**Experiment – 10**

**Aim:** CaseStudy of setup Snort and analyzing the logs.‍

**Requirements:**

Before you begin the installation, ensure your system meets the following requirements:

* A computer running Windows (preferably Windows 10 or later)
* Administrative access
* WinPcap or Npcap (packet capture library)

‍**Theory:**

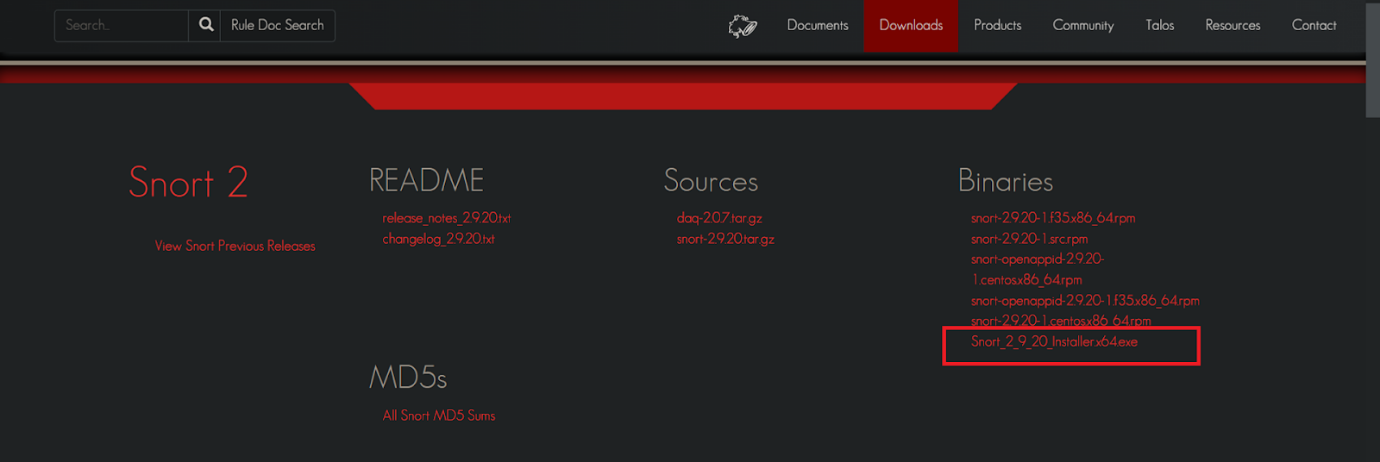
Snort can perform protocol analysis, and content searching/matching, and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, and more.

Snort is an open-source network intrusion detection system (IDS) and intrusion prevention system (IPS) developed by Cisco. It is highly regarded for its ability to perform real-time traffic analysis and packet logging. This guide will walk you through the steps to install and configure Snort on a Windows system.

**Steps to Install and Configure Snort**

**Step 1: Download Snort**

1. Visit the official [Snort download page](https://www.snort.org/downloads)
2. Download the latest Windows installer for Snort.



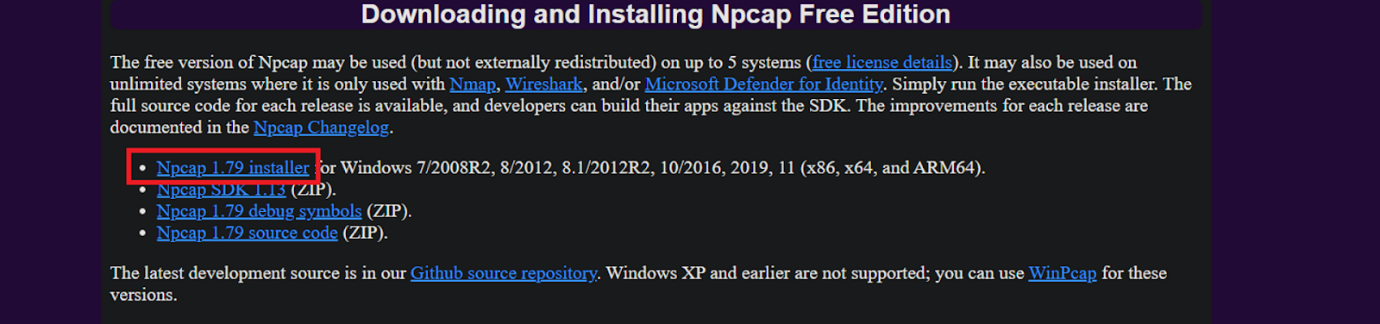
‍

**Step 2: Install WinPcap or Npcap**

Snort requires a packet capture library like WinPcap or Npcap to capture network traffic.

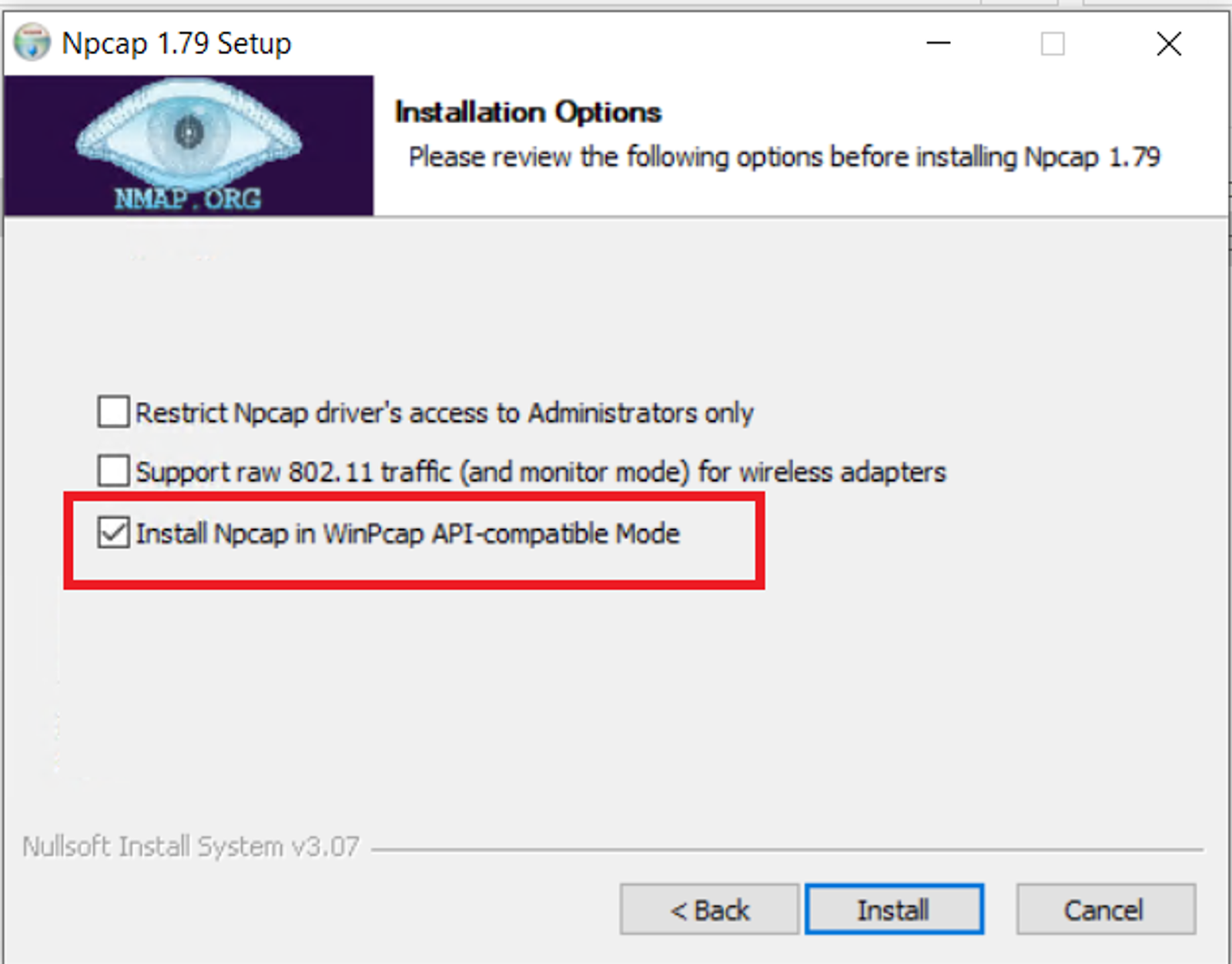
**Download and Install Npcap** (recommended):

* Visit the [Npcap download page](https://npcap.com/" \l "download)
* Download the latest version of Npcap.



‍

* Run the installer and follow the on-screen instructions to complete the installation.
* Make sure to select the option to install Npcap in "WinPcap API-compatible mode".

‍

‍

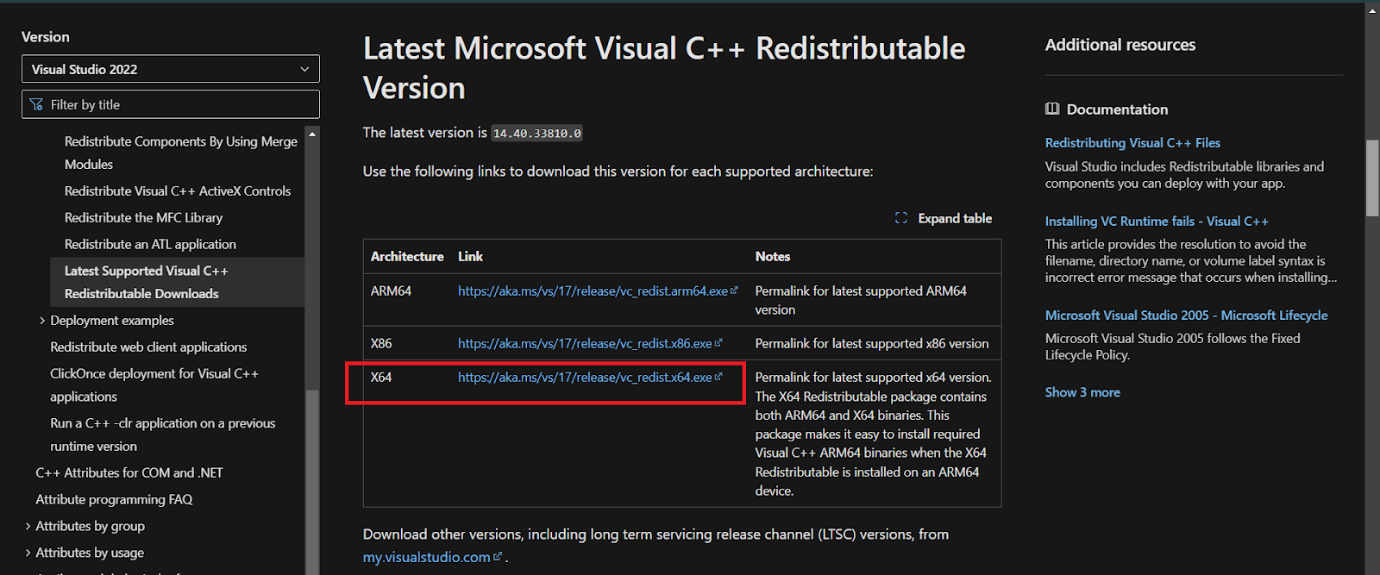
**Alternative: Download and Install WinPcap**:

* Visit the [WinPcap download page](https://www.winpcap.org/install/)
* Download and install the latest version of WinPcap.

**Step 3: Install Visual C++ Redistributable**

Snort requires the Visual C++ Redistributable package to run correctly.

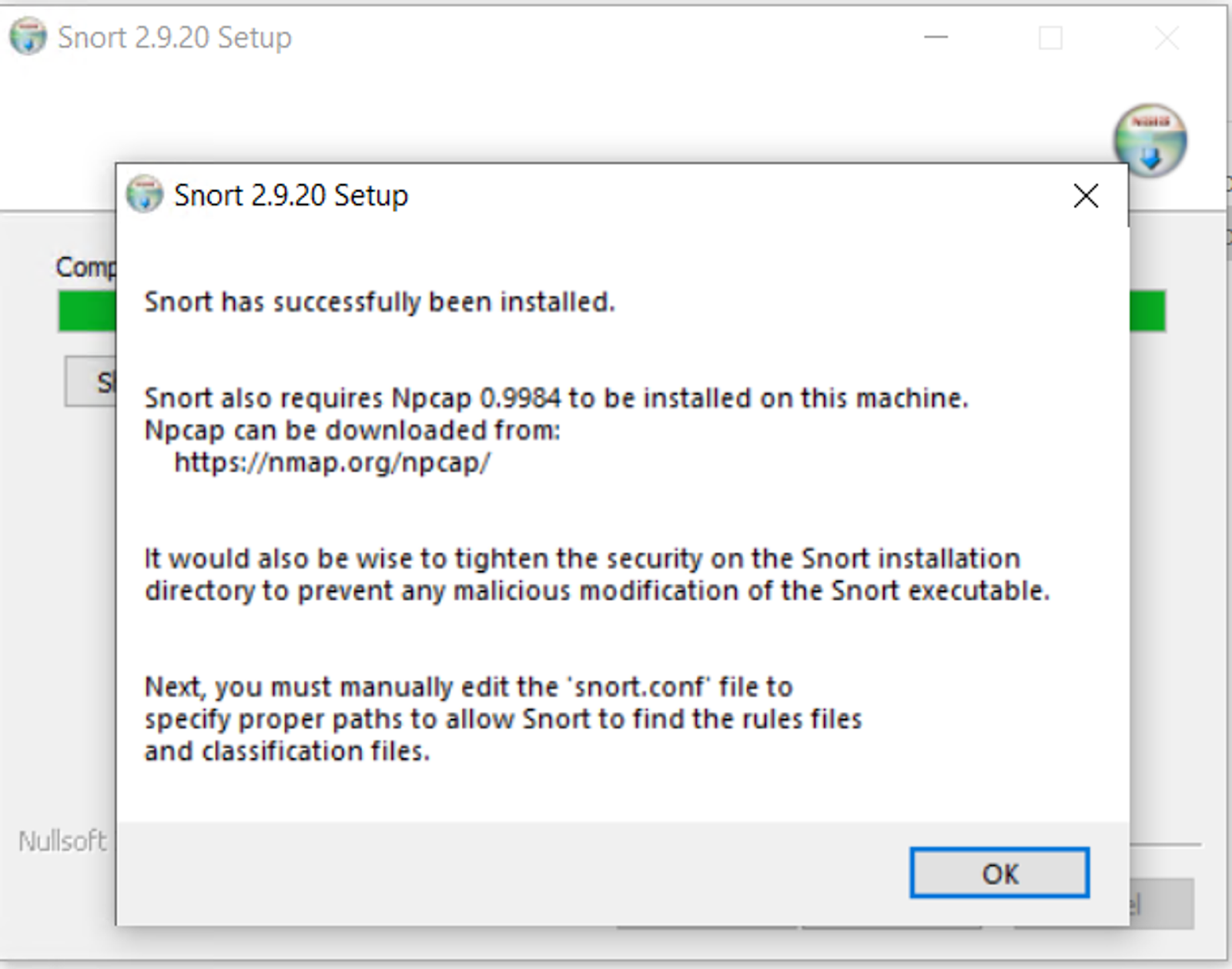
1. **Download and Install Visual C++ Redistributable**:  
    some text
   * Go to the official Microsoft download page for [Visual C++ Redistributable](https://support.microsoft.com/en-us/help/2977003/the-latest-supported-visual-c-downloads)
   * Download and install the Visual C++ Redistributable for Visual Studio 2015, 2017, 2019, and 2022:  
     + Visual C++ Redistributable x86
     + Visual C++ Redistributable x64



**Download and Update Rule Files**: If you need additional rules other than the official snort rules

**Step 4: Install Snort**

* Locate the downloaded Snort installer (typically named something like snort-2.9.x.x-installer.exe).
* Double-click the installer to start the installation process.
* Follow the on-screen instructions to complete the installation. Here are the typical steps:  
    
  + **Welcome Screen**: Click "Next" to proceed.
  + **License Agreement**: Read and accept the license agreement, then click "Next".
  + **Choose Installation Location**: Select the directory where you want to install Snort or leave it at the default location, then click "Next".
  + **Ready to Install**: Click "Install" to begin the installation.
  + **Installation Complete**: Click "Finish" to complete the installation.



**Step 5: Configure Snort**

**Locate Snort Configuration File**:

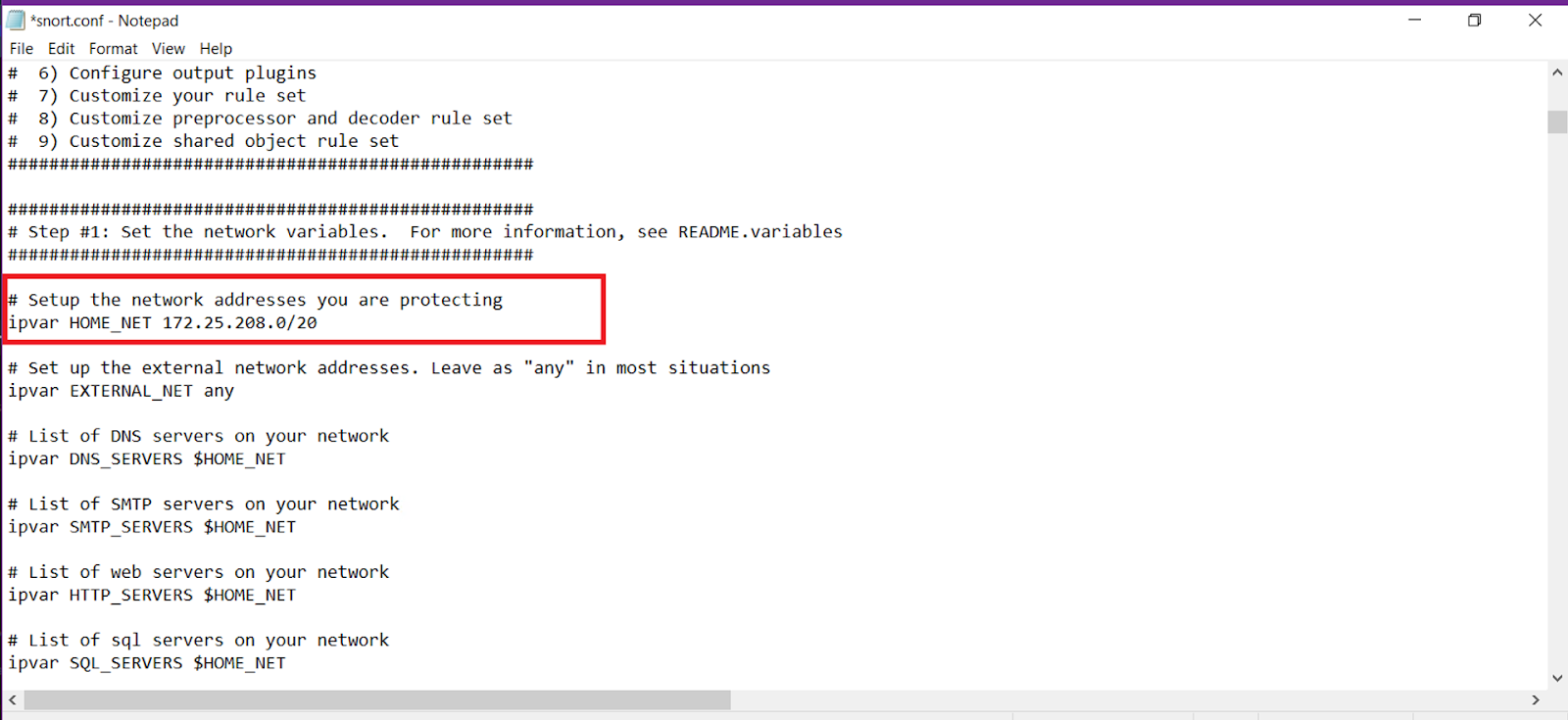
* Navigate to the directory where Snort is installed (e.g., C:\\Snort).
* Open the etc directory and locate the snort.conf file.

‍

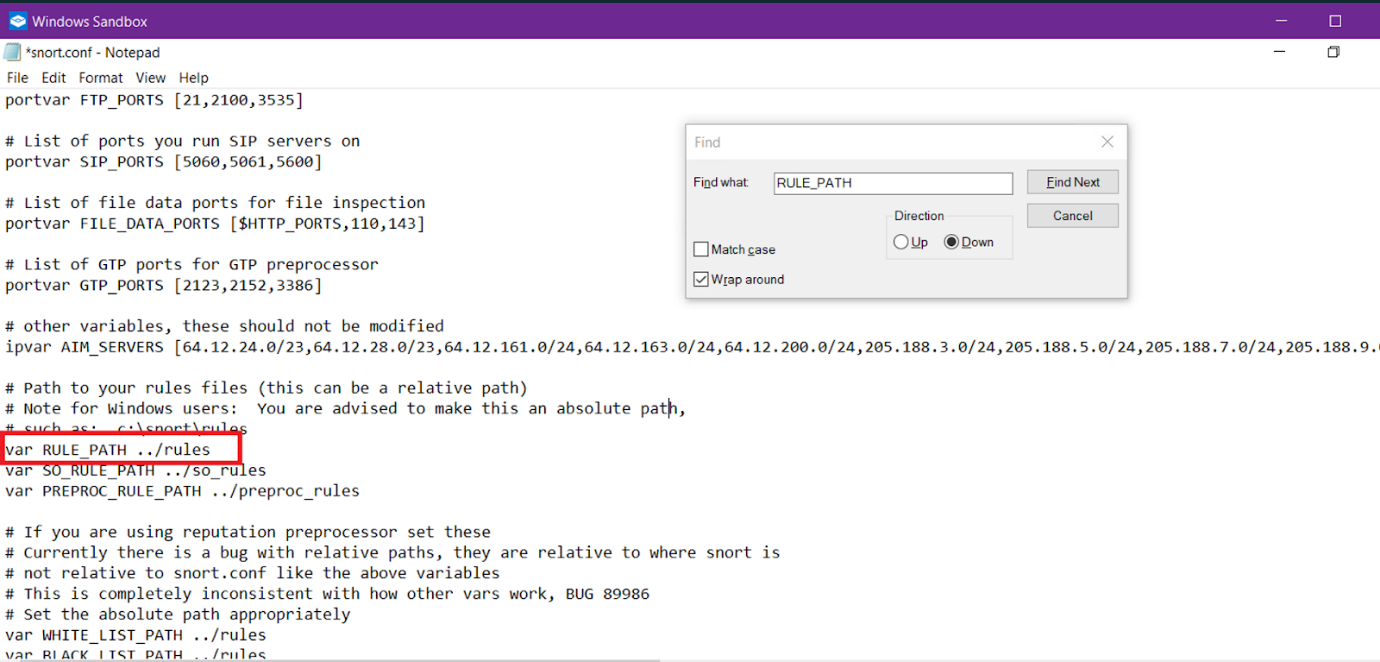
**Edit Snort Configuration File**:

* Open snort.conf with a text editor like Notepad++.
* Configure the network settings by editing the ipvar HOME\_NET variable to match your network configuration. For example: ipvar HOME\_NET 192.168.1.0/24

‍



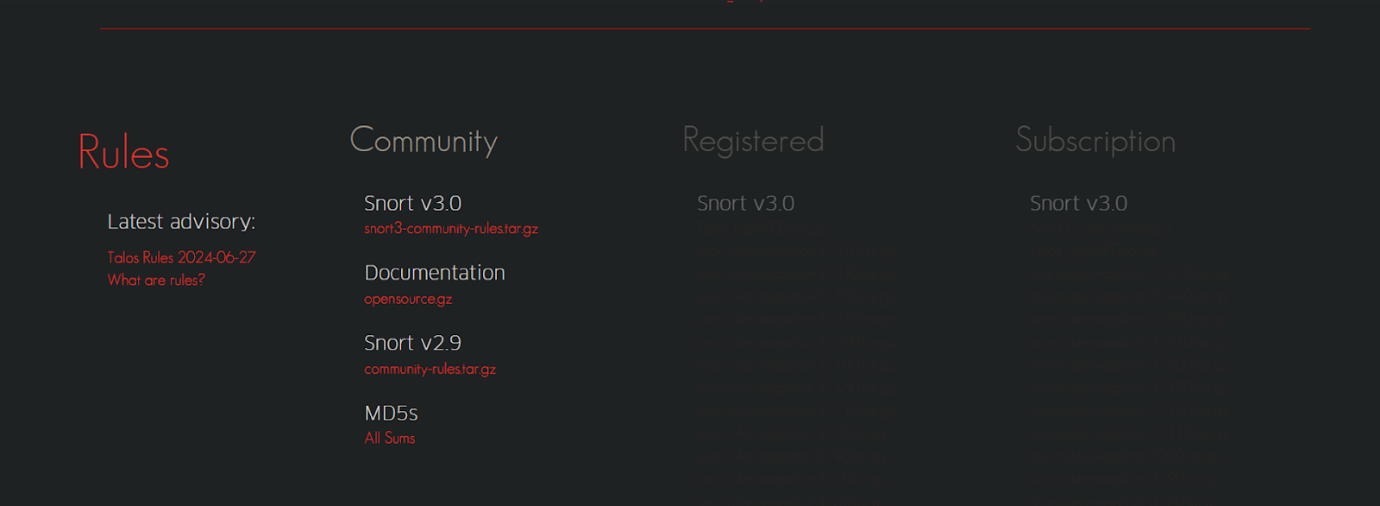
* You can get the network information using ipconfig /all
* Configure the path to the rule files. Ensure the var RULE\_PATH variable points to the correct directory where the rule files are stored.

‍

‍

**Download and Update Rule Files**: If you need additional rules other than the official snort rules

* Visit the [Snort rules download page](https://www.snort.org/downloads)
* Download the latest community rules or registered rules.



‍

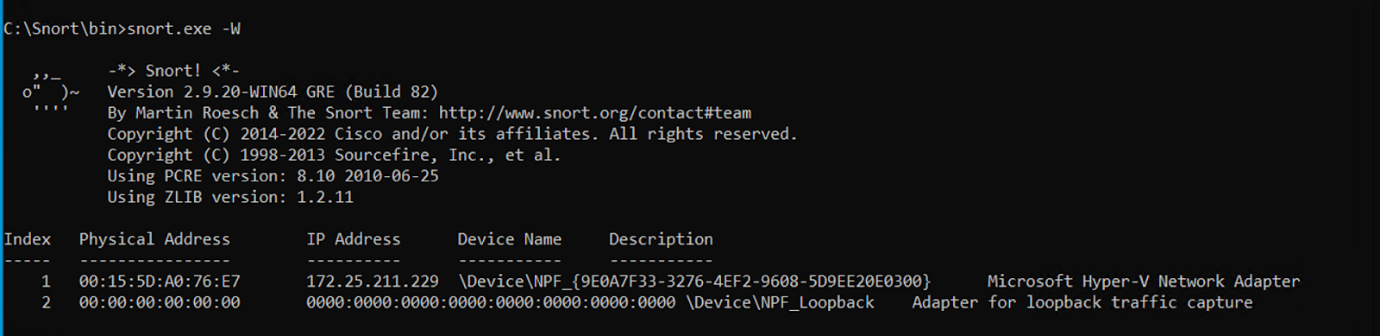
* Extract the downloaded rule files and place them in the rules directory of your Snort installation (e.g., C:\\Snort\\rules).
* Update the include statements in snort.conf to include the rule files you downloaded. For example: include $RULE\_PATH/community.rules

‍

**Step 6: Running Snort**

1. Open the command prompt as an administrator.
2. Navigate to the Snort installation directory (e.g., C:\\Snort\\bin).
3. Run Snort with the following command: Replace <interface> with the number corresponding to your network interface. You can find the interface number by running snort -W.

‍



‍

snort -i <interface> -A console

c:\Snort\bin>snort -i 4 -A console

‍

* **Note:** You can choose the index of the interface directly like this

‍

**Step 7: Verify Snort Installation**

1. Snort should start and begin analyzing network traffic based on the configured rules.
2. Monitor the console output for alerts and notifications.

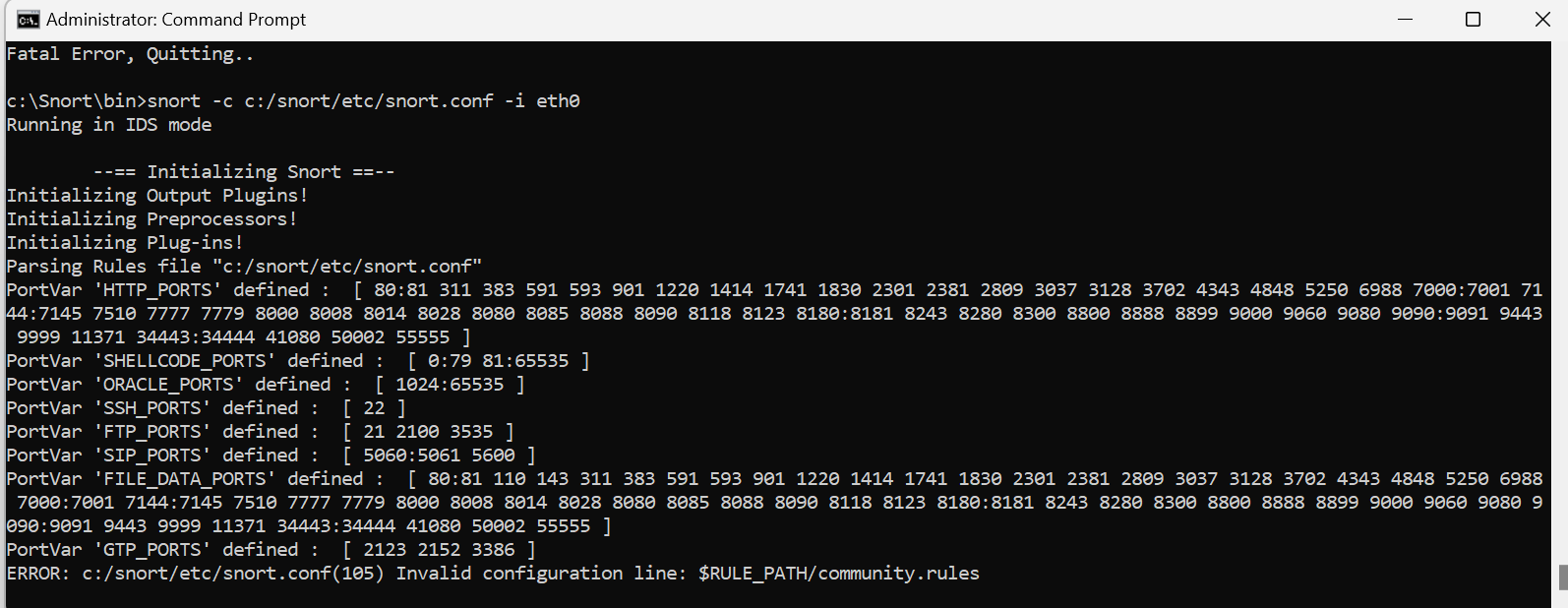


‍

**Useful Commands**

* To list available network interfaces: snort -W
* **For Intrusion Detection (IDS) Mode:**

Snort is usually set up to log and alert about suspicious activities on the network. Use the following command to run Snort in IDS mode:



* -c specifies the configuration file (in this case, /etc/snort/snort.conf).
* -i specifies the network interface (eth0 in this example).

In IDS mode, Snort will inspect traffic and log alerts based on rules defined in the configuration file, but it will not block any traffic.

### For Intrusion Prevention (IPS) Mode:

Snort can also be configured as an IPS, where it actively drops malicious traffic. To run Snort in inline mode (IPS mode), use the following command:

**1. Use IDS Mode on Windows**

If IPS functionality is not critical for your setup on Windows, you can continue using Snort in IDS mode to monitor and alert on suspicious activities.

**Command:**

cmd

Copy code

snort -c C:\Snort\etc\snort.conf -i <interface>

Linux

snort -Q -c /etc/snort/snort.conf -i eth0

* The -Q option is primarily intended for Unix-like systems and may not be supported or fully functional on Windows.
* For **Intrusion Prevention** on Windows, consider integrating Snort with a firewall or using additional tools to block malicious traffic based on Snort's alerts.
* If **IPS functionality** is crucial and you prefer a more straightforward setup, deploying Snort on a Linux-based system is recommended.
* Always ensure you're using the latest version of Snort and consult the official Snort documentation for platform-specific configurations and capabilities.

**Conclusion**

Installing and configuring Snort on Windows is a straightforward process if you follow the steps outlined in this guide. With Snort installed and properly configured, you'll be equipped to monitor network traffic and detect potential security threats effectively.