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.

```
Snort –V
Snort –v
Snort -vd
Snort –W
```

3. Run the following command to use snort in Packet logger mode. View the log file created. Observe the content of the 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 -dev -l C:\Snort\log
```

4. 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 -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/

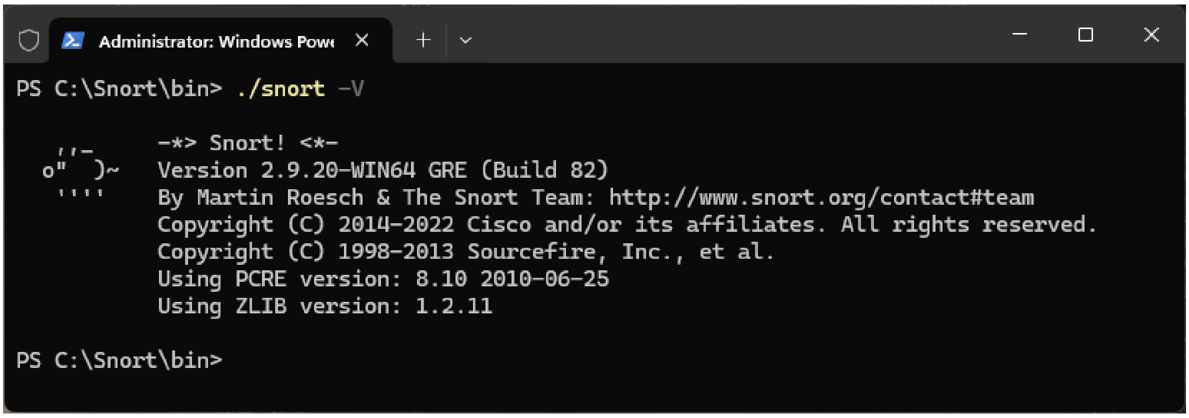
[2] Bart Lenaerts-Bergmans , "SNORT AND SNORT RULES EXPLAINED", https://www.crowdstrike.com/cybersecurity-101/threat-intelligence/snort-rules/

[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

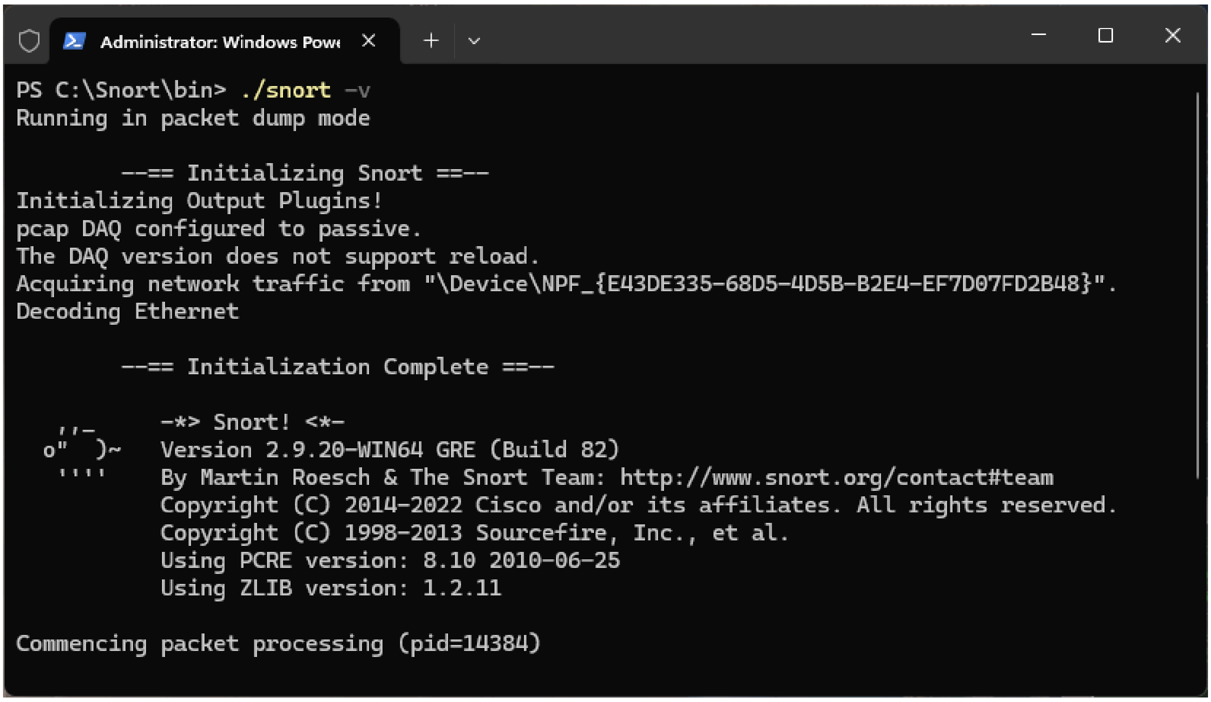
Snort -V



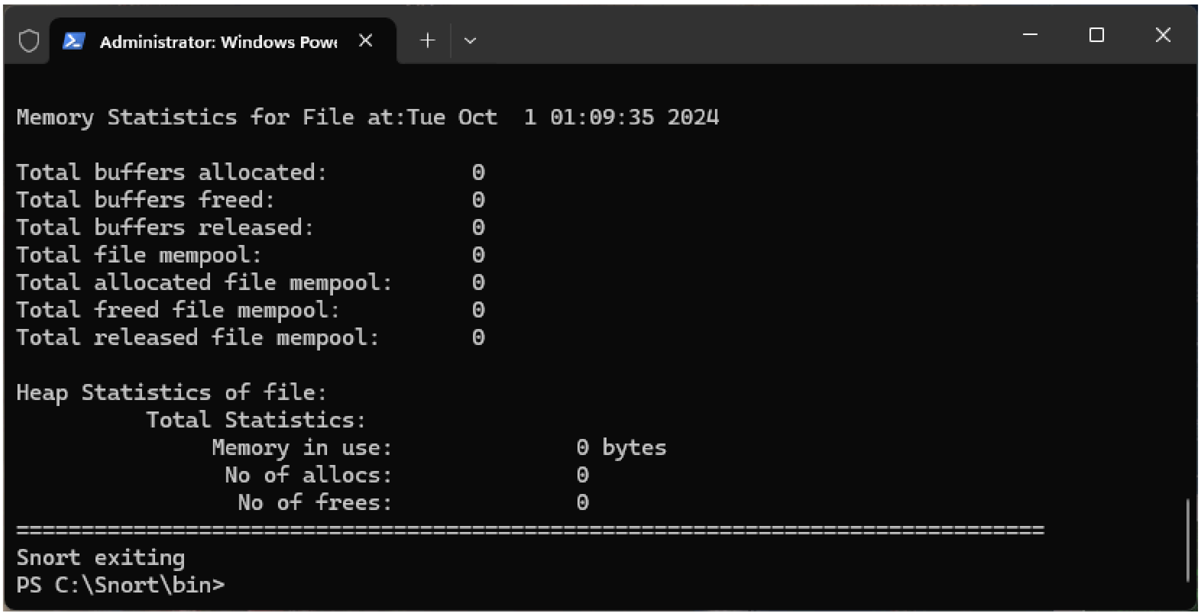
```
PS C:\Snort\bin> ./snort -V

   ,,_     -*> 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 -v



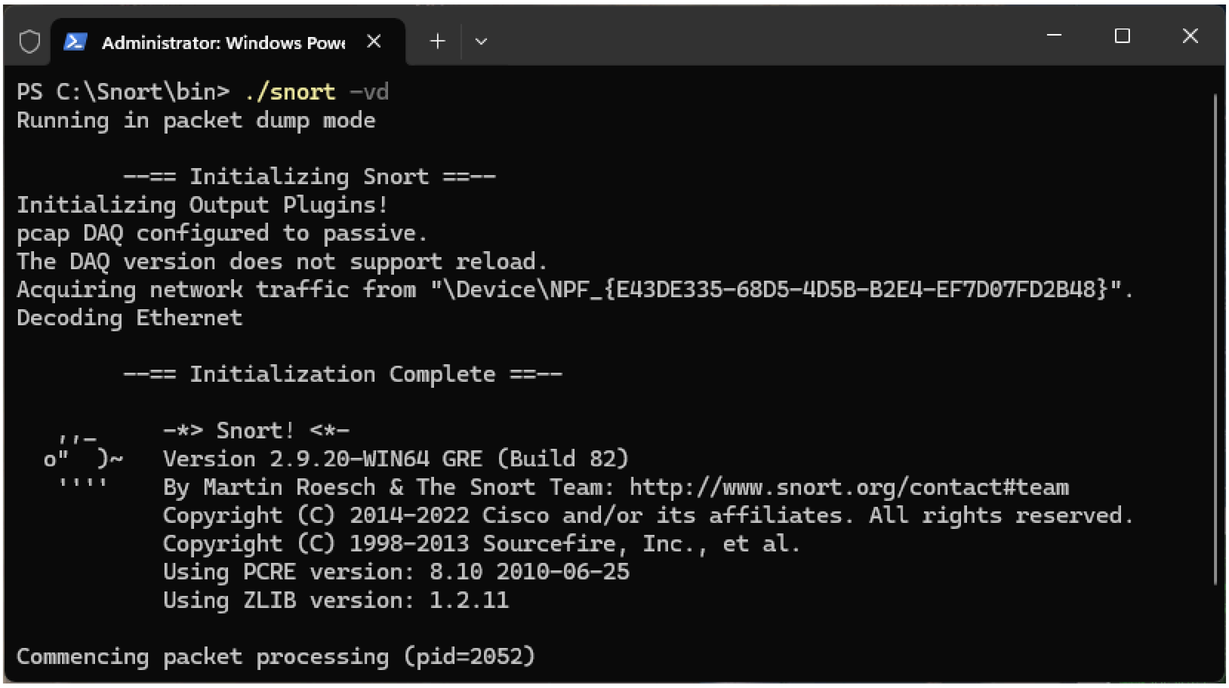
```
PS C:\Snort\bin> ./snort -v
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{E43DE335-68D5-4D5B-B2E4-EF7D07FD2B48}".
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=14384)
```



```
Memory Statistics for File at:Tue Oct  1 01:09:35 2024

Total buffers allocated:           0
Total buffers freed:               0
Total buffers released:            0
Total file mempool:                0
Total allocated file mempool:      0
Total freed file mempool:          0
Total released file mempool:       0

Heap Statistics of file:
          Total Statistics:
               Memory in use:              0 bytes
                No of allocs:              0
                 No of frees:              0
===============================================================================
Snort exiting
PS C:\Snort\bin>
```

- The snort -v command runs Snort in verbose mode, capturing and displaying raw packet headers.
- No intrusion detection rules or analysis are applied, only packet data is shown.
- Initializes plugins and configures the DAQ module in passive mode.
- Acquires network traffic from a specified network interface.
- Useful for basic traffic monitoring and troubleshooting network issues.
- Real-time packet processing is displayed without deep inspection.

Snort -vd



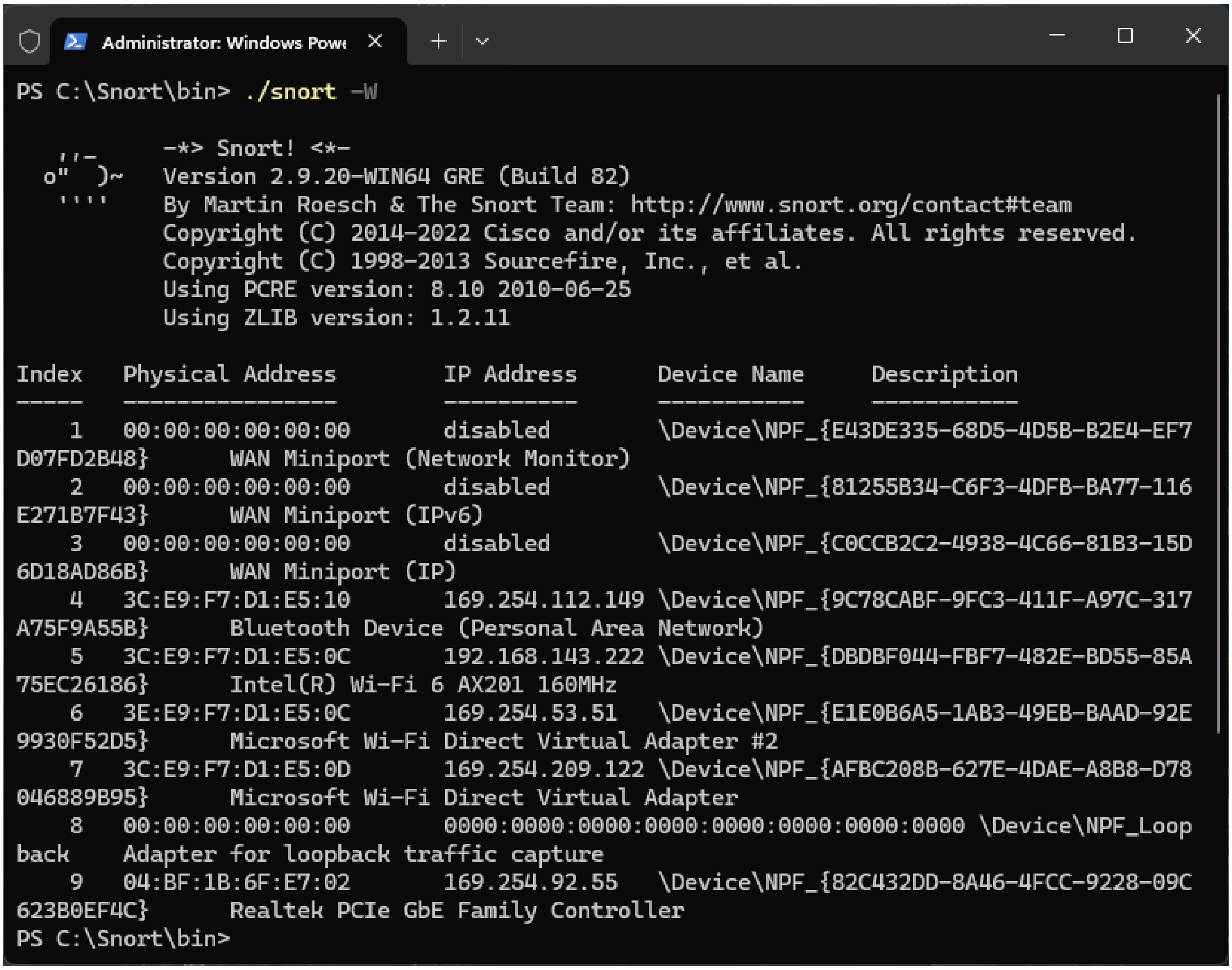
```
PS C:\Snort\bin> ./snort -vd
Running in packet dump mode

        --== Initializing Snort ==--
Initializing Output Plugins!
pcap DAQ configured to passive.
The DAQ version does not support reload.
Acquiring network traffic from "\Device\NPF_{E43DE335-68D5-4D5B-B2E4-EF7D07FD2B48}".
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=2052)
```

The Snort command ./snort -vd is running in packet dump mode, displaying both packet headers and the application layer data (payload). Here are the key details of the output:

- Verbose Mode (-v): Snort captures and displays packet headers.
- Dump Payload (-d): In addition to headers, Snort shows the application layer data of each packet.
- Packet Capture: Traffic is being captured from a network interface specified by the device path (shown as a UUID).
- Version Info: Snort version 2.9.20-WIN64 GRE (Build 82) is being used.
- Initialization: Plugins are initialized, and the Data Acquisition (DAQ) module is configured to passive mode, allowing Snort to passively capture packets without modifying the traffic.
- Packet Processing: Packet processing has started with process ID 2052.

In this mode, Snort is capturing and displaying both the headers and payload of network packets for detailed traffic analysis.

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_{E43DE335-68D5-4D5B-B2E4-EF7
D07FD2B48}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        \Device\NPF_{81255B34-C6F3-4DFB-BA77-116
E271B7F43}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        \Device\NPF_{C0CCB2C2-4938-4C66-81B3-15D
6D18AD86B}      WAN Miniport (IP)
    4   3C:E9:F7:D1:E5:10       169.254.112.149 \Device\NPF_{9C78CABF-9FC3-411F-A97C-317
A75F9A55B}      Bluetooth Device (Personal Area Network)
    5   3C:E9:F7:D1:E5:0C       192.168.143.222 \Device\NPF_{DBDBF044-FBF7-482E-BD55-85A
75EC26186}      Intel(R) Wi-Fi 6 AX201 160MHz
    6   3E:E9:F7:D1:E5:0C       169.254.53.51   \Device\NPF_{E1E0B6A5-1AB3-49EB-BAAD-92E
9930F52D5}      Microsoft Wi-Fi Direct Virtual Adapter #2
    7   3C:E9:F7:D1:E5:0D       169.254.209.122 \Device\NPF_{AFBC208B-627E-4DAE-A8B8-D78
046889B95}      Microsoft Wi-Fi Direct Virtual Adapter
    8   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loop
back    Adapter for loopback traffic capture
    9   04:BF:1B:6F:E7:02       169.254.92.55   \Device\NPF_{82C432DD-8A46-4FCC-9228-09C
623B0EF4C}      Realtek PCIe GbE Family Controller
PS C:\Snort\bin>
```

The command ./snort -W displays a list of available network interfaces on the system. Key points from the output:

- Lists Interfaces: Displays all network interfaces with details including the index, MAC (physical) address, IP address, device name, and description.

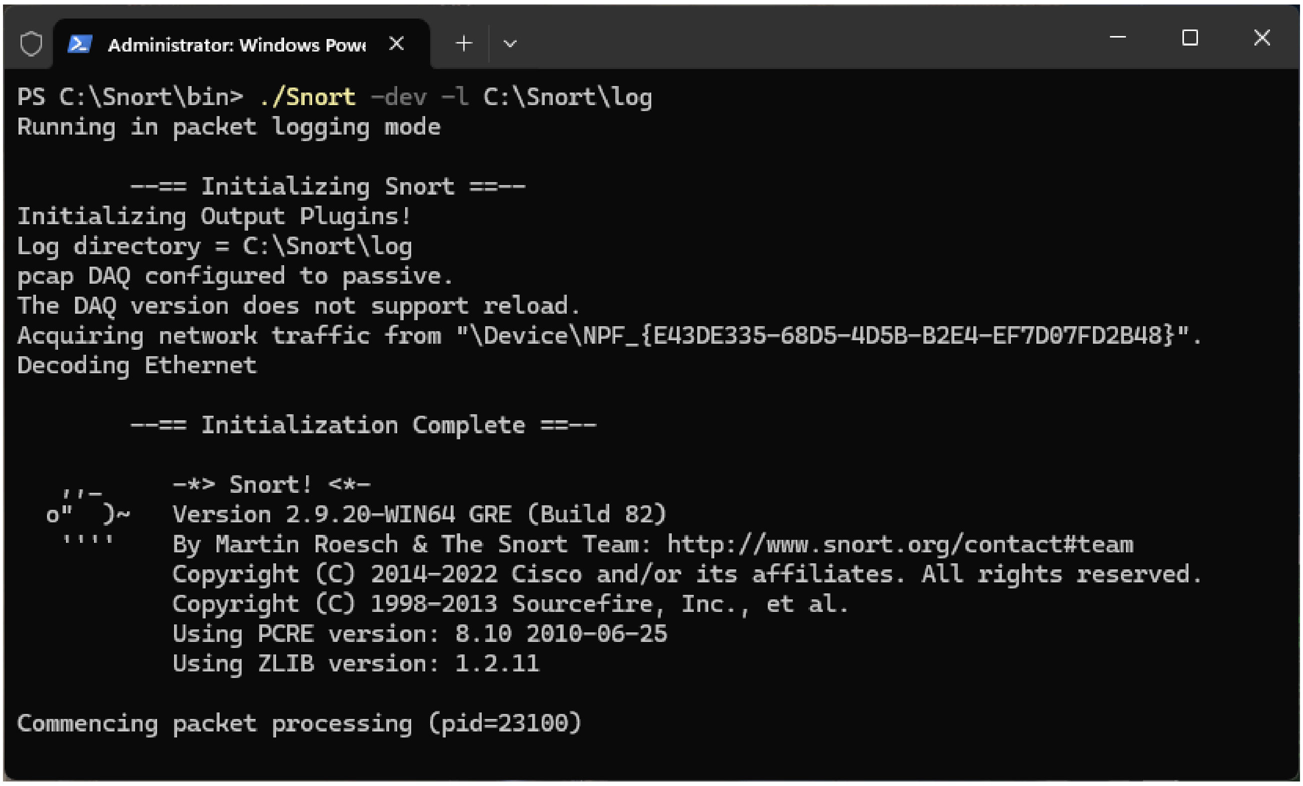
- Identifies Active Interfaces: Some interfaces, like the Wi-Fi adapter and Realtek PCIe controller, have active IP addresses, making them suitable for packet capture.

- Disabled Interfaces: Several interfaces (e.g., WAN Miniports) are shown as disabled with no IP address.

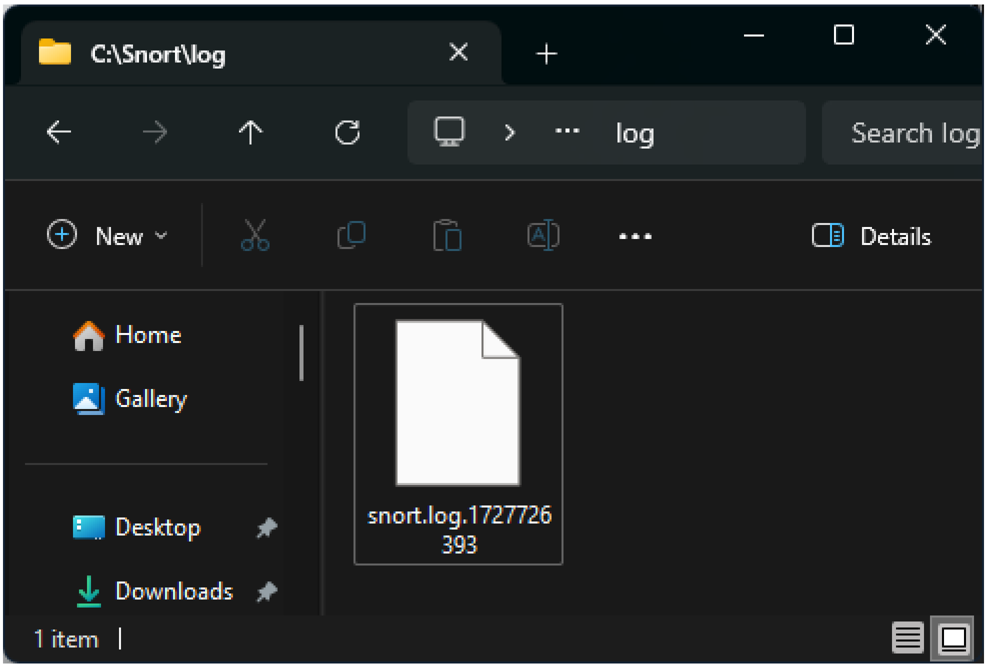
- Loopback Adapter: An interface for loopback traffic is listed, used for local traffic monitoring.

This output helps in selecting the appropriate interface for Snort packet capture based on its status and network connectivity.

Snort -dev -l



```
PS C:\Snort\bin> ./Snort -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_{E43DE335-68D5-4D5B-B2E4-EF7D07FD2B48}".
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=23100)
```



```
Command: ./snort -dev -l C:\Snort\log
```

Explanation:

- Mode: Runs Snort in packet logging mode, capturing and logging network packets.
- Log Directory: Specifies C:\Snort\log as the directory where logs will be stored.
- Network Interface: Snort acquires network traffic from the specified device interface.
- Initialization: Snort initializes output plugins, configures packet capture (pcap) to passive mode, and decodes Ethernet traffic.
- Version Info: Outputs the version of Snort being used, including build and copyright details.
- Dependencies: Details the versions of PCRE (Perl Compatible Regular Expressions) and ZLIB libraries being used.
- Packet Processing: Starts processing packets with a specific process ID (pid=23100).

This setup allows Snort to capture and log all network traffic for further analysis, which is crucial for network monitoring and intrusion detection.
