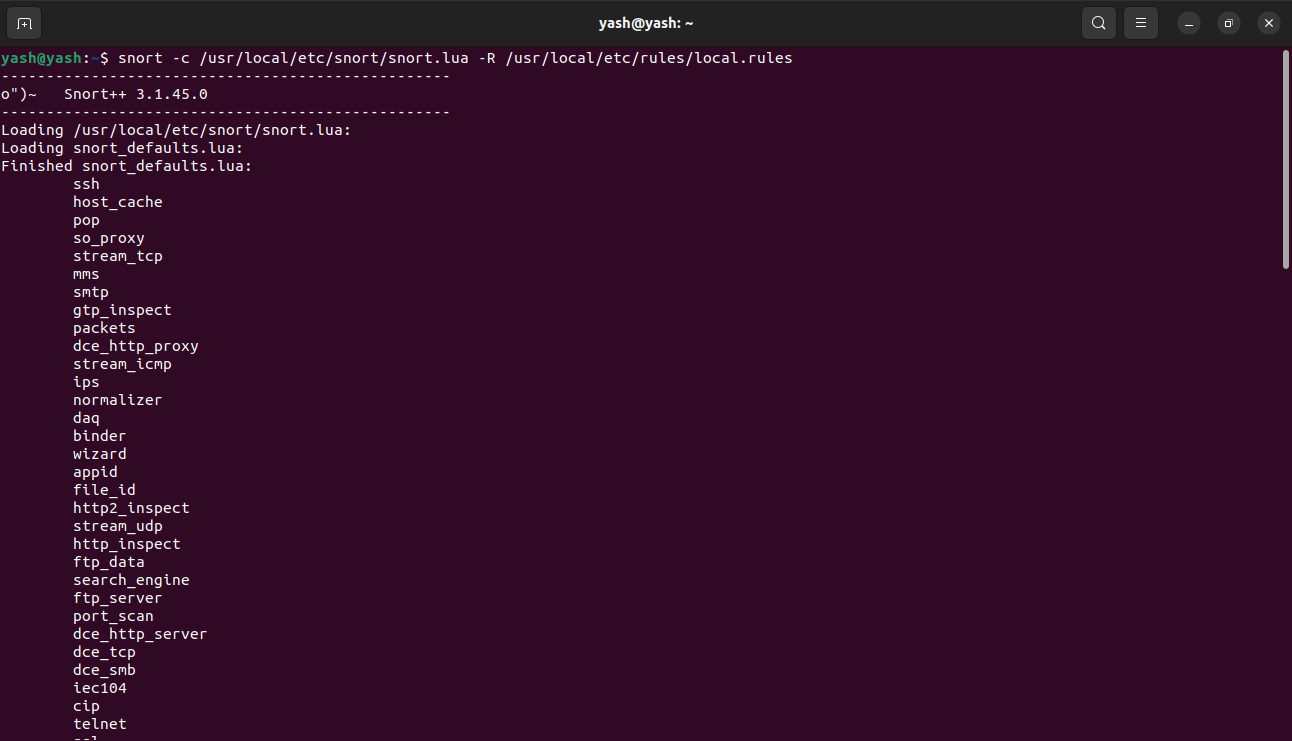
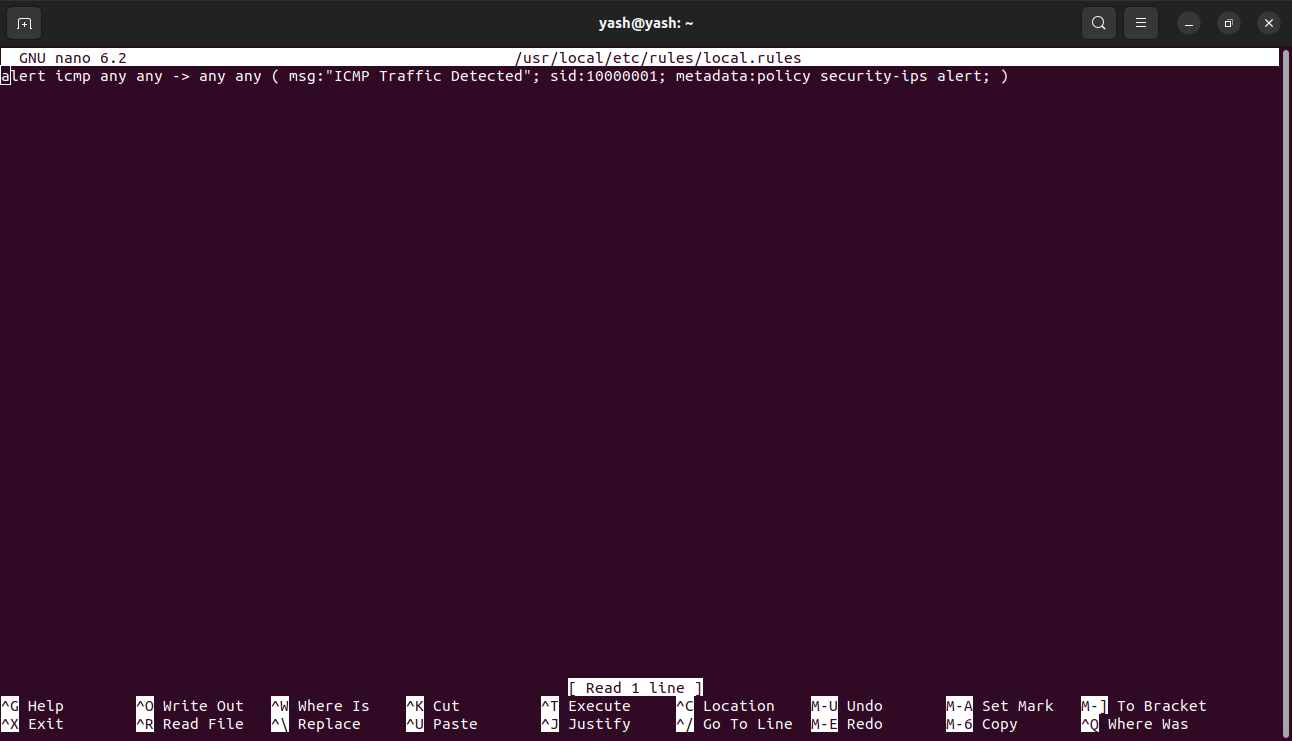
**Snort Installation**

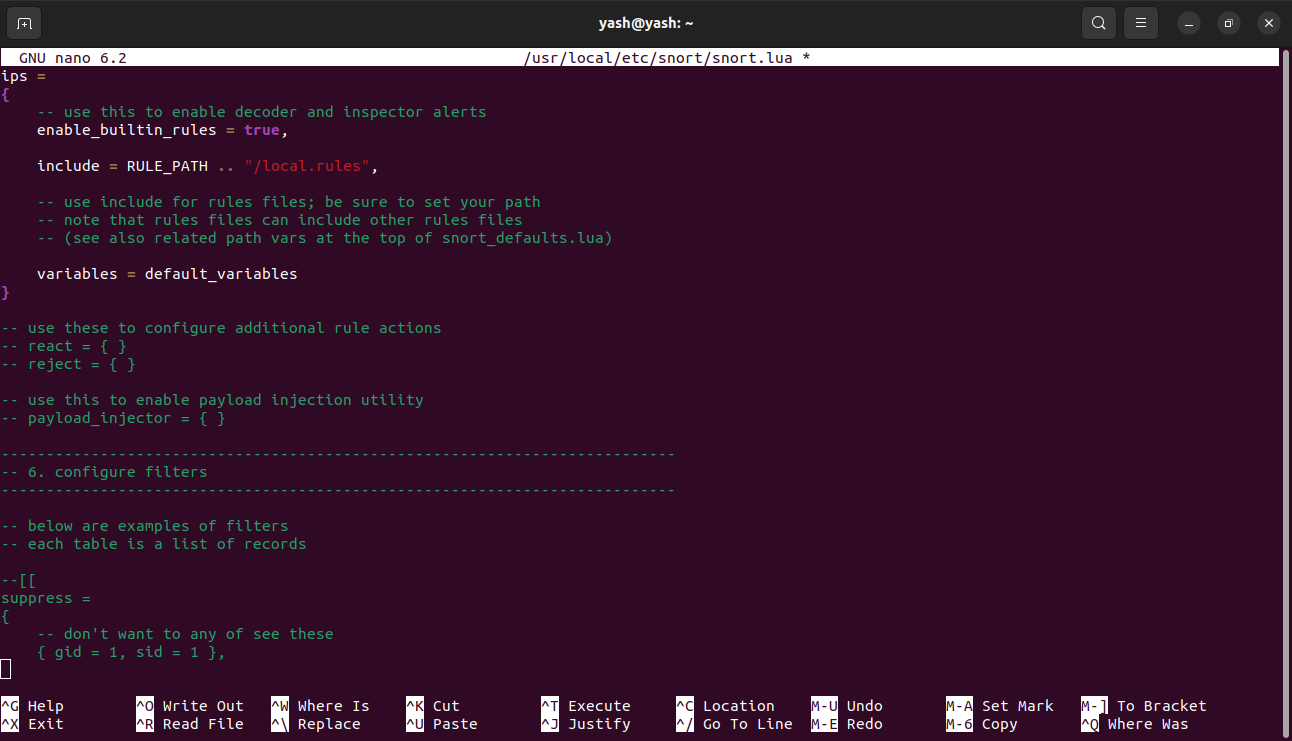
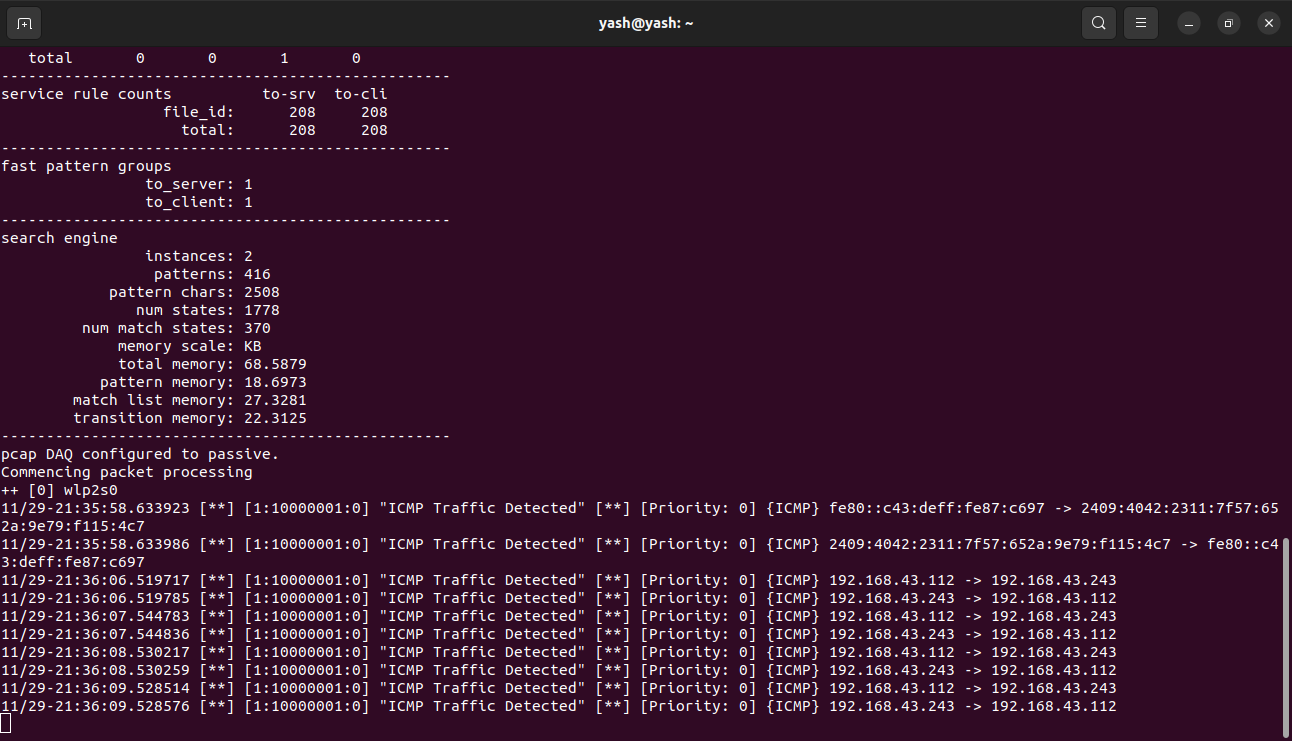
**Updating the Ubuntu server & Installing dependencies**

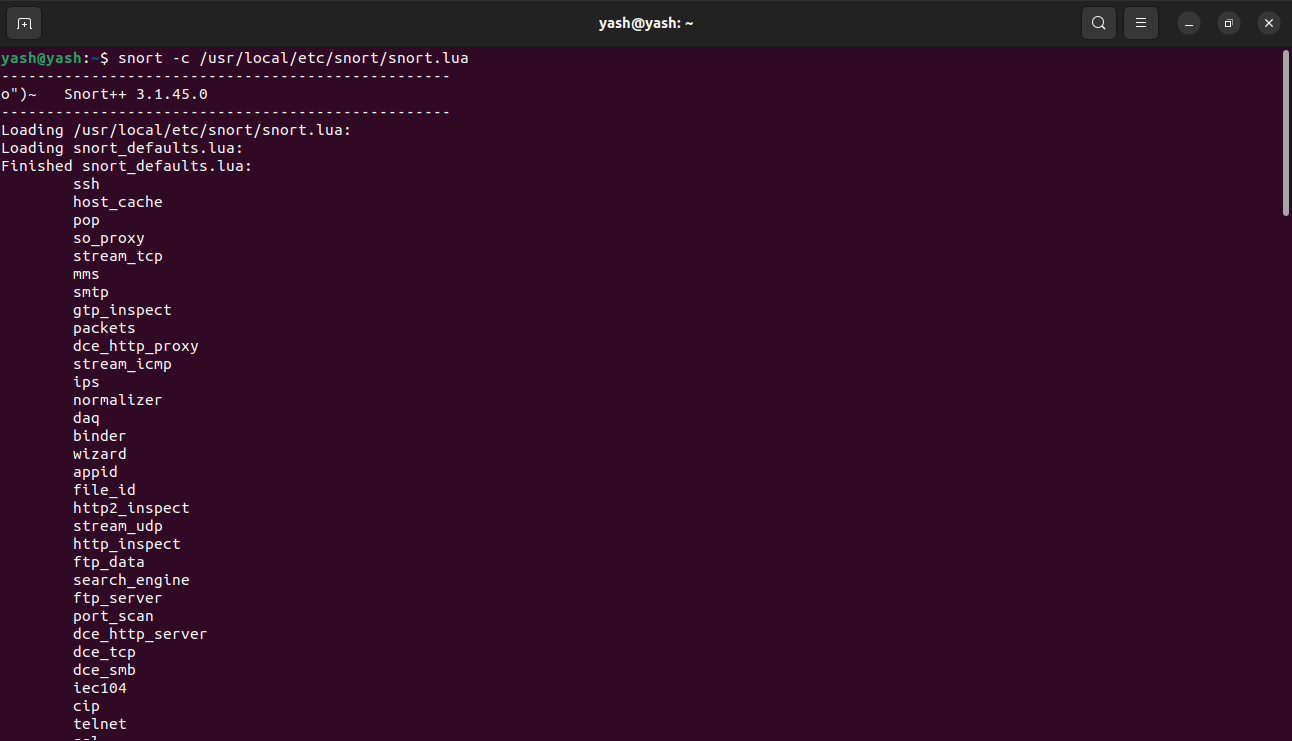
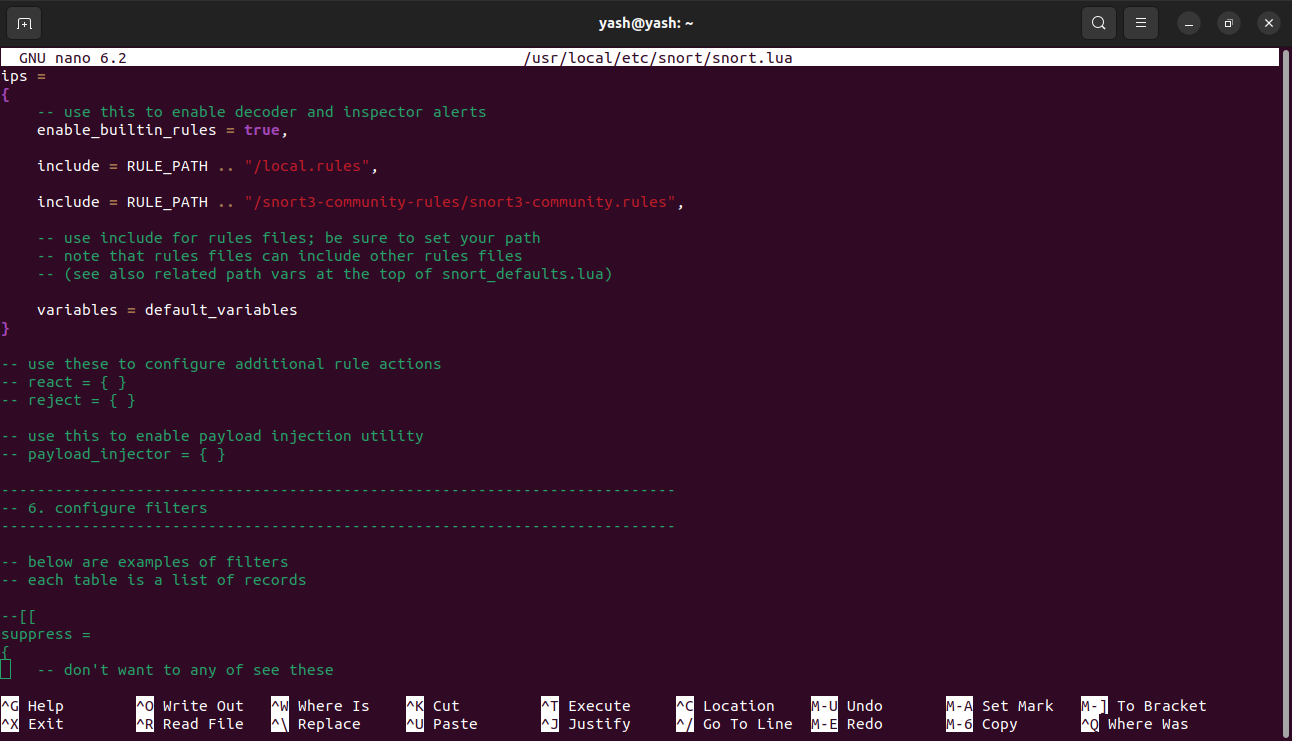
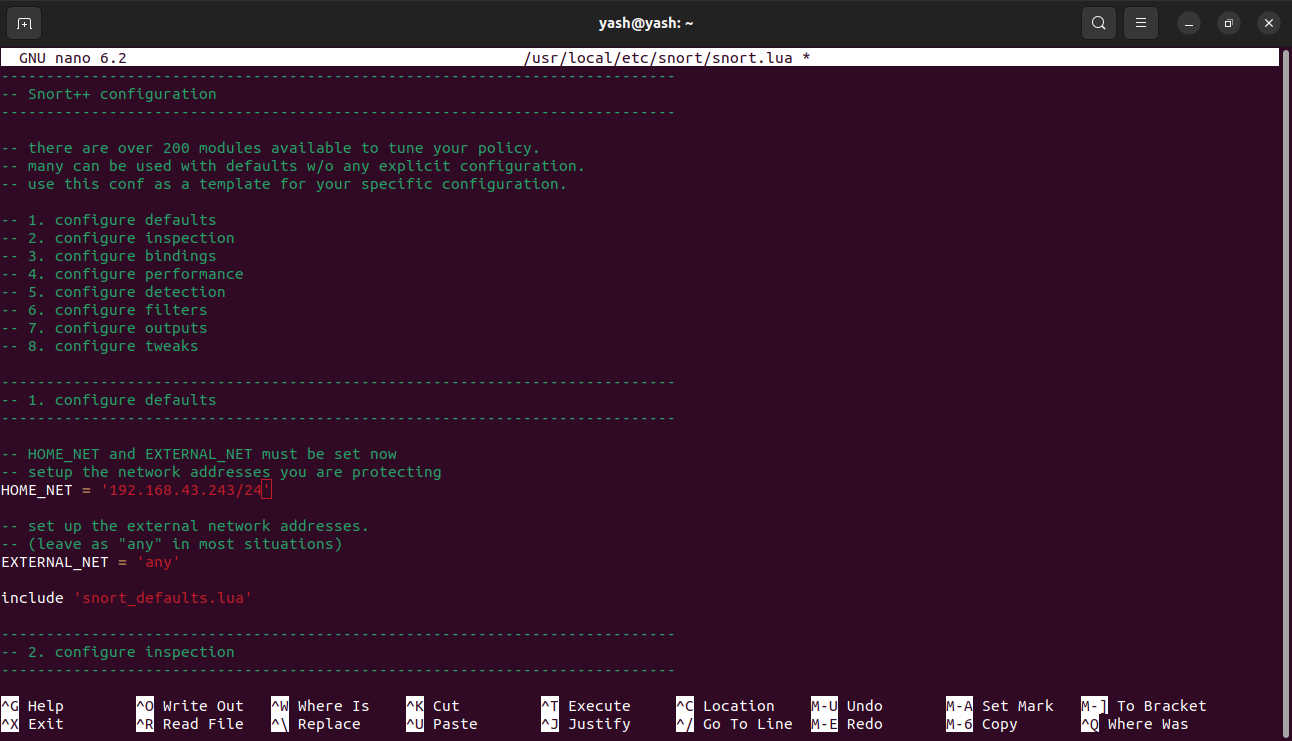
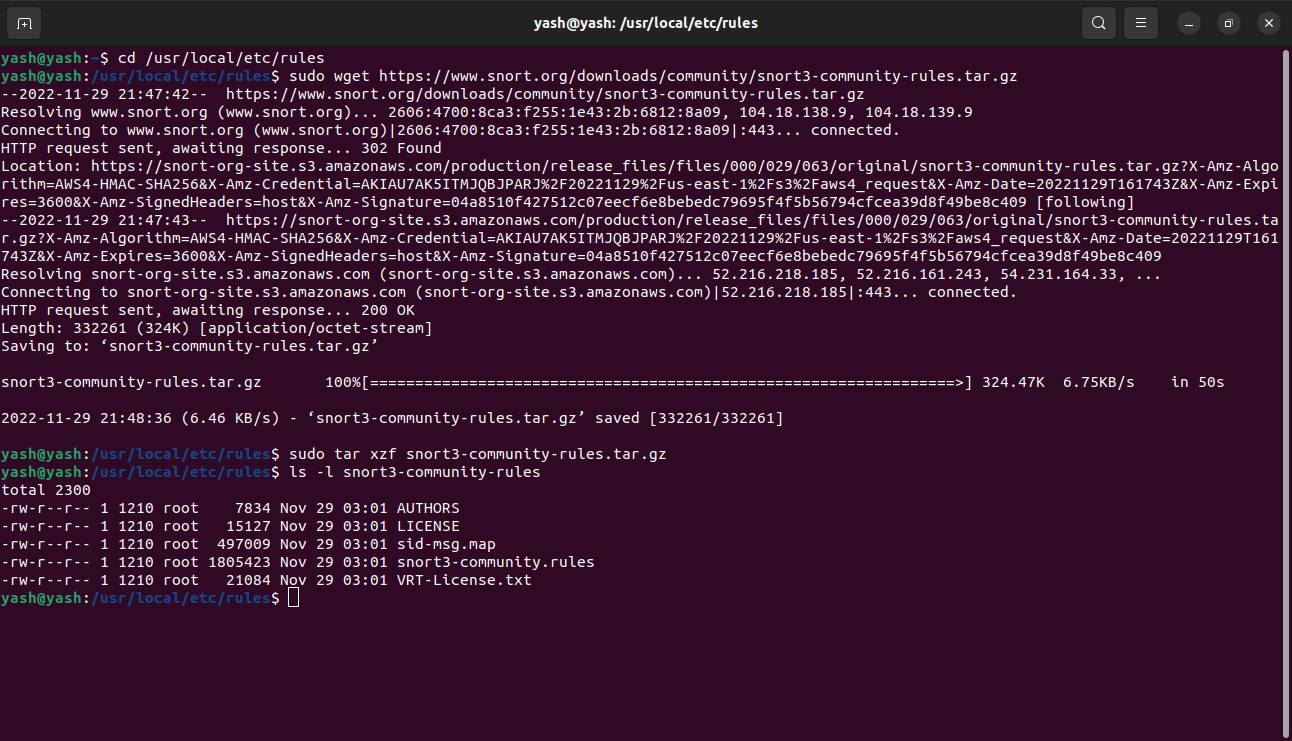
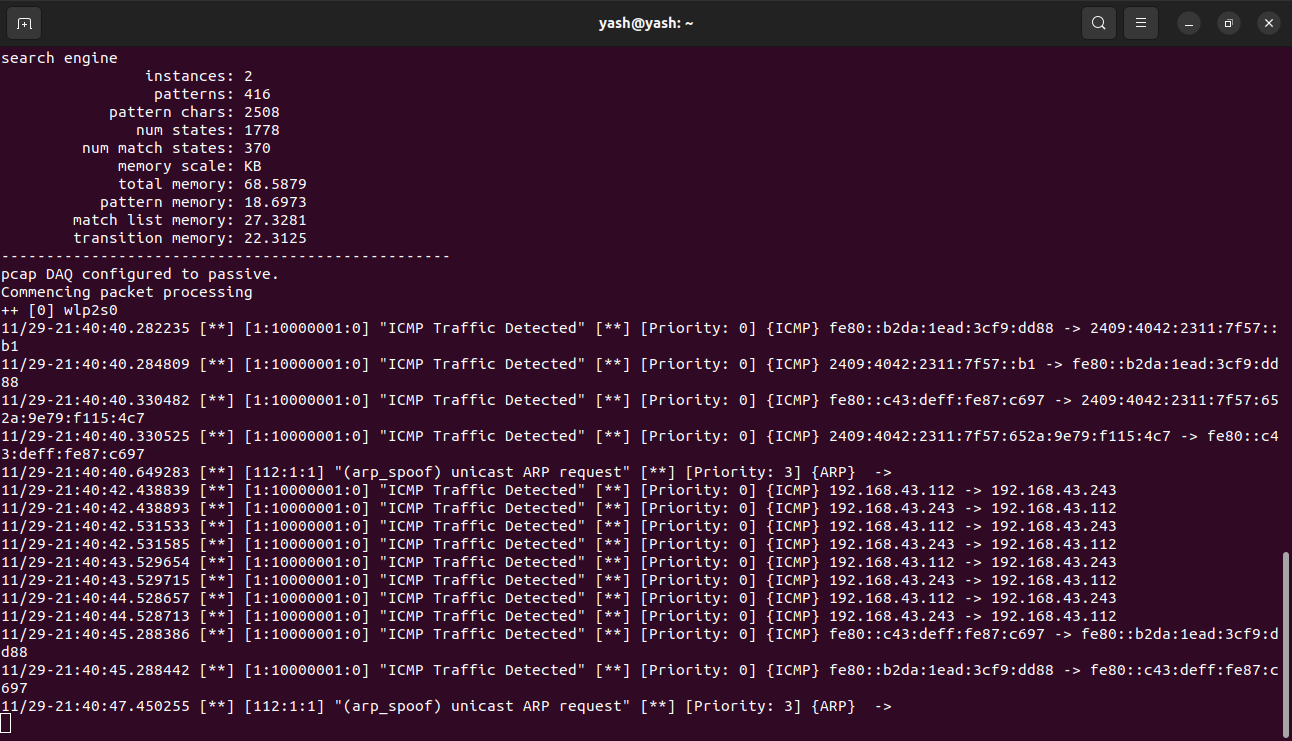
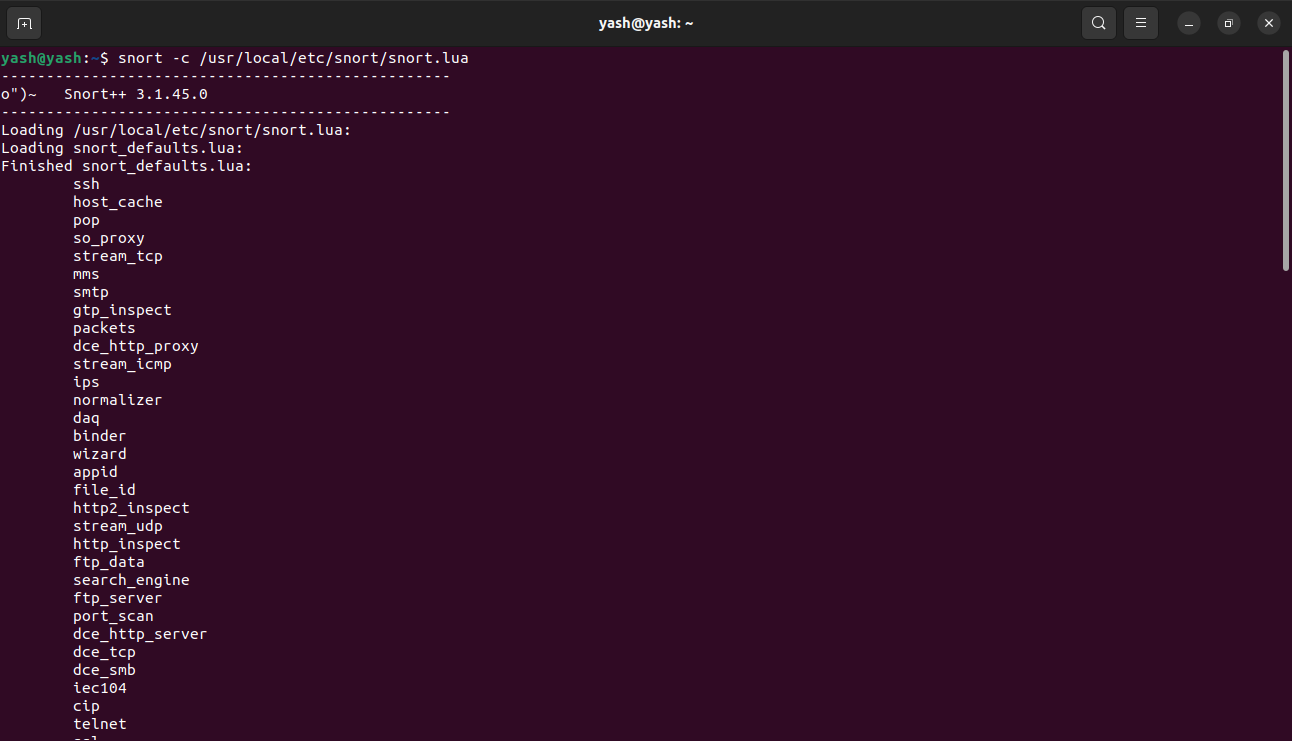
****

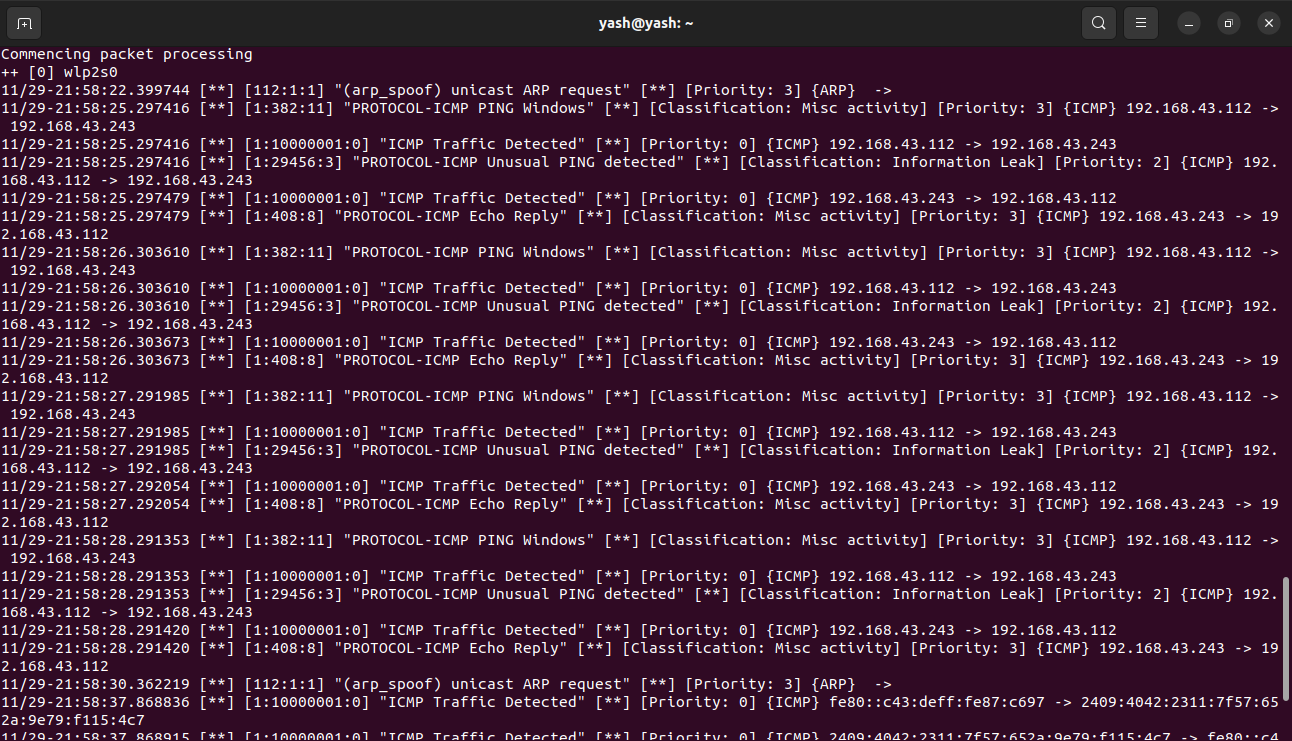
**Downloading and installing Snort from source code**

**Snort version 3.1.45.0**

**Configuring local rules**

**ICMP Traffic Detection**

**Local rules configuration verification**

**Snort Logs**

**Conclusion:**

**Snort analyzes the traffic and logs the output.**