METHODOLOGICAL APPROACHES TO THE SECURITY OF VIRTUAL AND PHYSICAL SERVERS BASED ON OS LINUX

Anatolie Cerbu, Dorin Grechin
Technical University of Moldova, Mivocloud International SRL, Chişinău, Republic of Moldova
anatol.cerbu@tse.utm.md,workingcode4@gmail.com

Information security has become a topic of growing interest not only in the Linux community, but in all areas of information technology.

As the Internet develops, there is an increase of number of Linux servers, as well as Linux vulnerabilities that are made public. A Linux user has a wide variety of tools and techniques to protect against most types of intrusions. Unfortunately, there is no a secure system. Nevertheless, by improving network security measures as well as their proper implementation, the system has become a more difficult target to break its security.

Linux [1] has a series of features:

- Flexibility: Linux is flexible because it supports high-performance server applications, desktop applications, and embedded systems.

- Stability: In the Linux system, if a new program or software is installed, it does not require periodic restart. therefore, it maintains the performance level of the system.

- Performance: does not degrade the performance level of the system, even if it manages a large number of users simultaneously.

- Network compliance: Linux is an easy-to-use operating system in terms of network functionality because it can be easily configured.

Server security requirements [1] fall into one of the following categories:

- Data confidentiality;
- Data integrity;
- User authentication and access control;
- Availability of data and services.

As the cost of maintaining effective security is constantly rising, server administrators have decided to migrate private infrastructure to Linux operating systems. In order to maintain effective security we cannot claim that the information is in the security of a perfect defensive system regardless of all its facilities, therefore the ability of any security configuration must include the adaptability of the infrastructure according to new attacks and stress-tests to reduce detected vulnerabilities.

References:

1. R. Blum, C. Bresnahan. *Linux Command Line and Shell Scripting BIBLE*, Wiley, 2015.