Experiment No. 8

**Aim**: To install Intrusion Detection System (SNORT) and study the logs.

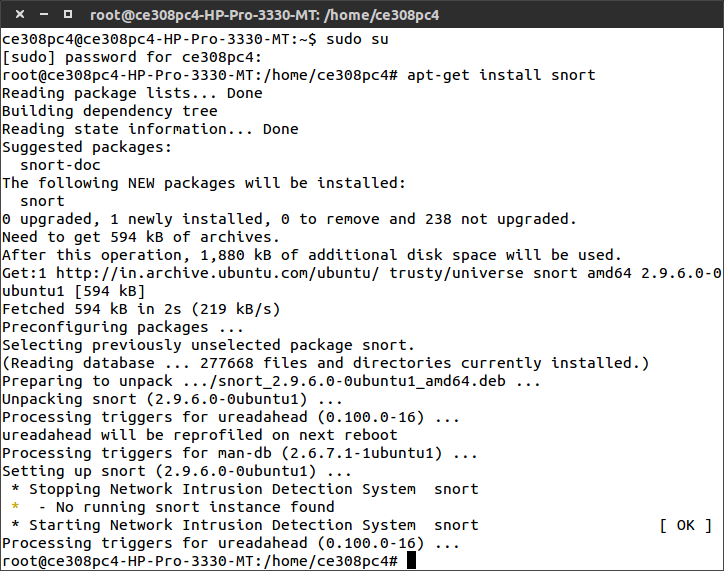
**Theory**:

An *Intrusion Detection System* (IDS) is a device or software application that monitors a network or systems for malicious activity or policy violations. Any detected activity or violation is typically reported to an administrator or collected centrally using Security Information and Event Management (SIEM). SIEM systems combines input from multiple sources, and uses the alarm filtering tech to distinguish malicious activity from false alarm. *SNORT* is an open source intrusion prevention system capable of real-time traffic analysis and packet logging.

**Commands:**

To install SNORT

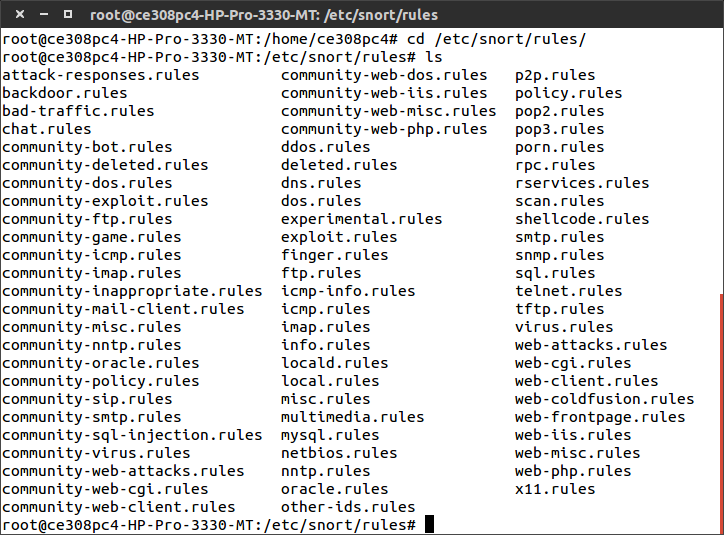
*sudo apt-get install snort*



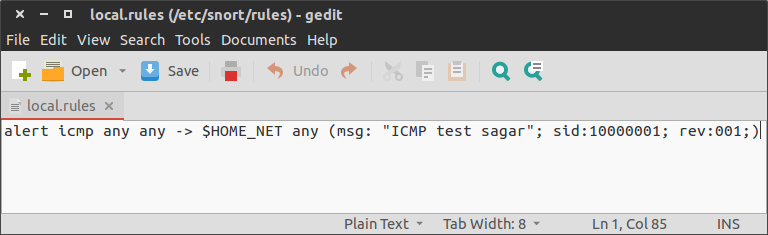
To create a new rule

*cd /etc/snort/rules*

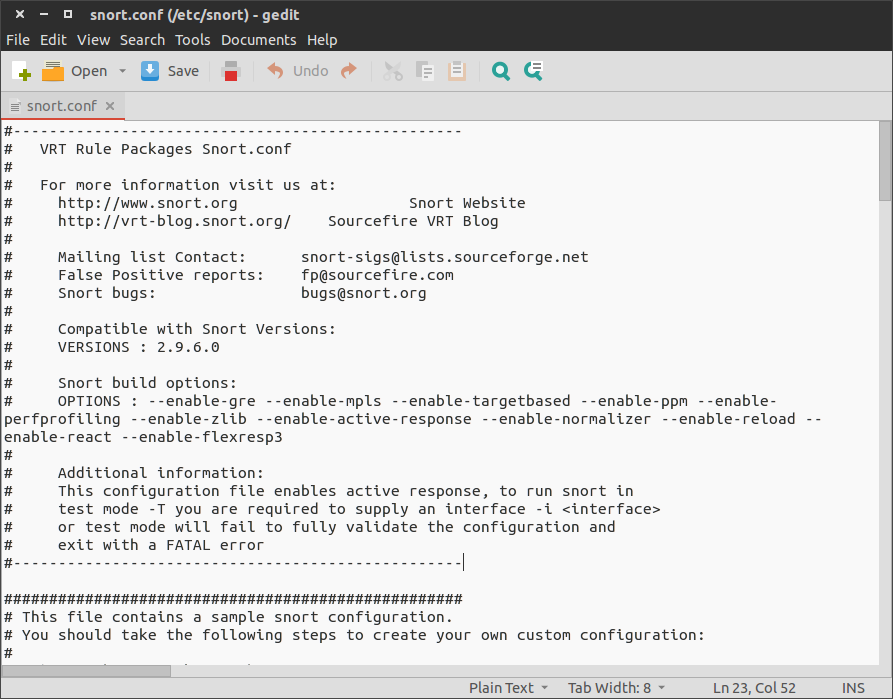
*ls*



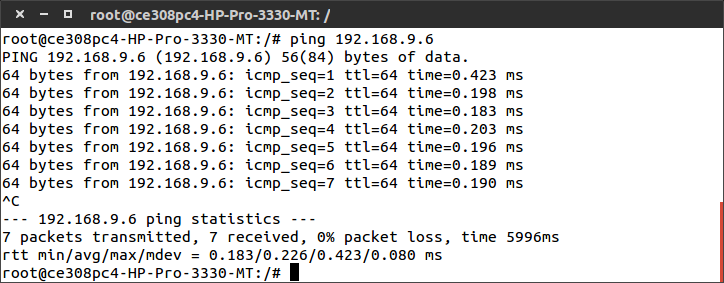
*sudo gedit local.rules*



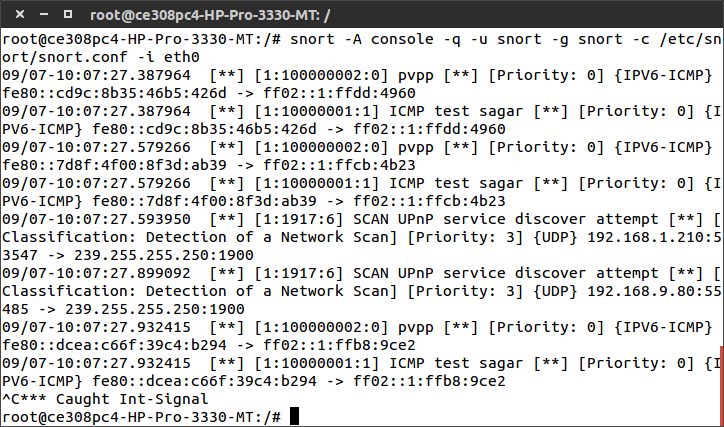
To open the config file

*sudo gedit snort.conf* 

*ping 192.168.9.6*



*snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i eth0*

******

***Conclusion***:

Hence SNORT is installed and its commands are studied and implemented.