Title: Installation and Configuration of Snort for Network Security and Protection against Cyber Threats

Objective:

The objective of this experiment is to install and configure Snort, an open-source intrusion detection and prevention system, for enhancing network security and providing protection against cyber threats.

Requirements:

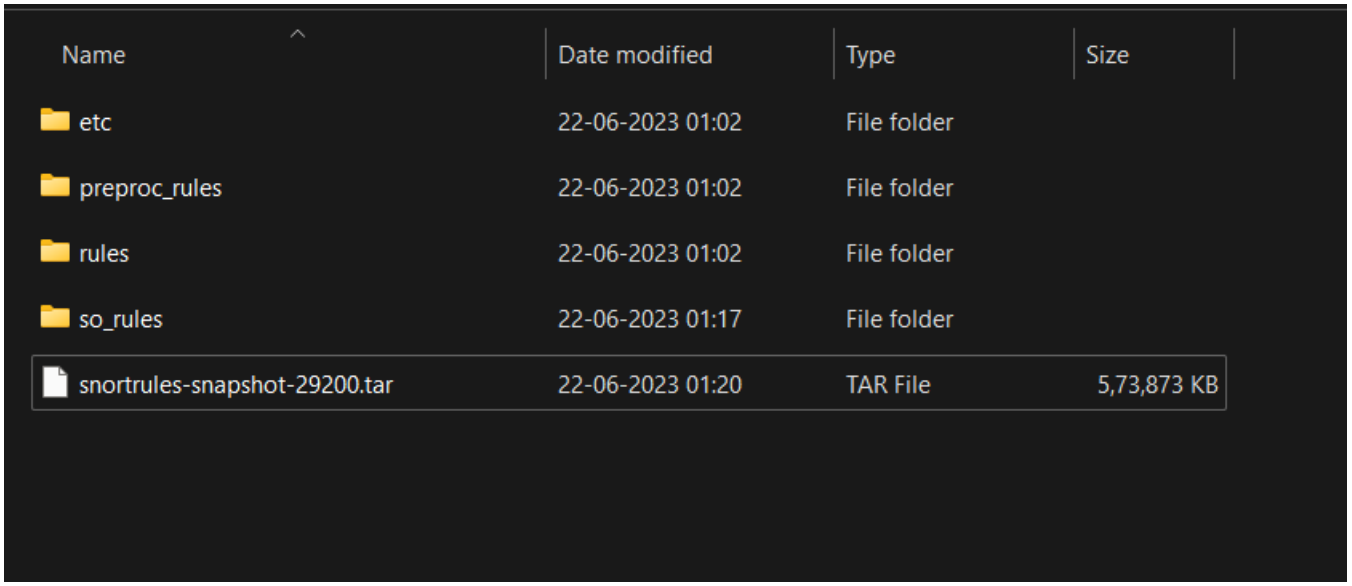
Snort installer

Procedure/Experiment Steps:

1. Download the latest version of Snort from the official website.
2. Launch the installer and follow instructions to install Snort.
3. Install Npcap because it's require for snort.
4. After installing Snort and Npcap. In command prompt open c:\ drive enter these commands in Command prompt to check snorts working
    a. cd snort
    b. cd bin
    c. snort -v

```
C:\Users\dhava>cd ..

C:\Users>cd ..

C:\>cd Snort

C:\Snort>cd bin

C:\Snort\bin>snort
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{AE347C8D-8D5E-4A4A-A887-CDE39C0AA904}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=9352)
```

    d. As we can see snort installed successfully
5. After installing Snort on Windows 10, Another important step to get started with Snort is configuring
    a. Go to "https://www.snort.org/downloads/#rule-downloads" and download latest snort rule file
    b. Extract 3 folders from the downloaded snortrules-snapshot-29200.tar folder into the Snorts corresponding folders in C drive.



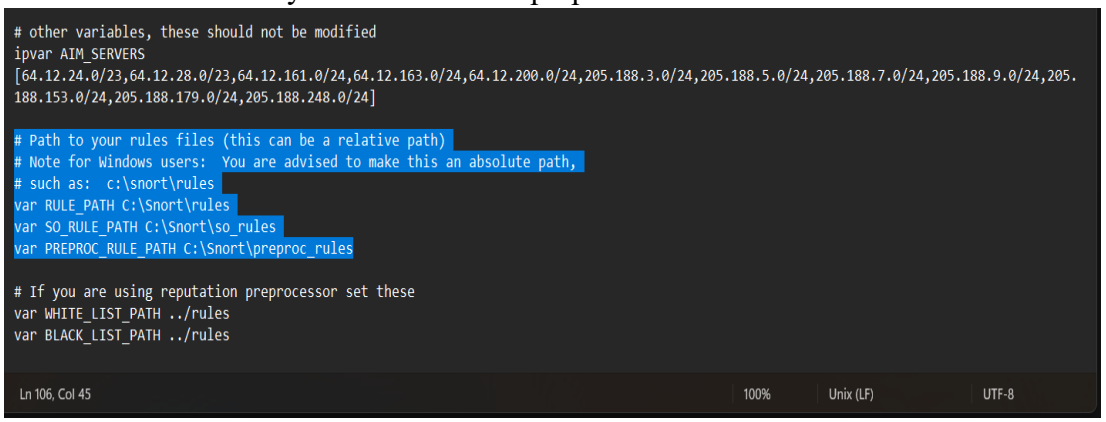
c. rules folder contains the rules files and the most important local.rules file. Which we will use to enter all our rules.

d. etc folder contains all configuration files and the most important file is snort.conf file which we will use for configuration

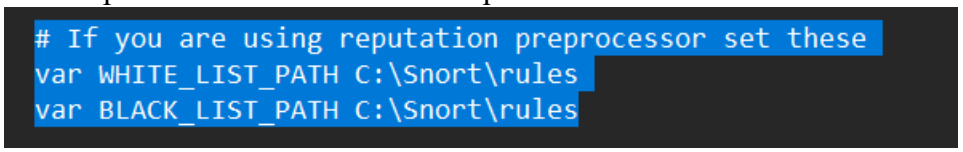
6. Now open the snort.conf file through the notepad++ editor or any other text editor to edit configurations of snort to make it work like we want it to.

a. Setup the network addresses you are protecting

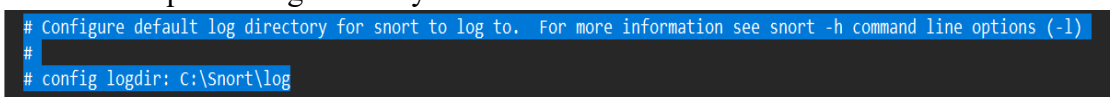
b. define the directory for our rules and preproc rules folder



c. setup our white list and black list path it will be in our snorts' rule folder



d. enable log directory, so that we store logs in our log folder. Uncomment this line and set absolute path to log directory



e. set the path to dynamic preprocessors and dynamic engine

```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor
```

f. do same thing for dynamic preprocessor engine

```
# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine
```

g. Converted back slashes to forward slashes in this entire step

```
##################################################
# Step #7: Customize your rule set
# For more information, see Snort Manual, Writing Snort Rules
#
# NOTE: All categories are enabled in this conf file
##################################################

# site specific rules
include $RULE_PATH/local.rules

include $RULE_PATH\app-detect.rules
include $RULE_PATH\attack-responses.rules
include $RULE_PATH\backdoor.rules
include $RULE_PATH\bad-traffic.rules
include $RULE_PATH\blacklist.rules
include $RULE_PATH\botnet-cnc.rules
include $RULE_PATH\browser-chrome.rules
include $RULE_PATH\browser-firefox.rules
include $RULE_PATH\browser-ie.rules
include $RULE_PATH\browser-other.rules
```

h. Again just convert forward slashes to backslashes and uncomment the lines below:

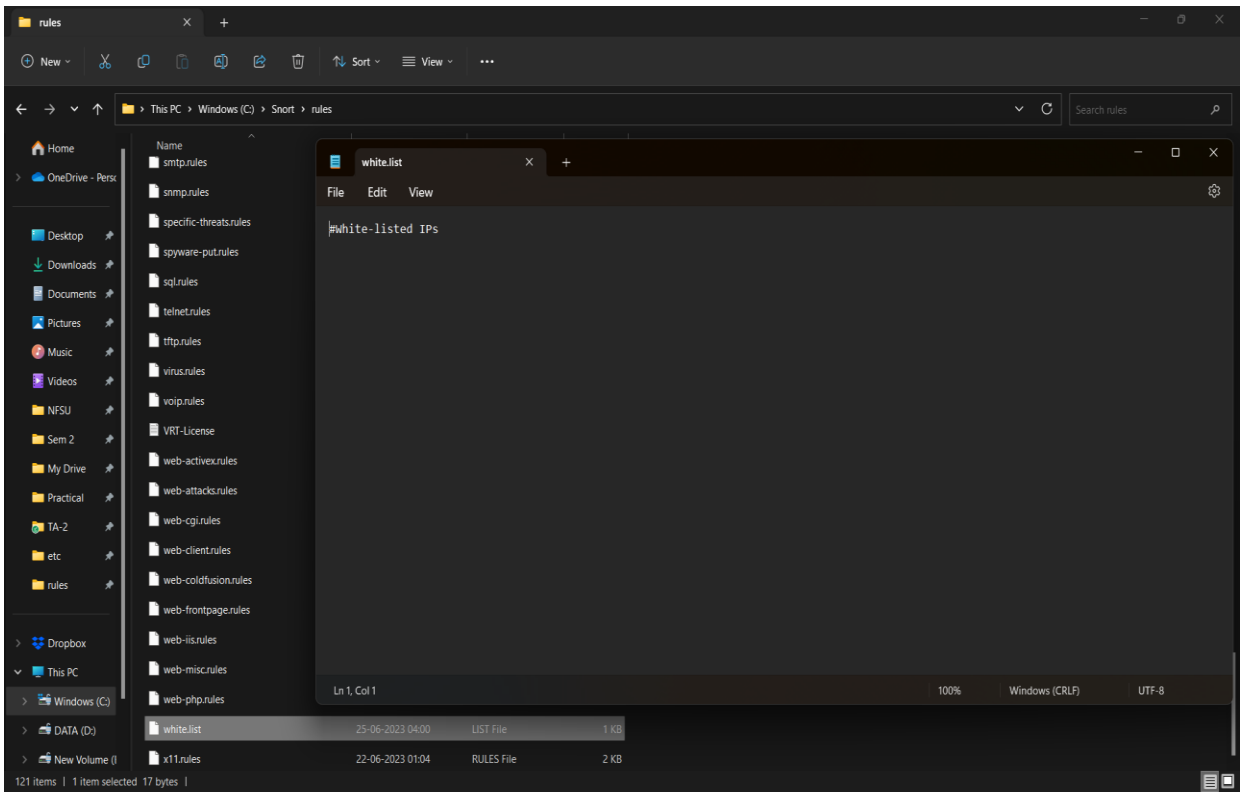
```
##################################################
# Step #8: Customize your preprocessor and decoder alerts
# For more information, see README.decoder_preproc_rules
##################################################

# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH\preprocessor.rules
# include $PREPROC_RULE_PATH\decoder.rules
# include $PREPROC_RULE_PATH\sensitive-data.rules
```

i. Now we just need to verify the presence of this command at the bottom of snort.conf file.

```
# include $SO_RULE_PATH/server-mysql.rules
# include $SO_RULE_PATH/server-oracle.rules
# include $SO_RULE_PATH/server-other.rules
# include $SO_RULE_PATH/server-webapp.rules

# Event thresholding or suppression commands. See threshold.conf
include threshold.conf
```

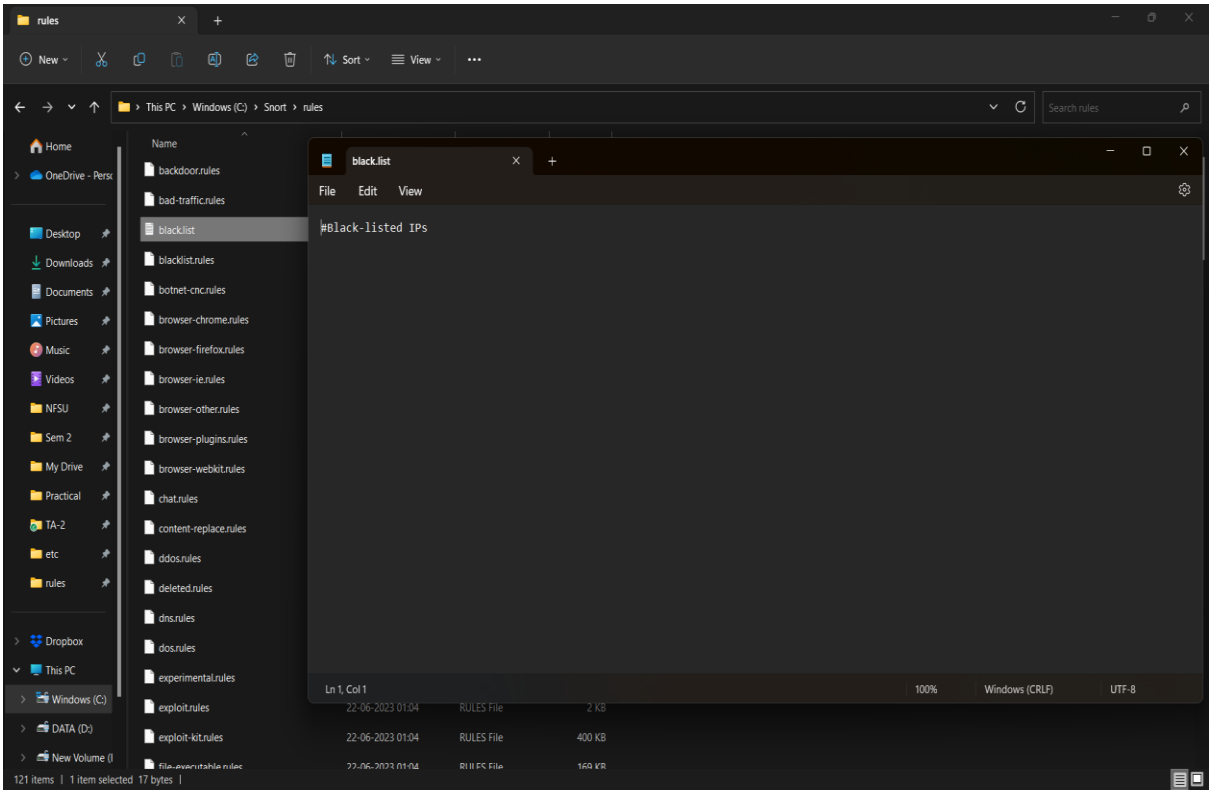
J. Click on Save file and save all changes to save the configuration file (snort.conf).

7. Now recalling the Step 13 white list , black list are not rules they are just the list of IP addresses labelled as black or white right now these files don't exist in our rule path which is why we have to create them manually , save them in this folder C:\Snort\rules.
    a. White-List
        i. Go to Notepad++ and create new file.
        ii. Comment it #White-listed IPs.
        iii. Name the file white.list and save the file.



    b. Black-List

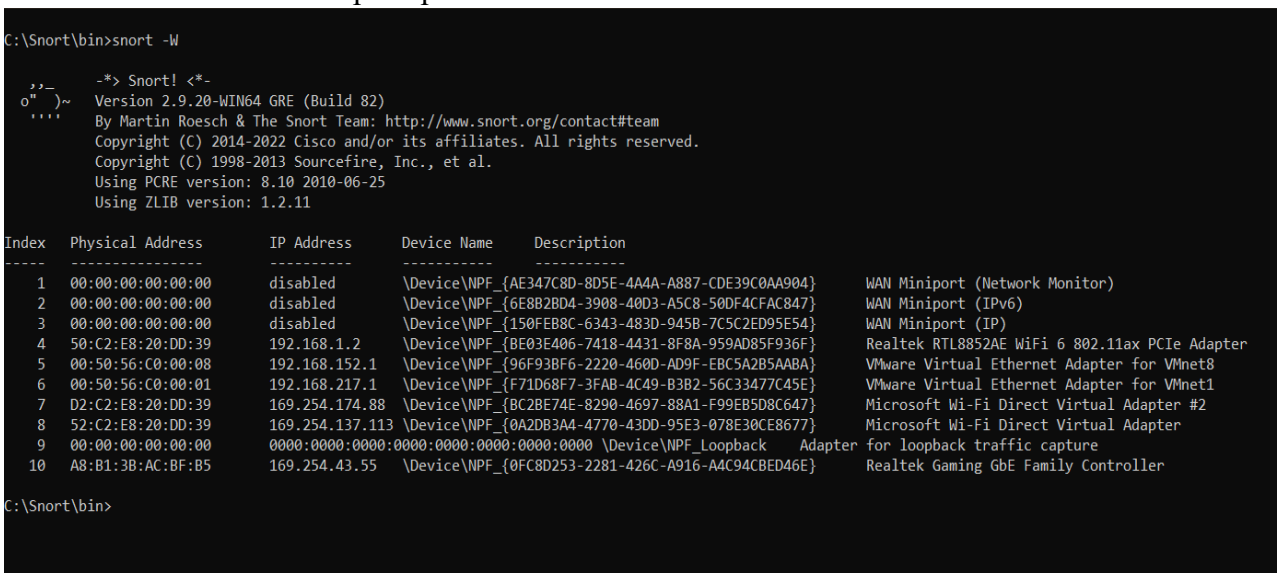
i. Create another new file.
ii. Comment it #Black-listed IPs.
iii. Name the file black.list and save the file.



8. Now we test snort again by running Command prompt as admin. To check if it's running fine after all the configurations.

```
C:\>cd Snort

C:\Snort>cdc bin
'cdc' is not recognized as an internal or external command,
operable program or batch file.

C:\Snort>cd  bin

C:\Snort\bin>snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{AE347C8D-8D5E-4A4A-A887-CDE39C0AA904}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.20-WIN64 GRE (Build 82)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.11

Commencing packet processing (pid=17656)
```

- We can also the check the wireless interface cards from which we will be using snort by using the command below we can see the list of our wireless interface cards through entering this command in command prompt.



Result:

By monitoring the network traffic using Snort, the system can detect and analyse various types of cyber threats, including intrusion attempts, malware activity, and suspicious network behaviours. The Snort alerts and log files provide valuable information for security analysts to investigate and respond to potential security incidents.

Conclusion:

The installation and configuration of Snort as an intrusion detection and prevention system significantly enhance network security and provide protection against cyber threats. Snort's ability to monitor and analyse network traffic helps in identifying and mitigating potential security risks in real-time.

Future Scope:

1. Continuously update the Snort ruleset to keep up with the latest threats and attack techniques.
2. Integrate Snort with other security tools, such as SIEM (Security Information and Event Management) systems, for centralized security monitoring and incident response.
3. Explore advanced features of Snort, such as protocol analysis and anomaly detection, to enhance network security capabilities.
4. Conduct regular audits and assessments to ensure the effectiveness of Snort in protecting the network against emerging cyber threats.