UDC 004.73

I.I. Yenina, Yu.M. Parhomenko, V.V. Bosko

Kirovograd national technical university, Kirovograd, Ukraine

REVIEW OF THE WAYS TO PROTECT COMPUTER NETWORKS FROM ATTACKS ON SECURITY

The results of the analysis of intrusion detection methods to computer networks are presented in this work, discussed their advantages and disadvantages. The mechanisms used in modern systems detect attacks and the uses of combinations were analyzed. Proposed the ways of improving the quality of protection and methods to overcome attempts.

Keywords: *security, protect computer networks.*

Introduction

One of the most widespread methods of attack is DoS-attack, which aims to make computer resources unavailable to users for whom the computer system was designed. If the attack occurs simultaneously with a large number of IP-addresses, then it is called a distributed (DDoS) [1 – 3]. The danger most of DDoS-attacks in their absolute transparency and normality, as if bug in the software can always be corrected, the total consumption of resources - a phenomenon almost everyday. They face many administrators when resource machine is not enough. If cut traffic and resources for everybody, it is possible to escape from DDoS, but at the same time lose most of the customers. There is actually no way out of this situation, but the consequences of DDoS-attacks and their effectiveness can be substantially lower due to the correct router, firewall and continuous analysis of anomalies in network traffic.

Static protective mechanisms, which include access control systems, authentication systems, in many cases, can not provide effective protection. Therefore dynamic methods to quickly identify and prevent security breaches are necessary. One of the technologies that can detect violations that can not be identified by traditional models of access control, identification technology is attack. In fact, this process is a process of evaluation of suspicious activity taking place in the corporate network. In other words, intrusion detection is the process of identifying and responding to suspicious activities aimed at computers or network resources.

The effectiveness of attack detection systems depends on the used methods of analysis of the information received. In the first intrusion detection system developed in the early 80s, used static methods. Currently, these methods added a number of new techniques, ranging from expert systems, fuzzy logic, and ending the use of neural networks.

Main material

The main advantage is the use of static methods already developed and proven system of mathematical statistics and adapting to the behavior of the subject. First, all of the analyzed system defined profiles. Any deviation from the reference profile used by the unauthorized activity. Static methods are universal, because the analysis does not require knowledge of possible attacks and vulnerabilities that they use. However, using these techniques raises the following problems: 1) "Static" systems are not sensitive to the order of events in some cases the same events, depending on the order in which they follow can characterize abnormal or normal activities; 2) it's hard to put the limits monitored attack detection system, the characteristics to adequately identify anomalous activity; 3) "Static" systems can eventually be "trained" violators so that attacking actions were regarded as normal.

It should also be mind that static methods are not allowed in cases where the user no typical pattern of behavior typical or unauthorized actions.

Expert systems consist of a set of rules covering human expert knowledge. The use of expert systems is a common method of intrusion detection, in which information on the attack is formulated in the form of regulations. These rules can be written as a sequence of actions or signatures. In carrying out any of them a decision on the presence of unauthorized activity. An important advantage of this approach is the almost complete lack of false alarms. Database of the expert system should contain a scenario most currently known attacks. To remain constantly relevant, expert systems require constant updating databases. Although these systems and offer the opportunity to view the data in the log files required updates can either ignored or performed manually by the administrator. At a minimum, this leads to weakened expert system capabilities. In the worst case, lack of proper maintenance reduces the degree of security of the entire network by introducing its deceptive about the actual level of security. The main disadvantage is the inability to display unknown attacks. However, even a small change already known attacks can be a serious obstacle to the functioning of attack detection. Using neural networks are a way of overcoming these problems. Unlike previous systems neural network analyzes the data and provides an opportunity to assess whether the data are consistent with the characteristics that she trained to recognize. While the degree of compliance with network presentation may reach 100% reli-

ability choice depends entirely on the quality system in analyzing examples of the problem.

Originally neural network is trained on proper identification of pre-picked examples sample domain. Her reaction is analyzed and the system is configured so as to achieve the desired results. The neural network is dialed experience over time, as she analyzes data relating to its subject area. An important advantage of neural networks in detecting fraud is their ability to "learn" the characteristics of deliberate attacks and identify items that are not similar to those observed previously in the network. As each of the above described method have several advantages and disadvantages, almost hard to find a system that implements only one of the following methods. Typically, they are used together.

Also, the existing systems used a wide range of methods of response, which can be divided into three categories: message, preservation, active response.

A simple and widely used method is the message that is sending administrator security reports attack on console systems detect attacks that can be set not every employee is responsible for safety, in addition, these employees may be of interest, not all security events, so you need to use other mechanisms messages. These mechanisms may be sending messages via email, pager, fax or telephone. The category of "preservation" are: event log database and play attacks in real time. The first variant is widespread in other systems of protection. To implement the second option should miss attacking the network and fix all its actions for later playback administrator in real time all activities undertaken attacking, analyze successful attacks and prevent them in the future, and use the data collected in the review process.

Active response includes the following options: blocking of the attack, the attacker complete session node network management equipment and protective equipment. Active response, on the one hand, very efficient and on the other - requires precise use, because improper use can lead to abnormal function of the system.

The mechanisms used in modern systems detect attacks based on several common methods are not mutually excluded. Many systems use a combination. Yes, they are classified in three ways: 1) by way of response; 2) the method of detecting attacks; 3) the method of gathering information about the attack.

Conclusion

We will consider a more detailed classification of the method of gathering information at the network, host or application. The system at the network level (network-based) is the type of sniffer, monitoring traffic on the network and identifying possible actions of intruders. Such systems using typically attacks and signature analysis "on the fly", which is to monitor network traffic in real or near real time and using appropriate detection algorithms. The system-level host is designed for monitoring, detecting and responding to malicious action on a particular host. These systems analyze logs operating systems or applications. Generally, the analysis of the log is in addition to other methods of intrusion detection, including the detection of attacks "on the fly". Using this method allows for "debriefing" after it has been recorded attack in order to develop effective measures to prevent similar attacks in the future. Systems of this class can be divided into 3 groups: system-level application, system-level operating systems and system-level database management system. The system at the application level (application-based) is based on identifying attacks on specific applications, for example, Web-server. An example of such a system is Real Secure OS Sensor or Web Stalker Pro. The system-level operating system (OS-based) can detect attacks on the operating system level. An example of such a system is or Real Secure Server Sensor Intruder Alert. The system-level database management system (DBMS-based) makes it possible to identify attacks on specific database. Each of these types of attack detection system has its advantages and disadvantages. Hybrid system, which is a combination of different types of systems usually include the possibility of several categories.

References

1. Технологии обнаружения атак [Електронний ресурс]. – Режим доступу: http://ypn.ru/448/intrusion-detection-technologies.

2. DoS-атака [Електронний ресурс]. – Режим доступу: http://uk.wikipedia.org/wiki/DoS-атака.

3. Современные методы и средства сетевой защиты [Електронний ресурс]. – Режим доступу: http:// www.lghost.ru/lib/security/kurs6/theme03_chapter04.htm.

Надійшла до редколегії 1.02.2016

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов Національний технічний університет «ХПІ», Харків.

ОБЗОР СПОСОБОВ ЗАЩИТЫ КОМПЬЮТЕРНЫХ СЕТЕЙ ОТ АТАК НА БЕЗОПАСНОСТЬ

И.И. Енина, Ю.М. Пархоменко, В.В. Босько

В данной статье представлены результаты анализа методов обнаружения вторжений в компьютерные сети, рассмотрены их преимущества и недостатки. Проанализированы механизмы, используемые в современных системах обнаружения атак. Предложены пути повышения качества защиты и методов преодоления атак.

Ключевые слова: *безопасность, защита компьютерных сетей.*

ОГЛЯД СПОСОБОВ ЗАХИСТУ КОМП'ЮТЕРНИХ МЕРЕЖ ВІД АТАК НА БЕЗПЕКУ

І.І. Єніна, Ю.М. Пархоменко, В.В. Босько

У даній статті представлені результати аналізу методів виявлення вторгнень у комп'ютерні мережі, розглянуті їх переваги та недоліки. Проаналізовано механізми, що використовуються в сучасних системах виявлення атак. Запропоновано шляхи підвищення якості захисту і методів подолання атак.

Ключові слова: *безпека, захист комп'ютерних мереж.*