Abstract

This paper illustrates the functionality of Wireshark as a sniffing tool in networks. This has been proven by an experimental setup which depicts the efficiency of detection of a malicious packet in any network. Testing has been achieved through experimentation on a real-time network analyzed by Wireshark. Inferences have been made which clearly depict Wireshark’s capabilities highlighting it as a strong candidate for future development into a robust intrusion detection system. This paper highlights the working of Wireshark as a network protocol analyzer and also accentuates its flexibility as an open source utility to allow developers to add possible functionalities of intrusion detection devices in it.

Reference
Evaluation of the Capabilities of WireShark as a tool for Intrusion Detection


Index Terms

Computer Science Security
Key words

Data

Intrusion Detection

Sniffing

WireShark