**Cryptography & Network Security Lab**

**PRN/ Roll No: 2019BTECS00090**

**Full name: Udaykumar Gadikar**

**Assignment No. 15**

**Title of assignment: Installation and Testing of Snort**

**Title:**

Installation and Testing of Snort

**Aim:**

To install and test snort

**Theory:**

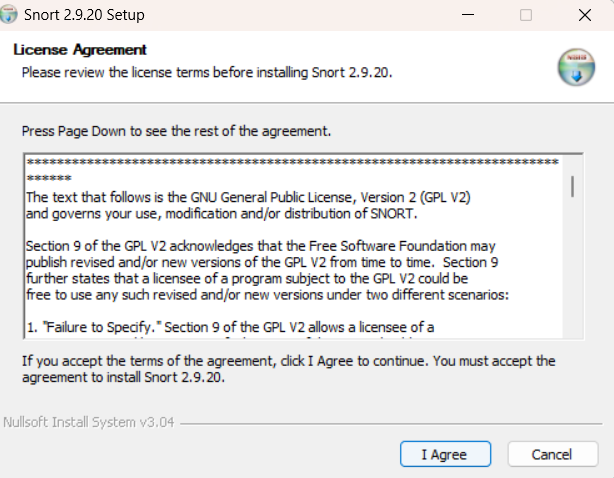
SNORT is a network-based intrusion detection system which is written in C programming language. It was developed in 1998 by Martin Roesch. Now it is developed by Cisco. It is free open-source software. It can also be used as a packet sniffer to monitor the system in real time. The network admin can use it to watch all the incoming packets and find the ones which are dangerous to the system. It is based on library packet capture tool. The rules are easy to create and implement and it can be deployed in any kind of operating system and any kind of network environment. The main reason of the popularity of this IDS over others is that it is a free-to-use software and open source because of which any user can be able to use it as the way he wants.

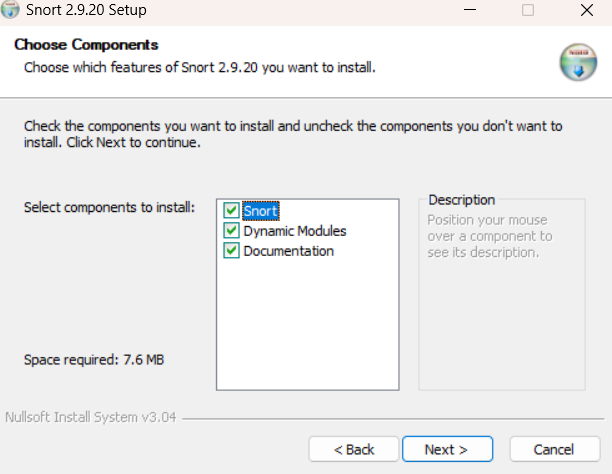
**Features**:

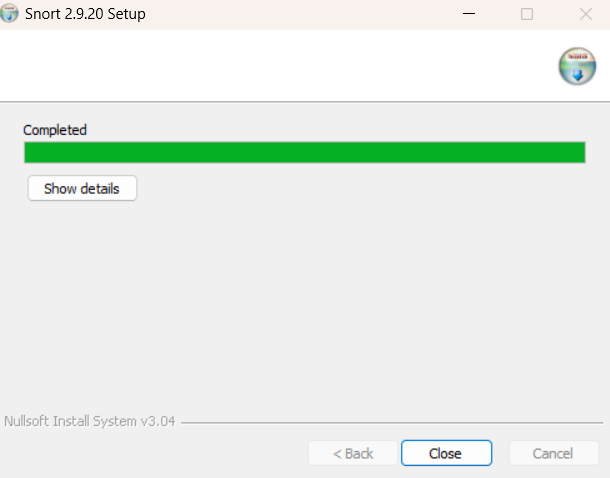
* Real-time traffic monitor
* Packet logging
* Analysis of protocol
* Content matching
* OS fingerprinting
* Can be installed in any network environment.
* Creates logs
* Open Source
* Rules are easy to implement

[**https://zaeemjaved10.medium.com/installing-configuring-snort-2-9-17-on-windows-10-26f73e342780**](about:blank)

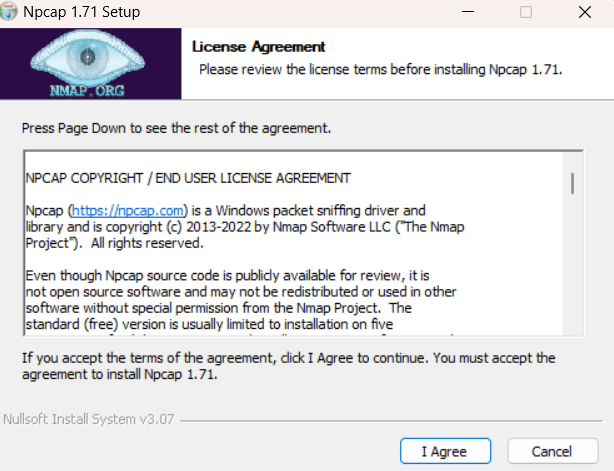
**Installation of snort:**

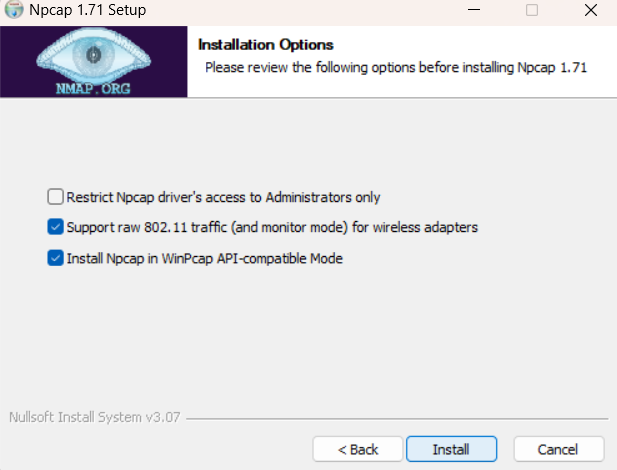
****

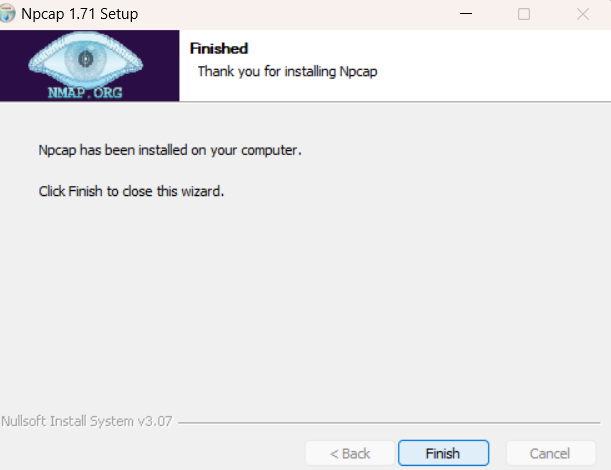
****

****

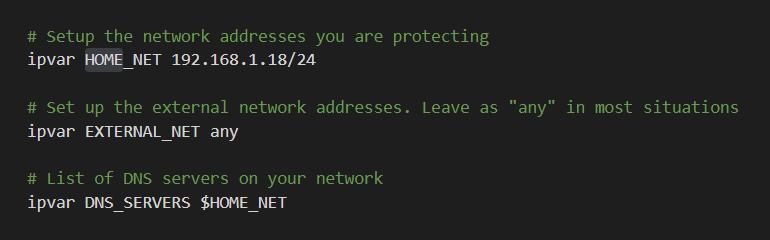
**Npcap installation :**

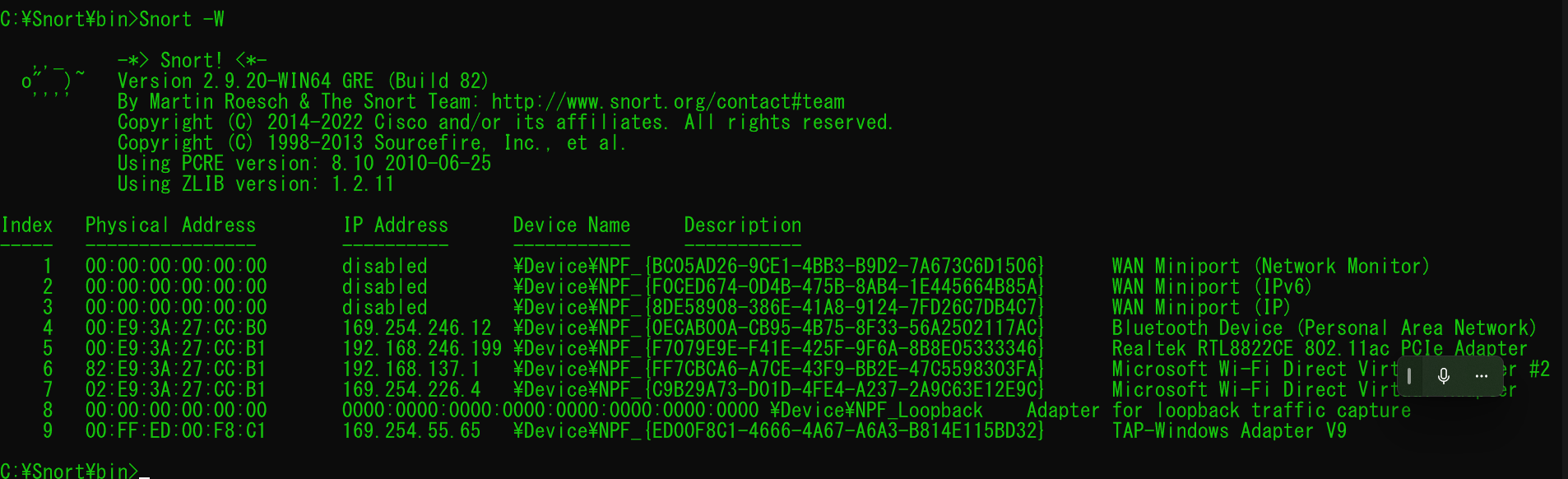
****

****

****

**Config:**

****

****

**Conclusion:**

**Performed the experiment successfully.**

**Snort is installed and tested successfully.**

**It is detecting ping attacks.**