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

UDK 004.056

Alaa Wahab

Audit security of information telecommunications networks to counter attacks

THESIS

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 2016

INTRODUCTION

Rapidly developing computer information technology are making significant changes in our lives. Actively developing Online trade, under intensive integration of local networks to the Internet. There are sites that contain critical resources, the cost of which sometimes exceed hundreds of times the cost of the system in which they are located.

Theoretically, the processes are possible only in a carefully designed and well protected environment. Modern methods of storage, processing and transmission of information contributed to the emergence of risks associated with possible loss, disclosure, modification of data, and other criminal acts. In most cases, non-secure protocols are used and potentially vulnerable software. For example, weak, or rather, the lack of on today's requirements, protection of basic TCP / IP protocols and existing operating systems.

The two main reasons for the success of network attacks the presence of "holes" in the software and error behavior of the operator of a computer system. But neither the one nor the other can not be guaranteed to eliminate. Using the latest updates of applications implies the possibility of introducing new errors and generally does not change the situation. In addition, along with the identification of "holes" there are many more undetected errors, and no one can argue that is completely safe.

According to the observations of third party experts, up to 90% of networks connected to the Internet, are vulnerable to such attacks.

The relevance and importance of the issue of information security due to the following factors:

- current levels and the pace of development of information security are far behind the level and pace of development of information technologies;
- a strong growth of personal computers used in various spheres of human activity (according to research company Gartner Dataquest currently the world's more than three billion personal computers);
- a sharp expansion of the range of users with immediate access to computing resources and data sets;
- the availability of computer equipment, and above all personal computers, has led to the spread of computer literacy in the general population;
- a significant increase in the volume of information collected, stored and processed by computers and other automation equipment (according to experts is currently about 85% of the company's intellectual capital is stored in digital form - databases, text files, tables);
- multiple vulnerabilities in software and network platforms;
- the rapid development of the global Internet, virtually preventing security

breaches of information processing systems worldwide. The shortage of IPv4 address space according to IANA, the organization, which currently has seven free networks of Class A (7 / 8s), will finally be distributed to all networks in March 2011. Regional Internet Registers (RIR) is agitating for the transition to a new version of the network layer protocol IPv6, the address space spanning thousands addresses.

Systems for detecting and preventing attacks are designed to protect a certain degree of reliability organizations and individuals from losses related to unauthorized access.

The use of traditional intrusion detection systems do not always reach the required level of true positives, and often skipped the event, or even a chain of events that have a weighty significance in identifying attempts of threats. Reduce the number of false positives, increase the accuracy of identification, to speed up the processing of traffic allows you to use in the process of intrusion detection data correlation of security events from various sources.

Therefore, the traditional method of detecting and countering attacks and techniques, which are based on the correlation data for information security in the information and communication systems and telecommunications networks in particular, should pay close attention.

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 purpose of dissertational work consists in working out of a program complex of imitation and detection of attacks for audit of the informational safety of networks of telecommunications.

For object in view achievement it was necessary to carry out following problems:

1. To analyze a problem of the informational security of modern telecommunication networks.

2. To develop the system simulating attacks and providing their detection.

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 XIII Belarus-Russian scientific and technical conference "Hardware components of protection of the information" (Minsk, 2015).

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 analysis of a modern state of affairs in the field of protection of networks of telecommunications against attacks is resulted and the urgency of the given problem is observed.

In chapter one. Security is one of the most important indicators of the efficiency of the telecommunications system, along with indicators such as reliability, fault tolerance, performance, and so on N. The protected telecommunication system should be implemented to realize the degree of adequacy in her defense mechanisms of information existing in the operational environment risks associated with the implementation of information security threats.

Modern methods of construction of the protected informational-communication systems and networks of telecommunications are observed including. Models are observed hierarchical three-level model of construction of networks and redundant centralised/decentralized. Installations of protection are analysed and possible threats of the informational safety are classified.

In the second chapter. Intercept user names and passwords creates a great danger, because users often use the same login and password for multiple applications and systems. Many users generally have a single password to access all resources and applications. If the application is running in client server mode and authentication data sent over the network in a readable text format, this information is likely to be used for access to other corporate or external resources.

In the given section of dissertational work principal views of attacks, such as sniffing, spoofing, DoS, scanning of ports, brutforce and others have been observed. Survey of the literature and studying of methods and a bucking means to the given attacks both at level of the service-provider, and at level of the end user have been executed.

In the third chapter. Intrusion Detection - this is another task performed by staff responsible for information security in the organization, while protecting against attacks. Intrusion Detection it is an active process in which detection occurs when a hacker attempts to penetrate into the system. Ideally, such a system only gives an alarm signal when attempting penetration. Intrusion Detection helps with preventive identification of active threats through alerts and warnings that the attacker collects the information necessary to carry out the attack. In fact, as will be shown in the lecture material, this is not always the case.

In the given chapter methods and sensors and buckings to attacks in informational-communication systems have been analysed. Having analysed possibilities of existing hardware components, their merits and demerits, are sampled the most suitable hardware components for complex system of protection, and also recommendations about use of the given system for higher efficiency of its

application are presented. The special attention is given detection of attacks on the basis of correlation of data from various sources, as to the most perspectiv, exact and productive combined method. Various types of correlation are observed and analysed. Various types of systems-traps and preferred circuits of their installation are observed.

In the fourth chapter in the given chapter the developed procedure of detection of attacks on the basis of correlation of data from various sources is presented. The given procedure differs application, along with traditional methods of system of detection of attacks, criteria, such as «a risk rating», which the quantitative characteristic of implementation of possible threat, and the "reputation", being parametre of "trust" to the certain address or the whole network. Also the programm complex of imitation and detection of attacks has been developed. The given complex is a platform for creation new exploit and testings of the new software on unforeseen vulnerability, an estimation of a degree of security of networks of telecommunications, revealing present vulnerability.

CONCLUSION

In this research were considered modern methods of construction of secure telecommunications networks, an analysis of possible threats to information security, the implementation of them with the most famous creature attacks, analyzed the methods and means of detection and counter attacks in the information and communication systems. After analyzing the possibilities of effective technological measures, their advantages and disadvantages, choose the most appropriate hardware for an integrated security system, and describes the recommendations for the use of this system for greater efficiency in its use. Particular attention is paid to intrusion detection based on correlation of data from different sources, as the most promising, precise and efficient combined method. Reviewed and analyzed various types of correlation.

The work methodology was developed intrusion detection based on correlation of data from different sources. This technique is characterized by using, along with traditional methods of intrusion detection systems, criteria such as "risk rating", which is a quantitative characteristic of the implementation of a possible threat, and "reputation" is an indication of "trust" a specific address or the entire network.

Proposed in the thesis simulation software package and intrusion detection is a flexible tool to configure and operate the system traps of varying degrees of interactivity, active by checking for vulnerabilities in a structure of information and communication system. This software package is also a platform for the creation of new exploits and testing new software to unforeseen vulnerabilities. The developed software allows us to estimate the degree of protection of telecommunication networks, identify vulnerabilities present different services, to trace the possible scenarios of malicious attacks through highly interactive systems traps validate the operation of the intrusion detection system based on correlate.

LIST OF PUBLICATIONS

1-А. Пономарчук, А.И. Программный комплекс аудита безопасности информационных систем для противодействия атакам / А.И. Пономарчук, Вахаб Алла, Т.В. Борботько, Юнис Али Аюб Юнис // XIII Белорусско-российская научно–техническая конференция "Технические средства защиты информации": Тезисы докладов, 4 -5 июня, 2015, Минск: БГУИР, 2015. — С. 24-25.