Problems of the detection systems usage and preventing intrusion into container environments

Misnik Oleksii

Pukhov Institute for Modelling in Energy Engineering, 15 General Naumov Str., Kyiv UA-03164, Ukraine, alexmisnik91@gmail.com

Abstract. *All the means of safety of the container environments are analyzed. There are generalized practical problems of using intrusion detection and prevention software, isolated application launch. Among them is emphasised functionality of this software. Emphasis is placed on the difficulties of implementing the privileged function. These difficulties lead to a decrease in the efficiency of its usage and, as a consequence, to the safety of container environments.*

Keywords: *container, container security, intrusion prevention system, intrusion detection system, docker.*

I. Introduction and Problem statement

Every year there is a growth of the information technology market. This determines the ways of developing container environments. While one of the important aspects of their usage is security. In particular, with the help of intrusion detection and prevention software, for example [1-2]: Snort, Suricata, Bro, Ossec, Prelude. The practical application of this software is limited by the difficulty of adapting their settings to ensure the safety of container environments. The following restriction also applies to isolated launch of applications, such as [3]: Seccomp, Apparmor, Selinux.

On the one hand, it is important to ensure the security of container environments by using intrusion detection and prevention software; isolated application launch. On the other hand, in practice it is easier said than done.

II. Problem solution and Results

The security of container environments through the usage of intrusion detection and prevention software involves the following issues:

- the similarity of models of information collection systems with each other and their disadvantages;
- the presence of a large number of false positive results in the detection of intrusions;
- software architecture limitations to detect and prevent intrusion while using in container environments [4];
- lack of effective means of automated analysis and visualization of information about incidents of information security;
- low efficiency and limited usage of software to detect and prevent intrusion in a container environment [5];
- the complexity of automated isolation of intrusion features by detection software [6].

Among them, one of the most significant problems is the limited software architecture for detecting and preventing intrusion in container environments [7]. As a consequence, their efficiency and safety in the container environment is reduced.

III. Conclusions

Therefore, the usage of intrusion detection and prevention software, isolated application launches for security in container environments is complicated to do in practice because of different architectural features. First of all, this is due to their limited functionality, in particular, when using the privileged function. Restrictions lead to a decrease in the efficiency of the specified software and, as a consequence, the difficulty of ensuring the security of container environments.

References

[1] T.I. Zorina, "Detection and prevention of attacks in computer networks" VISNIK OF THE VOLODYMYR DAHL EAST UKRAINIAN NATIONAL UNIVERSITY, Volodymyr Dahl East Ukrainian National University, No. 83, 2013, pp. 48-52

[2] Tereykovsky I., Korchenko A., Parashchuk T., Pedchenko Y., "Open intrusion detection systems analysis", Ukrainian Scientific Journal of Information Security,vol. 24, No. 3, 2018, pp. 201-216

[3] M.A. Kachanov, D.N. Kolegov, "Security analysis of the information flows by memory in the computer systems with functional and parametric associated entities", Mathematical Foundations of Computer Security, Tomsk State University, No. 2, 2008, pp. 76-80.

[4] A.S. Vishnyakov, A.E. Makarov, “Implementation of an external threat detection system in cloud computing”, Scientific journal, 2019

[5] Bondyakov Aleksey Sergeevich, "The basic modes of the intrusion prevention system (ids/ips suricata) for the computing cluster", International Scientific Journal "Modern Information Technology and IT-education", vol. 13, No. 3, 2017, p. 31-37

[6] O.I. Misnik, M.V. Antonishin, and V.V. Turcan, “Quality analysis web application vulnerability scanners”, Modeling and Information Technologies, No. 83, 2018, pp. 77-86.

[7] OWASP Docker-Security. [Online]. Available: https://github.com/OWASP/Docker-Security