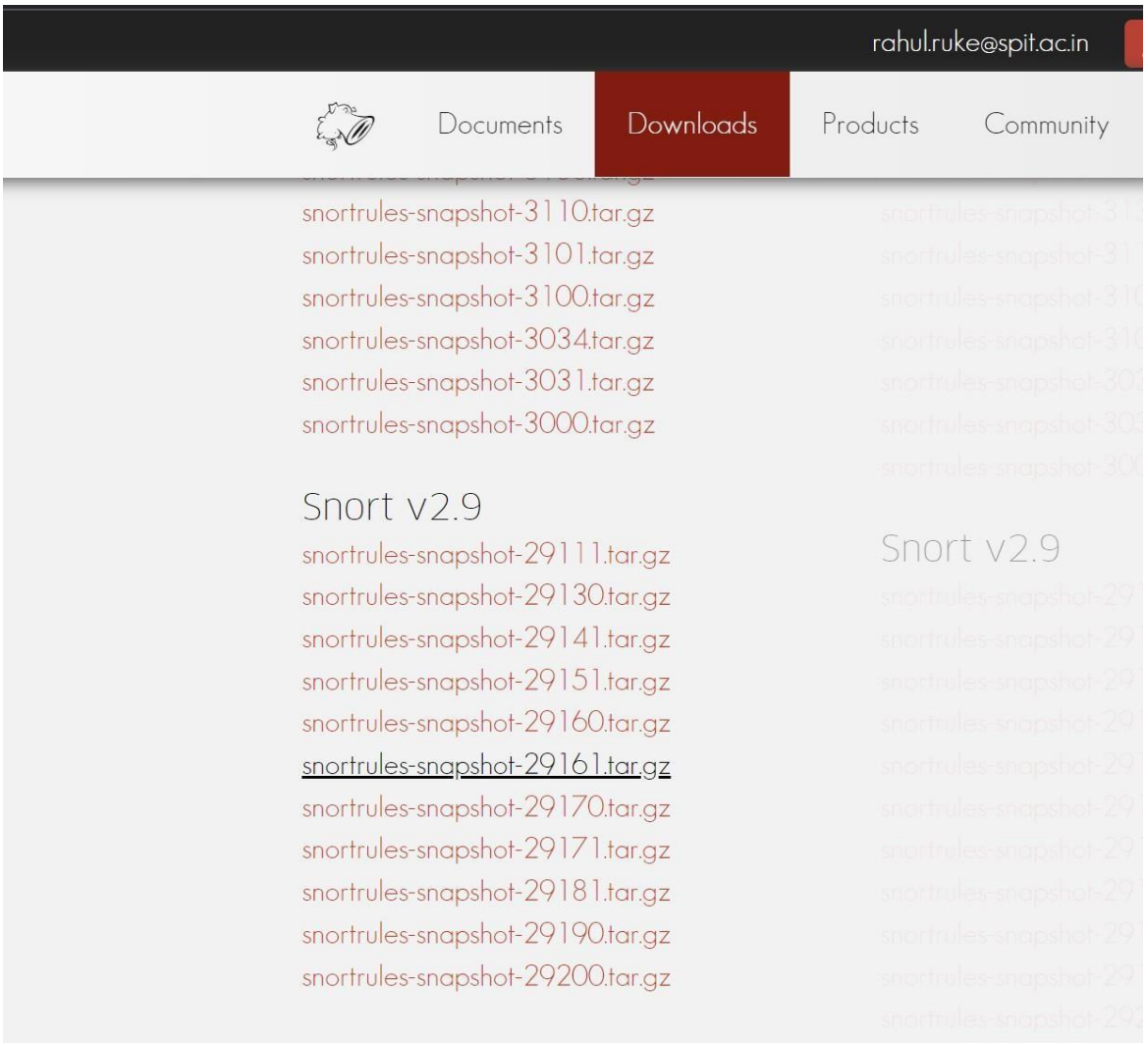
Name	**Hatim Sawai**
UID no.	**2021300108**
Experiment No.	9
AIM	Configure and application of SNORT Intrusion Detection System. Upload the compressed file as per the instruction in the lab session.

Step 1) Download Snort from snort.org and Choose the destination folder (default: `C:\Snort`).

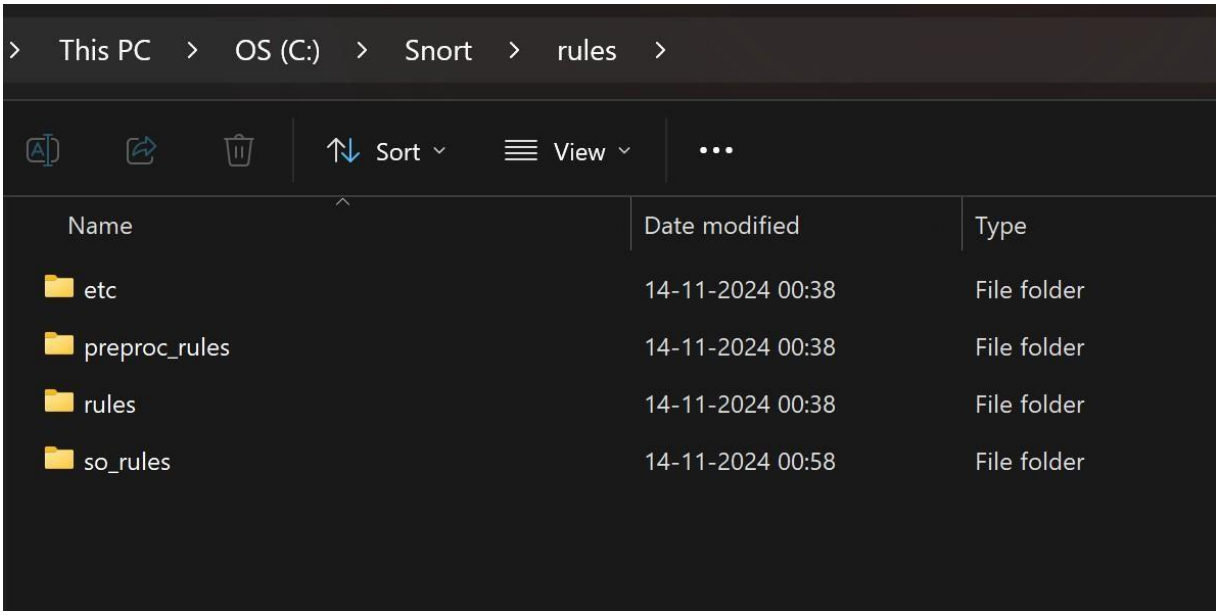
```
PS C:\Windows\system32> snort -V

   ,,_     -*> 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
```

Step 2) Download and Configure Rules (First you have to sign in to enable it)



Step 3) Extract this rule to C:\Snort\rules



Step 4) Editing the snort.conf file

```
# Step #1: Set the network variables.  For more information, see README.variables
#####################################################
ipvar HOME_NET 192.168.0.116
# Setup the network addresses you are protecting
ipvar HOME_NET any

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

```
# Note for Windows users:  You are advised to make this
# 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
```

```
# This is completely inconsistent with h
# Set the absolute path appropriately
var WHITE_LIST_PATH C:\Snort\rules
var BLACK_LIST_PATH C:\Snort\rules
```

```
# Configure default log directory for snort to log to.  For more informat
#
config logdir:C:\Snort\log
```

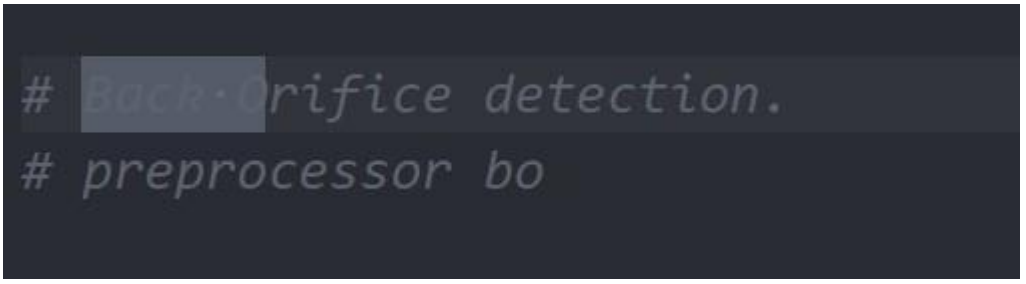
```
# path to dynamic preprocessor libraries
dynamicpreprocessor directory C:\Snort\lib\snort_dynamicpreprocessor

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

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

```
    utf_8 no \
    u_encode yes \
    webroot no
```

```
# Inline packet normalization. For more information, see README.normalize
# Does nothing in IDS mode
# preprocessor normalize_ip4
# preprocessor normalize_tcp: ips ecn stream
# preprocessor normalize_icmp4
# preprocessor normalize_ip6
# preprocessor normalize_icmp6
```




```
# Portscan detection.  For more information, see README.sfportscan
preprocessor sfportscan: proto  { all } memcap { 10000000 } sense_level { low }
```

```
# site specific rules
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
```

replacing the forward slash “/” with backslash “\”

```
# decoder and preprocessor event rules
# include $PREPROC_RULE_PATH\preprocessor.rules
# include $PREPROC_RULE_PATH\decoder.rules
# include $PREPROC_RULE_PATH\sensitive-data.rules
```

Put Decoders and Preprocessors Rules in Comments

```
PS C:\Windows\system32> 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_{091CE879-6833-48F5-A589-80E5DD71C55F}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{9201DD38-310A-49BF-A740-1310A4610E55}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{E21E6B76-A335-4C74-BF28-535A55D3DC38}      WAN Miniport (IP)
    4   A0:59:50:3A:9E:63       192.168.0.116   \Device\NPF_{62518E8F-10DA-4BA6-BD86-9C0A883B2638}      Intel(R) Wi-Fi 6E AX211 160MHz
    5   A2:59:50:3A:9E:63       169.254.250.189 \Device\NPF_{EE4E9351-8ABE-4065-9E29-F63CCAFF860C}      Microsoft Wi-Fi Direct Virtual Adapter #2
    6   A0:59:50:3A:9E:64       169.254.61.115  \Device\NPF_{468FF8AE-E10D-4028-AAB4-78ED0DEAA57E}      Microsoft Wi-Fi Direct Virtual Adapter
    7   0A:00:27:00:00:04       192.168.59.1    \Device\NPF_{1490E05C-FC57-4C94-884D-59DA89EE4977}      VirtualBox Host-Only Ethernet Adapter #2
    8   0A:00:27:00:00:0F       192.168.56.1    \Device\NPF_{A4930F34-2456-40DD-AA76-87BF53535FE8}      VirtualBox Host-Only Ethernet Adapter
    9   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback    Adapter for loopback traffic capture
```

Check the Interface

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

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Snort\etc\snort.conf"
C:\Snort\etc\snort.conf(45) Var 'HOME_NET' redefined.
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 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8
014 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 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
Tagged Packet Limit: 256
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
```

Execute the Snort tool in the command prompt by typing “snort –i 2 –c C:\Snort\etc\snort.conf

WRITE RULES TO DETECT SCANNING ATTACKS

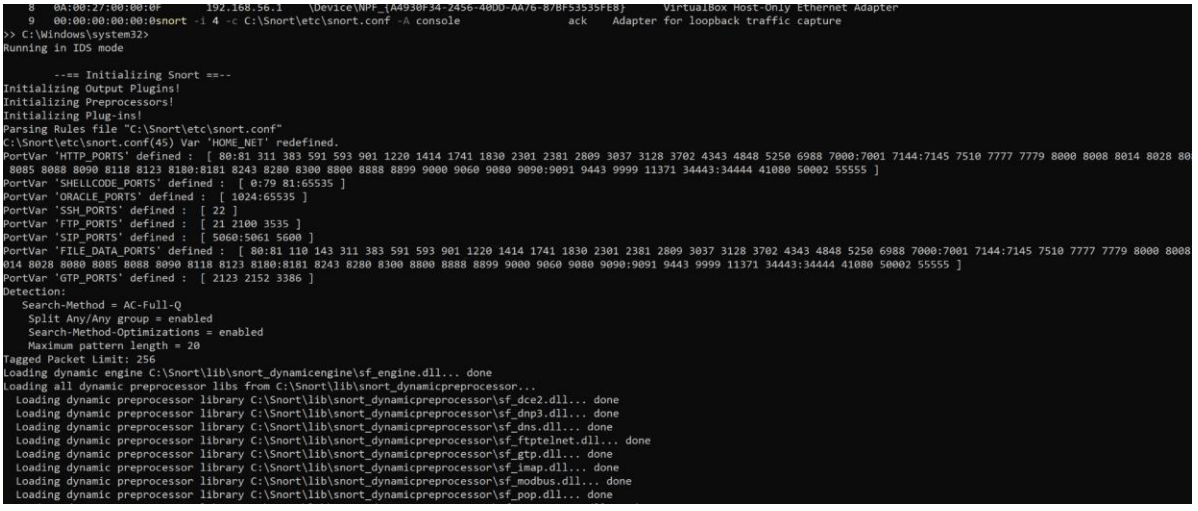
C: > Snort > rules > local.rules

snort inline

```
# Copyright 2001-2024 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 tcp any any -> any any (msg: "SYN attack"; flags: S; sid: 10000005;)
alert udp any any -> 192.168.0.116 any (msg: "UDP Scan"; sid: 10001; rev: 1;)
alert icmp any any -> 192.168.0.116 any (msg: "PING Scan"; dsize:0;sid:10002; rev: 1;)
alert tcp any any -> $HOME_NET any (msg: "FIN Scan";flags: F; sid: 10003;rev: 1;)
alert tcp any any -> $HOME_NET any (msg: "NULL Scan";flags: 0; sid: 10004;rev: 1;)
alert tcp 192.168.0.116 any -> $HOME_NET 22 (msg:"XMAS Scan"; flags: FPU; sid: 10005;rev: 1;)
alert tcp 192.168.0.116 any -> 192.168.0.116 any (msg:"TCP Scan"; flags: S,12; sid: 10006;rev: 1;)
```

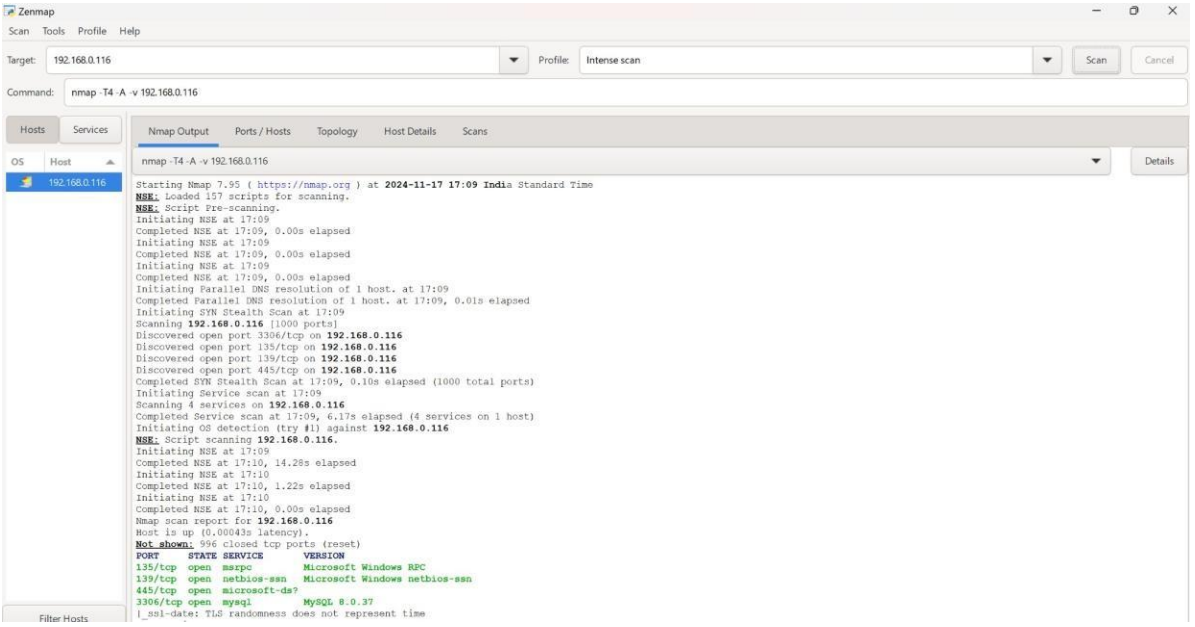
Adding Rules in local.rules



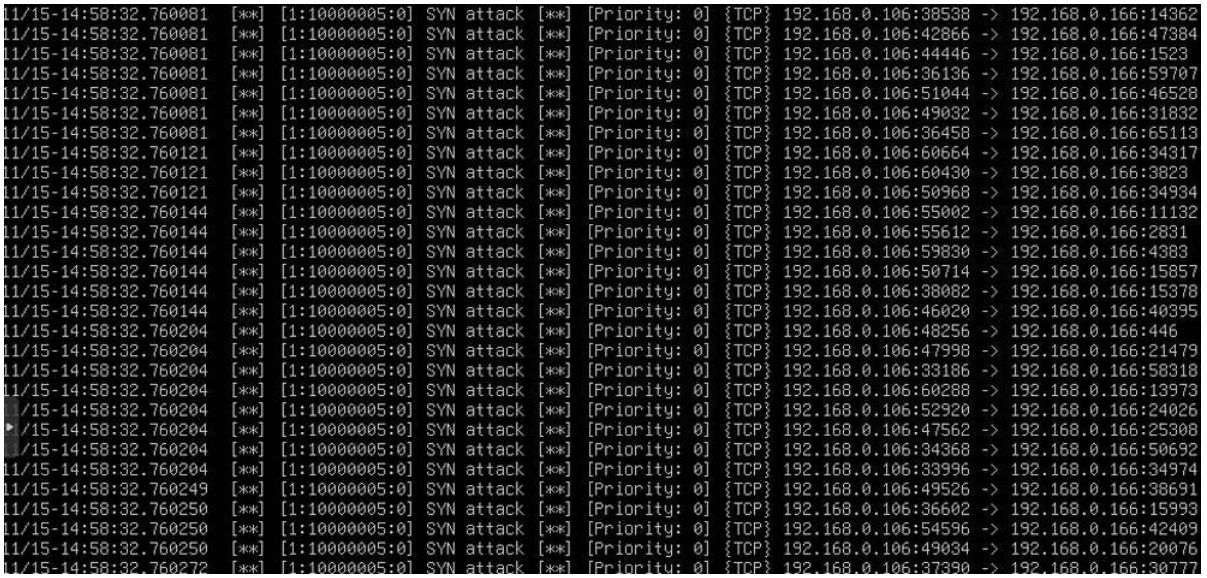
Running Snort in IDS mode

```
PS C:\> nmap -p 1-65535 -v 192.168.0.116
Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-17 17:18 India Standard Time
Initiating Parallel DNS resolution of 1 host. at 17:18
Completed Parallel DNS resolution of 1 host. at 17:18, 0.01s elapsed
Initiating SYN Stealth Scan at 17:18
Scanning 192.168.0.116 [65535 ports]
Discovered open port 445/tcp on 192.168.0.116
Discovered open port 3306/tcp on 192.168.0.116
Discovered open port 139/tcp on 192.168.0.116
Discovered open port 135/tcp on 192.168.0.116
Discovered open port 33060/tcp on 192.168.0.116
Discovered open port 49664/tcp on 192.168.0.116
Discovered open port 5040/tcp on 192.168.0.116
Discovered open port 49671/tcp on 192.168.0.116
Discovered open port 49665/tcp on 192.168.0.116
Discovered open port 49670/tcp on 192.168.0.116
Discovered open port 5433/tcp on 192.168.0.116
Discovered open port 49672/tcp on 192.168.0.116
Discovered open port 49686/tcp on 192.168.0.116
Completed SYN Stealth Scan at 17:18, 3.93s elapsed (65535 total ports)
Nmap scan report for 192.168.0.116
Host is up (0.000088s latency).
```

Network Scanning Attack with Nmap Tool



Network Scanning Attack with Zenmap Tool



Detection of Network Scanning Attack with Snort IDS