HACKING METHODS AND THEIR PROTECTION MEASURES

JURAYEV DIYORBEK UMIDJONUGLI

ABSTRACT

The article is devoted to methods of computer hacking and ways to prevent them. The motives pursued by hackers by carrying out this or that illegal act are investigated. The focus of the work is on the types of hacker attacks, as well as the rules that will protect the average user from computer hacking.

KEYWORDS: hacking,software attacks,methods of computer hacking,computer techologies,information security.

INTRODUCTION

The intensive development of modern society in the world has led to the global spread of new information technologies (IT) in various social spheres. The emergence of the hacker subculture was carried out in parallel with the formation of the World Wide Web. However, the Internet has become not only an arena for testing the most formidable forms of computer viruses, but also a place from which it has become possible to hack computers that are currently online, from where you can simply steal valuable information. Today, modern society has finally recognized the importance of solving the problem of protecting computer data. IT has radically changed the daily lives of millions of people. They have become an integral part of not only the economy, medicine, educational activities, but also other areas of human life. In countries with a high level of computerization, the issue of combating computer crime has long been one of the central problems [2]. It was with the development of computer technology that the first hackers appeared, such a direction of computer activity as hacking was born - computer hacking, the task of which is to gain access to confidential information stored in electronic form, and its further destruction, disclosure, modification or copying, that is, the implementation of unauthorized intrusion into the information system solely for criminal purposes.

Materials and methods: In order to understand the purpose for which this or that act of hackers is carried out, it is necessary to understand the motivation that prompts them to commit illegal actions. Consider the main motives of crackers [6]:

1. Gaining Attention: Once a system is compromised, hackers brag about their victories in an effort to earn "status in society" because any computer that has access to the Internet is a potential target for attack. 2. Greed: The main target of hackers is sites containing important information in order to obtain money, services or any data. 3. Malicious intent: in this case, the main goal of the attack is to harm a specific site or organization, the result of which is to cause significant damage to the system without official access to it. Software (SW) of any computer system consists of 3 elements: operating system (OS), network software (SW) and database management system (DBMS). Based on this division, all attempts to hack computer systems can be divided into 3 groups: 1. Attacks at the DBMS level. Due to the fact that the DBMS has a conditional internal structure, and the procedures for its elements are specified quite precisely, protecting the DBMS is one of the simplest tasks. In addition, there are two peculiar attack scenarios on the DBMS: 1) the results of arithmetic operations on the numeric fields of the DBMS are rounded down, and the difference between them is added to some other DBMS record [5]; 2) a hacker gains access to the fields of records of database management systems, for which only statistical information is open. The idea of hacking in this case is as follows: it is necessary to formulate the query in such a clever way that a lot of structured records are formed into one [3]. 2. Attacks at the OS level. As for the issue of protecting the operating system, here the prevention of unauthorized access is much more difficult than in the DBMS. This is due to the fact that the internal configuration of modern operating systems is very complex, which is why compliance with the security policy is a rather difficult and important task. Many people are mistaken when they say that attacks on operating systems organized by hackers are carried out only with the help of the most sophisticated means based on the latest achievements of science and technology. However, the art of a hacker is that it is necessary to be able to find a weak spot in a particular protection system. At the same time, the simplest methods of hacking to this day do not give way to the most sophisticated, because hackers use a certain rule: the more elementary the attack algorithm, the higher the probability of its completion without errors and failures. Any operating system can actually be subject to the following attacks [4]: 1) password theft (when a user enters a password, an attacker can spy on it); 2) obtaining a password from a file or any paper media; 3) theft of a material carrier (diskette, electronic key) of password information; 4) enumeration of all

possible password variations; 5) selection of a password by the frequency of occurrence of characters; 6) scanning of computer hard drives; 7) launching the program on behalf of a user with the necessary authority; 8) conversion of the code or data of the security subsystem of the OS itself; 9) denial of service, in order to disable the OS; 10) request bombardment and more. It is worth considering the fact that if the system administrator strictly adheres to the security policy of the computer system, then all of the above attacks are ineffective, although it is impossible to completely eliminate the threat of hacking at the operating system level. 3. Attacks at the level of network software. The most vulnerable piece of software is open source software. This is due to the fact that the communication channel through which various messages are transmitted is usually not secure, and anyone who has access to this channel can intercept and modify messages. In this regard, the following hacker attacks are distinguished: 1) listening to a local network segment; 2) intercepting messages on the router or creating a false one; 3) imposing messages; 4) denial of service. Since hacker attacks are provoked by the openness of network connections, it is reasonable to assume that in order to repel such attacks, it is necessary to protect communication channels as much as possible. Having studied the methods of computer hacking, we emphasize that in order to prevent it, it is necessary to adhere to the following rules. First, keep your operating system and web browser up to date as hackers attack when vulnerabilities exist. Secondly, it is worth installing a firewall (software that checks data received via the Internet or a network and blocks or allows it to the computer) and an anti-keylogger (keylogger protection module) to prevent external unauthorized access.

CONCLUSIONS.

It's best to buy or download antivirus software, change passwords monthly, and delete emails from unknown senders. Not everyone can know that they have been hacked. Therefore, you should always be aware of how your computer works and what programs are installed on it, since there is always a risk of hacking, even if the above rules were followed. Hackers are smart and constantly come up with new methods of hacking; these are highly qualified specialists, since it is their actions that pose the greatest threat to the security of computer systems. Information security of computer networks and individual computers is achieved through a unified policy of protective measures, as well as a system of measures of a legal, organizational and engineering nature.

REFERENCES

1. Sanctum Inc, "Ethical Hacking techniques to audit and secure web enabled applications", 2002.

2. P. Krensky, J. Hare. Hype Cycle for Data Science and Machine Learning, 2018. Gartner, 2018. Accessed: Sep. 10, 2019. [Online] Available at:https://www.gartner.com/en/documents/3883664/hype-cycle-for-data-science-and-machine-learning-2018

3. J. Han, J. Pei, M. Kamber. Data Mining: Concepts and Techniques. Morgan Kaufmann, 3rd edition, 2011, 744 p.

4. J. Danish and A. N. Muhammad, "Is Ethical Hacking Ethical? " , International journal of Engineering Science and Technology, Vol 3 No. 5, pp. 3758-3763, May 2011.

5. Ajinkya A.Farsole, Amurta G. Kashikar and Apurva Zunzunwala , "Ethical Hacking, International journal of Computer Applications (0975-8887), Vol. 1 No. 10, pp. 14-20, 2010.

6. S. Dilek, H. Qakir, M. Aydin. Applications Of Artificial Intelligence Techniques To Combating Cyber Crimes: A Review. International Journal of Artificial Intelligence & Applications (IJAIA), vol. 6, vo. 1, 2015, pp. 21-39.