**Lab Assignment – 4**

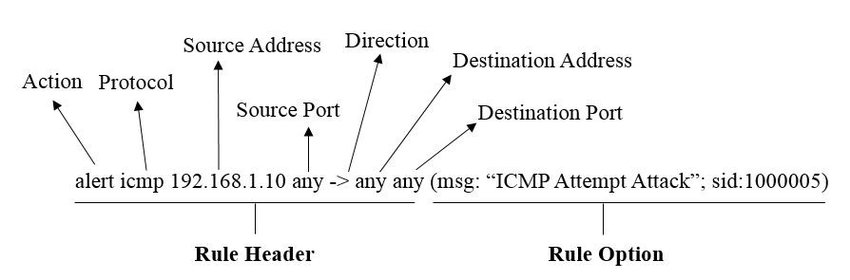
* **Snort**

Snort is an open-source network intrusion prevention and detection system (IDS/IPS) developed by Sourcefire. Combining the benefits of signature, protocol, and anomaly-based inspection, Snort is the most widely deployed IDS/IPS technology worldwide. With millions of downloads and nearly 400,000 registered users, Snort has become the de facto standard for IPS.

* **Snort Alert Modes**
* **Fast:** Snort alerts include the timestamp, sending an alert message, showing the source and destination IP addresses and ports. To implement this mode, use the ***-A fast***
* **Full:** Additionally, in the previously reported information in the fast mode, the full mode also prints the TTL, datagram length and packet headers, window size, ACK, and sequence number. To implement this mode, use the ***-A full***
* **Console:** It shows the real time alerts in the console. This mode is enabled with the ***-A console***
* **Cmg:** This mode is only useful for testing purposes.
* **Unsock:** This is used to export alerts to Unix sockets.
* **Syslog:** This mode (System Logging Protocol) instructs Snort to send a remote alert log. To run this mode, add ***-s***
* **None:** No alerts.
* **Running snort on fast mode**

sudo snort -A fast -c /etc/snort/snort.conf

* **Rule headers**
* alert – Rule action. Snort will generate an alert when the set condition is met.
* any – Source IP. Snort will look at all sources.
* any – Source port. Snort will look at all ports.
* -> – Direction. From source to destination.
* $HOME\_NET – Destination IP. We are using the HOME\_NET value from the snort.conf file.
* any – Destination port. Snort will look at all ports on the protected network.

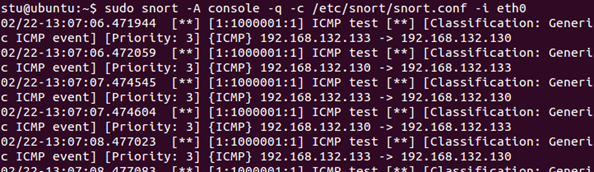


Snort rule

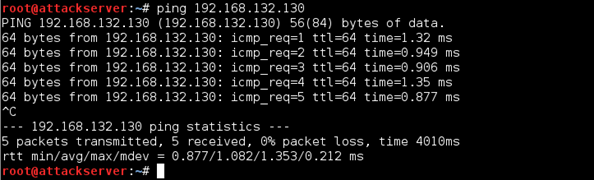
* **Analysing incoming packet**

alert icmp any any -> $HOME\_NET any (msg:”ICMP Test”; sid:1000001; rev:1)

1. sudo snort -A console -q -c /etc/snort/snort.conf -i eht0



1. ping 192.168.x.x



* **Analysing outgoing packet**

alert tcp 192.168.x.x any -> $HOME\_NET 21 (msg:”FTP connection attempt”; sid:1000002; rev:1)

1. sudo snort -A console -q -c /etc/snort/snort.conf -i eht0 -K ascii



1. ftp 192.168.x.x

