Analysis of Snort Rules to Prevent Synflood Attacks on Network Security

Volume 178
Number 40
Year of Publication: 2019

Authors:
Karmadenur, Raka Yusuf

Abstract

Snort rules are a form of the database whose attack pattern is applied to a Snort server to filter out the types of attacks, so that the type of attack detected can be isolated, the Snort rule database must be updated so that if there are new types of attack patterns it can be found by Snort rules. This analysis will provide input to update regularly so that if a new type of attack is detected and can be detected. Snort rules to prevent SYN Flood attacks, the type of denial of service that has been formulated using loopholes when connecting to TCP / IP is done. In network security analysis it is very important to formulate an attack pattern that will attack the network so that it can be overcome by Snort rules. Maintaining a secure network from interference can be overcome by Snort rules. Analysis of Snort's rules is to prevent SYN Flood attacks on network security and makes it easier for administrators to report the types of attacks that enter Snort rules and make it easier to make policies improve based on the logs in Snort rules.

References


Index Terms

Computer Science

Security

Keywords

Snort Rules, SYN Flood attack, Option Rules, DDoS