Assignments:-4

Module:- NDC(SNORT_Windows)

Name:- Prithviraj Nikam

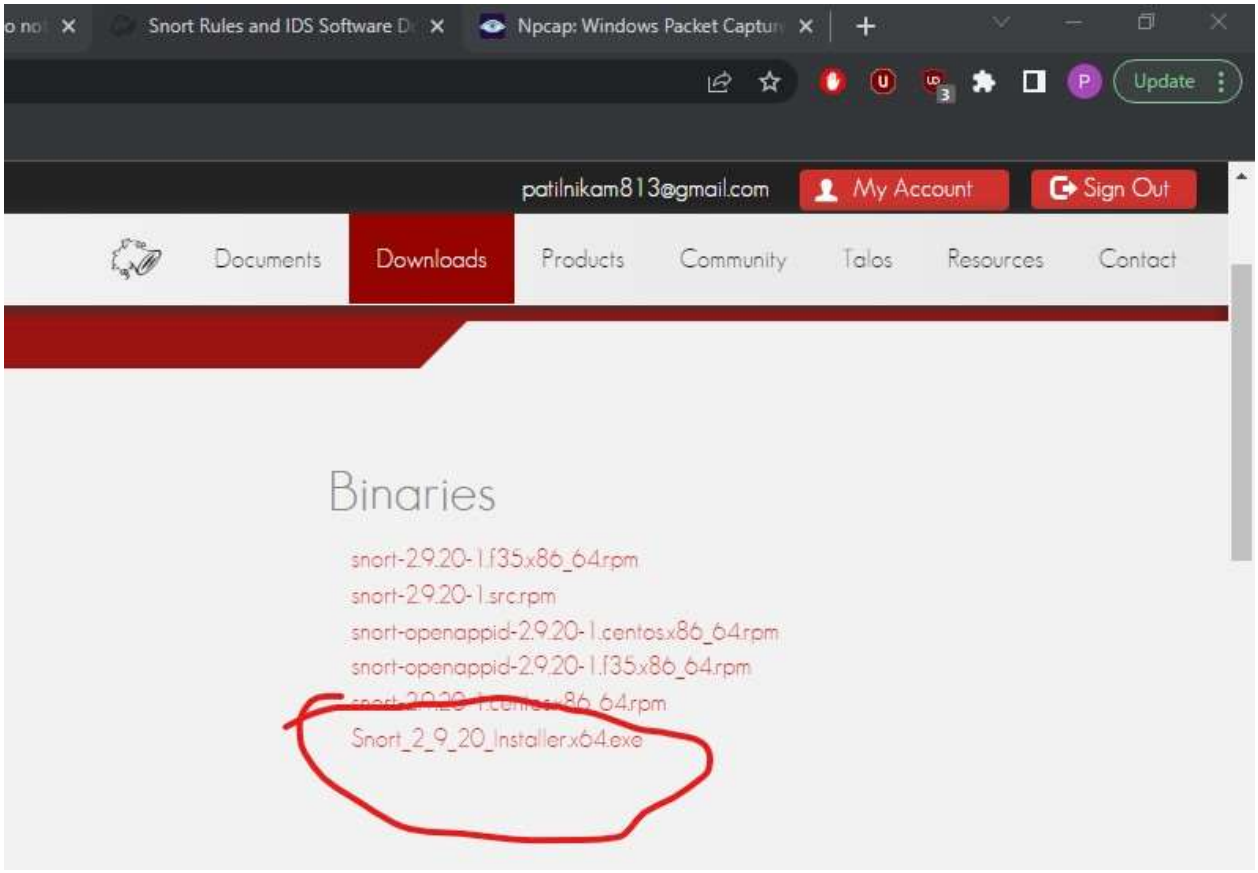
Lab Assignment :-

Install and configure SNORT-2.9.20 on following OS:

2. Windows 10/11

Step-1:- Go to Snort Official website and download Snort for windows

https://www.snort.org/downloads/snort/Snort_2_9_20_Installer.x64.exe



Step-2:- Go to npcap official website and download npcap for windows

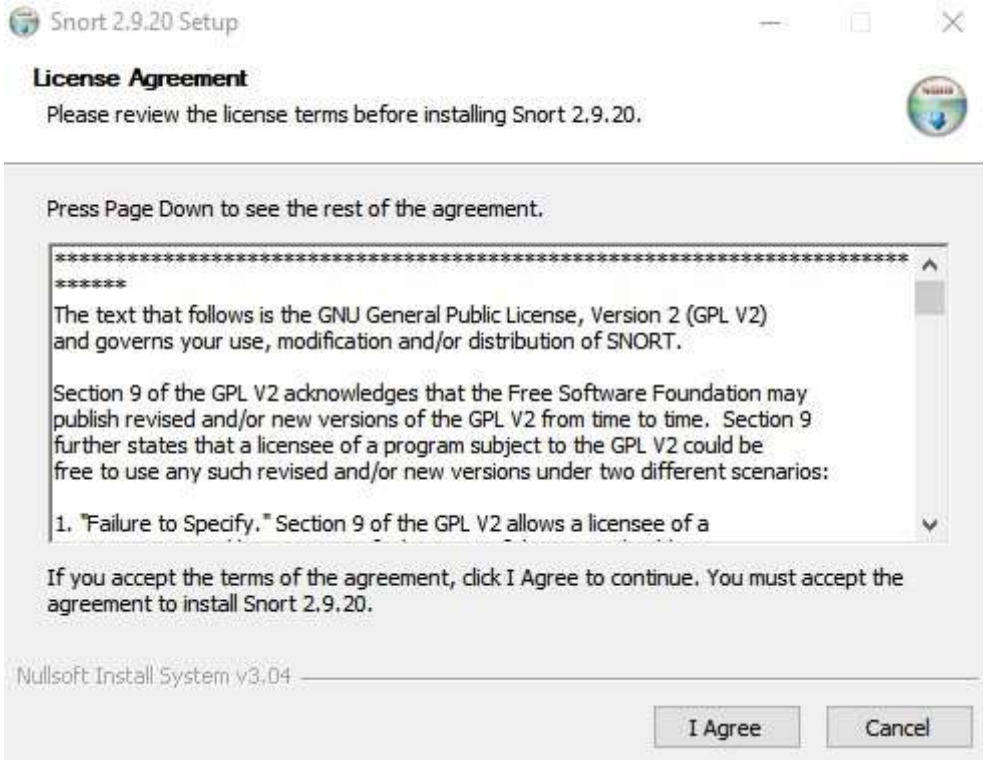
https://npcap.com/dist/npcap-1.71.exe

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).

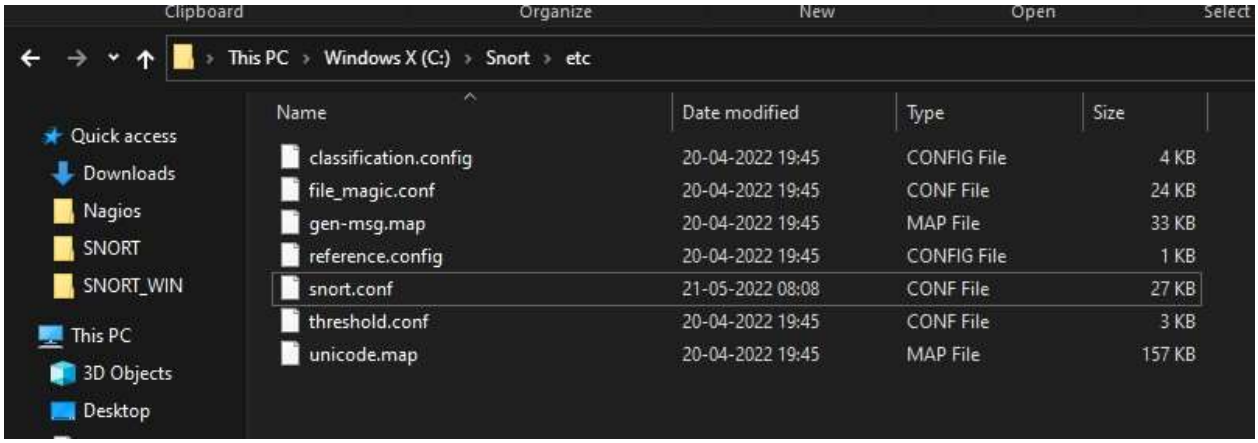
The latest development source is in our Github source repository. Windows XP and earlier are not supported; you can use WinPcap for these versions.

Step-3:- Install the Snort 2.9.20.



Step-4:- Install Npcap 1.71

Step-5:- Go to C drive on windows and open the Configure snort.conf



Step-6:-Configure SNORT
On line number 45 –
ipvar HOME_NET 192.168.3.140/32

On line number 48 –
ipvar EXTERNAL_NET !$HOME_NET

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.3.131/32

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

On line number 105 and 106
var SO_RULE_PATH /etc/snort/so_rules
var PREPROC_RULE_PATH /etc/snort/preproc_rules

```
# 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
```

On line number 113 and 114
var WHITE_LIST_PATH /etc/snort/rules
var BLACK_LIST_PATH /etc/snort/rules

```
89986
# Set the absolute path appropriately
var WHITE_LIST_PATH c:\snort\rules
var BLACK_LIST_PATH c:\snort\rules
```

Add the log

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

Add the dynamic rules and dynamicengine

```
# For more information, see Snort Manual, Configuring Snort -
Dynamic Modules
##################################################

# path to dynamic preprocessor libraries
dynamicpreprocessor directory 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 c:\snort\lib\snort_dynamicrules
```

Add the rules White list and Black List

```
# Reputation preprocessor. For more information see
README.reputation
preprocessor reputation: \
   memcap 500, \
   priority whitelist, \
   nested_ip inner, \
   whitelist $WHITE_LIST_PATH\white_list.rules, \
   blacklist $BLACK_LIST_PATH\black_list.rules
```

Modifies rule files from 548 till ------X11

```
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
include $RULE_PATH\browser-plugins.rules
include $RULE_PATH\browser-webkit.rules
include $RULE_PATH\chat.rules
include $RULE_PATH\content-replace.rules
include $RULE_PATH\ddos.rules
include $RULE_PATH\dns.rules
include $RULE_PATH\dos.rules
include $RULE_PATH\experimental.rules
include $RULE_PATH\exploit-kit.rules
include $RULE_PATH\exploit.rules
include $RULE_PATH\file-executable.rules
include $RULE_PATH\file-flash.rules
include $RULE_PATH\file-identify.rules
include $RULE_PATH\file-image.rules
include $RULE_PATH\file-multimedia.rules
include $RULE_PATH\file-office.rules
include $RULE_PATH\file-other.rules
include $RULE_PATH\file-pdf.rules
include $RULE_PATH\finger.rules
include $RULE_PATH\ftp.rules
include $RULE_PATH\icmp-info.rules
include $RULE_PATH\icmp.rules
include $RULE_PATH\imap.rules
include $RULE_PATH\indicator-compromise.rules
include $RULE_PATH\indicator-obfuscation.rules
include $RULE_PATH\indicator-shellcode.rules
include $RULE_PATH\info.rules
include $RULE_PATH\malware-backdoor.rules
include $RULE_PATH\malware-cnc.rules
include $RULE_PATH\malware-other.rules
include $RULE_PATH\malware-tools.rules
include $RULE_PATH\misc.rules
include $RULE_PATH\multimedia.rules
include $RULE_PATH\mysql.rules
include $RULE_PATH\netbios.rules
include $RULE_PATH\nntp.rules
include $RULE_PATH\oracle.rules
```

Step-7:- Modify the Local rules

```
# to the VRT Certified Rules License Agreement (v2.0).
#
#-------------
# LOCAL RULES
#-------------
alert icmp any any -> $HOME_NET any (msg:"ICMP
Testing";sid:100000020;)
```

Step-8:- Go to Windows Command Prompt

snort -W

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

Index   Physical Address        IP Address      Device Name     Description
-----   ----------------        ----------      -----------     -----------
    1   00:00:00:00:00:00       disabled        \Device\NPF_{05A524C0-5E23-4ED0-8CCE-703DC3CCD86F}      WAN Miniport (Ne
twork Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{6EBAB3D7-6DC2-42AF-867C-546EE67AE64F}      WAN Miniport (IP
v6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{BD01FD7B-3D01-4DED-9739-28C40113F013}      WAN Miniport (IP
)
    4   B0:83:FE:90:82:CE       192.168.3.104   \Device\NPF_{A8D68F85-9473-45C4-BD5C-0683AB07B580}      Realtek PCIe GbE
 Family Controller
    5   0A:00:27:00:00:07       192.168.56.1    \Device\NPF_{68C7DC25-6465-4A32-A447-752755EBB4C8}      VirtualBox Host-
Only Ethernet Adapter
    6   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback tra
ffic capture
```

Step-9:- snort.exe -T -i 4 -c c:\Snort\etc\snort.conf

```
C:\Snort\bin>snort.exe -T -i 4 -c c:\Snort\etc\snort.conf
```

```
            Preprocessor Object: SF_DNP3  Version 1.1  <Bui
            Preprocessor Object: SF_DCERPC2  Version 1.0  <

Total snort Fixed Memory Cost - MaxRss:2062234272
Snort successfully validated the configuration!
Snort exiting
```

Step-10:- snort.exe -A console -i 4 -c c:\Snort\etc\snort.conf

```
C:\Snort\bin>snort.exe -A console -i 4 -c c:\Snort\etc\snort.conf
```

Step-11:- go to another Windows and ping my system
ping 192.168.3.104

```
C:\Snort\bin>ping 192.168.3.104

Pinging 192.168.3.104 with 32 bytes of data:
Reply from 192.168.3.104: bytes=32 time=1ms TTL=128
Reply from 192.168.3.104: bytes=32 time<1ms TTL=128
Reply from 192.168.3.104: bytes=32 time<1ms TTL=128
Reply from 192.168.3.104: bytes=32 time=1ms TTL=128

Ping statistics for 192.168.3.104:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Snort\bin>
```

Step -12:- Go to my system and check OUTPUT

```
            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=9136)
12/13-18:09:11.091458  [**] [1:100000020:0] ICMP Testing [**] [Priority: 0] {ICMP} 192.168.3.131 -> 192.168.3.104
12/13-18:09:12.093608  [**] [1:100000020:0] ICMP Testing [**] [Priority: 0] {ICMP} 192.168.3.131 -> 192.168.3.104
12/13-18:09:13.098597  [**] [1:100000020:0] ICMP Testing [**] [Priority: 0] {ICMP} 192.168.3.131 -> 192.168.3.104
12/13-18:09:14.103293  [**] [1:100000020:0] ICMP Testing [**] [Priority: 0] {ICMP} 192.168.3.131 -> 192.168.3.104
```