Snort IDS system visualization interface

Nadja Gavrilovic, Vladimir Ciric, Nikola Lozo
University of Nis, Faculty of Electronic Engineering, Nis, Serbia

***Abstract*—Over the past decades, the rapid Internet development and the growth in the number of its users have raised various security issues. Despite numerous available security tools, the exchange of data over the Internet is becoming increasingly insecure. For this reason, it is of great importance to ensure the security of the network in order to enable the safe exchange of confidential data, as well as their integrity. One of the most important components of network attack detection is an Intrusion Detection System (IDS). Snort IDS is a widely used intrusion detection system, which logs alerts after detecting potentially dangerous network packets. The next step in successful network protection is the analysis of logged alerts in search of deviations from normal traffic that may indicate an intrusion. The goal of this paper is to design and implement a visualization interface that graphically presents alerts generated by Snort IDS, classifies them according to the most important attack parameters, and allows the users to easily detect possible traffic irregularities. An environment in which the system has been tested in real-time is described, and the results of attack detection and classification are given. One of the detected attacks is analyzed in detail, as well as the method of its detection and its possible consequences.**

***Index Terms*—IDS, snort, network intrusion detection, visualization interface**

Nadja Gavrilovic is with the Faculty of Electronic Engineering, University of Nis, Aleksandra Medvedeva 14, Nis, Serbia (e-mail:nadja.gavrilovic@elfak.ni.ac.rs).

Vladimir Ciric is with the Faculty of Electronic Engineering, University of Nis, Aleksandra Medvedeva 14, Nis, Serbia (e-mail:vladimir.ciric@elfak.ni.ac.rs).

Nikola Lozo is with the Faculty of Electronic Engineering, University of Nis, Aleksandra Medvedeva 14, Nis, Serbia (e-mail:nikolalozo@elfak.rs).