ST. FRANCIS INSTITUTE OF TECHNOLOGY
DEPARTMENT OF INFORMATION TECHNOLOGY
SECURITY LAB

Experiment – 10: Study of Intrusion detection system using SNORT

Aim: To study the Intrusion detection system using SNORT.

Objective: After performing the experiment, the students will be able to explore and use the Snort-IDS tool.

Lab objective mapped: L502.6: Students should be able to apply network security basics, analyze different attacks on networks and evaluate the performance of firewalls and security protocols, such as SSL, IPSEC, and PGP, and authentication mechanisms to design secure applications.

Prerequisite: Basic knowledge of network security.

Requirements: Windows OS, SNORT

Pre-Experiment Theory:

Snort is an open-source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

Snort can be configured to run in three modes:

1. **Sniffer mode**: It simply reads the packets of the network and displays them for you in a continuous stream on the console (screen)
2. **Packet Logger mode**: logs the packets to disk.
3. **Network Intrusion Detection System (NIDS) mode**: It performs detection and analysis on network traffic. This is the most complex and configurable mode.

Implementation:

1. Install snort on your system. Refer/download the snort user manual from its official website [1].
2. Test snort IDS using following commands, observe the output of each command. Take screenshots (SS). Write your observations under each SS.

```
a. Snort –V
b. Snort -h
c. Snort –W
d. Snort –i interface number -v
e. Snort –i interface number -vd
```

2. Run following command to use snort in Packet logger mode. View the log file created. Observe the content of log file using any packet logger software (e.g. Wireshark). Take SS of command output, the log file creation and the content of the log file. Write your observations under each SS.

```
Snort –i interface number -dev -1 C:\Snort\log
```

3. Learn commands to use snort as IDS. Observe the snort rule file *(i.e., snort.conf file)*. Analyze the rule file to configure it for your network environment.

```
Snort -i interface number -dev -l C:\Snort\log -h
192.168.1.0/24 -c snort.conf
```

Post Experimental Exercise- *(to be handwritten on journal sheets. Refer snort user manual for answers)*

1. _______ snort command displays packet header, packet data as well as the data link layer headers.
2. Explain the snort command that will be used for logging the packets on a high-speed network.
3. Explain the use of '-h' option/switch while writing the snort rule.
4. Explain in detail Snort's NIDS mode output options.
5. Explain the following snort command `'snort -c snort.conf -A fast -h 192.168.1.0/24'`

Conclusion:

In this experiment we were introduced to most used IPS/IDS software 'Snort'. Snort acts as a security guard for any network, providing a proactive detection and prevention of any type of intrusion. Snort can perform packet sniffing, logging, and intrusion detection. We studied various options/switches that can be used for writing intrusion detection rules, for sniffing the network and for logging the network traffic.

References:

[1] "Snort User's Manual 2.9.16", https://snort.org/

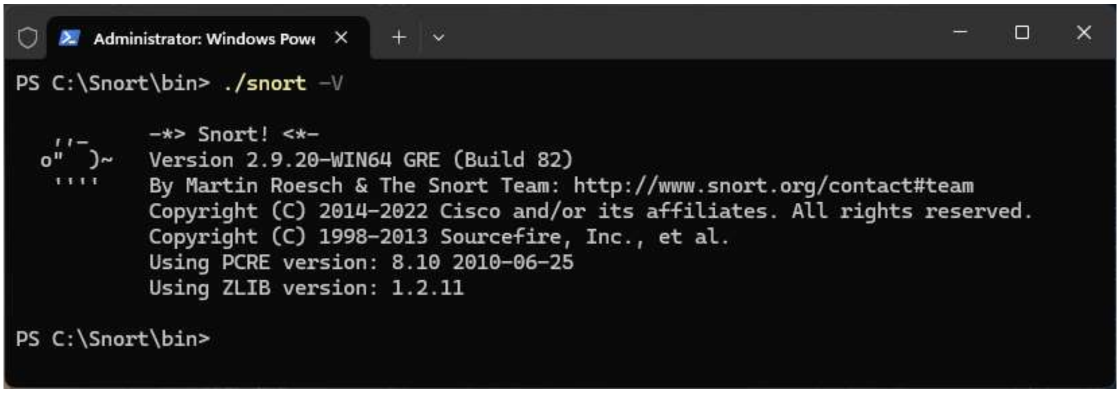
[2] Bart Lenaerts-Bergmans , "SNORT AND SNORT RULES EXPLAINED", https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/snort-rules/

[3] "Basic snort rules syntax and usage", https://resources.infosecinstitute.com/topics/penetration-testing/snort-rules-workshop-part-one/

[4] "Writing Snort Rules with Examples and Cheat Sheet", https://cyvatar.ai/write-configure-snort-rules/

[5] "INSTALLING & CONFIGURING SNORT| INSTALASI SNORT WINDOWS 11", https://youtu.be/V6B8B7_6gfE

Snort -V



```
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>
```

The command snort -V is used to display the version of Snort installed. In this output, Snort version 2.9.20 for Windows 64-bit (WIN64 GRE Build 82) is shown. It also provides information about the PCRE (Perl Compatible Regular Expressions) and ZLIB versions used. This helps verify that Snort is correctly installed and provides details on the underlying libraries it uses for regular expressions and compression.

Snort -h

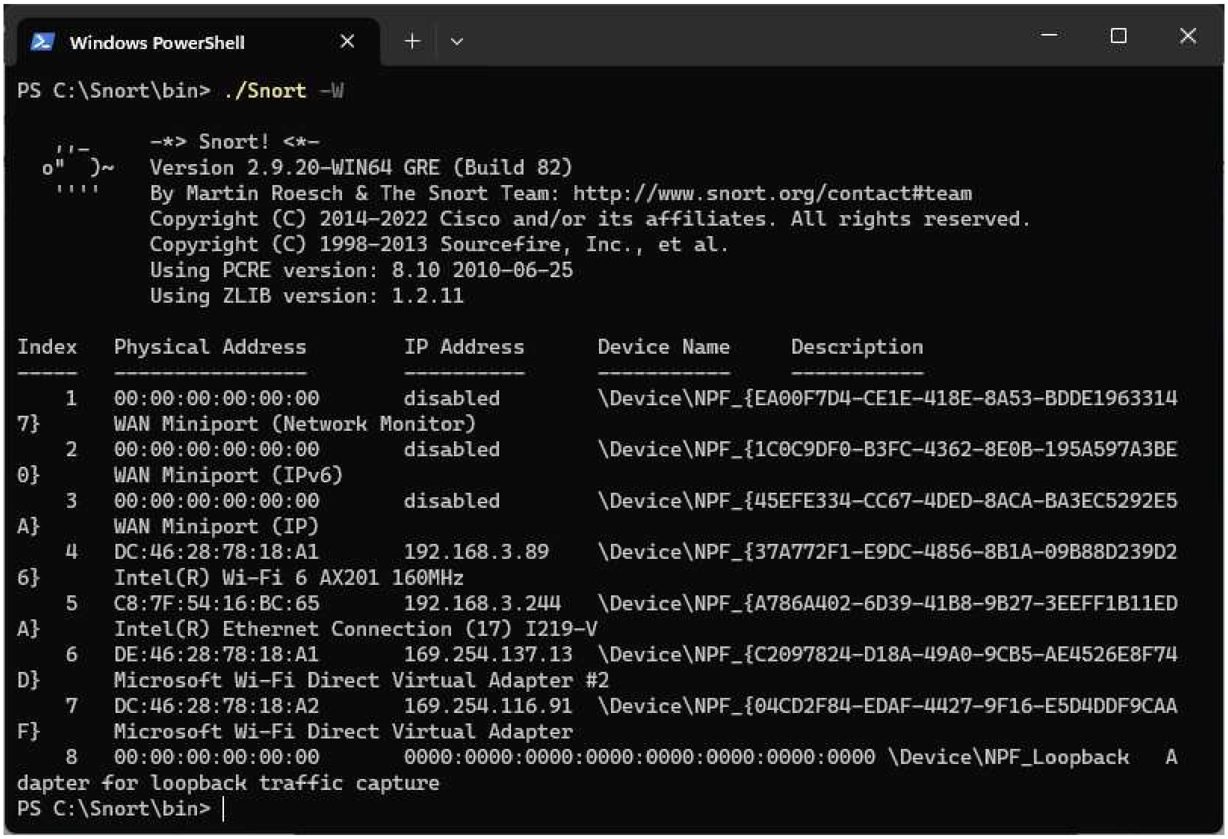
```
C:\Snort\bin\snort.exe: option requires an argument -- h

   ,,_     -*> 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: C:\Snort\bin\snort.exe [-options] <filter options>

       C:\Snort\bin\snort.exe /SERVICE /INSTALL [-options] <filter options>

       C:\Snort\bin\snort.exe /SERVICE /UNINSTALL

       C:\Snort\bin\snort.exe /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

        -F <bpf>   Read BPF filters from file <bpf>

        -G <0xid>  Log Identifier (to uniquely id events for multiple snorts)

        -h <hn>    Set home network = <hn>

                   (for use with -l or -B, does NOT change $HOME_NET in IDS
mode)

        -H         Make hash tables deterministic.

        -i <if>    Listen on interface <if>

        -I         Add Interface name to alert output

        -k <mode>  Checksum mode (all,noip,notcp,noudp,noicmp,none)

        -K <mode>  Logging mode (pcap[default],ascii,none)

        -l <ld>    Log to directory <ld>

        -L <file>  Log to this tcpdump file

        -n <cnt>   Exit after receiving <cnt> packets

        -N         Turn off logging (alerts still work)

        -O         Obfuscate the logged IP addresses

        -p         Disable promiscuous mode sniffing

        -P <snap>  Set explicit snaplen of packet (default: 1514)

        -q         Quiet. Don't show banner and status report

        -r <tf>    Read and process tcpdump file <tf>
        -R <id>    Include 'id' in snort_intf<id>.pid file name

        -s         Log alert messages to syslog

        -S <n=v>   Set rules file variable n equal to value v

        -T         Test and report on the current Snort configuration

        -U         Use UTC for timestamps

        -v         Be verbose

        -V         Show version number

        -W         Lists available interfaces. (Win32 only)

        -X         Dump the raw packet data starting at the link layer

        -x         Exit if Snort configuration problems occur

        -y         Include year in timestamp in the alert and log files

        -z <file>  Set the preproc_memstats file path and name

        -Z <file>  Set the performonitor preprocessor file path and name

        -?         Show this information

<Filter Options> are standard BPF options, as seen in TCPDump

Longname options and their corresponding single char version

   --logid <0xid>                  Same as -G

   --perfmon-file <file>           Same as -Z

   --pid-path <dir>                Specify the directory for the Snort PID file

   --snaplen <snap>                Same as -P

   --help                          Same as -?

   --version                       Same as -V

   --alert-before-pass             Process alert, drop, sdrop, or reject before
pass, default is pass before alert, drop,...

   --treat-drop-as-alert           Converts drop, sdrop, and reject rules into
alert rules during startup

   --treat-drop-as-ignore          Use drop, sdrop, and reject rules to ignore
session traffic when not inline.

   --process-all-events            Process all queued events (drop, alert,...),
default stops after 1st action group
```

```
   --enable-inline-test           Enable Inline-Test Mode Operation

   --dynamic-engine-lib <file>     Load a dynamic detection engine

   --dynamic-engine-lib-dir <path> Load all dynamic engines from directory

   --dynamic-detection-lib <file>  Load a dynamic rules library

   --dynamic-detection-lib-dir <path> Load all dynamic rules libraries from
directory

   --dump-dynamic-rules <path>     Creates stub rule files of all loaded rules
libraries

   --dynamic-preprocessor-lib <file>  Load a dynamic preprocessor library

   --dynamic-preprocessor-lib-dir <path> Load all dynamic preprocessor libraries
from directory

   --dynamic-output-lib <file>  Load a dynamic output library

   --dynamic-output-lib-dir <path> Load all dynamic output libraries from
directory

   --pcap-single <tf>              Same as -r.

   --pcap-file <file>              file that contains a list of pcaps to read -
read mode is implied.

   --pcap-list "<list>"            a space separated list of pcaps to read -
read mode is implied.

   --pcap-loop <count>             this option will read the pcaps specified on
command line continuously.

                                   for <count> times.  A value of 0 will read
until Snort is terminated.

   --pcap-reset                    if reading multiple pcaps, reset snort to
post-configuration state before reading next pcap.

   --pcap-show                     print a line saying what pcap is currently
being read.

   --exit-check <count>            Signal termination after <count> callbacks
from DAQ_Acquire(), showing the time it

                                   takes from signaling until DAQ_Stop() is
called.

   --conf-error-out                Same as -x

   --enable-mpls-multicast         Allow multicast MPLS

   --enable-mpls-overlapping-ip    Handle overlapping IPs within MPLS clouds
   --max-mpls-labelchain-len       Specify the max MPLS label chain

   --mpls-payload-type             Specify the protocol (ipv4, ipv6, ethernet)
that is encapsulated by MPLS

   --require-rule-sid              Require that all snort rules have SID
specified.

   --daq <type>                    Select packet acquisition module (default is
pcap).

   --daq-mode <mode>               Select the DAQ operating mode.

   --daq-var <name=value>          Specify extra DAQ configuration variable.

   --daq-dir <dir>                 Tell snort where to find desired DAQ.

   --daq-list[=<dir>]              List packet acquisition modules available in
dir.  Default is static modules only.

   --dirty-pig                     Don't flush packets and release memory on
shutdown.

   --cs-dir <dir>                  Directory to use for control socket.

   --ha-peer                       Activate live high-availability state sharing
with peer.

   --ha-out <file>                 Write high-availability events to this file.

   --ha-in <file>                  Read high-availability events from this file
on startup (warm-start).

   --suppress-config-log           Suppress configuration information output.
```

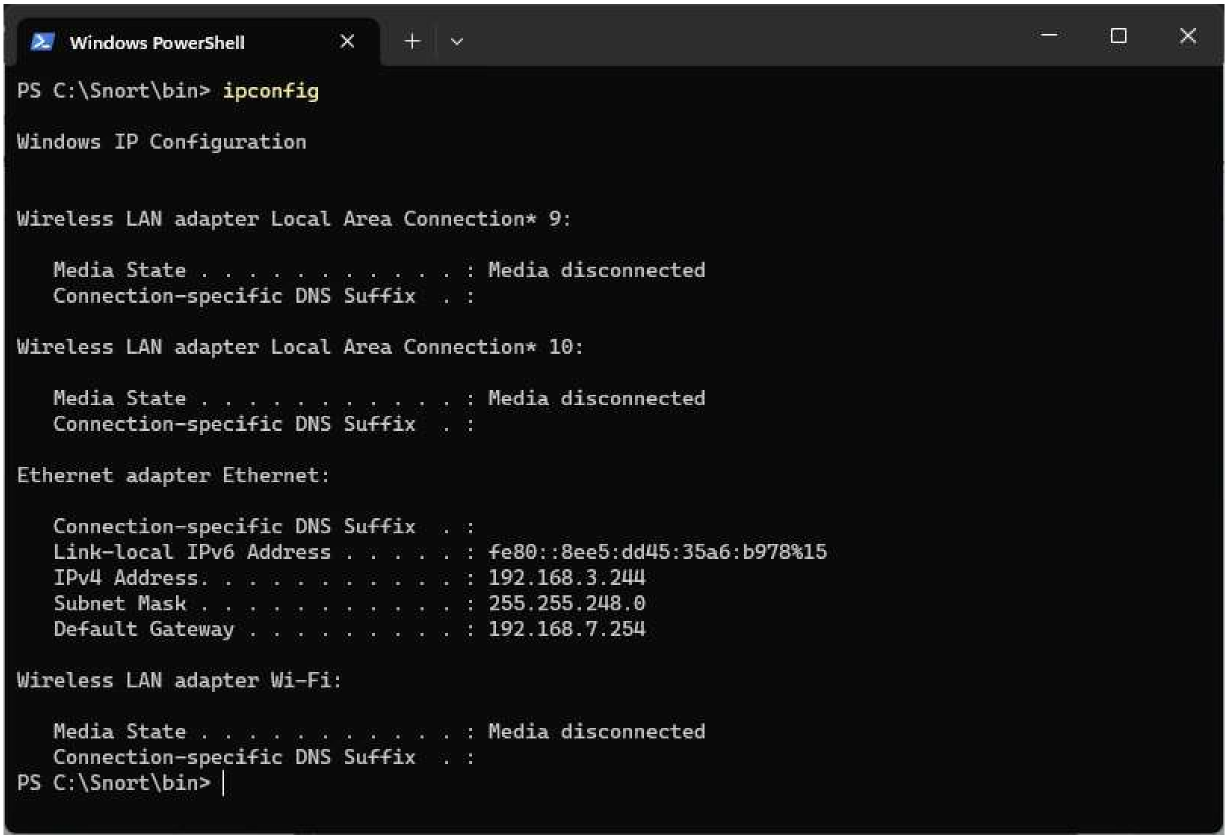
The command `snort -h` displays the help information for Snort, providing users with a list of available command-line options and flags. This is useful for understanding how to configure and run Snort for various purposes, such as packet capturing, intrusion detection, or logging.

—---

Snort -W



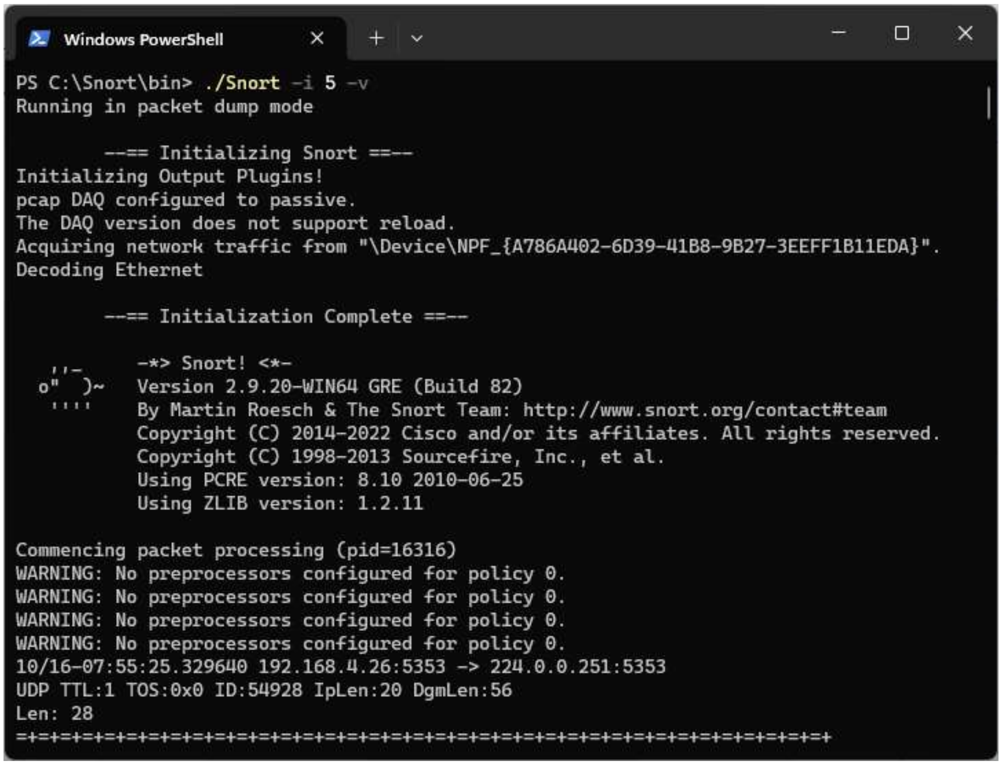
```
PS C:\Snort\bin> ./Snort -W

   ,,_     -*> 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_{EA00F7D4-CE1E-418E-8A53-BDDE1963314
7}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{1C0C9DF0-B3FC-4362-8E0B-195A597A3BE
0}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{45EFE334-CC67-4DED-8ACA-BA3EC5292E5
A}      WAN Miniport (IP)
    4   DC:46:28:78:18:A1       192.168.3.89    \Device\NPF_{37A772F1-E9DC-4856-8B1A-09B88D239D2
6}      Intel(R) Wi-Fi 6 AX201 160MHz
    5   C8:7F:54:16:BC:65       192.168.3.244   \Device\NPF_{A786A402-6D39-41B8-9B27-3EEFF1B11ED
A}      Intel(R) Ethernet Connection (17) I219-V
    6   DE:46:28:78:18:A1       169.254.137.13  \Device\NPF_{C2097824-D18A-49A0-9CB5-AE4526E8F74
D}      Microsoft Wi-Fi Direct Virtual Adapter #2
    7   DC:46:28:78:18:A2       169.254.116.91  \Device\NPF_{04CD2F84-EDAF-4427-9F16-E5D4DDF9CAA
F}      Microsoft Wi-Fi Direct Virtual Adapter
    8   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback   A
dapter for loopback traffic capture
PS C:\Snort\bin>
```



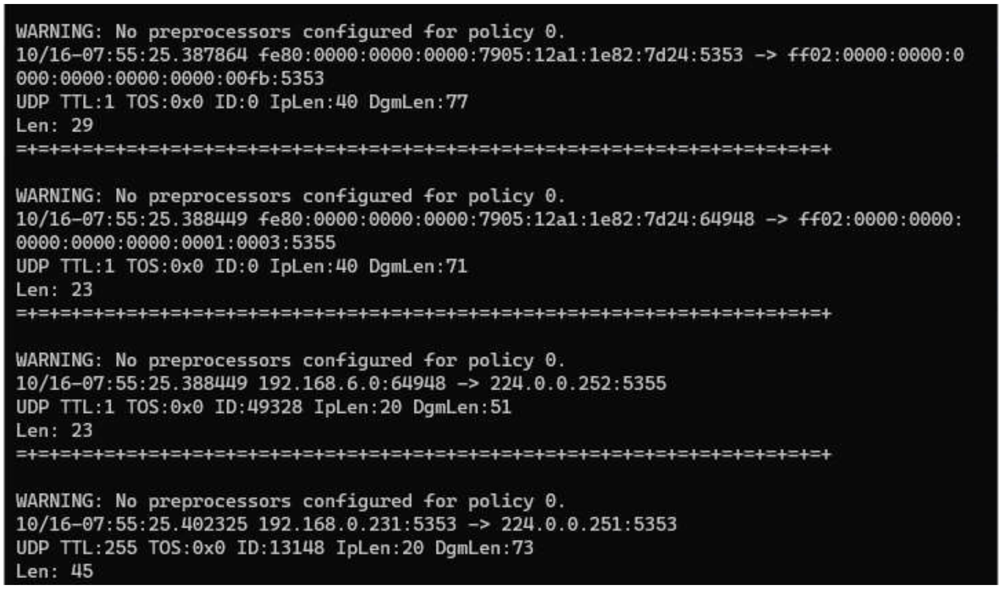
```
PS C:\Snort\bin> ipconfig

Windows IP Configuration


Wireless LAN adapter Local Area Connection* 9:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Local Area Connection* 10:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::8ee5:dd45:35a6:b978%15
   IPv4 Address. . . . . . . . . . . : 192.168.3.244
   Subnet Mask . . . . . . . . . . . : 255.255.248.0
   Default Gateway . . . . . . . . . : 192.168.7.254

Wireless LAN adapter Wi-Fi:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
PS C:\Snort\bin>
```

The command snort -W lists all available network interfaces on the system that Snort can use for packet capturing. This helps users identify which interface to monitor for network traffic, ensuring they select the correct one for their intrusion detection or analysis tasks.

Snort -i interface number -v



```
PS C:\Snort\bin> ./Snort -i 5 -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_{A786A402-6D39-41B8-9B27-3EEFF1B11EDA}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> 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

Commencing packet processing (pid=16316)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/16-07:55:25.329640 192.168.4.26:5353 -> 224.0.0.251:5353
UDP TTL:1 TOS:0x0 ID:54928 IpLen:20 DgmLen:56
Len: 28
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

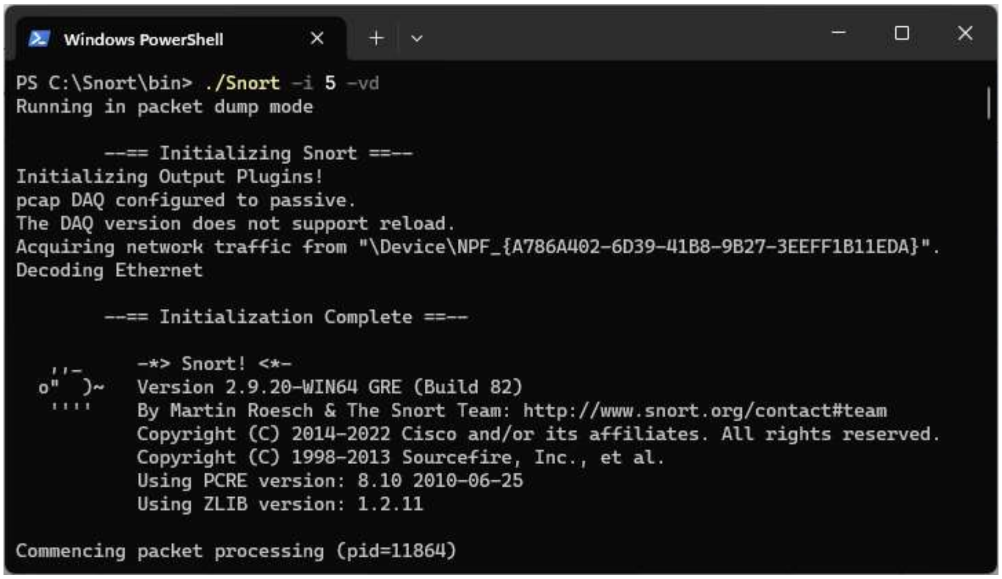


```
WARNING: No preprocessors configured for policy 0.
10/16-07:55:25.387864 fe80:0000:0000:0000:7905:12a1:1e82:7d24:5353 -> ff02:0000:0000:0
000:0000:0000:0000:00fb:5353
UDP TTL:1 TOS:0x0 ID:0 IpLen:40 DgmLen:77
Len: 29
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/16-07:55:25.388449 fe80:0000:0000:0000:7905:12a1:1e82:7d24:64948 -> ff02:0000:0000:
0000:0000:0000:0001:0003:5355
UDP TTL:1 TOS:0x0 ID:0 IpLen:40 DgmLen:71
Len: 23
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/16-07:55:25.388449 192.168.6.0:64948 -> 224.0.0.252:5355
UDP TTL:1 TOS:0x0 ID:49328 IpLen:20 DgmLen:51
Len: 23
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/16-07:55:25.402325 192.168.0.231:5353 -> 224.0.0.251:5353
UDP TTL:255 TOS:0x0 ID:13148 IpLen:20 DgmLen:73
Len: 45
```

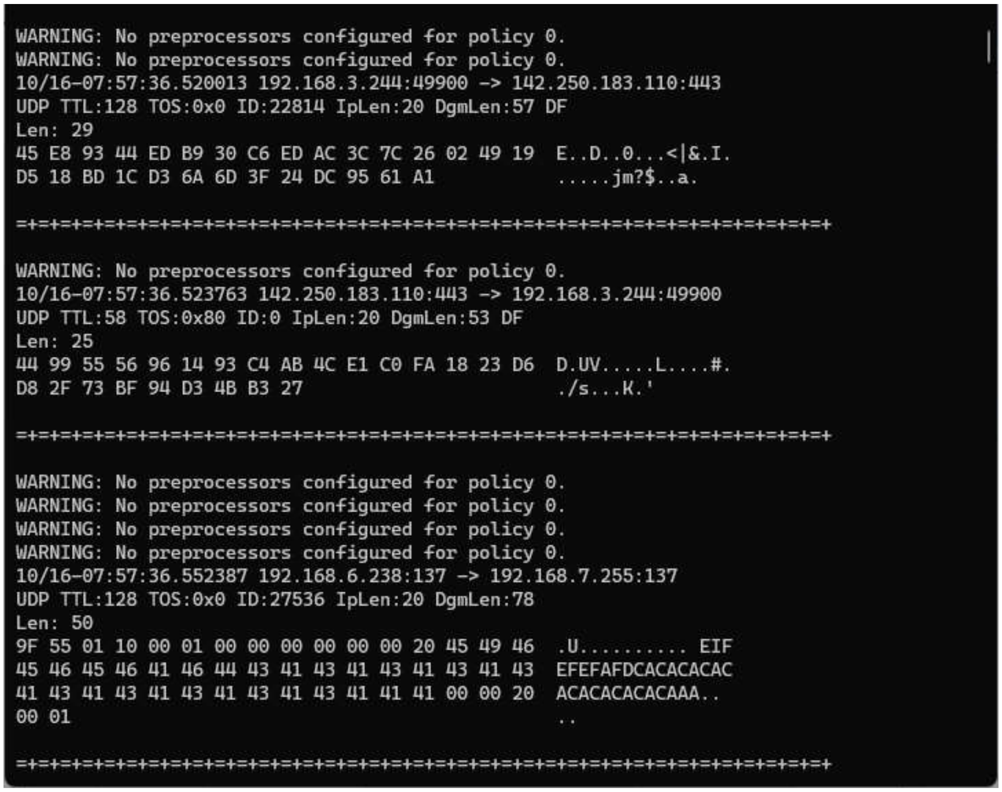
The command snort -i <interface_number> -v instructs Snort to operate on a specified network interface (indicated by the <interface_number>) and to display packet data in a verbose format. The -v flag provides a human-readable output of the captured packets, making it easier to analyze the traffic flowing through the selected interface in real time.

—---

Snort -i interface number -vd



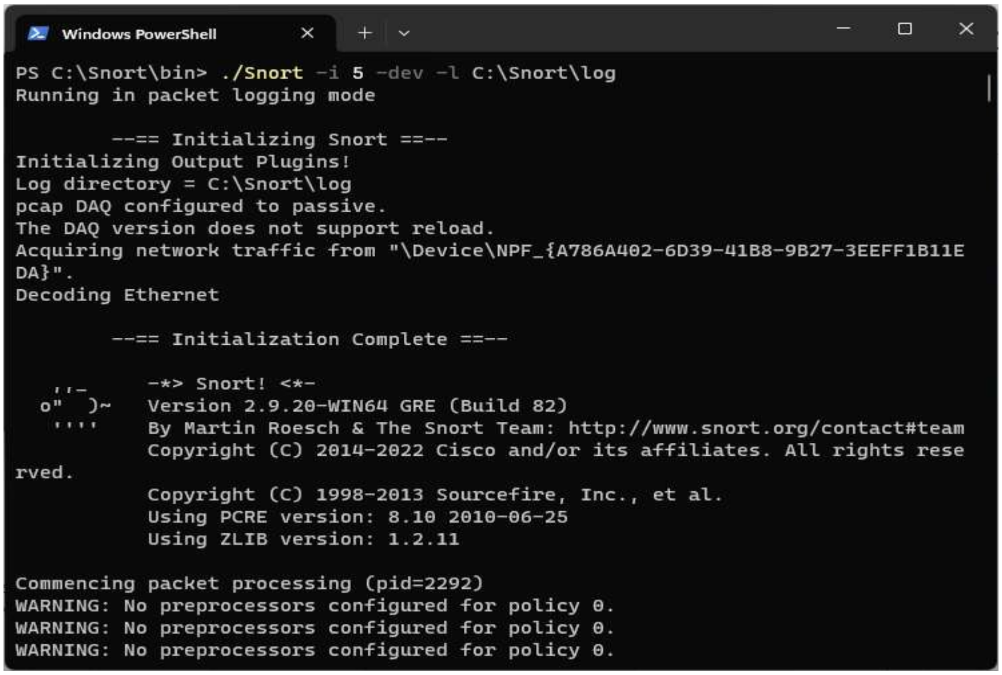
```
PS C:\Snort\bin> ./Snort -i 5 -vd
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{A786A402-6D39-41B8-9B27-3EEFF1B11EDA}".
Decoding Ethernet

        --== Initialization Complete ==--

   ,,_     -*> 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

Commencing packet processing (pid=11864)
```



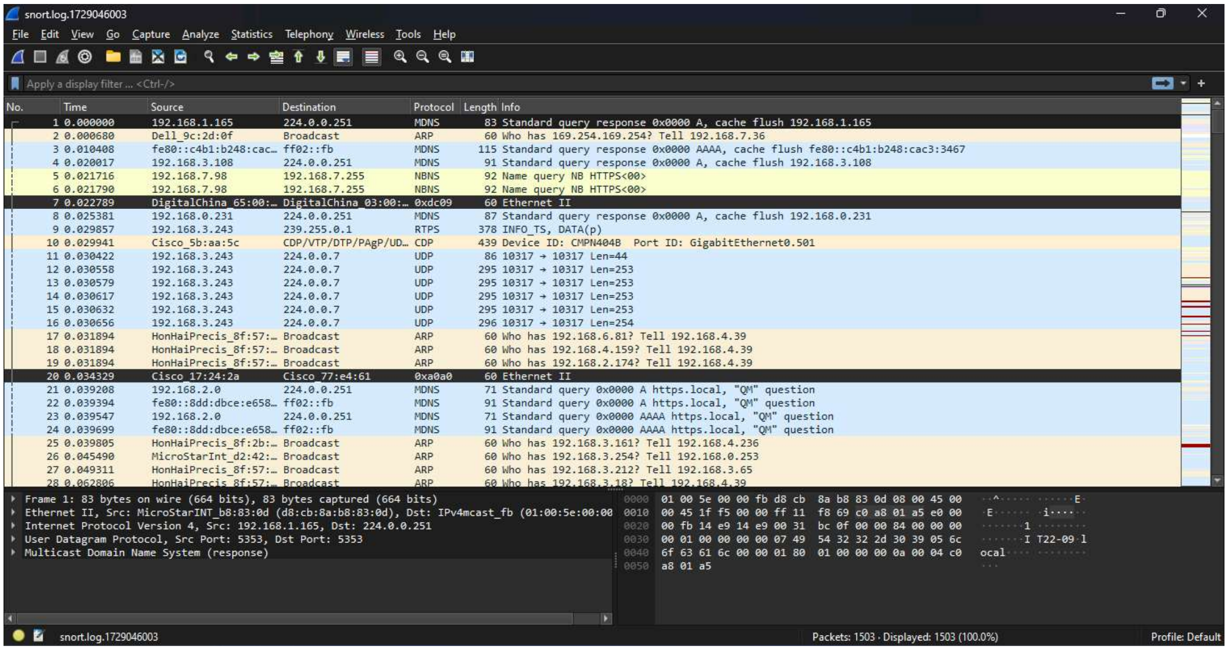
```
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/16-07:57:36.520013 192.168.3.244:49900 -> 142.250.183.110:443
UDP TTL:128 TOS:0x0 ID:22814 IpLen:20 DgmLen:57 DF
Len: 29
45 E8 93 44 ED B9 30 C6 ED AC 3C 7C 26 02 49 19  E..D..0...<|&.I.
D5 18 BD 1C D3 6A 6D 3F 24 DC 95 61 A1           .....jm?$..a.

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
10/16-07:57:36.523763 142.250.183.110:443 -> 192.168.3.244:49900
UDP TTL:58 TOS:0x80 ID:0 IpLen:20 DgmLen:53 DF
Len: 25
44 99 55 56 96 14 93 C4 AB 4C E1 C0 FA 18 23 D6  D.UV.....L....#.
D8 2F 73 BF 94 D3 4B B3 27                       ./s...K.'

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+

WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
10/16-07:57:36.552387 192.168.6.238:137 -> 192.168.7.255:137
UDP TTL:128 TOS:0x0 ID:27536 IpLen:20 DgmLen:78
Len: 50
9F 55 01 10 00 01 00 00 00 00 00 00 20 45 49 46  .U.......... EIF
45 46 45 46 41 46 44 43 41 43 41 43 41 43 41 43  EFEFAFDCACACACAC
41 43 41 43 41 43 41 43 41 43 41 41 41 00 00 20  ACACACACACAAA..
00 01                                            ..

=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

The command `snort -i <interface_number> -vd` tells Snort to listen on a specified network interface (indicated by `<interface_number>`) and to display packet data in a verbose and detailed format. The `-vd` option includes both the human-readable output of packet contents and additional information about the packet structure, which aids in in-depth analysis of network traffic.

Snort -i interface number -dev -l C:\Snort\log



```
PS C:\Snort\bin> ./Snort -i 5 -dev -l C:\Snort\log
Running in packet logging mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Log directory = C:\Snort\log
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{A786A402-6D39-41B8-9B27-3EEFF1B11E
DA}".
Decoding Ethernet

        --== Initialization Complete ==--

           ,,_     -*> 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 rese
rved.
                   Copyright (C) 1998-2013 Sourcefire, Inc., et al.
                   Using PCRE version: 8.10 2010-06-25
                   Using ZLIB version: 1.2.11

Commencing packet processing (pid=2292)
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
WARNING: No preprocessors configured for policy 0.
```



snort.log.1729046003
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.165	224.0.0.251	MDNS	83	Standard query response 0x0000 A, cache flush 192.168.1.165
2	0.000680	Dell_9c:2d:0f	Broadcast	ARP	60	Who has 169.254.169.254? Tell 192.168.7.36
3	0.010408	fe80::c4b1:b248:cac…	ff02::fb	MDNS	115	Standard query response 0x0000 AAAA, cache flush fe80::c4b1:b248:cac3:3467
4	0.020017	192.168.3.108	224.0.0.251	MDNS	91	Standard query response 0x0000 A, cache flush 192.168.3.108
5	0.021716	192.168.7.98	192.168.7.255	NBNS	92	Name query NB HTTPS<00>
6	0.021790	192.168.7.98	192.168.7.255	NBNS	92	Name query NB HTTPS<00>
7	0.022789	DigitalChina_65:00:…	DigitalChina_03:00:…	0xdc09	60	Ethernet II
8	0.025381	192.168.0.231	224.0.0.251	MDNS	87	Standard query response 0x0000 A, cache flush 192.168.0.231
9	0.029857	192.168.3.243	239.255.0.1	RTPS	378	INFO_TS, DATA(p)
10	0.029941	Cisco_5b:aa:5c	CDP/VTP/DTP/PAgP/UD…	CDP	439	Device ID: CMPN404B Port ID: GigabitEthernet0.501
11	0.030422	192.168.3.243	224.0.0.7	UDP	86	10317 → 10317 Len=44
12	0.030558	192.168.3.243	224.0.0.7	UDP	295	10317 → 10317 Len=253
13	0.030579	192.168.3.243	224.0.0.7	UDP	295	10317 → 10317 Len=253
14	0.030617	192.168.3.243	224.0.0.7	UDP	295	10317 → 10317 Len=253
15	0.030632	192.168.3.243	224.0.0.7	UDP	295	10317 → 10317 Len=253
16	0.030656	192.168.3.243	224.0.0.7	UDP	296	10317 → 10317 Len=254
17	0.031894	HonHaiPrecis_8f:57:…	Broadcast	ARP	60	Who has 192.168.6.81? Tell 192.168.4.39
18	0.031894	HonHaiPrecis_8f:57:…	Broadcast	ARP	60	Who has 192.168.4.159? Tell 192.168.4.39
19	0.031894	HonHaiPrecis_8f:57:…	Broadcast	ARP	60	Who has 192.168.2.174? Tell 192.168.4.39
20	0.034329	Cisco_17:24:2a	Cisco_77:e4:61	0xa0a0	60	Ethernet II
21	0.039208	192.168.2.0	224.0.0.251	MDNS	71	Standard query 0x0000 A https.local, "QM" question
22	0.039394	fe80::8dd:dbce:e658…	ff02::fb	MDNS	91	Standard query 0x0000 A https.local, "QM" question
23	0.039547	192.168.2.0	224.0.0.251	MDNS	71	Standard query 0x0000 AAAA https.local, "QM" question
24	0.039699	fe80::8dd:dbce:e658…	ff02::fb	MDNS	91	Standard query 0x0000 AAAA https.local, "QM" question
25	0.039805	HonHaiPrecis_8f:2b:…	Broadcast	ARP	60	Who has 192.168.3.161? Tell 192.168.4.236
26	0.045490	MicroStarInt_d2:42:…	Broadcast	ARP	60	Who has 192.168.3.254? Tell 192.168.0.253
27	0.049311	HonHaiPrecis_8f:57:…	Broadcast	ARP	60	Who has 192.168.3.212? Tell 192.168.3.65
28	0.062806	HonHaiPrecis_8f:57:…	Broadcast	ARP	60	Who has 192.168.3.18? Tell 192.168.4.39

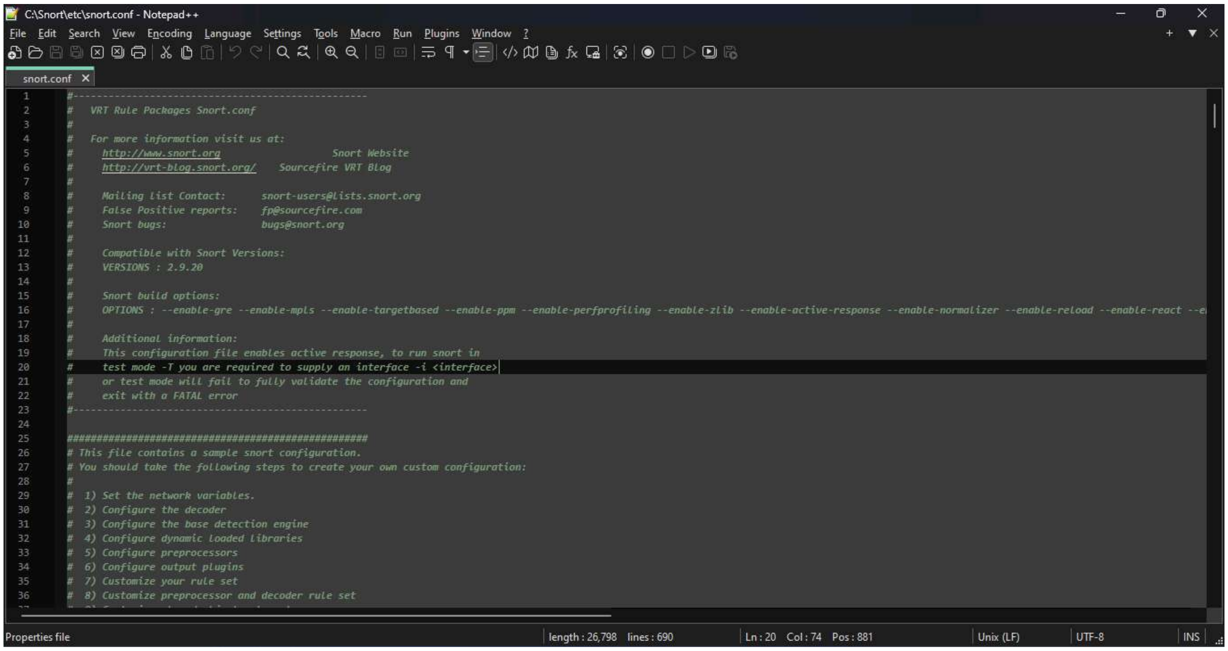
```
Frame 1: 83 bytes on wire (664 bits), 83 bytes captured (664 bits)
Ethernet II, Src: MicroStarINT_b8:83:0d (d8:cb:8a:b8:83:0d), Dst: IPv4mcast_fb (01:00:5e:00:00
Internet Protocol Version 4, Src: 192.168.1.165, Dst: 224.0.0.251
User Datagram Protocol, Src Port: 5353, Dst Port: 5353
Multicast Domain Name System (response)
```

```
0000  01 00 5e 00 00 fb d8 cb  8a b8 83 0d 08 00 45 00   ··^·····  ······E·
0010  00 45 1f f5 00 00 ff 11  f8 69 c0 a8 01 a5 e0 00   ·E······  ·i······
0020  00 fb 14 e9 14 e9 00 31  bc 0f 00 00 84 00 00 00   ·······1  ········
0030  00 01 00 00 00 00 07 49  54 32 32 2d 30 39 05 6c   ·······I  T22-09·l
0040  6f 63 61 6c 00 00 01 80  01 00 00 00 0a 00 04 c0   ocal····  ········
0050  a8 01 a5                                           ···
```

The command `snort -i <interface_number> -dev -l C:\Snort\log` configures Snort to listen on a specified network interface (`<interface_number>`) and to log the packet data in a detailed format. The `-d` option includes the data portion of the packets, the `-e` option shows Ethernet headers, and the `-l C:\Snort\log` specifies the directory where log files will be saved. This setup is useful for thorough analysis and record-keeping of network traffic.

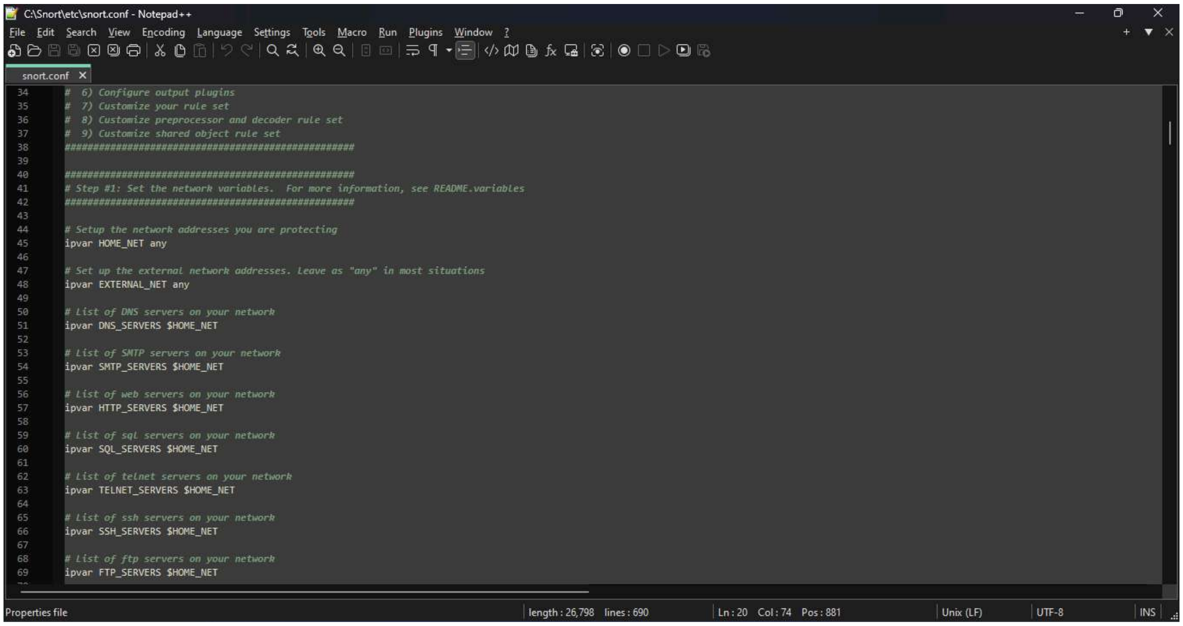
—---

snort -i 5 -dev -l C:\Snort\log -h 192.168.1.0/24 -c C:\Snort\etc\snort.conf

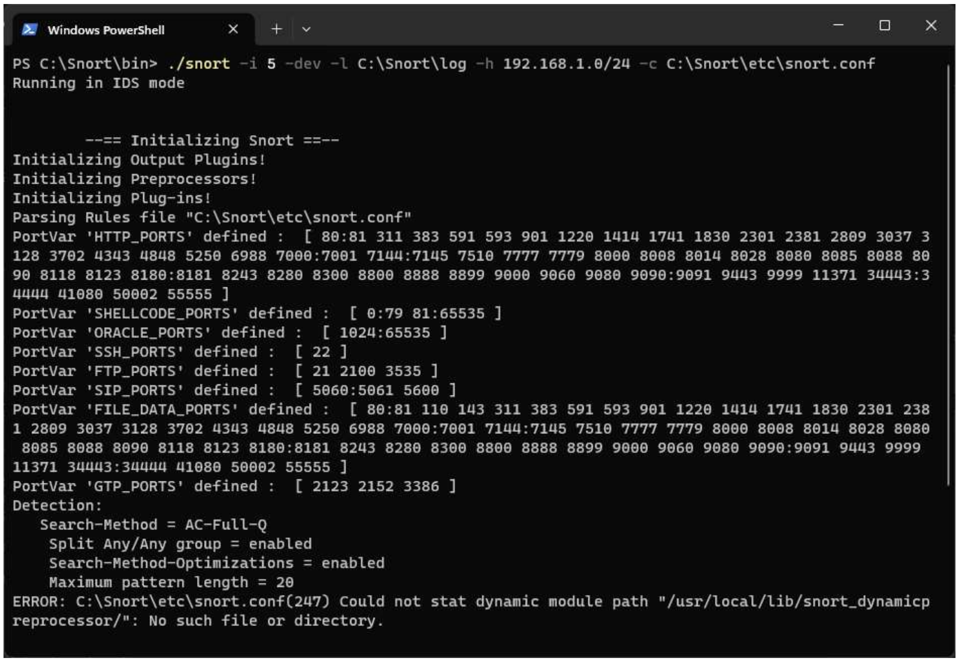

C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf

```
#--------------------------------------------------
#   VRT Rule Packages Snort.conf
#
#   For more information visit us at:
#     http://www.snort.org                   Snort Website
#     http://vrt-blog.snort.org/    Sourcefire VRT Blog
#
#     Mailing list Contact:      snort-users@lists.snort.org
#     False Positive reports:    fp@sourcefire.com
#     Snort bugs:                bugs@snort.org
#
#     Compatible with Snort Versions:
#     VERSIONS : 2.9.20
#
#     Snort build options:
#     OPTIONS : --enable-gre --enable-mpls --enable-targetbased --enable-ppm --enable-perfprofiling --enable-zlib --enable-active-response --enable-normalizer --enable-reload --enable-react --e
#
#     Additional information:
#     This configuration file enables active response, to run snort in
#     test mode -T you are required to supply an interface -i <interface>
#     or test mode will fail to fully validate the configuration and
#     exit with a FATAL error
#--------------------------------------------------

###################################################
# This file contains a sample snort configuration.
# You should take the following steps to create your own custom configuration:
#
#  1) Set the network variables.
#  2) Configure the decoder
#  3) Configure the base detection engine
#  4) Configure dynamic loaded libraries
#  5) Configure preprocessors
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
```

Properties file   length : 26,798   lines : 690   Ln : 20   Col : 74   Pos : 881   Unix (LF)   UTF-8   INS


C:\Snort\etc\snort.conf - Notepad++
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
snort.conf
Properties file
length : 26,798 lines : 690
Ln : 20 Col : 74 Pos : 881
Unix (LF)
UTF-8
INS

```
#  6) Configure output plugins
#  7) Customize your rule set
#  8) Customize preprocessor and decoder rule set
#  9) Customize shared object rule set
###################################################

###################################################
# Step #1: Set the network variables.  For more information, see README.variables
###################################################

# 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 any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET

# List of SMTP servers on your network
ipvar SMTP_SERVERS $HOME_NET

# List of web servers on your network
ipvar HTTP_SERVERS $HOME_NET

# List of sql servers on your network
ipvar SQL_SERVERS $HOME_NET

# List of telnet servers on your network
ipvar TELNET_SERVERS $HOME_NET

# List of ssh servers on your network
ipvar SSH_SERVERS $HOME_NET

# List of ftp servers on your network
ipvar FTP_SERVERS $HOME_NET
```



```
PS C:\Snort\bin> ./snort -i 5 -dev -l C:\Snort\log -h 192.168.1.0/24 -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"
PortVar 'HTTP_PORTS' defined :  [ 80:81 311 383 591 593 901 1220 1414 1741 1830 2301 2381 2809 3037 3
128 3702 4343 4848 5250 6988 7000:7001 7144:7145 7510 7777 7779 8000 8008 8014 8028 8080 8085 8088 80
90 8118 8123 8180:8181 8243 8280 8300 8800 8888 8899 9000 9060 9080 9090:9091 9443 9999 11371 34443:3
4444 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 238
1 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
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
ERROR: C:\Snort\etc\snort.conf(247) Could not stat dynamic module path "/usr/local/lib/snort_dynamicp
reprocessor/": No such file or directory.
```

The command `snort -i 5 -dev -l C:\Snort\log -h 192.168.1.0/24 -c C:\Snort\etc\snort.conf` configures Snort to listen on interface 5, logging detailed packet information to `C:\Snort\log`. The `-h 192.168.1.0/24` option sets the home network to include the specified subnet, allowing Snort to focus on traffic within that range. The `-c C:\Snort\etc\snort.conf` specifies the configuration file to use, which contains rules and settings for Snort's operation. This command sets up a comprehensive environment for monitoring and analyzing traffic specific to a local network.
