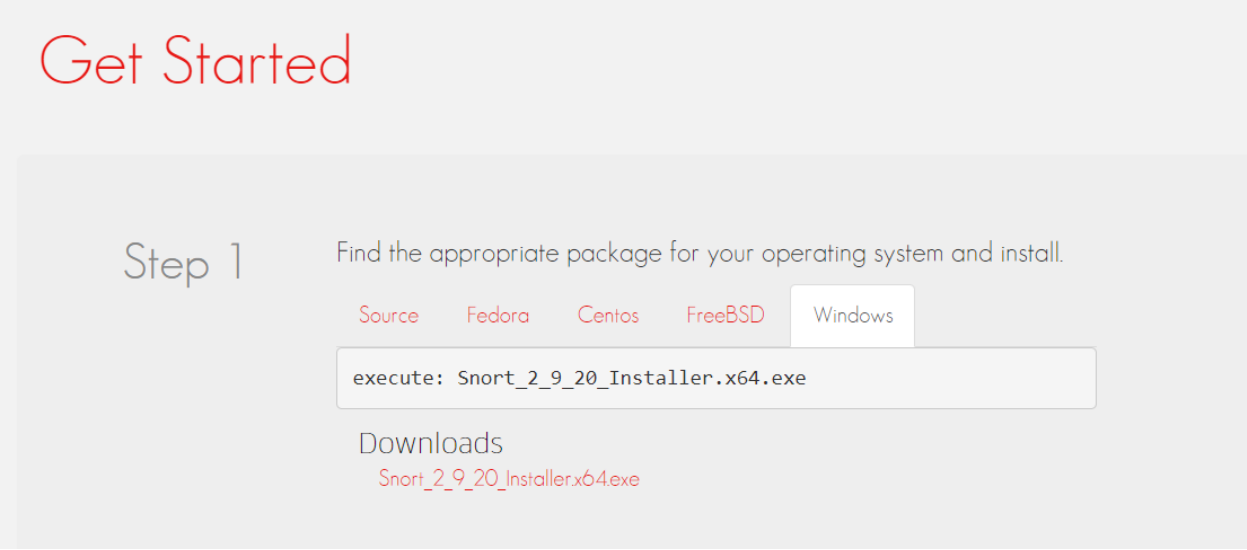
Cryptography and Network Security

Name: Piyush Mhaske Batch: B3
PRN : 2019BTECS00089

Snort Installation

Installed Snort



Check if Snort is running or not

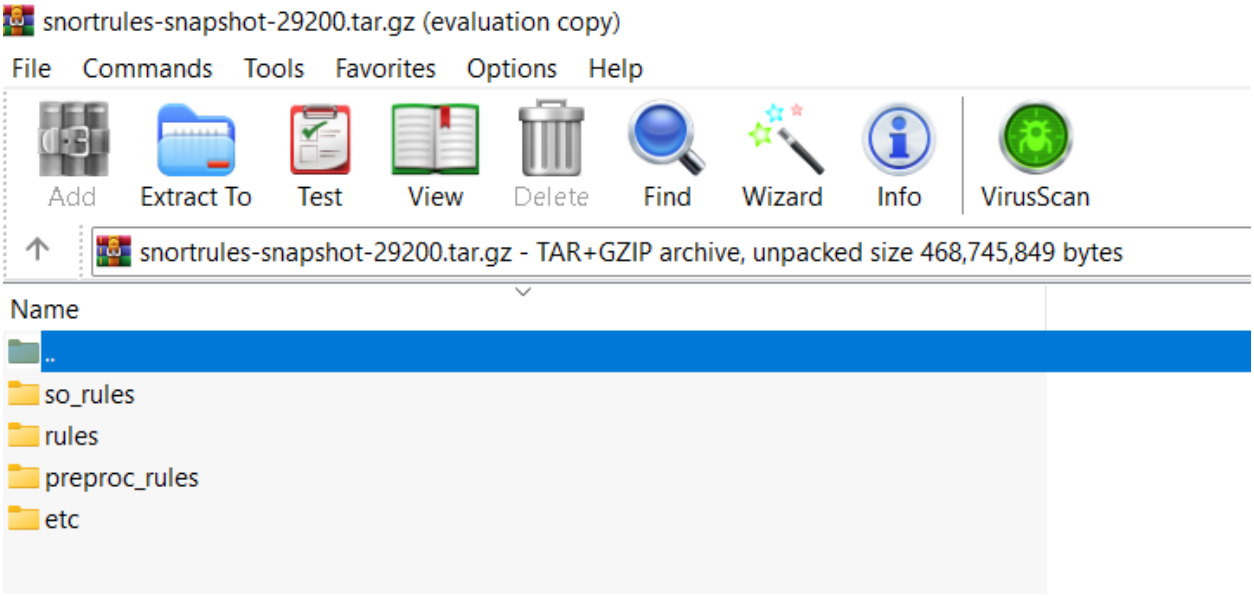
```
C:\Users\PIYUSH>cd \snort\bin\

C:\Snort\bin>snort -v

C:\Snort\bin>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_{EEE1FF57-4B95-4D93-AEE1-97ADE44AD4B9}".
Decoding Ethernet
```

Extract the below files



Add “rules” and “preproc_rules” to the c:\snort\rules and c:\snort\preproc_rules respectively

configure the snort.conf file

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.0.0/16

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

```
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_{EEE1FF57-4B95-4D93-AEE1-97ADE44AD4B9}      WAN Miniport (Ne
twork Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{4853F231-6318-433B-9488-DE41E26DC144}      WAN Miniport (IP
v6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{FBD8714C-2EBA-46DE-AF67-9AEC3705EDD9}      WAN Miniport (IP
)
    4   80:91:33:B7:2D:A3       10.40.7.3       \Device\NPF_{A34B63CC-94A7-4E31-86D3-6254CAC557CF}      Realtek 8821CE W
ireless LAN 802.11ac PCI-E NIC
    5   80:91:33:B7:2D:A2       169.254.105.186 \Device\NPF_{96E4B9E4-9A69-48B8-A09C-7442AB350041}      Bluetooth Device
```

Testing :

```
C:\Snort\bin>snort -i 4 -c c:\Snort\etc\snort.conf -T
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "c:\Snort\etc\snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 3702 4343 4848
5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 8243 8280 8300
8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 80:81 110 143 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3128 37
02 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180:8181 82
43 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:34444 41080 50002 55555 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
```

Add local.rules

and

Run :