Assignment No. :- 4

Title : Configure and demonstrate Snort tool for intrusion

Aim : Configure and demonstrate use of vulnerability assessment tool such as Snort tool for intrusion or SSL Web security

Objective :

Study any vulnerability assessment tool such as Snort tool and use its implementation features.

Theory :

**Intoduction to Snort :**

Snort is a popular choice for running a network intrusion detection systems or NIDS for short. It monitors the package data sent and received through a specific network interface.

NIDS can catch threats targeting your system vulnerabilities using signature-based detection and protocol analysis technologies. NIDS software, when installed and configured appropriately, can identify the latest attacks, malware infections, compromised systems, and network policy violations.

**Platforms on which Snort runs**

Sonrt runs on most UNIX and various windows.

• UNIX

o Applet, MAC, BEOS, JBM, AIX, BSD open etc.

• LINUX

o Mandrake LINUX, Red Hat, SUSE LINUX etc.

• WINDOWS

o Windows server 2003/XP/2000/NT

## What can I do with Snort?

Snort has three primary uses:

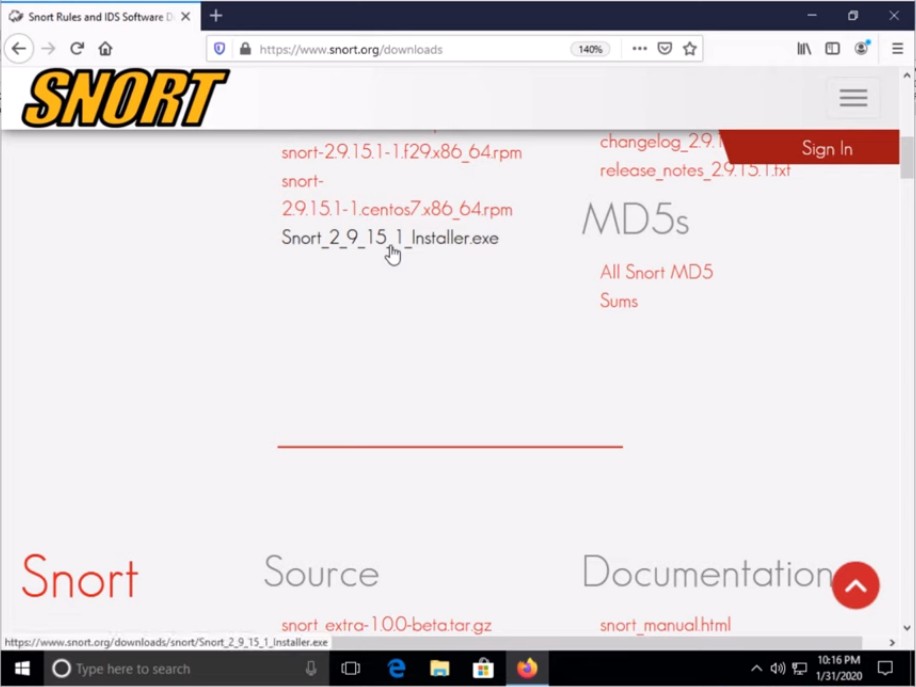
1. It can be used as a straight packet sniffer like tcpdump.
2. A packet logger (useful for network traffic debugging, etc).
3. As a full blown network intrusion prevention system.

Installation

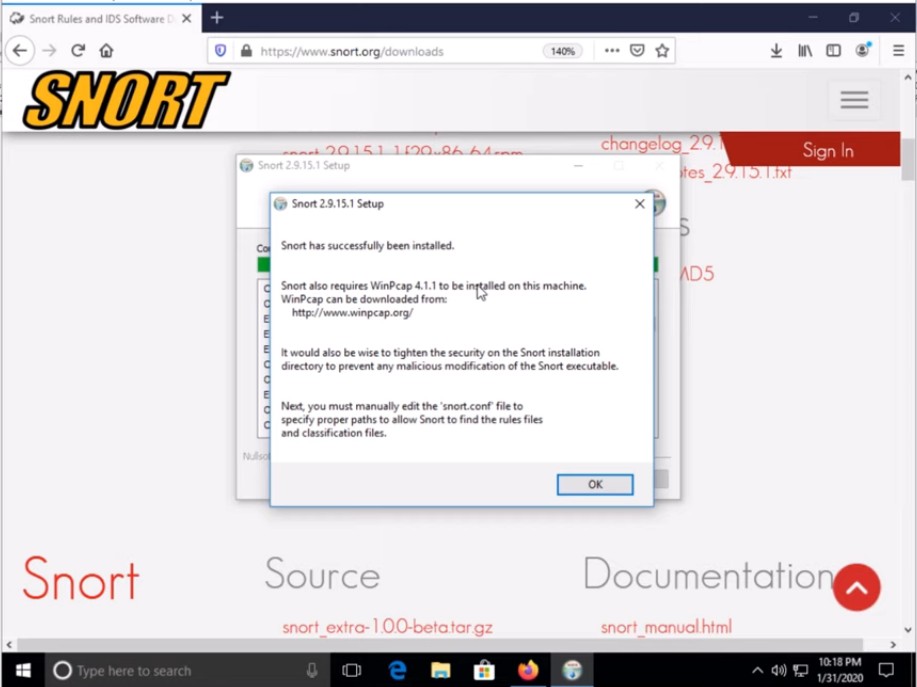
The installation and configuration of Snort :

Download snort from it main website:

<https://www.snort.org/downloads>



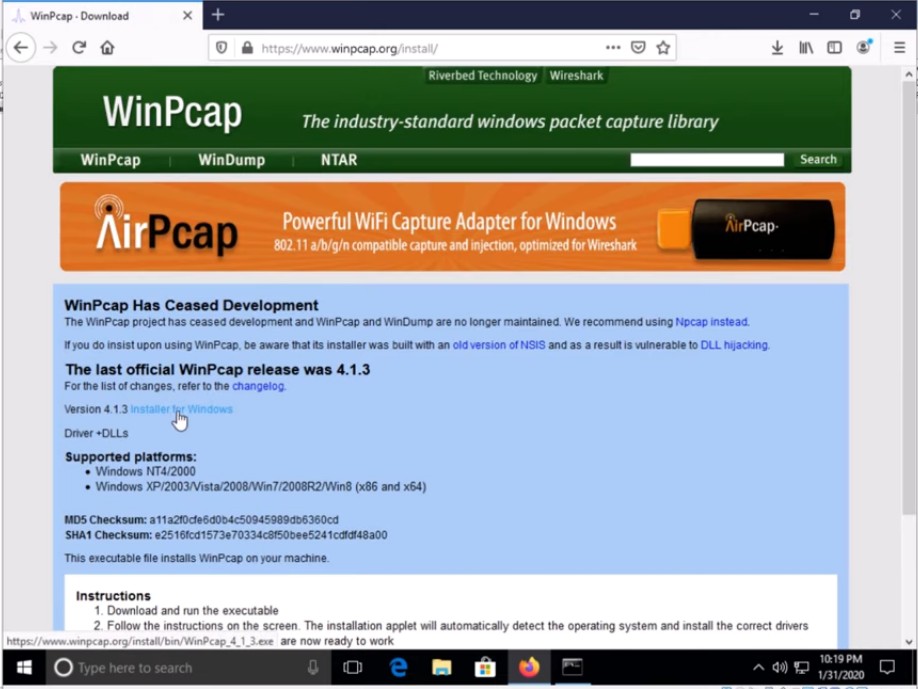
Download this package (generally called [Snort\_2\_9\_15\_1\_Installer.x86.exe](https://www.snort.org/downloads/snort/Snort_2_9_16_1_Installer.x86.exe))

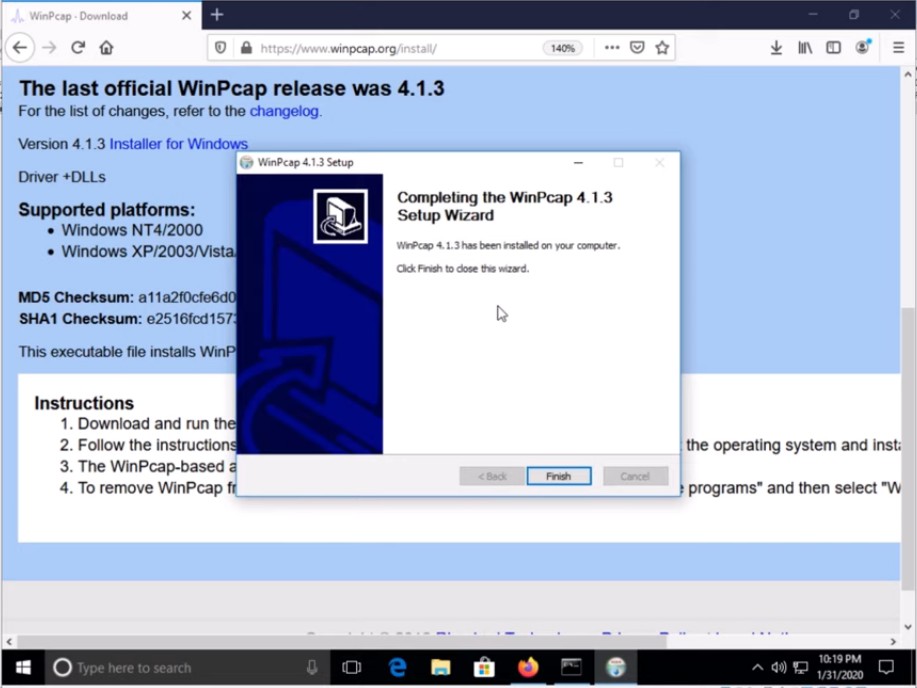


Installation of WinpCap :

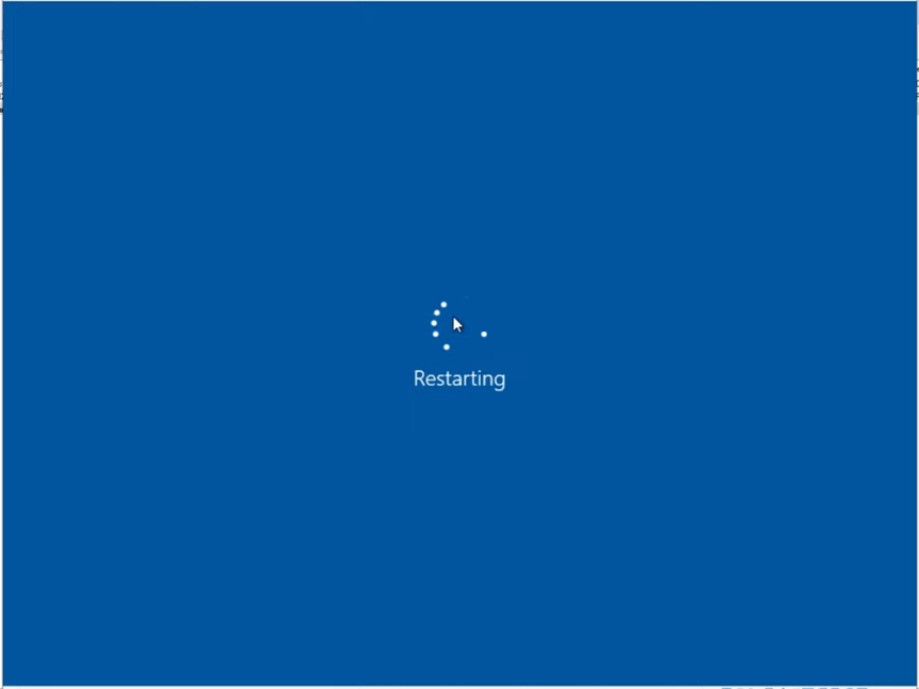
Download WinpCap from main website :

<https://www.winpcap.org/install>

click on the version 4.1.3 for windows



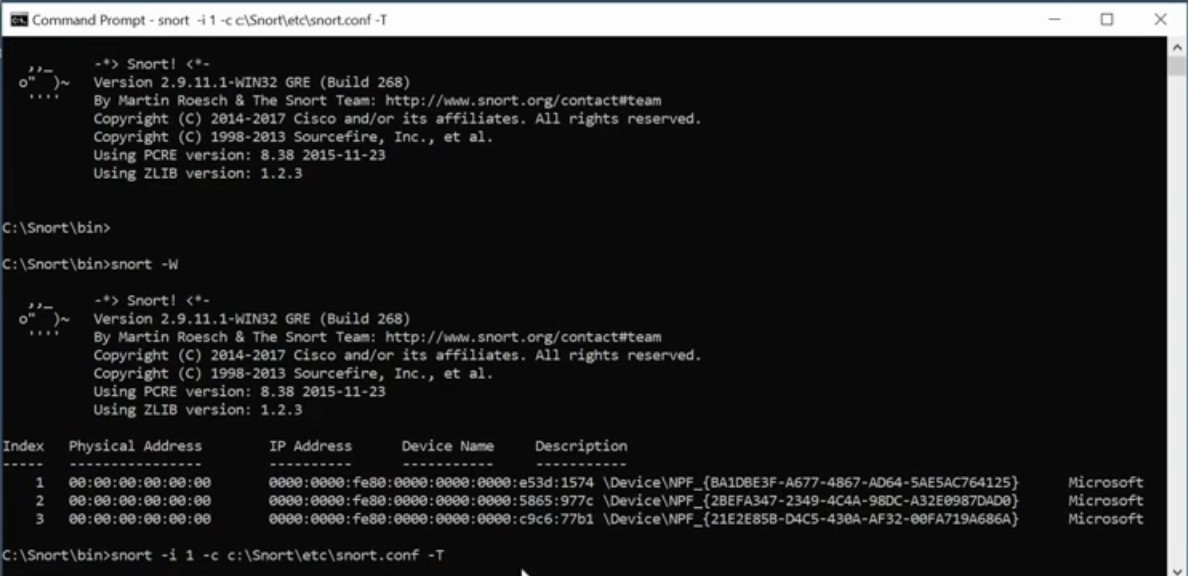
restart the computer

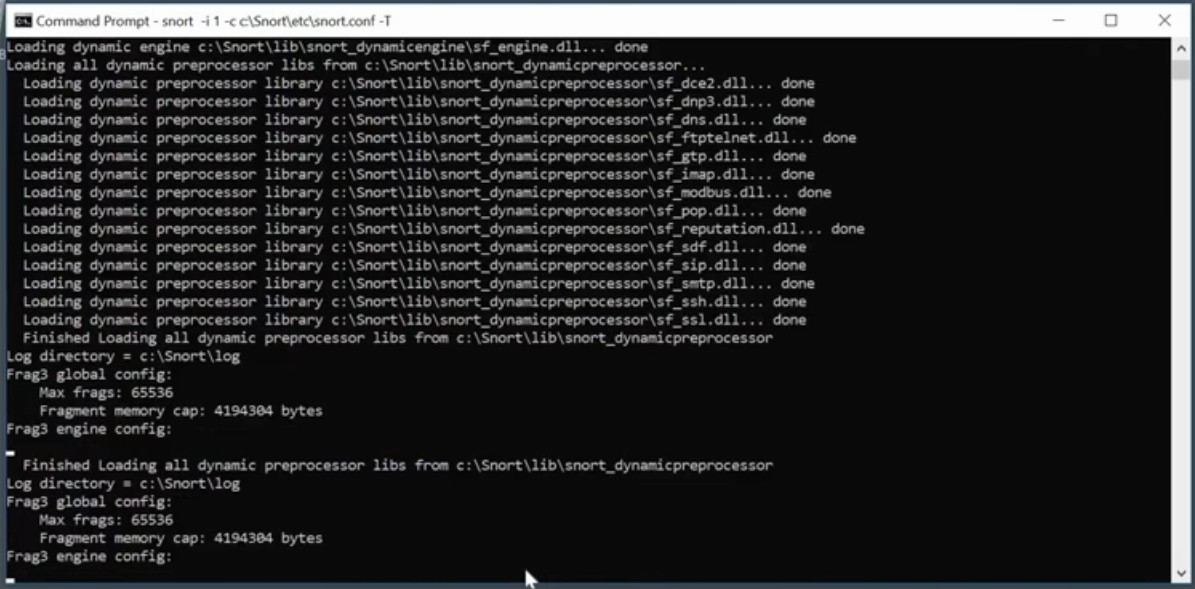


The Snort Rule configuration:

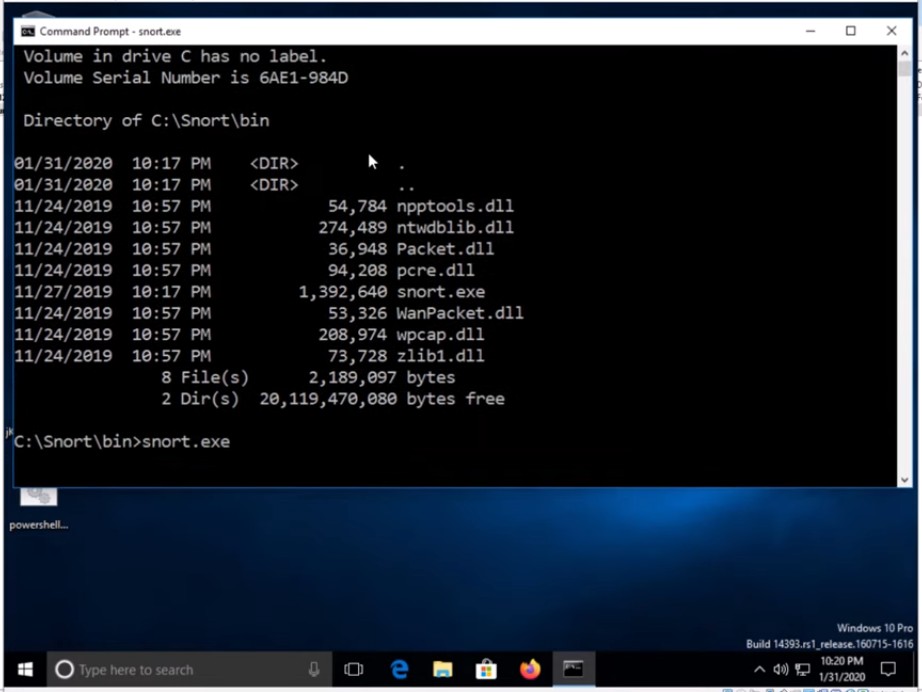
Run the command

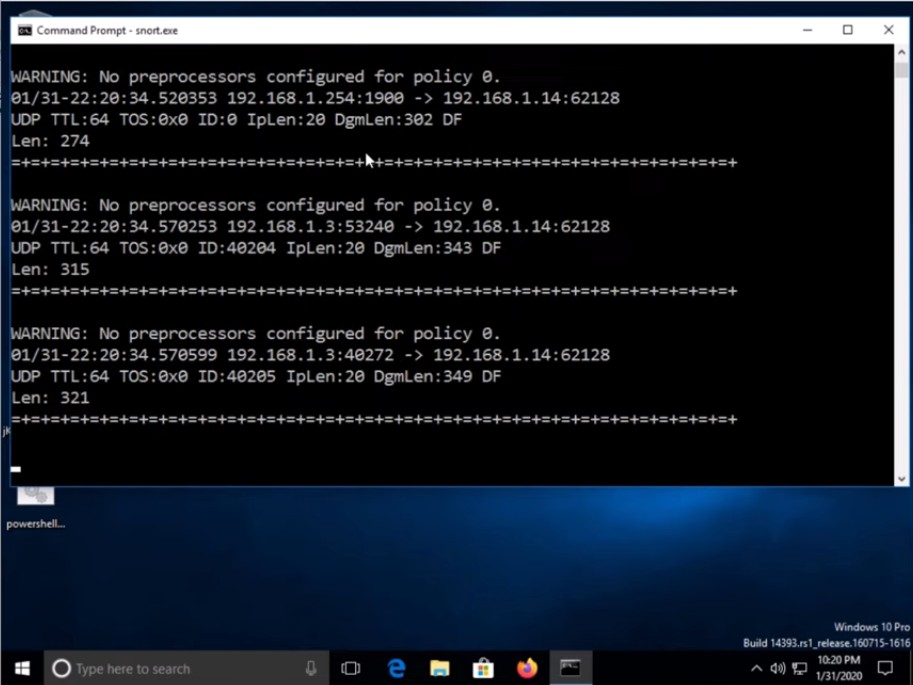
Snort –i 1 –c c:\Snort\etc\snort.conf -T





to command prompt and check whether it is working or not.





It is successfully working.

Conclusion :

The installation and the demonstration of the snort is successfully done.