Suricata intrusion detection and prevention system and its comparative analysis

Oleshko Inna[1]

Rykov Oleksandr[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave,
Kharkiv UA-61166, Ukraine,inna.oleshko@nure.ua

[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave,
Kharkiv UA-61166, Ukraine,oleksandr.rykov@nure.ua

Abstract. *The article is written about multitasking protecting program that helps users detecting intruders. It deals with application and shows how people can use this app to prevent stealing of their data. It was shown, that the Suricata program is one of the most popular and fast protector.*

Keywords: *administrator, traffic, network attack, Suricata, IDS, IPS, Snort.*

I. INTRODUCTION and Problem statement

Cyberattacks are one of the main problems faced by actors with information resources. Well-known antivirus programs and firewalls are only effective in protecting obvious access points to networks. However, attackers are able to find ways to bypass and vulnerable services even in the most advanced security systems. In today's world, Intrusion detection system / Intrusion prevention system (IDS / IPS) is a necessary element of protection against network attacks. The main task of these systems is to identify the facts of unauthorized access to the corporate network or unauthorized management of it, with the implementation of appropriate countermeasures (informing the administrators of the fact of intrusion, breaking the connection or re-configuring the firewall to block further actions of the attacker, etc.).

There are many intrusion detection and prevention systems. The urgent task is to choose one of them. The paper provides a comparative analysis of intrusion detection systems and concludes that Suricata is a faster and more reliable attack detector.

II. IDS / IPS- SYSTEMS

IDS / IPS systems are unique tools designed to protect networks from unauthorized access. They are hardware or software capable of promptly detecting and effectively preventing invasion. Measures taken to achieve the key IDS / IPS goals include informing security professionals about the facts of hacking and malware attacks, breaking off malicious connections, and re-configuring a firewall to block access to corporate data.

All intrusion detection and prevention systems that exist today are united by several common features, functions and tasks that can be solved by information security professionals. Such tools, in fact, perform continuous analysis of the exploitation of certain resources and identify any signs of atypical events.

Corporate network security can be based on several technologies that differ in the types of incidents detected and methods. In addition to the functions of continuous monitoring and analysis of what is happening, IDS systems perform the following functions:

- Collection and recording ofinformation;
- Alerts to network administrators of changes that have occured;
- Create reports for log summaries.

IPS systems can be considered as an extension of IDS, since the task of tracking attacks remains the same. In addition to the above, IPS technology can not only identify the threat and its source, but also block them. This speaks to the advanced functionality of such a solution. It is able to perform the following actions:

- Break off harmful sessions and prevent accessto critical resources;
- Change the configuration of the protection environment;
- Take action on attack tools (for example? Delete infected tools).

It is worth noting that the UTM firewall and any modern intrusion detection and prevention systems are the optimal combination of IDS and IPS technologies.

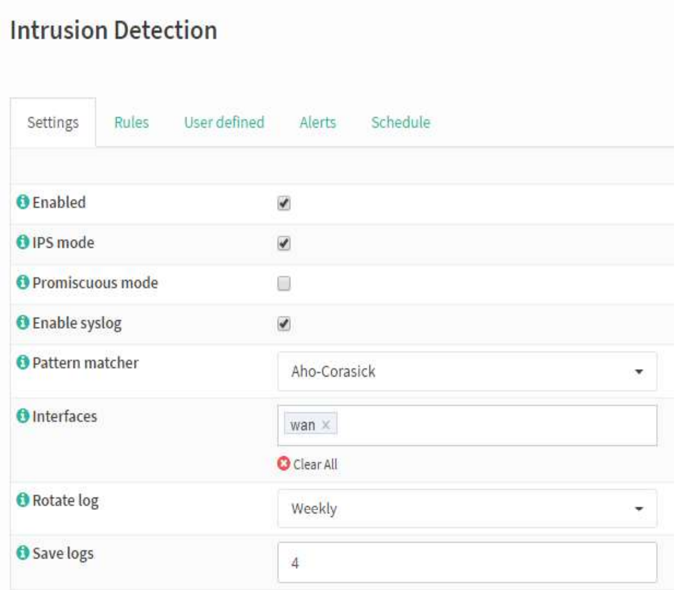
III. SURICATA ATTACK DETECTORS

Одним One of IPS's intrusion prevention solutions is attack detectors that are designed to detect a variety of malicious threats in a timely manner. In Internet Control Servers, they are implemented as a Suricata system, a multi-tasking and productive tool designed to protect networks, as well as collect and store information about any incoming signals. The work of the attack detector is based on the analysis of signatures and heuristics, and its convenience is due to the presence of open access to the source code. This approach allows you to customize the system performance for individual tasks.

The customizable Suricata settings include: rules that will be subject to traffic analysis, filters that limit the output of an admin alert, address ranges of different servers, active ports, and networks.

Thus, Suricata, as an IDS / IPS solution, is a fairly flexible tool that is subject to change depending on the nature of the attack, making it as effective as possible. Information and communication systems capture and store information about suspicious activity.

In the Suricata settings tab (Fig. 1) you can edit the settings of the attack detector. You can specify internal, external networks, address ranges of different servers, as well as the ports used. All of these variables are assigned a default value that the attack detector can correctly launch. By default, traffic to external interfaces is analyzed.



Intrusion Detection

Settings | Rules | User defined | Alerts | Schedule

Enabled ☑

IPS mode ☑

Promiscuous mode □

Enable syslog ☑

Pattern matcher: Aho-Corasick

Interfaces: wan ×

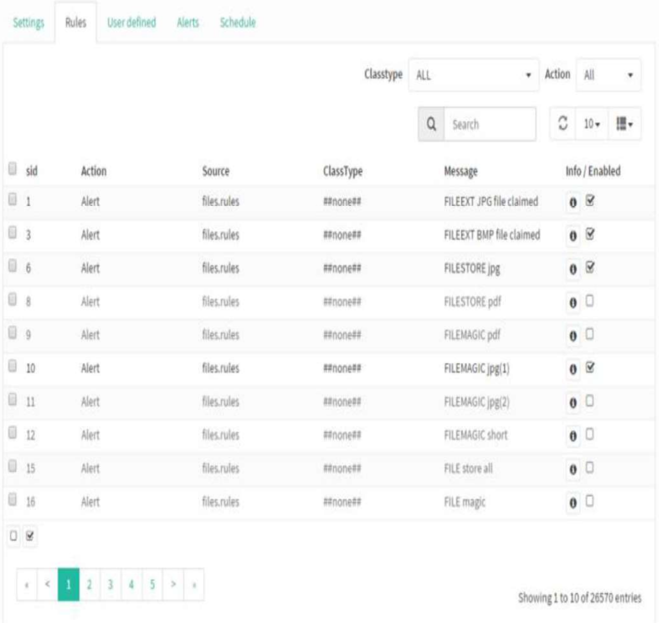
Clear All

Rotate log: Weekly

Save logs: 4

Figure 1. Suricata settings

Suricata Attack Detector can be connected to the rules by which it will analyze traffic. On the tab in Fig. 2, you can see the presence and contents of a rule file, and enable or disable its action (using the checkboxes to the right). In the upper right corner is a search by name or by the number of rules in the file.



Settings | Rules | User defined | Alerts | Schedule

Classtype: ALL   Action: All

Search   10

□ sid	Action	Source	ClassType	Message	Info / Enabled
□ 1	Alert	files.rules	##none##	FILEEXT JPG file claimed	☑
□ 3	Alert	files.rules	##none##	FILEEXT BMP file claimed	☑
□ 6	Alert	files.rules	##none##	FILESTORE jpg	☑
□ 8	Alert	files.rules	##none##	FILESTORE pdf	□
□ 9	Alert	files.rules	##none##	FILEMAGIC pdf	□
□ 10	Alert	files.rules	##none##	FILEMAGIC jpg(1)	☑
□ 11	Alert	files.rules	##none##	FILEMAGIC jpg(2)	□
□ 12	Alert	files.rules	##none##	FILEMAGIC short	□
□ 15	Alert	files.rules	##none##	FILE store all	□
□ 16	Alert	files.rules	##none##	FILE magic	□

« < 1 2 3 4 5 > »

Showing 1 to 10 of 26570 entries

Figure 2. Suricata rules

IV. Comparative analysis Suricata ta Snort systems

Snort is an IPS (Intrusion Prevention System) system for the network intrusion analysis. The software analyzes all traffic through the firewall searching for known attacks and anomalies. This program is free, open source GPL software and it is the most common IDS (and eventually IPS) in the world, thanks in large part to its openness and the work of authors.

More than 250 unit tests were conducted for Suricata and Snort systems. The test results are shown in Table 1.

The tests were conducted on 14 malware and viruses. As we can see from the table, Suricata has a better detection rate for malware and viruses than Snort.

On a set of 12 shells (virus hidden in another file), Suricata detected 12 shellcodes and Snort detected 7 shellcodes. In a set of 3 tests, both Suricata and Snort detected 3 DoS attacks against SSH and MSSQL. Tests have shown that Suricata is better than Snort for detecting client-side attacks. Out of 257 tests Suricata detected 157 attacks.

Table 1. Test results

Test group	Number of tests	Suricata score	Snort Score
Bad traffic	4	1	1
Broken packages	2	1	3
Malware	14	9	7
Denial of service (DoS)	3	3	3
Attacks from the client	257	157	127
Shells	12	12	7
Productivity	0	2	1
Total	297	185	149

V. Conclusions

Based on the above analysis, we conclude that Suricata Attack Detector is a fast and reliable system that maximizes the use of modern processors and GPUs. Tests have shown that Suricata is better than Snort for detecting client-side attacks and has better detection rate for malware and viruses than Snort. The disadvantage of Suricata can be considered a large number of settings and not enough detail in some issues documentation.

References

[1] Anderson, James P., "Computer Security Threat Monitoring and Surveillance, " Washing, PA, James P. Anderson Co., 1980.

[2] Electronic resource https://oisf.net (date of appeal 20.10.2019)

[3] Electronic resource https://suricata-ids.org (date of appeal 20.10.2019)

[4] Electronic resource https://xserver.a-real.ru (date of appeal 25.02.2020)

[5] Electronic resource http://docs.nethserver.org(date of appeal 25.02.2020)

[6] Electronic resource https://cybrary.it (date of appeal 25.02.2020)