

<b>Name</b>	<b>Akshat Biniwale</b>
<b>UID</b>	<b>2021300014</b>
<b>Branch</b>	<b>BE COMPS A</b>
<b>Batch</b>	<b>VI</b>
<b>Subject</b>	<b>Cryptography and System Security</b>
<b>Experiment</b>	<b>9</b>

### **Aim:**

Configure and application of SNORT Intrusion Detection System

### **Objective:**

- To configure and utilize Snort as a Network Intrusion Detection System (NIDS) to monitor and detect malicious activities such as SYN scans, UDP scans, and other network-based attacks.
- To write and implement custom Snort rules for identifying specific network attacks and analysing alerts generated during the intrusion detection process.

### **Theory:**

Snort is an open-source tool for Intrusion Detection and Prevention System. It uses a series of rules that help define malicious network activities and uses those rules to find packets that match against them and generates alerts for users.

Snort has 3 primary uses:

1. A packet sniffer like tcpdump
2. A packet logger - which is useful for network traffic debugging
3. As a full-blown network intrusion prevention system

Features:

- Rules: To generate rules to identify various kinds of scans such as TCP scan, UDP scan, FIN scan, etc.
- Attack Detection: To detect network scanning attacks, DoS attack, malware attack, etc.

## Procedure:

1. Download snort from their official website [www.snort.org/downloads](http://www.snort.org/downloads)

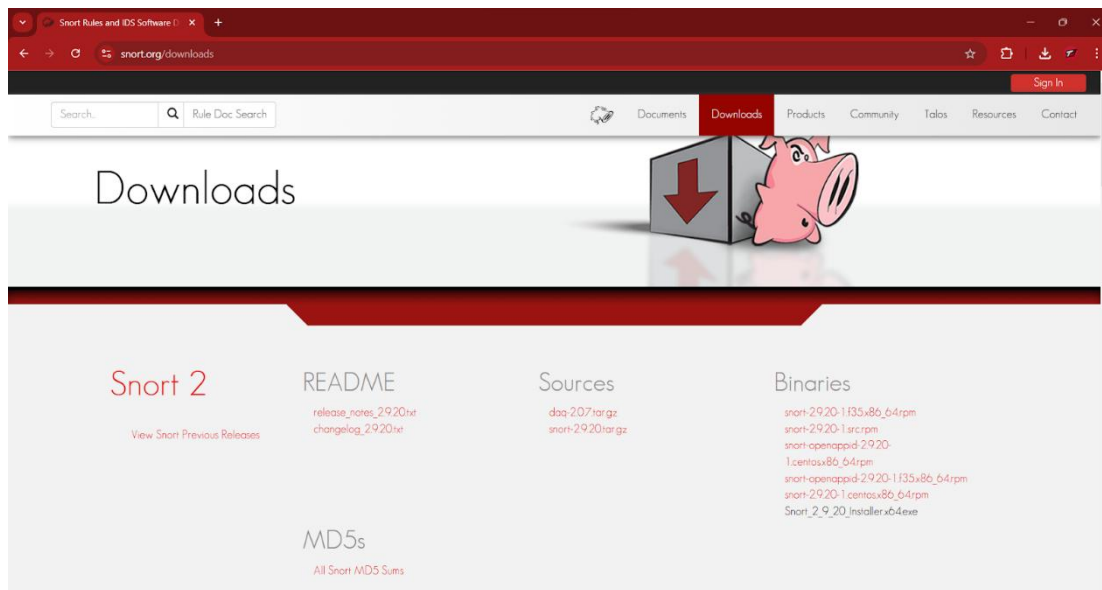


Fig 1.

2. Follow the setup wizard and install snort

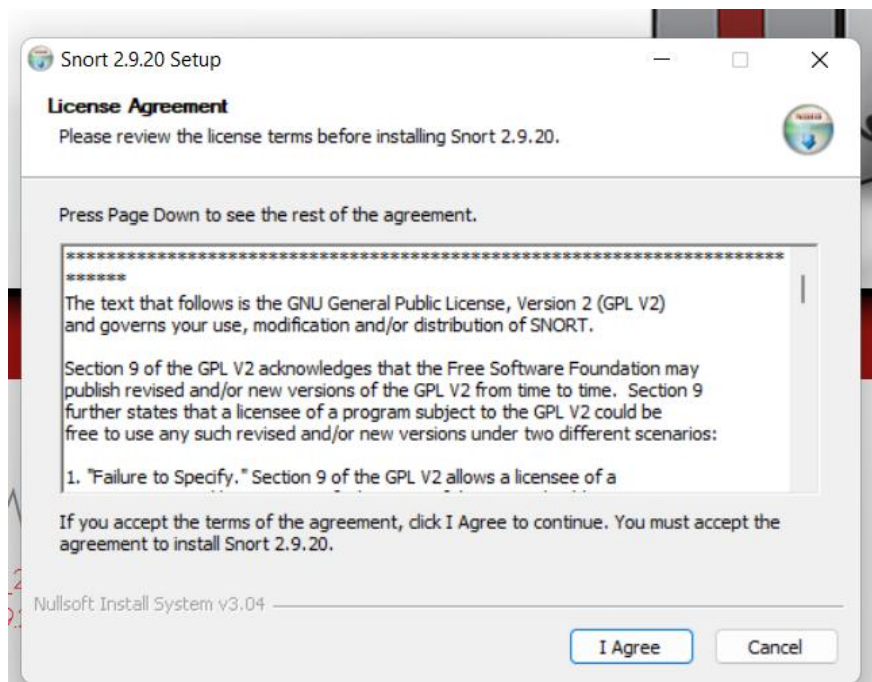


Fig 2.

- Go to C:/Snort/bin folder and check if snort is properly installed using the -V flag. If snort is properly installed it will show the version of Snort.

```
PowerShell
PS C:\Users\Qwerty> cd C:/Snort/bin
PS 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

PS C:\Snort\bin>
```

Fig 3.

- Login in Snort to download Snort rules

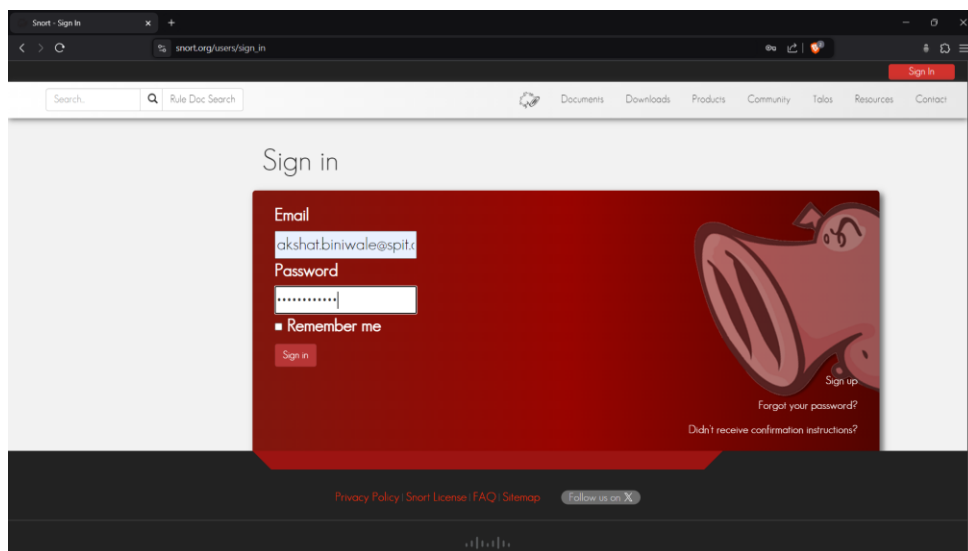


Fig 4.

- Download the rules of the correct installed version, here 2.9.20

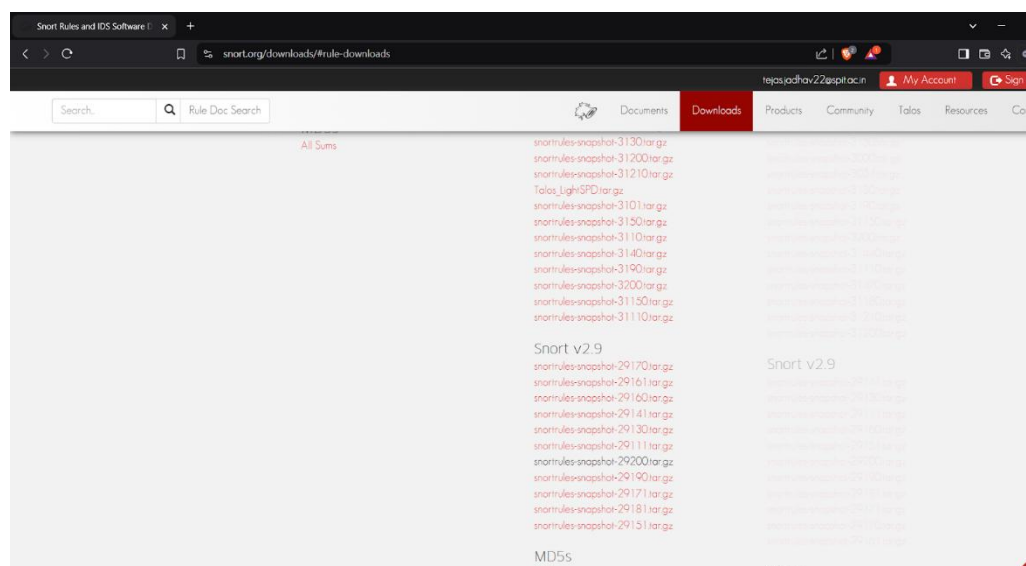


Fig 5.

## 6. Edit the snort.conf File:

- Navigate to C:\Snort\etc\snort.conf and configure:
  - Network variables like \$HOME\_NET and \$EXTERNAL\_NET.
  - Paths for rules, preproc\_rules, and log files.
  - Include custom rule files (e.g., local.rules).
- Define paths for white.list and black.list if using reputation-based detection.

## 7. Create and Add Custom Rules:

- Open local.rules in the Snort rules directory.
- Add custom rules to detect various attacks, such as SYN scans or ICMP packets.

## 8. Run Snort and Test Setup:

- Use the -W option to list available interfaces, then specify the correct one with -i.
- Run Snort in IDS mode with the command:
  - `snort -i <interface_number> -c C:\Snort\etc\snort.conf -A console`
- Perform network scans or attacks from another machine using tools like Nmap and verify that alerts are generated in the console or log files.

## Screenshots:

```
Administrator: Command Prompt - snort -i 2 -c C:\Users\aksha\Snort\etc\snort.conf
Base64 Decoding: Enabled
Base64 Decoding Depth: Unlimited
Quoted-Printable Decoding: Enabled
Quoted-Printable Decoding Depth: Unlimited
Unix-to-Unix Decoding: Enabled
Unix-to-Unix Decoding Depth: Unlimited
Non-Encoded MIME attachment Extraction: Enabled
Non-Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
  Ports: 110
  POP Maxcap: 838860
  MIME Max Mem: 838860
  Base64 Decoding: Enabled
  Base64 Decoding Depth: Unlimited
  Quoted-Printable Decoding: Enabled
  Quoted-Printable Decoding Depth: Unlimited
  Unix-to-Unix Decoding: Enabled
  Unix-to-Unix Decoding Depth: Unlimited
  Non-Encoded MIME attachment Extraction: Enabled
  Non-Encoded MIME attachment Extraction Depth: Unlimited
IMAP Config:
  Ports: 143
  IMAP Maxcap: 838860
  Base64 Decoding: Enabled
  Base64 Decoding Depth: Unlimited
  Quoted-Printable Decoding: Enabled
  Quoted-Printable Decoding Depth: Unlimited
  Unix-to-Unix Decoding: Enabled
  Unix-to-Unix Decoding Depth: Unlimited
  Non-Encoded MIME attachment Extraction: Enabled
  Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
  Ports: 502
  Modbus Maxcap: 262144
  Check Link-Layer CRCs: ENABLED
  Ports: 20000
Reputation config:
ERROR: C:\Users\aksha\Snort\etc\snort.conf(514) => Unable to open address file C:\Users\aksha\Snort\rules\white.list, Error: No such file or directory
Fatal Error, Quitting..
C:\Users\aksha\Snort\bin\snort -i 2 -c C:\Users\aksha\Snort\etc\snort.conf
Running in IDS mode

--= Initializing Snort =--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "C:\Users\aksha\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 5080 ]
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 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 'GTP_PORTS' defined : [ 2123 2152 3386 ]
Detection:
Search-Method = AC-Full-Q
```

Fig 6.

```
Administrator: Command Prompt - snort - 1 - C:\Users\aksha\Snort\snort.conf - A console
Alphabet Size : 256 Chars
Slurp State : Variable (1,2,4 bytes)
Instances : 226
1 byte states : 213
2 byte states : 11
4 byte states : 2
Characters : 228337
States : 181029
Transitions : 31652109
State Density : 68.3%
Patterns : 10735
Match States : 11829
Memory (MB) : 161.73
Patterns : 1.25
Match Lists : 2.84
DFA
1 byte states : 1.25
2 byte states : 18.95
4 byte states : 137.05

-----
Number of patterns truncated to 20 bytes: 645 ]
Ncap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "Device\NPF_{50947129-765A-41F4-8A6F-302CF9268C9}".
Decoding Ethernet

---- Initialization Complete ----

-> Snort! <-
Version 2.9.20-MIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contactteam
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

Administrator: Command Prompt
C:\Users\aksha\Snort\bin>

Preprocessor Object: SF_MQOBS Version 1.1 <Build 1>
Preprocessor Object: SF_DMP Version 1.0 <Build 1>
Preprocessor Object: SF_GIP Version 1.1 <Build 1>
Preprocessor Object: SF_FIPIELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DWP Version 1.1 <Build 1>
Preprocessor Object: SF_DKRPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=6918)
```

Fig 7.

```
Administrator: Command Prompt - snort - 1 - C:\Users\aksha\Snort\snort.conf - A console
2 byte states : 11
4 byte states : 2
Characters : 228337
States : 181029
Transitions : 31652109
State Density : 68.3%
Patterns : 10735
Match States : 11829
Memory (MB) : 161.73
Patterns : 1.25
Match Lists : 2.84
DFA
1 byte states : 1.25
2 byte states : 18.95
4 byte states : 137.05

-----
Number of patterns truncated to 20 bytes: 645 ]
Ncap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "Device\NPF_{D9A55857-3808-498F-9E25-8A6C258D1083}".
Decoding Ethernet

---- Initialization Complete ----

-> Snort! <-
Version 2.9.20-MIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contactteam
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_SHORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SOF 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_MQOBS Version 1.1 <Build 1>
Preprocessor Object: SF_DMP Version 1.0 <Build 1>
Preprocessor Object: SF_GIP Version 1.1 <Build 1>
Preprocessor Object: SF_FIPIELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DWP Version 1.1 <Build 1>
Preprocessor Object: SF_DKRPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=11912)

Administrator: Command Prompt
Microsoft Windows [Version 10.0.26100.2314]
(c) Microsoft Corporation. All rights reserved.

C:\Windows\System32>cd ..
C:\Windows>cd ..
C:\>cd Users\aksha/
C:\Users\aksha>map --version
Map version 7.95 ( https://nmap.org )
Platform: 1686-pc-windows-windows
Compiled with: nmap-liblua-5.4.6 openssl-3.0.13 nmap-libssh2-1.11.0 nmap-libz-1.3.1 nmap-libpcap2-10.43 Npcap-1.8
0 nmap-libndt-1.12 ipv6
Compiled without:
Available nsock engines: loop poll select

C:\Users\aksha>map -p 1-65535 -v 192.168.0.100
Starting Map 7.95 ( https://nmap.org ) at 2024-11-14 15:31:11 India Standard Time
Initiating Parallel DNS resolution of 1 host, at 15:31
Completed Parallel DNS resolution of 1 host, at 15:31, 0.01s elapsed
Initiating SYN Stealth Scan at 15:31
Scanning 192.168.0.100 (65535 ports)
Discovered open port 445/tcp on 192.168.0.100
Discovered open port 3386/tcp on 192.168.0.100
Discovered open port 139/tcp on 192.168.0.100
Discovered open port 135/tcp on 192.168.0.100
Discovered open port 4868/tcp on 192.168.0.100
Discovered open port 6896/tcp on 192.168.0.100
Discovered open port 49665/tcp on 192.168.0.100
```

Fig 8.

```
Administrator: Command Prompt - snort - 1 - C:\Users\aksha\Snort\snort.conf - A console
2 byte states : 11
4 byte states : 2
Characters : 228337
States : 181029
Transitions : 31652109
State Density : 68.3%
Patterns : 10735
Match States : 11829
Memory (MB) : 161.73
Patterns : 1.25
Match Lists : 2.84
DFA
1 byte states : 1.25
2 byte states : 18.95
4 byte states : 137.05

-----
Number of patterns truncated to 20 bytes: 645 ]
Ncap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "Device\NPF_{D9A55857-3808-498F-9E25-8A6C258D1083}".
Decoding Ethernet

---- Initialization Complete ----

-> Snort! <-
Version 2.9.20-MIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contactteam
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_SHORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSH Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SOF 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_MQOBS Version 1.1 <Build 1>
Preprocessor Object: SF_DMP Version 1.0 <Build 1>
Preprocessor Object: SF_GIP Version 1.1 <Build 1>
Preprocessor Object: SF_FIPIELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DWP Version 1.1 <Build 1>
Preprocessor Object: SF_DKRPC2 Version 1.0 <Build 3>
Commencing packet processing (pid=11912)

Administrator: Command Prompt
Read data files from: C:\Program Files (x86)\Nmap
Map done: 1 IP address (1 host up) scanned in 4.17 seconds
Raw packets sent: 65337 (2.88MB) | Recv: 131807 (5.50MB)

C:\Users\aksha>
```

Fig 10.



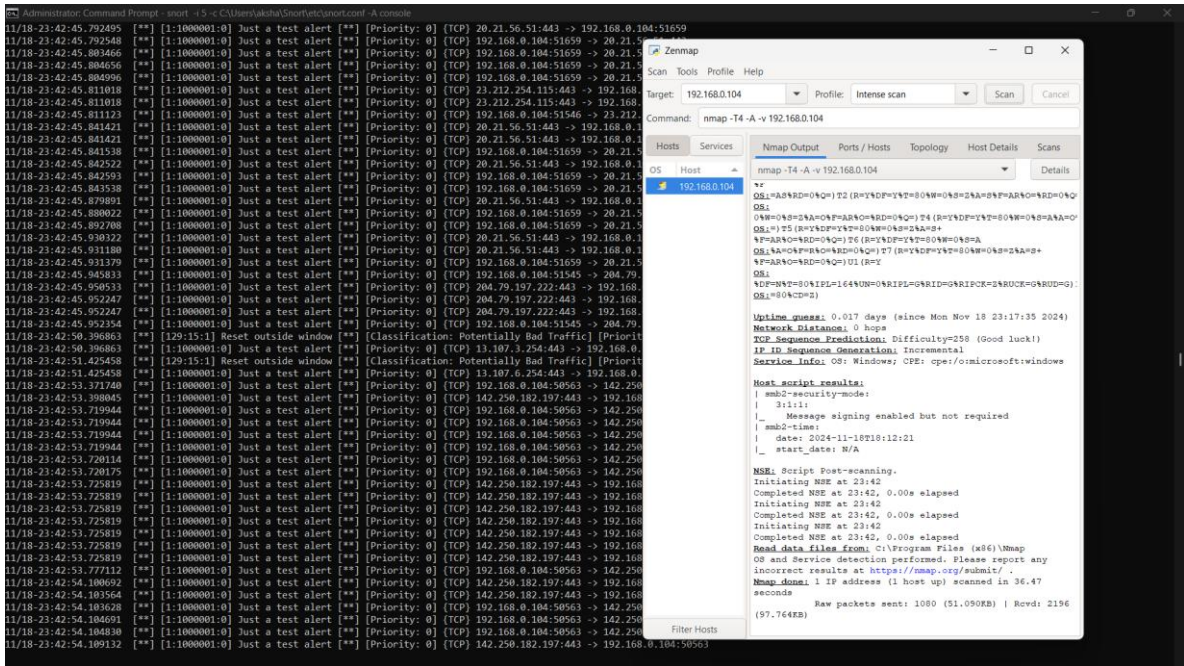


Fig 11.

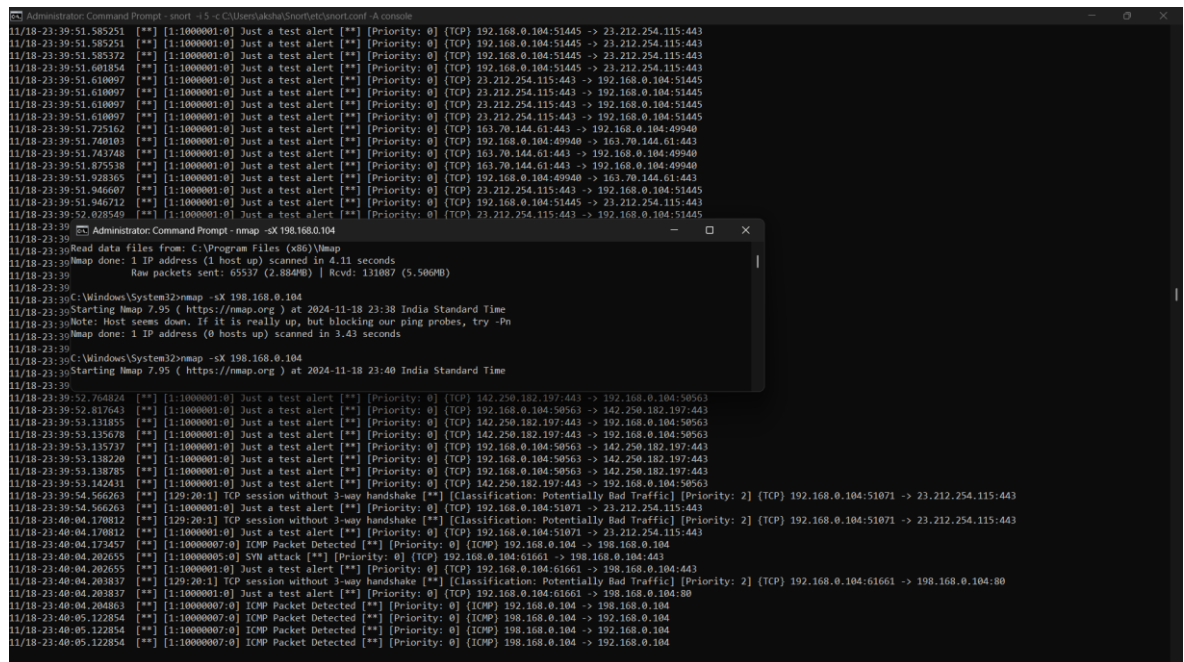


Fig 12.

## Conclusion:

This experiment demonstrated the effectiveness of Snort in detecting network intrusions, such as an Nmap OS scan attack, showcasing its utility as a powerful intrusion detection system (IDS). Snort provides real-time monitoring and alerts to help secure networks against potential threats.

- Snort can successfully detect reconnaissance attacks like Nmap OS scans, helping to prevent further exploitation.
- Configuring Snort rules enhances its accuracy and adaptability to diverse attack scenarios.