

# 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 required 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 ===

o''-  -*> 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.

Name	Date modified	Type	Size
etc	22-06-2023 01:02	File folder	
preproc_rules	22-06-2023 01:02	File folder	
rules	22-06-2023 01:02	File folder	
so_rules	22-06-2023 01:17	File folder	
snortrules-snapshot-29200.tar	22-06-2023 01:20	TAR File	5,73,873 KB

- 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

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.217.1
```

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

```
# other variables, these should not be modified
ipvar AIM_SERVERS
[64.12.24.0/23,64.12.28.0/23,64.12.161.0/24,64.12.163.0/24,64.12.200.0/24,205.188.3.0/24,205.188.5.0/24,205.188.7.0/24,205.188.9.0/24,205.188.153.0/24,205.188.179.0/24,205.188.248.0/24]

# Path to your rules files (this can be a relative path)
# Note for Windows users: You are advised to make this an absolute path,
# such as: c:\snort\rules
var RULE_PATH C:\Snort\rules
var SO_RULE_PATH C:\Snort\so_rules
var PREPROC_RULE_PATH C:\Snort\preproc_rules

# If you are using reputation preprocessor set these
var WHITE_LIST_PATH ../rules
var BLACK_LIST_PATH ../rules
```

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

```
# If you are using reputation preprocessor set these
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
```

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

```
# Configure default log directory for snort to log to. For more information see snort -h command line options (-l)
#
# config logdir: C:\Snort\log
```

- 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

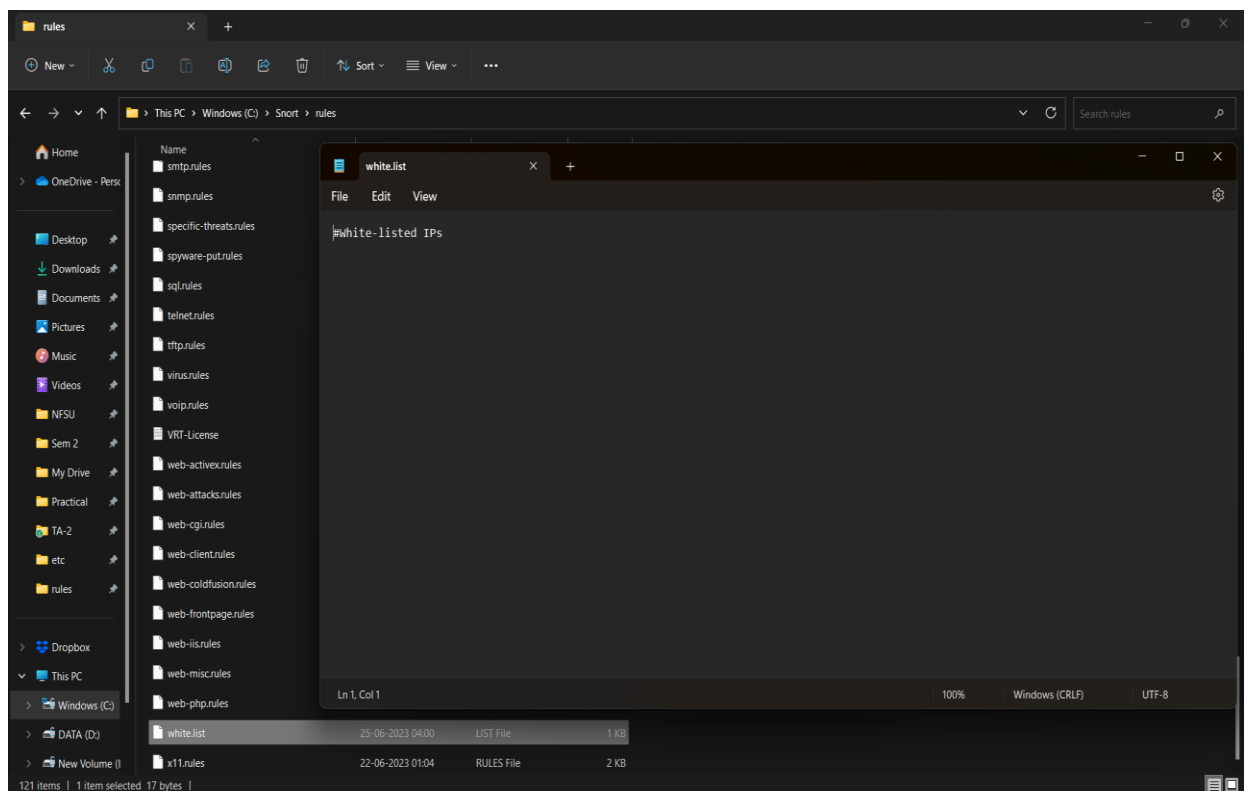
# Event thresholding or suppression commands. See threshold.conf
include threshold.conf
```

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.

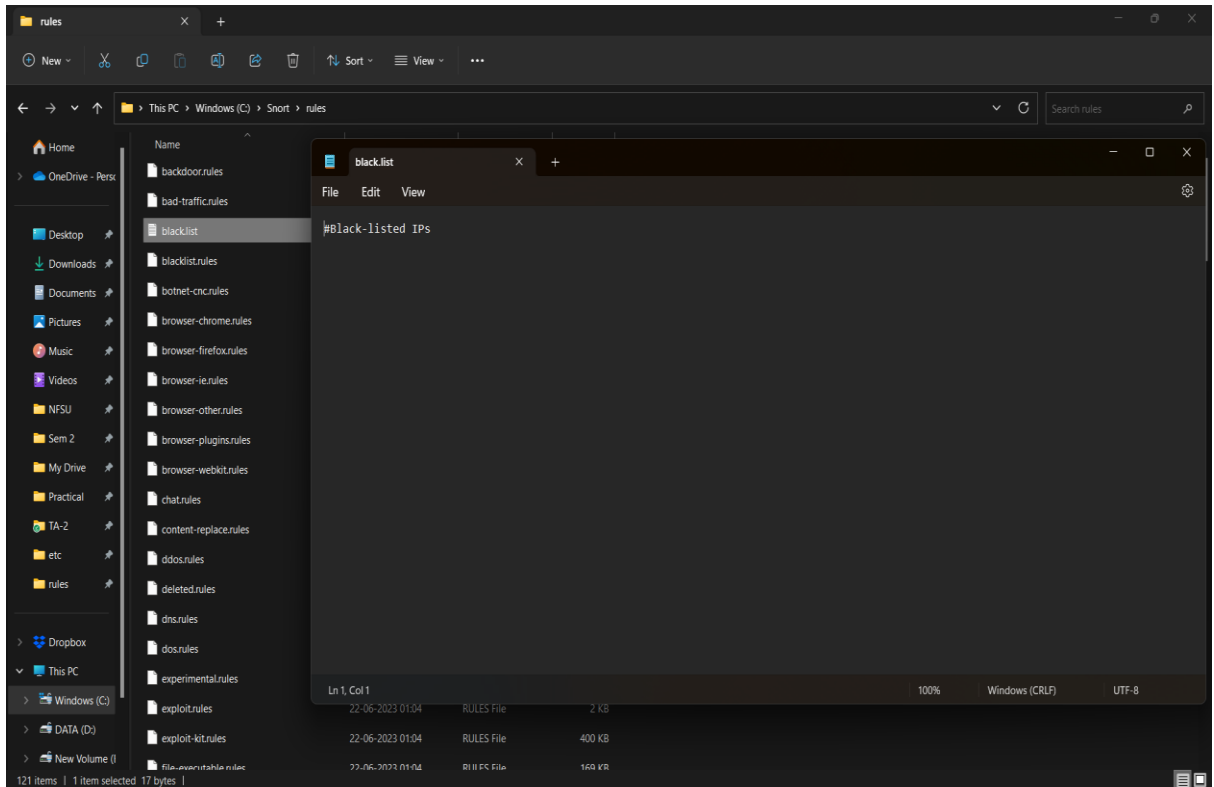
a. White-List

- 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 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.

```
C:\Snort\bin>snort -W

      _.-*-> Snort! <*-
    o"  )~ Version 2.9.20-WIN64 GRE (Build 82)
    ""' 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

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:00:00:00:00:00      disabled      \Device\NPF_{AE347C8D-8D5E-4A4A-A887-CDE39C0AA904}  WAN Miniport (Network Monitor)
2      00:00:00:00:00:00      disabled      \Device\NPF_{6E8B2BD4-3908-40D3-A5C8-50DF4CFAC847}  WAN Miniport (IPv6)
3      00:00:00:00:00:00      disabled      \Device\NPF_{150FEB8C-6343-483D-945B-7C5C2ED95E54}  WAN Miniport (IP)
4      50:C2:E8:20:DD:39      192.168.1.2    \Device\NPF_{BE03E406-7418-4431-8F8A-959AD85F936F}  Realtek RTL8852AE WiFi 6 802.11ax PCIe Adapter
5      00:50:56:C0:00:08      192.168.152.1  \Device\NPF_{96F93BF6-2220-460D-AD9F-EBC5A2B5AABA}  VMware Virtual Ethernet Adapter for VMnet8
6      00:50:56:C0:00:01      192.168.217.1  \Device\NPF_{F71D68F7-3FAB-4C49-B3B2-56C33477C45E}  VMware Virtual Ethernet Adapter for VMnet1
7      D2:C2:E8:20:DD:39      169.254.174.88 \Device\NPF_{BC2BE74E-8290-4697-88A1-F99EB5D8C647}  Microsoft Wi-Fi Direct Virtual Adapter #2
8      52:C2:E8:20:DD:39      169.254.137.113 \Device\NPF_{0A2DB3A4-4770-43D0-95E3-078E30CE8677}  Microsoft Wi-Fi Direct Virtual Adapter
9      00:00:00:00:00:00      0000:0000:0000:0000:0000:0000 \Device\NPF_{Loopback} Adapter for loopback traffic capture
10     A8:B1:3B:AC:BF:B5      169.254.43.55  \Device\NPF_{0FC8D253-2281-426C-A916-A4C94CBED46E}  Realtek Gaming GbE Family Controller

C:\Snort\bin>
```

## 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.