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.

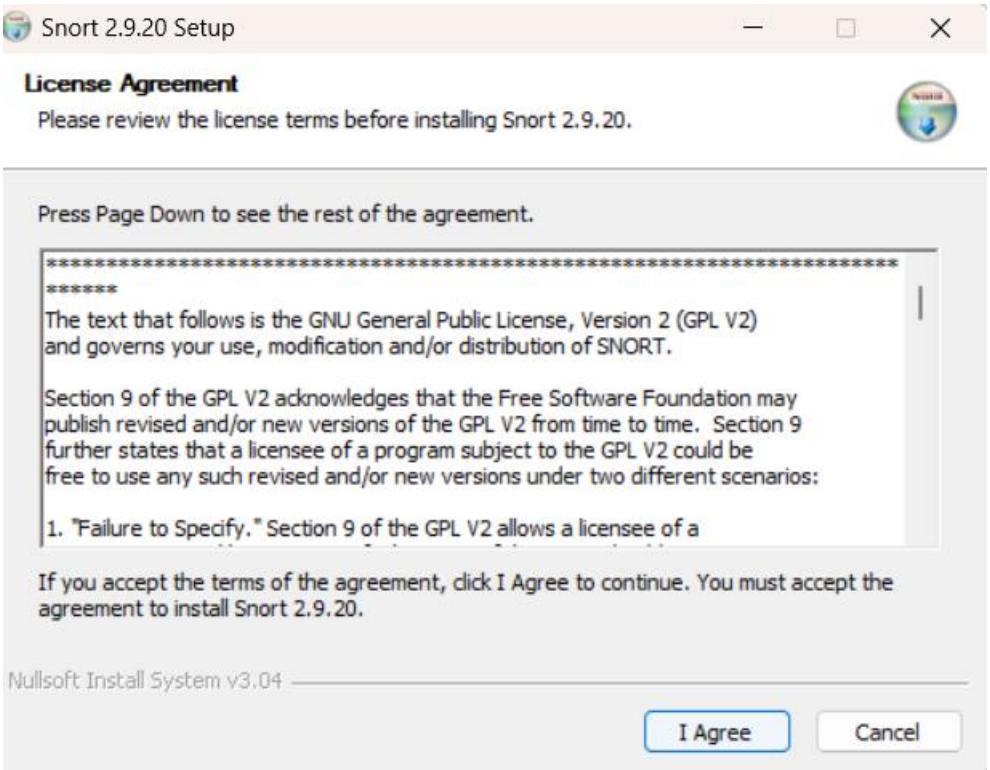
Features:

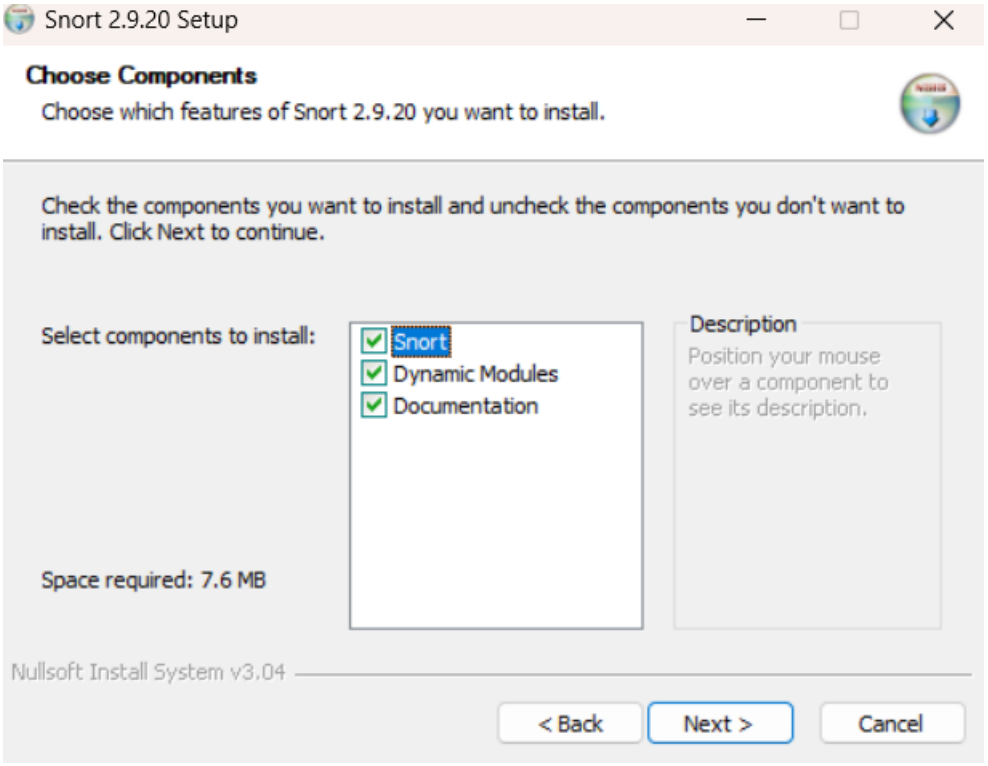
- Real-time traffic monitor
- Packet logging
- Analysis of protocol
- Content matching
- OS fingerprinting
- Can be installed in any network environment.
- Creates logs
- Open Source

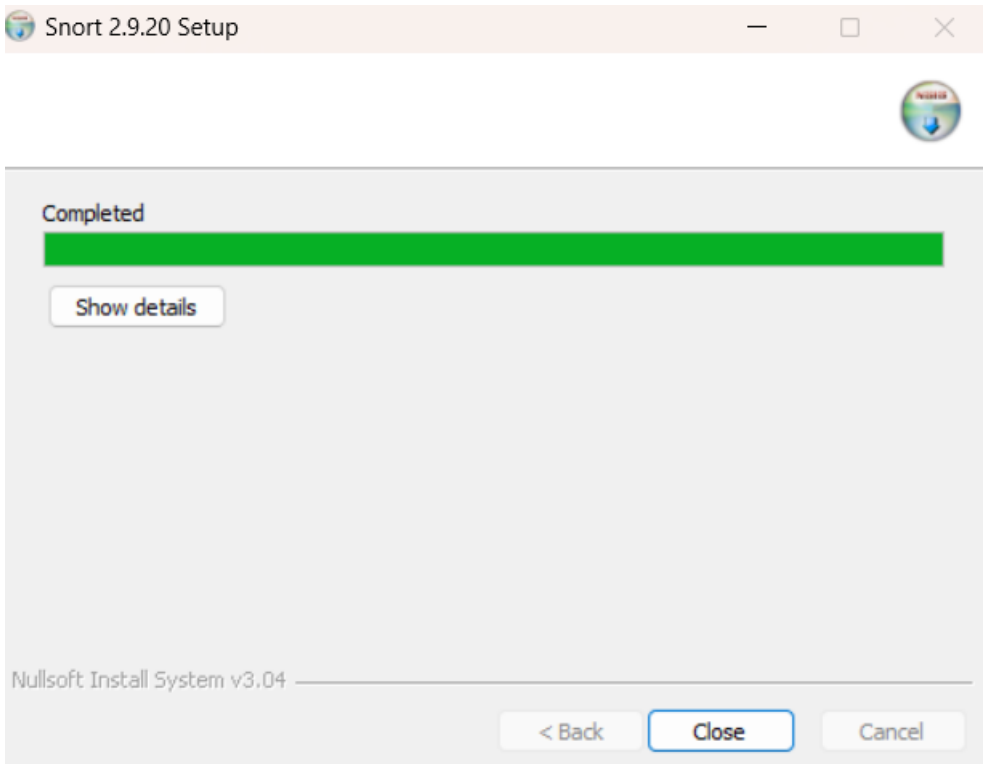
- Rules are easy to implement

https://zaeemjaved10.medium.com/installing-configuring-snort-2-9-17-on-windows-10-26f73e342780

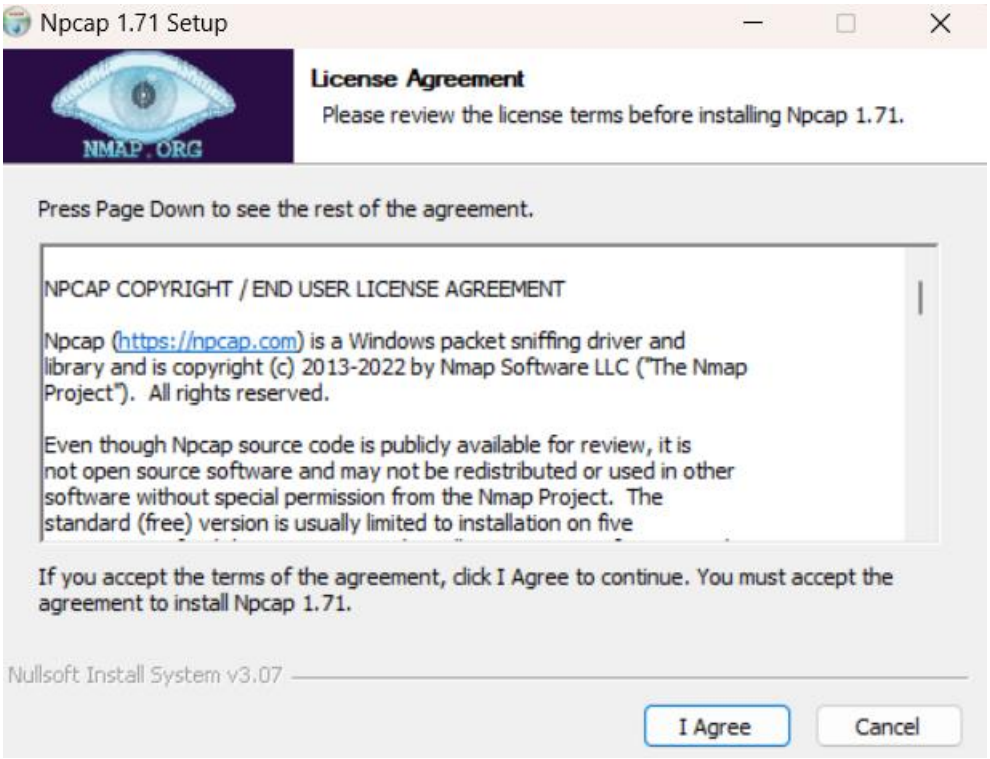
Installation of snort:

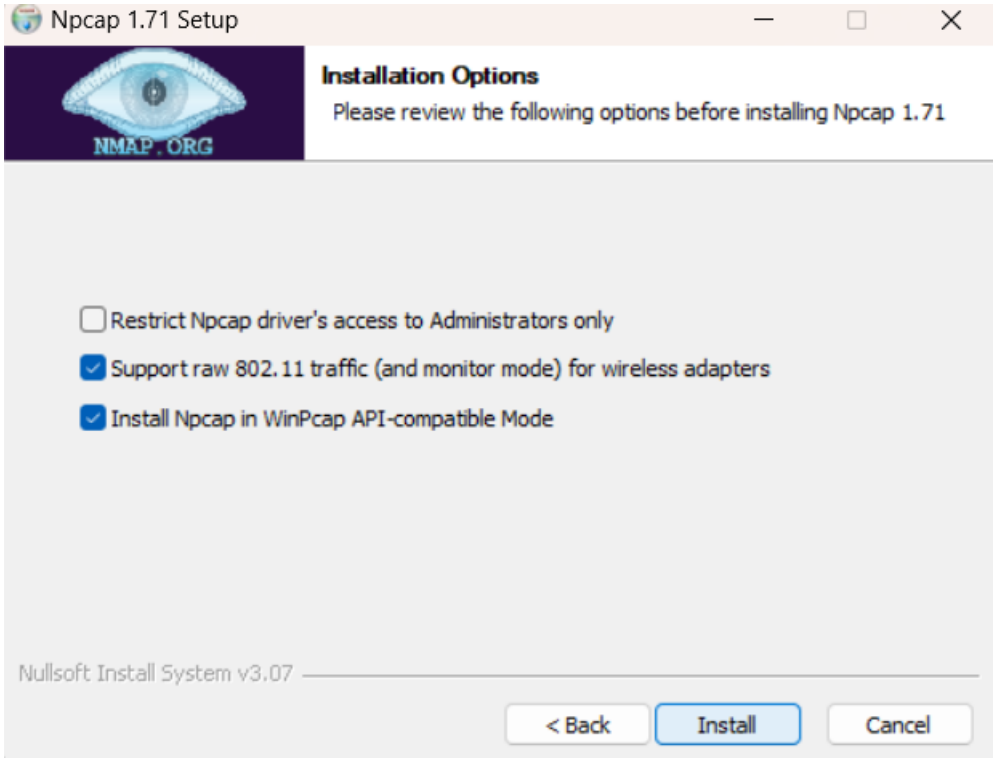


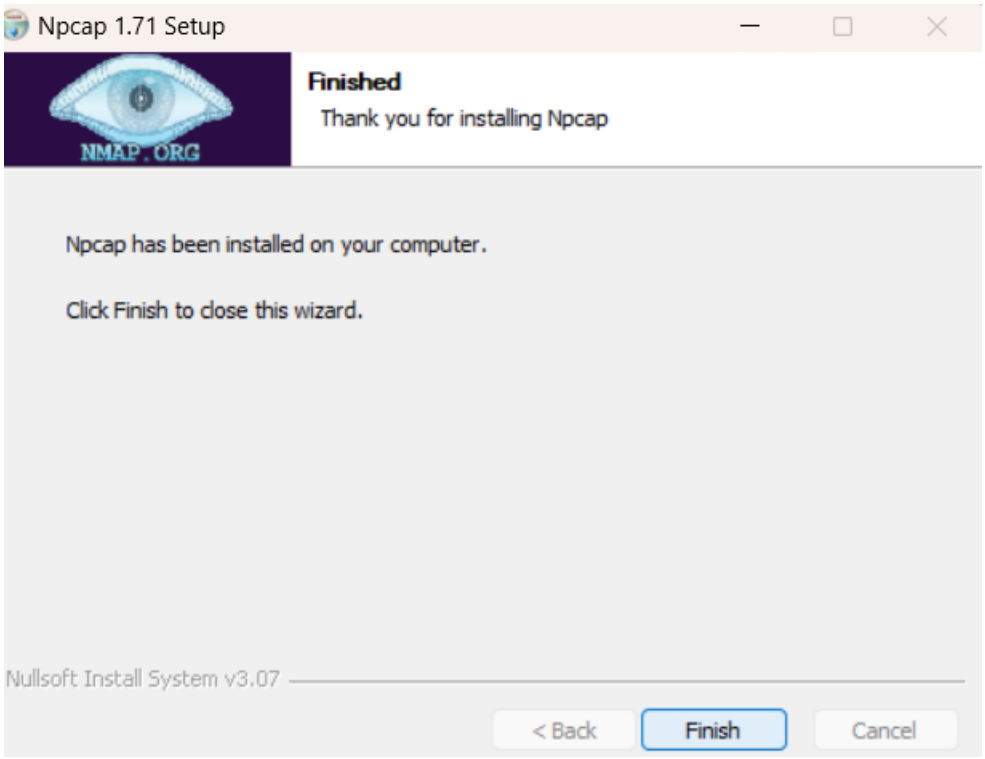




Npcap installation :


Npcap 1.71 Setup
NMAP.ORG
License Agreement
Please review the license terms before installing Npcap 1.71.
Press Page Down to see the rest of the agreement.
NPCAP COPYRIGHT / END USER LICENSE AGREEMENT
Npcap (https://npcap.com) is a Windows packet sniffing driver and library and is copyright (c) 2013-2022 by Nmap Software LLC ("The Nmap Project"). All rights reserved.
Even though Npcap source code is publicly available for review, it is not open source software and may not be redistributed or used in other software without special permission from the Nmap Project. The standard (free) version is usually limited to installation on five
If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Npcap 1.71.
Nullsoft Install System v3.07
I Agree
Cancel


Npcap 1.71 Setup
NMAP.ORG
Installation Options
Please review the following options before installing Npcap 1.71
Restrict Npcap driver's access to Administrators only
Support raw 802.11 traffic (and monitor mode) for wireless adapters
Install Npcap in WinPcap API-compatible Mode
Nullsoft Install System v3.07
< Back
Install
Cancel



Config:

```
# Setup the network addresses you are protecting
ipvar HOME_NET 192.168.1.18/24

# Set up the external network addresses. Leave as "any" in most situations
ipvar EXTERNAL_NET any

# List of DNS servers on your network
ipvar DNS_SERVERS $HOME_NET
```

```
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_{BC05AD26-9CE1-4BB3-B9D2-7A673C6D1506}      WAN Miniport (Network Monitor)
    2   00:00:00:00:00:00       disabled        ¥Device¥NPF_{F0CED674-0D4B-475B-8AB4-1E445664B85A}      WAN Miniport (IPv6)
    3   00:00:00:00:00:00       disabled        ¥Device¥NPF_{8DE58908-386E-41A8-9124-7FD26C7DB4C7}      WAN Miniport (IP)
    4   00:E9:3A:27:CC:B0       169.254.246.12  ¥Device¥NPF_{0ECAB00A-CB95-4B75-8F33-56A2502117AC}      Bluetooth Device (Personal Area Network)
    5   00:E9:3A:27:CC:B1       192.168.246.199 ¥Device¥NPF_{F7079E9E-F41E-425F-9F6A-8B8E05333346}      Realtek RTL8822CE 802.11ac PCIe Adapter
    6   82:E9:3A:27:CC:B1       192.168.137.1   ¥Device¥NPF_{FF7CBCA6-A7CE-43F9-BB2E-47C5598303FA}      Microsoft Wi-Fi Direct Virtual Adapter #2
    7   02:E9:3A:27:CC:B1       169.254.226.4   ¥Device¥NPF_{C9B29A73-D01D-4FE4-A237-2A9C63E12E9C}      Microsoft Wi-Fi Direct Virtual Adapter
    8   00:00:00:00:00:00       0000:0000:0000:0000:0000:0000:0000:0000 ¥Device¥NPF_Loopback    Adapter for loopback traffic capture
    9   00:FF:ED:00:F8:C1       169.254.55.65   ¥Device¥NPF_{ED00F8C1-4666-4A67-A6A3-B814E115BD32}      TAP-Windows Adapter V9

C:¥Snort¥bin>_
```

Conclusion:

Performed the experiment successfully.

Snort is installed and tested successfully.

It is detecting ping attacks.