NOVATEUR PUBLICATIONS
JournalNX- A Multidisciplinary Peer Reviewed Journal
ISSN No: 2581 - 4230
VOLUME 8, ISSUE 4, Apr. -2022

SPECIFIC FEATURES OF THE STRUCTURE AND OPERATION OF NETWORK ATTACK DETECTION SYSTEMS

Usmanbayev Doniyorbek Shukhratovich
TUIT named after Muhammad al-Khwarizmi
Assistant of the Department of Information Security
doniyorbekush@gmail.com

ANNOTATION:

Computer attack detection systems are one of the most important elements of information security systems for networks of any modern enterprise, given how the number of problems associated with computer security has been growing in recent years. Although IDS technology does not provide complete protection of information, nevertheless it plays a very prominent role in this area. Here we will discuss in more detail the modern products on the market and the directions for further development of IDS.

Keywords: computer, information Security, IDS - Intrusion Detection Systems, technology.

INTRODUCTION:

Computer intrusion detection systems (IDS - Intrusion Detection Systems) are one of the most important elements of information security systems for networks of any modern enterprise, given how the number of problems associated with computer security has been growing in recent years. Although IDS technology does not provide complete protection of information, nevertheless it plays a very prominent role in this area. A brief history of the issue, as well as some experimental and commercial systems, were discussed in the article "Intrusion detection systems". Here we will discuss in more detail the modern products on the market and the directions for further development of IDS.

The market for IDS systems has been rapidly developing since 1997. It was at this time that ISS (http://www.iss.com) offered its product called Real Secure. A year later, Cisco Systems (http://www.cisco.com), realizing the feasibility of developing IDS, bought the NetRanger product along with the Wheel Group. It is impossible not to mention here the merger of SAIC and Haystack Labs into Centrax Corporation (http://www.centrax.com).

It should be noted that conventional IDSs detect only known types of attacks in a timely manner. They work in the same mode as anti-virus programs: known ones are caught, unknown ones are not. Detecting an unknown attack is a difficult task bordering on the realm of artificial intelligence systems and adaptive security management. Modern IDS are able to monitor the operation of network devices and the operating system, detect unauthorized actions and automatically respond to them in almost real time. When analyzing current events, past events can be taken into account, which makes it possible to identify attacks spaced apart in time and thereby predict future events.

In the 1980s, most attackers were experts in hacking and created programs and methods for unauthorized penetration into computer networks; automated means were rarely used. Now a large number of "amateurs" have appeared, with a weak level of knowledge in this area, who use automatic intrusion tools and exploits (exploit is a malicious code that uses known errors in software and is used by an attacker to disrupt the normal operation of

the software and hardware complex). In other words, as automatic intrusion tools improved, the level of knowledge and skills of most intruders decreased.

There are many different types of attacks, and they can be ranked according to their increasing risk as follows:

- Password guessing
- Replication code
- Password cracking
- Exploiting known vulnerabilities
- Disable/bypass audit systems
- Data theft
- Back doors (special entrances to the program that occur due to errors when writing it or left by programmers for debugging)
- Use of sniffers and sweepers (content control systems)
- Using network diagnostic programs to obtain the necessary data
- Using automated vulnerability scanners
- Data spoofing in ip packets
- Denial of service (dos) attacks
- Attacks on web servers (cgi scripts)
- Covert scanning technologies
- Distributed means of attack.

Now the attack lasts no more than a few seconds and can cause very sensitive damage. For example, a denial of service attack can disable a Web store or an online exchange for a long time. These attacks are the most common, and ways to protect against them are evolving rapidly.

The goal of any IDS is to detect an attack with as few errors as possible. In this case, the object of attack (the victim) usually wants to get an answer to the following questions.

What happened to my system?

What was attacked and how dangerous is the attack?

Who is the attacker?

When did the attack start and from where?

How and why did the invasion take place?

The attacker, in turn, usually tries to find out the following. ·

What is the target of an attack?

Are there vulnerabilities and what are they?

What harm can be done?

What exploits or means of penetration are available?

Is there a risk of being exposed?

First of all, IDS uses various methods to detect unauthorized activity. The problems associated with attacks through the firewall (firewall) are well known. The firewall allows or denies access to certain services (ports), but does not check the flow of information passing through an open port. IDS, in turn, tries to detect an attack on the system or on the network as a whole and warn the security administrator about it, while the attacker believes that he has gone unnoticed.

Here you can draw an analogy with the protection of the house from thieves. Locked doors and windows are a firewall. And the alarm for burglary notification corresponds to IDS.

There are various ways to classify IDS. So, according to the method of response, passive and active IDS are distinguished. Passive ones simply record the fact of the attack, write data to the log file and issue warnings. Active IDSs attempt to counter the attack, for example by reconfiguring the firewall or generating router access lists. Continuing the analogy, we can say that if the alarm in the house turns on a sound siren to scare away a thief, this is an analogue of an active IDS, and if it gives a signal to the police, this corresponds to a passive IDS.

According to the method of detecting an attack, signature-based and anomaly-based systems are distinguished. The first type is based on comparing information with a pre-installed database of attack signatures. In turn,

it is possible to classify attacks by type (for example, Ping-of-Death, Smurf). However, systems of this type cannot catch new, unknown types of attacks. The second type is based on the control of the frequency of events or the detection of statistical anomalies. Such a system is focused on identifying new types of attacks. However, its disadvantage is the need for constant training. In the home security example, the analog of this more advanced IDS system is neighbors who know who has come to your house, carefully watch strangers and collect information about an emergency situation on the street. This corresponds to the anomalous IDS type.

The most popular classification according to the method of collecting information about the attack: network-based, host-based, application-based. The system of the first type works like a sniffer, "listening" to traffic on the network and determining the possible actions of intruders. The attack is searched according to the principle "from host to host". The operation of such systems until recently was difficult in networks where switching, encryption and high-speed protocols (more than 100 Mbps) were used. But recently solutions from NetOptics (http://www.netoptics.com) and Finisar (http://www.finisar.com) companies have appeared for working in a switched environment, in particular, SPAN-port technologies (Switched Port Analyzer) and Network Tap (Test Access Port). Network Tap (as a standalone device or built into the switch) allows you to monitor all traffic on the switch. At the same time, Cisco and ISS have made some progress in implementing such systems in high-speed networks.

Systems of the second type, host-based, are designed to monitor, detect and respond to the actions of intruders on a specific host. The system, located on the protected host, checks and detects actions directed against it. The third type of IDS, application-based, is based on finding problems in a specific application. There are also hybrid IDS, which are a combination of different types of systems.

The operation of modern IDS and various types of attacks.

The general scheme of IDS functioning is shown in fig. Recently, there have been many publications about systems called distributed IDS (dIDS). dIDS consists of multiple IDSs located in different parts of a large network and linked to each other and to a central management server. Such a system enhances the security of the corporate subnet by centralizing information about the attack from various IDS, dIDS consists of the following subsystems: central analysis server, network agents, attack information collection server.

The central analysis server usually consists of a database and a Web server, which allows you to save information about attacks and manipulate data using a convenient Web interface.

The Network Agent is one of the most important components of dIDS. It is a small program whose purpose is to report an attack to a central analysis server.

The attack information collection server is a part of the dIDS system, logically based on a central analysis server. The server determines the parameters by which information received from network agents is grouped. Grouping can be carried out according to the following parameters:

- Attacker's IP address;
- Recipient port;
- Agent number;
- Date, time;
- Protocol
- Type of attack, etc.

Despite numerous reproaches and doubts about the efficiency of IDS, users are

already widely using both commercial tools and freely distributed ones. Developers equip their products with the ability to actively respond to an attack. The system not only detects, but also tries to stop the attack, and can also retaliate against the attacker. The most common types of active response are session termination and firewall reconfiguration.

Session termination is the most popular because it does not use external device drivers such as a firewall. For example, TCP RESET packets (with the correct sequence/acknowledgement number) are simply sent to both ends of the connection. However, ways for attackers to bypass such protection already exist and are described (for example, using the PUSH flag in a TCP/IP packet or using the current pointer trick).

The second way - reconfiguring the firewall, allows an attacker to find out about the presence of a firewall in the system. By sending a large stream of ping packets to the host and seeing that after some time access has stopped (ping does not pass), the attacker can conclude that the IDS has reconfigured the firewall by setting new ping deny rules on the host. However, there are ways to get around this protection. One of them is to apply exploits before reconfiguring the firewall. There is also an easier way. An attacker, attacking a network, can set IP addresses of well-known companies (ipspoofing) as the sender address. In response to this, the firewall reconfiguration mechanism regularly blocks access to the sites of these companies (for example, ebay.com, cnn.com, cert.gov, aol.com), after which numerous calls from indignant users to the support service of "closed" companies begin and the administrator is forced to disable this mechanism. This is very reminiscent of turning off a car alarm at night, the constant operation of which does not allow residents of neighboring houses to fall asleep. After that, the car becomes much more accessible to car thieves.

At the same time, it must be remembered that there are already tools for detecting IDS operating in the traffic "listening" mode (http://www.securitysoftwaretech.com/antisniff/download.html); in addition, many IDS are susceptible to DoS (denial of service) attacks.

The most advanced in this area are the "free" developers of the posix world. The simplest attacks exploit vulnerabilities associated with the use of signature-based IDS.

Of course, IDS system developers have been aware of these changes and catching attacks for a long time, but there are still poorly written attack signatures.

There are attacks based on polymorphic shell code. This code was developed by the author http://ktwo.ca/ and is based on the use of viruses. This technology is more effective against signature-based systems than against anomaly- or protocol analysis-based systems. The polymorphic code uses a variety of techniques to bypass string-matching systems (which can be found at http://cansecwest.com/noplist-v1-1.txt).

We can also recall attacks using packet fragmentation, IDS service denial, attack splitting between multiple users, ebcdic encoded attack encoding with terminal type change to ebcdic, encrypted channel attack implementation, snoop port suppression, routing table modification, to avoid traffic getting to the intrusion detection system, etc.

IDS systems are used to detect not only external but also internal violators. As practice shows, they are sometimes much more than external ones. Internal attacks are not among the general types of attacks. Unlike external intruders, an internal one is an authorized user who has official access to intranet resources, including those that circulate confidential information. The common practice is to use

information security services to protect the perimeter of the intranet, while protecting against internal threats is given much less attention. This is where IDS help. Setting up an IDS to protect against internal attacks is not an easy task; it requires painstaking work with rules and user profiles. To combat internal attacks, a combination of different IDSs must be used.

REFERENCES:

1. Branitskiy, A. Analiz i klassifikatsiya metodov obnarujeniya setevix atak / A. A. Branitskiy, I. V. Kotenko // Trudi SPIIRAN. - 2016. - T. 2, № 45. - S. 207-244.
2. Branitskiy, A. Network attack detection based on combination of neural, immune and neuro-fuzzy classifiers / A. Branitskiy, I. Kotenko // In Proceedings of the 18th IEEE International Conference on Computational Science and Engineering (IEEE CSE2015). - IEEE. Oct. 2015. - Pp. 152-159.
3. Pawar S.N. Intrusion Detection in Computer Network using Genetic Algorithm Approach: A Survey // International Journal of Advances in Engineering & Technology. 2013. vol. 6. Issue 2. pp. 730–736.
4. Chandrasekhar, A. M. Intrusion detection technique by using k-means, fuzzy neural network and SVM classifiers / A. M. Chandrasekhar, K. Raghuveer // In Proceedings of International Conference on Computer Communication and Informatics (ICCCI). - IEEE. 2013. - Pp. 1-7.
5. Ennert, M. Testing of IDS model using several intrusion detection tools / M. Ennert, E. Chovancova, Z. Dudlakova // Journal of Applied Mathematics and Computational Mechanics. - 2015. - Vol. 14, no. 1. - Pp. 55-62.
6. Brindasri, S. Evaluation Of Network Intrusion Detection Using Markov Chain / S. Brindasri, K. Saravanan // International Journal on Cybernetics & Informatics (IJCI). - 2014. - Vol. 3, no. 2. - Pp. 11-20.
7. Jiang H., Ruan J. The Application of Genetic Neural Network in Network Intrusion Detection // Journal of computers. 2009. vol. 4. no. 12. pp. 1223–1230.
8. YacineBouzida, Frederic Cuppens “Neural networks vs. decision trees for intrusion detection” in 2011.SIGMOD Record, 30 (4), 25-34.
9. www.networkworld.com
10. www.http://opensourceforu.com