DOI: https://doi.org/10.30837/csitic52021232178

# Software and Hardware Simulator of Company Security Audit

Illia Fedorov[1]

Gennady Khalimov[2]

[1]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: illia.fedorov@nure.ua

[2]Kharkiv National University of Radio Electronics, 14 Nauky Ave, Kharkiv UA-61166, Ukraine, e-mail: hennadii.khalimov@nure.ua

***Abstract**. To ensure the tasks of training professionals in the field of cybersecurity, a software and hardware complex has been created that provides training in various methods of protecting information and countering attacks. The possibilities of the complex are considered, as well as the experiments that were carried out during its development.*

***Keywords:** information security, incident, event, classic model, MDR model, mixed model, maturity level, security operations model, modeling of vulnerabilities, protection check*

## I. Introduction

Today, organizations are devoting more and more funds to the introduction of new technologies in digital transformation projects, which not only creates many new opportunities, but also leads to new vulnerabilities and threats. It is necessary to understand that without the trust of the user, such a transformation cannot be successful. Cybersecurity must become part of the corporate philosophy, and for this, at least, it should be integrated into the business development strategy [1].

In today's reality, the problem of information security is becoming more acute in everyday life, which is why cybersecurity experts have been and remain one of the most popular in any company.

## II. Problem Solution and Results

Ukraine's cybersecurity strategy envisages the development of cyber protection of state electronic information resources and information infrastructure designed for information processing, cyber protection of critical infrastructure, development of security and defense sector potential in the field of cybersecurity, fight against cybercriminals.

Training of qualified cybersecurity specialists is important in the development of certain tasks. To achieve this goal, it is proposed to create a software and hardware complex for modeling systems for various functional purposes, configured for a given, specific operating systems and configurations. The purpose of this complex is to create a simulator for modeling and assessing the security of cybersecurity objects: communication systems used in the field of e-government, e-government services, e-commerce, e-document management.

The offered software and hardware complex is built on Raspberry Pi 4 and orange Pi One microcomputers, Mikrotik router and Mikrotik candle. The block diagram of the complex is presented in Figure 1. For modeling vulnerable operating systems, proprietary, specially vulnerable, distributions based on the Linux operating system have been developed, and a website, server and other applications are additionally placed on them.

The choice of the proposed scheme is determined by the ease of use, functional completeness, and relatively low cost.

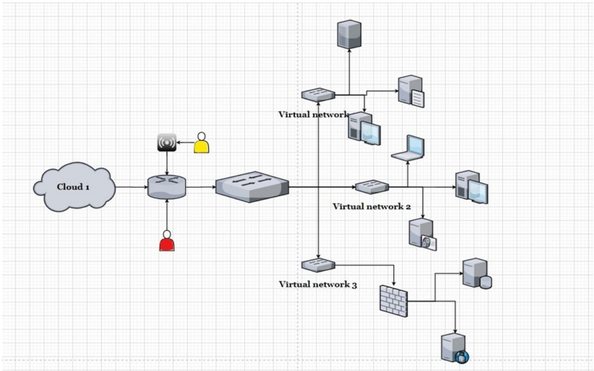

Figure 1 - General scheme of the complex

The functionality of the software and hardware complex allows:

- model modern systems and work out attacks using their vulnerabilities;
- track incidents in information systems;
- detect suspicious traffic on the network;
- build secure systems;
- model cybercrimes and organize the process of their investigation.

Currently, on the basis of this complex, you can work out several vulnerabilities, the most common in the information space [2]:

- testing databases using SQL injections;
- exploitation of the vulnerability in the PHP server (running malicious code in the image);
- use of the vulnerability in the plugin of the site, which changes the language of the site, and its further exploitation to obtain root rights;
- exploitation of the Eternal Blue vulnerability.
- exploitation of FTP vulnerabilities;
- search for passwords for SSH connections and root privileges;
- building a network of bots;
- testing DDoS attacks on simulated sites.

## III. Conclusion

Thus, due to the use of this complex it is possible to move away from virtualization in learning and move to the construction of real systems with the ability to build and test systems for their protection.

## REFERENCES

[1] Brill, Alan, Kristina Misheva, and Metodi Hadji-Janev, eds. Toward Effective Cyber Defense in Accordance with the Rules of Law. Vol. 149. IOS Press, 2020.

[2] Richard Stiennon. Cyber Defense: Countering Targeted Attacks. Rowman & Littlefield Pub Incorporated, 2012 – 192