2012 International Conference on Computer Technology and Science (ICCTS 2012)
IPCSIT vol. 47 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V47.38

The Acquisition Design of the Network Behavior Data

WANG Jing-zhong, HU Liu-wu*

College of Information Engineering, North China University of Technology, Beijing 100144, China

Abstract: In this article, the definition and characteristic of network behavior is given, and also collect the network behavior data. The main task is to simulate the network behavior by the network data and capture their dangerous behaviors. The method of capture network behavior called WHCAPTURE is proposed. The experimental is designed to test and verify the performance of the WHCAPTURE program. The result of the experimental is analyzed and some conclusions are given in the end.

Keyword: Network Behavior, Network Data Description, Sniffer, Data Analysis

1. Introduction

Today, network have become an important infrastructure of building a harmonious society, it play an important role in communications, transportation, finance, emergency service, energy dispatch, electric power dispatch and so on. As network security techniques constant evolution and the meaning of the network security continue to extend, from the initial`s confidentiality of information to integrity, usability, manageability and non-repudiation, then to the security of the system service, many different safety prevention mechanism appear subsequently including firewall, intrusion detection system, virus prevention and so on in order to improve the network`s security.

However, as the improvement of the management and maintenance which make the whole information system become more complex and hard to realize. Some scattered, independent, single defense and external additional network security system have not ever to response the attack and destruction which have the characteristics of diversity, randomness, hidden, dissemination and so on. So to acquire the network behavior is the premise to realize the trusted network, on this basis to analysis, assess and forecast the network, find and handle the abnormal network behavior in time to make the whole network more security and reliable.

In current market, there are many network data capture tools, including TCPDUMP in Linux, Wires hark in Windows, they have their own characteristics, such as TCPDUMP, it can capture many data property items, but the content of the packets is show as hex which is hard to read; although the Wireshark can capture less property items of the data, its packets format and content is more easy to understand, even so, the content it showed is still hard to read. The common shortcomings of them is that they can not show the packets content completely, which make the analysis much hard, in view of this, we give a new method of network packets capture—WHCAPTURE.

2. Network Behavior Characteristics

2.1. Definition of Network Behavior

Network behavior is that people reply the Internet to do a completely new form of realistic behavioral activity; it can be divided into narrow and broad network behavior. Narrow network behavior: specifically refers to people do some things in cyberspace. Broad network behavior: not limited to narrow part, and at

* Corresponding author. Tel: 13001204464; fax: 01088803007
E-mail address: email:boyhlw@126.com

same time, it includes those closely related to the Internet and need to get help from and dependence on the Internet to do some things successfully.

The key of study the network behavior is to find the Internet abnormal behavior, the abnormal behavior is that use the computer to delete, change the function, data and application of the information system, or destruct the computer information, fraud, instigated, crime, sexual transmission in the net. At present time, we kwon some abnormal network behavior as hackers, Trojan, viruses, malicious e-mail, spam, congestion and so on, but to define the network behavior is not limit to this, because on the internet, a network behavior may be is normal, but if some behaviors come together, it may be a abnormal behavior. So to define and judge the network behavior need to be stricter.

2.2. The Description of Network Behavior Data

Network behavior analogy to people`s daily live behavior, it has its own rules, just like how to descript it to make it understood by people easily, therefore we need to define some network properties including number, time stamp, elapsed time(second), protocol type, source address, destination address, source port, destination port, data content, manual tagging(using for describing the possible attack), and so on, having this properties the data is clearer for people to study. A network behavior data record is given in the following:
<8, 10/May/2010, 16:29:50, 10, http, 192.168.1.100, 202.117.98.141, 4639, 80, 0>

3. The Method of NetworkBehavior Data Acquisition

3.1. The Principle of Sniffer

Data is transported by the unit of frame on the internet, data frame is formed by some parts, and different part has different function. Data go through different layer in TCP/IP architecture, every layer add some different message, after the data become a frame, it is formed by network driver, then it is transmitted into line by network adapter, when the data come to the destination host, it is handled through TCP/IP architecture in opposite direction, then the data is received.

Every computer`s network adapter MAC address is unique, usually, a net port only correspond two data frame, one is the destination address in the frame match its MAC address, the other is the broadcast frame. But if set the network adapter as promiscuous mode, it can capture all the message and frame on the network, analysis and diagnosis network or implement attack.

Because of its own character, sniffer originally should use for network management soft, is utilized by hacker to do some illegal data capture, this may be bring such endanger: capture network password, capture the access authority of a host, capture the user`s bank count and password, capture dedicate or secret information, pry on low protocol information, analyze network architecture.

3.2. The Designation of WHCAPRUE

WHCAPRUE is sniffer designed in Windows environment; it captures the head of the packet transmitted on the internet in order to be analyzed. It support filter of network layer, protocol, net or port. The programming flowchart is as follow.

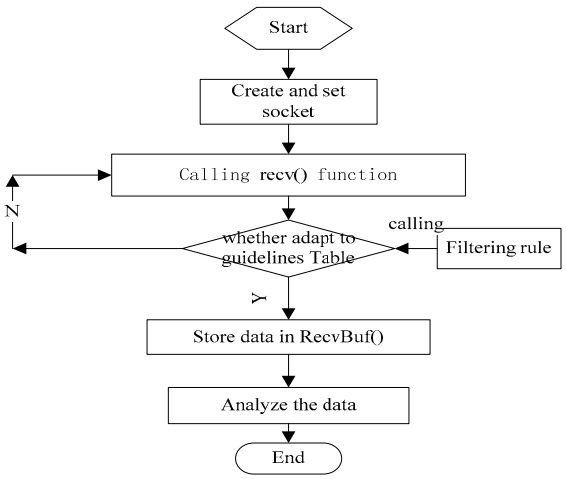

Figure1：WHCAPTURE programming flowchart)

From figure1 we know that if we want to realize WHCAPTRE, firstly should create and set a socket in order to function calling; then what need to do is capture the packet, it need to calling capture function library Libpcap during the capture, there is capture function and realize method in detail in the Libpcap, and during the process execution, it calling filter function to filter the packets arriving at network adapter in order to get rid of those useless or unusable to analysis packets and reduce abundance of packets` capture, improve the later analysis efficiency; store the packets captured on the internet for the later analysis calling; at last, analyze the packets captured and find out the abnormal behavior on the internet.

3.3. Create and Set Row Socket

From figure1 we know that we need to create and set raw in the program. After the socket is created, it need to be bided to a local address, then set SIO_RCVALL to control the code, at last enter into an endless loop to continue calling receive function to receive packets through local network adapter. The socket program only respond to those the same MAC address or broadcast frame, so the network adapter`s work mode should be set to promiscuous mode, only in this mode can it accept all the packets, this is the first step to realize capture.

During the creation and setting socket, some functions are used as follow:

1>Create raw socket:

Sock=socket(AF_INET,SOCK_RAW, IPPROTO_RAW);

2>Set the head option of IP to handle the IP head:

setsockopt(sock,IPPROTO_IP, IP_HDRINCL, (char*)&flag, sizeof(flag);

3>Bind the socket to the local network adapter:

Bind(sock,(PSOCKADDR)&ADDR_in, sizeof(addr_in)；

4>Set raw socket to SIO_RCVALL in order to receive all IP packets:

Ioctlsocket(sock,SIO_RCVALL, &dwValue)

3.4. The Acquisition of Packet

It is time to enter the part of acquisition packet after finishing setting raw socket, to acquisition packet is still through socket function, but at this time it is not only to capture data information, is to capture data information including IP head or TCP head, this is the almost original state of the data transmitted on the internet. Through repeated calls of recv () function on network adapter to receive data

Because the number of the packet on the net is out of count, if not filter the captured packet, there will be many uselessness packets which will add pressure to the equipment and difficulty to analysis. It needs a filtering rule table during the filtration, this table is the behavior recorded in the database of network behaviour.

3.5. Data Analysis and Extraction of Network Behavior

This part is to Extract data from catch to analyze, the main content to be analyzed is data`s property and packet content introduced above. Extract network behavior which is more familiarly to people through

the analysis, although we analyze by program we need to analyze some packet by manual sometime, such as illegal attacker try to get user`s count and password, maybe every packet is normal, but the behavior is done for three time, we can determine it as an abnormal behavior.

At this point, we can capture behavior data through sniffer tool WHCAPTURE, filter out some irrelevant packets, gain what we want, improve the efficiency of the capture and analyze the packet to extract network behavior, provide a basis for further analysis.

4. Experimental Verification and Test

After designing the sniffer of WHCAPTURE, we can test its original function through experimental. Experimental environment is a network security laboratory. Equipment: ten personal computers, four servers, two routers, a gateway, some virtual machines, a network attack and defense platform, a network vulnerability scanning platform and some host in the internet.

Experiment: open all the equipment in this experimental, run WHCAPTURE on a host to monitoring, the experiment start from 8:00 AM to 12:00 PM, statistics once per hour to monitor the running state of the LAN, requiring person operate the system just like usual, network vulnerability scanning platform operate normally, at one time point to use network attack and defense platform to attack the LAN.

After the experiment, stop the WHCAPTURE, store the result of the experiment and analyze it. Table1 show the statistics data of the experiment.

Table1:the data statistics in different time interval

data	Time interval	Normal data number	Abnormal data number	Total number	Abnormal rate
2010/8/20	8:00-9:00	2646	0	2646	0
010/8/20	9:00-10:00	7421	1265	8686	14.56%
2010/8/20	10:00-11:00	6886	4215	11101	37.97%
2010/8/20	11:00-12:00	15446	7652	23098	33.13%
2010/8/20	12:00-13:00	6550	3554	10104	35.17%
2010/8/20	13:00-14:00	5372	3428	8800	38.95
2010/8/20	14:00-15:00	6319	3483	9802	35.53%
2010/8/20	15:00-16:00	4273	4421	8694	50.85%
2010/8/20	16:00-17:00	3816	4012	7828	51.25%
2010/8/20	17:00-18:00	4828	1321	6149	21.48%
2010/8/20	8:00-19:00	2462	39	2501	1.56%
2010/8/20	19:00-20:00	1695	36	1731	2.08%
2010/8/20	20:00-21:00	2205	34	2239	1.52%
2010/8/20	21:00-22:00	2395	36	2431	1.48%
2010/8/20	22:00-23:00	1252	1126	2378	47.35%
2010/8/20	23:00-00:00	1804	1231	3035	40.56

Combination of the above data analysis shows that in different time interval the amount of network data and the abnormal network behavior rate, especially from 8:00 to 9:00, the abnormal behaviors are few, this means in the interval the net is relatively safe, from 18:00 to 21:00 is also relatively safe, but from 9:00 to 17:00, the abnormal rat is high, this means many people are using computer in this interval, the amount of data is more than other time interval, abnormal behavior is more easily appear especially from 15:00 to 17:00, although the abnormal behavior is not means net attack, combination of the above analysis can give reference value to network management, that to say when should pay more attention to the security of the network and when should slightly relax.

As in a unit time especially in a LAN, sometime the appear rate of the abnormal behavior is small, in many cases it is shielded outside the LAN by the Intrusion Detection System before entering, so in this experimental we use network attack and defense system to select some attack to inject some abnormal behavior to the LAN, this can detect the usefulness of the WHCAPTURE, and at the same time, abnormal behavior not equal attack, so we need further study of this issue, but the basic function of the program have been proved by the experimental.

5. Conclusion

In this study, we realize how to capture packet and simply analyze the data, this will useful to the monitoring of the network, improve the security of the net and good for people to enjoy the online world harmony. Of course, our study dose not over yet, the whole system still have some problem need to be solved, such as analyze the network behavior data more in-depth, capture more abnormal behavior to perfect our network behavior database, increase the implementation of the whole system to discover the abnormal behavior in time, realize automatic or semi-analytical of the packet and so on. All these issues need to be further studied.

6. Acknowledgment

This works supported by the Beijing Education Committee project (NO. KZ2010009008, NO.KM201010009004) National Natural Science Foundation of China (NO. 60972077).

7. References

[1] Richard P. Lippmann, David J. Fried, et al. Evaluating Intrusion Detection Systems: The 1998 DARPA Off-line Intrusion Detection Evaluation [J].IEEE, 1999.

[2] Li-Ping Wang, Na An, Xiao-Nan Wu, Ding-Yi Fang. Intrusion detection system behavior pattern mining[J]. Communications, 2004-7:168~175.

[3] Yi Li. Network behavior of a brief analysis of the concept of network sociology[J]. Lanzhou University.2006-9:48~53.

[4] Xian-Liang Wang. Computer network security and prevention of common attacks[J]. Information and Computer.2010:94.

[5] Qiang Ran, Jing-Xiong Huang, Yan-Yong Xu. Implementation of the core principles of sniffer [J]. Computer Security. 2008-7:90~92.

[6] Ya Yu, Jun Li. NDIS intermediate layer based on the design and implementation of sniffer [J]. Hubei Institute for Nationalities. 2006-12:388~390.

[7] Chang-Bing Xu, Li-fen Zhao. Principle and Application sniffer [J]. Information Technology and Information. 2004 3: 18 ~ 20.

[8] Chuang Lin, Xu-Hai Peng. Trusted Network [J]. Computers. 2005, Vol. 28 No. 5:751-758.

[9] Chuang Lin, Feng-Yuan Ren. Controllable generation of reliable and scalable Internet [J]. Software. 2004, Vol.15, o.12:1815-1821.