Experiment 12

Study of Network security: Set up Snort and study the logs.

Roll No.	14
Name	Ishika Sanjay Devare
Class	D15-A
Subject	Security Lab
LO Mapped	LO6: Demonstrate the network security system using open-source tools.

Aim: Study of Network security: Set up Snort and study the logs.

Introduction:

What is Snort?

Snort is an open source network intrusion detection system created Sourcefire founder and former CTO Martin Roesch. Cisco now develops and maintains Snort. Snort is referred to as a packet sniffer that monitors network traffic, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies. Long a leader among enterprise intrusion prevention and detection tools, users can compile Snort on most Linux operating systems (OSes) or Unix. A version is also available for Windows.

How does Snort work?

Snort is based on library packet capture (libpcap). Libpcap is a tool that is widely used in Transmission Control Protocol/Internet Protocol address traffic sniffers, content searching and analyzers for packet logging, real-time traffic analysis, protocol analysis and content matching. Users can configure Snort as a sniffer, packet logger -- like TCPdump or Wireshark -- or network intrusion prevention method.

Intrusion Prevention System Mode: As an open-source network intrusion prevention system, Snort will monitor network traffic and compare it against a user-defined Snort rule set -- the file would be labeled snort.conf. This is Snort's most important function.

Snort applies rules to monitored traffic and issues alerts when it detects certain kinds of questionable activity on the network.

It can identify cybersecurity attack methods, including OS fingerprinting, denial of service, buffer overflow, common gateway interface attacks, stealth port scans and Server Message Block probes. When Snort detects suspicious behavior, it acts as a firewall and sends a real-time alert to Syslog, to a separate alerts file or through a pop-up window.

Advantage of SNORT over other tools:

1. Scalability: Snort can be successfully deployed on any network environment.

2. Flexibility and Usability: Snort can run on various operating systems including Linux, Windows, and Mac OS X.

3. Live and Real: Time: Snort can deliver real-time network traffic event information.

4. Flexibility in Deployment: There are thousands of ways that Snort can be deployed and a myriad of databases, logging systems, and tools with which it can work.

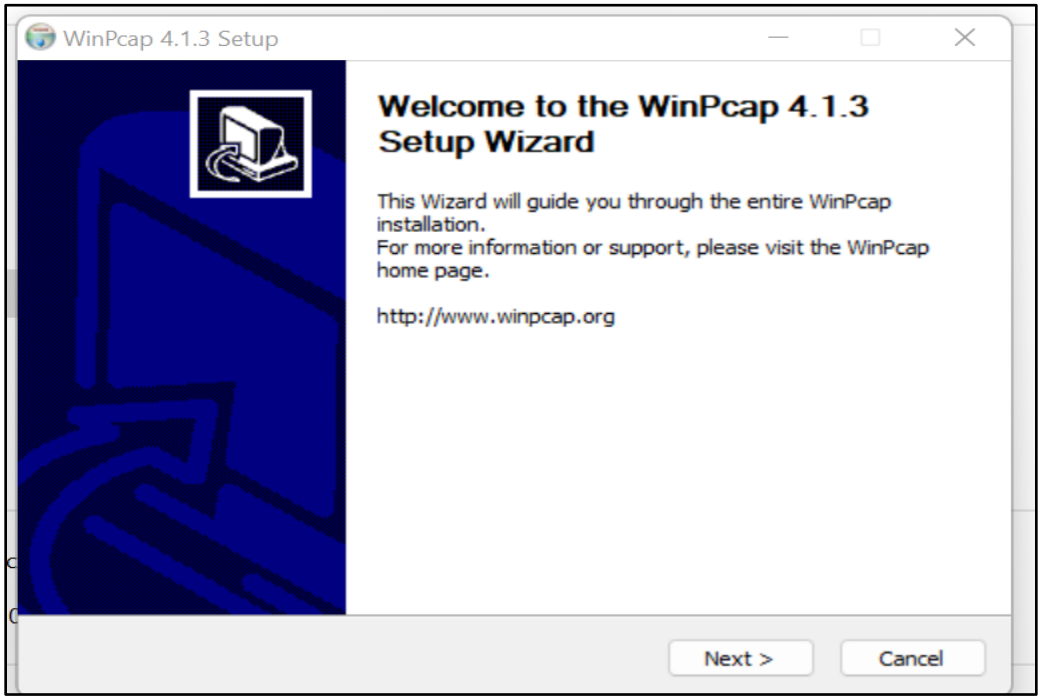
5. Speed in Detecting and Responding to Security Threats: Used in conjunction with a firewall and

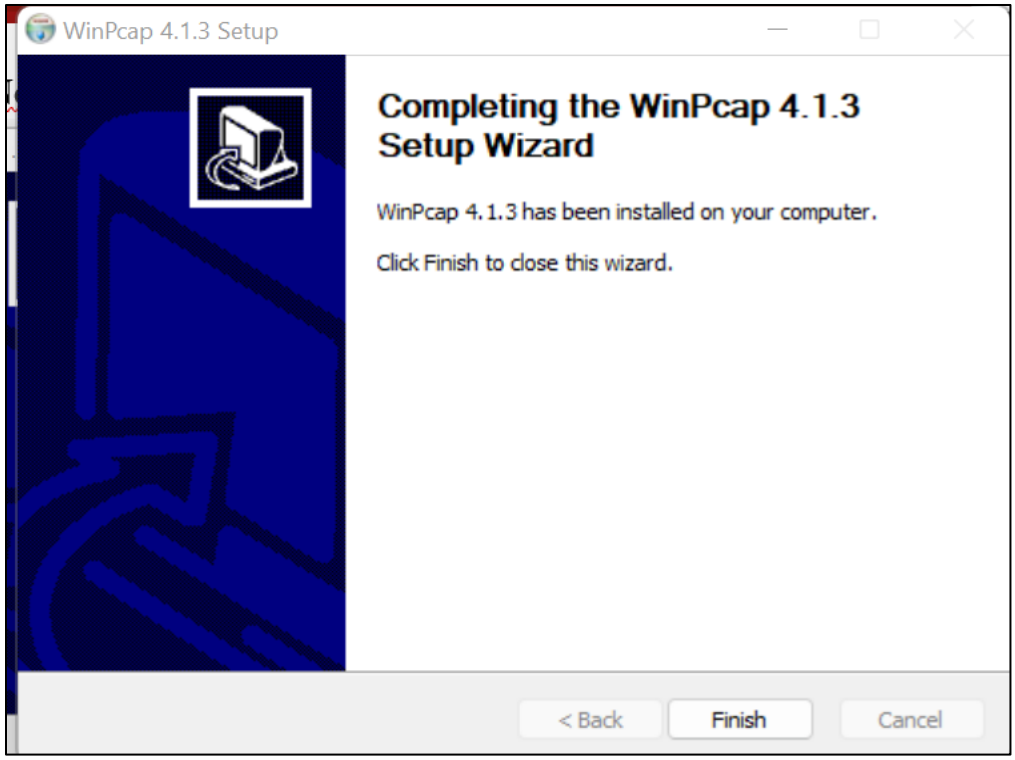
other layers of security infrastructure, Snort helps organizations detect and respond to system crackers, worms, network vulnerabilities, security threats, and policy abusers that aim to take down network and computer systems.

6. Modular Detection Engine: Snort sensors are modular and can monitor multiple machines from one physical and logical location. Snort be placed in front of the firewall, behind the firewall, next to the firewall, and everywhere else to monitor an entire network. As a result, organizations use Snort as a security solution to find out if there are unauthorized attempts to hack in the network or if a hacker has gained unauthorized access into the network system.

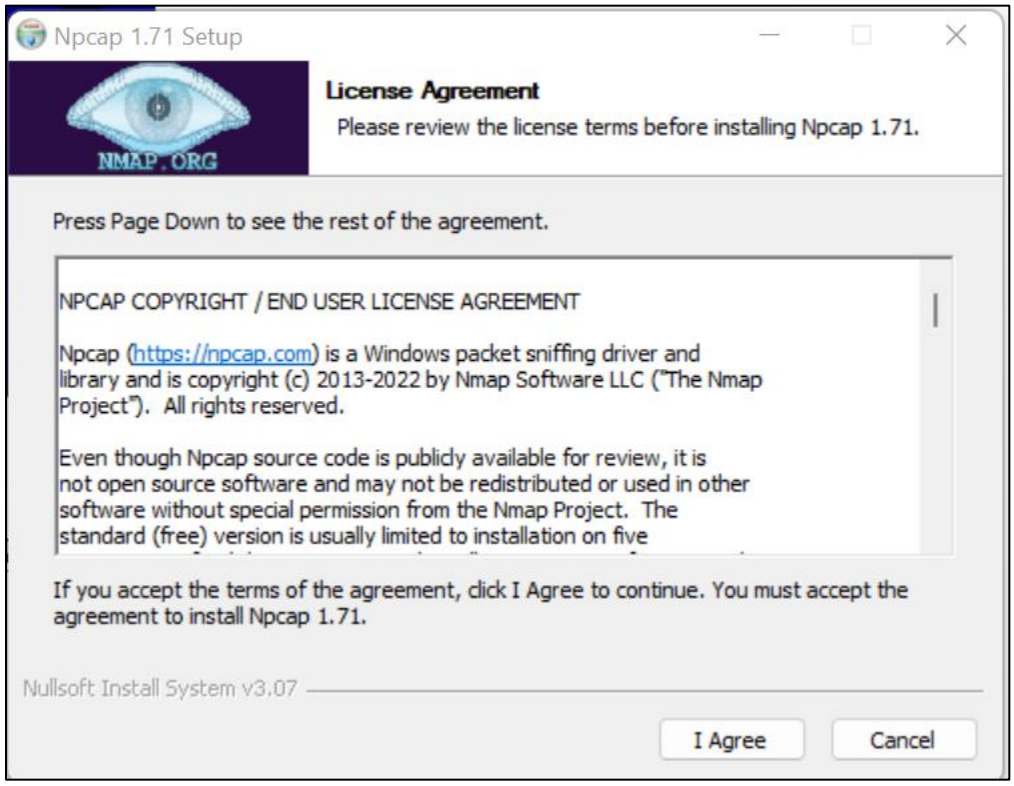
Implementation:

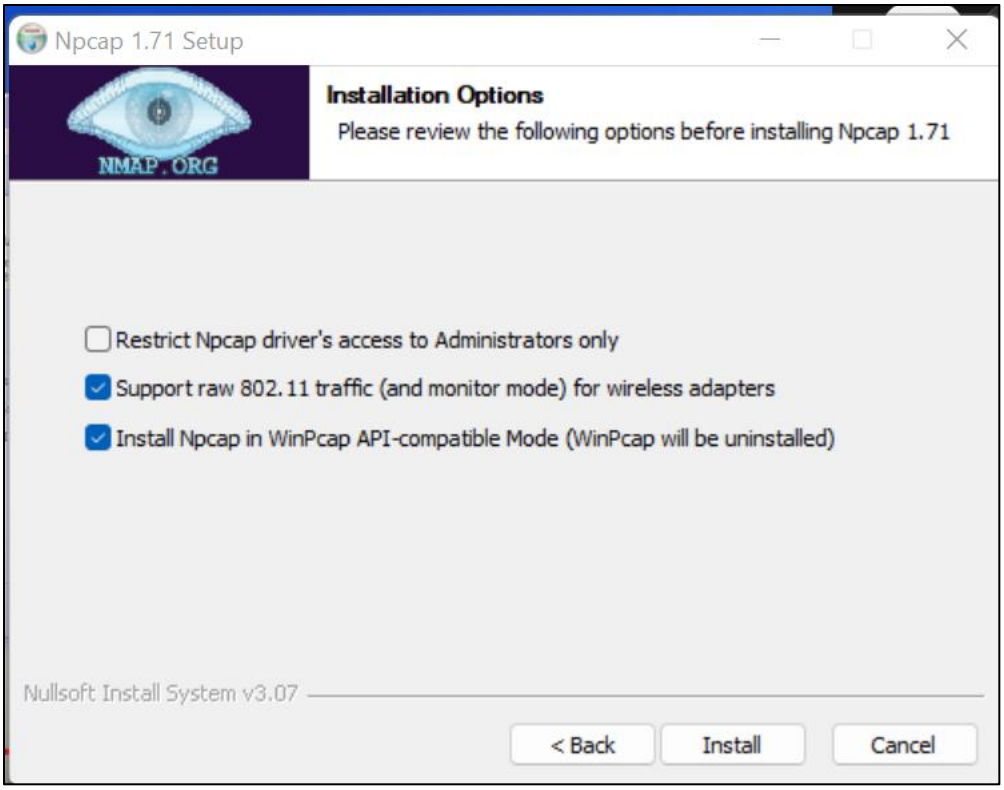
Installing WinPcap

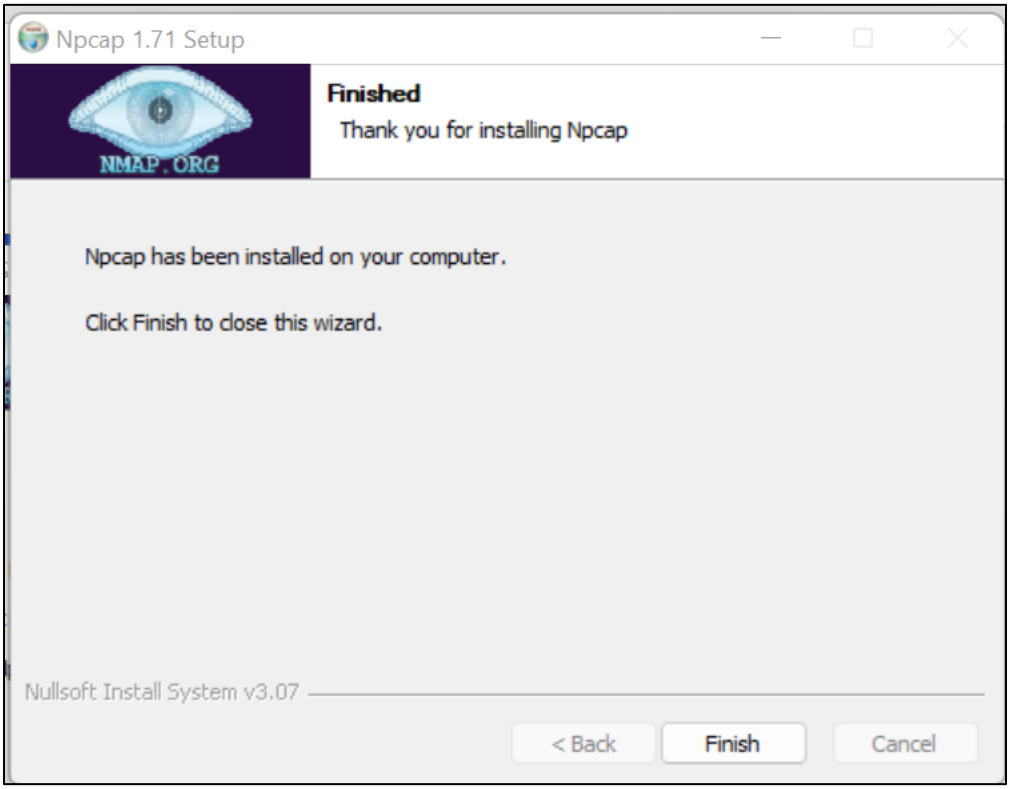




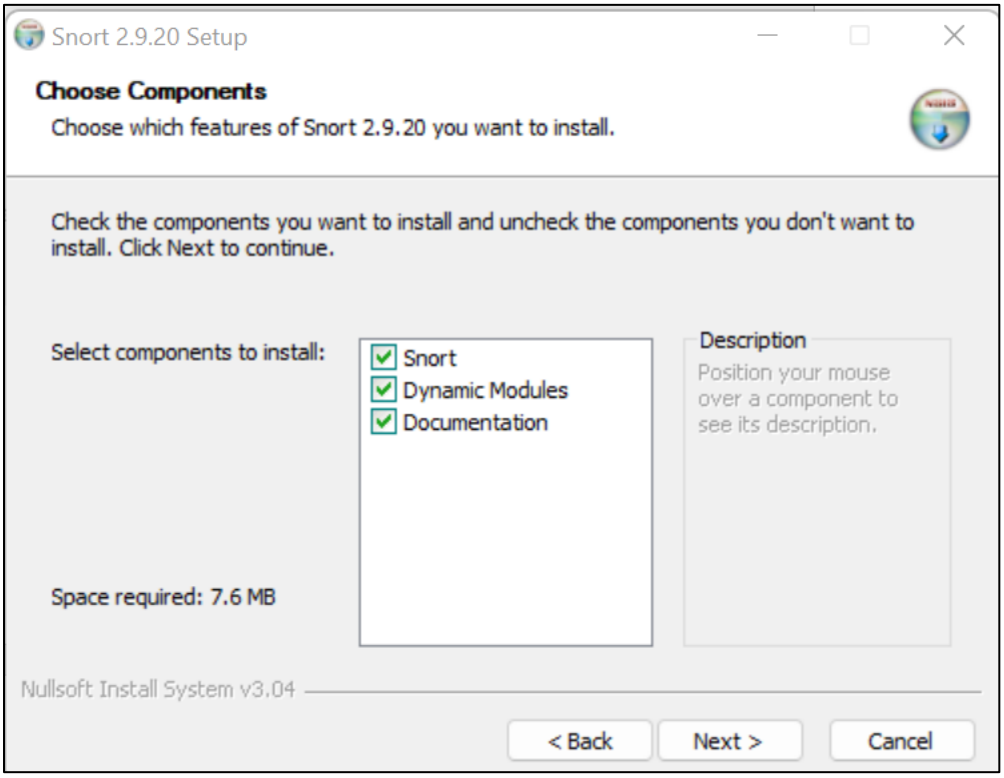
Installing Ncap

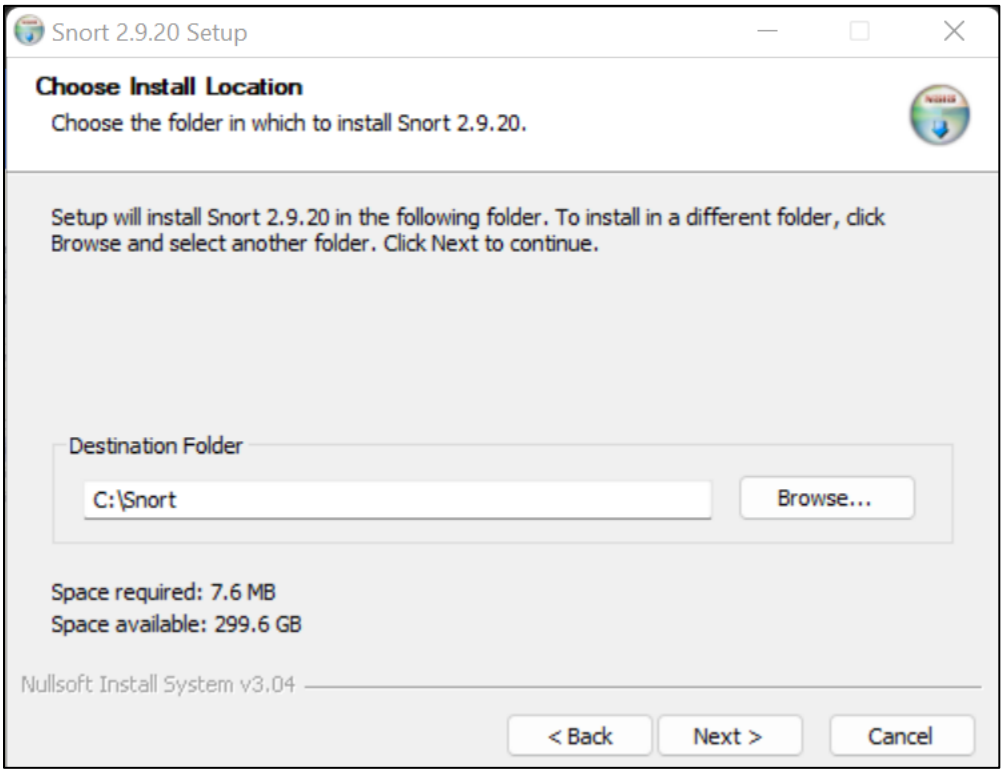


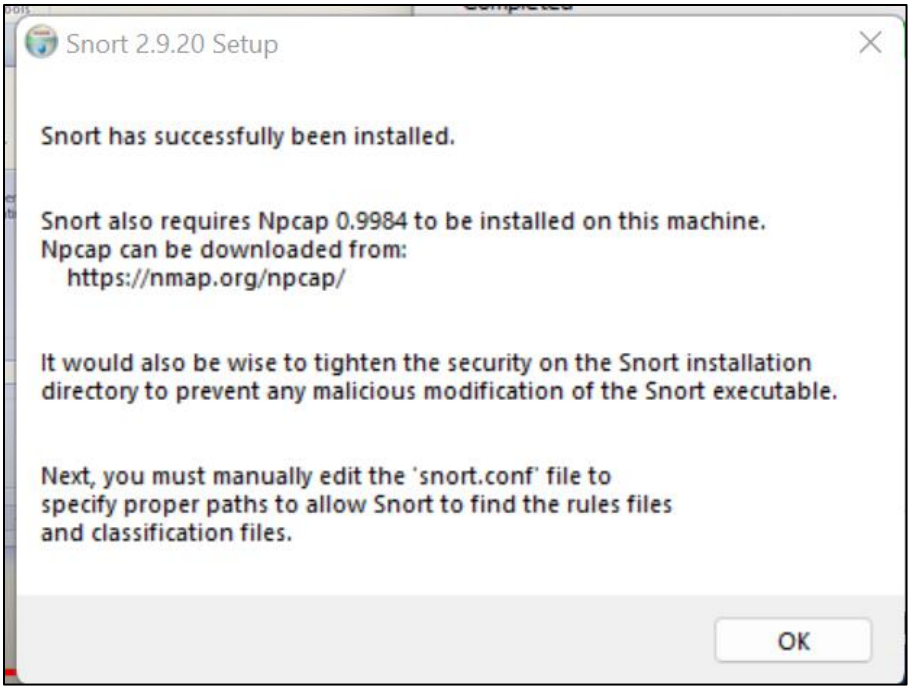

Npcap 1.71 Setup
NMAP.ORG
Installation Options
Please review the following options before installing Npcap 1.71
Restrict Npcap driver's access to Administrators only
Support raw 802.11 traffic (and monitor mode) for wireless adapters
Install Npcap in WinPcap API-compatible Mode (WinPcap will be uninstalled)
Nullsoft Install System v3.07
< Back
Install
Cancel


Npcap 1.71 Setup
NMAP.ORG
Finished
Thank you for installing Npcap
Npcap has been installed on your computer.
Click Finish to close this wizard.
Nullsoft Install System v3.07
< Back
Finish
Cancel

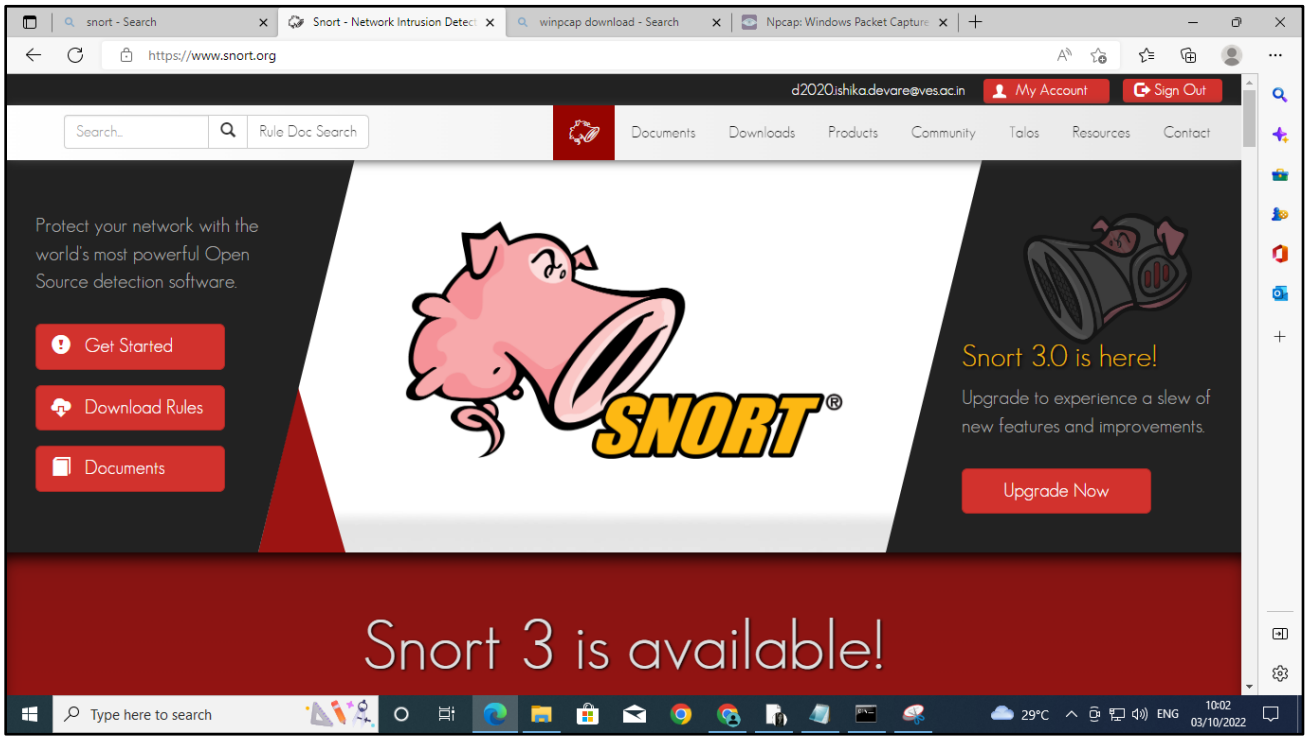
Installing Snort



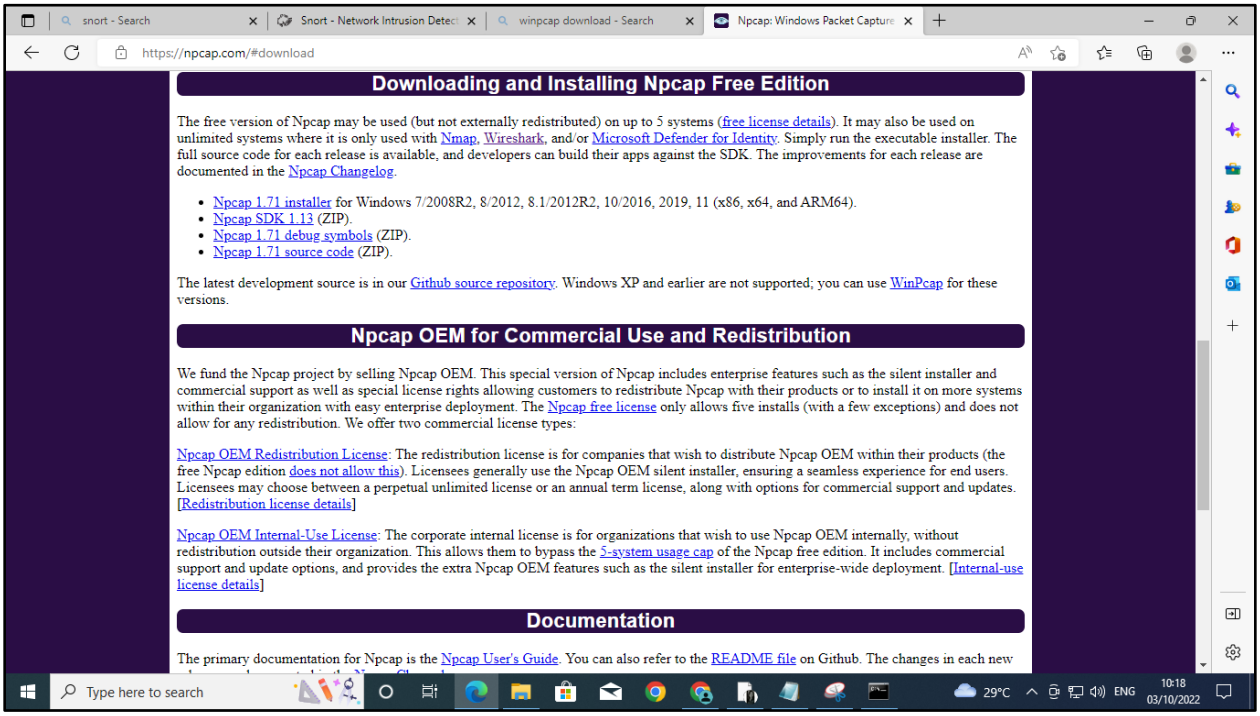




Install snort on windows 10 from https://www.snort.org/downloads.



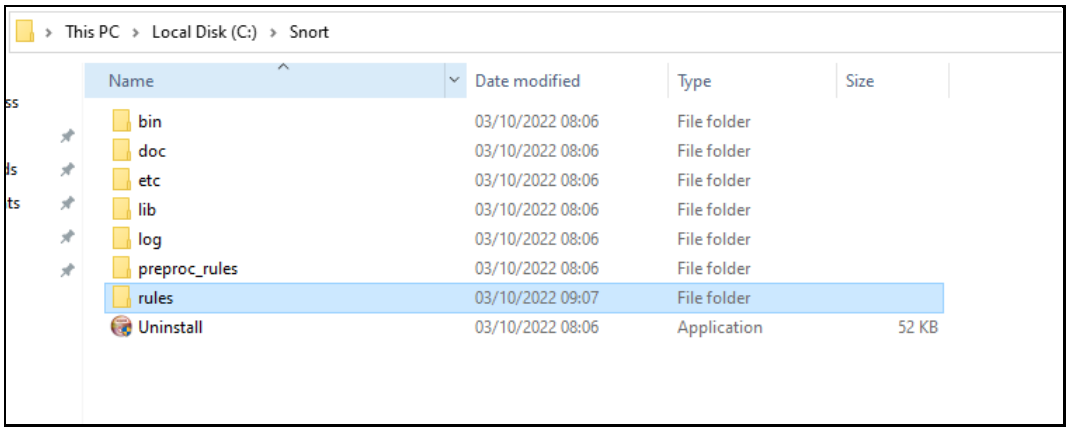
Install Npcap which is required by snort for proper functioning, Npcap for Windows 10 can be downloaded from https://npcap.com/



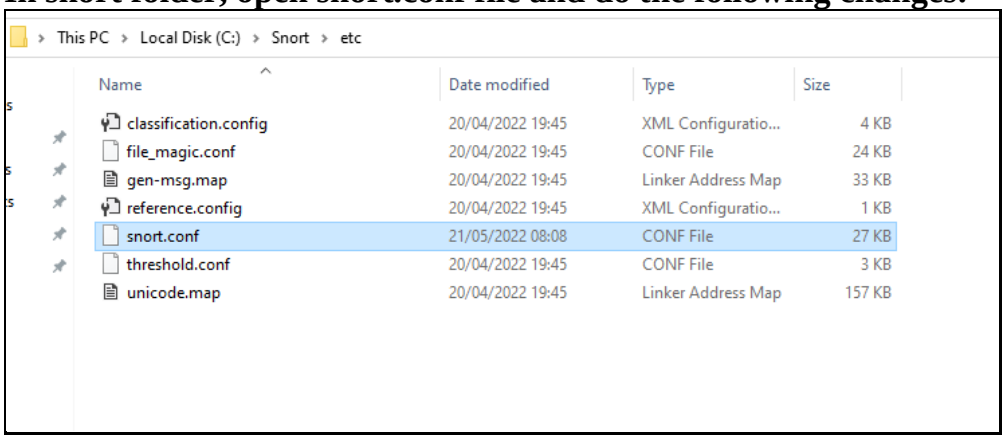
After installing Snort and Npcap enter these commands in windows 10 Command prompt to check snorts working

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

   ,,_     -*> 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


C:\Snort\bin>
```

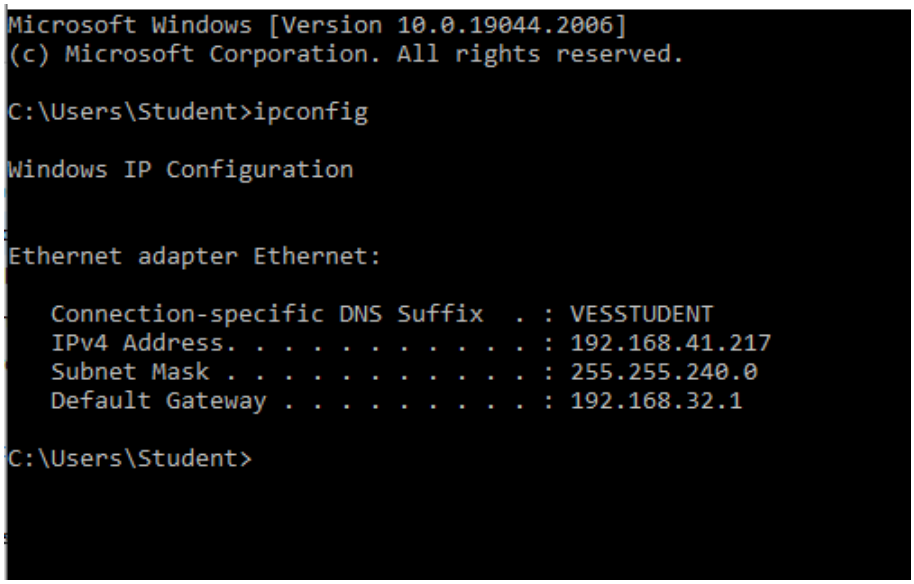
Configuring Snort 2.9.17 on Windows 10:
Snort folder



In snort folder, open snort.conf file and do the following changes:



In command prompt enter command ipconfig



Configuring Snort 2.9.17 on Windows 10:
After installing Snort on Windows 10, Another important step to get started with Snort is configuring it on Windows 10.
1. Go to this link and download latest snort rule file.

2. Extract 3 folders from the downloaded snortrules-snapshot-29170.tar folder into the Snorts corresponding folders in C drive.
Folders to be extracted are: rules , preproc_rules , etc
• rules folder contains the rules files and the most important local.rules file. Which we will use to enter all our rules.
• etc folder contains all configuration files and the most important file is snort.conf file which we will use for configuration

3. 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.

4. Setup the network addresses you are protecting
ipvar HOME_NET any
Note: Mention your own host IP addresses that you want to protect.

5. Setup the external network into anything that is not the home network. That is why ! is used in the command it denotes ‘not’.
Set up the external network addresses. Leave as “any” in most situationsipvar EXTERNAL_NET any

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.0/24

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

6. Now we have to define the directory for our rules and preproc rules folder
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\rulesvar RULE_PATH ../rulesvar SO_RULE_PATH../so_rulesvar PREPROC_RULE_PATH ../preproc_rules

```
# 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 ../so_rules
var PREPROC_RULE_PATH c:\Snort\preproc_rules
```

7. Now we have to setup our white list and black list path it will be in our snorts' rule folder
If you are using reputation preprocessor set thesevar WHITE_LIST_PATH ../rulesvar BLACK_LIST_PATH ../rules

```
# Set the absolute path appropriately
var WHITE_LIST_PATH c:\Snort\rules
var BLACK_LIST_PATH c:\Snort\rules
```

8. Next we have to enable to 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:

```
#
# config logdir: c:\Snort\log
```

9. We will do same thing for dynamic preprocessor engine
path to base preprocessor
enginedynamicengine/usr/local/lib/snort_dynamicengine/libsf_engine.so

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

10. Again just convert forward slashes to backslashes and uncomment the lines below:
decoder and preprocessor event rules# include $PREPROC_RULE_PATH/preprocessor.rules# include $PREPROC_RULE_PATH/decoder.rules# include $PREPROC_RULE_PATH/sensitive-data.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
```

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

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

   ,,_     -*> 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
```

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 - **Snort — W**

```
C:\Snort\bin>snort --W
snort: unrecognized option `--W'

   ,,_     -*> 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

USAGE: snort [-options] <filter options>
       snort /SERVICE /INSTALL [-options] <filter options>
       snort /SERVICE /UNINSTALL
       snort /SERVICE /SHOW
Options:
       -A         Set alert mode: fast, full, console, test or none  (alert file alerts only)
       -b         Log packets in tcpdump format (much faster!)
       -B <mask>  Obfuscated IP addresses in alerts and packet dumps using CIDR mask
       -c <rules> Use Rules File <rules>
       -C         Print out payloads with character data only (no hex)
       -d         Dump the Application Layer
       -e         Display the second layer header info
       -E         Log alert messages to NT Eventlog. (Win32 only)
       -f         Turn off fflush() calls after binary log writes
```

Configuration validation check command:
Now we will enter a command To check validation of snort's configuration
by choosing a specific wireless interface card (1) the rest of command shows the config file path **The command is : snort -i 1 -c C:\Snort\etc\snort.conf -T**

```
   ,,_     -*> 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

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <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>

Total snort Fixed Memory Cost - MaxRss:-764988768
Snort successfully validated the configuration!
Snort exiting

C:\Snort\bin>
```

```
C:\Users\Student>ipconfig/all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : INFT513-17
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : VESSTUDENT

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . : VESSTUDENT
   Description . . . . . . . . . . . : Realtek PCIe GBE Family Controller
   Physical Address. . . . . . . . . : F4-6B-8C-86-45-AD
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.41.217(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Lease Obtained. . . . . . . . . . : 3 October 2022 07:56:02
   Lease Expires . . . . . . . . . . : 4 October 2022 07:55:45
   Default Gateway . . . . . . . . . : 192.168.32.1
   DHCP Server . . . . . . . . . . . : 192.168.32.1
   DNS Servers . . . . . . . . . . . : 192.168.32.1
                                       8.8.8.8
   NetBIOS over Tcpip. . . . . . . . : Enabled
```

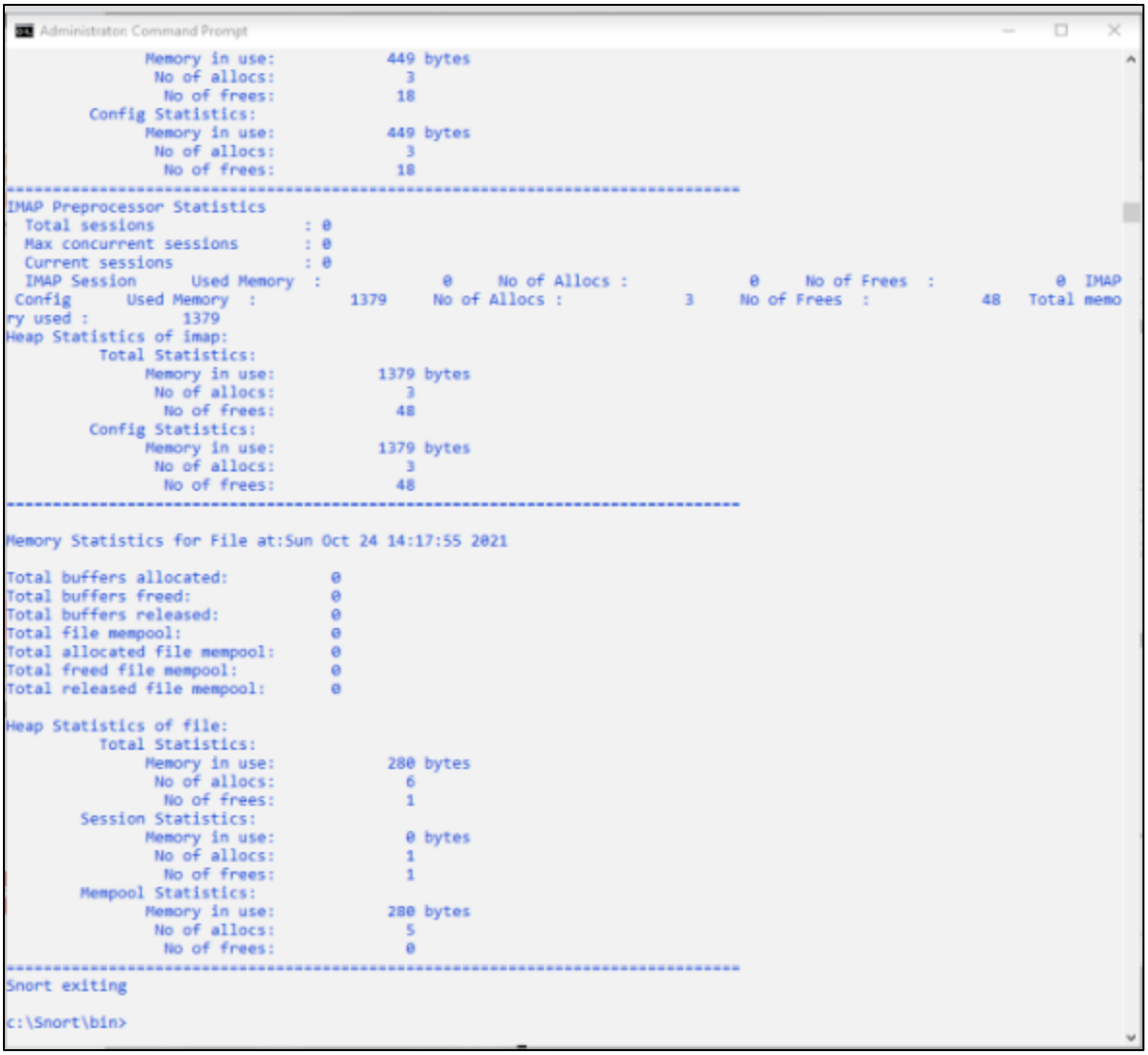
local.rules - Notepad

File Edit Format View Help

```
# Copyright 2001-2022 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;)
```

Administrator: Command Prompt - snort -i 1 -c c:\Snort\etc\snort.conf -A console

```
    4 byte states : 1
Characters        : 205090
States            : 162808
Transitions       : 29061190
State Density     : 69.7%
Patterns          : 9746
Match States      : 10029
Memory (MB)       : 116.81
  Patterns        : 1.13
  Match Lists     : 2.56
  DFA
    1 byte states : 1.06
    2 byte states : 46.34
    4 byte states : 65.36
+-------------------------------------------------------------------
[ Number of patterns truncated to 20 bytes: 554 ]
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{209F97D8-A4D4-4EA7-8F8A-CE4602DCC1E2}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.18.1-WIN64 GRE (Build 1005)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
           Copyright (C) 2014-2021 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

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.2  <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>
Commencing packet processing (pid=15336)
```



Conclusion: In this practical we successfully Set up Snort and study the logs.