10-1-2016

Active snort rules and the needs for computing resources: Computing resources needed to activate different numbers of snort rules

Chad A. Arney
Michigan Technological University

Xinli Wang
Michigan Technological University

Follow this and additional works at: https://digitalcommons.mtu.edu/technology-p

Part of the Databases and Information Systems Commons, and the Information Security Commons

Recommended Citation
http://dx.doi.org/10.1145/2978178.2978189
Retrieved from: https://digitalcommons.mtu.edu/technology-p/1

Follow this and additional works at: https://digitalcommons.mtu.edu/technology-p

Part of the Databases and Information Systems Commons, and the Information Security Commons
Active Snort Rules and the Needs for Computing Resources

– Computing Resources Needed to Activate Different Numbers of Snort Rules

Chad A. Arney
Michigan Technological University
Houghton, MI 49931, USA
carney@mtu.edu

Xinli Wang
Michigan Technological University
Houghton, MI 49931, USA
xinlwang@mtu.edu

ABSTRACT

This project was designed to discover the relationship between the number of enabled rules maintained by Snort and the amount of computing resources necessary to operate this intrusion detection system (IDS) as a sensor. A physical environment was set up to loosely simulate a network and an IDS sensor monitoring it.

The experiment was conducted in five trials. A different number of Snort rules was enabled in each trial and the corresponding utilization of computing resources was measured. Remarkable variation and a clear trend of CPU usage were observed in the experiment.

Categories and Subject Descriptors

H.3.4 [Information Systems]: Systems and Software—Performance evaluation

Keywords

Snort; Rule Set; Performance; Utilization of Computer Resources; Tuning

EXECUTIVE SUMMARY

A physical network was set up with two computers to discover the relationship between the number of active rules loaded by Snort and the amount of computing resource that is needed for its operation. One computer (Host A) ran Security Onion Linux providing Snort of version 2.9.8.0. The other (Host B) ran Kali Linux of version 2016.1 to simulate an attacker. The sysstat software tool was used to measure resource utilization by Snort on Host A. Five trials were designed for our experiment. Groups of rules were disabled by categories to achieve the desired number of enabled rules for each trial.

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).

Acknowledgment

The work is supported by the National Science Foundation (NSF) TUES grant award#: 1140308.