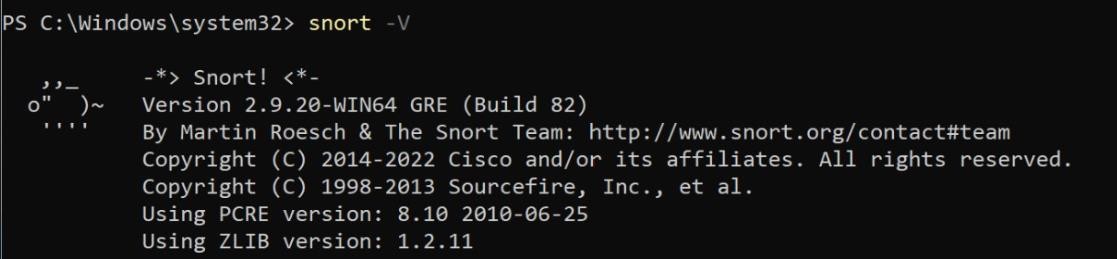
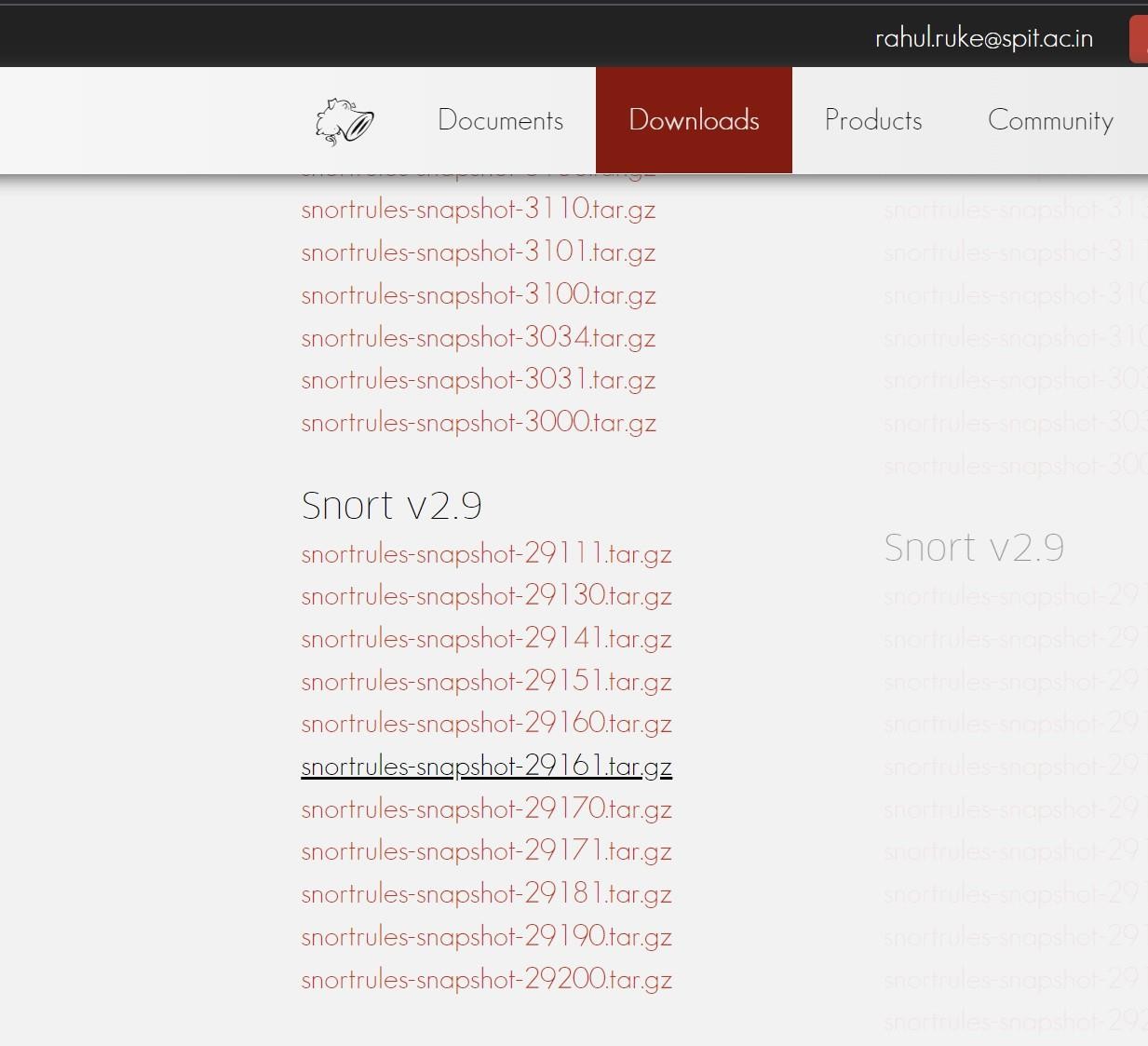
|  |  |
| --- | --- |
| **Name** | **Hatim Sawai** |
| **UID no.** | **2021300108** |
| **Experiment No.** | 9 |
| **AIM** | Configure and application of SNORT Intrusion Detection System. Upload the compressed file as per the instruction in the lab session. |

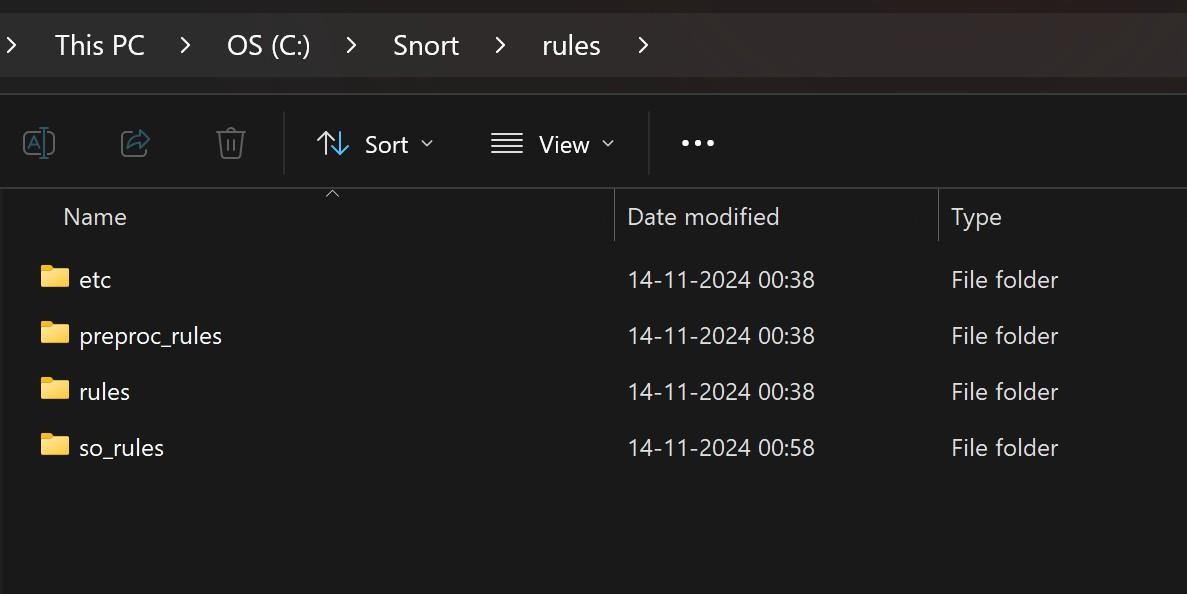
Step 1) Download Snort from snort.org and Choose the destination folder (default:

C:\Snort).

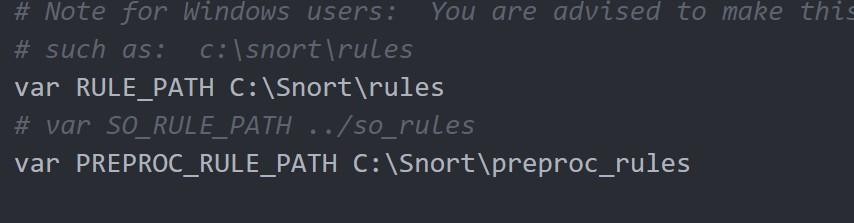
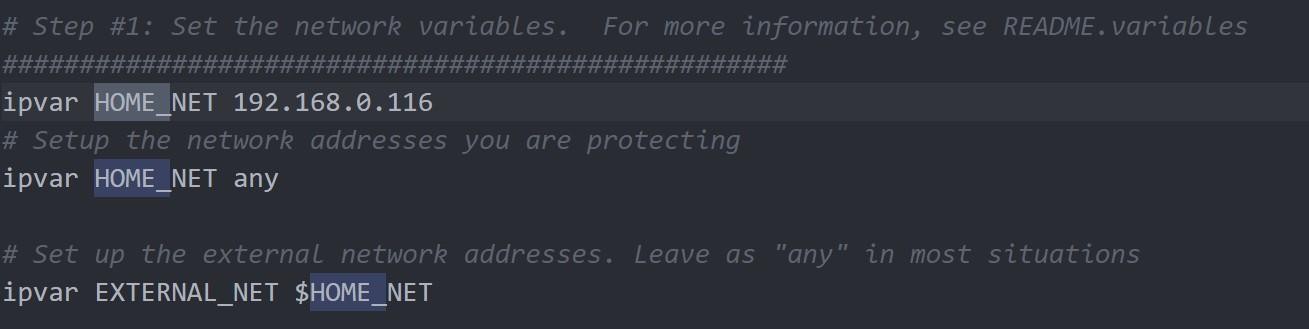
Step 2) Download and Configure Rules ( First you have to sign in to enable it)

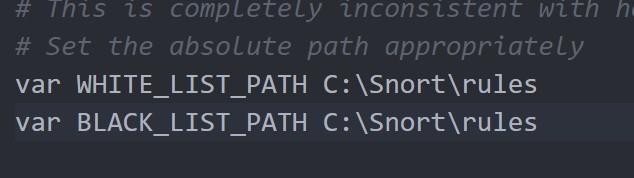


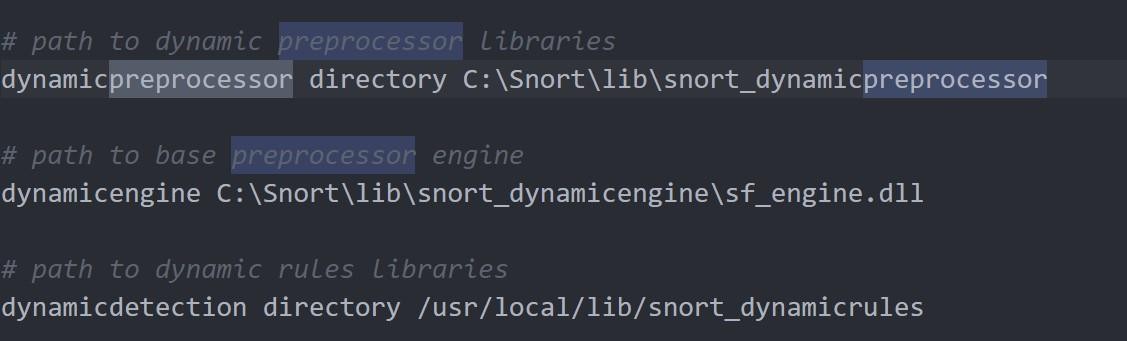
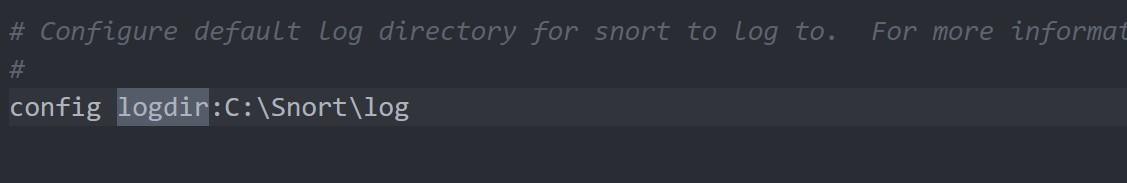
Step 3) Extract this rule to C:\Snort\rules

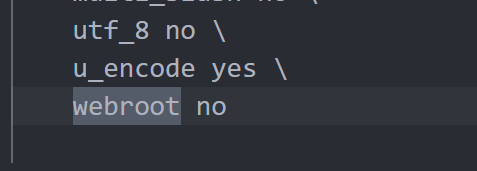


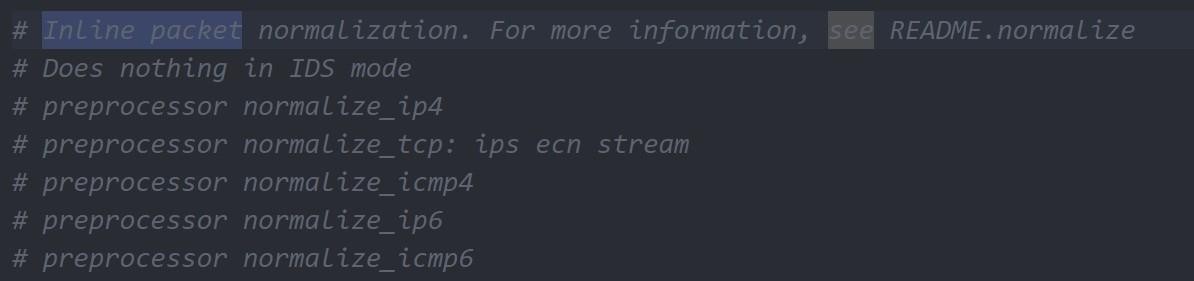
Step 4) Editing the snort.conf file

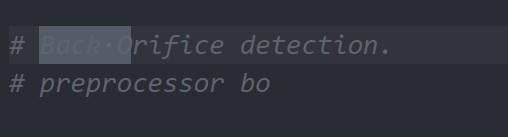


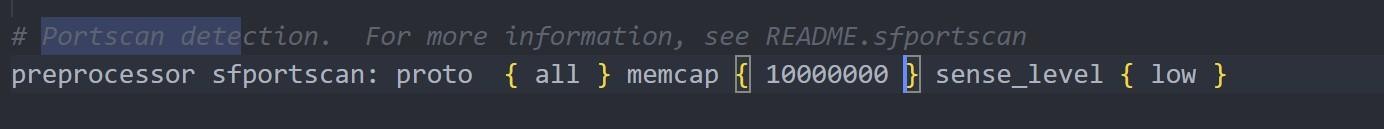


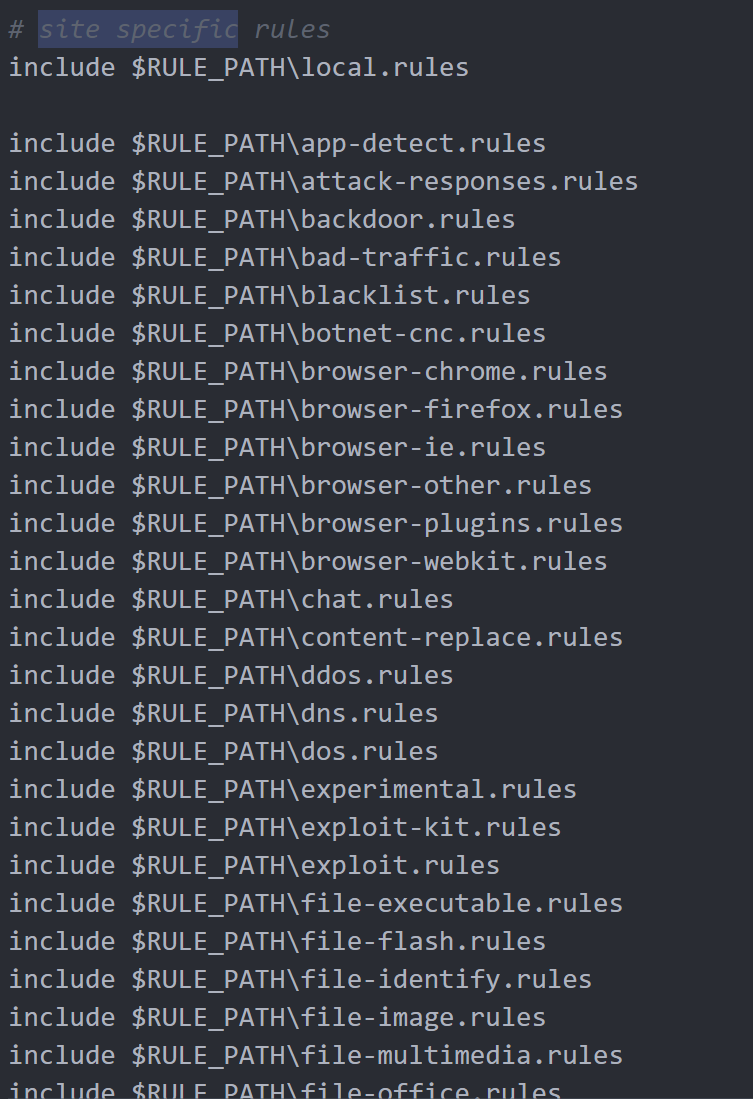




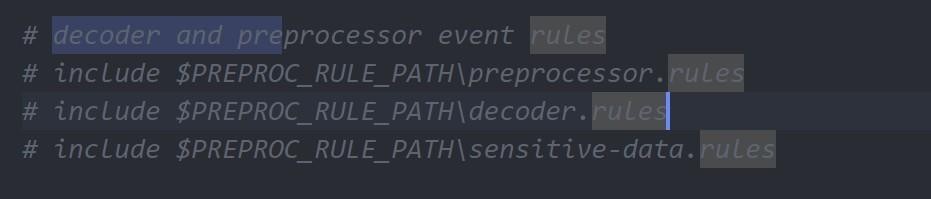


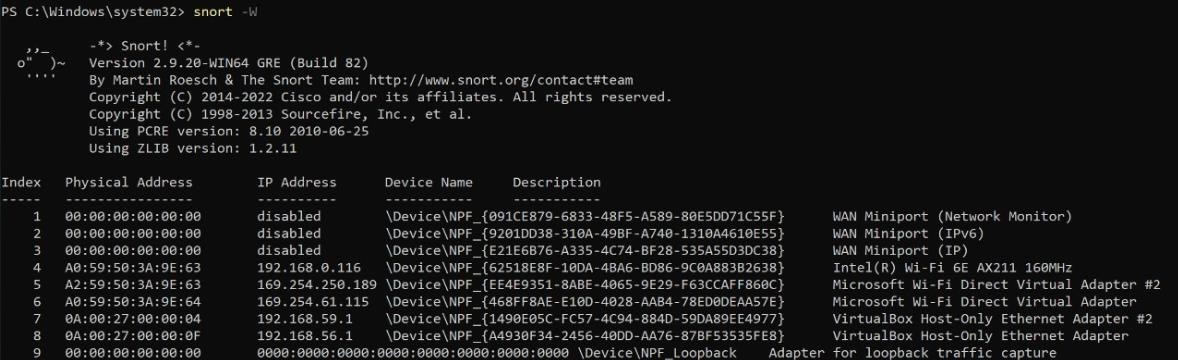




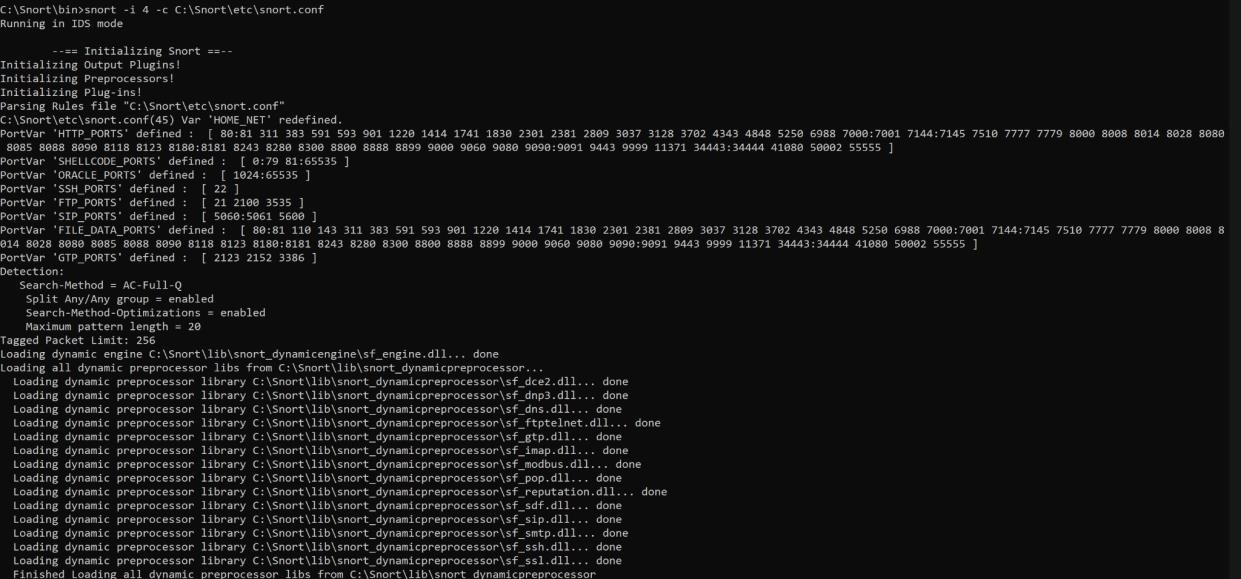


replacing the forward slash “/” with backslash “\”



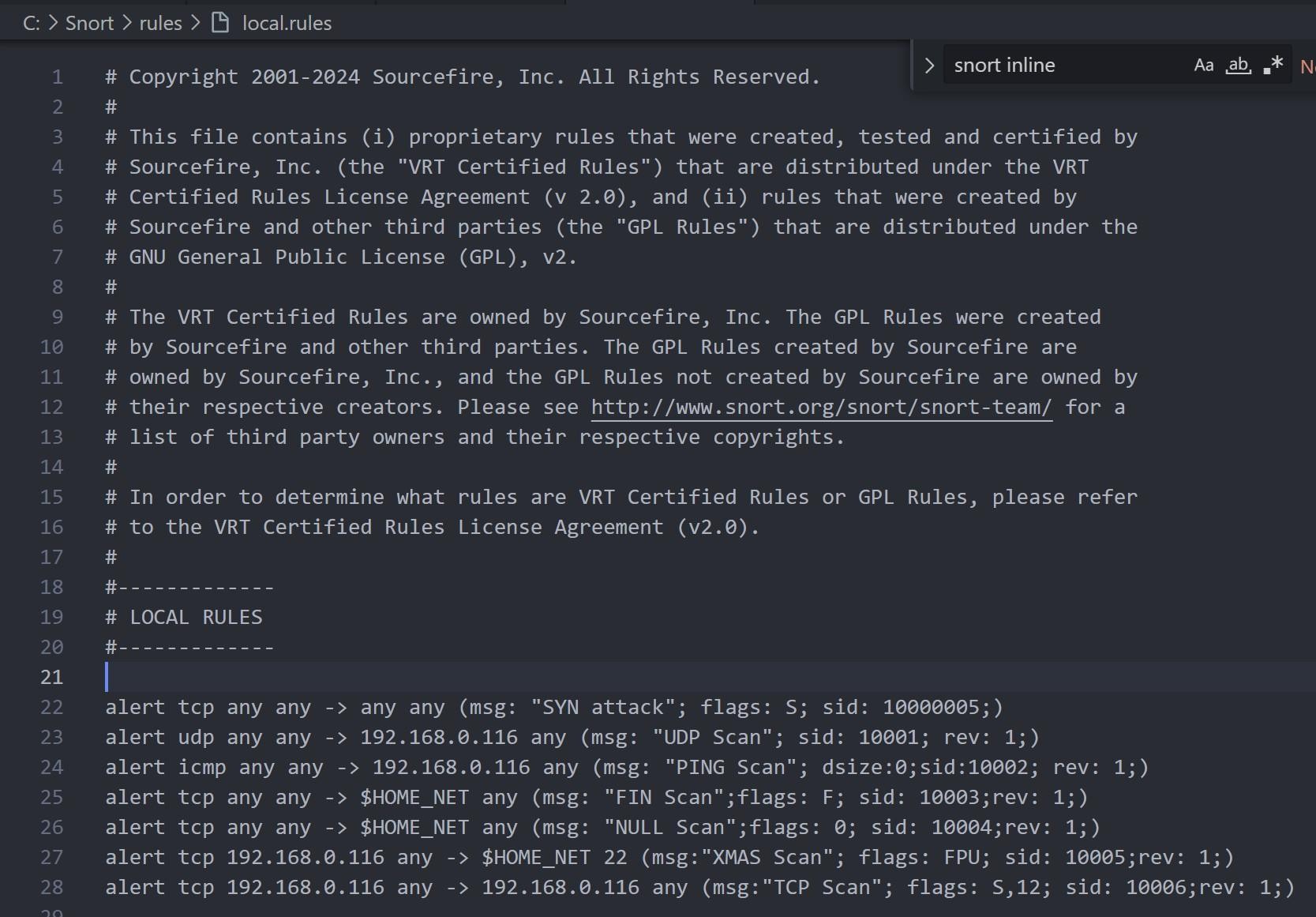
Put Decoders and Preprocessors Rules in Comments

Check the Interface

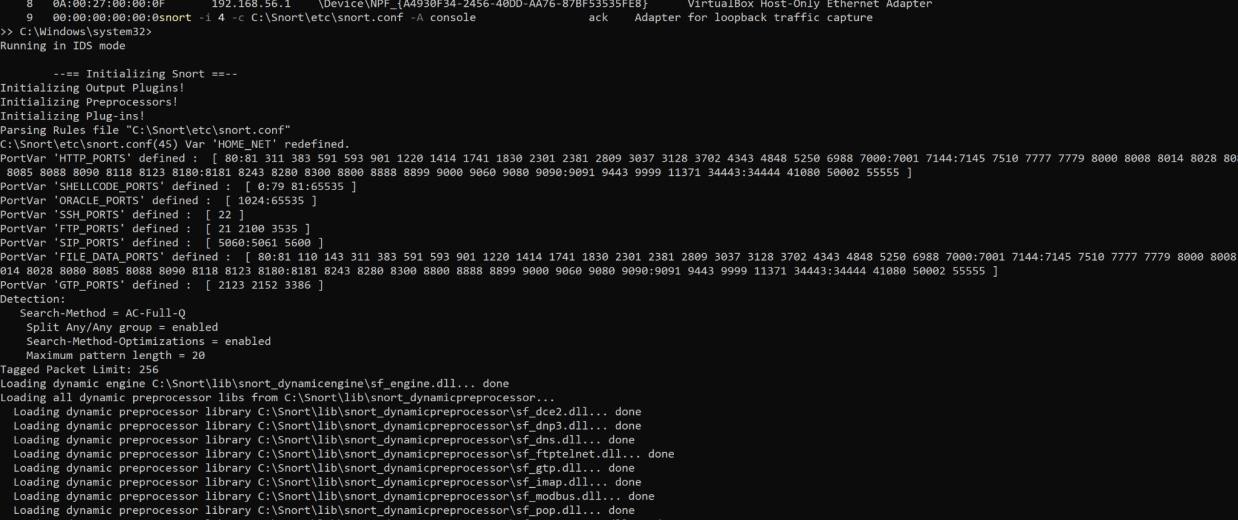


Execute the Snort tool in the command prompt by typing “snort –i 2 –c C:\Snort\etc\snort.conf

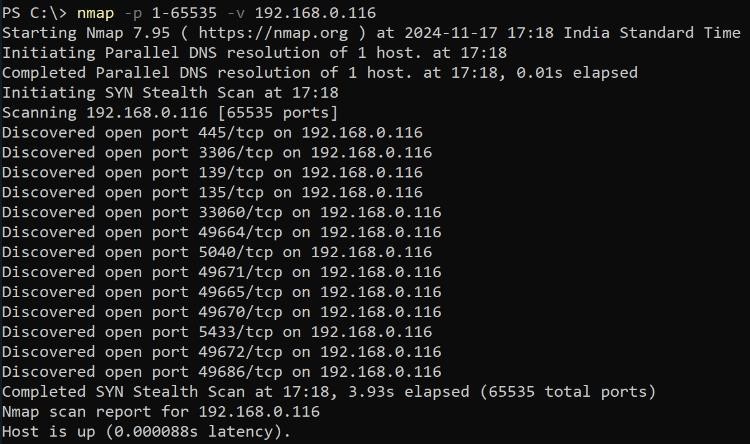
**WRITE RULES TO DETECT SCANNING ATTACKS**



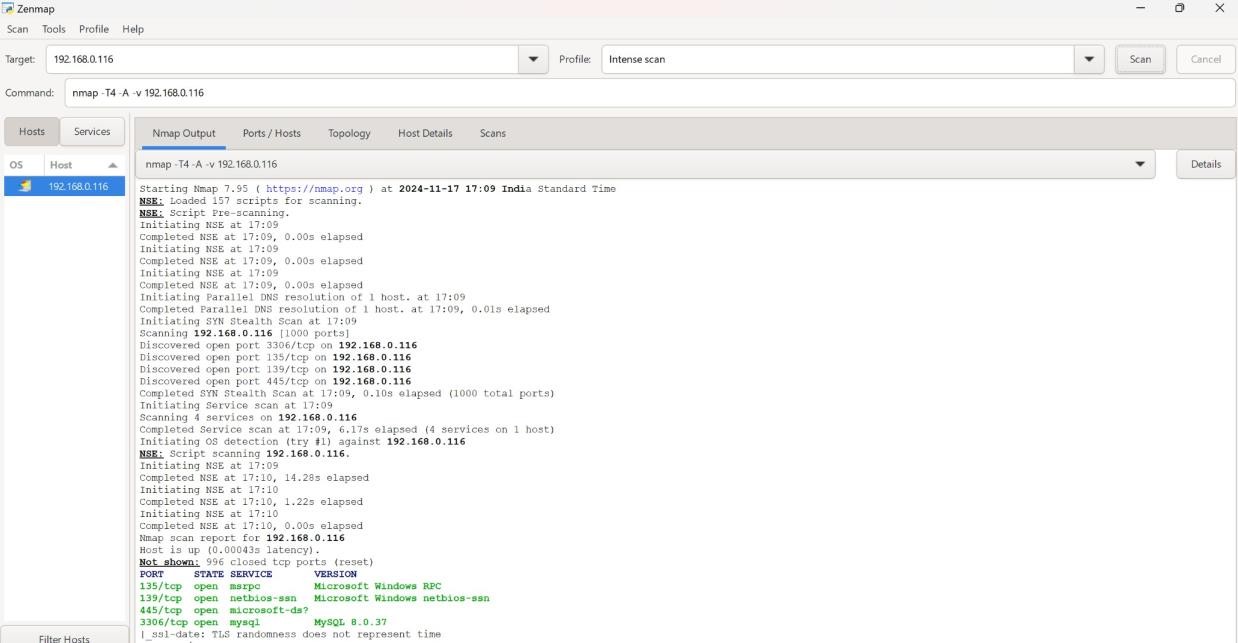
Adding Rules in local.rules



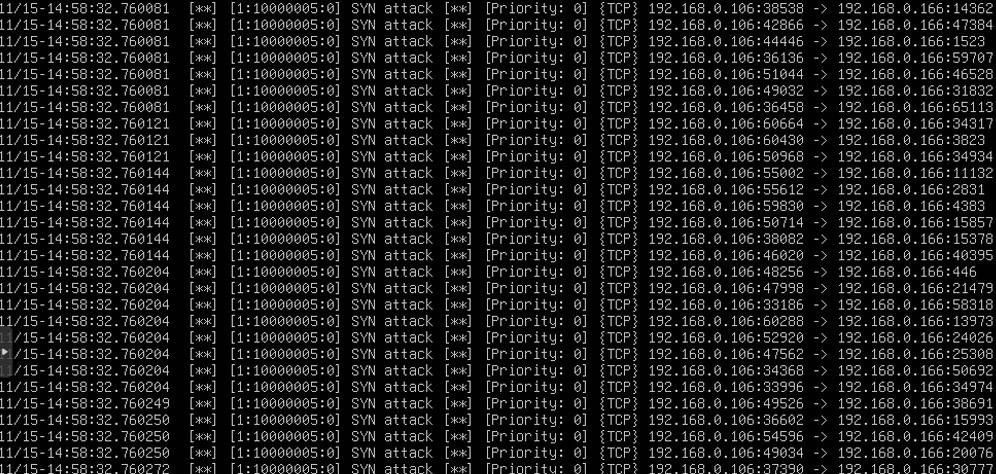
Running Snort in IDS mode



Network Scanning Attack with Nmap Tool



Network Scanning Attack with Zenmap Tool



Detection of Network Scanning Attack with Snort IDS