# How to Use the Snort IDS/IPS Complete Practical Guide

By **Tamil S** - May 9, 2023


Snort is a widely used open-source Network Intrusion Detection System (NIDS) that can analyze network traffic and detect potential security threats.

It works by analyzing network traffic in real time and comparing it against a set of rules, which the user or administrator defines.

> It can detect various attacks, such as port scans, buffer overflows, and malware infections. When Snort detects an attack, it can generate an alert, log the event, and even block the offending traffic.

The tool can be deployed on various operating systems, including Windows, Linux, and macOS. It can be configured to monitor traffic on a single host or an entire network.

It also has a variety of add-ons and plugins that can extend its functionality.

## Table of Contents



## Key Features

- **Packet sniffing** – It can capture network packets and analyze the headers and payloads.
- **Rule-based detection** – It uses a rules file to detect malicious traffic. The rules are based on signatures of known attacks.
- **Protocol analysis** – It can analyze various protocols like TCP, UDP, IP, HTTP, FTP, SMTP, etc.
- **Preprocessors** – It has preprocessors for decoding HTTP, FTP and other protocols. Preprocessors extract useful info from the protocols before the rules engine analyzes the packets.
- **Logging and alerting** – It can log packets to the disk and generate alerts for malicious traffic.
- **Configuration** – It is highly configurable using the snort.conf file. Rules, preprocessors, outputs, etc can be configured.
- **Open source** – It is open source, free and frequently updated.

## Basic Steps for Deployment

- Download and install Snort on a Linux server.
- Configure the snort.conf file as per your needs. Configure rules, preprocessors, outputs, etc.
- Start Snort in sniffing mode to analyze network traffic.
- View the alerts and logs to detect any malicious activity.
- Update the rules regularly to keep up with the latest threats.
- Fine tune the configuration to reduce false positives.
- Investigate any detected attacks and take appropriate actions

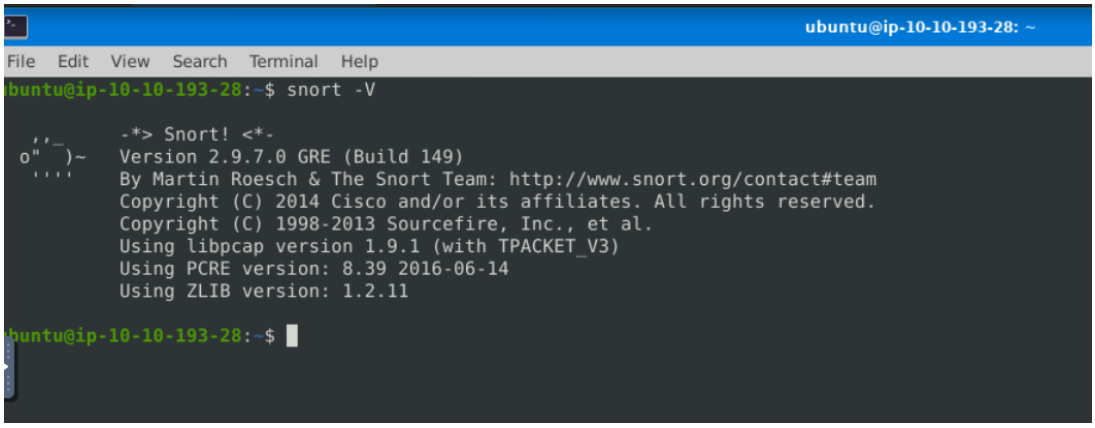
## Demonstration

SNORT can be configured to run in three modes:

- Sniffer mode
- Packet Logger mode
- Network Intrusion Detection System mode

## Steps of Operation (for all modes):

- To verify the installation

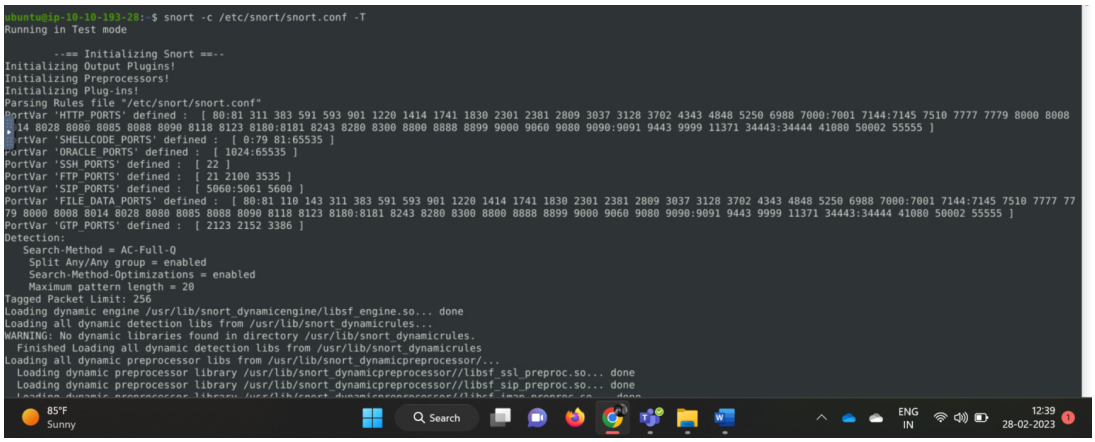


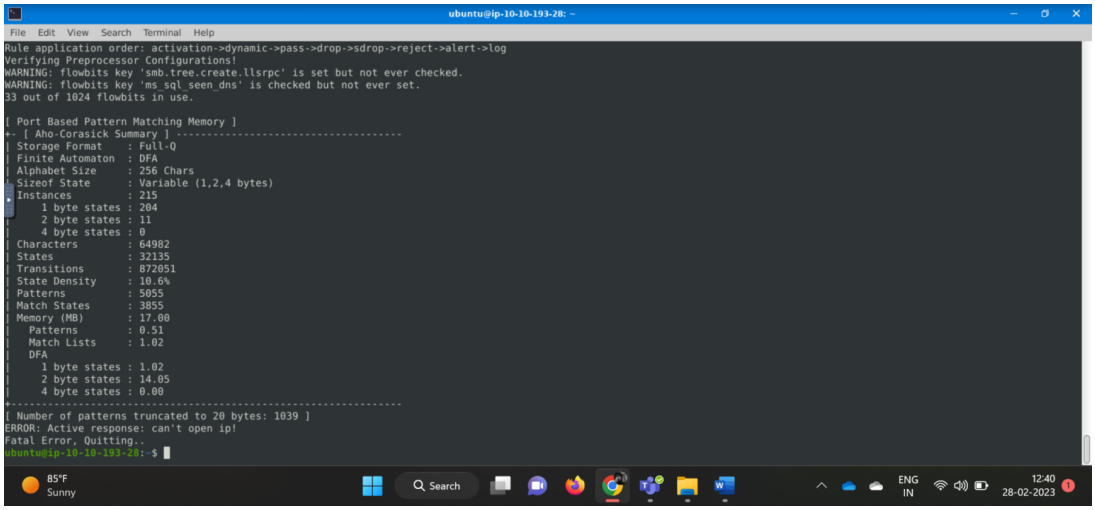

### Checking the Configuration Files are Valid

In Linux configuration files of snort are stored in **/etc/snort/snort.conf**.

Snort rules are written in a language called Snort Rules Language (SRL), which is similar to a programming language.

These rules define the conditions that must be met for Snort to generate an alert. Rules can be customized to fit the specific needs of an organization or network





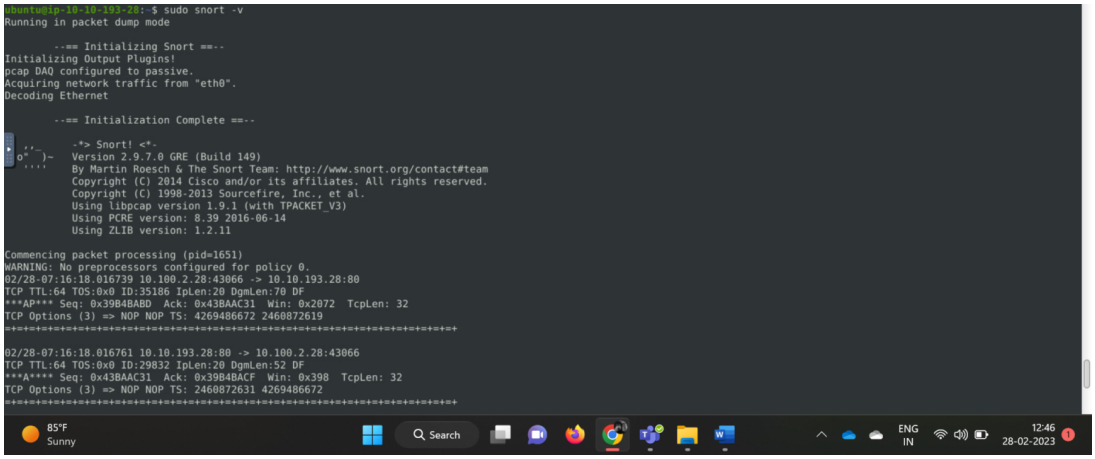

## Operation Mode 1: Sniffer Mode

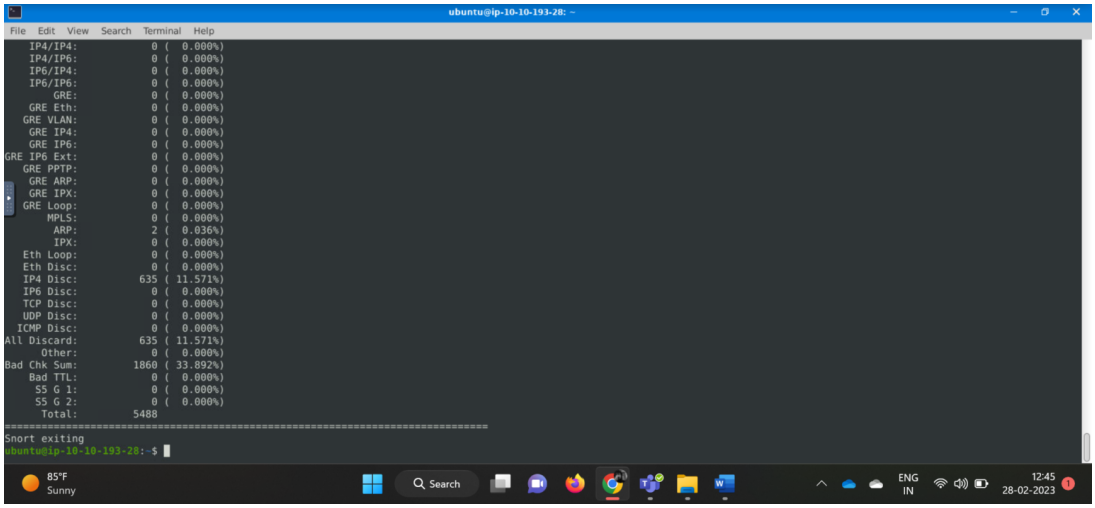
In Sniffer mode, it behaves like a network sniffer and captures packets passing through the network interface.

The tool displays the captured packets on the console or in a log file, allowing the user to analyze the network traffic.

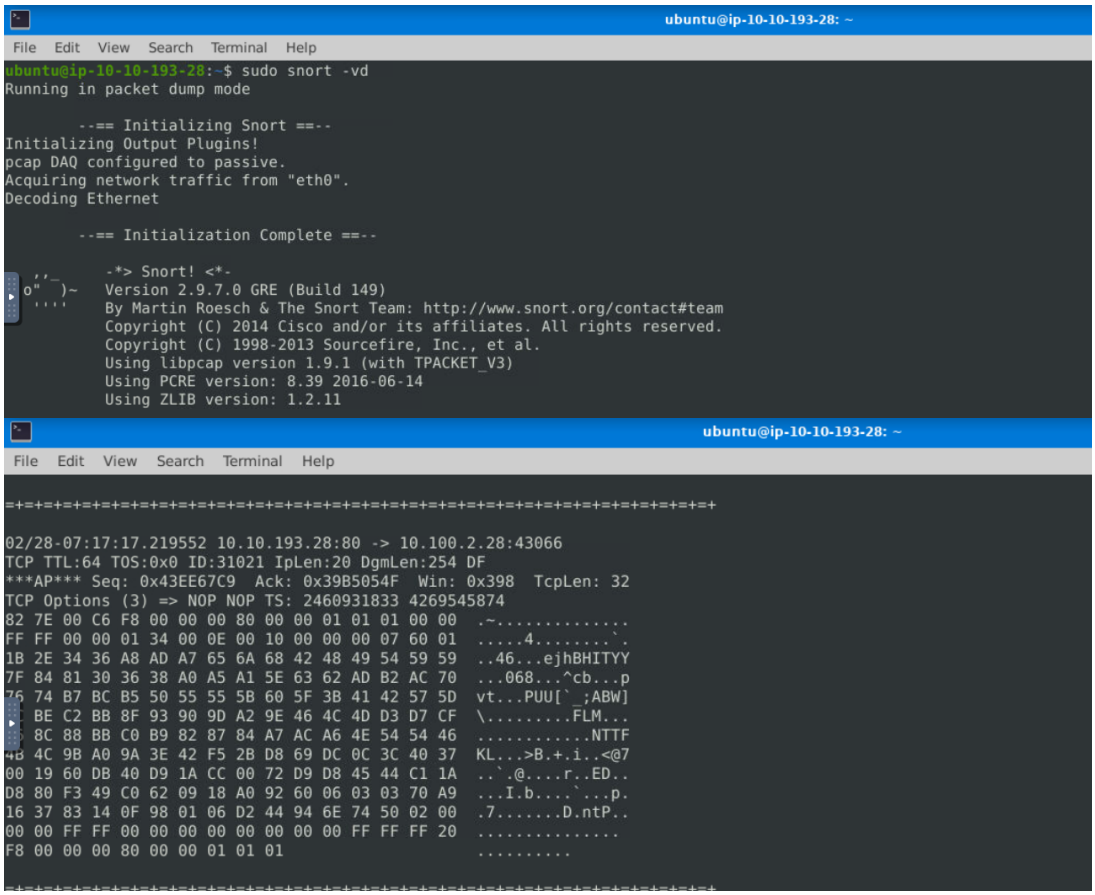
This mode can be useful for network troubleshooting and monitoring, but it does not provide any intrusion detection or prevention capabilities.

**`sudo snort -v`** : `Prints out the TCP/IP packets header on the screen`

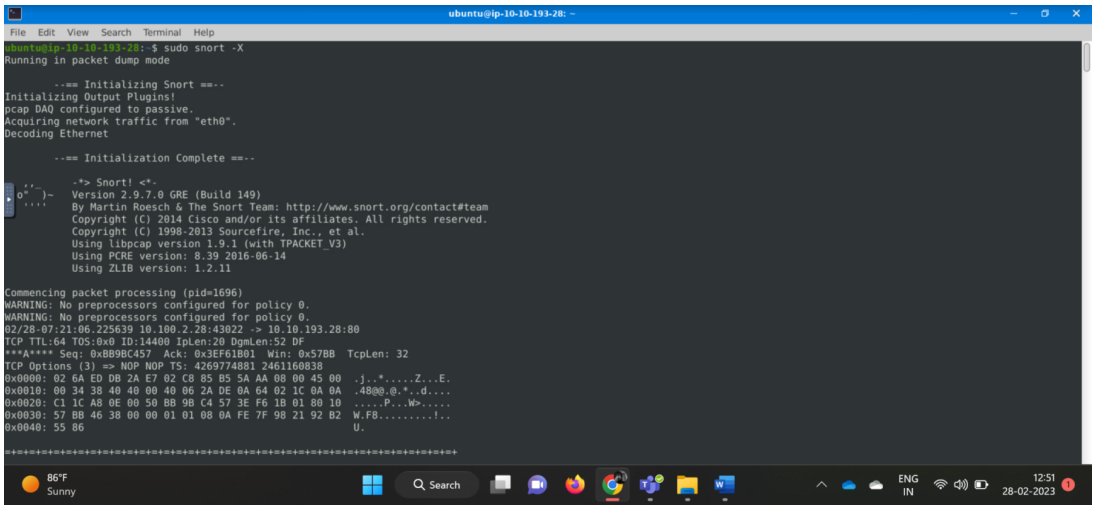





**sudo snort -vd** : shows the TCP/IP ICMP header with application data in transmit




**sudo snort -X** : Displays the full packet details in HEX.




## Operation Mode 2: Packet Logger Mode

In Packet Logger mode, the tool logs each packet that it captures to a file for later analysis. This mode can be useful for forensic analysis or for capturing packets for offline analysis.

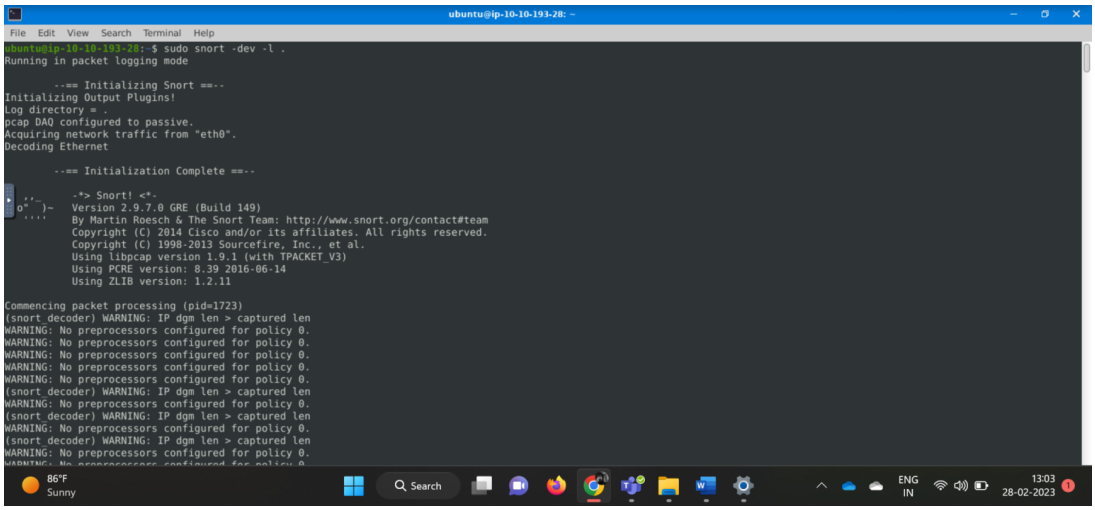
However, like Sniffer mode, it does not provide any intrusion detection or prevention capabilities.

**Parameter "-l" –** It enables the logger mode, target **log and alert** output directory. Default output folder is **/var/log/snort**. The default action is to dump as tcpdump format in **/var/log/snort.**

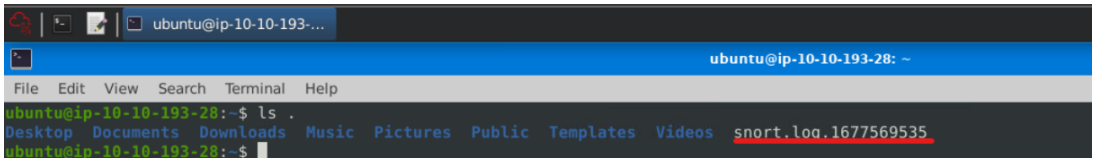
#### Starting SNORT in packet Logger Mode

```
sudo snort -dev -l .

//The "-l ."part of the command creates the logs in the current directory.
```



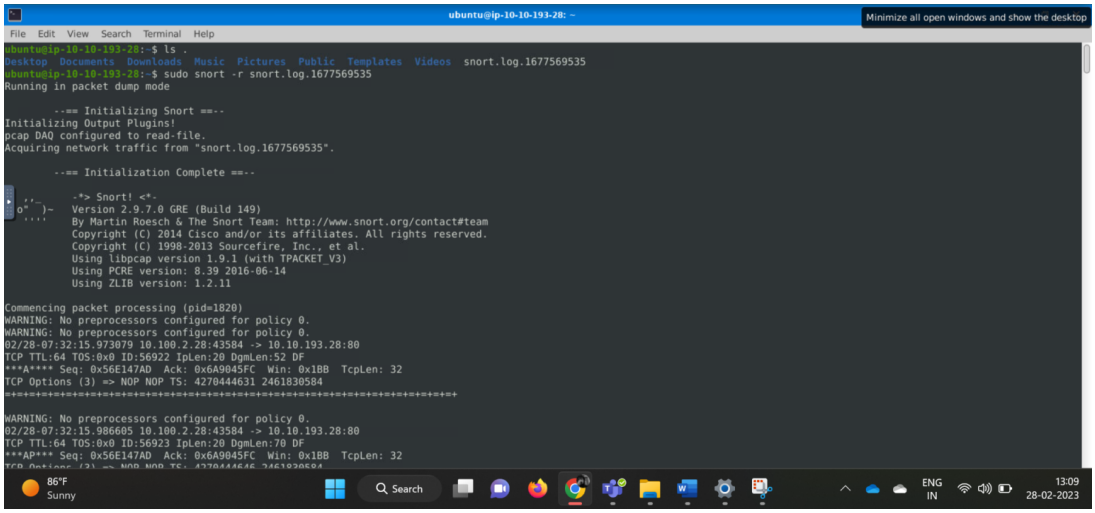

**–>** Log file is created of the captured traffic.




**–>** Next step is to read the log file generated using the command:

```
sudo snort -r <your_log_file_name>
```

```
// Here "-r" is Reading option to read the dumped logs in
Snort.
```

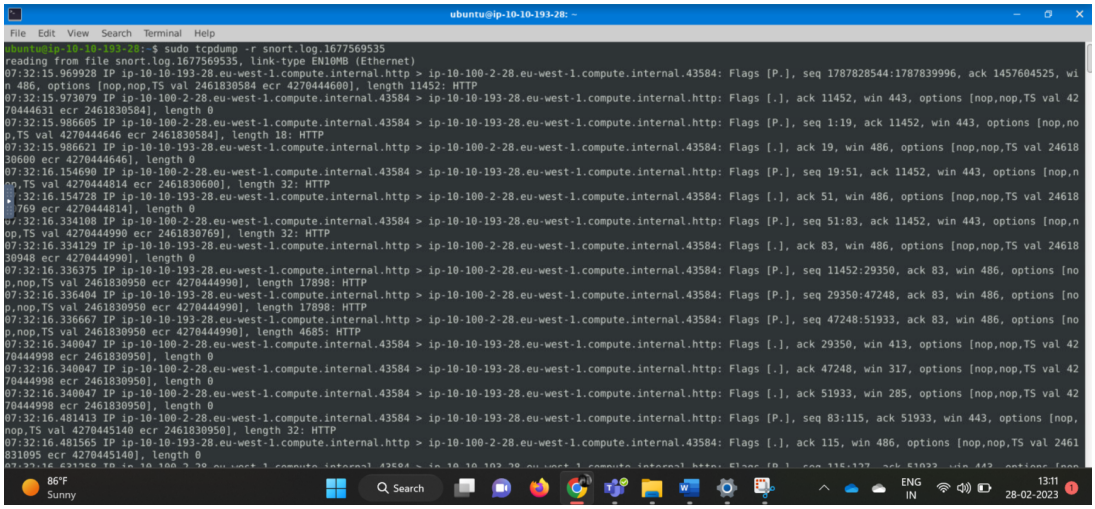



It can read and handle the binary like output.However, if we create logs with the "**-K ASCII**" parameter, or in laymen terms, in ASCII format, Snort will not read them.

Thus to open such log files tcpdump or wireshark is needed.

### Opening Log file with tcpdump

```
sudo tcpdump -r <log_file_name>
```



## Operation Mode 3: IDS/IPS

In Network Intrusion Detection mode, Snort analyzes network traffic in real-time and compares it against a set of rules.

When it detects a packet that matches a rule, it generates an alert, which can be sent to a console, a log file, or an external system such as an email server or a SIEM.

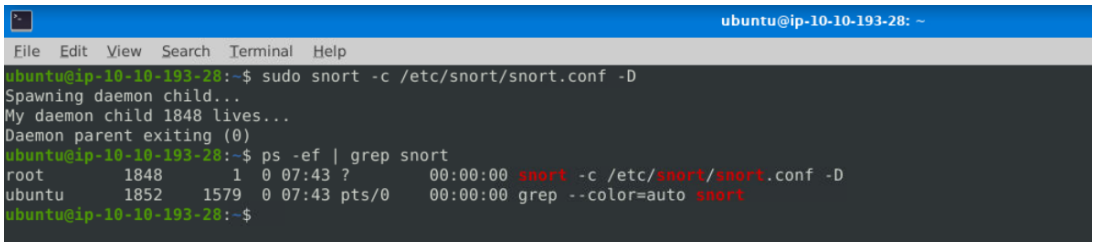
This mode provides real-time intrusion detection and prevention capabilities and is the primary mode of operation for Snort.

**Parameter "-D" –** This parameter is mainly used in scripts to start the Snort service in the background.

```
sudo snort -c /etc/snort/snort.conf -D

// -c : Used to define the comfiguration file
// -D: Background Mode.
```

Above command will start the snort instance in background and capture the traffic. Once the traffic is generated, snort will start processing the packets. Also the corresponding process can be checked with "**ps**".

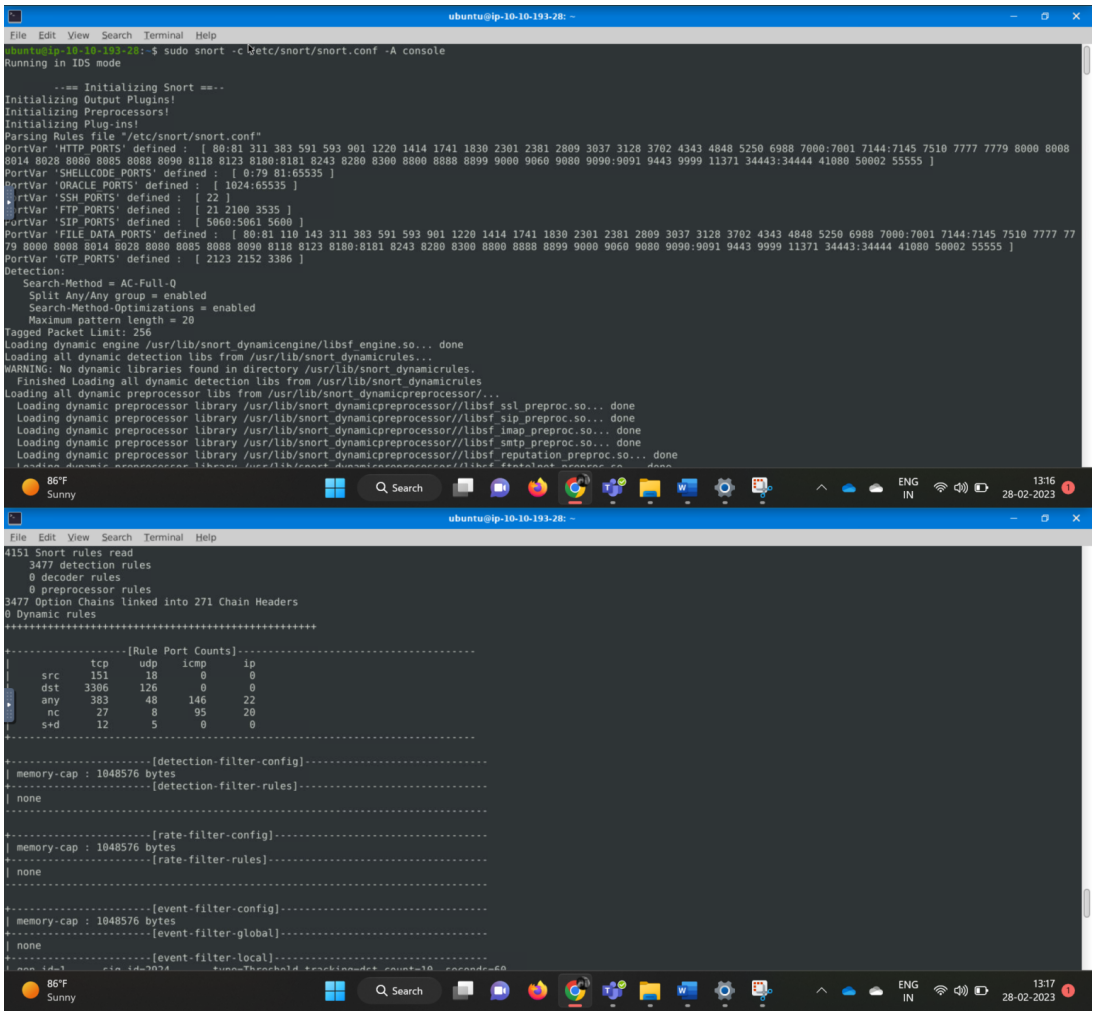



## Alert Modes in IDS/IPS

- **console** : displays alerts quickly on the console screen.
- **cmg** : provides basic header information and payload in hexadecimal and text format.
- **full** : provides all possible information about the alert.
  - **fast** : shows only essential information such as the alert message, timestamp, source and destination IP addresses, and port numbers.
- **none** : disables alerting altogether.

To use alert modes "**-A**" parameter is used. For example to use a console alert mode below command can be used.

```
sudo snort -c /etc/snort/snort.conf -A console
```




# Conclusion

Snort is a powerful IDS that can help detect and prevent security threats in network traffic. It offers a range of customization options and can be used in various modes of operation.

It can detect a variety of attacks and generate alerts, logs, and block offending traffic.

Snort is a signature-based IDS that can also perform anomaly detection and has three modes of operation, sniffer, packet, and IDS/IPS.

It is free and open-source software with a large user community and is a popular choice for organizations looking to enhance their network security.

This demonstration of the instruction detection using Snort tool can be done using Windows operating system too.

**Please consider following and supporting us to stay updated with the latest info**

**Tamil S**

*http://kalilinuxtutorials.com*

Tamil has a great interest in the fields of Cyber Security, OSINT, and CTF projects. Currently, he is deeply involved in researching and publishing various security tools with Kali Linux Tutorials, which is quite fascinating.