**IT8761 – Security Laboratory**

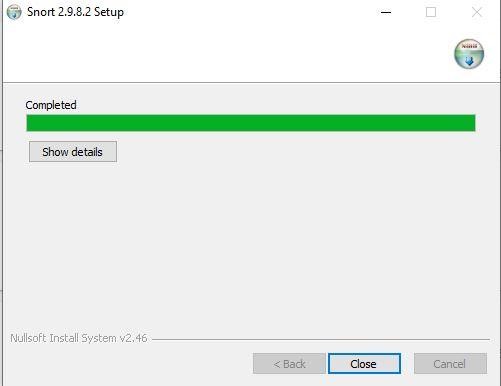
**Reshma Ramesh Babu**

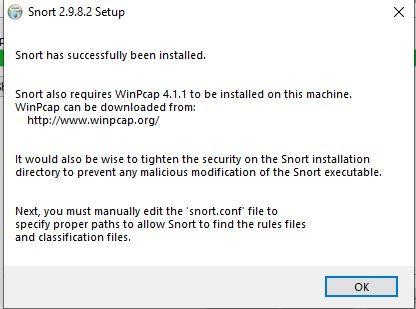
**312217104129**

**Exercise 10**

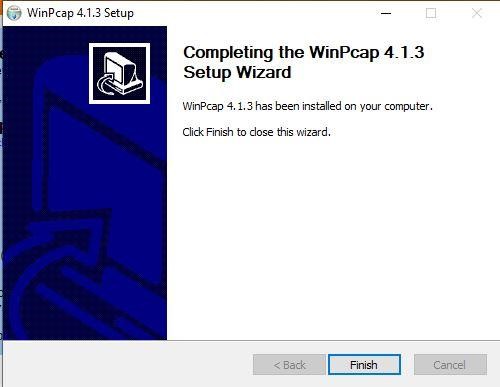
**Aim:** Intrusion Detection System (ids) using snort

**Step 1:** Installing Snort 2.9.8.2

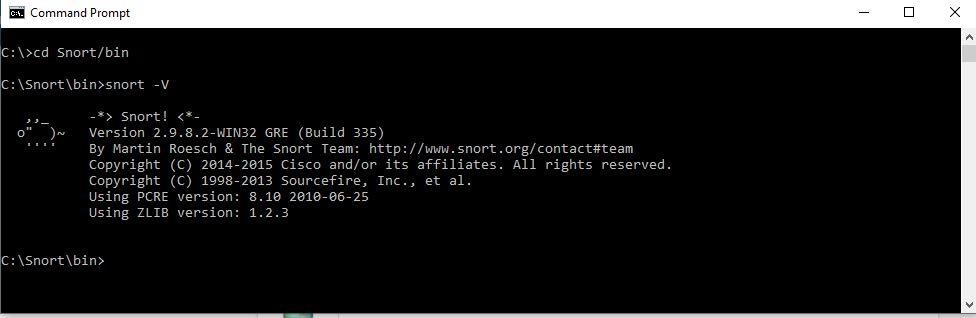




**Step 2:** Snort requires Wincap to be installed, so install wincap and restart the system



**Step 3:** Open command prompt and navigate to C:\Snort\bin and run the command: **snort -V** to check if installation was successful

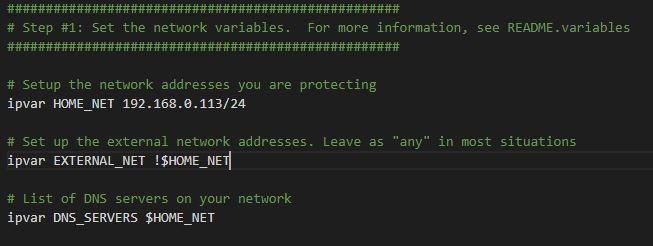


**Step 4:** Download the snortrules-snapshot-2900.tar.gz file and extract it, replace the rules, preproc\_rules folder in C:\Snort with the corresponding folders that were extracted.

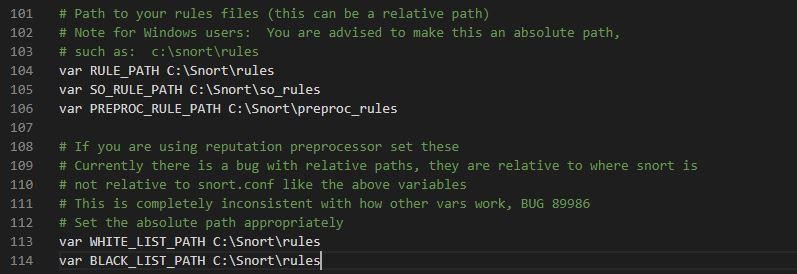
**Step 5:** Open the C:\Snort\etc\snort.conf file and make the following changes in order to configure snort to match your local environment and operational preferences.

Note: Remember to change all ‘/’ to ‘\’ (for Windows)

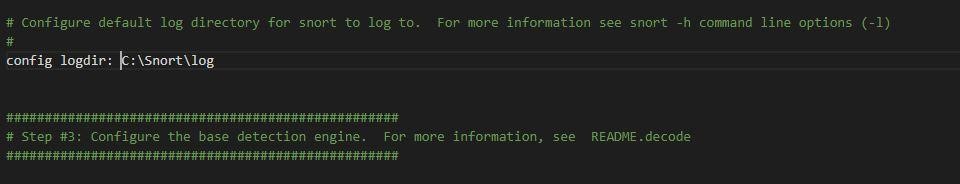
Make HOME\_NET reflect the system’s ip address and EXTERNAL\_NET is any ip that is not HOME\_NET



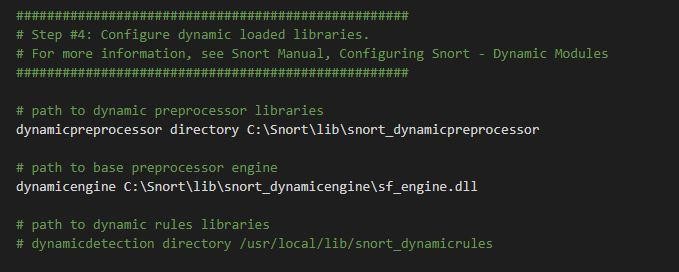
Set appropriate paths



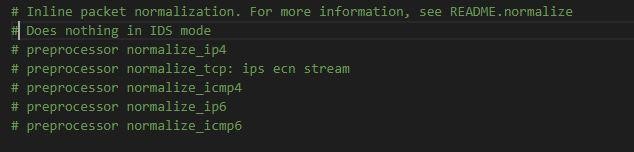
Set log dir path



Set appropriate paths



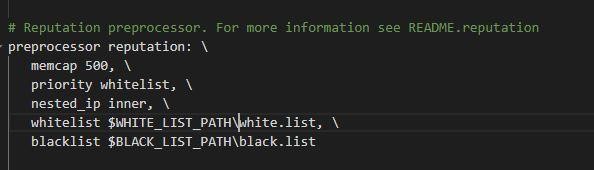
Comment the following lines as we are using only IDS mode on Windows



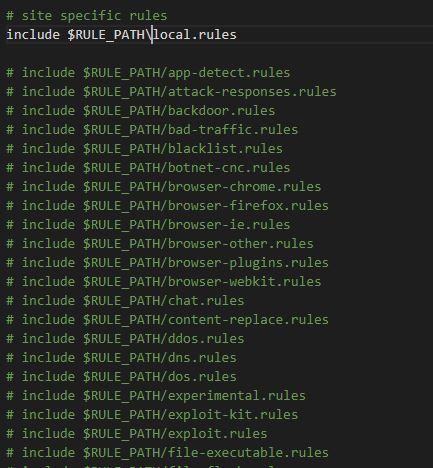
Enable portscan detection



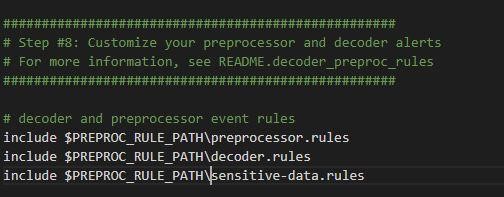
Set appropriate paths for whitelist and blacklist ip addresses and enable repudiation preprocessor



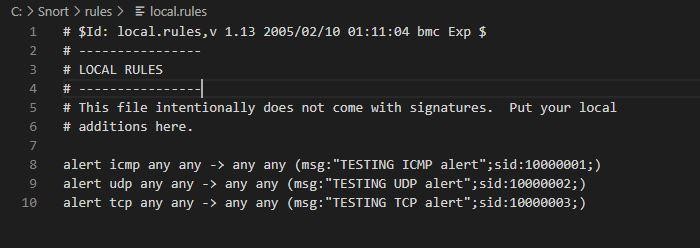
Include only local.rules, can include others as well.



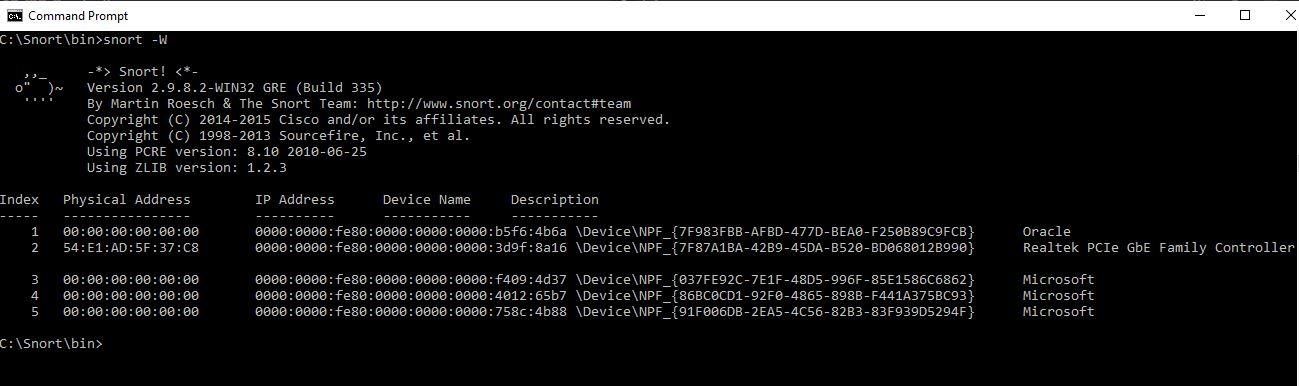
Uncomment pre-processor and decoder alerts and set appropriate paths



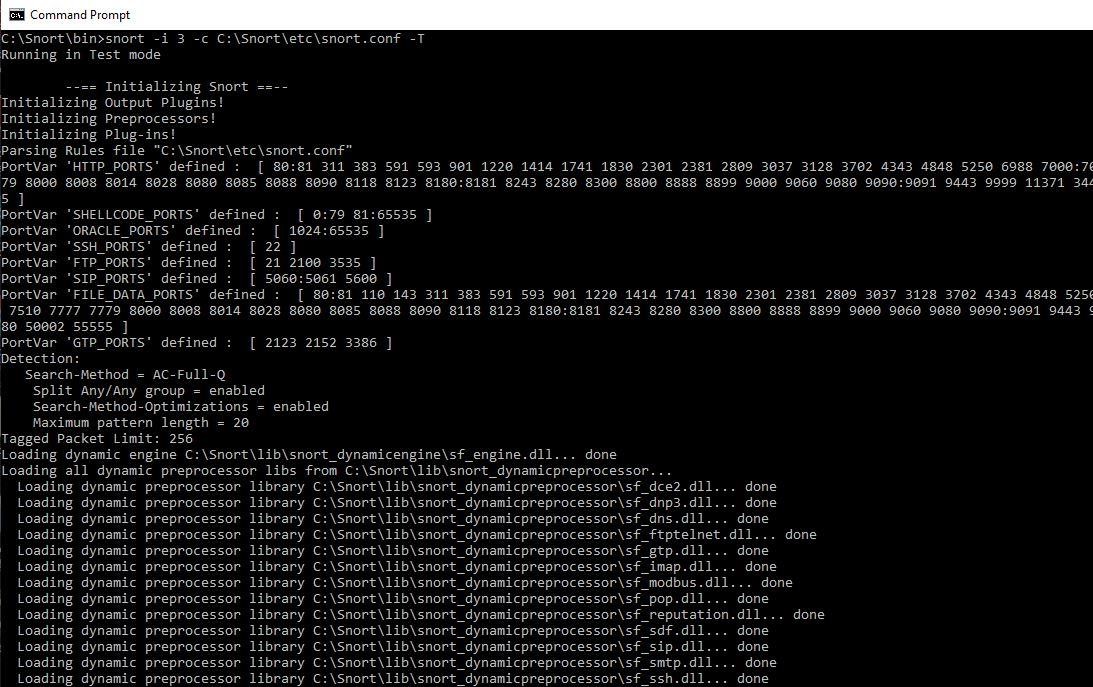
**Step 6:** Updating local.rules, this is where we will write our own rules, and create empty files white.list and black.list in C:\Snort\rules.

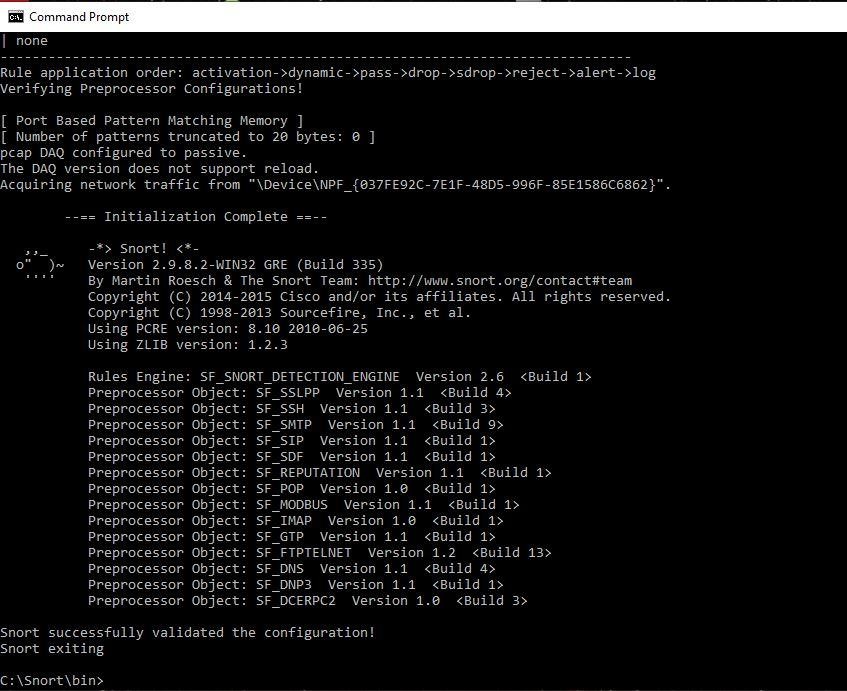


**Step 7:** Check the list available interfaces snort can listen to and choose the appropriate one.

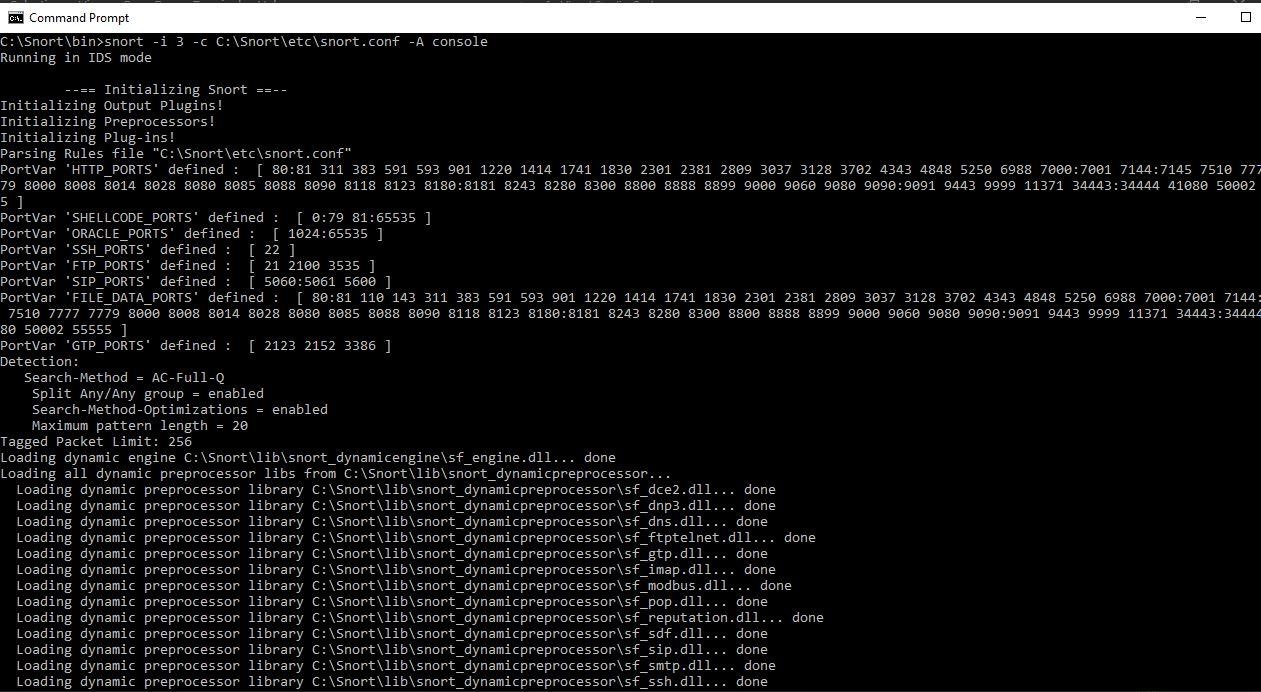


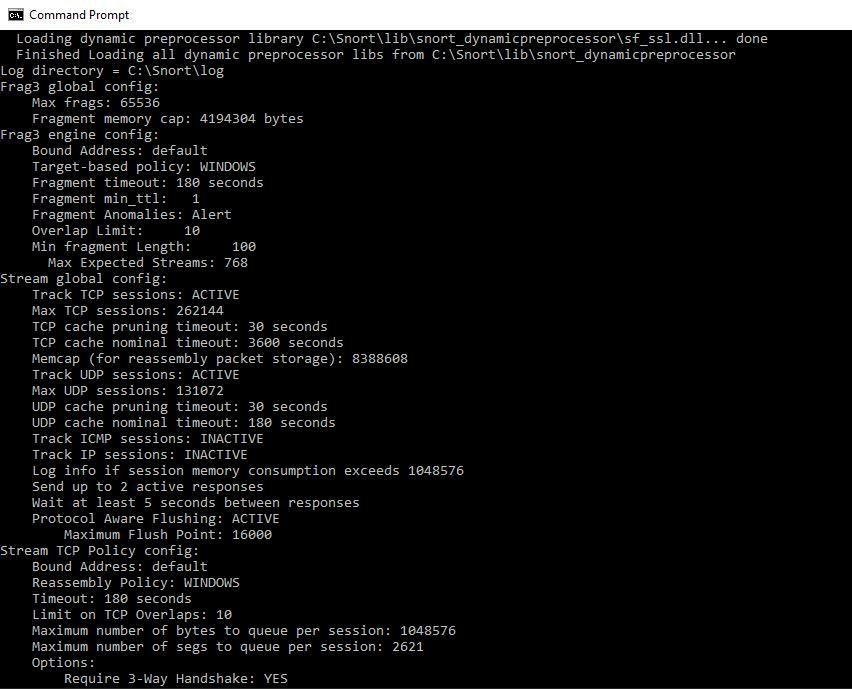
**Step 8:** Test if the configuration set for snort is valid using the command **snort -i 3 -c C:\Snort\etc\snort.conf -T**

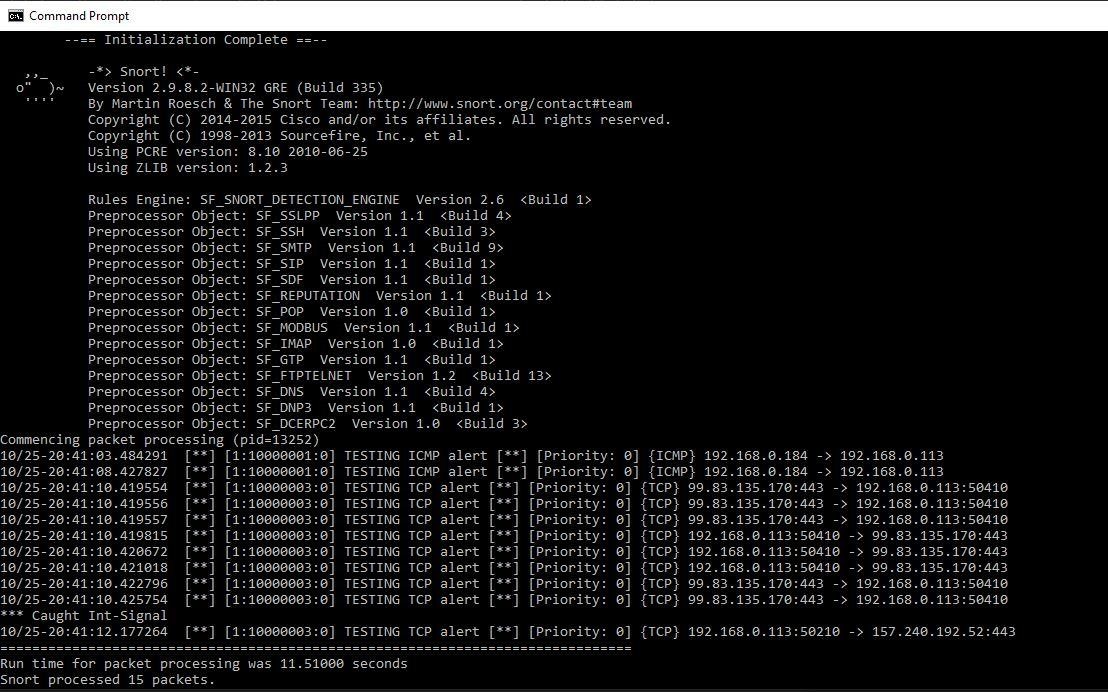




**Step 9:** Start snort using the command **snort -i 3 -c C:\Snort\etc\snort.conf -A console**



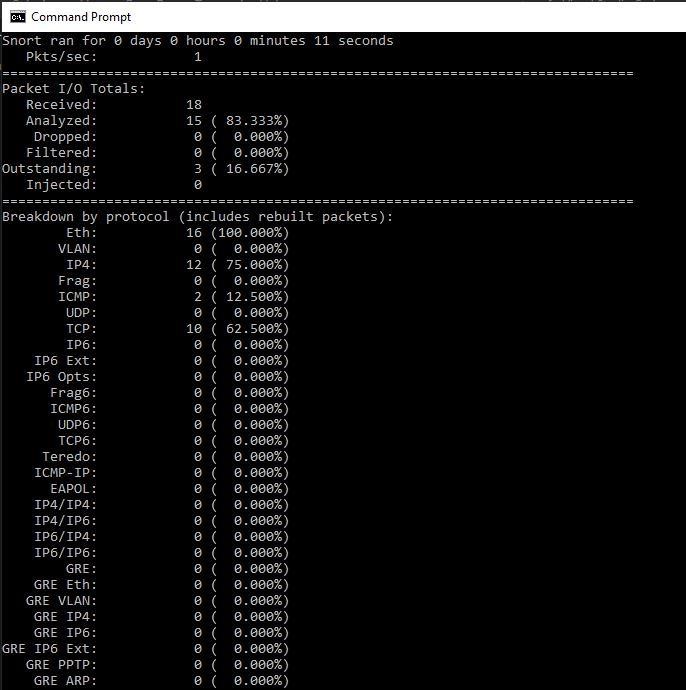


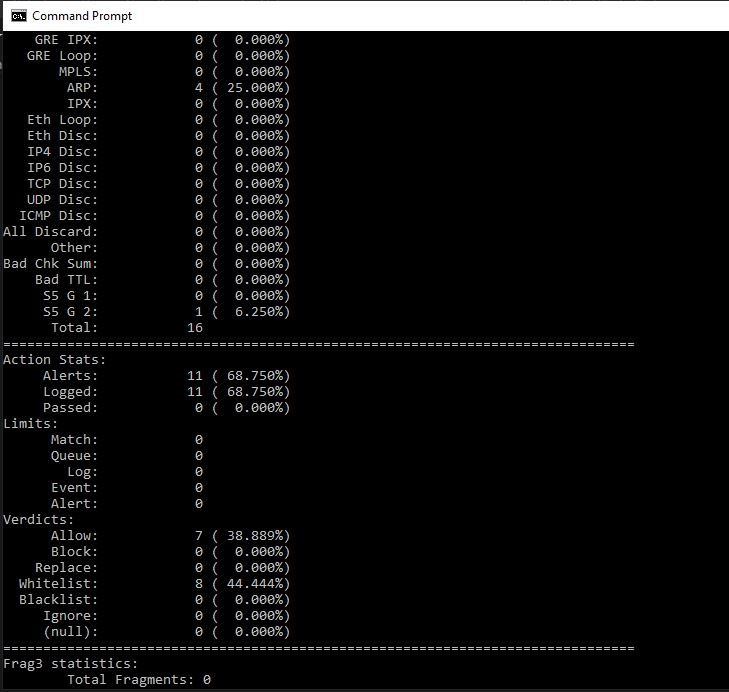


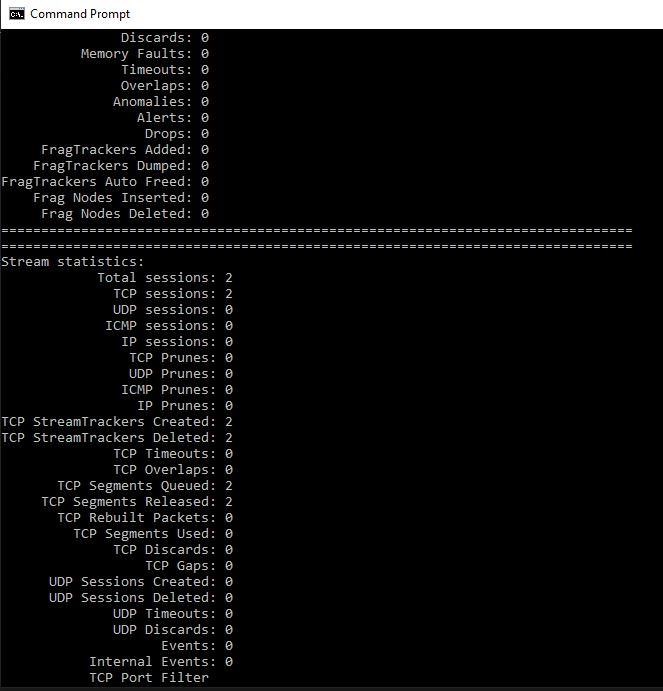
The system with snort was pinged with another system on the same network with an ip address 192.168.0.184 as can be seen from the ICMP alert generated by snort.

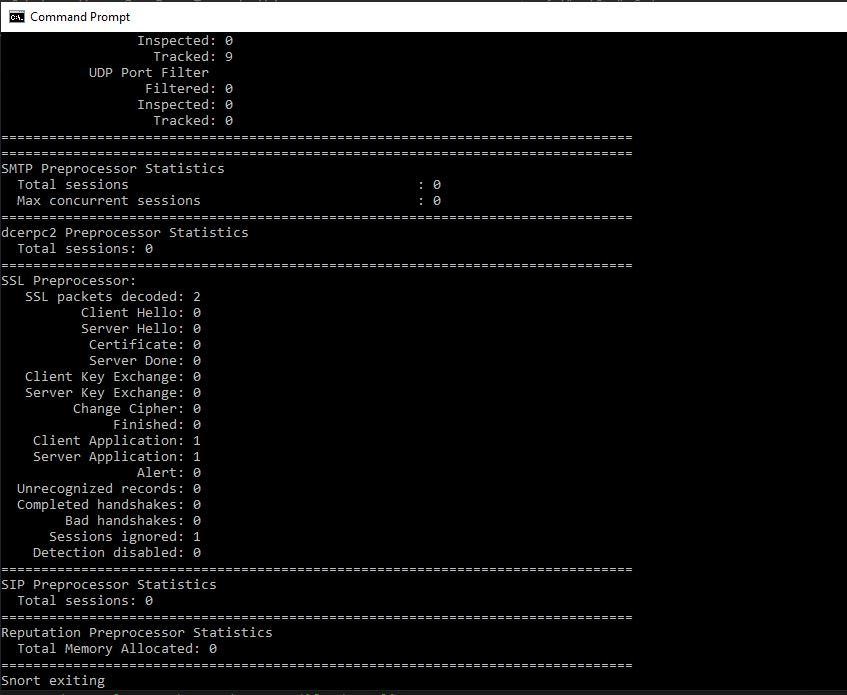
To exit snort press **cntl+c**

A summary of all packets processed is presented.

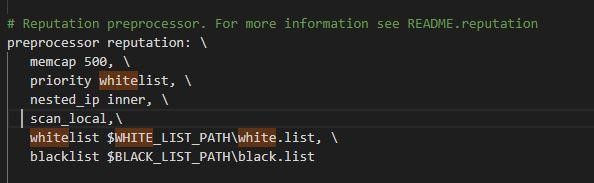


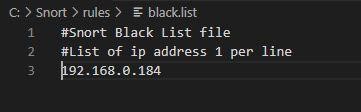






**Step 10:** Detecting access by a black listed ip. In the C:\Snort\etc\snort.conf file ensure scan\_local is added (since the blacklisted ip will be a local one).

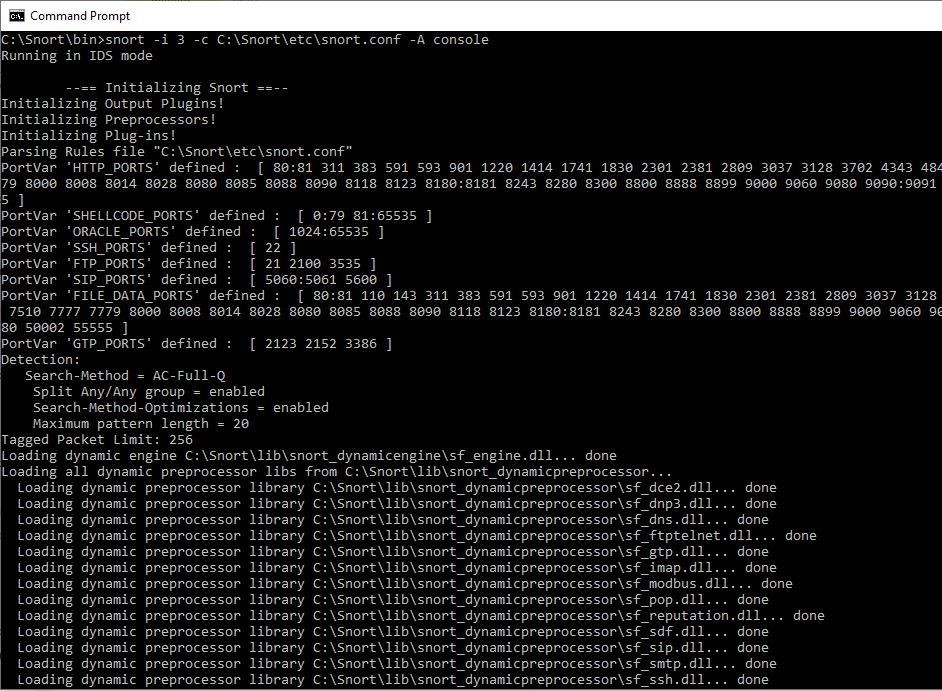
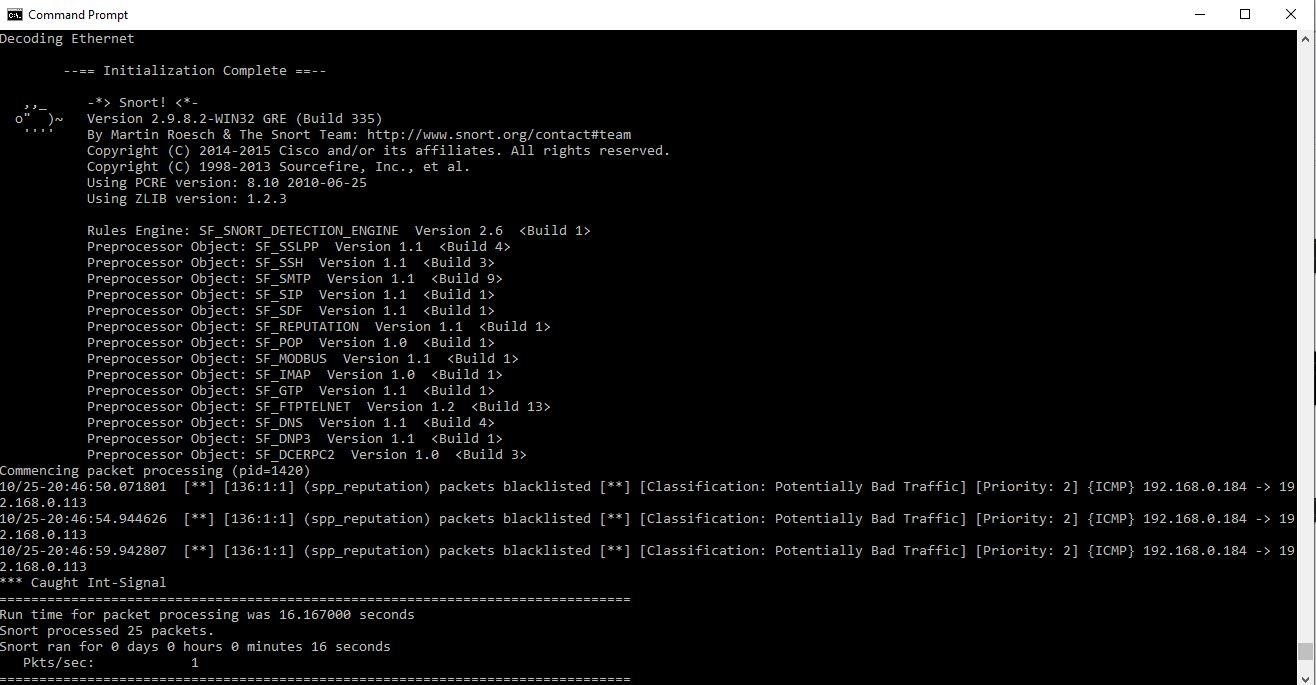
 Add the following lines to C:\Snort\rules\black.list file



Edit C:\Snort\rules\local.rules to include the following 2 rules.



Run snort using **snort -i 3 -c C:\Snort\etc\snort.conf -A console** command



As seen above when the machine was pinged with another on the local network with the blacklisted ip 192.168.0.184 snort raised an alert. Exit by pressing **cntl+c**

