CL7 Assignment 4

Name: Anish Kulkarni
Roll Number: 43227
Batch: Q10
Class: BE 10

Title:

Configuration and Demonstration of Snort as an Intrusion Detection System

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

Uses of Snort:

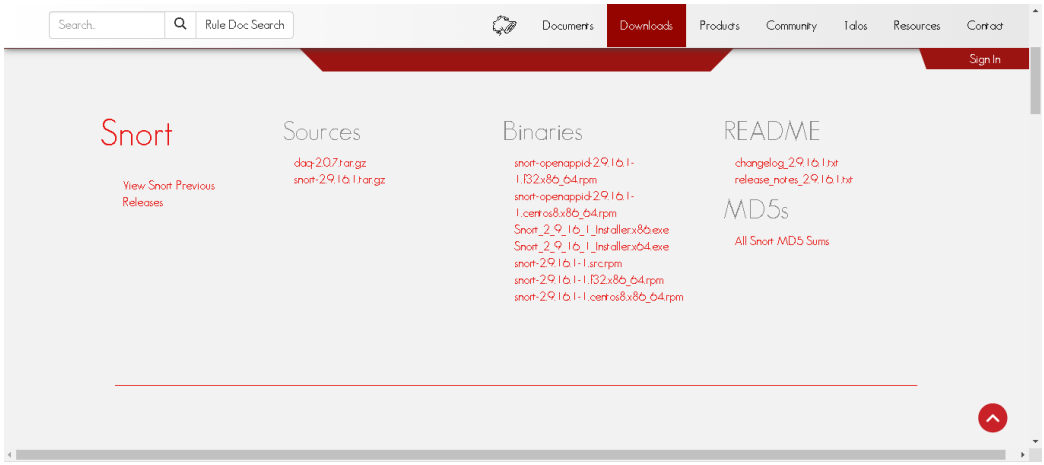
Snort has three primary uses:

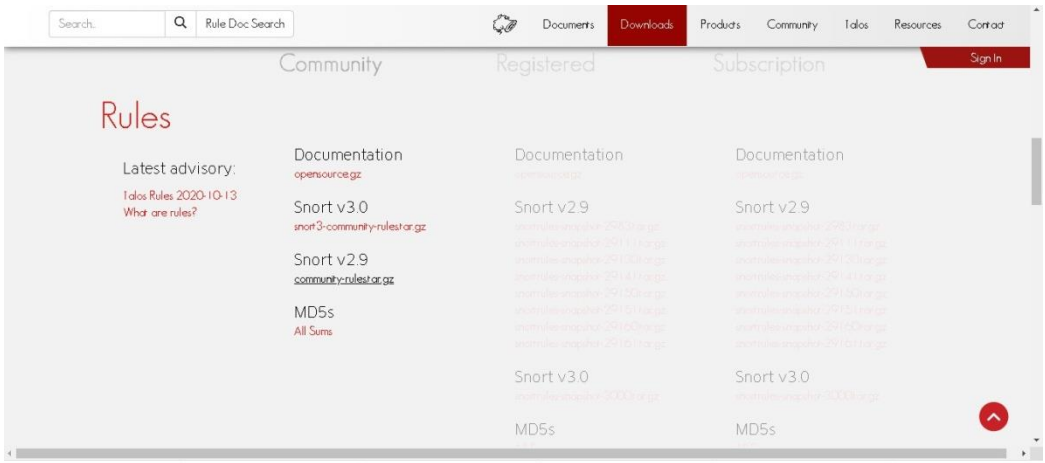
- It can be used as a straight packet sniffer like tcpdump.
- A packet logger (useful for network traffic debugging, etc).
- As a full blown network intrusion prevention system.

Installation:

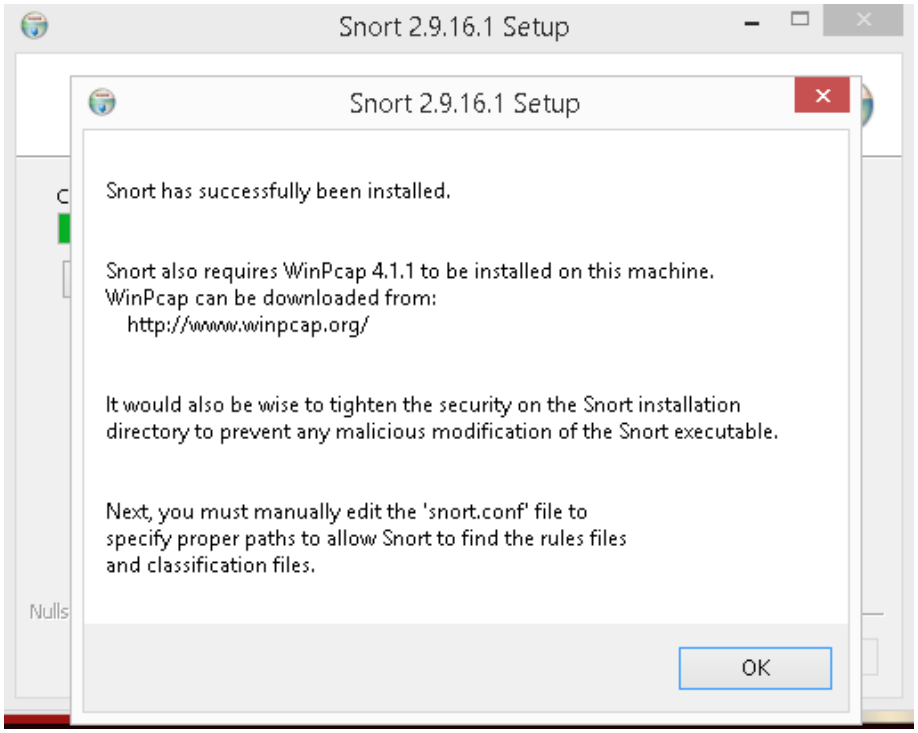
The installation and configuration of Snort :

Download snort and rules from main website:
https://www.snort.org/downloads





Install this package (Snort_2_9_16_1_Installer.x86.exe)

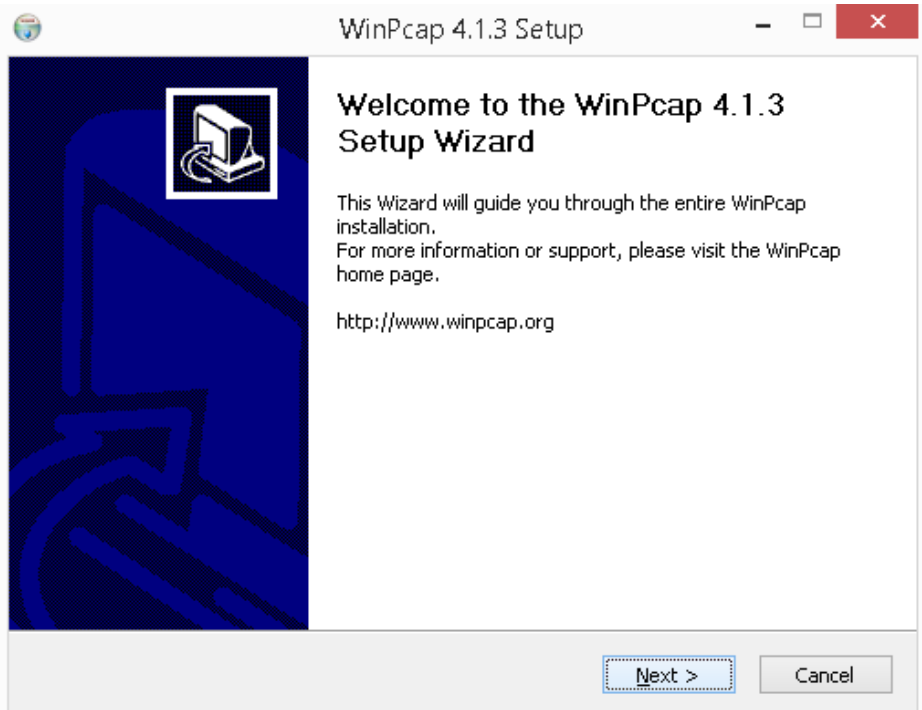


Installation of WinPcap:

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.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.10240]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Snort\bin

C:\Snort\bin>
```

Check for the Snort version.

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

   ,,_     -*> 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


C:\Snort\bin>
```

Check interfaces from which we will test snort.

```
Administrator: Command Prompt
          Using PCRE version: 8.10 2010-06-25
          Using ZLIB version: 1.2.3


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   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:8488:47b0 \Device\NPF_{D7E953F6-A614-4AD3-B111-D39460B5F45
6}      Microsoft
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:4116:3651 \Device\NPF_{8B0D7C92-A93D-4239-AE63-979BF033835
A}      Microsoft
    3   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:6963:d3f7 \Device\NPF_{CA33EBA0-9938-4546-9DF1-6A6A8AADB99
B}      Microsoft
    4   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:3de6:8461 \Device\NPF_{95FC514E-D593-4E39-B4EF-8EFB9C560B7
2}      Realtek PCIe GBE Family Controller
    5   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:899e:59ef \Device\NPF_{0633F5E1-48AC-4811-9EDB-C4F60C9175E
5}      Microsoft
    6   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:d4dd:78e1 \Device\NPF_{FB702E91-DC54-4CC6-BAF2-856DE315C1A
3}      Oracle

C:\Snort\bin>
```

The Snort Rule configuration:

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

```
snort.conf   local.rules   white.list   black.list

# Copyright 2001-2020 Sourcefire, Inc. All Rights Reserved.
#
# 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 tcp any any -> any any (msg: "Testing TCP!"; sid: 1000002;)
alert udp any any -> any any (msg: "Testing UDP!"; sid: 1000003;)
```

Run the command snort –i 1 –c c:\Snort\etc\snort.conf -T > C:\Snort\log\pingtest.txt on the cmd.

```
Command Prompt - snort -i 1 -c c:\Snort\etc\snort.conf -T
Loading dynamic engine c:\Snort\lib\snort_dynamicengine\sf_engine.dll... done
Loading all dynamic preprocessor libs from c:\Snort\lib\snort_dynamicpreprocessor...
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dce2.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dnp3.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_dns.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ftptelnet.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_gtp.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_imap.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_modbus.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_pop.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_reputation.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_sdf.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_sip.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_smtp.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ssh.dll... done
  Loading dynamic preprocessor library c:\Snort\lib\snort_dynamicpreprocessor\sf_ssl.dll... done
  Finished Loading all dynamic preprocessor libs from c:\Snort\lib\snort_dynamicpreprocessor
Log directory = c:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:

  Finished Loading all dynamic preprocessor libs from c:\Snort\lib\snort_dynamicpreprocessor
Log directory = c:\Snort\log
Frag3 global config:
    Max frags: 65536
    Fragment memory cap: 4194304 bytes
Frag3 engine config:
```

Let the command run for sometime and press ctrl+c.

Open the file C:\Snort\log\pingtest.txt.

```
snort.conf   local.rules   pingtest.txt   white.list   black.list
1  10/05-00:51:38.679653  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 52.114.14.121:443 -> 192.168.43.52:50406
2  10/05-00:51:38.729671  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 192.168.43.52:50406 -> 52.114.14.121:443
3  10/05-00:51:38.776282  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 192.168.43.52:50406 -> 52.114.14.121:443
4  10/05-00:51:38.947566  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 52.114.14.121:443 -> 192.168.43.52:50406
5  10/05-00:51:41.236976  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 2404:6800:4009:0812:0000:0000:0000:200e:443 ->
   2405:0204:9511:ea78:fd33:63f3:c118:b910:50494
6  10/05-00:51:41.237138  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 2404:6800:4009:0812:0000:0000:0000:200e:443 ->
   2405:0204:9511:ea78:fd33:63f3:c118:b910:50494
7  10/05-00:51:41.237139  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 2404:6800:4009:0812:0000:0000:0000:200e:443 ->
   2405:0204:9511:ea78:fd33:63f3:c118:b910:50494
8  10/05-00:51:41.237178  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 2405:0204:9511:ea78:fd33:63f3:c118:b910:50494 ->
   2404:6800:4009:0812:0000:0000:0000:200e:443
9  10/05-00:51:42.255502  [**] [1:1000003:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.43.52:15350 -> 77.109.122.154:1270
10 10/05-00:51:42.839535  [**] [1:1000003:0] Testing UDP! [**] [Priority: 0] {UDP} 77.109.122.154:1270 -> 192.168.43.52:15350
11 10/05-00:51:46.238090  [**] [1:1000001:0] Testing ICMP! [**] [Priority: 0] {IPV6-ICMP} fe80:0000:0000:0000:70b7:aaff:fe32:65a9
   -> 2405:0204:9511:ea78:fd33:63f3:c118:b910
12 10/05-00:51:46.238149  [**] [1:1000001:0] Testing ICMP! [**] [Priority: 0] {IPV6-ICMP} 2405:0204:9511:ea78:fd33:63f3:c118:b910
   -> fe80:0000:0000:0000:70b7:aaff:fe32:65a9
13 10/05-00:51:49.246997  [**] [1:1000003:0] Testing UDP! [**] [Priority: 0] {UDP} 192.168.43.52:15350 -> 147.135.136.65:8680
14 10/05-00:51:49.560712  [**] [1:1000003:0] Testing UDP! [**] [Priority: 0] {UDP} 147.135.136.65:8680 -> 192.168.43.52:15350
15 10/05-00:51:54.996990  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 2404:6800:4009:0812:0000:0000:0000:200e:443 ->
   2405:0204:9511:ea78:fd33:63f3:c118:b910:50494
16 10/05-00:51:55.047395  [**] [1:1000002:0] Testing TCP! [**] [Priority: 0] {TCP} 2405:0204:9511:ea78:fd33:63f3:c118:b910:50494 ->
   2404:6800:4009:0812:0000:0000:0000:200e:443
```

It is successfully working.

Conclusion:

Successfully understood intrusion detection system. Successfully configured snort and demonstrated snort for intrusion detection.