

Name: Abdurrahman Qureshi

Roll No: 242466

Practical No: 10

Date Of Performance: 01/10/2025

Aim: To Set up Snort Tool and study the logs.

Lab Outcome: To develop comprehensive theoretical understanding of keyloggers, their deployment mechanisms, data capture techniques, and implement best practices for detection, removal, and prevention.

Theory:

Introduction to Snort

Snort is a powerful open-source Intrusion Detection and Prevention System (IDS/IPS). It performs real-time traffic analysis, packet logging, and can be configured to detect a wide range of attacks, such as buffer overflows, stealth port scans, and malware. It operates by matching network traffic against a set of user-defined rules.

Core Components:

- Packet Decoder: Captures and prepares network packets from various interfaces (Ethernet, Wi-Fi) for processing.
- Pre-processors: Normalize and analyse traffic for anomalies that complex attacks might use to evade detection (e.g., packet fragmentation, TCP stream reassembly).

- Detection Engine: The core of Snort. It analyses decoded packets using a set of predefined rules to identify malicious activity.
- Logging and Alerting System: Generates alerts and logs packet data based on the detection engine's findings. Logs can be stored in various formats (e.g., unified2, ASCII).

Key Operational Modes:

- Sniffer Mode: Reads and displays network packets to the console. Useful for basic traffic inspection.
- Packet Logger Mode: Captures and logs packets to disk for later analysis.
- Network Intrusion Detection System (NIDS) Mode: The primary mode. Analyses traffic against a rule set and generates alerts and logs for suspicious activity.

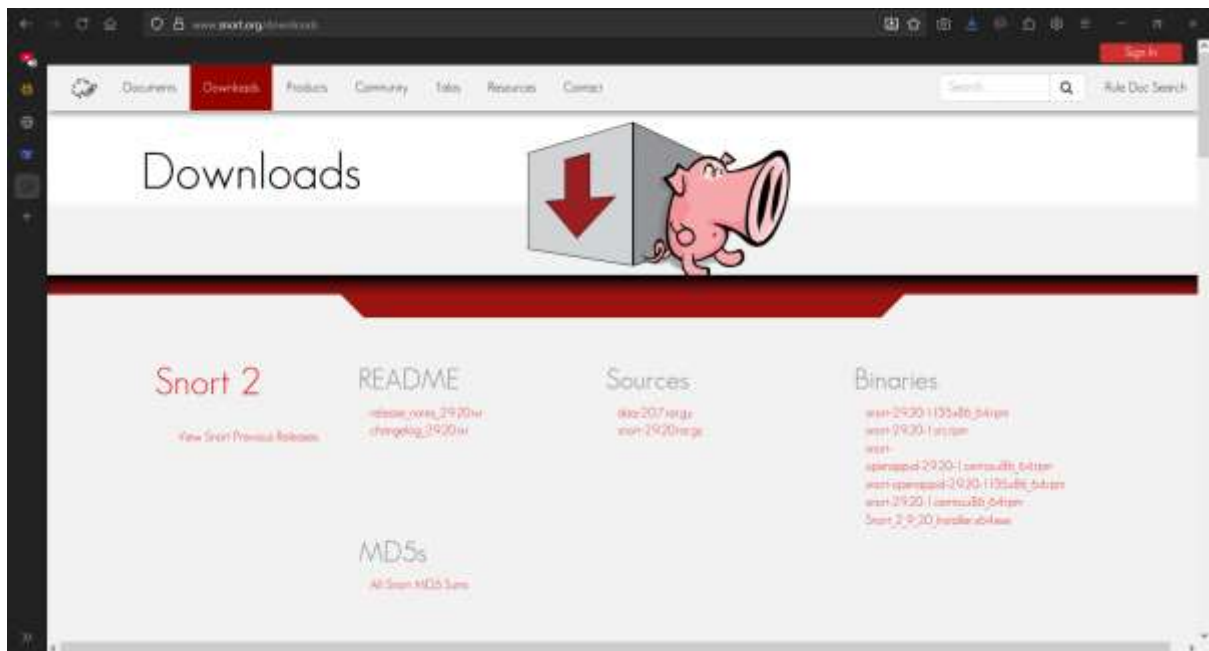
Studying Snort Logs

After running Snort in NIDS mode, you must analyse the output to identify threats.

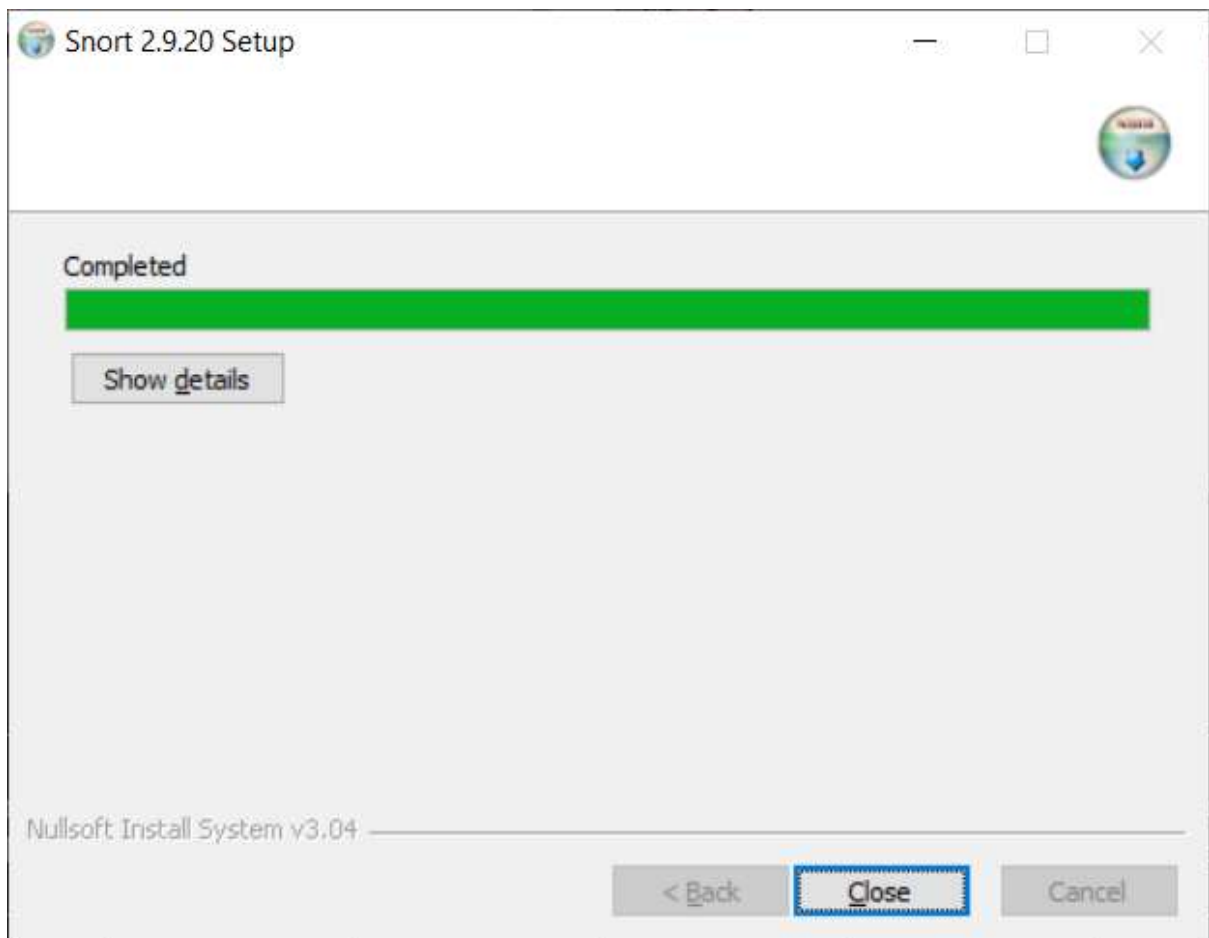
Default Log Location: `/var/log/snort/`

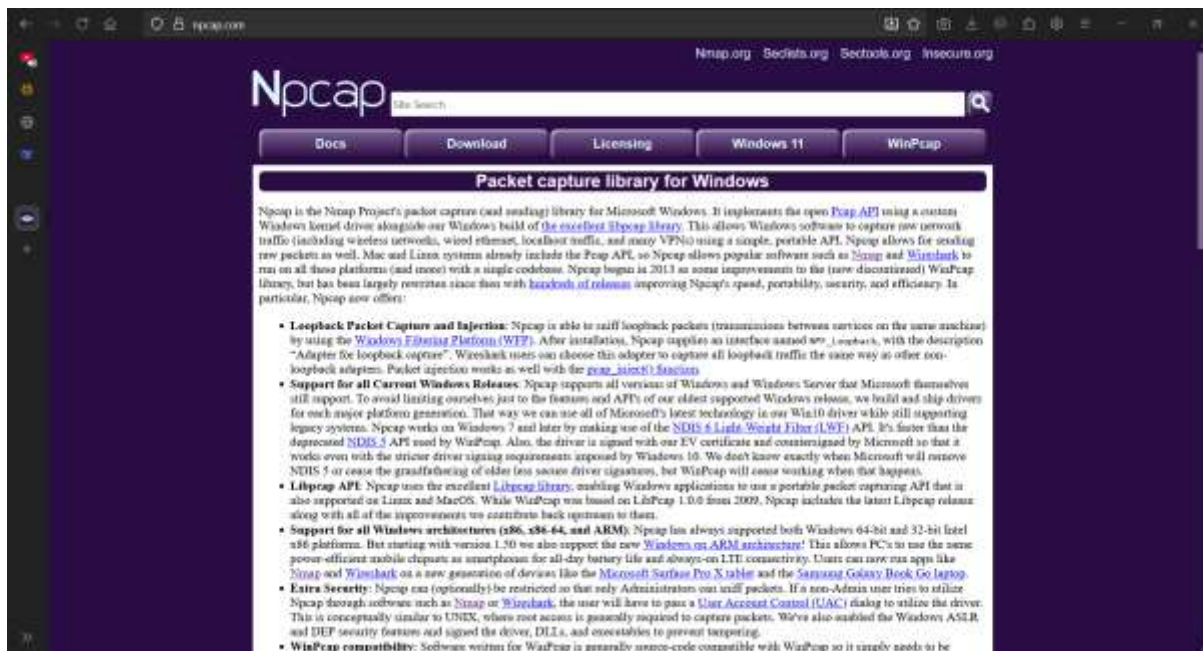
Log Formats:

- Alert File (alert): Contains a summary of triggered alerts, including timestamp, source/destination IPs, and the alert message.
- Unified2 Binary Logs: Efficient, binary format logs that require tools like barnyard2 or u2spewfoo for reading.
- PCAP Logs: Full packet capture data, which can be analysed in-depth using tools like Wireshark.

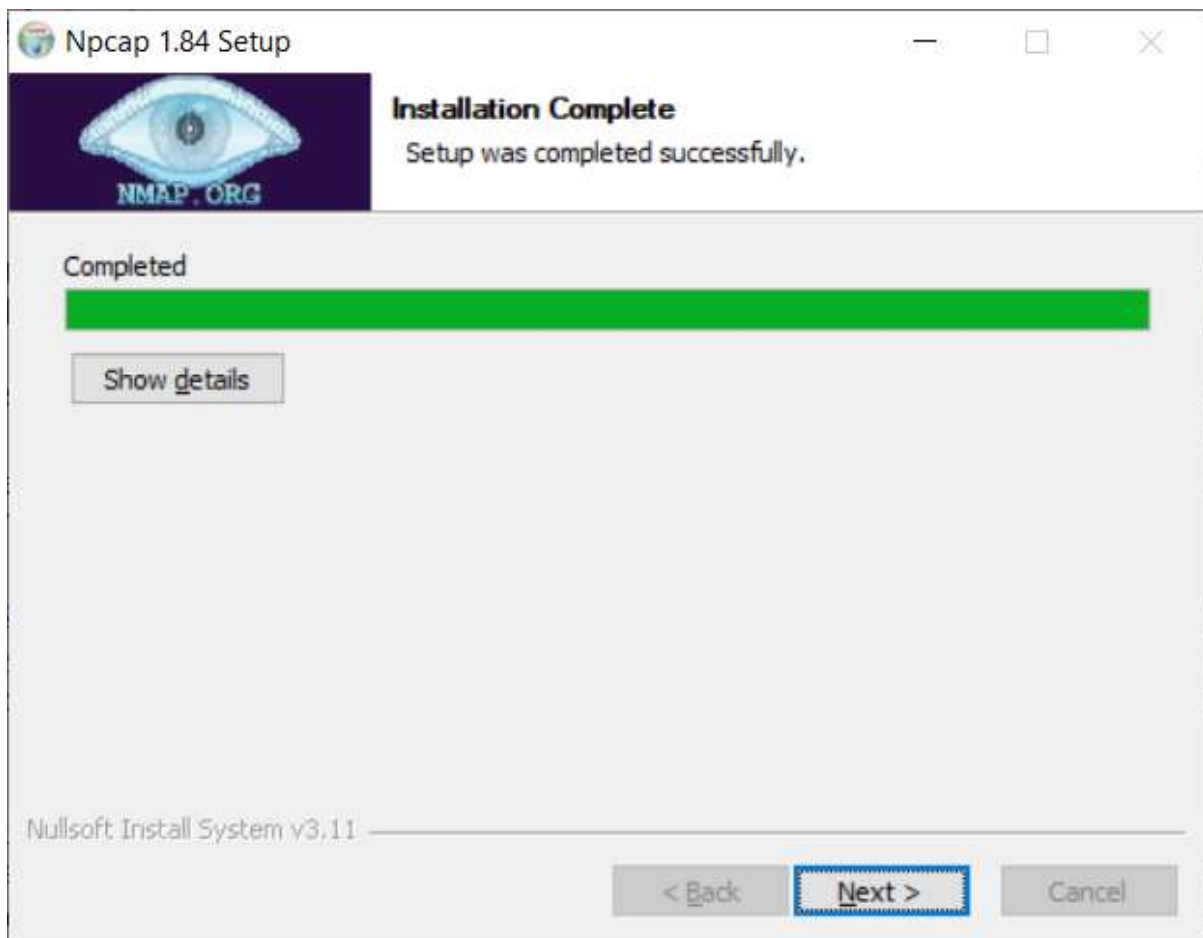


Downloading Snort



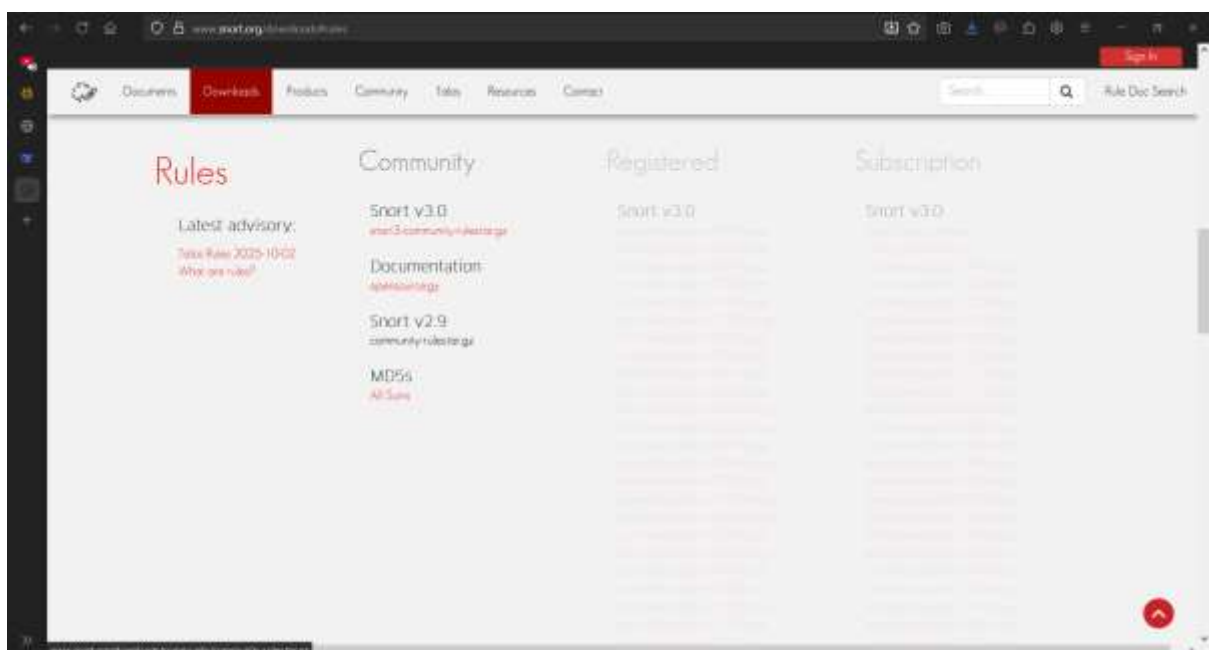


Downloading NCap

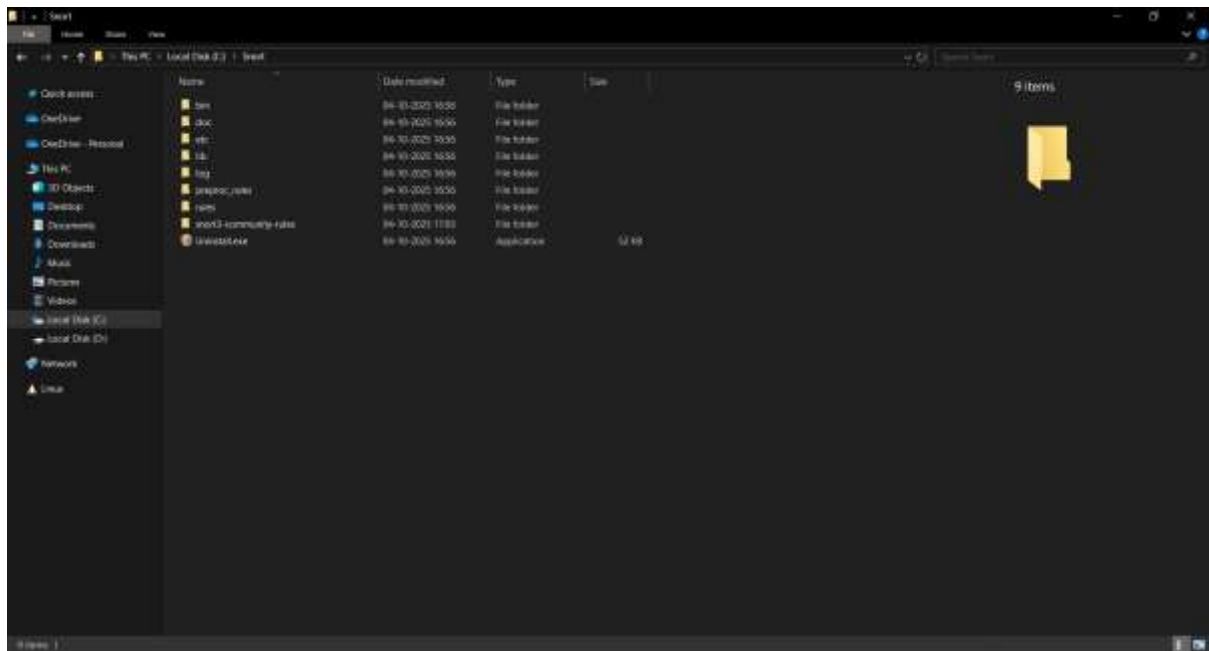


```
snort.conf
25 #####
26 # This file contains a sample snort configuration.
27 # You should take the following steps to create your own custom configuration:
28 #
29 # 1) Set the network variables.
30 # 2) Configure the decoder
31 # 3) Configure the base detection engine
32 # 4) Configure dynamic loaded libraries
33 # 5) Configure preprocessors
34 # 6) Configure output plugins
35 # 7) Customize your rule set
36 # 8) Customize preprocessor and decoder rule set
37 # 9) Customize shared object rule set
38 #####
39
40 #####
41 # Step #1: Set the network variables. For more information, see README.variables
42 #####
43
44 # Setup the network addresses you are protecting
45 ipvar HOME_NET 192.168.0.100
46
47 # Set up the external network addresses. Leave as "any" in most situations.
48 ipvar EXTERNAL_NET any
49
50 # List of DNS servers on your network
51 ipvar DNS_SERVERS $HOME_NET
52
53 # List of SMTP servers on your network
54 ipvar SMTP_SERVERS $HOME_NET
55
56 # List of web servers on your network
57 ipvar HTTP_SERVERS $HOME_NET
58
59 # List of sql servers on your network
60 ipvar SQL_SERVERS $HOME_NET
61
62 # List of telnet servers on your network
63 ipvar TELNET_SERVERS $HOME_NET
64
65 # List of rsh servers on your network
66
```

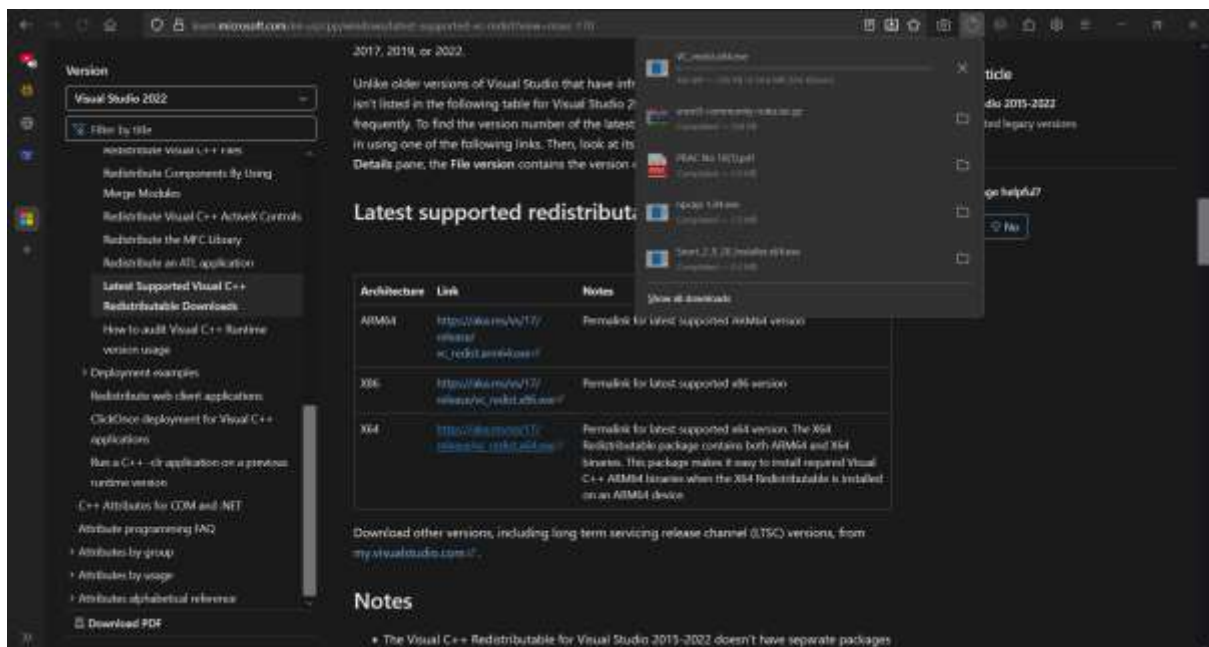
Configuring snort.conf



Downloading Snort Rules



Extracted and pasted rules



Downloading C++ Redistributable

```
C:\snort\bin>snort.exe -W

--== Snort! ==--
nt' ]- 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) 1998-2023 Sourcefire, Inc., et al.
      Using PCRE version: 8.10 2018-06-25
      Using ZLIB version: 1.2.11

Index  Physical Address  IP Address  Device Name  Description
-----
1  00:00:00:00:00:00  disabled  \Device\NPF_{484B483D-C732-4860-8A99-310E980C1440}  WAN Miniport (Network Moni
tor)
2  00:00:00:00:00:00  disabled  \Device\NPF_{A6985120-0A61-4C1D-9DC1-168F320EA765}  WAN Miniport (IPv6)
3  00:00:00:00:00:00  disabled  \Device\NPF_{6C4KCD0-31A6-4F47-8884-591E077F5EED}  WAN Miniport (IP)
4  70:97:79:EB:49:1C  169.254.155.102 \Device\NPF_{3103FA90-0620-4668-8B65-3C0075118961}  Bluetooth Device (Personal
Area Network)
5  70:97:79:EB:49:1B  192.168.8.165   \Device\NPF_{4A3745FA-7A47-4DA5-A2A5-E443EC39CF7}  Realtek 8821CE Wireless LA
N 802.11ac PCI-E NIC
6  00:50:56:C0:00:00  192.168.163.1  \Device\NPF_{FA2027B0-E3F8-433C-8A3D-2A6F1A90BA95}  VMware Virtual Ethernet Ad
apter for VMnet8
7  00:50:56:C0:00:01  192.168.44.1   \Device\NPF_{1EEAE653-2C20-4702-A941-9B183A67C3E6}  VMware Virtual Ethernet Ad
apter for VMnet1
8  70:97:79:EB:49:1B  169.254.245.72 \Device\NPF_{03D87139-D9FC-4928-9066-B06219542D4A}  Microsoft Wi-Fi Direct Vir
tual Adapter
9  00:00:00:00:00:00  0000:0000:0000:0000:0000:0000 \Device\NPF_{loopback}  Adapter for loopback traffic captu
re

C:\snort\bin>
```

```
C:\snort\bin>snort -i 1 -A console
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_{484B483D-C732-4860-8A99-310E980C1440}".
Decoding Ethernet

--== Initialization Complete ==--

--== Snort! ==--
nt' ]- 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) 1998-2023 Sourcefire, Inc., et al.
      Using PCRE version: 8.10 2018-06-25
      Using ZLIB version: 1.2.11

Commencing packet processing (pid=15092)
```

Executing Snort.exe

Performance (7M)	Journal (3M)	Lab Ethics (2M)	Attendance (3M)	Total (15M)	Faculty Signature

