### **SURICATA INSTALLATION AND CONFIGURATION ON WINDOWS**

Before we start with the installation and configuration of suricata on windows, it is crucial to note that Suricata cannot intercept traaffic on its own on Windows unlike Linux. The reason for this is the fundamental difference between how both the operating systems handle network traffic

#### **Linux**

Linux operating systems provide a standard library called the libpcap, which provides direct access of raw network packets to the applications. With the help of libpcap, Suricata or any similar application can directly interact with the kernel and get a copy of the raw network packets for their use.

#### **Windows**

Windows handles user application access to kernel differently, it does not allow user applications, direct, low-level access to network interfaces. To capture raw network packets on windows a driver would be required, which would then intercept low level network traffic and pass it on to Suricata. WinPcap(Windows Packet capture) was the original library or driver developed to perform this activity. Since WinPcap is not actively maintained and does not support newer versions of Windows, Npcap is widely being used for this purpose. Although Npcap is developed on the same code base as WinPcap, it is actively developed and supports newer versions of Windows and uses NDIS(Network Driver Interface Specification) 6 API.

#### **Downloading required programs and files**

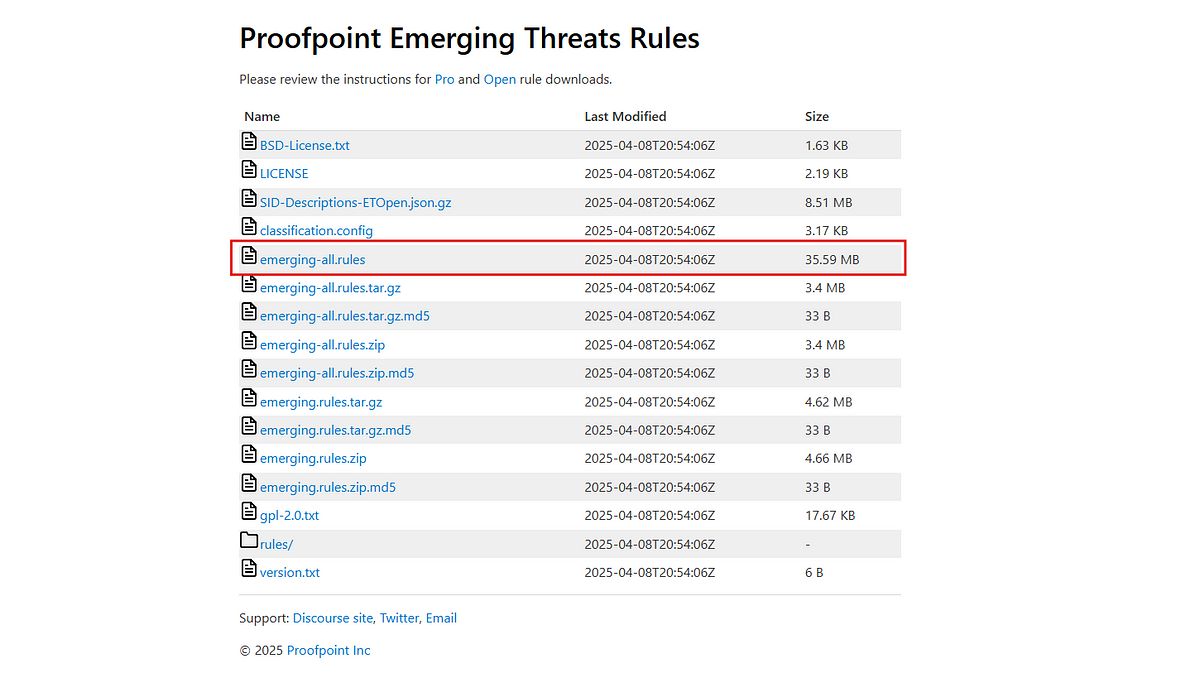
**Suricata download:**

The latest version of Suricata can be downloaded from [here](https://suricata.io/download/).



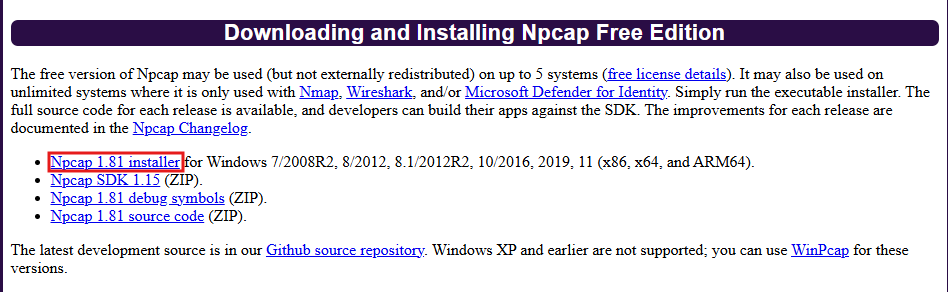
Rules for suricata:

Suricata uses predefined rule files to detect threats. Various rule sets are available for suricata, but we will be using Emerging Threats open rule set which is developed and maintained by proof point. This can be downloaded from [here](https://rules.emergingthreats.net/open).



**Npcap Download**

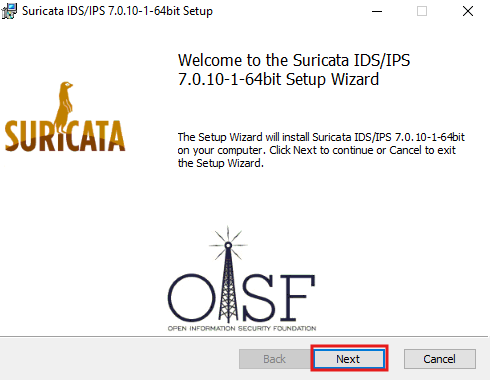
Npcap is a modern packet capture library for Windows, serving as a more secure and actively developed alternative to the older WinPcap. It allows applications to capture and transmit network traffic by interacting with the network adapter driver. It can be downloaded from [here](https://npcap.com/#download).



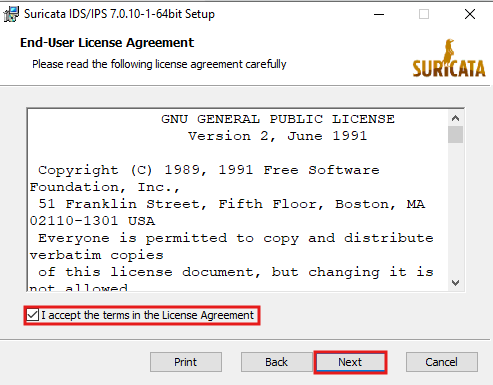
#### **Installations**

**Suricata Installation:**

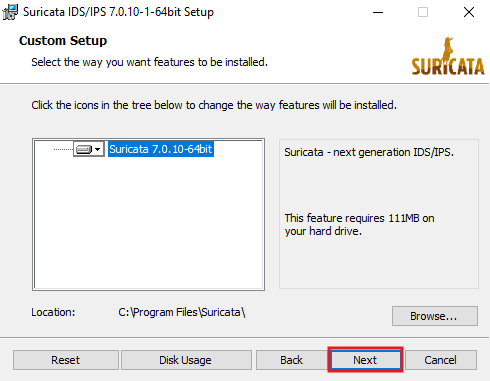
Click on the downloaded suricata msi file. Once the installation window opens click on Next.



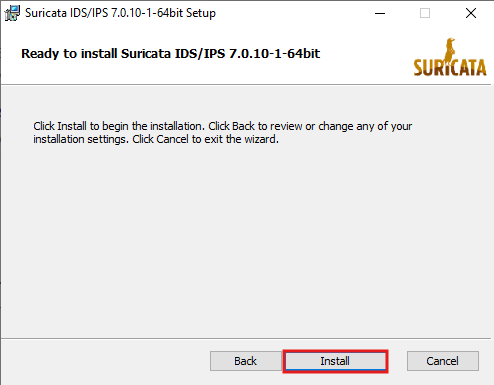
Then accept the terms and click Next.



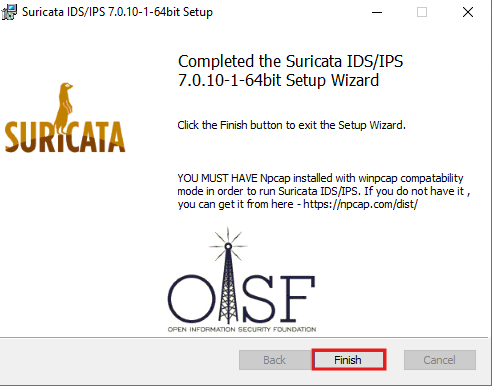
On the cusom setup screen, leave default and click next.



Then, click on install to start the installation process.

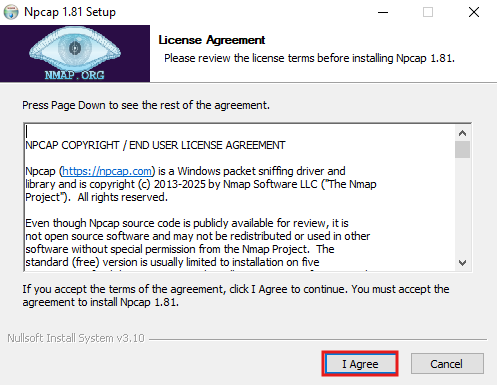


Once the installation is completed, click finish to end the installation process.

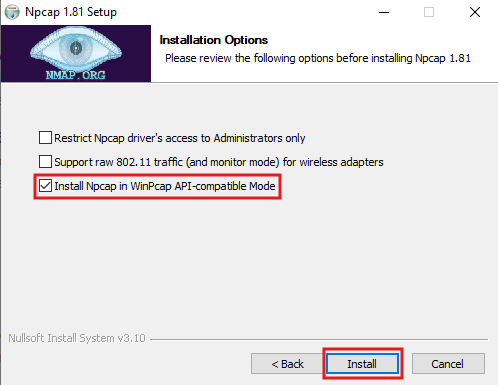


**Npcap Installation:**

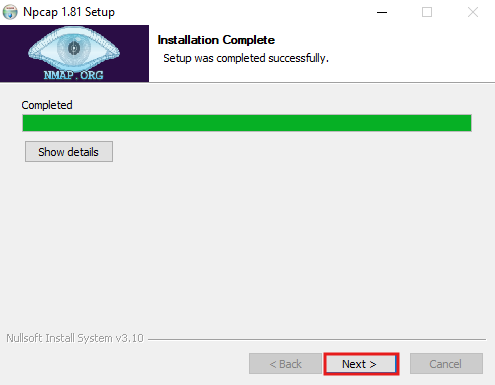
Click on the downloaded npcap exe file. Once the installation window opens, click on I agree to accept the license terms.



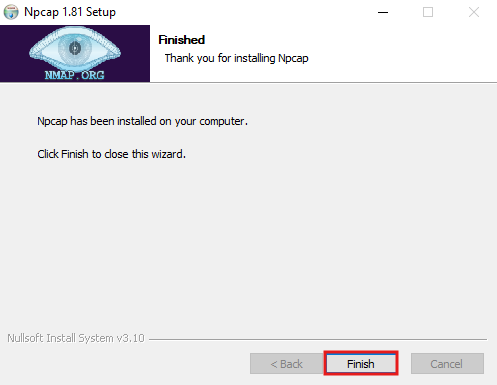
Then check the “Install Npcap in Winpcap API compatible mode” option and click Install.



Once the installation is complete, click on next.

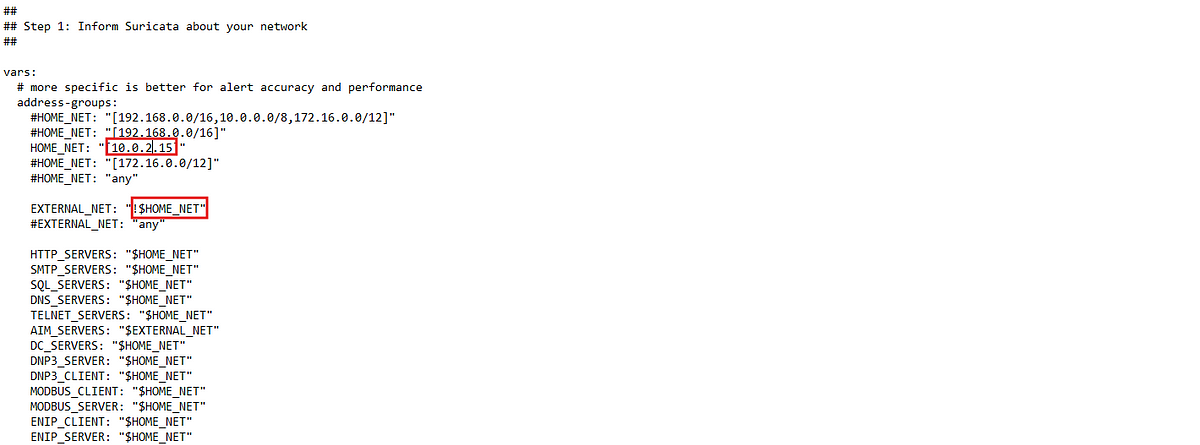


Then click on Finish to end the installation process and closs the installation window.

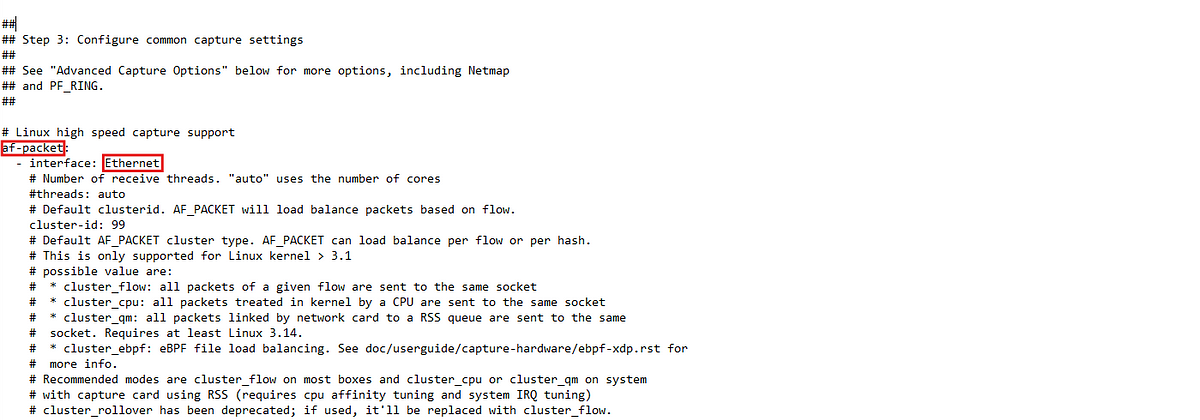
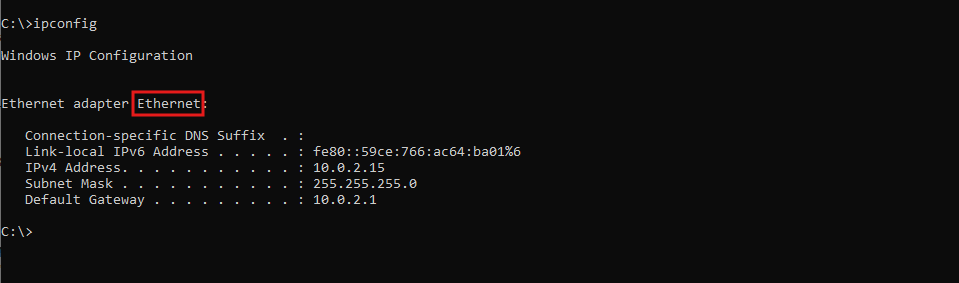


#### **Configuring Suricata**

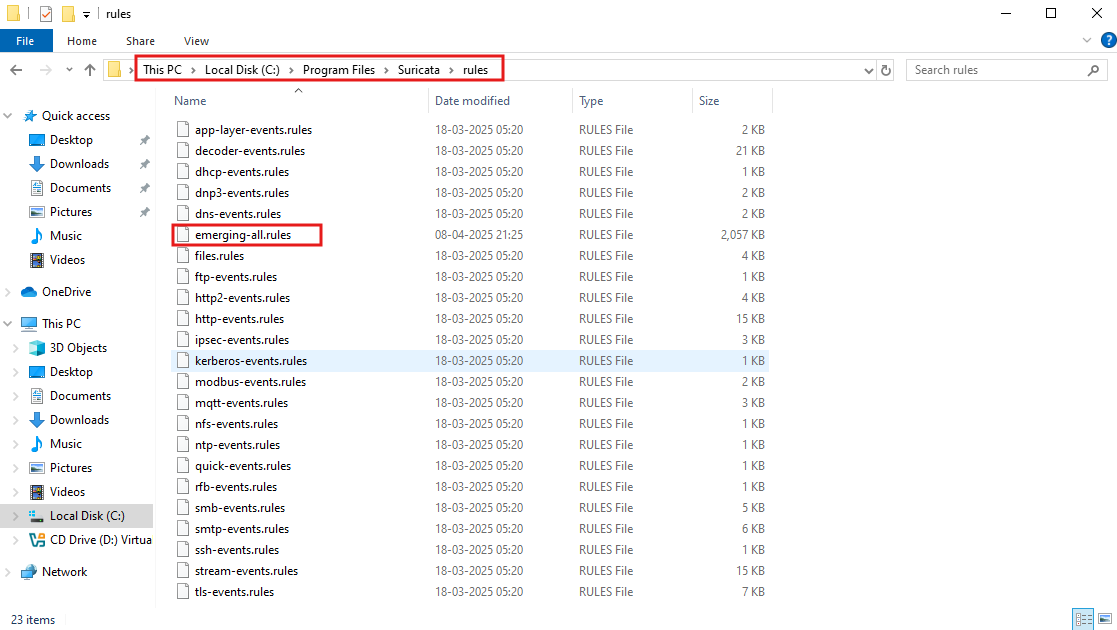
Navigate to the suricata folder at C:\Program Files\Suricata and open the suricata.yaml file. Then set the HOME\_NET to the ip address of the machine. This usually will be a subnet, but for convenience I had added just one IP address. Then set EXTERNAL\_NET to !HOME\_NET.



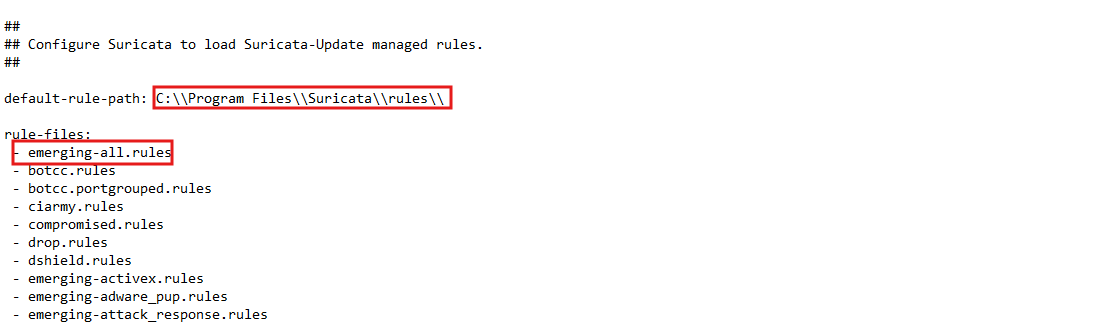
In the suricata.yaml file, search for af-packet variable and set it to the name of the network interface of the windows system. This can be found out by running ipconfig in the command prompt.



Now, copy the downloaded emerging-all.rules file to the rules folder of Suricata located at C:\Program Files\suricata\rules.

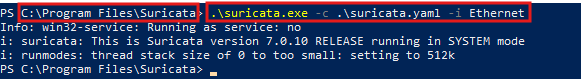


Now add this file to the rule-files section of the suricata.yaml file for Suricata to be able to reference these rules.

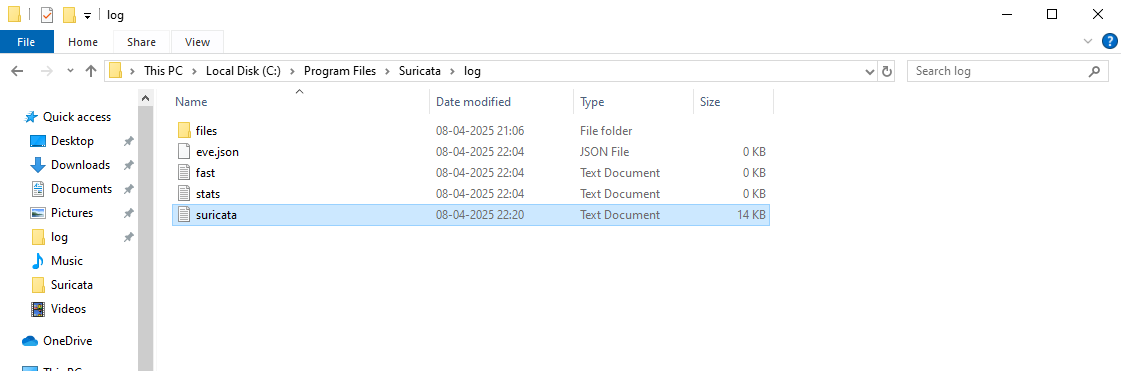


Now, we can run suricata by running the following command under the C:\Program Files\Suricata directory. Replace the <interface> with the network interface of the system.

suricata.exe -c suricata.yaml -i <interface>



We can check if the Suricata is running as intended by checking the log files under the C:\Program Files\Suricata\log.



Now, Suricata is successfully installed and configured on the Windows machine.