ASSIGNMENT NO. 4
(43152)

TITLE :
Configure and demonstrate Snort tool for intrusion.

AIM :
Configure and demonstrate use of vulnerability assessment tools such as Snort tool for intrusion.

OBJECTIVE :
Study any vulnerability assessment tool such as Snort tool and use its implementation features.

THEORY :

Introduction
Snort is a popular choice for running a network intrusion detection system or NIDS for short. It monitors the package data sent and received through a specific network interface. NIDS can catch threats targeting your system vulnerabilities using signature-based detection and protocol analysis technologies. NIDS software, when installed and configured appropriately, can identify the latest attacks, malware infections, compromised systems, and network policy violations.

Platforms on which Snort runs

- Snort runs on most UNIX and various windows.
- UNIX
    - Applet, MAC, BEOS, JBM, AIX, BSD open etc.
- LINUX
    - Mandrake LINUX, Red Hat, SUSE LINUX etc.
- WINDOWS
    - Windows server 2003/XP/2000/NT

What can I do with Snort?

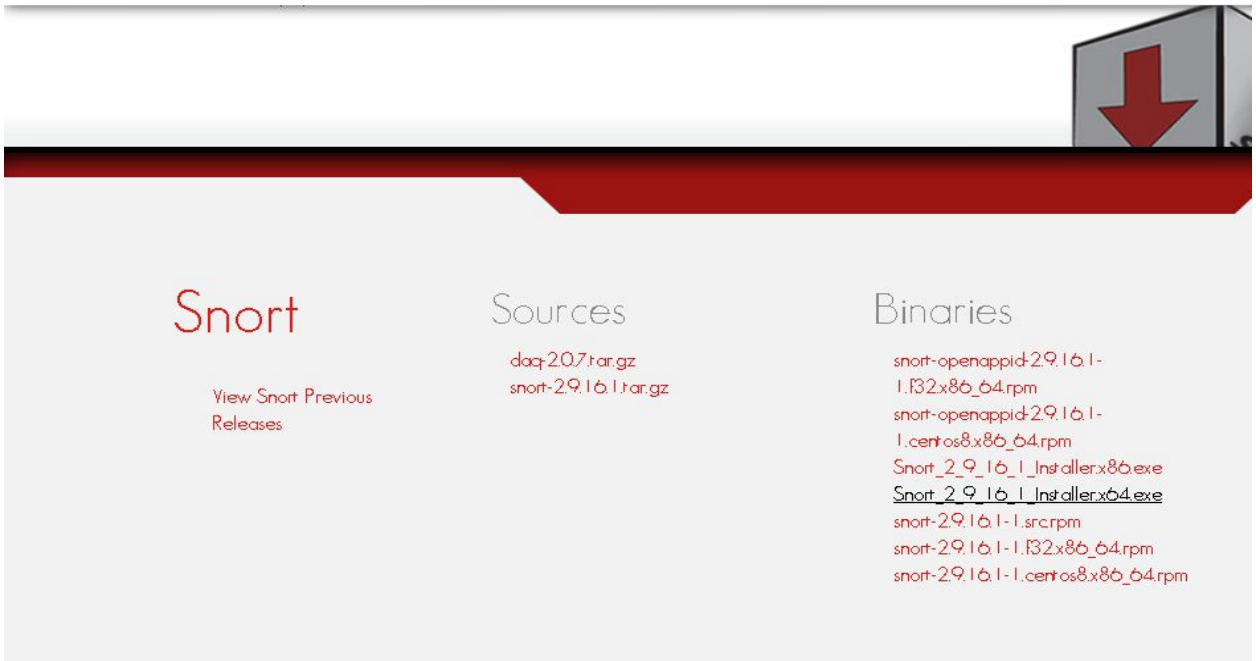
Snort has three primary uses:

- It can be used as a straight packet sniffer like tcpdump.
- A packet logger (useful for network traffic debugging, etc).
- As a full blown network intrusion prevention system.

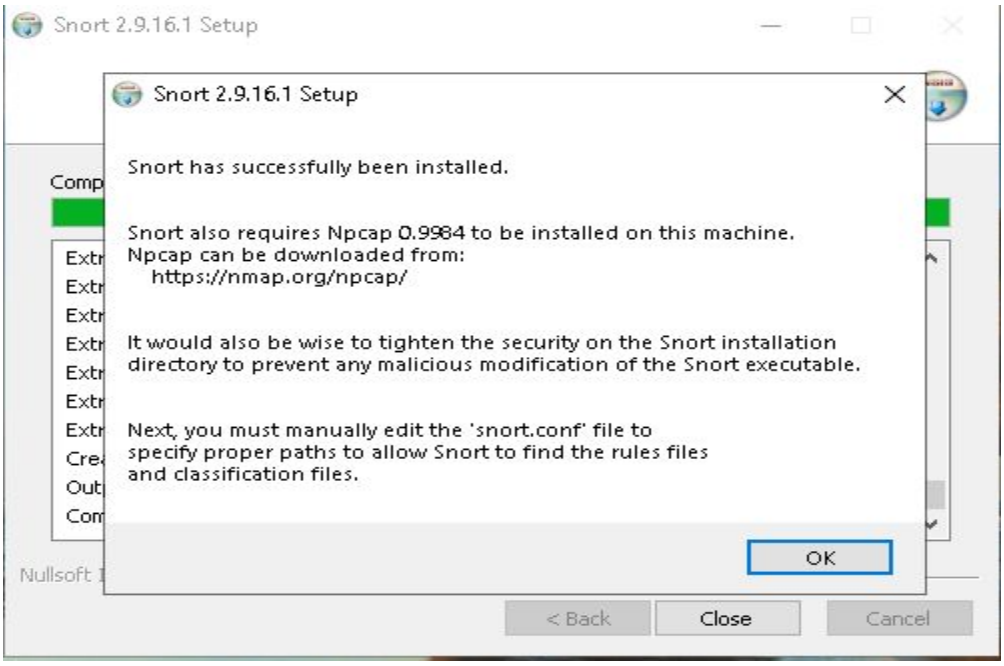
Installation

The installation and configuration of Snort :

- Download snort from it main website : https://www.snort.org/downloads

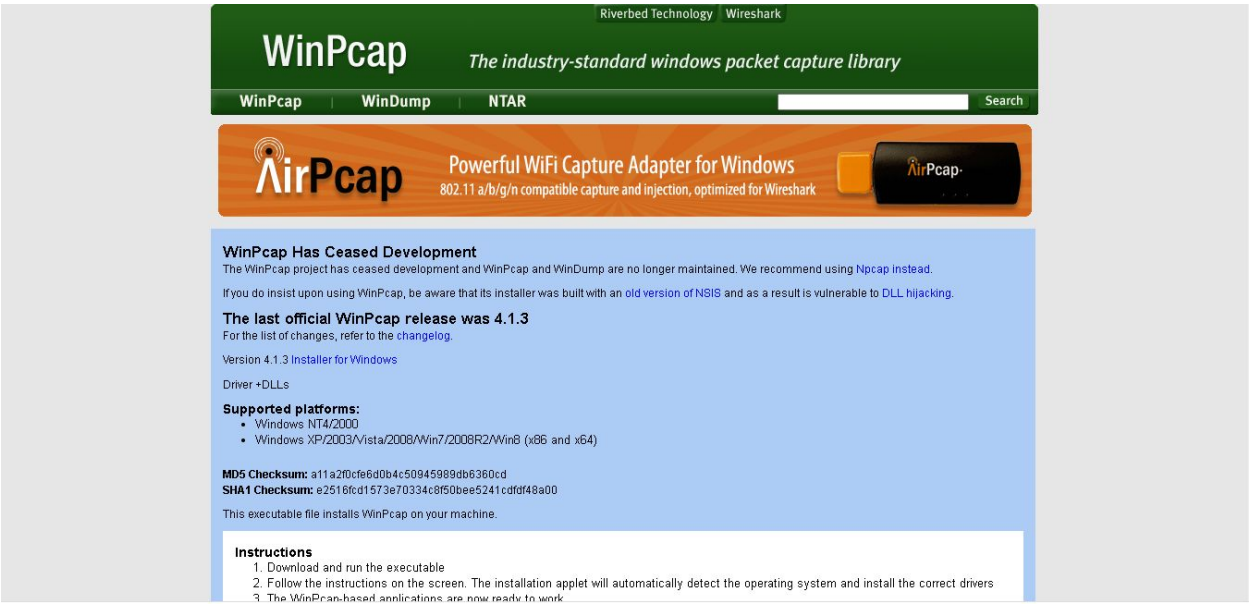


- Install this package (Snort_2_9_16_1_Installer.x86.exe)

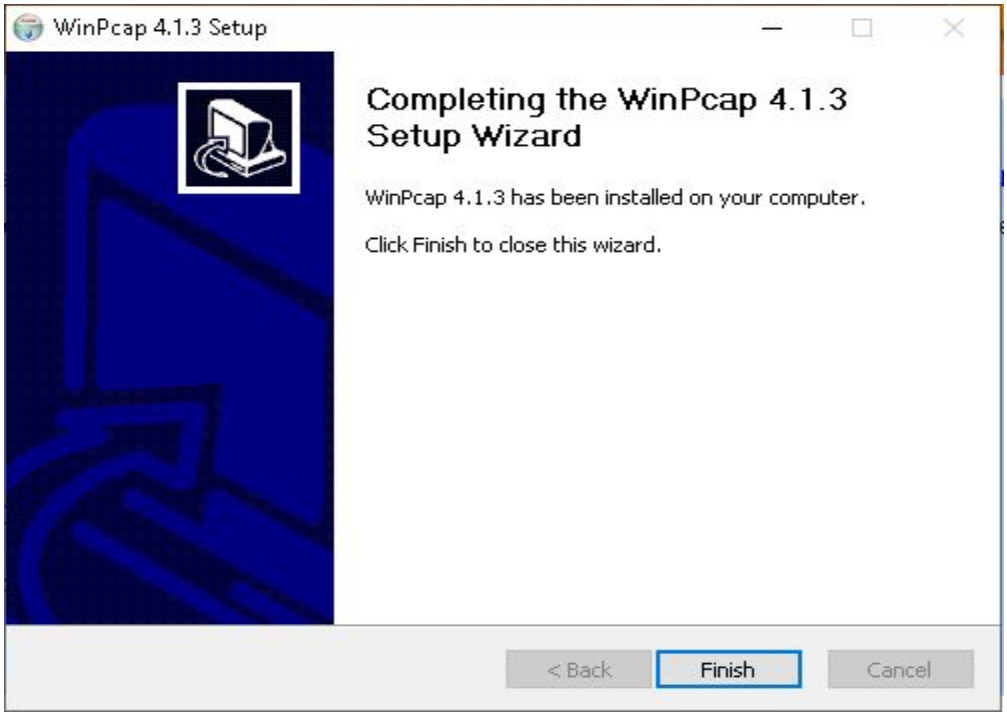


Installation of WinpCap :

- Download WinpCap from main website : https://www.winpcap.org/install



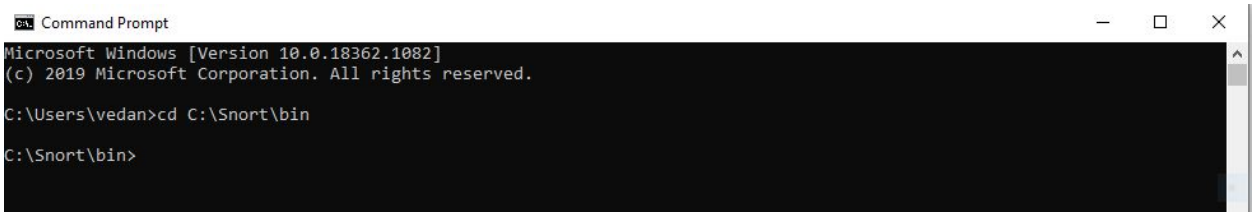
- Click on the version 4.1.3 for windows



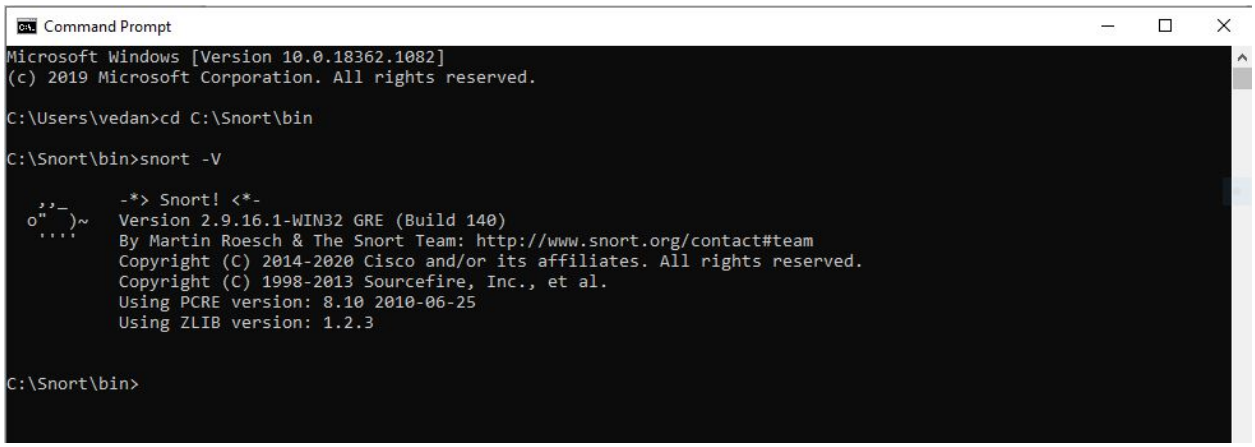
- Restart the computer

Check Snort Installation:

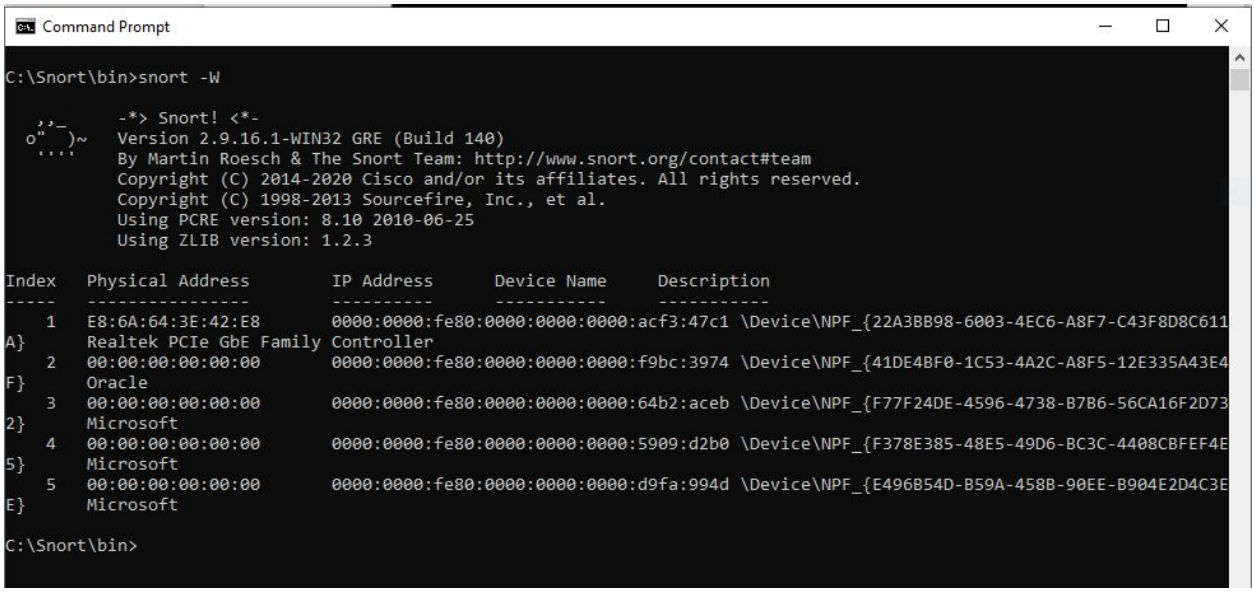
- Open command prompt as administrator
- Change directory to C:\Snort\bin



- Check for the Snort version.



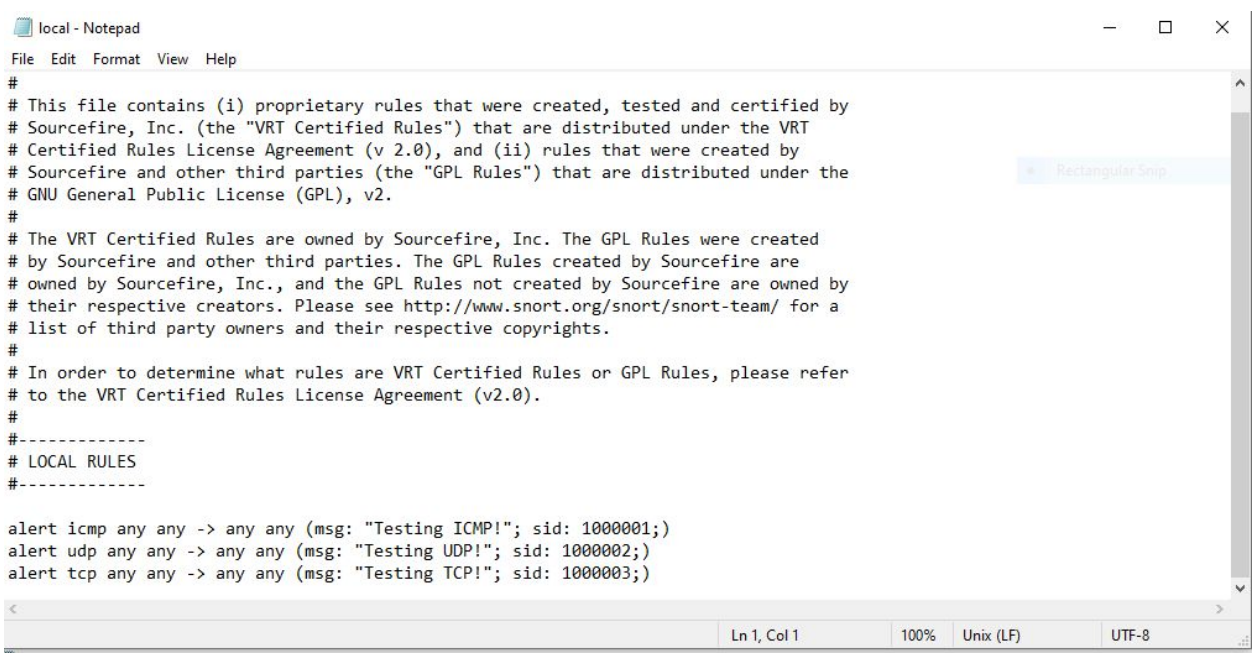
- Check interfaces from which we will test snort.



```
Command Prompt

C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.16.1-WIN32 GRE (Build 140)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2020 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: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   E8:6A:64:3E:42:E8       0000:0000:fe80:0000:0000:0000:acf3:47c1 \Device\NPF_{22A3BB98-6003-4EC6-A8F7-C43F8D8C611
A}      Realtek PCIe GbE Family Controller
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:f9bc:3974 \Device\NPF_{41DE4BF0-1C53-4A2C-A8F5-12E335A43E4
F}      Oracle
    3   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:64b2:aceb \Device\NPF_{F77F24DE-4596-4738-B7B6-56CA16F2D73
2}      Microsoft
    4   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:5909:d2b0 \Device\NPF_{F378E385-48E5-49D6-BC3C-4408CBFEF4E
5}      Microsoft
    5   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:d9fa:994d \Device\NPF_{E496B54D-B59A-458B-90EE-B904E2D4C3E
E}      Microsoft

C:\Snort\bin>
```

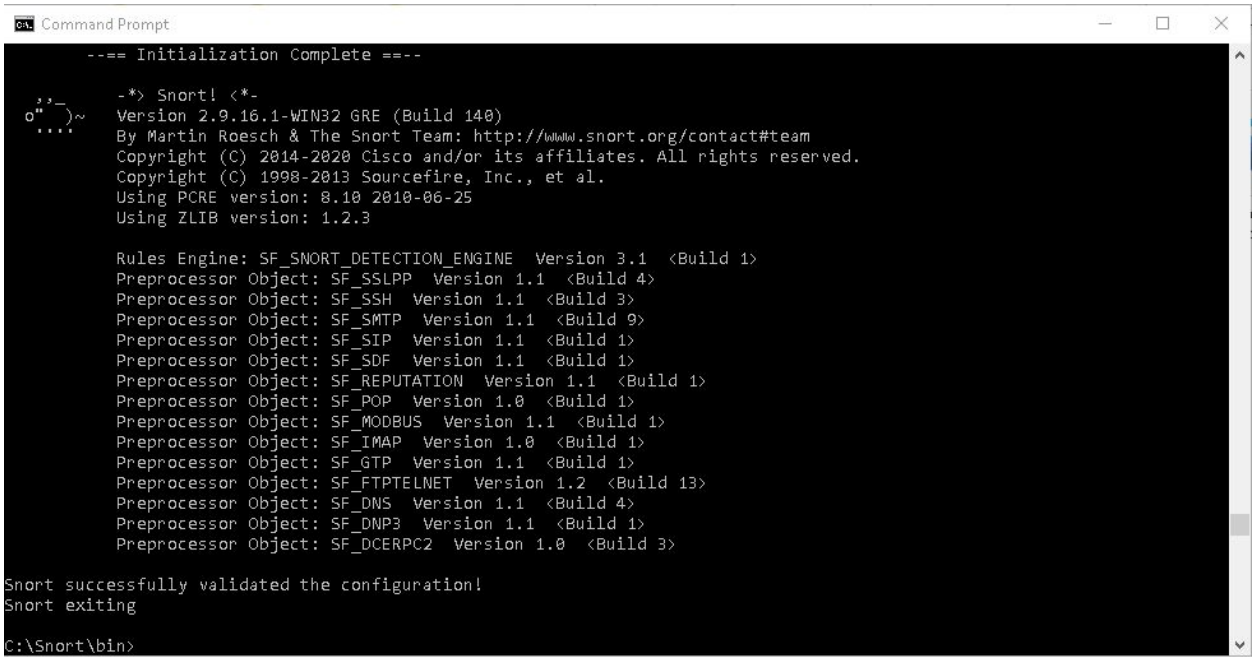
The Snort Rule configuration:

- Open the local rules file from C:\Snort\rules\local.rules
- Type the following rules

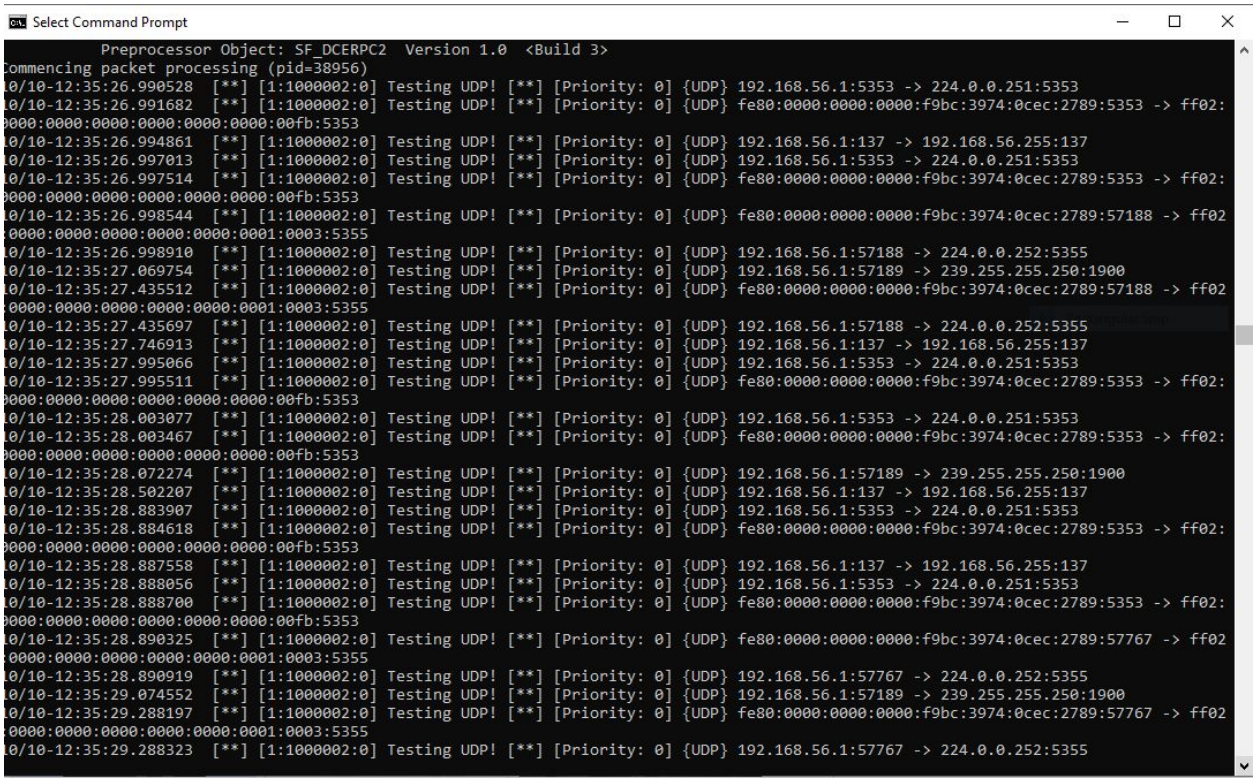


```
local - Notepad
File  Edit  Format  View  Help
#
# This file contains (i) proprietary rules that were created, tested and certified by
# Sourcefire, Inc. (the "VRT Certified Rules") that are distributed under the VRT
# Certified Rules License Agreement (v 2.0), and (ii) rules that were created by
# Sourcefire and other third parties (the "GPL Rules") that are distributed under the
# GNU General Public License (GPL), v2.
#
# The VRT Certified Rules are owned by Sourcefire, Inc. The GPL Rules were created
# by Sourcefire and other third parties. The GPL Rules created by Sourcefire are
# owned by Sourcefire, Inc., and the GPL Rules not created by Sourcefire are owned by
# their respective creators. Please see http://www.snort.org/snort/snort-team/ for a
# list of third party owners and their respective copyrights.
#
# In order to determine what rules are VRT Certified Rules or GPL Rules, please refer
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------

alert icmp any any -> any any (msg: "Testing ICMP!"; sid: 1000001;)
alert udp any any -> any any (msg: "Testing UDP!"; sid: 1000002;)
alert tcp any any -> any any (msg: "Testing TCP!"; sid: 1000003;)
Ln 1, Col 1   100%   Unix (LF)   UTF-8
```

- Run the command
  snort –i 2 –c c:\Snort\etc\snort.conf -T



- Run the command
  snort –i 1 –c c:\Snort\etc\snort.conf -A console
- Let the command run for sometime and press ctrl+c.
- The following is displayed on the console as the above command mentions that the output be written to the console.



```
Select Command Prompt
          Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=38956)
10/10-12:35:26.990528  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:5353 -> 224.0.0.251:5353
10/10-12:35:26.991682  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:5353 -> ff02:
0000:0000:0000:0000:0000:0000:00fb:5353
10/10-12:35:26.994861  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:137 -> 192.168.56.255:137
10/10-12:35:26.997013  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:5353 -> 224.0.0.251:5353
10/10-12:35:26.997514  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:5353 -> ff02:
0000:0000:0000:0000:0000:0000:00fb:5353
10/10-12:35:26.998544  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:57188 -> ff02
:0000:0000:0000:0000:0000:0001:0003:5355
10/10-12:35:26.998910  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:57188 -> 224.0.0.252:5355
10/10-12:35:27.069754  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:57189 -> 239.255.255.250:1900
10/10-12:35:27.435512  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:57188 -> ff02
:0000:0000:0000:0000:0000:0001:0003:5355
10/10-12:35:27.435697  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:57188 -> 224.0.0.252:5355
10/10-12:35:27.746913  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:137 -> 192.168.56.255:137
10/10-12:35:27.995066  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:5353 -> 224.0.0.251:5353
10/10-12:35:27.995511  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:5353 -> ff02:
0000:0000:0000:0000:0000:0000:00fb:5353
10/10-12:35:28.003077  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:5353 -> 224.0.0.251:5353
10/10-12:35:28.003467  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:5353 -> ff02:
0000:0000:0000:0000:0000:0000:00fb:5353
10/10-12:35:28.072274  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:57189 -> 239.255.255.250:1900
10/10-12:35:28.502207  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:137 -> 192.168.56.255:137
10/10-12:35:28.883907  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:5353 -> 224.0.0.251:5353
10/10-12:35:28.884618  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:5353 -> ff02:
0000:0000:0000:0000:0000:0000:00fb:5353
10/10-12:35:28.887558  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:137 -> 192.168.56.255:137
10/10-12:35:28.888056  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:5353 -> 224.0.0.251:5353
10/10-12:35:28.888700  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:5353 -> ff02:
0000:0000:0000:0000:0000:0000:00fb:5353
10/10-12:35:28.890325  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:57767 -> ff02
:0000:0000:0000:0000:0000:0001:0003:5355
10/10-12:35:28.890919  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:57767 -> 224.0.0.252:5355
10/10-12:35:29.074552  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:57189 -> 239.255.255.250:1900
10/10-12:35:29.288197  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} fe80:0000:0000:0000:f9bc:3974:0cec:2789:57767 -> ff02
:0000:0000:0000:0000:0000:0001:0003:5355
10/10-12:35:29.288323  [**] [1:1000002:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.56.1:57767 -> 224.0.0.252:5355
```

- It is successfully working.

CONCLUSION :

The installation and the demonstration of the snort is successfully done.