Date / /
Page No.

ASSIGNMENT 4

Aim: To study, install and configure SNORT

Theory:

Snort is an intrusion detection system written by Martin Roesch. Snort is a lightweight network intrusion detection system, capable of performing real-time traffic analysis and packet logging on IP networks.

It can perform protocol analysis, content searching/matching and can be used to detect a variety of attacks and probes, such as buffer overflows, stealth port scans, CGI attacks, SMB probes, OS fingerprinting attempts and much more.

Snort uses a flexible rules language to describe traffic that it should collect or pass, as well as a detection engine that utilises a modular plugin architecture.

Snort can be configured to run in three modes:

1) Sniffer mode, which simply reads the packets off of the network and displays them for you in a continuous stream on the console.

2) Packet logger mode, which logs packets to disk

3) Network Intrusion Detection system mode, the most complex and configurable configuration, which allows Snort to analyse network traffic for matches against a user-defined rule set and performs several actions based upon what it sees.

4) Inlie mode, which obtains packets from iptables instead of from libpcap and then causes iptables or pass packets based on Snort rules that use inlie specific rule types.

Conclusion: SNORT tool was implemented, installed and configured successfully.