Practical Security Management

Usmonov Makhsud

Tashkent University of Information Technologies, Karshi branch 3rd year student
+99891 947 13 40
maqsudusmonov22@gmail.com

Abstract: *Global security management policy within the organization network. Formulation of local security policy. Carry out local security policy to all information security devices. The use of computer and information technologies, telecommunications, data transmission networks, Internet services, which are included in the priorities of our country's policy, is developing and modernizing. The widespread introduction of modern information technologies in all spheres of our society in our daily lives will ensure the achievement of our future goals. The use of the Internet in any industry increases productivity.*

Keywords: Eavesdropping, Denial-of-service, Port scanning, IPSec, IDC, VPN.

INTRODUCTION

1. Types of threats to network security

2. Technologies that are effective against hearing and altering information transmitted over a network

Global security management policy within the organization network. Formulation of local security policy. Carry out local security policy to all information security devices. The use of computer and information technologies, telecommunications, data transmission networks, Internet services, which are included in the priorities of our country's policy, is developing and modernizing. The widespread introduction of modern information technologies in all spheres of our society in our daily lives will ensure the achievement of our future goals. The use of the Internet in any industry increases productivity. Quick data sharing using a network can save time. In particular, the formation of the e-government system in our country and the organization of strengthening the interaction between government agencies and the population on its basis will be carried out using the network. Effective use of the network will ensure the formation of a democratic information society. In such a society, the speed of information exchange will increase, and there will be faster results in the collection, storage, processing and use of information. However, protection against problems such as unauthorized 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 threats to network security, but they fall into several categories: • Eavesdropping; • Refusal to provide services; (Denial-of-service) • Port scanning. In the process of transmitting information, information can be listened to, altered and blocked without the user's knowledge, through the use of telephone lines, instant messaging via the Internet, video conferencing and faxing with a hearing and change attack. This attack can be carried out through several network analysis protocols. Through attack software, CODEC (Convert Video or Audio Analog to Digital Signal and Conversely) easily converts digital audio to high quality but large volume audio files (WAV). Usually the process of performing this attack is not noticeable to the user at all. The system performs the specified operations without excessive stress and noise.

METHODS

There is no doubt about the theft of information. Only those who are aware of this threat in advance and want the information sent to maintain its value will be able to exchange information through a secure network as a result of special network security measures. There are several effective technologies against hearing and altering information transmitted over a network: • IPSec (Internet Protocol Security); • VPN (Virtual Private Network) virtual private network; • IDS (Intrusion Detection System). Ipsec (Internet protocol security) allows secure exchange of information over the network using these security protocols and encryption algorithms. Computers in the network through this special standard g Enables interoperability of software and data and hardware. The Ipsec protocol ensures the confidentiality of the information transmitted over the network, ie only the sender and receiver can understand it, the purity of the information and the authentication of packets. The use of modern information technology has become a necessary tool for the development of any organization, and the Ipsec protocol provides effective protection for: • bog‘ When connecting headquarters and branches to the global network; • Long-distance management of the enterprise via the Internet; • Protecting a network connected to sponsors; • Improving the security of e-commerce. A VPN (Virtual Private Network) is defined as a virtual private network. This technology is based on the formation of an internal network within another network to share all information between users, aimed at providing reliable protection. The Internet is used as the network base for a VPN. The advantage of VPN technology. By connecting local area networks to a common VPN network, a low-cost, high-security tunnel can be built. To create such a network, you need to install a special VPN gateway on one computer in each part of the network to exchange information between branches. The information exchange in each department is simple. If you need to send data to another part of the VPN network, then all the data will be sent to the gateway. The gateway, in turn, processes the data, encrypts it using a reliable algorithm, and sends it over the Internet to another branch's gateway. At the designated point, the data is decrypted and transmitted to the final computer in a simple manner. All this is done in a way that is completely imperceptible to the user and is no different from working on a local network. Using the eavesdropping attack, the information heard becomes incomprehensible. In addition, a VPN is a great way to connect a separate computer to an organization's local area network. Let's say you're on a business trip with your laptop and you need to connect to your network or get some information from there. With a special program, you can connect to a VPN gateway and act like any other employee in the office. It is not only convenient but also inexpensive. The principle of operation of a VPN. In addition to new hardware and software, setting up a VPN requires two main components: a data protocol and security tools.

Using an unauthorized access detection system (IDS) identifies the method or means by which an attempt is made to compromise a system or network security policy. Unauthorized access detection systems have a history of almost a quarter of a century. The first models and prototypes of unauthorized access detection systems used the analysis of computer system audit data. This system is divided into two main classes. It is divided into the Network Intrusion Detection System and the Host Intrusion Detection System. Figure 14.1. The unauthorized access detection system model The architecture of IDS systems includes: • a sensor part system that collects and analyzes the security situation of protected systems; • Analytical system for detecting suspicious actions and attacks based on sensor data; • A warehouse that collects analysis results and initial data; • □A management console that allows you to configure the IDS system, monitor the status of the IDS and the protected system, and monitor the conflicts detected by the analysis partition systems. This system is divided into two main classes. It is divided into the Network Intrusion Detection System and the Host Intrusion Detection System. The principle of operation of the system of unauthorized access to the network (NIDS) is as follows: 1. Checks the traffic that has access to the network; 2. Restricts harmful and unauthorized packages. Eavesdropping can be effectively protected by using the security steps listed. DOS (Denial-of-service) This type of network attack is called a denial-of-service attack. The attacker tries to prevent legal users from using the system or service. Often, these attacks are carried out by overflowing infrastructure resources with service access requests. Such attacks can target the entire network, as well as the individual host. Before carrying out an attack, the object is thoroughly examined, that is vulnerabilities or deficiencies in the protection against network attacks, what operating system is installed, and when the facility is at its peak. Based on the results of the following detection and verification, a special program is written. In the next step, the created program is sent to the servers of the highest position. Servers send to registered users in their database. The user who receives the application installs the application knowingly or unknowingly that it was sent by a trusted server. This can happen to thousands or even millions of computers. All at the time the program is scheduled

activates on computers and sends requests to the server of the object to be attacked continuously. The server is busy answering incessant requests and is unable to perform basic operations. The server fails to serve. Figure 14.2 Model of service denial attack The most effective ways to protect against denial of service are: • Firewall technology; • secIPsec protocols. The firewall is the first protection device of the inner and outer perimeters. The firewall manages incoming and outgoing data in information and communication technologies (ICTs) and provides ICT protection by filtering data, performing information verification based on established criteria and deciding whether packets to enter the system. The firewall sees all packets passing through the network and checks the packets in both directions (input, output) according to the established rules and decides whether to allow them or not. The firewall also provides protection between two networks, that is, it protects the protected network from an open external network. The advantages of the protection tool listed below, especially the packet filtering function, are an effective means of protection against DOS attacks. Packet filters control: • □physical interface, where the packet comes from; • IP address of the source; • IP address of the recipient; • Source and receiving transport ports. The firewall does not provide full protection against DOS attacks due to some shortcomings:

• Design errors or omissions - various technologies of firewalls do not cover all the intrusions into the protected network; • Implementation Disadvantages - Each firewall has errors as long as it is in the form of a complex set of software (hardware). In addition, there is no common test methodology that allows to determine the quality of software implementation and ensure that all specified features are implemented on the firewall; • Operational shortcomings - firewalls are very difficult to manage, configure based on security policies, and in many cases there are cases of incorrect configuration of firewalls. These shortcomings can be addressed using the IPsec protocol. Summarizing the above, it is possible to provide adequate protection against DOS attacks through the proper use of firewalls and the IPsec protocol. The attack type of port scan is more commonly used on computers that provide network services. We need to pay more attention to virtual ports to ensure network security. Because ports are a means of transporting data over a channel. The computer has 65,536 standard ports. Computer ports can be likened to a door or window in a house. The attack on the port checkpoints seems to indicate that the thieves knew whether the doors and windows were open or closed before entering the house. If a thief notices that the window is open, it will be easier to enter the house. The hacker uses the Ports Check attack to get information about whether a port is open or not being used during an 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. Figure 14.3. Types of attack and means of protection Port control check against attack an effective protection solution The efficient use of firewall display technology gives the expected result. An attack can be prevented by introducing a special rule on the firewall to respond to requests to check all ports at the same time.

RESULTS

Using an unauthorized access detection system (IDS) identifies the method or means by which an attempt is made to compromise a system or network security policy. Unauthorized access detection systems have a history of almost a quarter of a century. The first models and prototypes of unauthorized access detection systems used the analysis of computer system audit data. This system is divided into two main classes. It is divided into the Network Intrusion Detection System and the Host Intrusion Detection System. Figure 14.1. The unauthorized access detection system model The architecture of IDS systems includes: • a sensor part system that collects and analyzes the security situation of protected systems; • Analytical system for detecting suspicious actions and attacks based on sensor data; • A warehouse that collects analysis results and initial data; • □A management console that allows you to configure the IDS system, monitor the status of the IDS and the protected system, and monitor the conflicts detected by the analysis partition systems. This system is divided into two main classes. It is divided into the Network Intrusion Detection System and the Host Intrusion Detection System. The principle of operation of the system of unauthorized access to the network (NIDS) is as follows: 1. Checks the traffic that has access to the network; 2. Restricts harmful and unauthorized packages. Eavesdropping can be effectively protected by using the security steps listed. DOS (Denial-of-service) This type of network attack is called a denial-of-service attack. The attacker tries to prevent legal users from using the system or service. Often, these attacks are carried out by overflowing infrastructure resources with service access requests. Such attacks can target the entire network, as well as the individual host. Before carrying out an attack, the object is thoroughly examined, that is vulnerabilities or deficiencies in the protection against network attacks, what operating system is installed, and when the facility is at its peak. Based on the results of the following detection and verification, a special program is written. In the next step, the created program is sent to the servers of the highest position.

DISCUSSION

Using an unauthorized access detection system (IDS) identifies the method or means by which an attempt is made to compromise a system or network security policy. Unauthorized access detection systems have a history of almost a quarter of a century. The first models and prototypes of unauthorized access detection systems used the analysis of computer system audit data. This system is divided into two main classes. It is divided into the Network Intrusion Detection System and the Host Intrusion Detection System. Figure 14.1. The unauthorized access detection system model The architecture of IDS systems includes: • a sensor part system that collects and analyzes the security situation of protected systems; • Analytical system for detecting suspicious actions and attacks based on sensor data; • A warehouse that collects analysis results and initial data; • □A management console that allows you to configure the IDS system, monitor the status of the IDS and the protected system, and monitor the conflicts detected by the analysis partition systems. This system is divided into two main classes. It is divided into the Network Intrusion Detection System and the Host Intrusion Detection System. The principle of operation of the system of unauthorized access to the network (NIDS) is as follows: 1. Checks the traffic that has access to the network; 2. Restricts harmful and unauthorized packages. Eavesdropping can be effectively protected by using the security steps listed. DOS (Denial-of-service) This type of network attack is called a denial-of-service attack. The attacker tries to prevent legal users from using the system or service. Often, these attacks are carried out by overflowing infrastructure resources with service access requests. Such attacks can target the entire network, as well as the individual host. Before carrying out an attack, the object is thoroughly examined, that is vulnerabilities or deficiencies in the protection against network attacks, what operating system is installed, and when the facility is at its peak. Based on the results of the following detection and verification, a special program is written. In the next step, the created program is sent to the servers of the highest position. Servers send to registered users in their database. The user who receives the application installs the application knowingly or unknowingly that it was sent by a trusted server. This can happen to thousands or even millions of computers. All at the time the program is scheduled activates on computers and sends requests to the server of the object to be attacked continuously. The server is busy answering incessant requests and is unable to perform basic operations. The server fails to serve. Figure 14.2 Model of service denial attack The most effective ways to protect against denial of service are: • Firewall technology; • secIPsec protocols. The firewall is the first protection device of the inner and outer perimeters. The firewall manages incoming and outgoing data in information and communication technologies (ICTs) and provides ICT protection by filtering data, performing information verification based on established criteria and deciding whether packets to enter the system. The firewall sees all packets passing through the network and checks the packets in both directions (input, output) according to the established rules and decides whether to allow them or not. The firewall also provides protection between two networks, that is, it protects the protected network from an open external network. The advantages of the protection tool listed below, especially the packet filtering function, are an effective means of protection against DOS attacks. Packet filters control: • physical interface, where the packet comes from; • IP address of the source; • IP address of the recipient; • Source and receiving transport ports. The firewall does not provide full protection against DOS attacks due to some shortcomings:

CONCLUSION

However, protection against problems such as unauthorized 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 threats to network security, but they fall into several categories: • Eavesdropping; • Refusal to provide services; (Denial-of-service) • Port scanning. In the process of transmitting information, information can be listened to, altered and blocked without the user's knowledge, through the use of telephone lines, instant messaging via the Internet, video conferencing and faxing with a hearing and change attack. This attack can be carried out through several network analysis protocols. Through attack software, CODEC (Convert Video or Audio Analog to Digital Signal and Conversely) easily converts digital audio to high quality but large volume audio files (WAV). Usually the process of performing this attack is not noticeable to the user at all. The system performs the specified operations without excessive stress and noise.

REFERENCES

1 Seymour Bosworth, Michel E. Kabay, Eric Whyne. Computer security handbook. Wiley.2014.

2 Bulletin of the Oliy Majlis of the Republic of Uzbekistan. - T., 2003. - №1. - 2-m.

3Information security in the field of communication and information: Terms and definitions. Network standard: TSt 45-010: 2010.

4 Bulletin of the Supreme Council of the Republic of Uzbekistan. - T., 1993. - №5. - 232-m.

5 Sean Harris. ALL IN ONE CISSP. McGraw-Hill. 2013.

6 Explanatory dictionary of information and communication technologies (second edition). - T., 2010.