Security Tools as a Service

Petr Velan
CESNET, a.l.e.
Zikova 4, Prague

petr.velan@cesnet.cz

Keywords. network, security, tools, detection, monitoring

Abstract

The amount of network based attacks against services and end-users is gradually increasing. Although strict security policies, timely patches, and good antivirus software can mitigate most of the attacks, no system is perfectly secure. Network monitoring and analysis provides tools detect both successful and failed attacks as well as a presence of compromised systems. However, deployment of a network monitoring and analysis system is a complex task that is beyond the capabilities of most users and difficult even for seasoned administrators. For this reason, we have created a *Security Tools as a Service* (STaaS) appliance which provides a network monitoring and analysis system that is easy to deploy and maintain. The STaaS automates the deployment of multiple tools for network monitoring and analysis that were created at CESNET and are already used to monitor attacks at the CESNET2 network.

The data source for STaaS is flow data in IPFIX or NetFlow format. The flow data can be exported by networking devices such as routers and switches. Software flow exporters are available for advanced home appliances such as Turris of MikroTik routers. STaaS has two primary functions: it is a fully equipped flow data collector and automated flow data analysis tool. As a flow collector, the STaaS provides tools for flow data collection, storage, and querying. Therefore, it can be used to retain records of network traffic, which is convenient for investigation of detected breaches. As a flow data analysis tool, the STaaS runs a complex system of modules that allow detection and reporting of various security incidents, such as brute force detections, port scans, communication with suspicious domains or IP addresses, or VoIP misuse. The details about detected incidents are stored for inspection and easy access to relevant flow data helps the administrator to speed up the investigation. It is also possible to collaborate with other organisations and share the detected incidents using Warden information sharing system.

The STaaS is deployed using Ansible automation and is capable of running in a virtual machine with as little as 2 GB of memory and a single CPU core. The disk space requirements depend on the desired flow data history and the size of the monitored network. Custom configuration of the STaaS appliance is separated from the deployment scripts, therefore it is as easy to maintain multiple STaaS appliances as it is to maintain a single one. Monitoring of the deployed STaaS instances is ensured by Nagios and Munin systems which provide the administrators with real-time event notifications as well as a history of service states. The STaaS is available for public use at its Github repository[1].

Acknowledgment

This work was supported by the "CESNET E-Infrastructure" (LM2015042) funded by the Ministry of Education, Youth and Sports of the Czech Republic.

[1] https://github.com/CESNET/STaaS