SEM - VII - 2022-23
CNS Lab

B3 - 2019BTECS00094 - Sweety Shrawan Gupta

Assignment 15

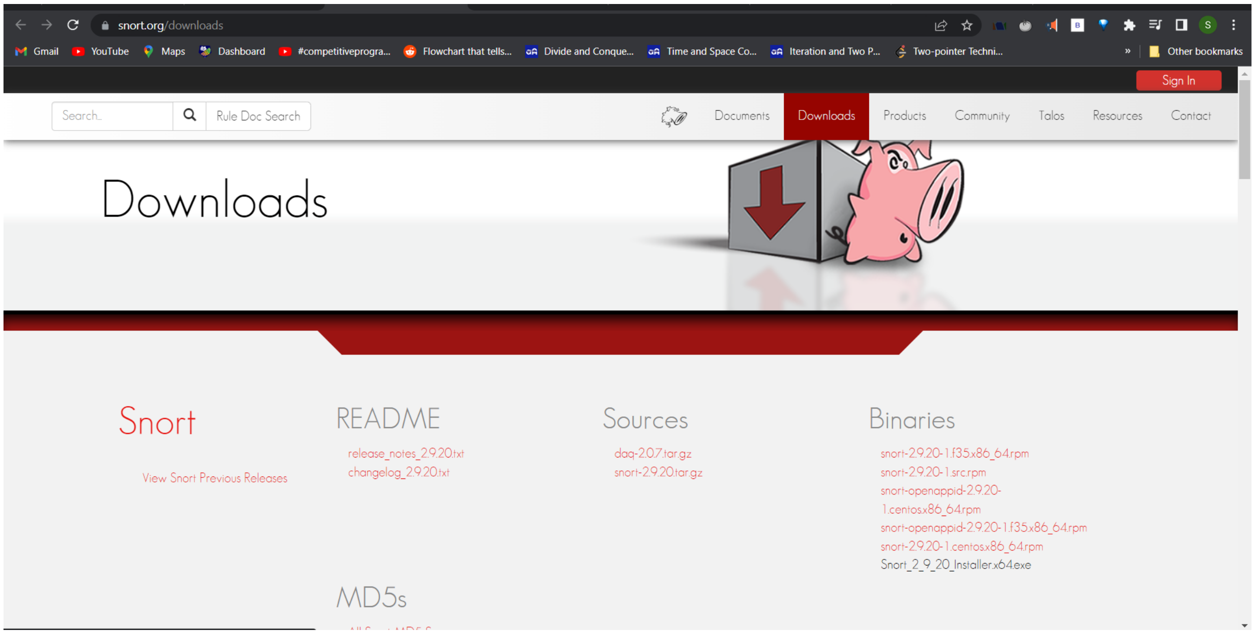
Snort Installation And Configuration

Theory:

SNORT is a network based intrusion detection system which is written in C programming language. It is free open-source software. It can also be used as a packet sniffer to monitor the system in real time. The network admin can use it to watch all the incoming packets and find the ones which are dangerous to the system. It is based on library packet capture tool. The rules are fairly easy to create and implement and it can be deployed in any kind of operating system and any kind of network environment.

Snort Installation:

https://www.snort.org/downloads



Downloads

Snort

View Snort Previous Releases

README

release_notes_2.9.20.txt
changelog_2.9.20.txt

Sources

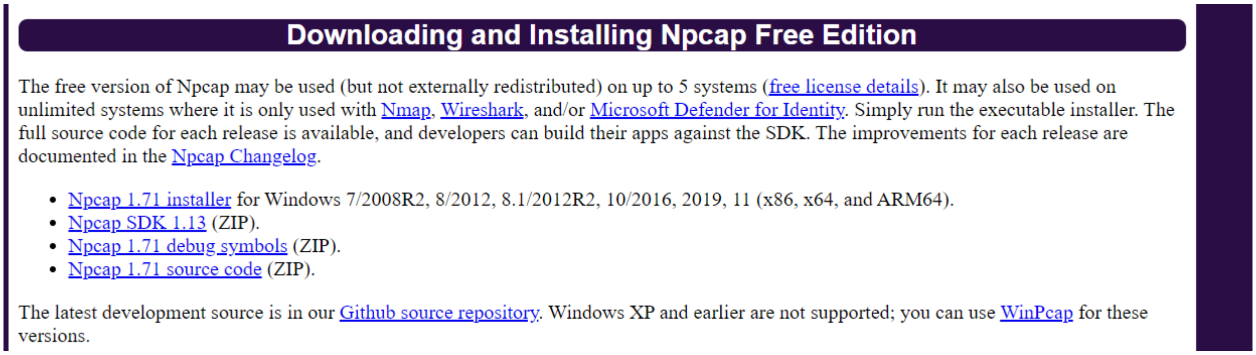
daq-2.0.7.tar.gz
snort-2.9.20.tar.gz

Binaries

snort-2.9.20-1.f35.x86_64.rpm
snort-2.9.20-1.src.rpm
snort-openappid-2.9.20-1.centos.x86_64.rpm
snort-openappid-2.9.20-1.f35.x86_64.rpm
snort-2.9.20-1.centos.x86_64.rpm
Snort_2_9_20_Installer.x64.exe

MD5s

https://npcap.com/#download

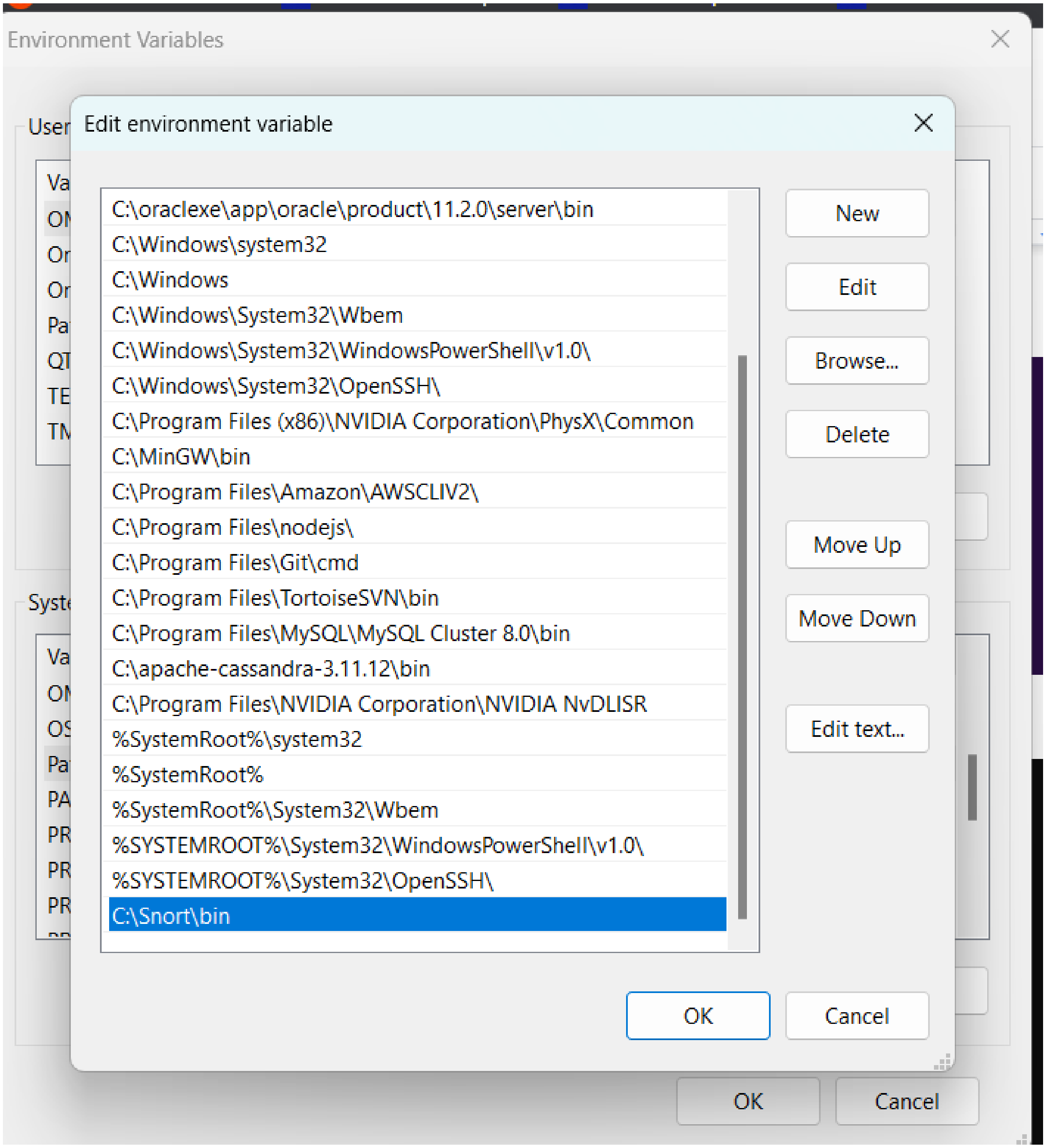


Downloading and Installing Npcap Free Edition

The free version of Npcap may be used (but not externally redistributed) on up to 5 systems (free license details). It may also be used on unlimited systems where it is only used with Nmap, Wireshark, and/or Microsoft Defender for Identity. Simply run the executable installer. The full source code for each release is available, and developers can build their apps against the SDK. The improvements for each release are documented in the Npcap Changelog.

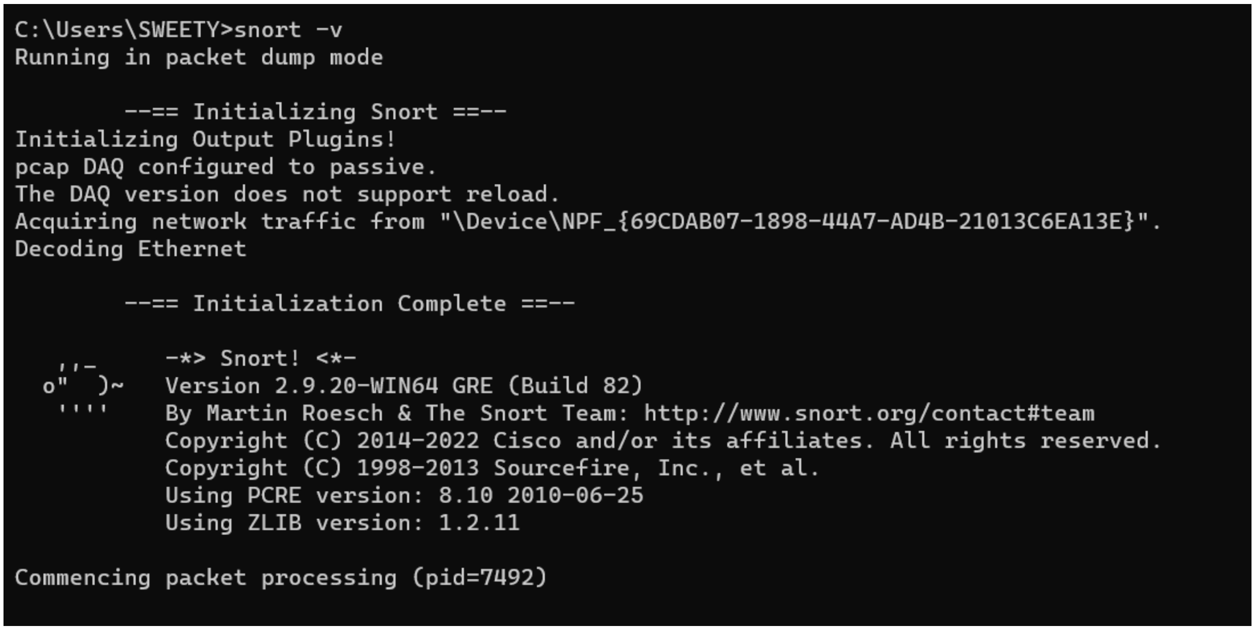
- Npcap 1.71 installer for Windows 7/2008R2, 8/2012, 8.1/2012R2, 10/2016, 2019, 11 (x86, x64, and ARM64).
- Npcap SDK 1.13 (ZIP).
- Npcap 1.71 debug symbols (ZIP).
- Npcap 1.71 source code (ZIP).

The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.



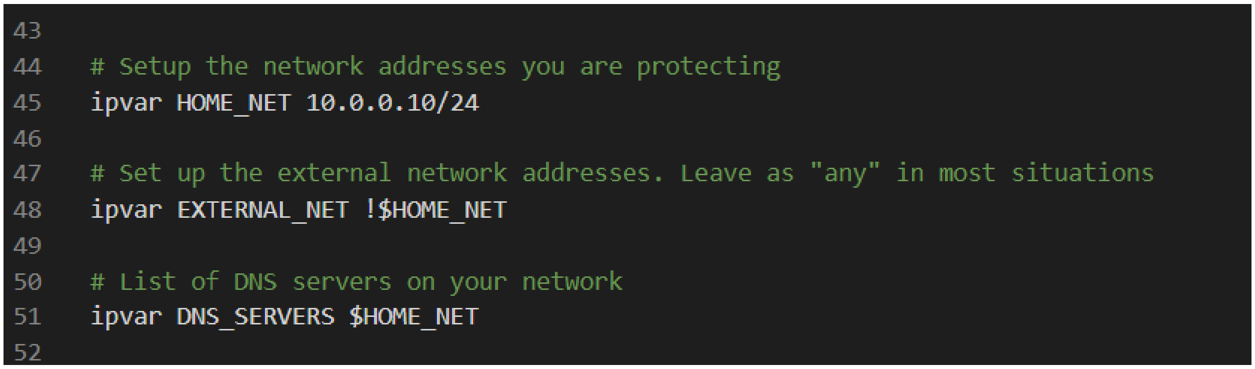
Edit environment variable

C:\oraclexe\app\oracle\product\11.2.0\server\bin
C:\Windows\system32
C:\Windows
C:\Windows\System32\Wbem
C:\Windows\System32\WindowsPowerShell\v1.0\
C:\Windows\System32\OpenSSH\
C:\Program Files (x86)\NVIDIA Corporation\PhysX\Common
C:\MinGW\bin
C:\Program Files\Amazon\AWSCLIV2\
C:\Program Files\nodejs\
C:\Program Files\Git\cmd
C:\Program Files\TortoiseSVN\bin
C:\Program Files\MySQL\MySQL Cluster 8.0\bin
C:\apache-cassandra-3.11.12\bin
C:\Program Files\NVIDIA Corporation\NVIDIA NvDLISR
%SystemRoot%\system32
%SystemRoot%
%SystemRoot%\System32\Wbem
%SYSTEMROOT%\System32\WindowsPowerShell\v1.0\
%SYSTEMROOT%\System32\OpenSSH\
C:\Snort\bin

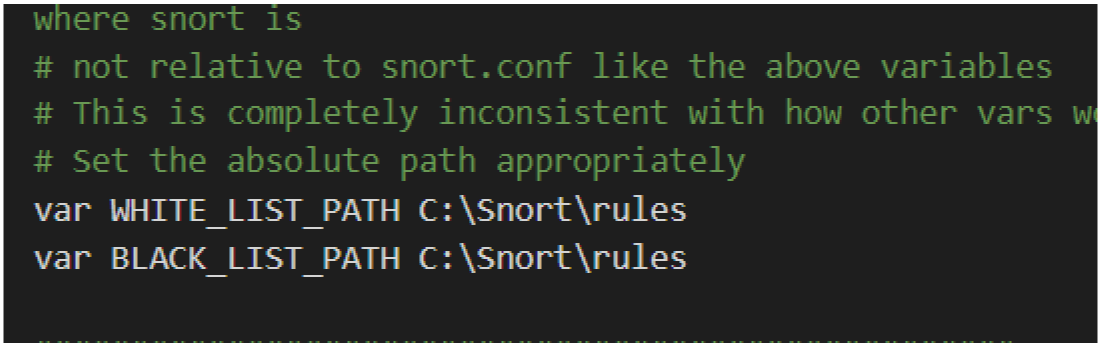


```
C:\Users\SWEETY>snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{69CDAB07-1898-44A7-AD4B-21013C6EA13E}".
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=7492)
```

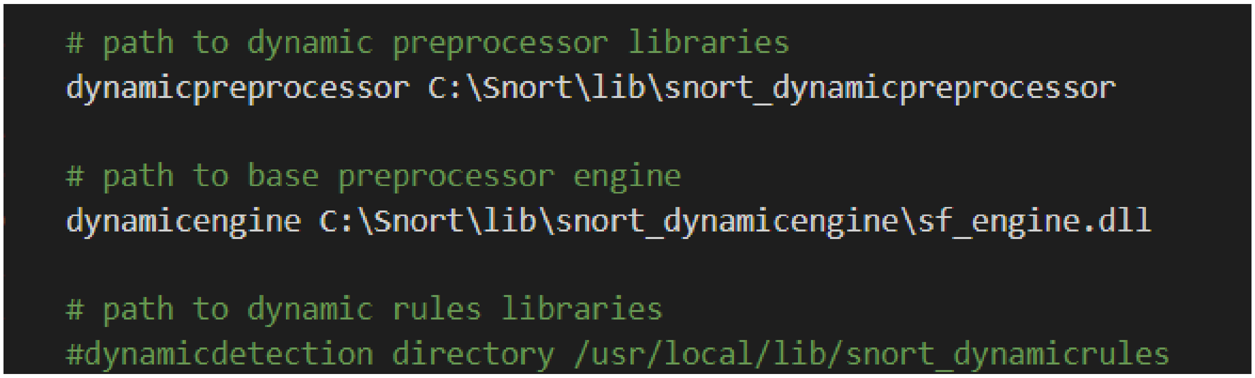
Making changes in snort.conf file



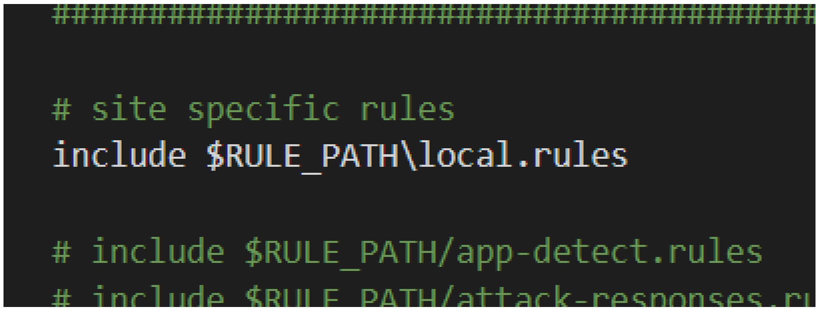
```

# Setup the network addresses you are protecting
ipvar HOME_NET 10.0.0.10/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET !$HOME_NET

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

```



```
where snort is
# not relative to snort.conf like the above variables
# This is completely inconsistent with how other vars w
# Set the absolute path appropriately
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
```

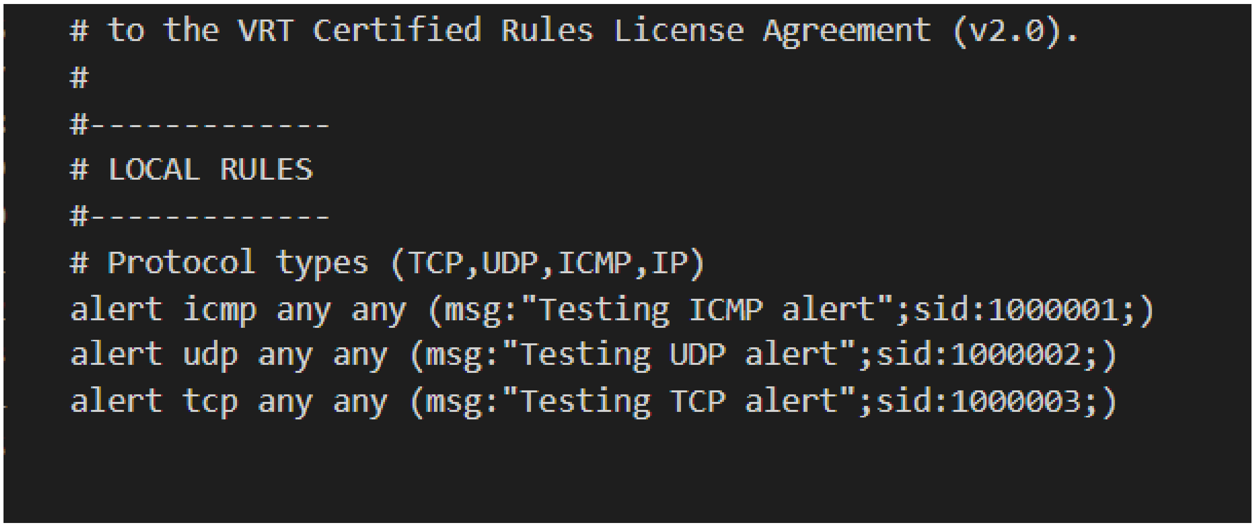


```
# path to dynamic preprocessor libraries
dynamicpreprocessor C:\Snort\lib\snort_dynamicpreprocessor

# path to base preprocessor engine
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll

# path to dynamic rules libraries
#dynamicdetection directory /usr/local/lib/snort_dynamicrules
```



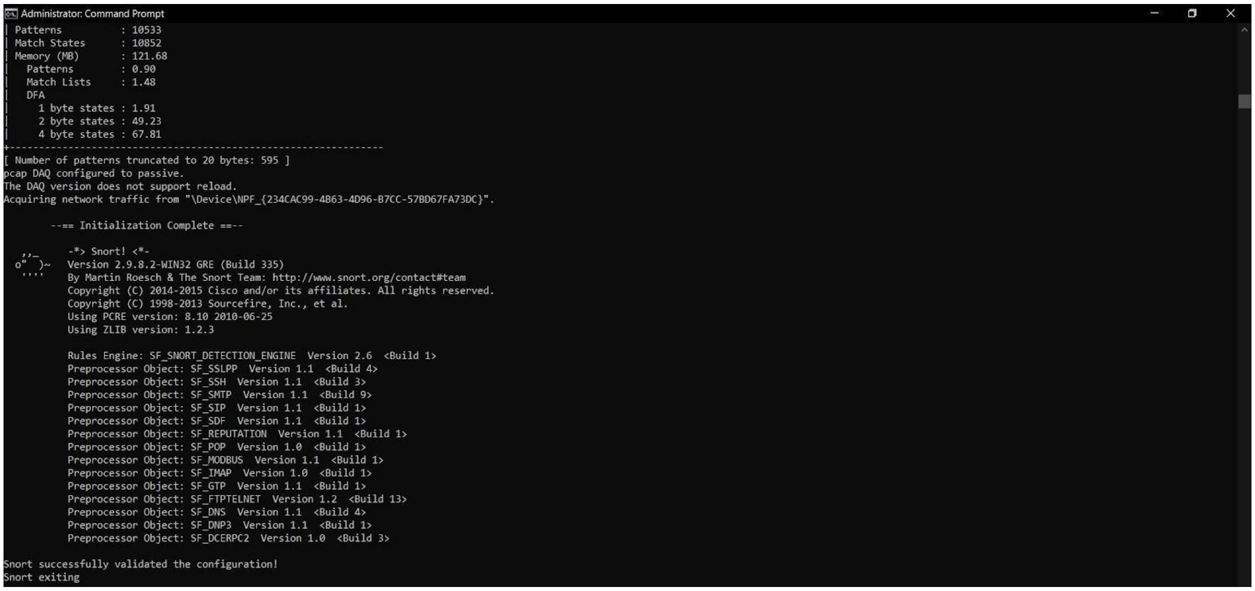
```
##########################################

# site specific rules
include $RULE_PATH\local.rules

# include $RULE_PATH/app-detect.rules
# include $RULE_PATH/attack-responses.ru
```

Add rules in local.rules file



```
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------
# Protocol types (TCP,UDP,ICMP,IP)
alert icmp any any (msg:"Testing ICMP alert";sid:1000001;)
alert udp any any (msg:"Testing UDP alert";sid:1000002;)
alert tcp any any (msg:"Testing TCP alert";sid:1000003;)
```

Initializing configuration:



```
| Patterns         : 10533
| Match States     : 10852
| Memory (MB)      : 121.68
|   Patterns       : 0.90
|   Match Lists    : 1.48
|   DFA
|     1 byte states : 1.91
|     2 byte states : 49.23
|     4 byte states : 67.81
+----------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 595 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{234CAC99-4B63-4D96-B7CC-57BD67FA73DC}".

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.8.2-WIN32 GRE (Build 335)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2015 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

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.6  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>

Snort successfully validated the configuration!
Snort exiting
```