# **Name: Abdurrahman Qureshi**

# **Roll No: 242466**

Practical No: 10

Date Of Performance: 01/10/2025

Aim: To Set up Snort Tool and study the logs.

Lab Outcome: To develop comprehensive theoretical understanding of keyloggers, their deployment mechanisms, data capture techniques, and implement best practices for detection, removal, and prevention.

Theory:

Introduction to Snort

Snort is a powerful open-source Intrusion Detection and Prevention System (IDS/IPS). It performs real-time traffic analysis, packet logging, and can be configured to detect a wide range of attacks, such as buffer overflows, stealth port scans, and malware. It operates by matching network traffic against a set of user-defined rules.

Core Components:

* Packet Decoder: Captures and prepares network packets from various interfaces (Ethernet, Wi-Fi) for processing.
* Pre-processors: Normalize and analyse traffic for anomalies that complex attacks might use to evade detection (e.g., packet fragmentation, TCP stream reassembly).
* Detection Engine: The core of Snort. It analyses decoded packets using a set of predefined rules to identify malicious activity.
* Logging and Alerting System: Generates alerts and logs packet data based on the detection engine's findings. Logs can be stored in various formats (e.g., unified2, ASCII).

Key Operational Modes:

* Sniffer Mode: Reads and displays network packets to the console. Useful for basic traffic inspection.
* Packet Logger Mode: Captures and logs packets to disk for later analysis.
* Network Intrusion Detection System (NIDS) Mode: The primary mode. Analyses traffic against a rule set and generates alerts and logs for suspicious activity.

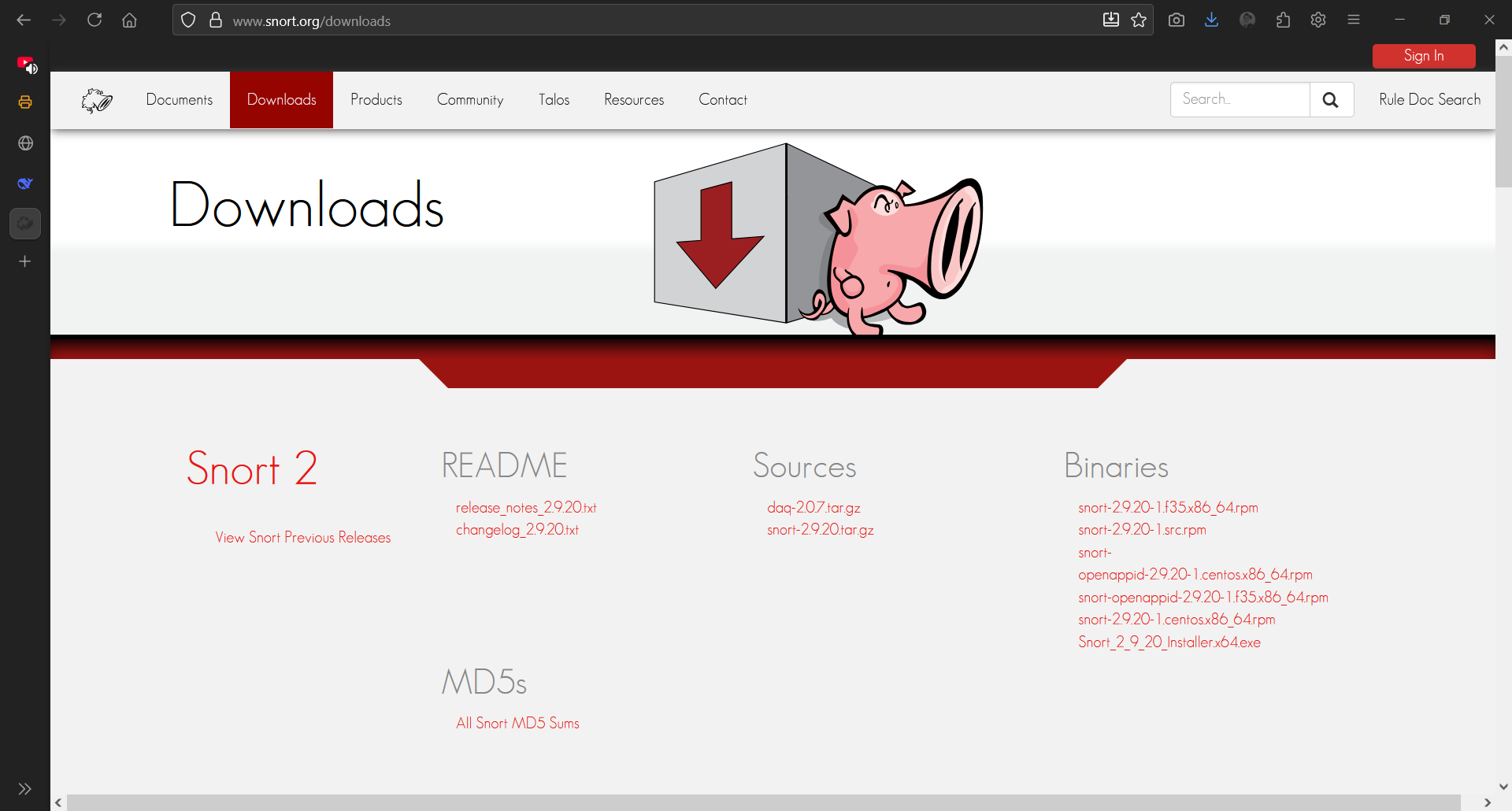
Studying Snort Logs

After running Snort in NIDS mode, you must analyse the output to identify threats.

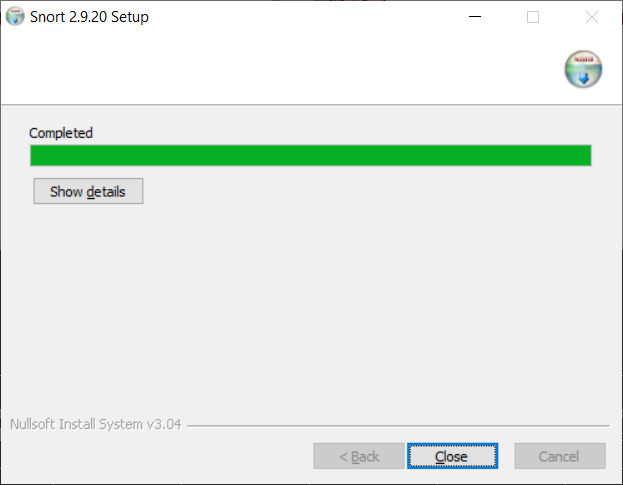
Default Log Location: /var/log/snort/

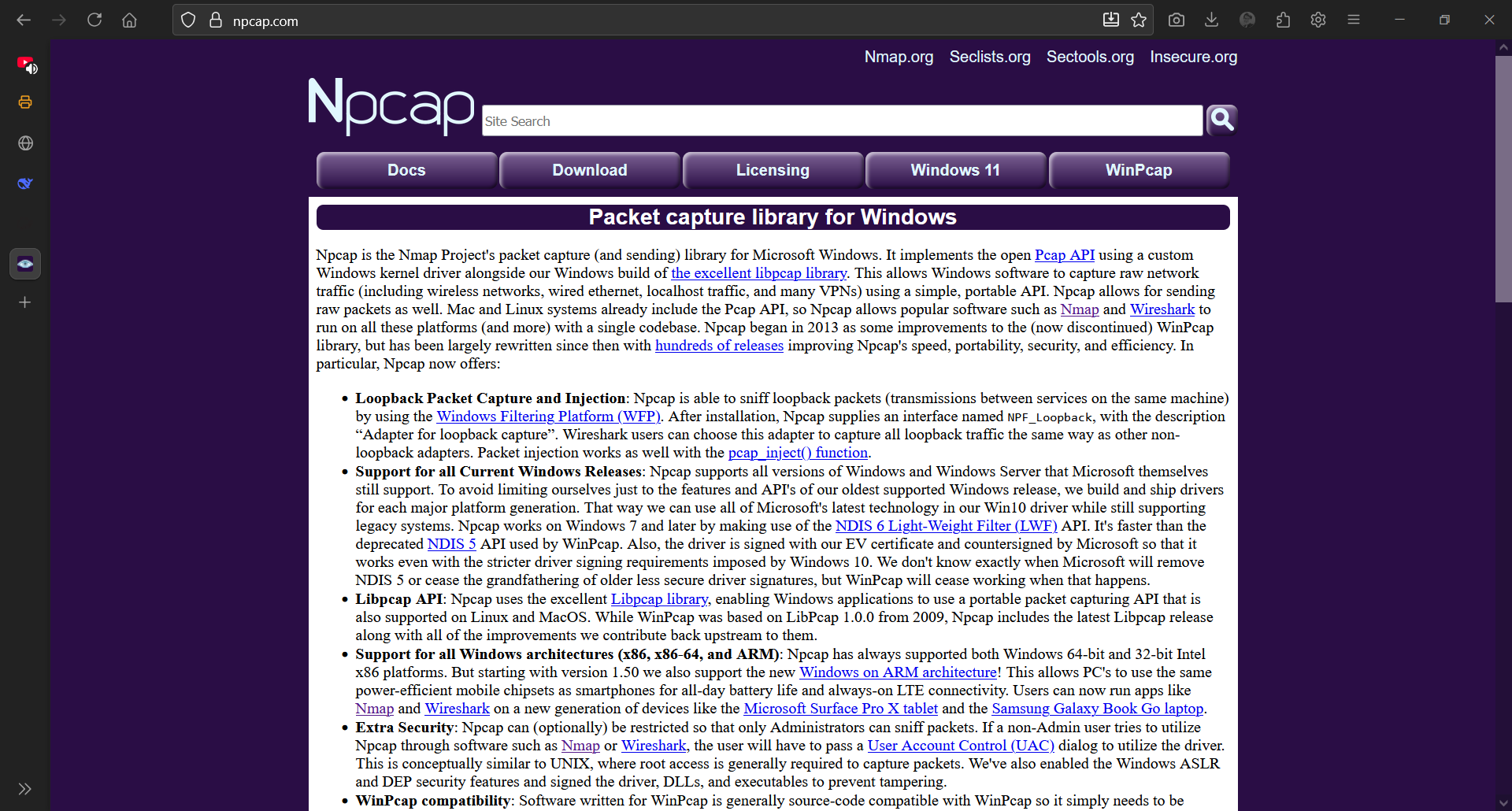
Log Formats:

* Alert File (alert): Contains a summary of triggered alerts, including timestamp, source/destination IPs, and the alert message.
* Unified2 Binary Logs: Efficient, binary format logs that require tools like barnyard2 or u2spewfoo for reading.
* PCAP Logs: Full packet capture data, which can be analysed in-depth using tools like Wireshark.

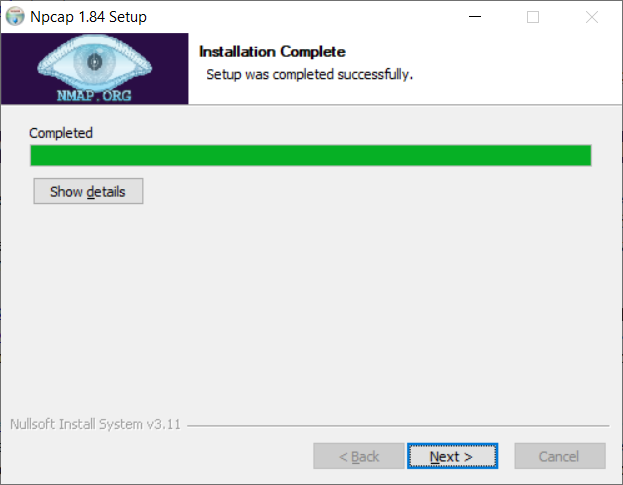


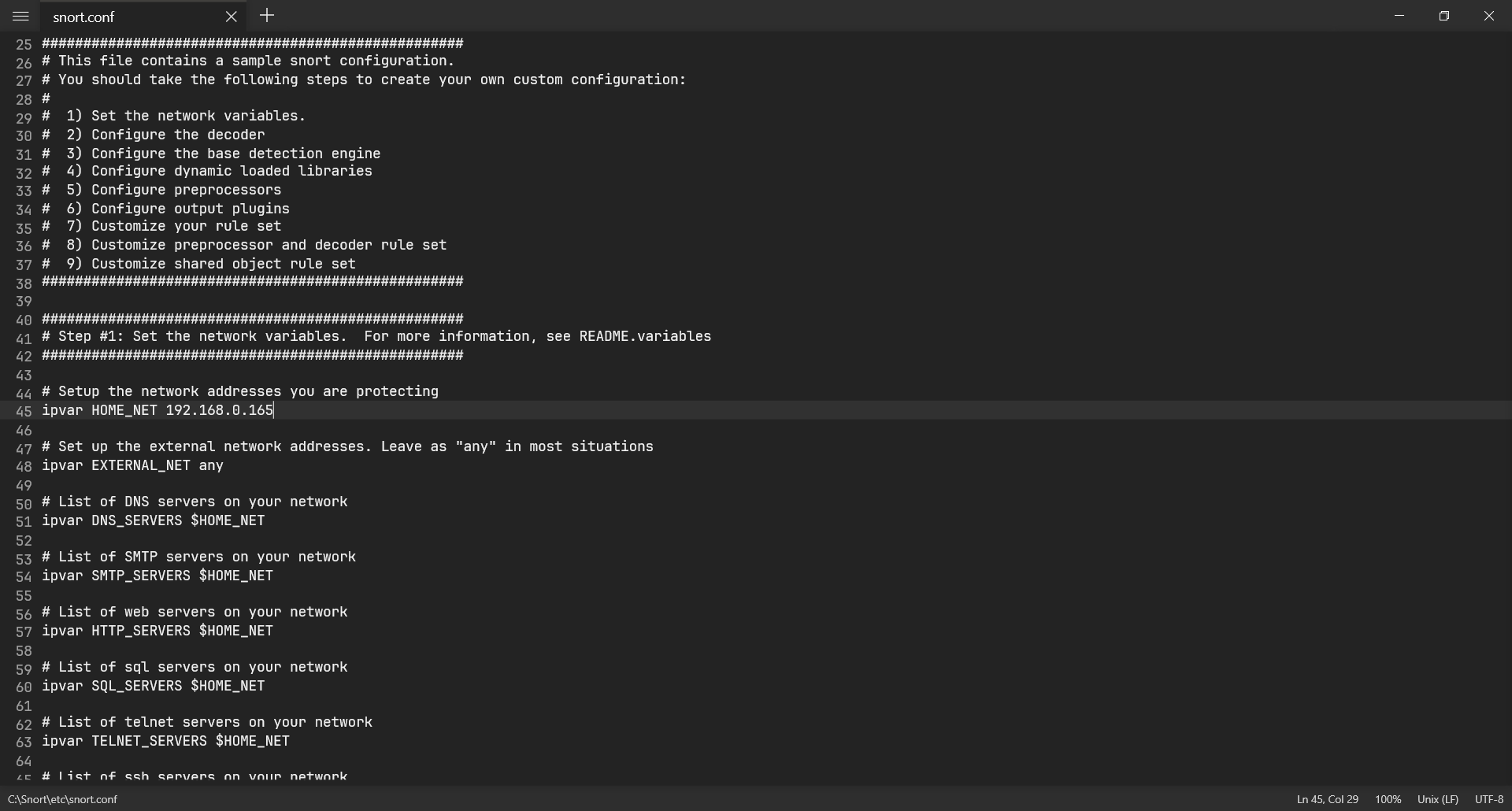
Downloading Snort



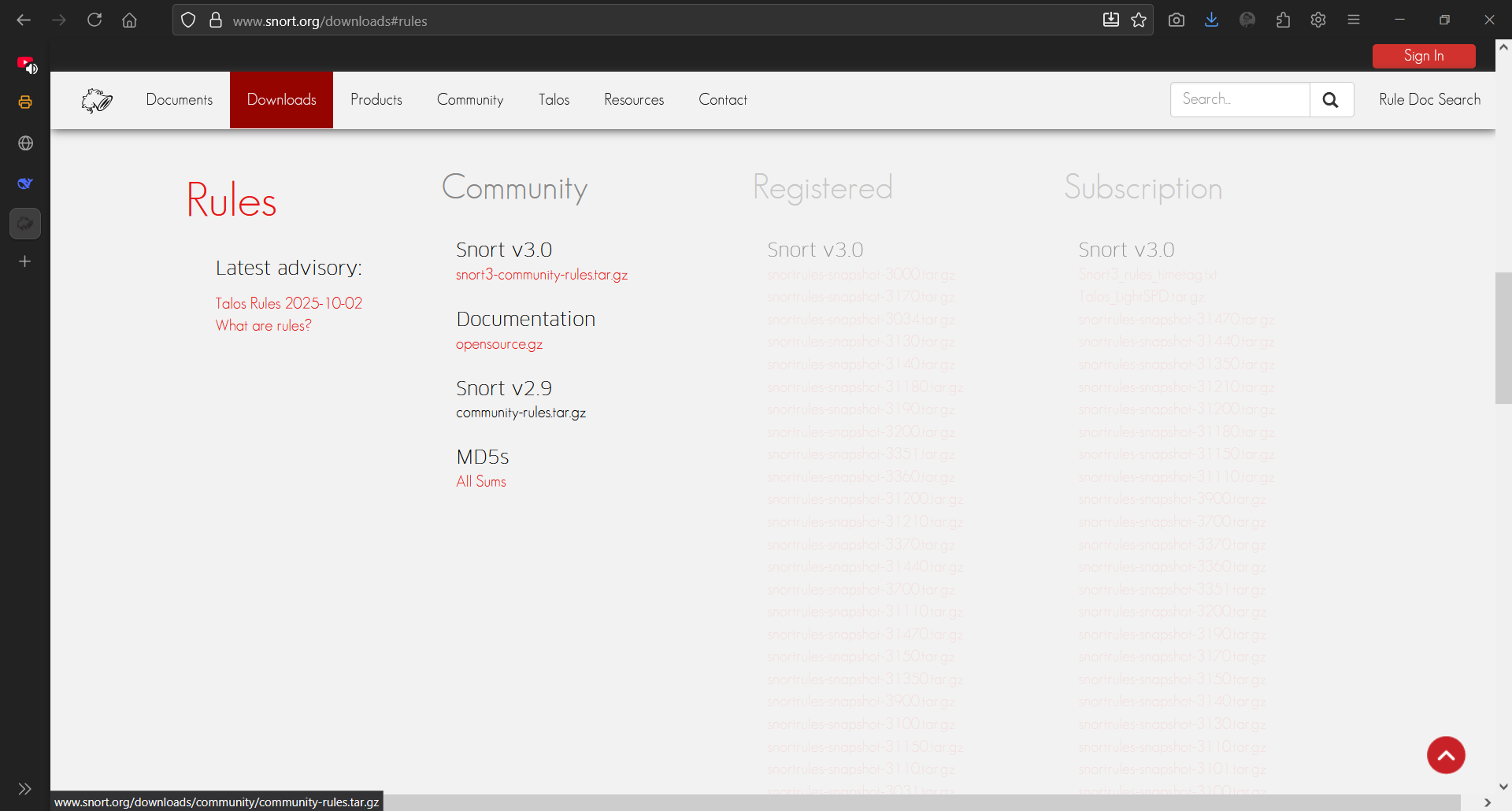


Downloading NCap

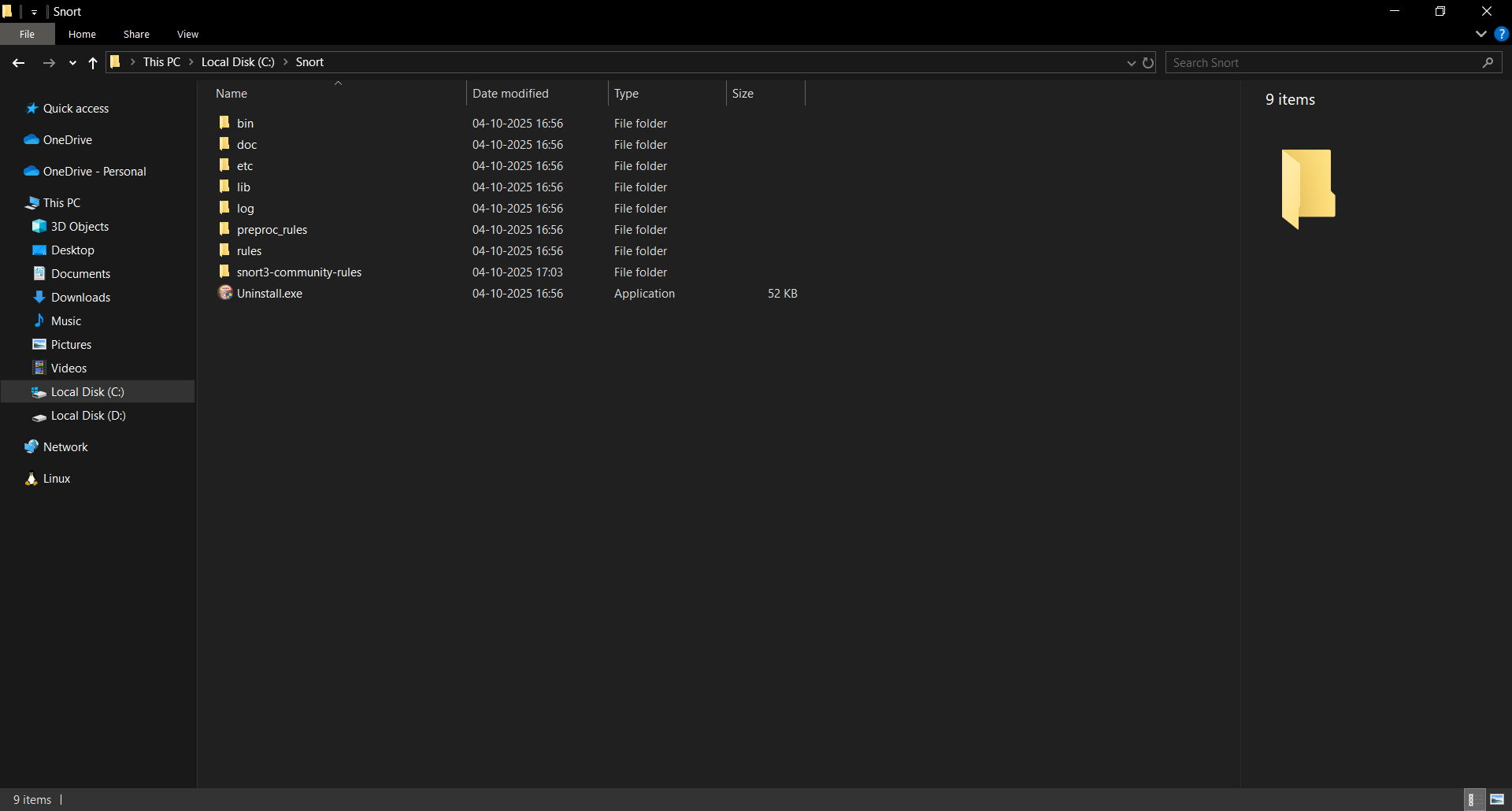




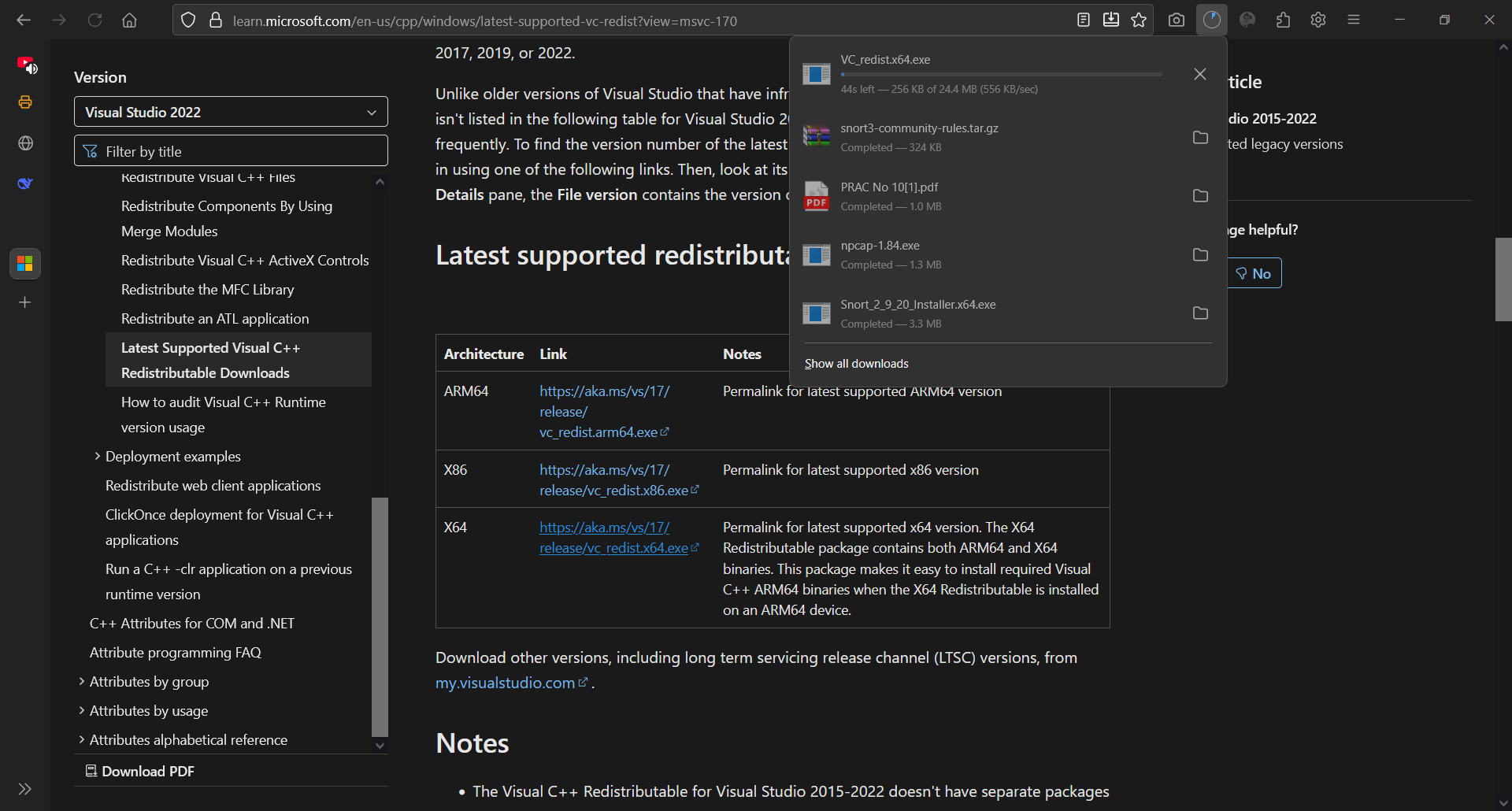
Configuring snort.conf



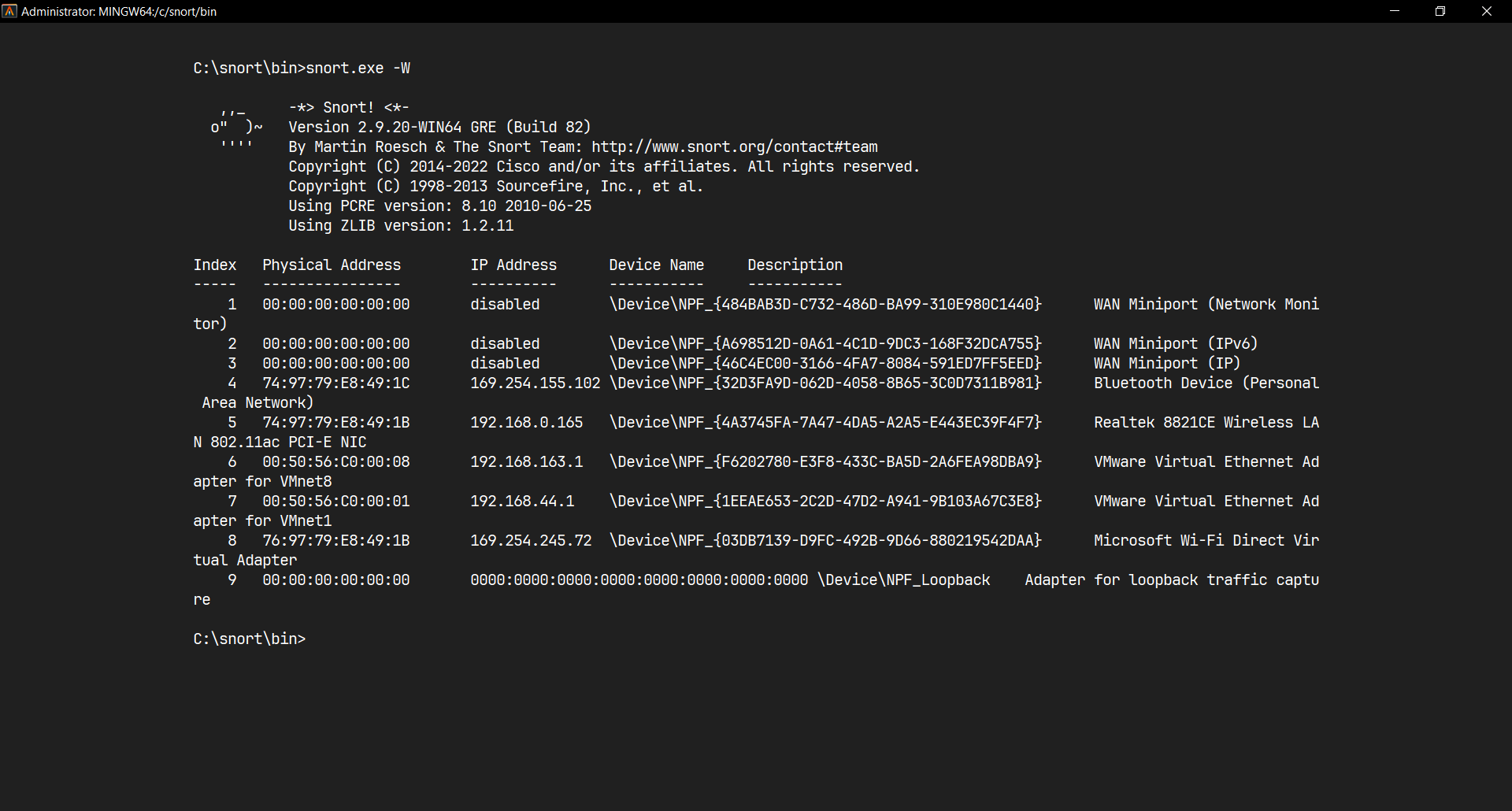
Downloading Snort Rules

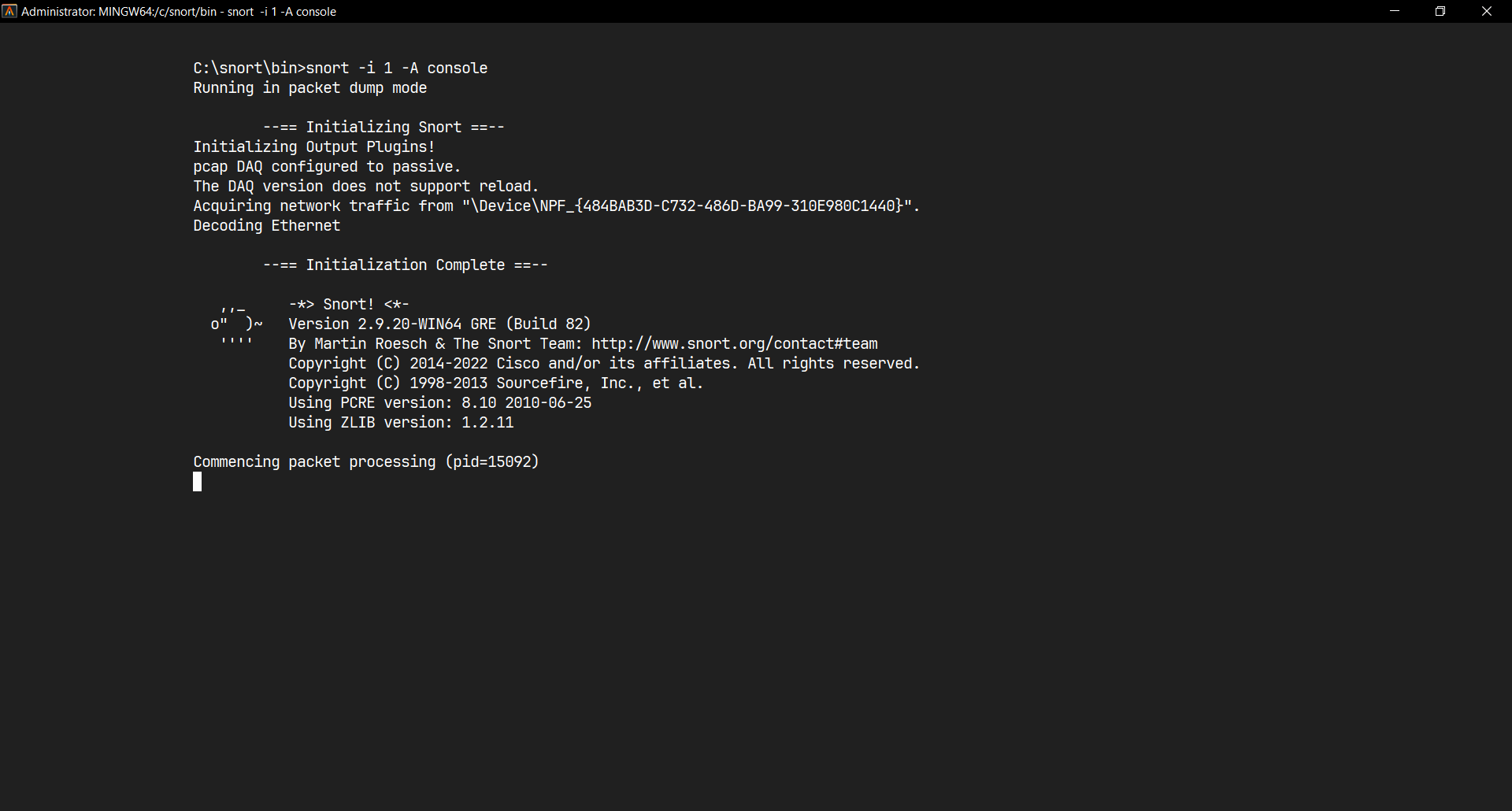


Extracted and pasted rules



Downloading C++ Redistributable





Executing Snort.exe

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Performance  (7M) | Journal  (3M) | Lab Ethics  (2M) | Attendance  (3M) | Total  (15M) | Faculty Signature |
|  |  |  |  |  |  |