Prof. Dr.-Ing. habil. Falko Dressler
Data Communications and Networking – TKN

Technische Universität Berlin

Bachelor's Thesis

Speeding-up Snort with Traffic Classification

A firewall is well-known as the first layer of defense for your network. However, intruders are developing new techniques every day to bypass the firewall and gain access to the network. Following, researchers introduce Intrusion Detection System (IDS) as a new layer of defense after the firewall to make the intruders' life more painful than ever.

The current volume of network traffic is on a scale that is exceeding the processing capacity of an IDS developed based on the most accurate approach (Deep Packet Inspection(DPI)). A DPI-based IDS is equipped with a list of different attack patterns and IDS checks each received traffic to identify the presence of any pattern exhaustively. Despite the accuracy of this workflow, it demands high processing capability. The volume of the traffic and the number of patterns which should be chek are the main players that put pressure on the processor.
We can optimize the processing consumption of an IDS via splitting the traffic into different categories and limit the pattern checking process just to the related patterns. In this way, a considerable number of unnecessary pattern chacking processes will be eliminated. Consequently, IDS can detect any intrusion faster than before.

Goals of the Thesis

You, as a well-prepared engineer, are in charge of designing a system that classifies network traffic according to their application protocol and then enforces an IDS to look for the attack patterns relevant to the protocol. in your journey, the following tools will help you:

- ***Libprotoident*** [1] is an open-source C library that classifies the network traffic according to its application protocol.
- ***Snort***[2] is an open-source network Intrusion Detection System

You need C and Python programming language knowledge for modifying the tools according to your desire and working with datasets in you way. Of course, you will not be alone in your journey and your supervisor will guide you to take each step and will keep a close eye on you to correct any deviation toward the goal. In the end, you will finish your journey by defencing your thesis and introduce yourself to the academic community with (a) valuable publication(s). Besides, you will have a repository to maintain that host a precious tool to protect the online activity of thousands of people. Please do not hesitate to contact me for more explanation about this project.

Keywords

Network Security, Network Traffic Classification, Intrusion Detection System

[1] https://wand.net.nz/trac/libprotoident
[2] https://www.snort.org/

Contact:
Hossein Doroud: <h.doroud@tu-berlin.de>
Website:
www.tkn.tu-berlin.de