

Simple IDS system with Snort – Small group assignment.

You will need to discuss with your tutor how to install and configure your IDS using Snort. Then you will have to read the snort manual and design the rules to do the following things. You are required to test your IDS to make sure the rules work properly.

1. Alert the system if there is any one trying to telnet to your system as super user.
2. Log the information if there is a telnet session from a particular IP address.
3. Alert the system and log the information if there is an ftp attempt with root from a particular machine.
4. Alert the system and log the information if there are attempts to ssh to your system from a particular network.
5. Alert the system and log the information if there are attempts to shut down your system remotely.