**Final Year B. Tech., Sem VII 2022-23**

**Cryptography And Network Security Lab**

**Assignment submission**

**PRN No: 2019BTECS00022**

**Full name: Prachi R. Chobhare**

**Batch: B6**

**Assignment: 15**

**Title of assignment: Implementation of IDS- Intrusion Detection System**

**Title:**

Implementation of IDS- Intrusion Detection System.

**Aim:**

In this lab we will explore the Snort IDS. This is a signature based intrusion detection system used to detect network attacks. Snort can also be used as a simple packet logger, however we won't be doing that in this lab. Snort has multiple modes of operation, for the lab we will use snort as a packet sniffer, not inline.

**Theory:**

* An **Intrusion Detection System (IDS)** is a system that monitors **network traffic** for suspicious activity and issues alerts when such activity is discovered. It is a software application that scans a network or a system for the harmful activity or policy breaching. Any malicious venture or violation is normally reported either to an administrator or collected centrally using a security information and event management (SIEM) system. A SIEM system integrates outputs from multiple sources and uses alarm filtering techniques to differentiate malicious activity from false alarms.
* Although intrusion detection systems monitor networks for potentially malicious activity, they are also disposed to false alarms. Hence, organizations need to fine-tune their IDS products when they first install them. It means properly setting up the intrusion detection systems to recognize what normal traffic on the network looks like as compared to malicious activity.
* Intrusion prevention systems also monitor network packets inbound the system to check the malicious activities involved in it and at once send the warning notifications.

**Detection Method of IDS:**

* **Signature-based Method:**  
  Signature-based IDS detects the attacks on the basis of the specific patterns such as number of bytes or number of 1’s or number of 0’s in the network traffic. It also detects on the basis of the already known malicious instruction sequence that is used by the malware. The detected patterns in the IDS are known as signatures.

Signature-based IDS can easily detect the attacks whose pattern (signature) already exists in system but it is quite difficult to detect the new malware attacks as their pattern (signature) is not known.

* **Anomaly-based Method:**  
  Anomaly-based IDS was introduced to detect unknown malware attacks as new malware are developed rapidly. In anomaly-based IDS there is use of machine learning to create a trustful activity model and anything coming is compared with that model and it is declared suspicious if it is not found in model. Machine learning-based method has a better-generalized property in comparison to signature-based IDS as these models can be trained according to the applications and hardware configurations.

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.

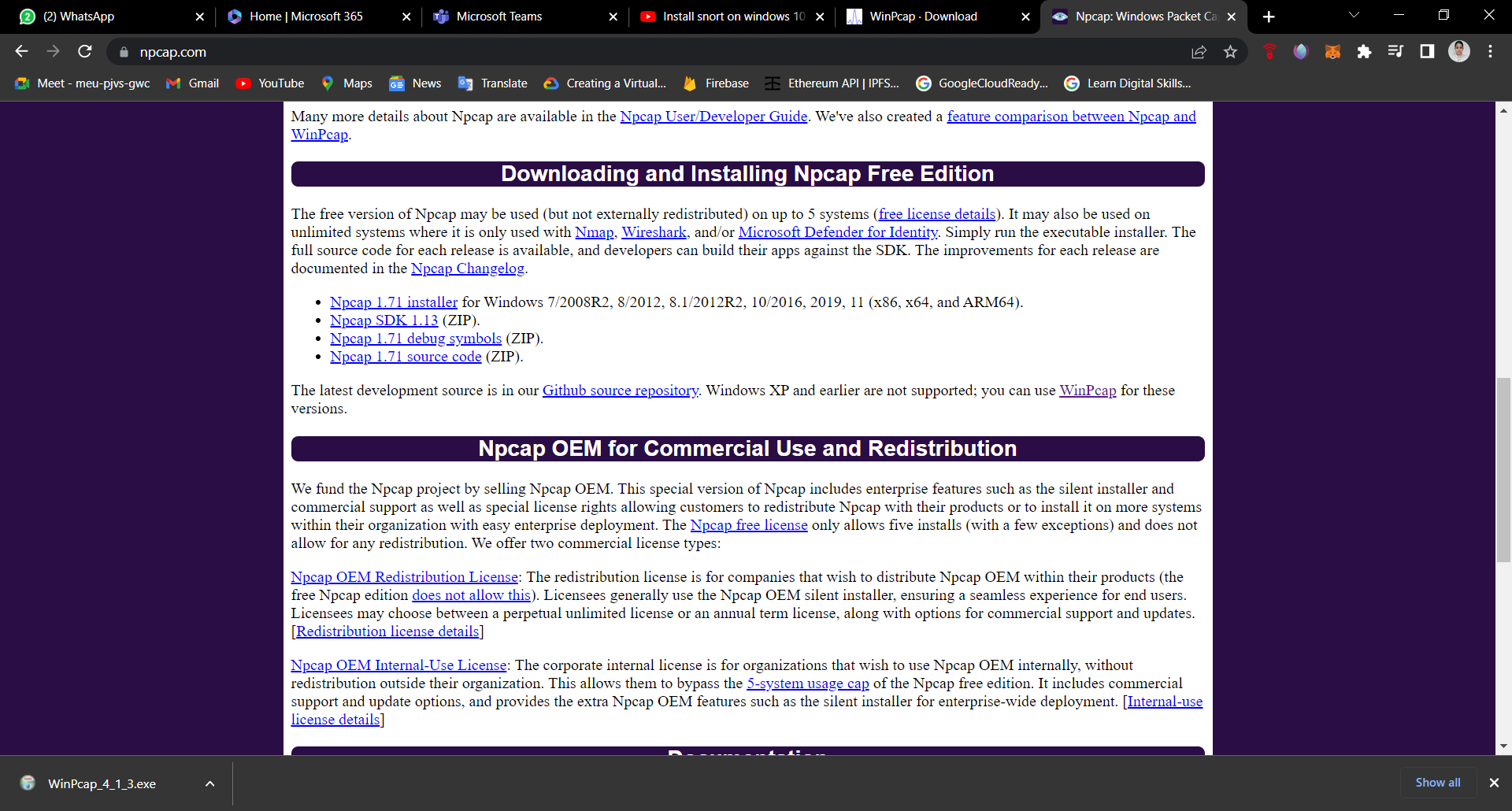
**Snaps of Installations:**

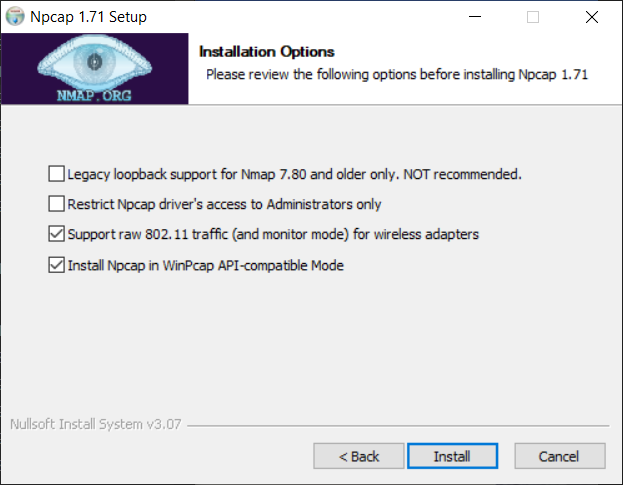
1. **Wincap**

****

**But I have already downloaded this software with Wireshark so the installation part is skipped.**

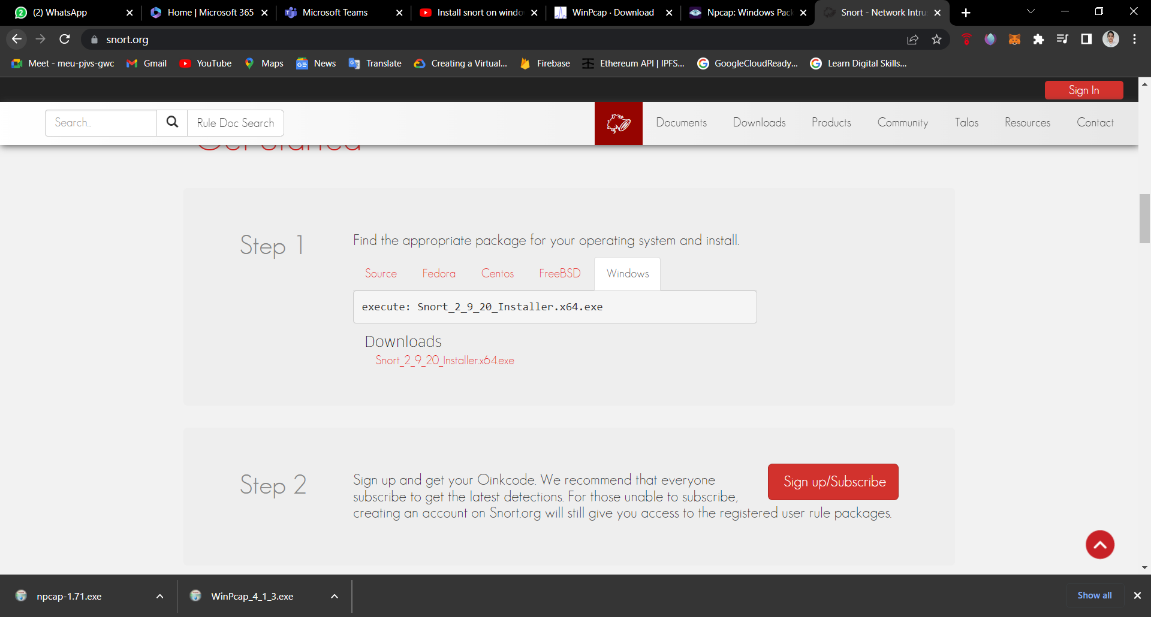
1. **Npcap**

****

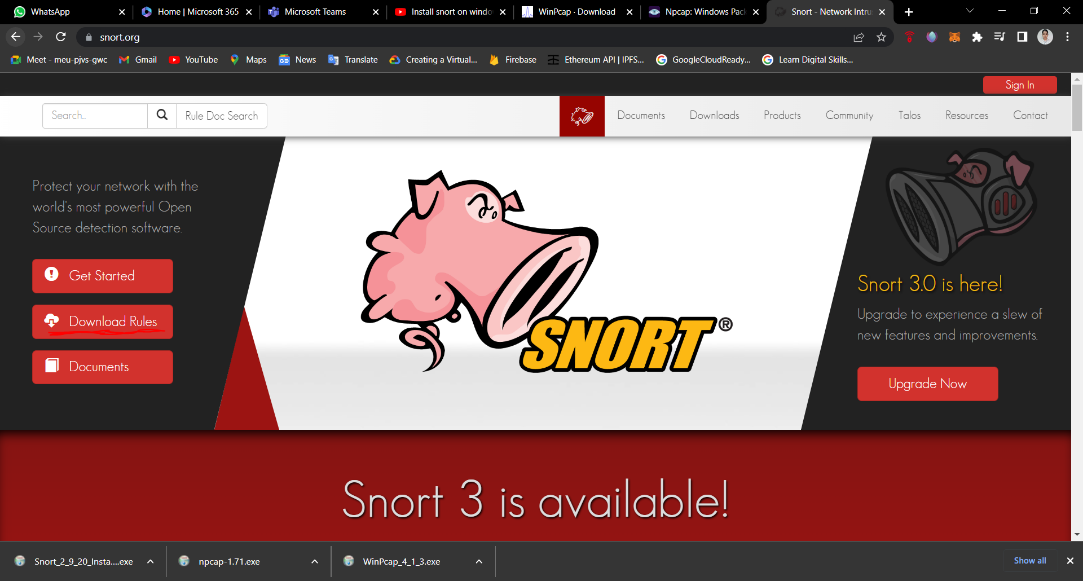
****

1. **Snort and Snort Rules :**

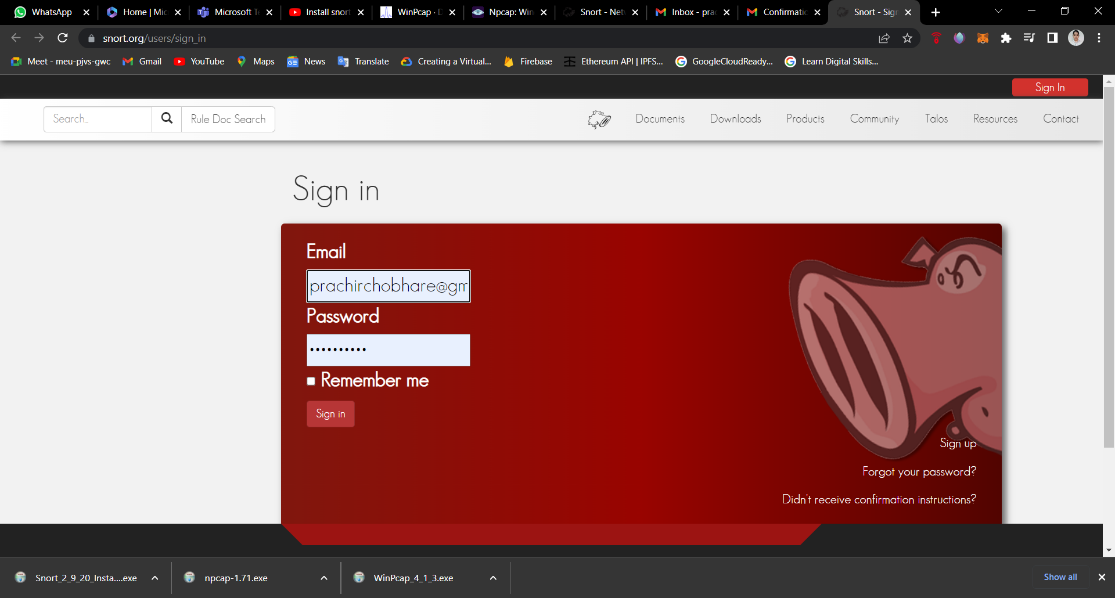
**Download via link**



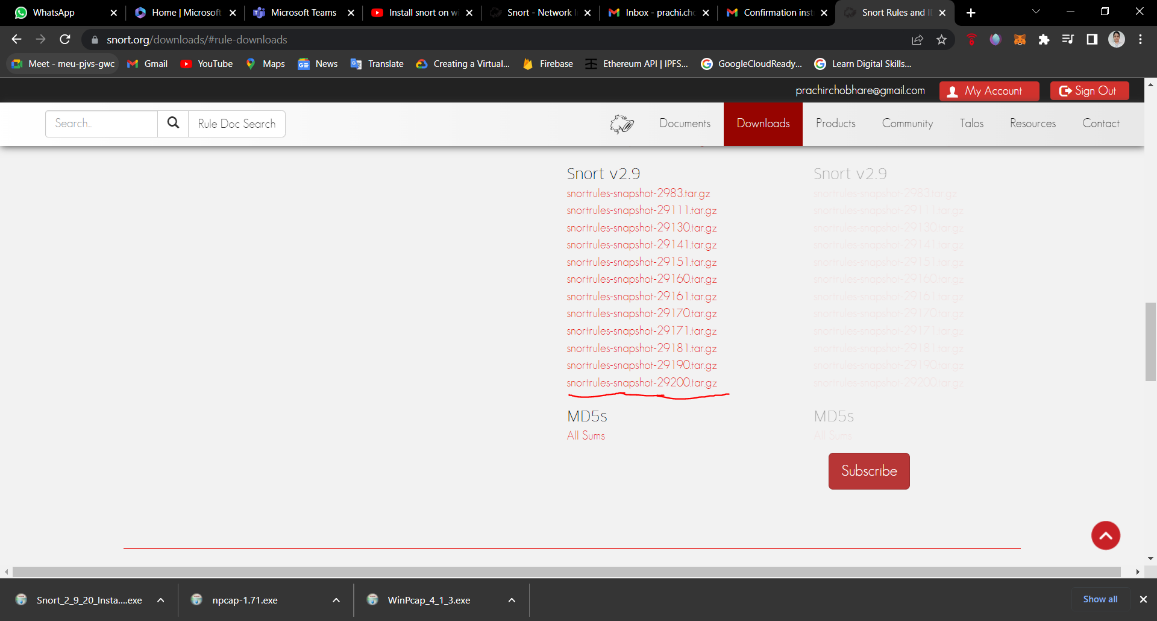
Download snort rules by checking download rule button…



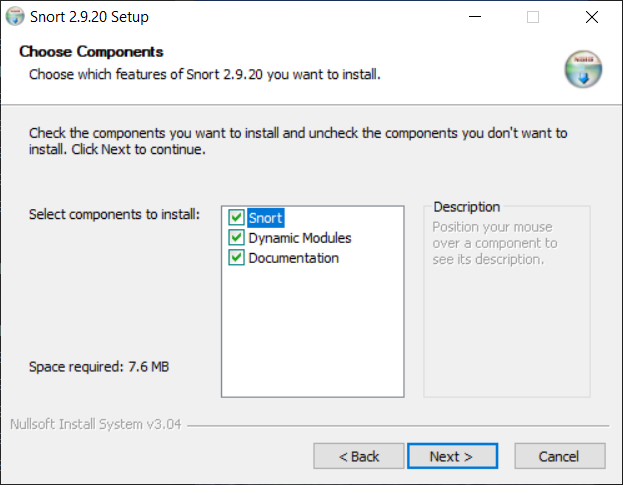
But We need to sign up for rules file. So, after registered you got mail open the link and download rules….

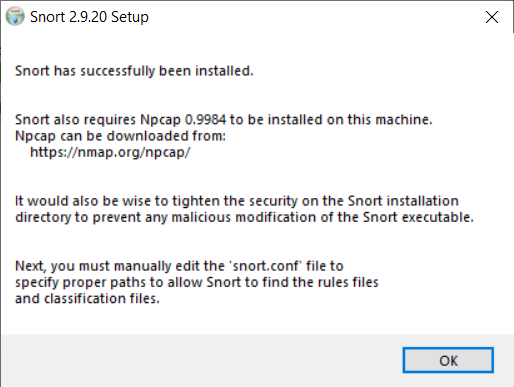


Now, download marked version of rules zipfile.

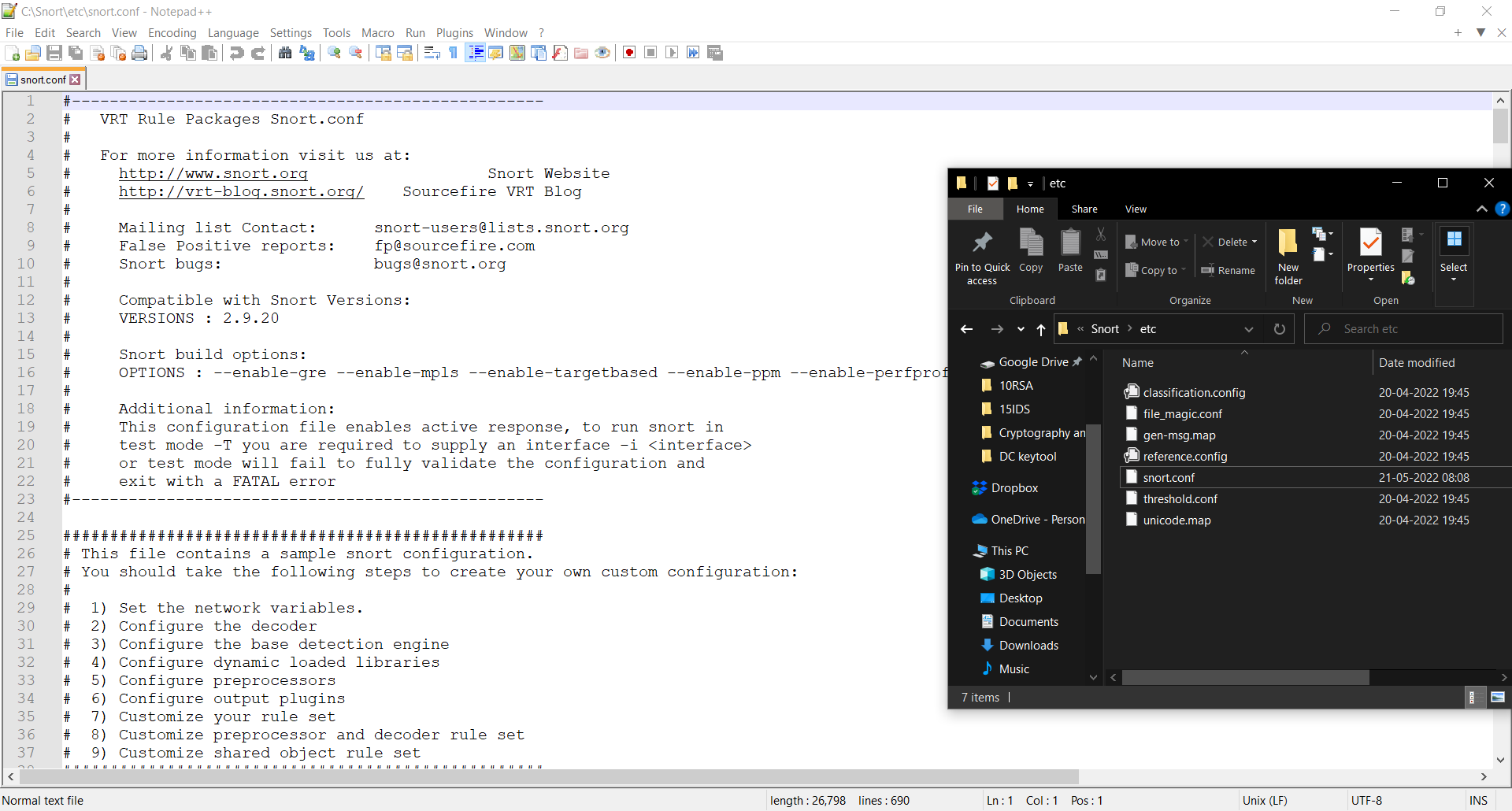


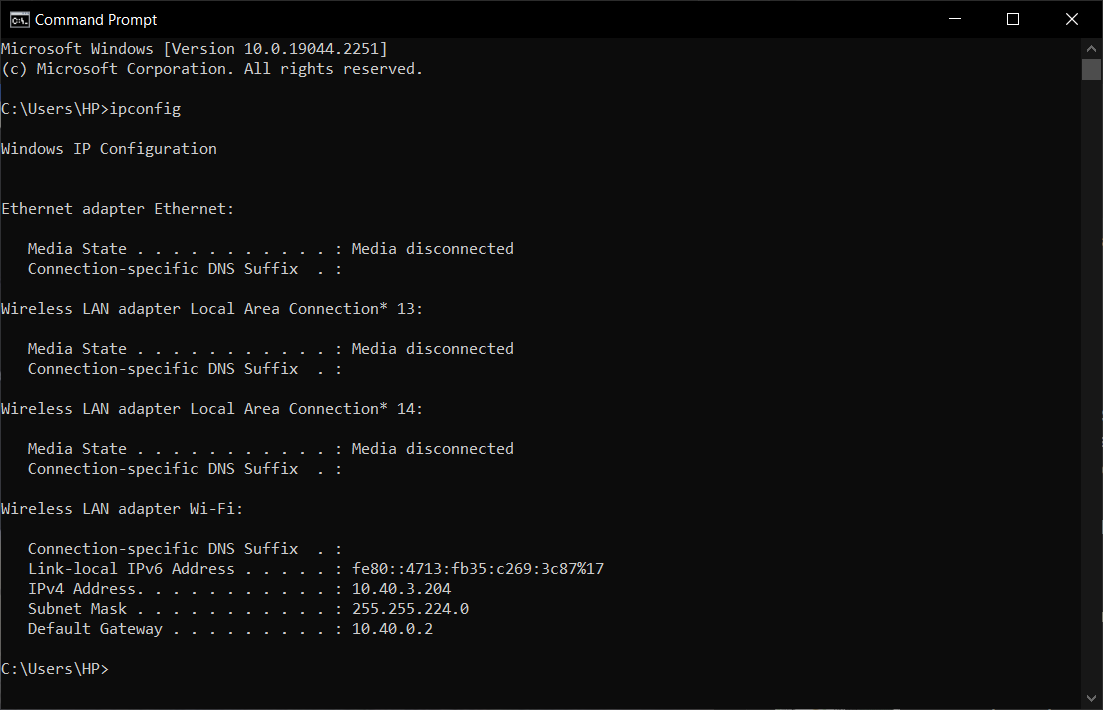
Installation in PC

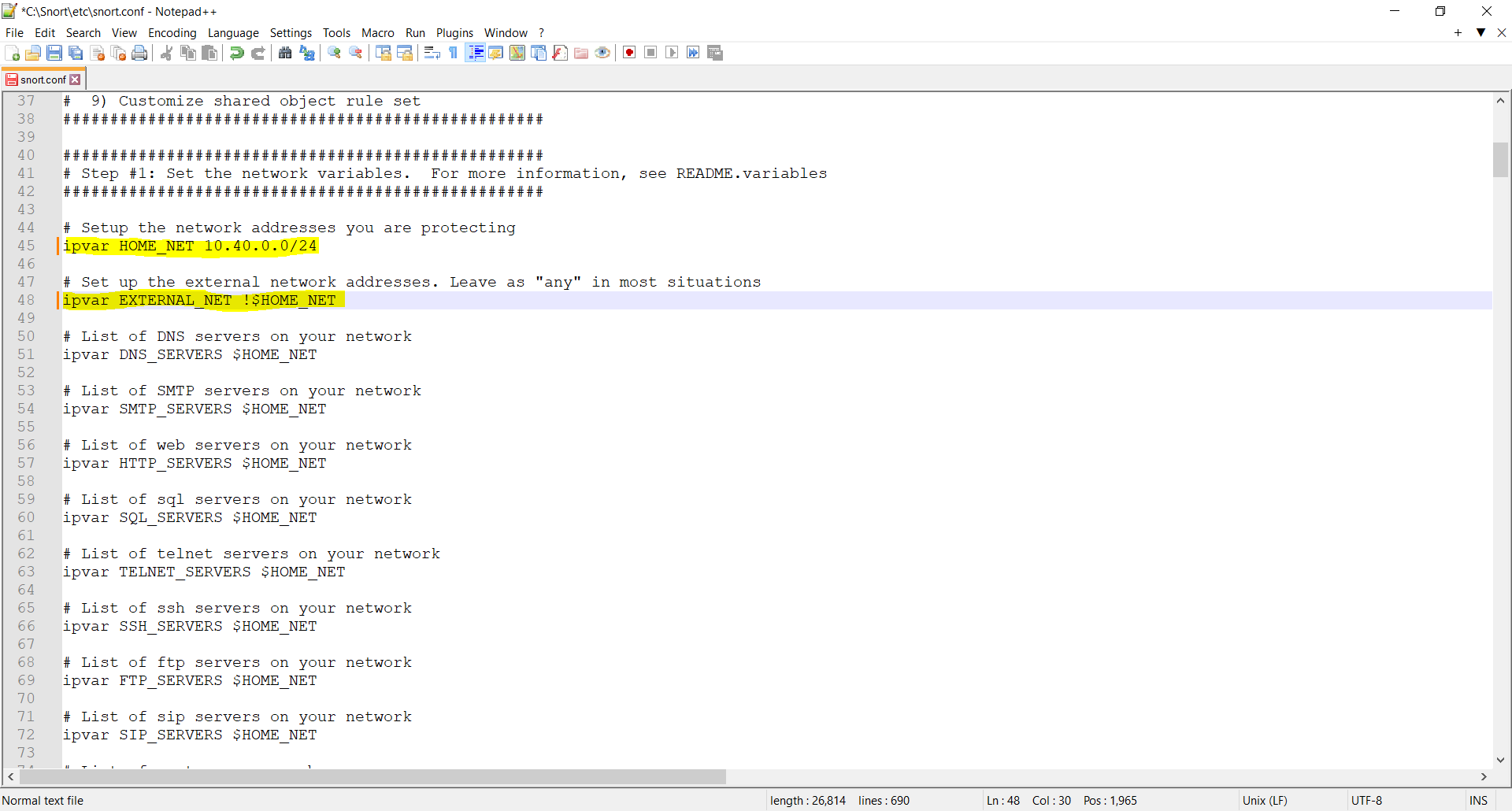


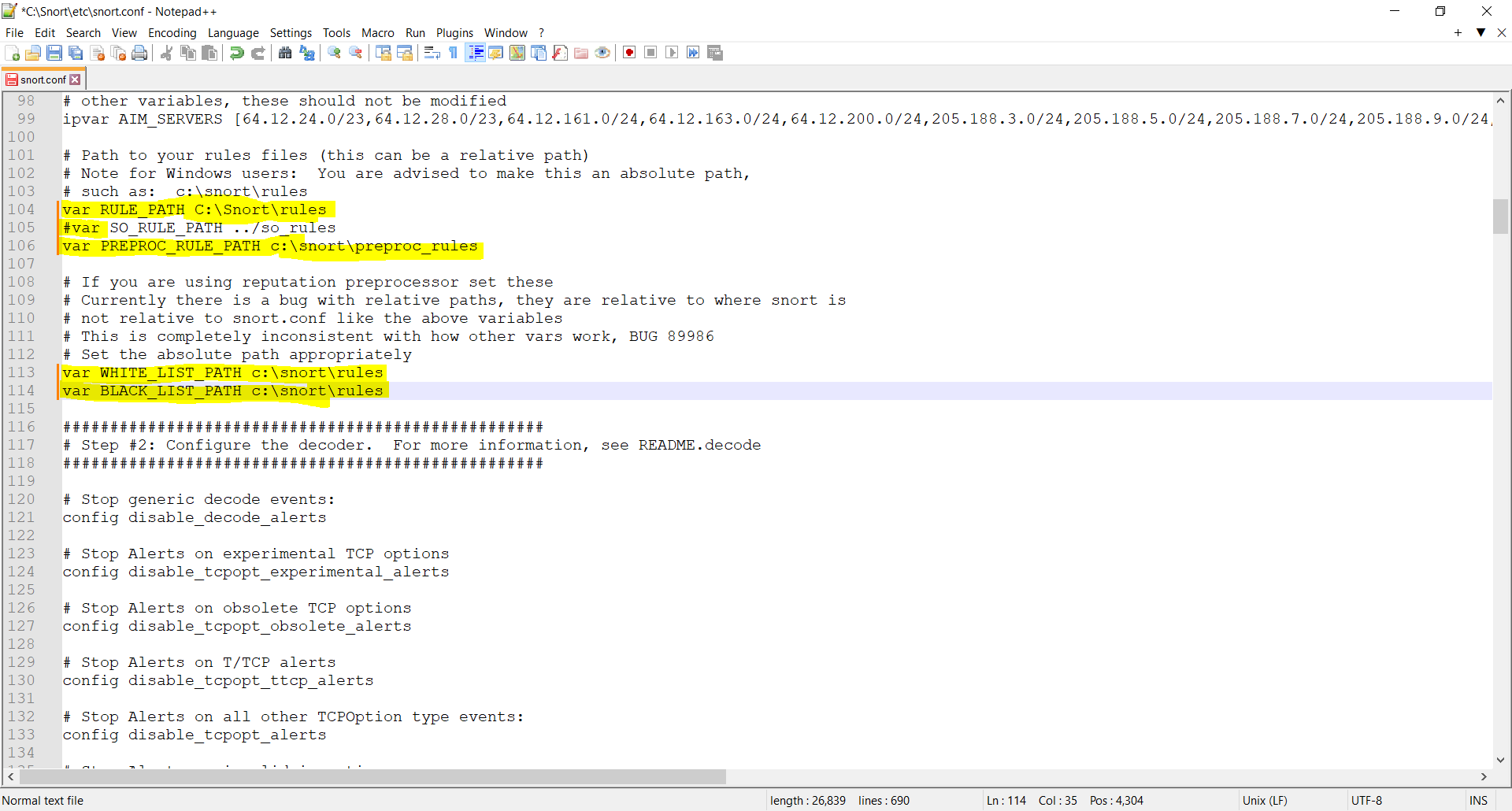


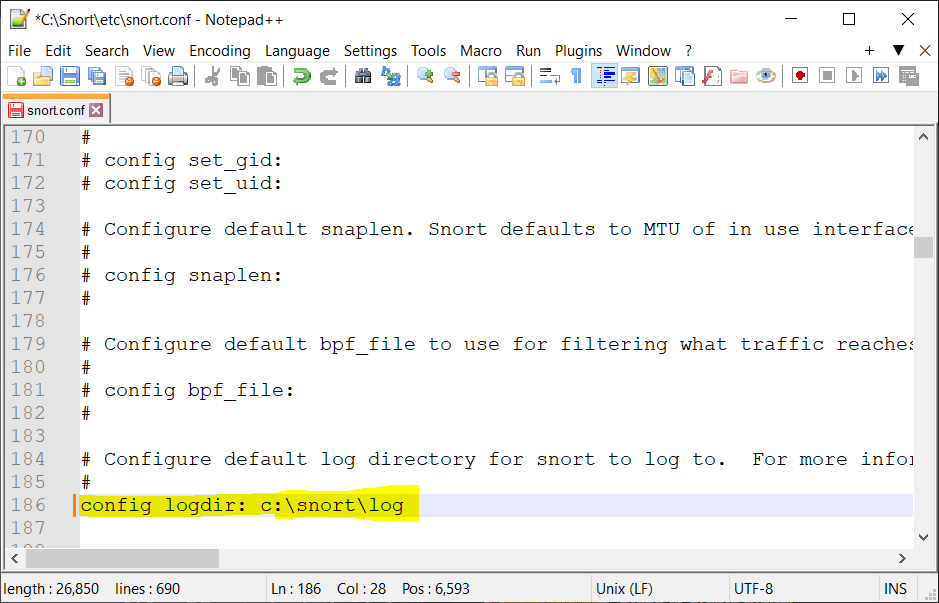
**Configuration of Rules:**

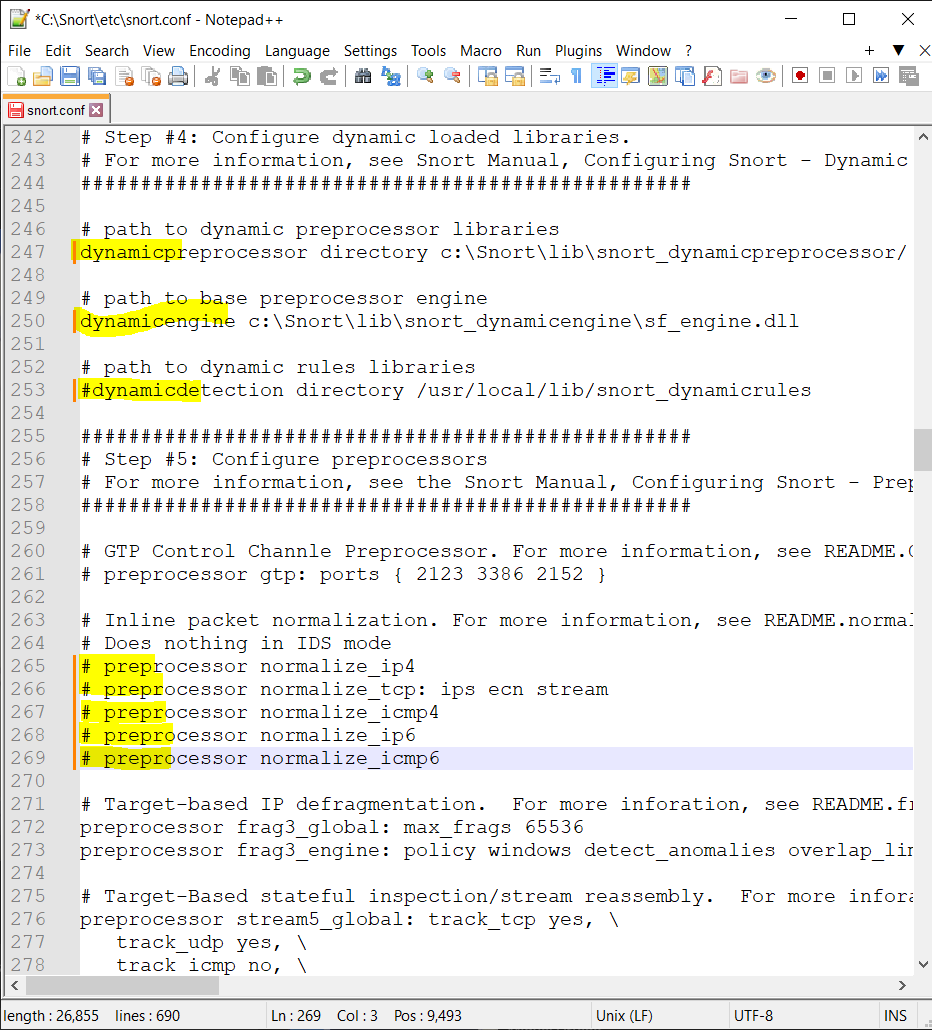
****

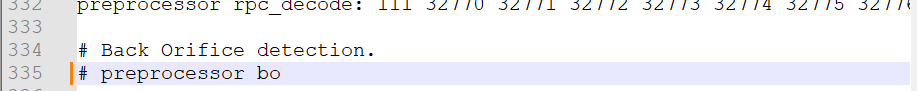


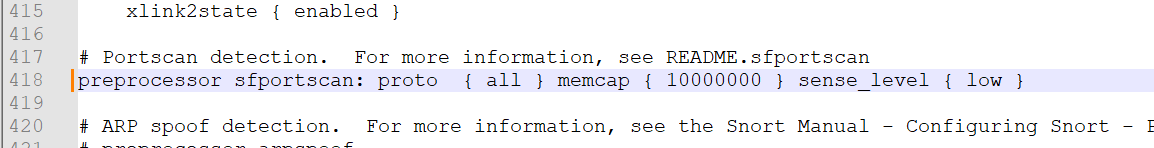




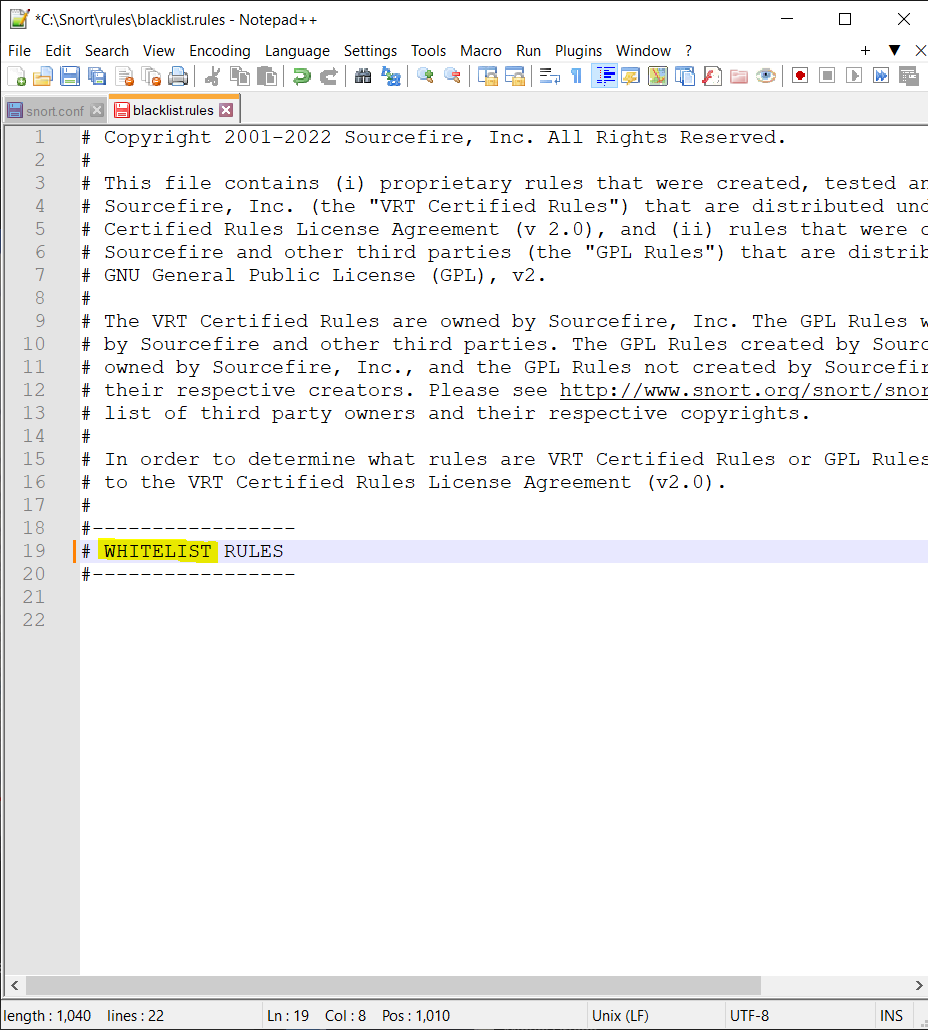


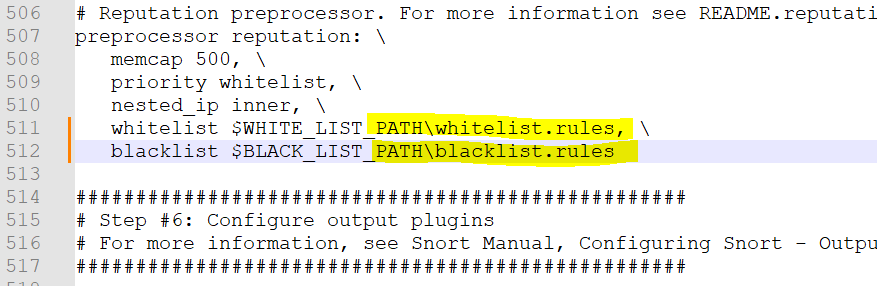


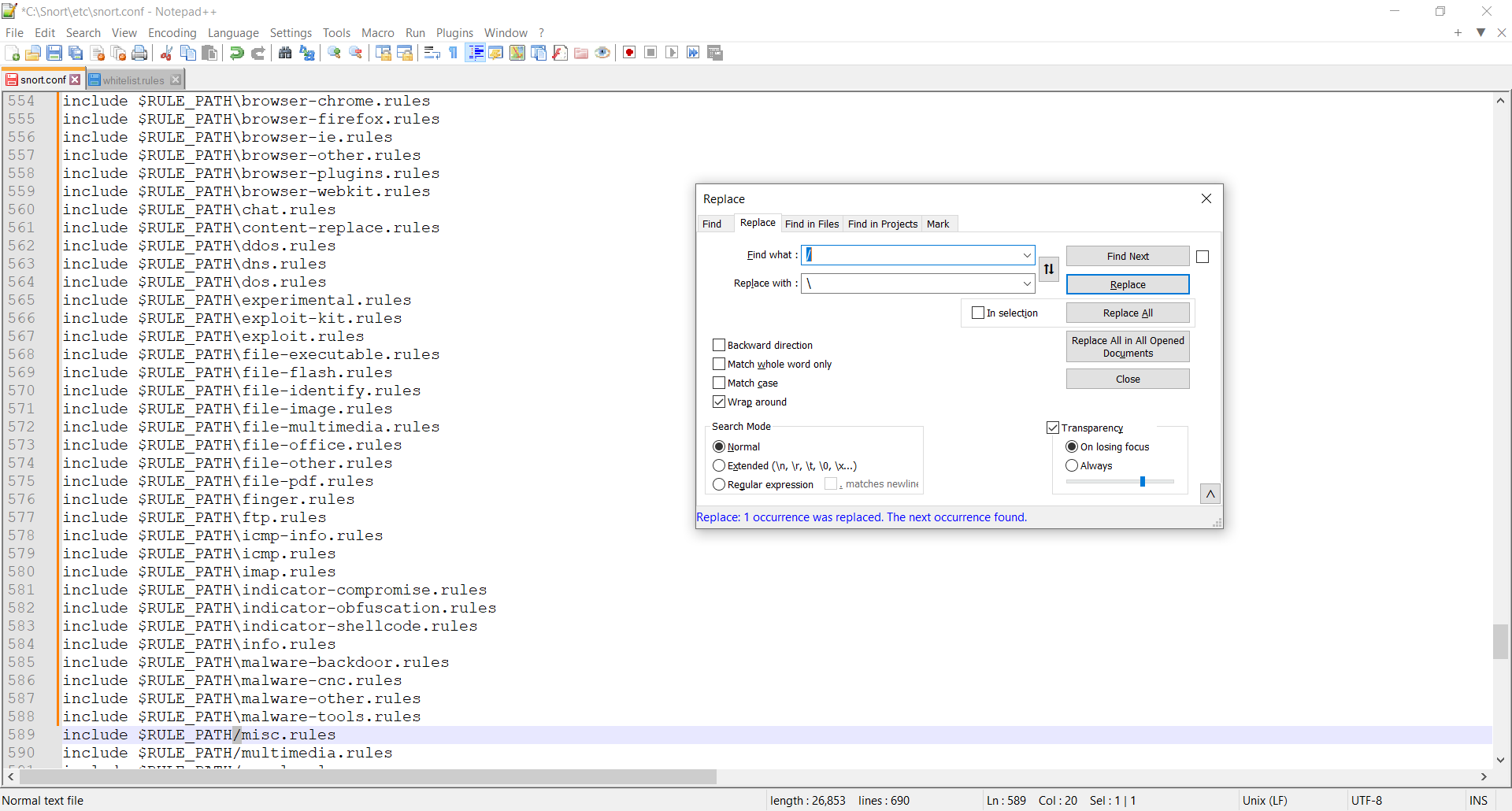


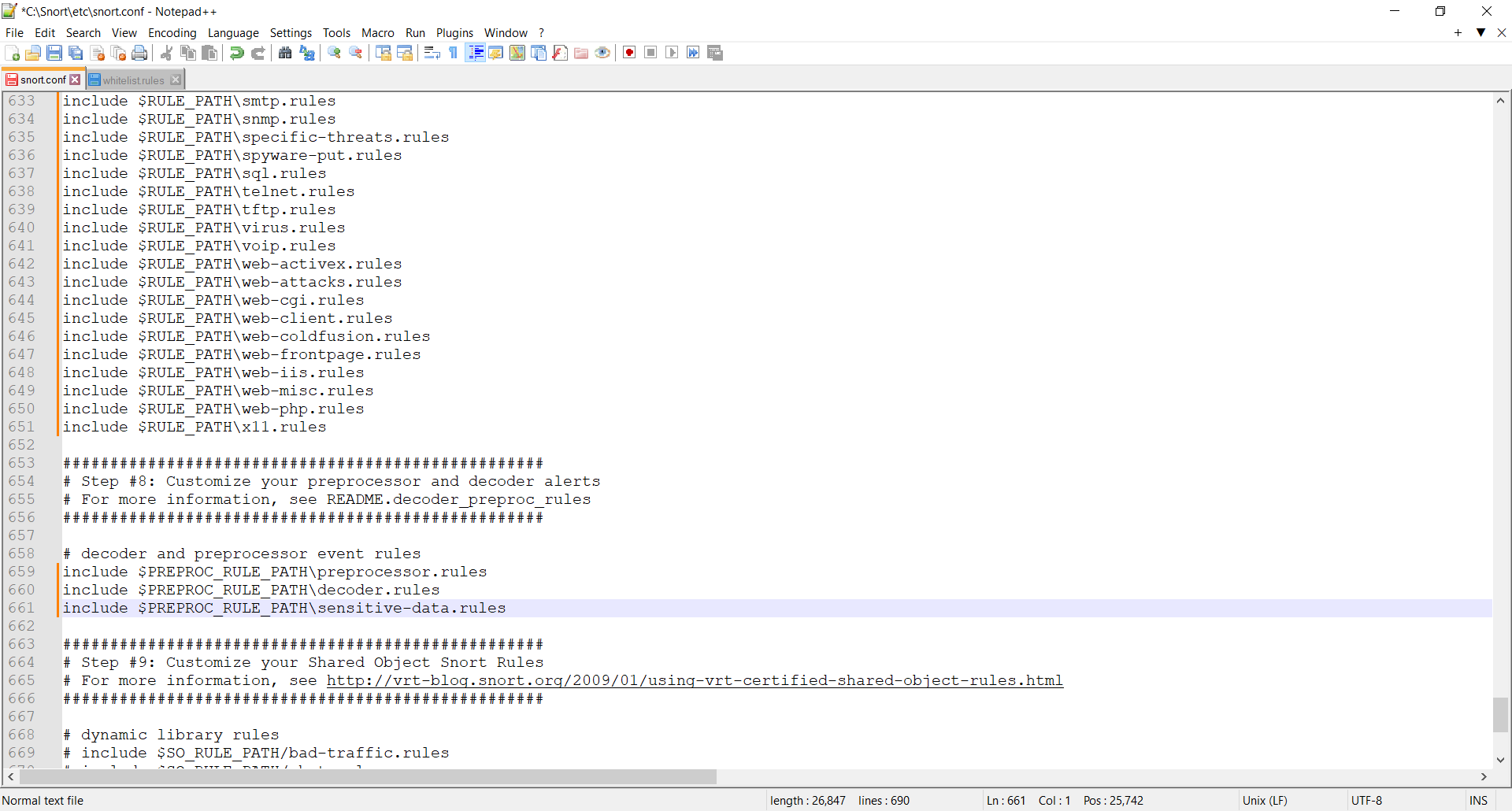


We create whitelist.rule









**Output:**

**Conclusion:**

Performed the experiment successfully.