Ministry of education of the Republic of Belarus
Educational Institution
Belarusian state university of informatics and radioelectronics

UDK 004.056

Momoh Angelo Osivue

The method of attack detection in corporative network

AVTOREFERAT

for the degree of master of science

on a speciality 1-98 80 01 «Methods and systems of information protection, information security»

_____

Scientific supervisor

T.V. Borbotko

Doctor of science, professor

_____

Minsk 2017

INTRODUCTION

At present, computer networks constitute the core component of information technology infrastructures in areas such as power grids, financial data systems, and emergency communication systems. Protection of these networks from malicious intrusions is critical to the economy and security of our nation. Vulnerabilities are regularly discovered in software applications which are exploited to stage cyber attacks. Currently, management of security risk of an enterprise network is more an art than a science. System administrators operate by instinct and experience rather than relying on objective metrics to guide and justify decision making. In this report, we develop models and metrics that can be used to objectively assess the security risk in an enterprise network, and techniques on how to use such metrics to guide decision making in cyber defense. To improve the security of enterprise networks, it is necessary to measure the amount of security provided by different network configurations. The objective of our research was to develop a standard model for measuring security of computer networks. A standard model will enable us to answer questions such as “Are we more secure than yesterday?” or “How does the security of one network configuration compare with another?” Also, having a standard model to measure network security will bring together users, vendors, and researchers to evaluate methodologies and products for network security.

GENERAL DESCRIPTION OF THE WORK

Communication of operation with large scientific programs (designs) and themes

The theme of dissertational work matches to subsection 13 «Safety of the person, a society, the state» the priority directions of scientific researches of Byelorussia for 2016-2020, confirmed by the Decision of Ministerial council of Byelorussia on March, 12th, 2015, № 190. Work was carried out in formation establishment «Belarusian state university of informatics and radioelectronics».

The purpose and research problems

The work purpose is working out of actions for protection of corporate networks against attacks. For object in view reaching it was necessary to carry out following tasks:

1. To analyze typical attacks in corporate networks, methods and means of counteraction to it.

2. To develop actions for protection of corporate networks from attacks.

The personal contribution of the competitor

All basic results stated in dissertational work, are gained by the competitor independently. In common published works to the author belong: definition of the purposes and statement of research problems, sampling of methods of research, direct participation in their conducting, and also machining, the analysis and interpretation of the gained results, the formulation of leading-outs.

Approbation of effects of the dissertation

Substantive provisions and effects of the dissertation were discussed at XV Belarus-Russian scientific and technical conference "Hardware components of protection of the information" (Minsk, 2017).

Publications on a dissertation theme

By results of the examinations presented to the dissertations, 1 operation, including 1 paper in collectors of materials of conferences are published.

THE BASIC CONTENT OF WORK

In **Introduction** the substantiation of an urgency of operation is resulted.

Chapter 1 the analysis of security of corporate networks from attacks is made. Problems of decrease in risks are considered at attacks to information systems. The description of a typical corporate network and services with which it provides is resulted. Objects in, a part of corporate networks which are subject to protection are considered. Examples of typical threats of information safety for corporate networks are resulted.

The **second chapter** is devoted a problem of counteraction to attacks. Here questions of realization of such typical attacks as denial of service are in detail considered. The special attention is given modern harmful programs, including data carrying out enciphering, and as providing their interception. Typical approaches in counteraction to similar threats are considered

In the **third chapter** results of system engineering of counteraction to attacks based on signature methods of detection of attacks are resulted. For protection of corporate networks it is offered to use system of detection of intrusions. Requirements to signatures by typical kinds of attacks which are considered chapter 2 are formulated. For monitoring of a corporate network it is offered to use honeypot. Practical recommendations about protection of corporate networks from attacks are formulated.

In the **Conclusion** the main results of the thesis are formulated.

CONCLUSION

Cybersecurity is a never-ending battle. A permanently decisive solution to the problem will not be found in the foreseeable future. For the most part, cybersecurity problems result from the inherent nature of information technology (IT), the complexity of information technology systems, and human fallibility in making judgments about what actions and information are safe or unsafe from a cybersecurity perspective, especially when such actions and information are highly complex. None of these factors is likely to change in the foreseeable future, and thus there are no silver bullets or even combinations of silver bullets that can "solve the problem" permanently.

In addition, threats to cybersecurity evolve. As new defenses emerge to stop older threats, intruders adapt by developing new tools and techniques to compromise security. As information technology becomes more ubiquitously integrated into society, the incentives to compromise the security of deployed IT systems grow. As innovation produces new information technology applications, new venues for criminals, terrorists, and other hostile parties also emerge, along with new vulnerabilities that malevolent actors can exploit. That there are ever-larger numbers of people with access to cyberspace multiplies the number of possible victims and also the number of potential malevolent actors.

Thus, enhancing the cybersecurity posture of a system and by extension, the organization in which it is embedded - must be understood as an ongoing process rather than something that can be done once and then forgotten. Adversaries especially at the high-end part of the threat spectrum constantly adapt and evolve their intrusion techniques, and the defender must adapt and evolve as well.

LIST OF PUBLICATIONS

1. Kahtan Hussein. Software solution for vulnerability detection / Kahtan Hussein, Momoh Angelo, A.I. Bukshtynova // Технические средства защиты информации : материалы XV Белорусскороссийской науч.-техн. конф., Минск – Нарочь, 6 июня 2017 г. / БГУИР ; редкол. : М.П.Батура [и др.]. – Минск, 2017. – С. 38.