TELKOMNIKA, Vol. 11, No. 10, October 2013, pp. 5684 ~ 5693
ISSN: 2302-4046

A Method for Detecting and Blocking Instant Messaging Software

Hao Zhang*[1], Guangli Xu[1], Jiongzhao Yang[1], Jianmin Li[2]
[1]Qinggong College, Hebei United University, Tangshan 063000, Hebei, China
[2] Institutes of Electronics, Chinese Academy of Sciences, Beijing 100000, China
*Corresponding author, e-mail: mox012@163.com

Abstract

Instant messaging software, as a convenient network communication tool, is becoming more and more popular. At the same time, it also brings risks in security of local area network (LAN). Through studying in typical instant messaging software and detected by the combination of misuse detection and protocol analysis, an architecture of detecting and blocking mechanism of instant messaging software is proposed in this paper and its prototype system is achieved on Windows platform. This new system effectively solves the problems that the efficiency of traditional firewall application layer data filtering is low and the firewall cannot dynamically adjust the filtering rules, providing a good application value for the protection of the security of local area network.

Keywords*: Instant Messaging Software, Protocol Analysis, Intrusion Detection, Blockade*

1. Introduction

In recent years, with the popularity of the Internet, people don't need to leave home to get a wealth of information resources and access to the global network system. However, with the increase of information sharing and business processing on the network, network security is becoming more and more crucial. Network intrusion events occur frequently [1], and people are often faced with online security problems. Instant messaging software brings new security problems when it brings people lots of convenience. At present, the main problems instant messaging software faces are as follows [2]: first, it is dangerous to the safety of the state and society. There is new opportunity for online criminals due to the popularity and low cost of communication software. They can easily use instant messaging software, and talk about illegal content via the Internet, vent dissatisfaction with society, spread disinformation, illegal information and so on. Second, it is vulnerable to be attacked by viruses, Trojans, and other malicious code. Currently in popular instant messaging software, there are many design flows which is easy for hackers to exploit with viruses. A lot of instant messaging software itself does not provide encryption mechanisms. Besides, script defects, and the problem of identity theft are the threat to personal security. Thirdly, it is lack of international standards. Most of instant messaging software still cannot achieve communication protocol yet this is not conducive to detect.

At present, the firewall is one of the effective methods to prevent network attacks; it can protect the internal network from the outside threats of intrusion. Intrusion detection [3, 4, 5] is considered as the second gate to the firewall. How to detect intrusion and how to react after intrusion has always been the focus. Intrusion detection technology is a new kind of computer network security technology which has emerged in recent years. The purpose is to provide real-time intrusion detection and take corresponding protective measures, such as logging, disconnected from a network and so on. As a kind of detection and controlling technology, it plays a very important role in network security. In spite of immature intrusion detection technology without a full-fledged defense, it plays a significant role in the whole security system.

Some foreign network security companies have introduced monitoring software for instant messaging programs. In the domestic market at present, there are various kinds of detecting software, such as Emexur, LaneCat, etc [6]. For reasons of safety and performance, it has been inconvenient to introduce the foreign products. Domestic research focuses on instant

Received April 27, 2013; Revised June 29, 2013; Accepted July 14, 2013

messaging software in client/server mode and P2P mode, not communication mode. A comprehensive analysis of network architecture of instant messaging software has not been conducted; it has only been partly studied. Duan Bing [7] has analyzed instant messaging software QQ protocol, without the research on QQ in the communication process when using HTTP tunnel technology. He only makes a vivid analysis on tencent QQ instant messaging software. Yet he has not been proposed corresponding detecting method. Fang Jian [8] analyzes and studies the communication protocols, Google Talk on MSN, Yahoo Messenger, ICQ, analyses and compares the old and the new protocol, but is in lack of instant messaging software of network architecture and analysis and research of the communication technology. Domestic products cannot fully meet the needs of function and operation, so that in-depth analysis of the instant messaging software models and protocols is needed and these products can be designed to adapt to the special needs of the instant messaging software detecting and blocking systems.

2. Network Architecture and Communication Mode of Instant Messaging Software

2.1. Network Architecture of Instant Messaging Software

There are two main types of network architecture about instant messaging software, the first kind is client/server mode, in this kind, different client send messages through server. MSN, QQ, Sina UC, Yahoo Messenger is using this mode to send messages. Another kind is point to point pattern, which is using the P2P technology; customer sends information to others via UDP or TCP protocol [9] but not through the server. Instant messaging software client adopts different ways of communication according to the different network environment. When burden of communication software server is too big, the communication between different clients is in point to point mode, while the network is not stable and the packet lost too much, the communication between client and server is client/server mode.

In recent years, the HTTP tunnel technology is widely used in instant messaging software; it can make instant messaging software bypass the firewall and avoid being blocked by port. The encapsulation of data packet at the two ends of the firewall is required by the protocol type of the firewall or port, and then the packet is sent from the firewall. When encapsulated packet reach its destination, the encapsulation packet is restored, and the corresponding program will process the data.

(1) Client/Server mode

The client of instant messaging software connect to the server through the Internet, the client information are forwarded by the server. The structure of this mode is shown in Figure 1.

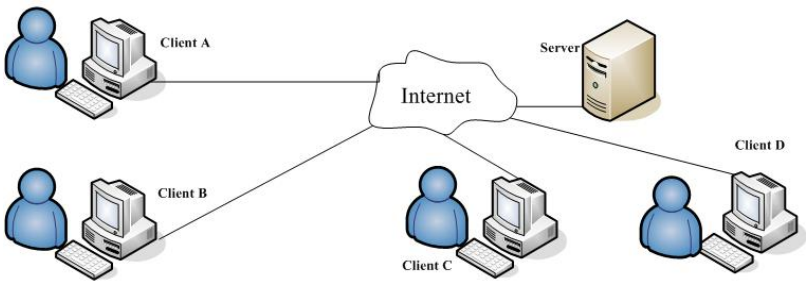

Figure 1. The client/server mode of instant messaging software network structure

(2) Point-to-point mode

After establishing the connection between the instant messaging software client and server, the corresponding initial state information will be obtained, such as other client IP addresses and port number. Then each client can chat or transfer files with UDP or TCP. The structure of this mode is shown in Figure 2.

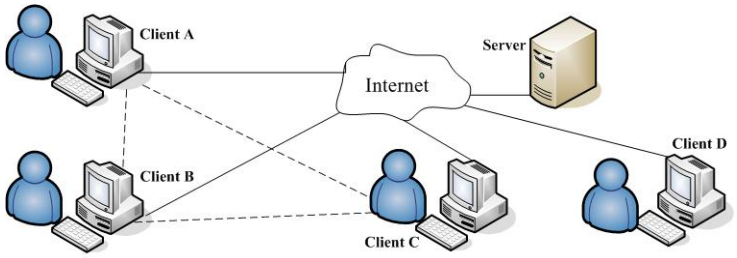

Figure 2. The P2P mode of instant messaging software network structure

2.2. The Communication Mode of Instant Messaging Software

The clients of the instant messaging software communicate with server through UDP mode or other clients. When UDP communication is failure, the clients automatically choose to use TCP to communicate with the server and client. Through the port 80 of TCP protocol is called HTTP tunnel communication way, in this way the messages can escape the detection of the firewall. Of course, the client also use the port 443 of TCP with communications, QQ members usually use this port. Instant messaging software client also supports agent login, such as using the HTTP proxy and SOCKS5 agent.

Before transporting information, the latest version of the instant messaging software has been encrypted. When the client and the server start to communicate, they will exchange key, and encrypt the data that is to be sent, and decrypt the data that has been received. With the development of network technology, the encryption of the instant messaging software algorithm is becoming more and more complicated.

Instant messaging software has hundreds or even thousands of servers, and the quantity has been still increasing. Instant messaging software can log a different server every time to communicate. If QQ have specialized distribution of server to provide forwarding the address, when users login QQ, distributed server will choose a few closer from the QQ to forward the IP address of the server, then QQ client select a log in randomly, if the login fails, change other forwarding server address to log in again. In this way, the IP address of the QQ client login server is different usually. A number of proxy server often be used on the network, the proxy server IP address also changes frequently, but instant messaging software is also able to use the proxy server to log in.

3. Instant Messaging Software Detecting Methods

Firewall has the congenital weakness of detecting application layer data, which is the detection efficiency is low, influence the normal speed of the network. While intrusion detection can find unsafe behavior instantly in the Internet do not affect the normal velocity of the network, and has high detection efficiency. So the use of intrusion detection system to detect the instant messaging software has higher efficiency than the firewall. Compared the advantages and disadvantages of various technologies in the intrusion detection system, using combined misuse detection and protocol analysis method can better to complete the analysis of the application layer data.

3.1. Analysis of Instant Messaging Software Environment

Instant messaging software company is in business operations way, all has their software communication protocol in order to benefit. Most of these protocols are different and even not public. So it is necessary to analyze mainstream instant messenger software communication protocol. Instant messaging software protocol analysis environment is shown in figure 3.

The hardware environment is included three PCs, a Ethernet hub, and a gateway. A local area network (LAN) is consists of PC A and B with a hub, and C is the PC in the Internet.

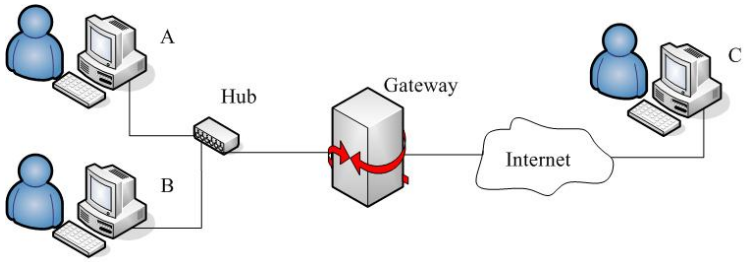

Figure 3. The protocol analysis environment

Software environment includes QQ 2008, MSN instant messaging software, Kaspersky Internet Security 7.0 and WinPcap 4.0.1 and network protocol analysis tool Ethereal (Ethereal 0.99.0). All clients are using Windows XP SP3 operating system. On the client A uses Ethereal, the captured data packets in the ethereal network adapter is set to promiscuous mode, and in three clients shut down other applications that using the network. Client A can capture and record all transmission of packets within small internal local area network (LAN). Through setting the Ethereal filtering rules to capture and record the concerned packet so that to rule out other packets. QQ, MSN and Kaspersky Internet Security 7.0 trial version are installed on the client B and C. With KIS 7.0's built-in firewall blocking test information and the necessary port information of Instant messaging software can be obtained.

3.2. Approach of the Detection and Blockade

(1) Keyword extraction method

Instant messaging software has its fixed communication data formats; it can conclude the general protocol format through the analysis of a large number of data packets. The transport layer protocols are TCP and UDP, analyzing the two kinds of protocol in application layer data, and summarizing in statistics way, instant messaging software protocol format will be gotten.

Through the above experimental environment, which can capture all the transmission of packets within small internal LAN on the client A, and it can use Kaspersky Internet Security firewall on client B banned all TCP connection, the instant messaging software can only through the UDP protocol to communicate, to analysis and summary the UDP that be captured, and to catch package many times. After getting the format of UDP about instant messaging software, using the same method to research instant messaging software communication protocol, the TCP format will be obtained.

(2) Keyword verification method

The client version is different, capture the packets are also different. It needs to verify this instant messaging software communication protocol. On the client A capture all the packets, use Ethereal software to view the application layer data, to pick up the remote IP address and port of the communication first protocol packet, using Kaspersky Internet Security software on the client B to blockade the remote IP address and port, then look at whether instant messaging software on the client B can communication, if it continues to communicate, which means the protocol is not correct, or it represents the protocol is right.

(3) Protocol analysis technology

Protocol analysis's function is to distinguish the packet type, which use the corresponding data analysis program to detect packets. Putting all of the protocols in a protocol tree, such as it can be represented in a binary tree (as shown in figure 4), every node in the tree corresponds to a specific protocol. A network packet analysis is a path from the root to a leaf node. The custom nodes that can be added to in the tree structure, protocol analysis function can be realized in the process of maintenance and configuration of the tree dynamically. Protocol analysis is the third generation of detection technique of attack in intrusion detection system, it has the advantage of parsing command string, detect fragments attack and protocol confirmed, reduce the rate of false positives, improve the detection performance, etc.

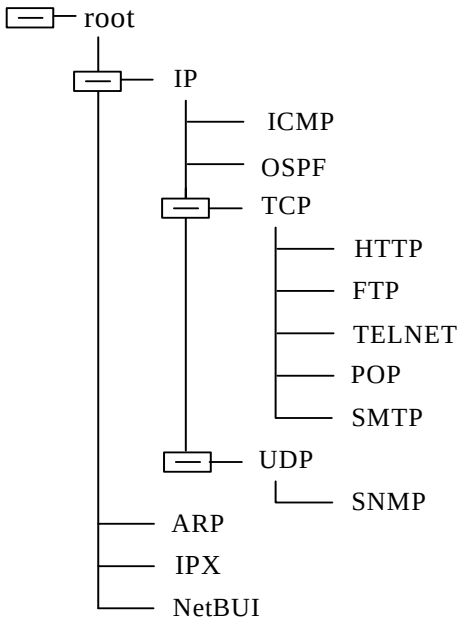

Figure 4. Schematic diagram of protocol tree

3.3. Analysis of the Communication Protocol Format

In accordance with the research environment and methods, the communication protocol format of instant messaging software QQ with UDP and TCP protocol can be represented as follows. As shown in figure 5 and 6.

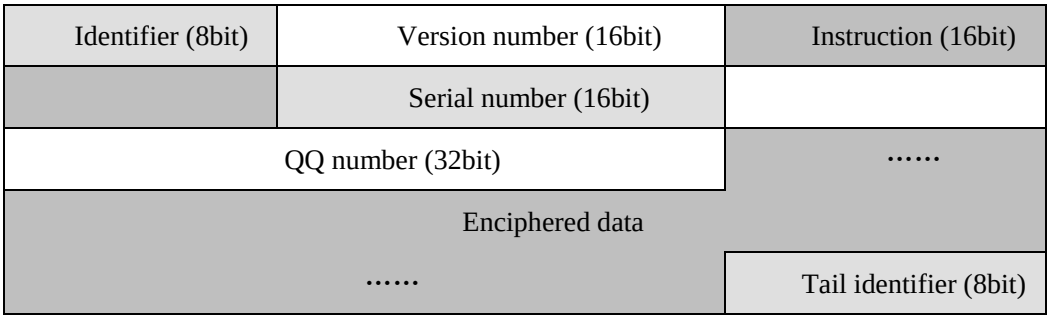

Figure 5. QQ protocol format of UDP package

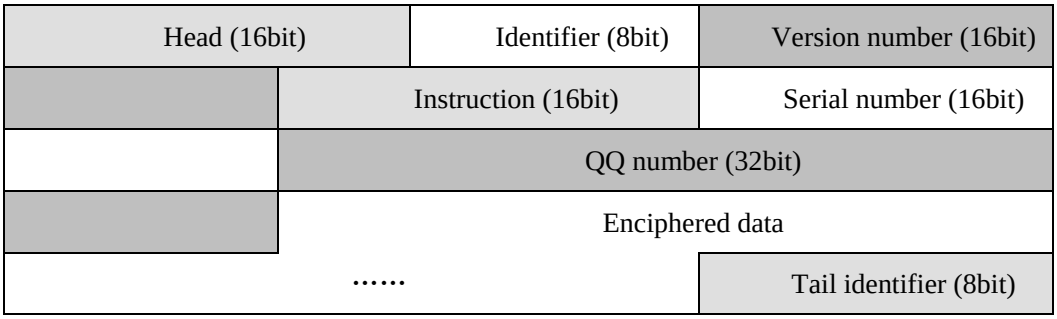

Figure 6. QQ protocol format of TCP package

4. Development for Detecting and Blockade System

4.1. The Architecture of the Instant Messaging Software Detecting and Blockade System

The architecture of the instant messaging software detecting and blockade system is shown in figure 7. This system is consists of two parts, the left side of the dotted line frame referred detection module, which is installed on the host in the LAN to detect part of the instant messaging software, the dotted line frame on the right side box is called block module, which is set in the import and export of local area network as a software firewall deployment. Dotted box contained is each part of the functional modules, the two parts through TCP to communicate with each other.

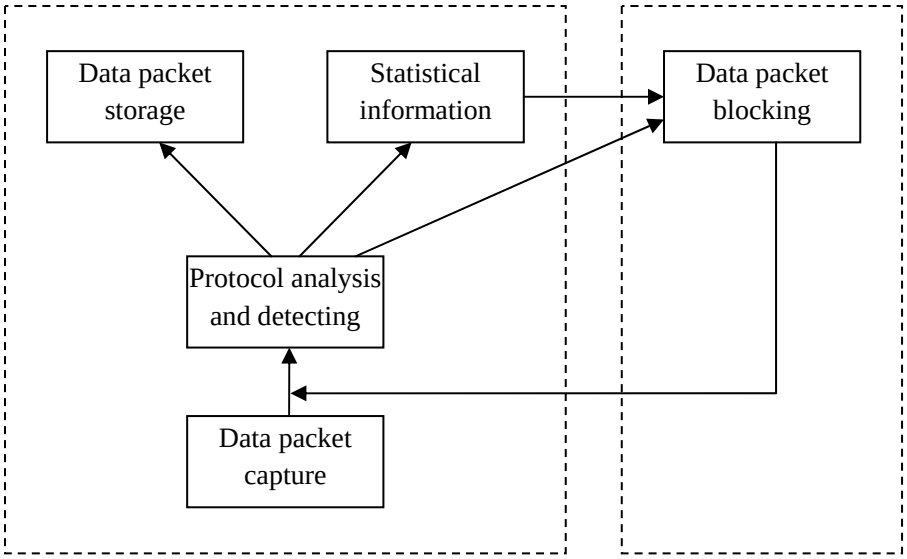

Figure 7. The system architecture

(1) Packet capture module

In this module, all the data packet can be captured in the case of does not affect the network performance within the local area network, and sent the captured data to the protocol analysis and detecting module.

(2) Protocol analysis and detecting module

In this module, we can use protocol analysis and intrusion detection technology to analysis the captured packet in the capture module, and analysis the DNS packets that was sent by block module at the same time, and pass all packets that conform to the rule and DNS packet to the packet storage module, the results meets the detection rules packet will be sent to statistical information module, the priority processing results also need to be transmitted to the packet blocking module. Part of the rule in detection module is loaded from the config file.

(3) Packet storage module

In this module, the detected packet can be stored comply with certain format; the system will store the data packets by extension "pcap" format.

(4) Statistical information module

To analysis and statistic relevant content of the data packets that has been captured in this module, the information includes instant messaging software, remote IP address and port, data flow, time and so on. After being analysed, the statistical results need to be sent the information to the instant messaging software block module. Another function of statistical information module is to display the received data in the system detecting module interface.

(5) Packet blocking module

This module has the function of firewall, some received information such as the IP address and port can be updated to blockade rule base, and the relevant DNS packets are sent

to the protocol analysis and detecting module. Packet blocking module consists of packet filters program and blocking rule base configuration.

4.2. Development Environment of the System

The detection system of the instant messaging software is running in Windows XP operating system, and it was developed using the C language and the Microsoft foundation class library MFC under the environment of Microsoft Visual Studio 2005, using WinPcap dynamic link libraries Wpcap.dll and Packet.dll to capture network packet. Instant messaging software blockade system is running in Windows Server 2003, using Microsoft Windows Server 2003 Server Pack 1 Driver Development Kit (DDK), and Microsoft Visual c++ 6.0 development environments and Microsoft Debugging Tools for Windows (WinDbg.exe) to debug the program in the Windows Server 2003. System development and runtime environment is shown in figure 8.

In figure 8, the operating system of three clients is Windows XP, in which the client A is running system detection module, client B and C install instant messaging software MSN and QQ, Windows Server 2003 Server is installed on the sever to run the blockade module.

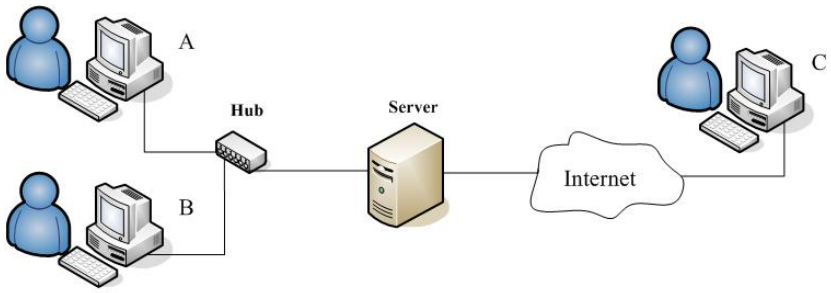

Figure 8. Network environment of detecting and blocking system

In paper [10], packet capture model has been introduced; the block module will be discussed in the following. Block module is mainly complete the blockade of instant messaging software, which means filtering the packet, the middle layer of the NDIS driver can filter all of the data packets, and the data packets that matches the blocking rule base will be discarded. Writing process of the middle layer of the NDIS driver, the method of filter packets and block matching algorithm of rule base will be discussed respectively in this section.

NDIS middle layer driver is in the central of the transmission driver and miniport driver; it transmitted driver to the upper NDIS and provided a group callback function, and provided to the lower NDIS miniport driver a set of protocol callback function.

The following process is writing the middle layer of the NDIS driver:

(1) The NdisMinitializeWrapper() fuction is called by the main entry function DirverEntry() in NDIS driver to register entrance of output function set, which notifying the NDIS that a new miniport driver is initialized, and get the handle called NdisWrapperHandle_MP which is the type of NDIS_HANDLE;

(2) Using the handle NdisWrapperHandle_MP which is gotten from the first step to call the function NdisIMRegisterLayeredMiniport() registering a set of callback function for the NDIS middle driver layer, so that the upper protocol will regard the middle layer drivers as network card, and through the NDIS library calls the callback function;

(3) Call NdisRegisterProtocol () function, and register a callback function that named Protocol for the NDIS middle layer, so that the lower card will regard the middle layer driver as a protocol, and through the NDIS library to call these functions;

(4) When the operating system found NIC, NDIS called the function ProtocolAdapterBind_MP() that registered by middle layer driver to support plug and play function, this function calls the function NdisOpenAdapt() to open the network adapter initialization, and binds the upper protocol that has been called and network card driver or the NDIS middle layer driver;

(5) The function MiniportSend () or MiniportSendPackets() that have been rgistered in step (2) is to deal with the upper protocol packets, the function ProtocolReceivePacket() and ProtocolReceive() that have been registered in step (3) is to deal with packets which received by network card; setting the filter rules, or calling the packet by using the filter function.

(6) Packet filters can be judged in these four functions independently, and can write a separate filter function for packet filtering.

4.3. Packet filtering method

For the packets that are sent by upper application, using the registration function MiniportSend() or MiniportSendPackets() to filter. This function implements the filter by sending or not sending the packet to the next layer, then through the function NdisMSendComplete() to tell the upper that packets have been sent. Lower level driver call the fuction ProtocolReceivePacket() and ProtocolReceive() to handle the received packets, as long as the two functions don't transfer packets to the upper, the upper application doesn't know the packet has already been discarded.

The four filter function only inspect for TCP/IP protocol's first data in order to improve the speed and efficiency of the driverof NDIS middle layer.

The driver of NDIS middle layer the block rule base is deposited according to the order, so you can use binary search method to check whether the IP address of the packet match block rules in the library. For packets received from the underlying, it is to test the source IP address, for packets to be sent, it is to make matching test for the destination IP address and the IP filtering rules list. If the match is successful, it will discard the packet. The program is as follows:

```
for (lowPos = 0, highPos = pAddrArr->NumberElements - 1; lowPos <= highPos;
{
   midPos = (lowPos + highPos)/2;
   if (IPAddr == pAddrArr -> IPAddrArray[midPos])
   {
      *pBDecision = TRUE;
      break;
   }
   if (IPAddr < pAddrArr -> IPAddrArray[midPos])     highPos = midPos - 1;

   else
      lowPos = midPos + 1;
}
```

5. The Linkage of Blockade and Detecting

Detection module sends the updated rule to the block module through TCP, configuration program block rule base in block module through WMI interface to update the driver of NDIS middle layer.

Windows Management Instrumentation (WMI) is a specification and infrastructure; it can access, configure, manage, and monitor all resources of Windows. In this system, user programs interact by the the driver of NDIS middle layer and WMI interface. User program based on WMI can control local and remote driver instances, and it can also get statistics imformation. By calling the function NdisAcquireReadWriteLock() to obtain a lock that can read and write driver thread of shared resources, and then through the function NdisMoveMemory() to copy the array in rule library to the driver of the NDIS middle layer. At last, unlock shared resource of the driver thread through function NdisReleaseReadWriteLock().

6. Experimental Results and Discussion

The driver of NDIS middle layer debug environment consists of two computers in LAN, one of the clients (A or B in figure 8) as the host is running Windows XP system and installing WinDbg and instant messaging software detecting program. The target machine is the sever in figure 8 runs Windows Server 2003 Server system, and installs the driver of NDIS middle layer and the blocking rule base configuration program.

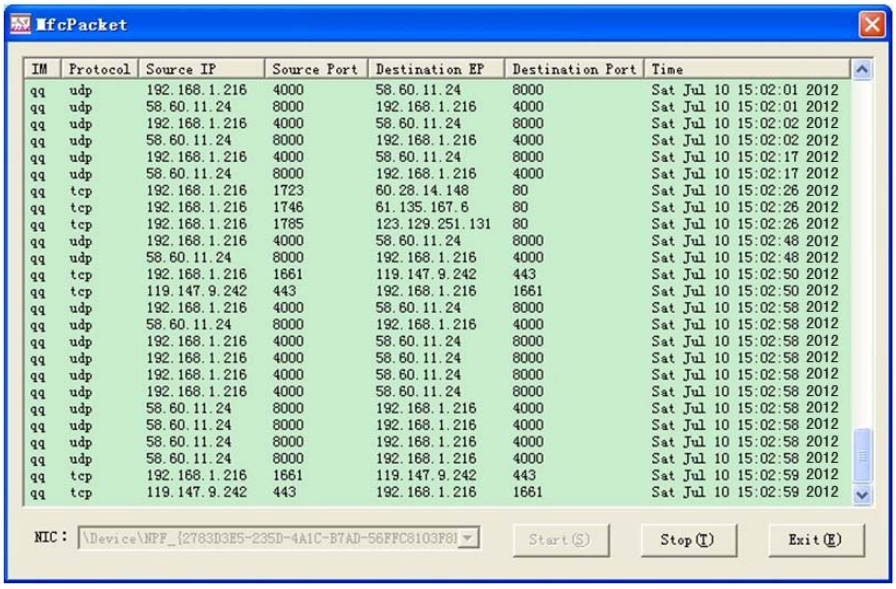

Figure 9. The detection results

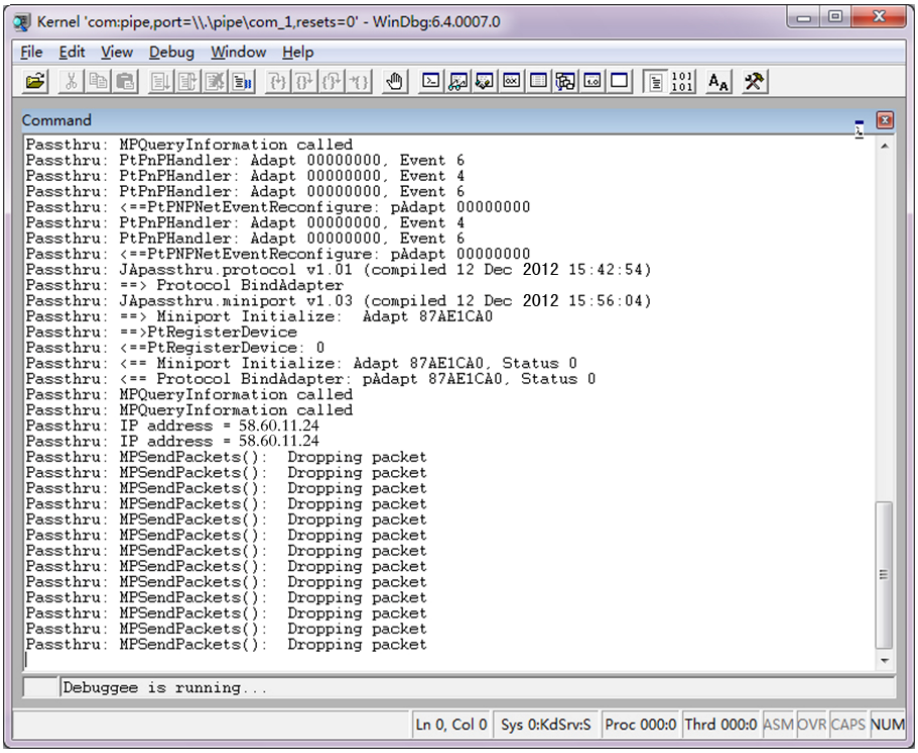

Figure 10. Dropping packet of Intermediate driver

Instant messaging software running is detected by detection system in the local area network is shown as Figure 9, the IP address of instant messaging software on the server is 58.60.11.24, and the port is 8000. IP address is transmitted to the rule configuration program of target machine through TCP, and filtering rules updates the driver of NDIS middle layer in blockade rule base, the output of the debug version on middle layer driver through WinDbg program can be displayed is shown as figure 10, we can see in the figure that the driver of

middle layer makes processing of packet loss whose address is 58.60.11.24. At this time, the client which runs the instant messenger software on the client shows that instant messaging software has been dropped. The above data shows that instant messaging software detecting and blocking system is able to complete the detection for instant messaging software of local area network (LAN), and carries on the block function.

7. Conclusion

Instant messaging software brings threat to LAN environment such as some enterprises and institutions, companies and families. Based on the study of network architecture and communication protocol, the thesis introduces the detection technology inspection on instant messaging software. With the combined misuse detection and protocol analysis method, it tests the software communication protocol. This method of communication protocol for testing is suitable for most of the instant messaging software. System block modules use the middle tier of the NDIS driver in Windows Server 2003 platform technology implementation. Detection module and blockade the linkage of the module by WMI interface implementation. The system put the detection rules library and blockade inventory in different configuration file, which at the same time realized detection and blockade of a variety of instant messaging software, so that it effectively safeguards the security of local area network (LAN).

References

[1] Mohammadi, Mehdi. New class-dependent feature transformation for intrusion detection systems. *Security and Communication Networks.* 2012; 5(12): 1296-1311.
[2] Wang Xiaoqiang. Study on genetic algorithm optimization for support vector machine in network intrusion detection. *Advances in Information Sciences and Service Sciences.* 2012; 4(2): 282-288.
[3] Hu Weihua. Anides: Agent-based network intrusion detection expert system. *International Review on Computers and Software*. 2012; 7(4): 1453-1457.
[4] Chen, Rung-Ching. An isolation intrusion detection system for hierarchical wireless sensor networks. *Journal of Networks.* 2010; 5(3): 335-342.
[5] Hubballi, Neminath. Network specific false alarm reduction in intrusion detection system. *Security and Communication Networks*. 2011; 4(11): 1339-1349.
[6] Xu, Jing. Intrusion detection using continuous time bayesian networks. *Journal of Artificial Intelligence Research*. 2010; 39(1): 745-774.
[7] Duan Bing. Study on the Secure Communication Technology of Skype and QQ. Information *Security and Communications Privacy.* 2007; 5(11): 58-60.
[8] Fang Jian. Based on the Real-time Communication of Intrusion Detection System Design. *Computer Knowledge and Technology*. 2012; 8(18): 4401-4403.
[9] Thinh, Tran Ngoc. High performance TCP reassembly for network intrusion detection system. *International Review on Computers and Software*. 2012; 7(6): 3320-3325.
[10] Zhang Hao. Research on detection of instant messaging software. International Symposium on Information and Automation. Guangzhou. 2010; 664-669.