Design of an audit system for the control of systems and services in a computer network

Peter Simkovic[a,*]

[a] *Brno University of Technology, Faculty of Business and Management, Kolejní 2906/4, 612 00 Brno, Czech Republic*

Abstract

Purpose of the article The purpose was to develop appropriate tool based on detection and audit of computer network. Several conditions have been set to achieve the goal. One of the conditions was to make the tool portable and compatible as possible. Second condition was to use only free open-source programs, so the solution can be freely available for general public. The last condition was to make the tool easy to use, so no specialist would be needed to operate it. Summing up, the purpose is to find a way of developing free, easy to use and available solution to improve computer security.

Methodology/methods Risk analysis of the corporate environment was used to obtain basis for verifying existence of real risk operating due to absence of monitoring computer network. After evaluating findings of risk analysis, a further research of best practices in the field of IT security was necessary. Based on the results of analysis, an analytical tool was developed to provide an overview of potential vulnerabilities affecting the network and the equipment located within it.

Scientific aim Creating an easily portable scanning tool to identify vulnerabilities within a computer network. The output must be easy to read and process even for non-professional.

Findings There are many free open-source tools, that as individual programs each partially meet defined requirements. Containerisation is used to achieve portability and compatibility with different operating systems. Regarding of simplicity, it is accomplished by appropriate combination of available scanning program, and custom scripts.

Conclusions It is possible to develop tool, that meets all the conditions set to freely approximate security matters to general public. Use of the solution in practice also showed that even the network and equipment managed by an IT specialist, contains several vulnerabilities that can harm company, both financially and operationally.

Keywords: Computer network, Detection, Scanning, Security, Services, Ports, Container, Docker, Nmap, Virtualization

JEL Classification: M15, M21

[*] Corresponding author.
E-mail address: peter.simkovic9@gmail.com