**Cryptography And Network Security Lab**

**PRN No: 2019BTECS00038**

**Batch: B2**

**Assignment: 13**

**Title of assignment****: Installation and Configuration of Snort Application an Intrusion Detection System**

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

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

**Objectives:**

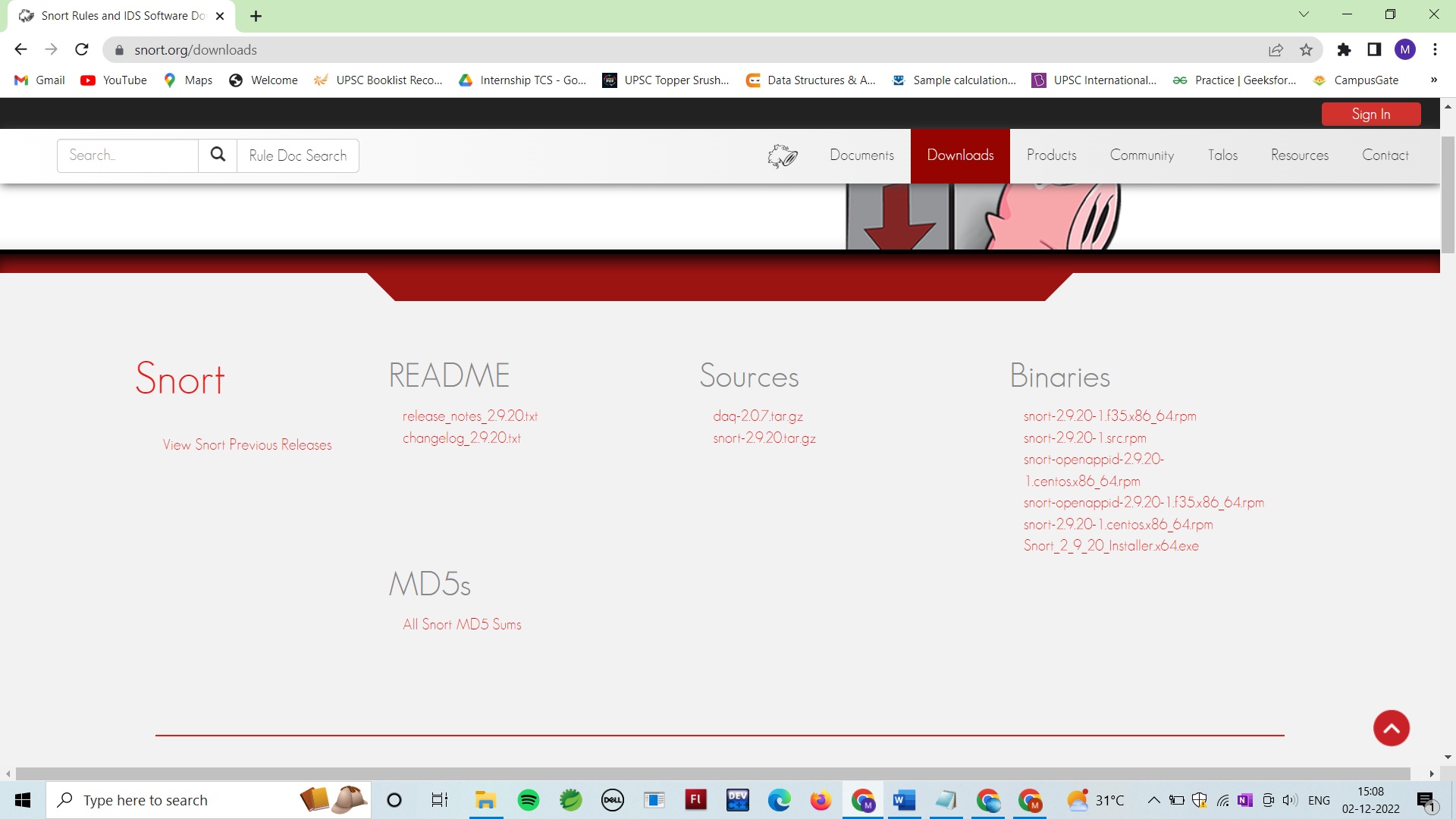
* To install snort ids
* To configure snort ids

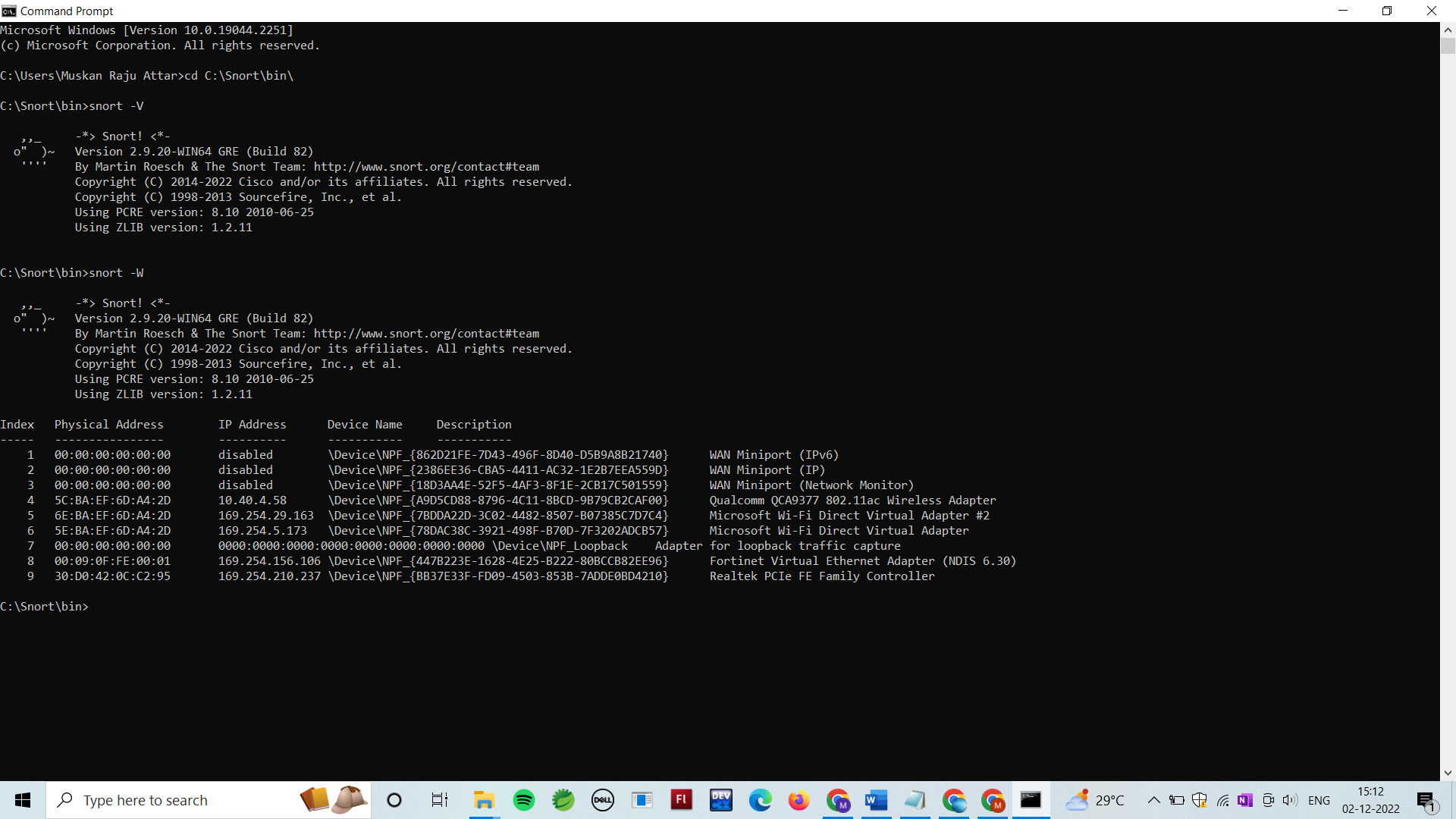
**Theory:**

Snort is the foremost Open Source Intrusion Prevention System (IPS) in the world. Snort IPS uses a series of rules that help define malicious network activity and uses those rules to find packets that match against them and generates alerts for users.

Snort can be deployed inline to stop these packets, as well. Snort has three primary uses: As a packet sniffer like tcpdump, as a packet logger — which is useful for network traffic debugging, or it can be used as a full-blown network intrusion prevention system. Snort can be downloaded and configured for personal and business use alike.

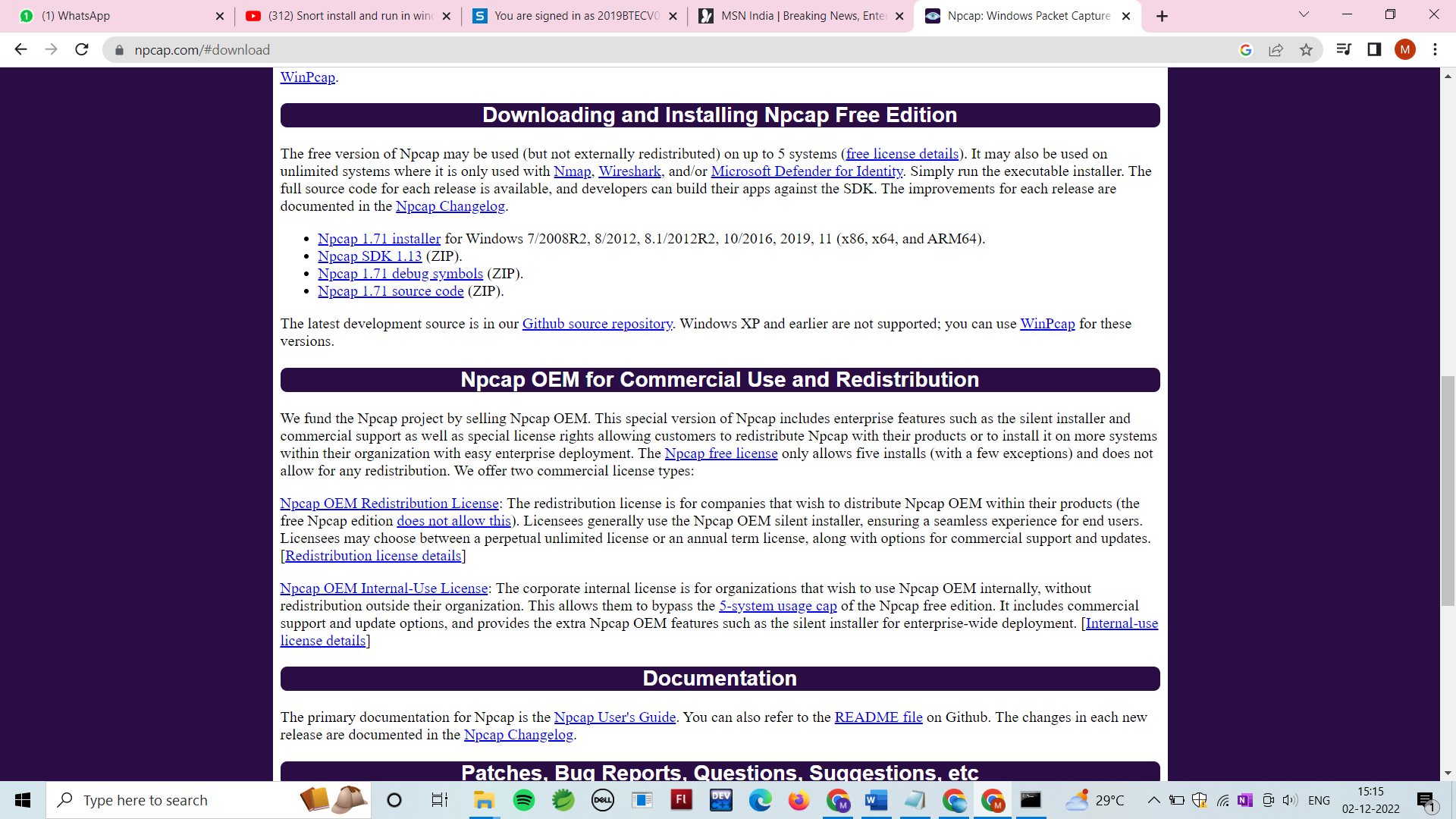
Snort installation:



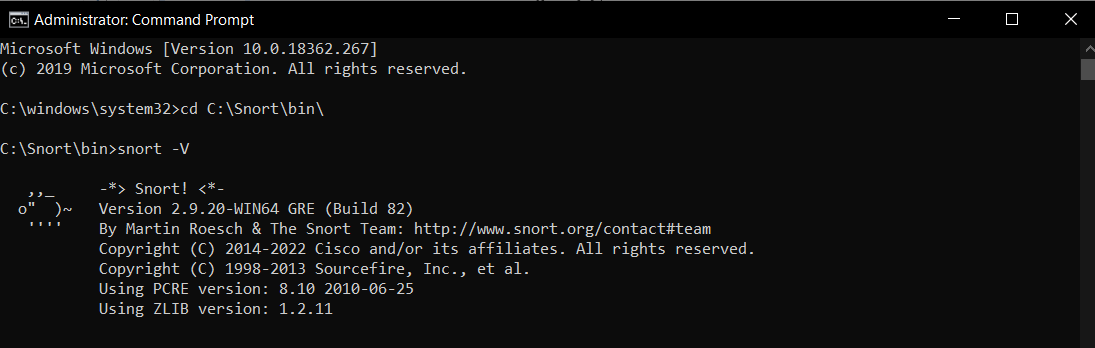


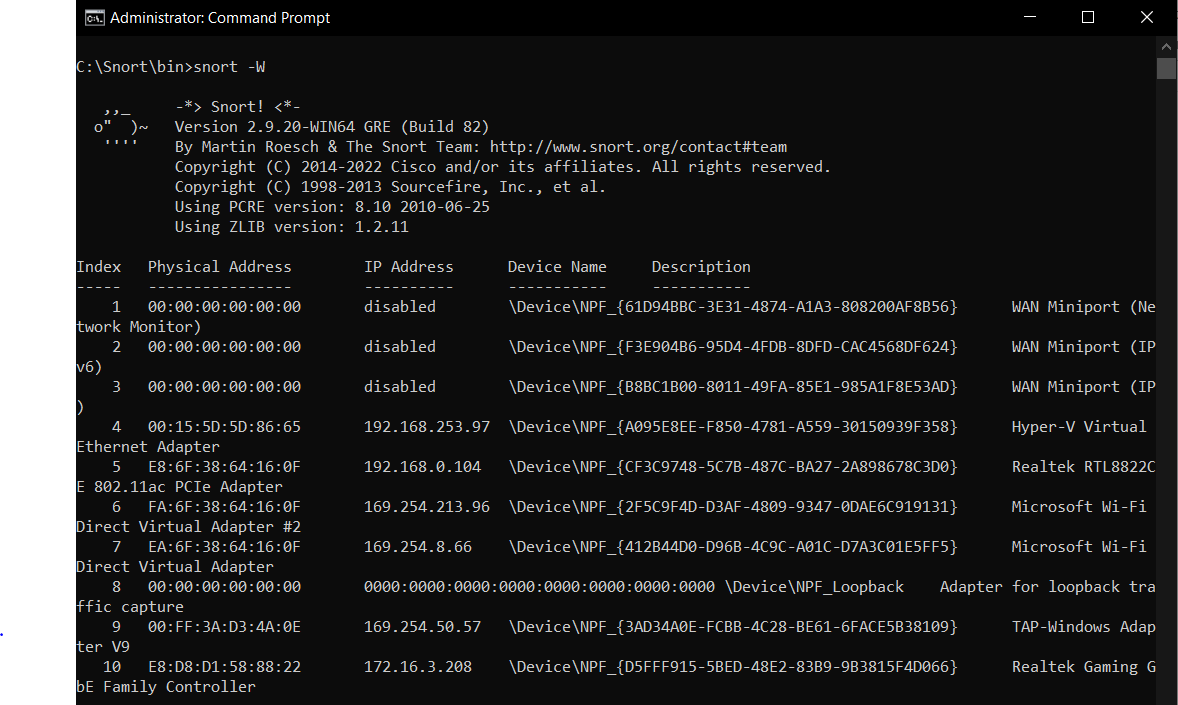
Downloading and Installing Npcap:

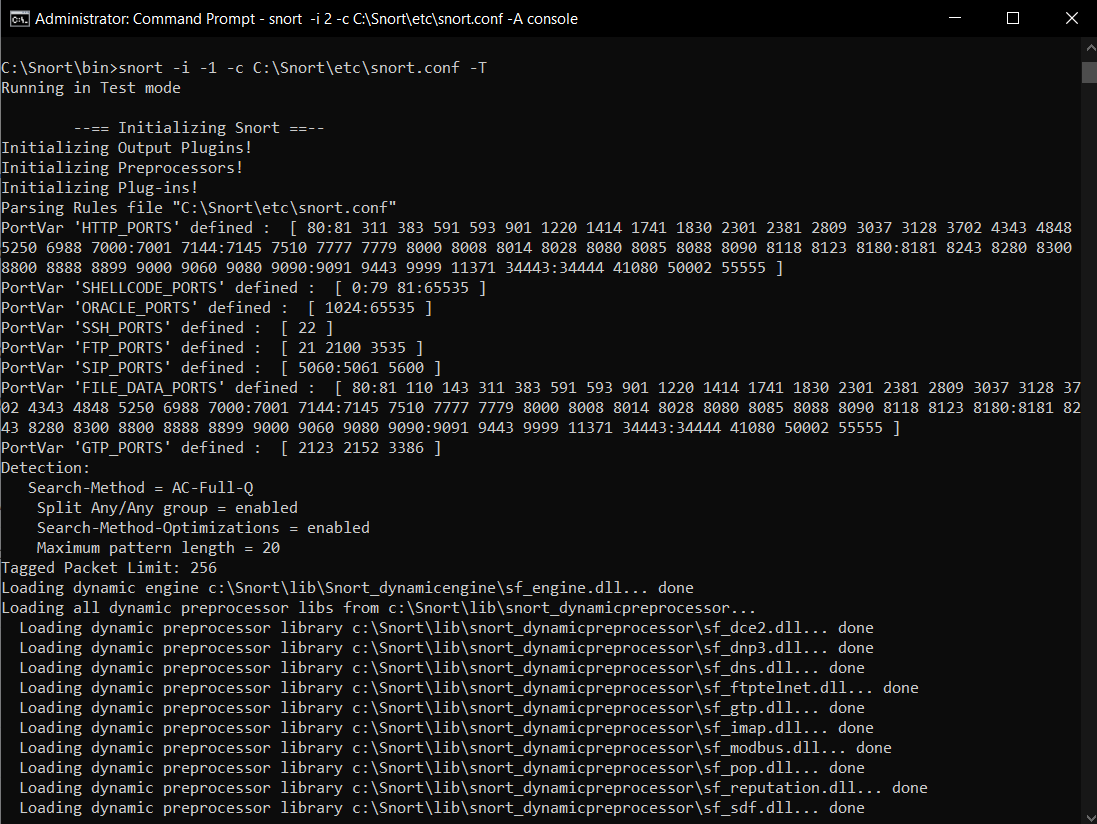
Npcap is the Nmap Project's packet capture (and sending) library for Microsoft Windows.

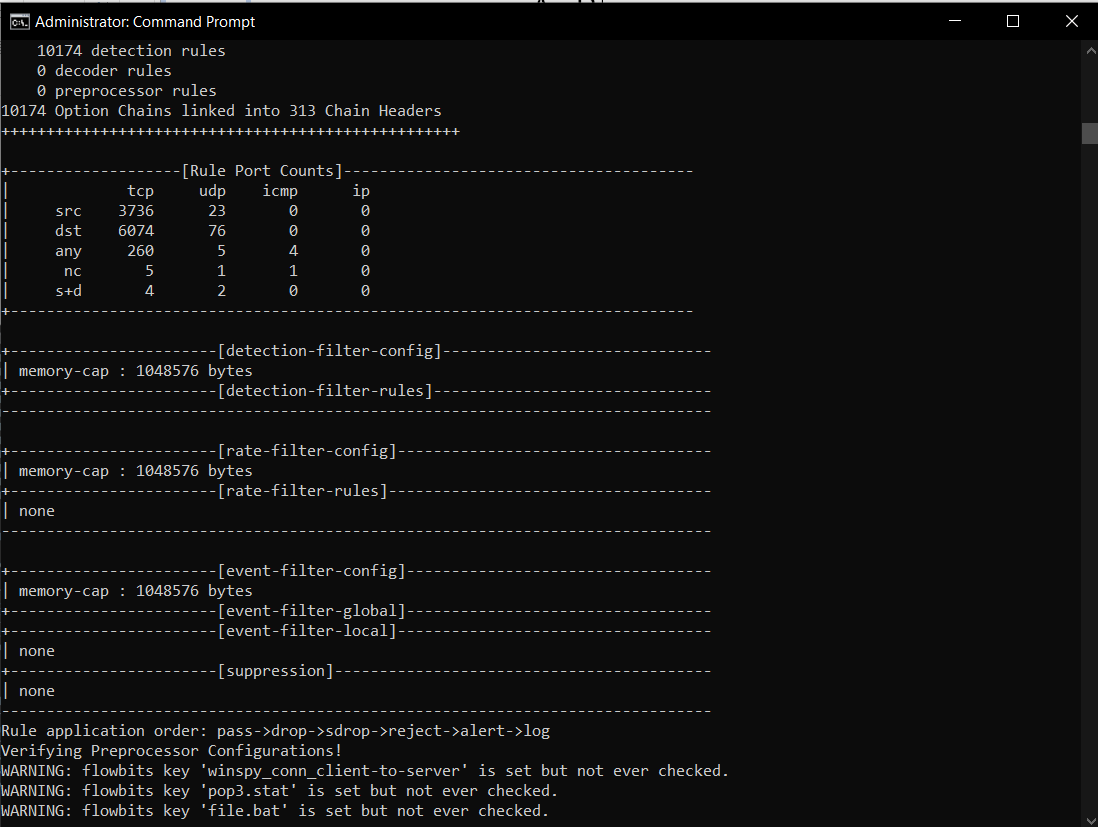


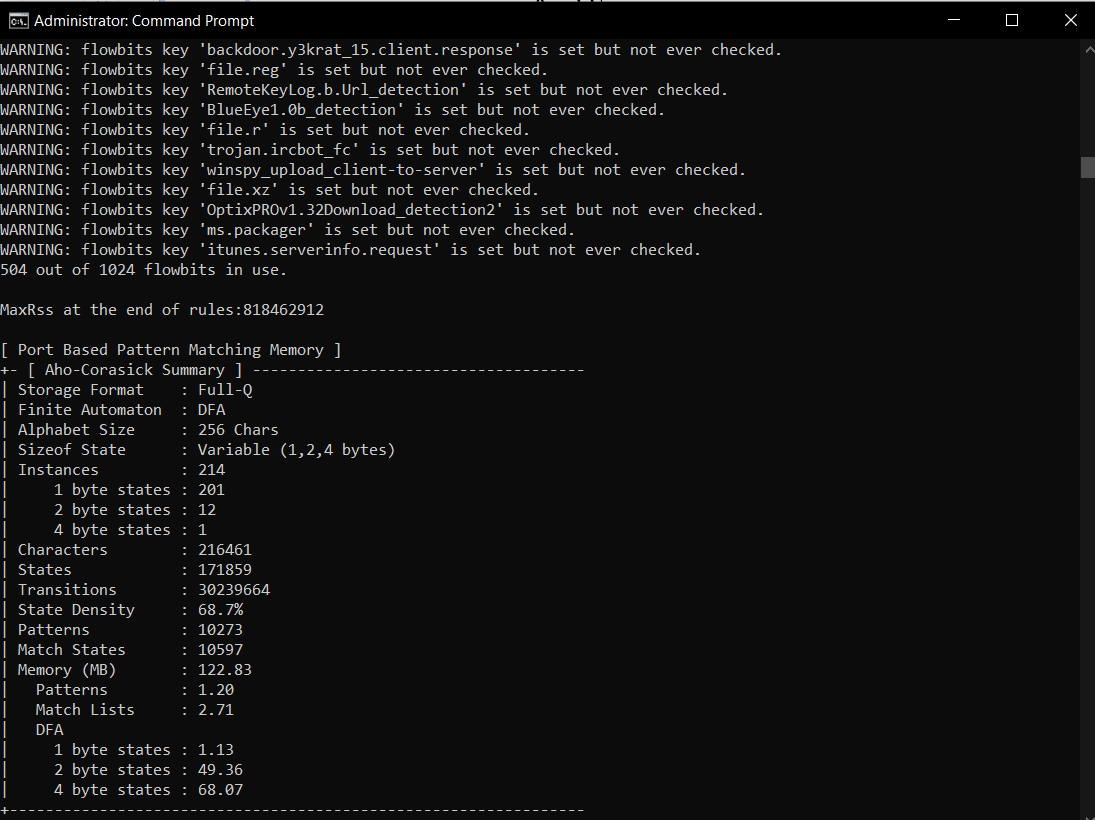
Snort Configuration :

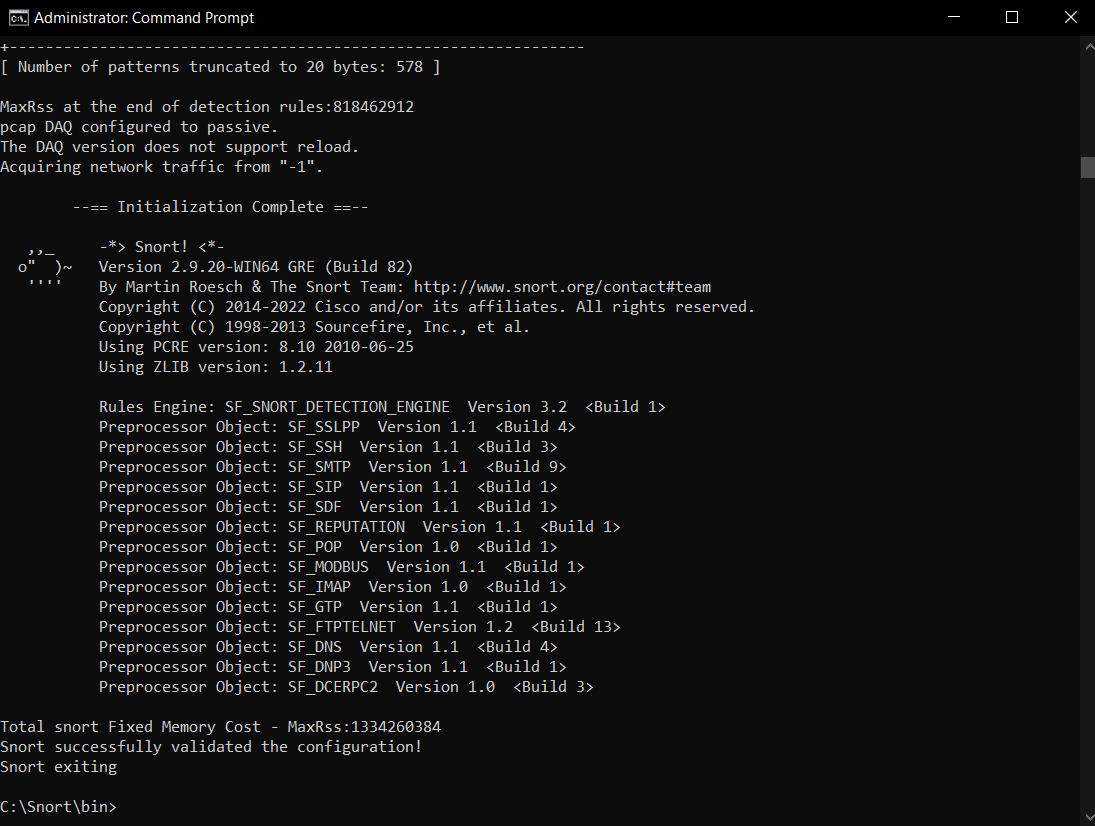












**Conclusion:**

Successfully installed and configured IDS in system.