« DEVELOP METHODS AND ALGORITHMS TO PROTECT WEBSITES FROM ATTACKS SUCH AS DDOS »

Sobirjonov Jaxongir
Tashkent University of Information Technologies
Named after Muhammad al-Khwarizmi

Annotation

The article mainly provides information about websites and methods of analysis of DDOS attacks. Forming the concept of algorithms in the protection of websites from threats and security. Methods of work on the basis of the developed algorithms are shown.

Keywords:

Interface, algorithm, website, operating system, DDOS, application.

Introduction

In the modern world, we cannot imagine our lives without computers. Computer technology is widely used in all areas of our daily lives (education, manufacturing, medicine, economics, etc.) in the rapid and verbal implementation of the work of receiving, processing and transmitting information. Currently, the term "information" is used as a special trademark that can be bought, sold, or exchanged for another product. At the same time, the value of information is often several hundred thousand times higher than the cost of the computer system in which it is located. Therefore, it is only natural that there is a strong need to protect information from unauthorized access, intentional alteration, theft, loss and other criminal acts. The protection of information in computer systems and networks means the use of various tools and methods, the taking of measures and the implementation of measures in order to systematically ensure the reliability of the information transmitted, stored and processed. Network operating system. It is associated with the emergence of local and global networks and is designed to provide the user with access to all the resources of computer networks.

Materials And Methods

The following typical representatives of network operating systems are Novell NetWare, Microsoft Windows NT, Banyan Vines, Solaris and others. An operating system is a set of special programs that allow computers connected to a network to work alone and together. This operating system provides services such as data exchange, storage, processing, transmission within the network.

Protecting against problems such as illegal access to the network, use and alteration of information, loss of information has become a topical issue. Businesses, organizations, and government agencies that connect to the network must pay close attention to network security before connecting to the network to share information.

Network security is achieved through the use of a variety of tools and methods, measures, and measures to ensure that information transmitted, stored, and processed is provided in a reliable and systematic manner. Network security tools need to be able to quickly identify and respond to threats. There are many types of network security threats, but they fall into several categories:

• Eavesdropping by attacking the transmission of information;
• Refusal to provide services; (Denial-of-service)
• Port scanning.

In the process of transmitting information, information can be listened to, modified and blocked without the user's knowledge, through the use of telephone lines, instant messaging over the Internet, video conferencing and faxing with a hearing and change attack. This attack can be carried out through several network analysis protocols. With the help of attack software, CODEC (convert video or audio analog signal

to digital signal and vice versa) easily converts digital audio to high quality but large volume audio files (WAV).

The following incidents occur as a result of an attack during the transmission of information

• Disconnection;
• Retention;
• Variation;
• Counterfeiting.

Retention - unauthorized use of a resource. As a result, the confidentiality of information is violated. Such users can be an individual, a program, or a computer.

Diversification - not only is the resource misused, but the resource is altered by the intruder. As a result, the integrity of the information is compromised. Examples of such interruptions are changes in the content of the data in the file, modification of the program to change its functions and characteristics, changes in the content of information transmitted over the network.

There are four common DDOS strategies that cybercriminals use to try to take over websites. They are all brute force attacks, and they make up the majority.

1. **TCP** connection attacks Try to do all the available work available on your site. This site includes all physical devices such as routers, firewalls and application servers. Physical devices always have limited communication.

2. **Volumetric** Attacks Fill your site's network with data. It works by getting rid of your server or even downloading all available bandwidth header to your server. Imagine a flood or traffic jam where nothing can move.

3. **Paragraph** attacks send bits and multiple data packets to the server. So your server can't do anything else trying to reassemble them.

4. **Software** Attacks in particular, you achieve one-sided or service-oriented goals that you have. This is very dangerous because by achieving a limited goal, you can realize that you are under attack until something breaks

Counterfeiting - a counterfeit object is entered into the system. As a result, the accuracy of the information is compromised. Examples of such violations are the transmission of artificial data over a network or the addition of records to a file. While the above violations are classified by the terms passive and active attack, we can see that interruption, diversification, and falsification belong to the active threat, while the passive threat refers to the retention.

Network intelligence is the collection of information through shared information and applications. An attacker usually tries to gather as much information about a network as possible before attacking it. There is no way to get rid of network intelligence completely. For example, if you cut off the echo response on the exon imp and peripheral router, you will avoid the echo test, but you will lose the data needed to diagnose network failures.

A port check attack uses a port check attack to obtain information about whether a port is open or not being used at the time of the hacker attack. A message is sent to analyze all ports at the same time, resulting in real-time determining which port the user is using on the computer, which is considered the computer's thin point. It is possible to tell exactly which service the user is using by the known port number. For example, if the analysis reveals the following port numbers, it is possible to determine the name of the service used by these numbers

• Port # 21: FTP (File Transfer Protocol) file sharing protocol;
• Port # 35: Private printer server;
• Port # 80: HTTP traffic (Hypertext Transfer [Transport] Protocol) hypertext exchange protocol;
• Port # 110: POP3 (Post Office Protocol 3) E-mail port.

To prevent potential threats, it is necessary not only to protect and control the use of operating systems and software, but also to identify the category of intruders and the methods they use. Some companies provide technical ways to search for cyber criminals. Based on the expertise of the experts dealing with this issue, it is possible to find not only the hacker who carried out the DDoS attack, but also the client himself.

This solution is very suitable for small and medium business. For large companies, enterprises and government agencies, there are whole hardware systems to fight DDoS attacks, which have high cost as well

as excellent protection features. Blocking and filtering incoming traffic only reduces the likelihood of an attack. In some cases, it is possible to completely undo a DDoS attack on the server. There are two main ways to filter traffic - firewall and full list routing. Filtering using lists (ACL) allows you to filter small protocols without compromising TCP performance and reducing access to a protected source. However, if hackers use botnets or high-frequency queries, then this method will be ineffective. They are much better protected from DDoS attacks, but their only downside is that they are only intended for private and non-commercial networks. After telling you all about such misfortunes like DDoS attack (what is it and how to deal with it) we can finally give one good piece of advice. Many large organizations offer their services to prevent and deter such attacks. Basically, such companies use all measures and various mechanisms to protect your business from many DDoS attacks. There are their own experts and specialists working there, so if your resource is dear to you, the best option (even if not cheap) is to contact one of these companies the most popular and dangerous way to start DDoS attacks is to use botnets (BotNets). A botnet is a set of computers with special software bookmarks (bots) installed, in English a botnet is a network of bots. Bots are usually developed by hackers separately for each botnet, and their main purpose is to send requests to a specific source on the Internet through a command received from the botnet management server - the Botnet command and the management server. The botnet management server is managed by a hacker or by the person who bought the botnet from the hacker and has the ability to launch a DDoS attack. Bots are distributed on the Internet in a variety of ways, as a rule - attacking computers with vulnerable services or installing software bookmarks on them or deceiving users and removing them under the guise of providing other services or programs that are harmful or not working. by forcing the installation. even a useful feature. There are many ways to distribute bots; new methods are constantly being invented.

Discussions And Results

An unreliable employee with his or her actions solves a problem (possibly even more) that is dangerous to hackers. On top of that, it is more difficult to determine its existence.

It also has to eliminate the internal protection of the network, which is usually less rigid, rather than the external protection of the network. In this case, the risk of unauthorized use of corporate information is higher than that of a person with any other malicious intent. The above categories of information security violators can be grouped by their qualifications: amateur (adventure seeker), specialist (ideological hacker, unreliable employee), professional (hacker-professional). If we compare the causes of security breaches with these groups and the technical armament of each group, a generalized model of the information security breach can be obtained.

Conclusion

The article focuses on the types of attacks that occur on websites, each of which is divided into separate groups according to their classification. At the same time, ensuring that such systems are not used for any negative purpose is to ensure that they are used only by the right people, for the right purpose. In this regard, in the era of globalization, the application of the methods we have described in this course will be highly effective in ensuring the security of the exchange of the most valuable data. Therefore, it is time to ensure a high level of security.

References

1. G'aniev. S.K, Karimov. MM, Tashev KA, Information Security. Security of information and communication systems. Tashkent 2008.
2. V.F Shangin Information security of computer systems and networks.
3. http://www.ziyonet.uz
4. http://www.uzinfocom.uz
5. www.yandex.ru