УДК 61:004.651 (075.8)

І.Є. Андрущак
Луцький національний технічний університет

ОСОБЛИВОСТІ ТА СПЕЦИФІКА ТЕХНОЛОГІЇ МЕРЕЖЕВИХ АТАК

В роботі проведено огляд та питання особливості та специфіки технології мережевих атак в компютерних мереж, стан та перспективи розвитку методів, засобів захисту та безпеки в мережах. Виділено ключові площини аспектів застосування технологій систем захисту та безпеки в сучасних компютерних мережах.

Ключові слова: *мережеві атаки, сніффер пакетів, криптографія, інформаційна безпека, контоль доступу, ідентифікатори програм.*

И.Е. Андрущак
Луцкий национальный технический университет

ОСОБЕННОСТИ И СПЕЦИФИКА ТЕХНОЛОГИИ СЕТЕВЫХ АТАК

В работе проведен обзор и вопросы особенности и специфики технологии сетевых атак в компьютерных сетей, состояние и перспективы развития методов, средств защиты и безопасности в сетях. Выделены ключевые плоскости аспектов применения технологий систем защиты и безопасности в современных компьютерных сетях.

Ключевые слова: *сетевые атаки, сниффер пакетов, криптография, информационная безопасность, контоль доступа идентификаторы программ.*

I.Ye. Andruschak
Lutsk national technical university

FEATURES AND SPECIFIC TECHNOLOGY NETWORK ATTACKS

In this work, a review and issue the specific features and technologies of computer network attacks in networks state and prospects of development of methods of plant protection and security networks. Highlight key aspects plane use of technology protection and security of computer networks today.

Keywords: *network attacks, packet sniffer, cryptography, information security, access kontol IDs programs.*

There is a huge variety of different configurations of computers, operating systems and network equipment, however, is not a barrier to access to the global network. This situation was made possible thanks to the universal network protocol TCP / IP, which establishes certain standards and rules for data transmission over the Internet. Unfortunately, such versatility has meant that computers that use this protocol were vulnerable to outside influence, and because the TCP / IP protocol is used on all computers connected to the Internet, the attackers no need to develop individual means of access to other people's cars.

Network attack - an attempt to influence the remote computer using software methods. Generally, the purpose of network attack is a violation of privacy, that is, stealing information. In addition, network attacks are carried out to access someone else's computer and further changes in files located on it.

There are several types of classification of network attacks. One of them - on the basis of impact. Passive network attacks designed to obtain confidential information from a remote computer. These attacks, for example, the reading of incoming and outgoing e-mail. As for the active network attacks, their task is not only access to some information, but their modification. One of the most significant differences between these types of attacks is to detect passive intervention is almost impossible, while the effects of active attack is usually visible.

Strong authentication is the most important means of protection method sniffinha packages. By "strong" we understand these authentication methods that are difficult to get around. An example of such authentication is a one-time passwords (One-Time Passwords, OTP).

Packet sniffer is an application that uses a network card which works in promiscuous mode (in this mode all packets received on physical channels, network adapter sends the application for processing). This sniffer intercepts all network packets that are transmitted through a domain. Currently sniffer works on a completely legitimate. With sniffer can find useful and sometimes sensitive information (eg usernames and passwords).

Another way to combat sniffinhom packets in a network environment is to create a switched infrastructure. If used throughout the organization switched Ethernet, hackers can gain access only to the traffic coming to the port to which they are connected.

Antysniffery - a Fight sniffinhom is to install hardware or software that recognize sniffers that are

running on the network.

Cryptography - the most effective means of combating sniffinhom packets while not preventing interception and sniffer does not recognize the work, but does the job vain.[1]

IP-spoofing occurs when a hacker that is inside a corporation or beyond, impersonating the authorized user. The threat of spoofing can be weakened by using these measures:

Access Control - the easiest way to prevent IP-spoofing is the proper selection of access control. The administrator can prevent the spoofing another's networks by users of its network. You must cull any outgoing traffic starting address is not one of the IP-addresses of your organization.

The most effective method of dealing with IP-spoofing - the same as in the case of packages sniffinhom:

- need to make the attack completely ineffective. IP-spoofing can function only on condition that the authentication is based on IP-addresses. Therefore, the introduction of additional authentication methods for making such attacks useless.

- denial of Service Denial of Service (SDS), without a doubt, is the best known form of hacker attacks. Among hackers, DoS attacks are considered child's play, and their application is contemptuous smile, because of DoS minimum required knowledge and skills. Nevertheless, it is the ease of implementation and the huge scale of the damage caused to SDS attract the attention of administrators responsible for network security.

Most DOS attacks designed not to software errors or breaches in security, and the general weakness of the system architecture. The threat of such attacks SDS can be reduced in three ways:

- the correct configuration antyspufinha functions on routers and firewalls to help reduce the risk of SDS.

- the correct configuration of anti-SDS features on routers and firewalls may limit the effectiveness of attacks. These features often limit the number of half-open channel at any given time.

Restricting traffic (traffic rate limiting). The organization can ask the provider (ISP) to limit traffic. This type of filtering allows you to limit the amount of non-critical traffic that passes through your network. A common example is to limit the volume of traffic ICMP, which is used only for diagnostic purposes.

Hackers can perform password attacks using a variety of methods such as simple brute (brute force attack), Trojan horse, IP-spoofing and sniffinh packages. Although login and password are often available through IP-spoofing and packet sniffinha, hackers often try to steal your password and login, using many access attempts. This approach is called a simple enumeration (brute force attack).

Often such attacks, a special program that tries to access public resources (such as servers). Password attacks can be avoided if you do not use passwords in text form. One-time passwords or cryptographic authentication can virtually nullify the threat of such attacks. Unfortunately, not all applications, hosts and devices support the above authentication methods [2].

For such attacks Man-in-the-Middle hacker need access to the packets transmitted over the network. Such access to all packets transmitted from the provider to any other network can get employee of the provider. For this type of attack is often used sniffer packet transport protocols and routing protocols. Effectively deal with such attacks Man-in-the-Middle is through cryptography.

The attacks at the application level can be performed in several ways. The most common of them - the use of the known weaknesses of the server software (sendmail, HTTP, FTP). The main problem in the attacks at the application level is that hackers often use ports that are allowed to pass through the firewall. Measures that can be done to reduce vulnerability to attacks of this type - a reading log files and network operating systems, log files and analyze them using specific analytical applications [3].

Network intelligence - a collection of information about the network using public data and applications. In preparation for an attack against any network hacker usually tries to get her on which more information.

Methods of protection:

- use the latest versions of operating systems and applications and the latest correction modules ("patches");

- use of detection of attacks (IDS).

Breach of trust - this type of action is not in the full sense of the word attack or assault. It is a malicious use of trust relationships that exist in the network. A classic example of this abuse is the situation in the peripheral part of the corporate network. In this segment are often servers DNS, SMTP and HTTP. Since they all belong to the same segment, breaking any of them leads to breaking all the others, because these servers are trusted by other systems of the network. The risk of abuse of trust can be

reduced due to tighter control of levels of trust within their network.

Forwarding ports is a form of abuse of trust when broken host used to pass through the firewall traffic that otherwise would necessarily rejected. The main way to combat the use of port forwarding is a reliable model of trust.

Workstations end users are very vulnerable to viruses and Trojan horses. Viruses known malicious programs implemented in other programs to perform a specific function unwanted workstation end user.

Trojan horse - is not soft paste and true program that at first glance seems to be a useful application, but in fact performs harmful role. Fighting viruses and Trojan horses is through effective antivirus software running on the user level and possibly at the network level [4].

By way of implementation of all measures to ensure the security of computer systems are divided into:

- regulatory (legislative);
- ethical;
- organizational (administrative);
- software and hardware.

Regulatory support - this includes regulations, regulations, instructions, manuals, requirements that are mandatory within the scope of their actions, as well as the rules and regulations of agencies, services, facilities, implementing information security function, various techniques that provide user activity while performing their work in terms of solid information security requirements. By ethical measures include combating all kinds of behavior norms that have traditionally formed or in the society or the country. These rules are generally not binding as the legislatively approved, but their failure usually leads to a drop in credibility, prestige person, group or organization's image.

Organisational protection measures - a point that regulate the functioning of the processing, use of resources, the activities of the staff, and also for user interaction with the system so that most hinder or exclude the possibility of implementing security threats.

Technical (hardware and software) protection referred to various electronic devices and special programs that perform (alone or in combination with hardware) protection functions (identification and authentication of users, access to resources, event registration, encryption information, etc.).

Organizational remedies COP include:

- development of rules of information processing in the Constitutional Court;
- measures taken in the design, construction, equipment and facilities, nodes and other objects of the information system, excluding the impact of natural disasters, the possibility of unauthorized penetration into buildings, etc .;
- measures taken in the selection and training of personnel.

In this case, the test provided for hired employees, creating conditions under which staff would be interested in the integrity of the data, learning the rules of working with classified information, review of measures of responsibility for violation of protection, etc. [7].

One of the most important organizational measures is the creation of special regular services in information security information systems closed as a security administrator and network administrator of distributed databases and data banks. Security Service is an independent organizational unit of the organization that submits directly to the head of the organization.

Organizational measures are critical link in the formation and implementation of integrated information security and a system of security. You must first determine that (a list of controlled objects and resources), why (analysis of potential threats) and how (development requirements, the definition of security policy and the development of administrative and hardware and software measures to ensure in practice developed security policy) protect.

The software data protection - a system of special programs included in the software, and functions that implement information security in computer systems for various purposes and means of processing (collection, storage, preservation, processing and transmission) of data.

Software protection have the following types of special programs:

- identification of means, files, and user authentication;
- the registration and control of the technical facilities and users;
- service processing modes;
- the protection of computer operating tools and applications users;
- destruction of information in zapam`yatovuyuchomu device after use;
- subsidiary protection programs for various purposes.

To ensure reliable protection using password protection systems is organized so that the likelihood

of disclosing secret password and establish whether a particular file or ID terminal is at least. To do this periodically change your password, and the number of characters in it set pretty high. Obtaining permission to access certain resources can be achieved not only through the use of these secret password and authentication and identification. You can do a more detailed way that takes into account various features modes of users, their powers, the categories of data and resources requested. This method is implemented special programs that analyze the relevant characteristics of users, content objectives, parameters of hardware and software, memory devices, and others. To protect against alien invasion necessarily assumed by security measures [8].

The procedure for identification and authentication involves checking whether a subject that access (or object which is being accessed), because they say they are. Such inspections may be one-time or periodic (especially in cases of prolonged sessions).

The most common method is identifying levels of password authentication. Practice has shown that the password protection of data is a weak link because the password could eavesdrop or spy, the password can be intercepted or just vzlamaty.

To protect the password itself produced by recommendations on how to make a reliable password:

- password must contain at least eight characters;
- do not use a password obvious character set, such as name, date of birth, names of relatives or the name of the program;
- do not call anyone your password, do not write it;
- periodically change your password.

To identify the programs and data are often resorted to calculating checksums, however, as in the case of password authentication, it is important to exclude the possibility of forgery while maintaining the correct checksum. This is achieved through the use of sophisticated methods of controlling summation based cryptographic algorithms. To provide data protection against forgery (imitostiykist) can, using different methods of encryption and digital signature techniques based on cryptographic systems, public key.

Protection level hardware and software provides control access to computing resources, individual devices, memory, operating system, a special office or personal user applications.

Data protection is aimed at the data:

- The protection of information when applying to it while working on the PC and perform only authorized operations on them;
- To protect information during transmission via communication channels between different computers. Controlling access to information to answer the question of who can perform operations;
- Over what data is allowed to perform the operation.

The object, access to which is controlled can be a file, record or file a separate field record file, as well as the factors governing the access - defined event data value, system status, user credentials, background and other data addressing [9].

Access controlled event involves blocking user appeal. For example, at certain intervals or when applying with specified terminal. Access, depending on the state, is dependent on the current state of the computer system that manages applications and security systems. Access, which depends on the powers involves addressing user programs, data, equipment, depending on the given mode. These modes can be "read only", "read and write", "execute only" and others. The basis of most means of access is a particular representation matrices access.

Another approach to the construction of access remedies based on the control of information flow and sharing of facilities and access to the classes of confidentiality. Means register as access control, include effective measures to protect against unauthorized actions. However, if access control designed to prevent such actions, the task of registration - to find already taken their acts or attempts.

Means copy protection to prevent the use of stolen copies of the software and is currently the only reliable means of spreading illegal copies of software. When the means of copy protection refers to the means for implementation of the program of their functions recognizable only at certain unique element that is not copied. This element (a key) can be a file, disk, CD, or a special device that connects to the PC.

Under the environment, which will run a program meant diskette, CD-ROM or PC (if installation is on your hard drive). Identification of the environment is to some extent poimenuvaty environment to further its authentication. Identify the environment - then fix him some specially created or are rarely repeated, characteristics that are difficult counterfeited - ID [10].

Identification data carrier can be made in two ways. The first is based on applying the marker on some of the surface of the floppy disk or CD-ROM. The second method of identification based on special

formatting a floppy disk or CD-ROM. The response to the launch of unauthorized Environment course boils down to issuing a notification.

References

1. Simmonds. A; Sandilands. P; van Ekert. L (2004). An Ontology for Network Security Attacks. Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285. с. 317–323. doi:10.1007/978-3-540-30176-9_41. ISBN 978-3-540-23659-7.

2. Role-Based Trusted Network Provides Pervasive Security and Compliance - interview with Jayshree Ullal, senior VP of Cisco.

3. Dave Dittrich, Network monitoring/Intrusion Detection Systems (IDS), University of Washington.

4. Haykovych V.Y. Necessary condition for successful application / V.Yu.Haykovych, D.V. Ershov // "systems of security, communications and telecommunications", №3, - 2007.

5. Yershov D.V., Popov Z. Computer Security Training / D.V. Ershov, Z.V. Popov // "KomLoh», №2, - 2007.

6. Kadirov M.M. Information safety of computer networks / M.M. Kadirov, N.O. Karimov // Young scientist. - 2016. - №8. - S. 124-126.

7. Lukatsky A.V. New approaches to information security network / A.V. Lukatsky // Computer-Press. - № 7. - 2007.

8. Lukatsky A.V. Adaptive security. Fashion or perceived need / A.V. Lukatsky // PCWeek, - №37. - 2009.

9. Lukatsky A.V. The family of adaptive security management tools / A.V. Lukatsky // «Network», - № 10. - 2008.

10. Novikov S.M. Information security in communication networks with guaranteed quality of service. / S.M. Novikov // Novosibirsk. - 2003. - S.18-31.

Стаття надійшла до редакції 15.03.2017