**4CS372 : Cryptography and Network Security**

**B.Tech. (CSE) – I [ 2022-23 ]**

**Assignment**

**Snort Intrusion Detection System (IDS)**

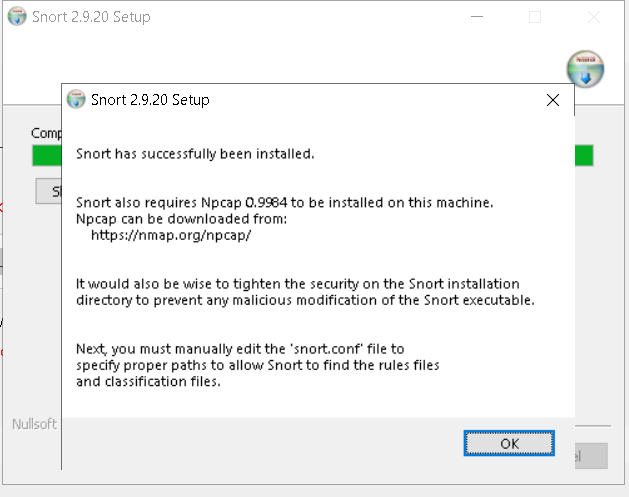
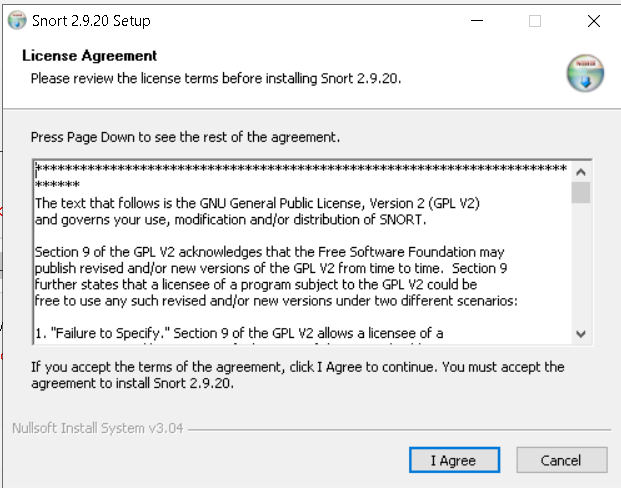
**Title: Snort Intrusion Detection System (IDS)**

**Aim: To Demonstrate Snort Intrusion Detection System (IDS)**

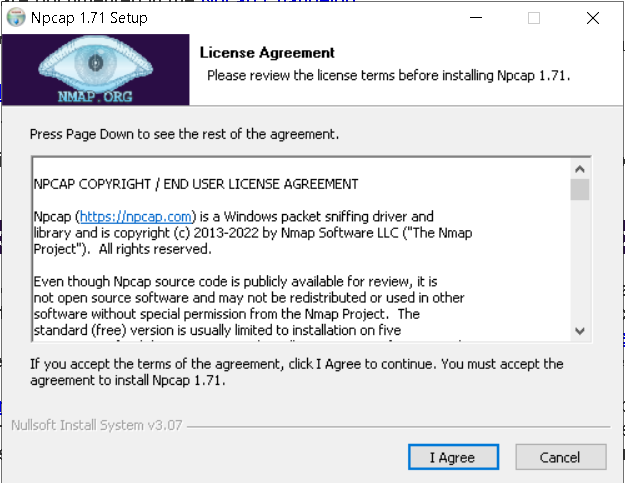
**Theory:**

**In this lab we will explore the Snort IDS. This is a signature based intrusion detection system used to detect network attacks. Snort can also be used as a simple packet logger, however we won't be doing that in this lab. Snort has multiple modes of operation, for the lab we will use snort as a packet sniffer, not inline.**

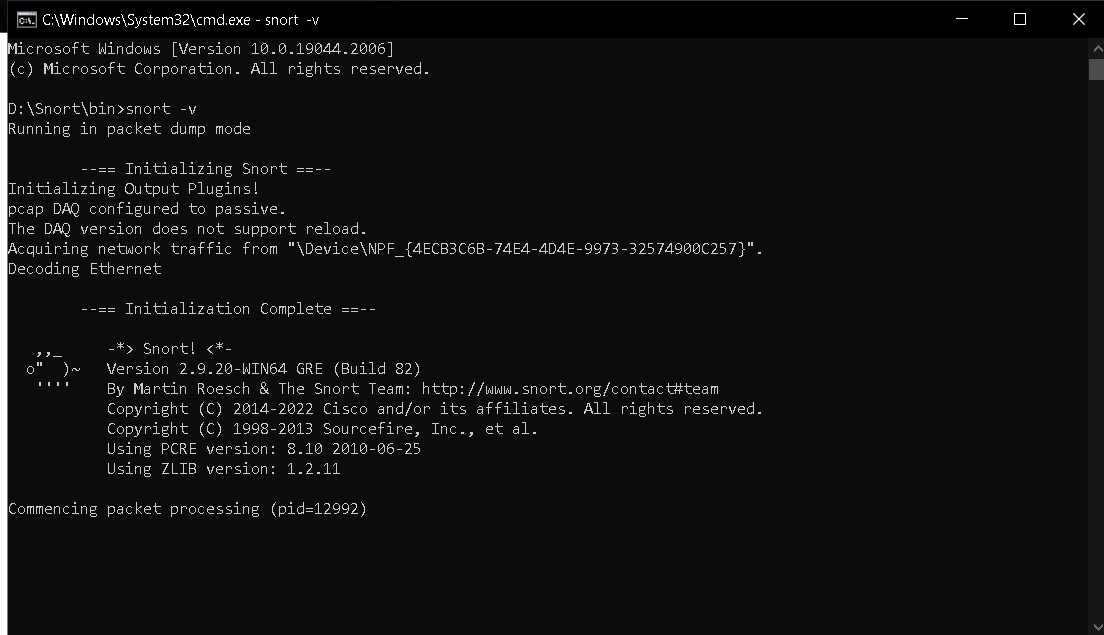
**Installed Snort:**

****

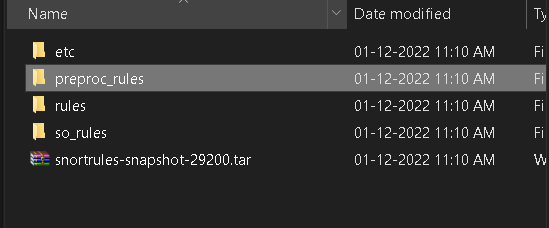
**Installing Npcap is required by snort for proper functioning.Npcap for Windows 10 can be downloaded from [here](https://nmap.org/npcap/" \t "https://zaeemjaved10.medium.com/_blank)**.**Opening Npcap setup file, Click on ‘I Agree’ To license agreement.**

****

**After installing Snort and Npcap enter these commands in windows 10 Command prompt to check snorts working**

****

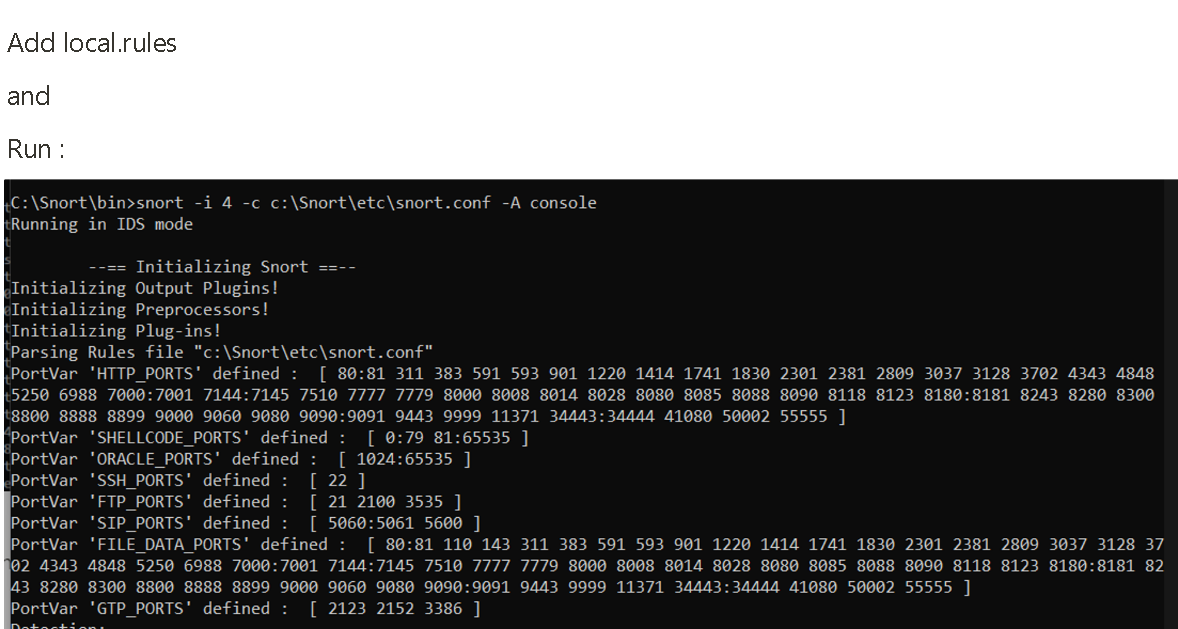
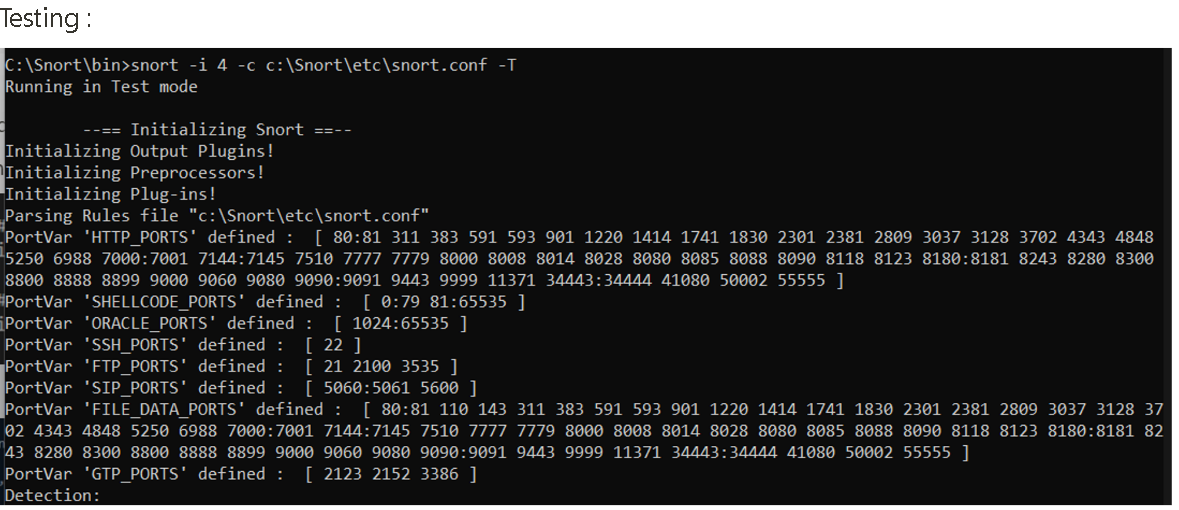
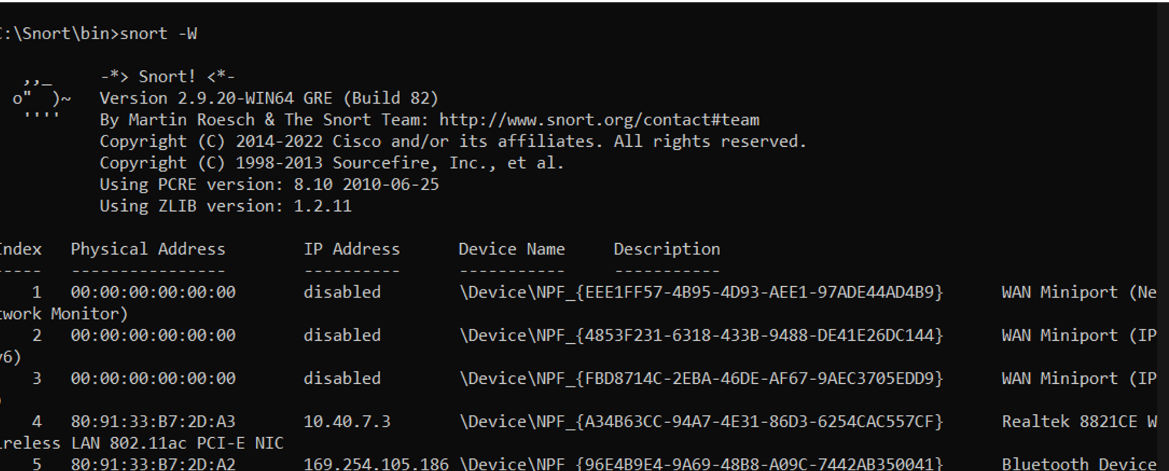
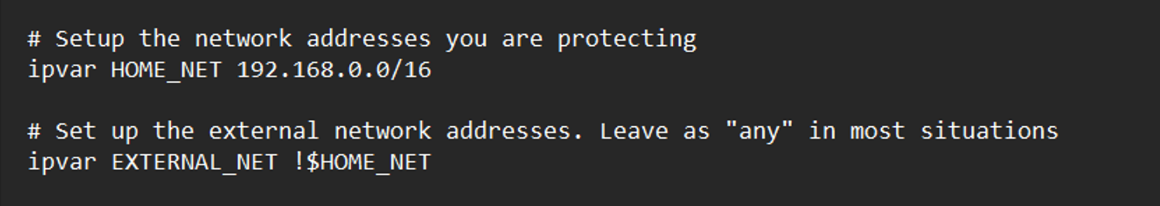
**As you can see in the above figure that snort runs successfully.**

****

**Add “rules” and “preproc\_rules” to the c:\snort\rules and c:\snort\preproc\_rules respectively**

**configure the snort.conf file**

**Now open the **snort.conf** file through the notepad++ editor or any other text editor to edit configurations of snort to make it work like we want it to.**

****