Example of network forensics research paper

Sociology, Violence

Research paper

Permanent control over the work of local network, which is a fundamental of any corporate network, is needed to maintain it in working condition. Control - a necessary first step that must be done in the management of the network. Given the importance of this function, it is often separated from other functions of management systems and implemented by special means. Such division of control functions and actually management is useful for small and medium-sized networks, for which the installation of the integrated management system is not economically sensible. The use of autonomous means of control helps the network administrator to identify problem areas and devices of the network, and their disabling or reconfiguration he may perform in this case manually. The process of network monitoring is usually divided into two phases - the monitoring and analysis. At the stage of monitoring more simple procedure is performed - a procedure for collecting primary data on the network: the statistics on the number of frames circulating in the network and packets of different protocols, port status hubs, switches and routers, etc. The next step is analysis, which is understood as more complex and intellectual process of information reflection collected at the stage of monitoring, comparing it with the data obtained before and development of hypotheses about possible causes of slow or unreliable network operation.

While intrusion detection system monitors the appearance of outside threats, the system of network monitoring performs network monitoring for problems caused by overloaded and / or failed servers, other devices or network connections. For example, in order to determine the state of the Web- server program, which performs monitoring, can periodically send an HTTP request to receive the page; for mail servers can be sent a test message via SMTP and obtained by IMAP or POP3. Failed requests (for example, in the case where the connection can not be established, it is terminated by a timeout, or when the message was not delivered) commonly cause reaction from the monitoring system. As the reaction can be:

sent an alarm signal to the system administrator;

automatically activated the system of protection against failures that temporarily withdraw problematic server from operation, as long as problem is not resolved and so on. (Junwei Huang et al. 2009)

A perfect tool for monitoring the network is a protocol analyzer. Protocol analyzer represents a specialized device, or personal computer, typically a laptop, Notebook, equipped with a special network card and appropriate software. Applicable network card and software must conform to the network technology (Ethernet, Token Ring, FDDI, and Fast Ethernet). The analyzer is connected to the network in the same way as a normal node. The difference is that the analyzer can receive all data packets transmitted over the network, while the ordinary station - only addressed to it. To this end, a network protocol analyzer adapter is transferred to " indiscriminate" capture - promiscuous mode. Software Analyzer consists of a core that supports the work of the network adapter and software decoding data link layer protocol, with which operates a network adapter and the most common upper-layer protocols such as IP, TCP, ftp, telnet, HTTP, IPX, NCP, NetBEUI , DECnet, etc. The composition of some analyzers can also include an expert system that allows the user to issue recommendations about which experiments should be carried out in this situation, what may mean certain measurements, how to eliminate some types of network failure. (Ed Tittel, 2002)

One of the important protocols is TCP and UDP. TCP and UDP use a protocol IP for data transmission. The IP protocol is responsible for transmitting packets to a destination with minimum cost, while TCP and UDP are used to prepare data to be sent, by dividing them into packets. The TCP provides a channel for bilateral connection between two correspondents using the two data streams. Before sending or receiving data TCP establishes a channel with the destination node. In order to channel could miss two data streams, TCP breaks the data into packets and ensures that the packages would have been delivered without errors and in the correct order. That's why applications that use TCP do not care about the correctness of the data. The use of TCP allows them to remain confident that the data will be passed successfully and completely. UDP is the simplest protocol for transmitting data packets. It simply adds a header to the data and sends them to their destination, without paying attention to whether there is a recipient node and whether it expects data. UDP does not guarantee that packets will be delivered in the same order as they were sent. If the packets are exchanged between two networks using different ways, they can be delivered in the wrong order. Caring for the correctness in this case rests on the application. However, for applications to which transfer speed is important, it is useful, despite the fact that some packets will be lost or their order is wrong. Almost all of the applications that use video and voice streams use UDP. (Achyut S. Godbole et al. 2003)

Protocol analyzers have some common characteristics:

Possibility (except packet capture) of measuring average traffic indicators in the segment of the local network in which a network adapter of analyzer is installed. Utilization rate of segment, matrix of cross traffic nodes, the number of good and bad frames passing through the segment are usually measured.

Ability to work with multiple agents, supplying the captured packets from different local network segments. These agents often interact with the protocol analyzer at their own application layer protocol different from SNMP or CMIP.

Availability of developed graphical interface that allows presenting the results of decoding packets with varying degrees of details.

Filtration of captured and displayed packets. Filtering conditions are set depending on the source and destination addresses, protocol type or values of certain fields of the packet. Package is either ignored or stored in the capture buffer. The use of filters considerably accelerates and simplifies the analysis because precludes capture or viewing unnecessary at this time packages.

Using triggers. Triggers are in this case specified by the administrator some conditions for beginning and cessation of the data capturing process from the network. Such conditions may include: time of day, length of the capture process, the appearance of certain values in data frames. Triggers can be used in conjunction with filters, allowing more detailed and subtle analyzing, as well as more productive spending of a limited amount of the capture buffer.

Multichannel capability. Some protocol analyzers allow simultaneous recording of packets from multiple network adapters that is convenient for comparing the processes taking place in different network segments.

Protocol analyzers' opportunities for network problems analysis are minimal at the physical level because all of the information they get from the standard network adapters. So they send and synthesize information of the physical layer, which gives them network adapter, and it largely depends on the type of network adapter. Some network adapters report more detailed data about frame errors and intensity of collisions in the segment, and some even do not transmit this information to the upper layers protocols, by which a protocol analyzer operates. (Ed Tittel, 2002)

Network traffic analysis is a way to obtain passwords and user IDs in the Internet. The analysis is carried out using special software - packet analyzer (sniffer), which intercepts all packets on the network segment and stands out among them those, in which user ID and password are transmitted. In many protocols, the data is transmitted in the open, not encrypted manner.

Analysis of network traffic allows the interception of data, transmitted by FTP and TELNET (user IDs and passwords), HTTP (Hypertext Transfer Protocol - Hypertext Transfer between WEB-server and browser, including entered ones by the user in the forms on the web data-Pages), SMTP, POP3, IMAP, NNTP (e-mail and conference) and IRC - Internet Relay Chat (online-conversations, chat). So can be intercepted passwords for access to e-mail systems from web - interface, credit card numbers when dealing with e-commerce systems and various personal information, the disclosure of which is undesirable.

Currently different exchange protocols have been developed that help protect the network connection and encrypt traffic. Unfortunately, they have not changed their old protocols and did not become the standard for each user. To a certain extent they have prevented the spread of existing in a number of countries export restrictions on strong cryptography tools. Because of this, the implementation of these protocols either have not embedded in the software, or significantly weakened (limited to a maximum length of the key), which led to their practical uselessness as codes could be opened within a reasonable time.

Analysis of network traffic allows:

1. First, examine the logic of distributed computing network that is to receive one-to-one correspondence of events occurring in the system and commands sent to each other by its objects at the time of occurrence of these events (if to pursue further analogy with the hacker tools, the analysis traffic in this case replaces the router). This is achieved through capturing and analyzing packets of exchange on the link layer. Knowledge of the logic of the distributed computing network allows at the practice implementing and simulating typical remote intrusions discussed in the following paragraphs with reference to specific distributed computing networks.
2. Second, network traffic analysis allows intercepting the flow of data, by which objects of distributed computing network are exchanged. Thus, the remote intrusion (attack) of this type obtains unauthorized access to the information exchanged between two network subscribers on the remote object. It should be noted that in this case there is no possibility of modifying the traffic and the analysis itself is possible only within a single network

segment. An example of intercepted information with the help of the typical network attack can serve a user name and password which are sent unencrypted over the network.

One of the security problems of distributed CN is the lack of identification and authentication of its remote from each other objects. The main difficulty lies in the implementation of the unique identification of messages transmitted between subjects and objects of interaction. Normally in the distributed CN this problem is solved as follows: in the process of creating a virtual channel objects of distributed CN share certain information that uniquely identifies the channel. Such an exchange is commonly called handshake. However, it should be noted that not always for connection of two remote sites a virtual channel is created. Practice shows that often, especially for service messages (e. g., from routers) transmission of single messages is used, which do not require confirmation. For addressing messages a network address is used that is unique for each object in the system. The network address can also be used to identify objects of distributed computing network (CN). However, the network address can be simply counterfeited and therefore to use it as the only means of identification of objects is not allowed. In the case when the distributed CN uses unstable algorithms of identification remote objects, typical distant attack is possible consisting in the transmission of the messages on behalf of any object or subject. At the same time, there are two varieties of the typical remote attack: attack at the established virtual channel, attack without a specific virtual channel.

In the case of established virtual connection attack will consist in conferring the rights of a trusted entity of interaction legally connected to the object of the system that allows an attacker to conduct work session with the object of a distributed system on behalf of a trusted entity. Implementation of remote attacks of this type usually consists in exchange packet transmission with attacking object on the target of attack on behalf of a trusted entity of interaction (the sent messages will be received by the system as correct). For the implementation of attack of this type it is necessary to overcome system of identification and message authentication, which in principle can use the checksum, computed using a public key and dynamically generated when setting the channel, random multi-bit packet and network addresses of stations. However, in practice, for example, Novell NetWare 3. 12-4. 1 OS for exchange packet identification uses two 8-bit counters - channel numbers and a packet number; in TCP for identification are used two 32-bit counters. As noted above, for service messages is often used transmission of single messages, which do not require confirmation, it is not required to create a virtual connection. Attack without a specific virtual connection is to transmit service messages on behalf of network control device, for example, on behalf of routers. The substitution of the trusted object is an active influence, committed to violate the confidentiality and integrity of information. This remote intrusion can be both intra-segment and inter-segment, as with feedback and without feedback from the attacked object and carried out at the network and transport layers of an OSI. (Xinwen Fu et al. 2003) Receiving control over the passing flow of information between objects, false object of computing network may use different methods of influencing the intercepted information. The introduction of false object in the distributed CN is the goal of many remote attacks, and poses a serious threat to security of CN. One of the intrusions, which can carry out a false object, is intercepting of information transmitted between subject and object of interaction. It is important to note that the fact of interception of the information (for example, files) is possible due to the fact that when performing certain file operations (read, copy, etc.) the contents of the files is transmitted over the network, and thus goes on a false object. The simplest way to implement interception is saving in files all received packets of exchange by false object. However, this method of the information interception is not sufficient informative. This is due to the fact that in packets of exchange except the data fields exist service fields, to which the attacker does not have immediate interest. Consequently, in order to obtain directly the transferred files it is necessary to carry out on the false object the dynamic semantic data flow analysis for its selection.

One of the features of any system, built on the basis of false object, is that it is able to modify the intercepted information. It should be noted that this is one of the ways to programmatically modify the flow of information between objects of distributed computing network from another object. After all, for the realization of information interception on the network it is not necessarily to attack the distributed computing network according to the scheme " false object". Attack, which analyzes network traffic, will be effective, allowing receiving all packets passing through the communication channel, but, in contrast to remote attack according to the scheme of " false object", it is not able to modify the information. One of the functions, which may have the impact system, built on the principle of " false object" is a modification of the data transmitted. As a result of selection of the intercepted information flow and its analysis, the system can detect the type of transferred files (executable or text). Accordingly, in the case of detection a text file or data file appears the ability to modify data passing through the false object. A particular threat this function represents for networks of handling confidential information. Another type of modification may be a modification of the transmitted code. False object, conducting a semantic analysis of the information passing through it, can allocate the executable code from the data stream. Therefore, in order to determine what is transmitted on the network - the code or data – it is necessary to use certain features peculiar to the implementation of network exchange in particular distributed CN or some particular features specific to types of executable files in the local operating system.

The false object allows not only modify, but also substitute the intercepted information. If modification of the information leads to its partial distortion, the substitution - to its complete change. When certain event appears on the network, which is controlled by false object, to one of the participants of exchange a prepared disinformation is sent. Thus, such disinformation depending on monitored event may be interpreted either as executable code or as data. Here is an example of this kind of misinformation. Suppose that a false object controls the event, which is connecting the user to the server. In this case, it waits, for example, running of the appropriate login program. If this program is on the server, then when it starts, an executable file is sent to the workstation. Instead of executing this action, the false entity sends to the workstation a code of written in advance special program - invader of passwords. This program performs the same action visually as the real login program, for example, asking for user name and password, after which obtained information are sent to the wrong object, for user appears error message. Thus, the user thinking that he incorrectly entered password (normally it is not displayed) runs the program again to connect to the system (at this time real one), and after second attempt receives access. The result of such an attack - user name and password saved on the wrong object. (Soon Tee Teoh et al. 1998)

References

Junwei Huang, Yinjie Chen, Zhen Ling, Kyungseok Choo, Xinwen Fu. (2009). A framework of network forensics and its application of locating suspects in wireless crime scene investigation. University of Massachusetts Lowell Press, 1-6.

Ed Tittel. (2002). Scene of the Cybercrime: Computer Forensics . Syngress Publishing, 302-307.

Achyut S. Godbole, Atul Kahate. (2003). Web Technologies: TCP/IP to Internet Application Architectures. Tata McGraw-Hill Publishing, 98-117.

Fanglu Guo, Tzi-cker Chiueh. (2008). Traffic Analysis: From Stateful Firewall to Network Intrusion Detection System. Stony Brook University Press, 2-8.

Xinwen Fu, Bryan Graham, Riccardo Bettati and Wei Zhao. (2003). Active Traffic Analysis Attacks and Countermeasures. Texas A&M University Press, 1-8.

Soon Tee Teoh, T. J. Jankun-Kelly, Kwan-Liu Ma, S. Felix Wu. (1998). Visual Data Analysis for Detecting Flaws and Intruders in Computer Network Systems. Mississippi State University Press, 1-10.