Abstract

The attacks on computer networks are not a new deal. In general except for financial institutions and military or intelligence organizations nobody bothers about it. But in recent times it is being observing that it effects much more than the said calculations. Assuming that somebody (attacker) blocked the access of particular seller’s website at peak times then it results that his customer would like to choose another seller’s website whose outcome may result to tremendous loss of permanent seller. Likewise, there are many instances where the impact on network attacks has been observed from top notch to common people. Snort has emerged as a powerful solution to those organizations that could not spent much on purchasing licensed intrusion detection and prevention system as snort is free ware. This paper is aiding to popularize the techniques that can help everybody to identify and prevent from these attacks. The discussed medium in this paper is SNORT, an open source and powerful network intrusion detection and prevention tool.
The Implementation and Assessment of Snort Capabilities


Index Terms

Computer Science

Security
Keywords

Snort, Libcap, swatch, sendmail, packet logging