Design and Implementation of LAN-sensitive Information Interception and Analysis System

Lin Shaofeng
Department of Information Safety
Xi'an Communications Institute
Xi'an China , 710106
e-mail: 448537556@qq.com

Fan Linna
Department of Information Safety
Xi'an Communications Institute
Xi'an China , 710106
e-mail: fanlinnafanlinna@163.com

Sun Weifeng
Department of Information Safety
Xi'an Communications Institute
Xi'an China , 710106
e-mail: sunweifengswf@yahoo.com.cn

Wang Hua
Xi'an Interception center of
The state administration of radio film television
Xi'an China , 710101
e-mail: wanghua-2009.03@163.com

***Abstract*—The LAN usually hides internal network structure by NAT to share a public IP address in the internal network, and thus it is hard to locate the source host precisely distributing sensitive information for a large-scale information monitoring system by analyzing the intercepted packets. So it is hard to fulfill monitoring work efficiently. This paper puts forward a scheme to intercept and analyze the sensitive information in the LAN environment. It studies the ARP spoofing principle and the sniffer technology based on WINPCAP. The scheme includes 7 modules named NIC capture module, packet filtering module and so on. And it achieves sensitive information filtering and matching by the configured rules, such as "keywords", "URL", "QQ number" and so on. The scheme provides a solution for tracking the source host leaking sensitive information within the LAN.**

Keywords-Network Security Monitor*; *Protocol Analysis; ARP Spoof; WinPcap; TCP/IP

I. INTRODUCTION

The key evidence for designing the LAN-sensitive information interception and analysis system is the difference of addressing between the Internet and LAN[1]. The Internet finds a destination host by its public IP address. Whereas the internal LAN is by the MAC address, and usually the LAN adopts NAT to share one public IP address. The Internet security monitoring system can visit the public Internet network, get sensitive data packets, and locate the public IP address of one LAN or one host, but it can't accurately locate the host sending the sensitive information behind a LAN using NAT. It is necessary to develop a LAN sensitive information interception and analysis system to resolve this problem and eliminate the monitoring blind spots of Internet security monitoring system. It is of great significance to monitor sensitive information distribution behavior in LAN.

This paper puts forward one applying topology of the system and the principle to implement the system. By developing ARP spoofing, packet capture, packet parsing and the keyword matching modules, the system can audit and locate the source host precisely in LAN distributing sensitive information.

II. SYSTEM DESIGNING

A. System topology

The general topology of LAN is shown in Figure 1. There are two methods to monitor all hosts in the LAN. One is bypass monitoring mode and the other is random monitoring mode. Bypass monitoring is to monitor any host in a sub-LAN by a mirroring port in the core switch. If the monitor host's performance is good enough, it can monitor thousands of computers in the entire LAN. The shortcoming is that the core switch or router may not configure mirroring port, or there is no reserved port left. It needs complicated operations, and it is hard to deploy. The random monitor method can set any host in the LAN as the monitoring host, and can monitor each host in the same subnet, without the administrator's work. Thus it is easy to deploy. The disadvantage of random monitoring method is we need to find different host running the monitoring software in different subnet if the LAN is divide into several sub-networks. This paper focuses on random network monitoring mode.

B. System working principle

When the monitoring software startup, it first initializes the NIC card working in promiscuous mode, so that it can receive all the link-layer packets in the LAN. Then the monitor host sends ARP spoofing packets to the LAN, and forces communication peers send the packets to the monitor host[5]. By setting specific keywords in the packet filtering module, the software can filter out the application-independent data packet to promote the performance. Then unpack and analysis the data packet meeting the requirement to get the details of the packet, and execute the keyword matching. If the packet is matched, it will output the IP and MAC address of the host spoofed, or the thread continue

Published by Atlantis Press, Paris, France.

next loop. After inserting the communication link between the client and gateway, we must forward all the captured packets to the correct gateway.

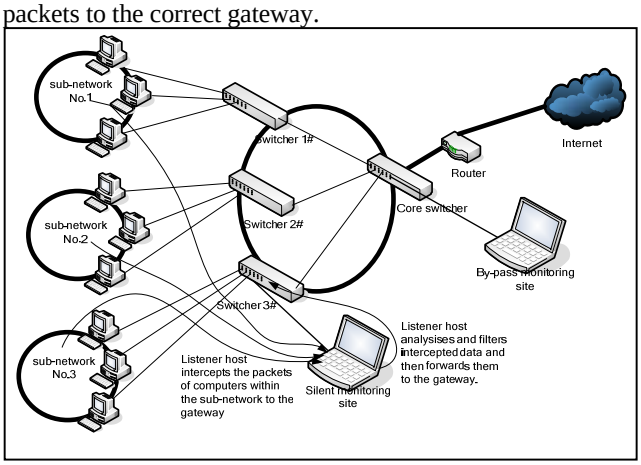

Figure 1 Random Monitoring Mode for LAN based on ARP Spoofing

C. Technical Scheme

On the system design stage, we pay attention to the commonly used protocols, such as ARP, IP, TCP, UDP, HTTP, FTP and so on[2, 3]. Using Windows XP operating system as the platform, Delphi as development environment, applying ARP protocol to broadcast packets to the spoofed client and gateway, then all the spoofed client of the subnet will send packets to the monitoring host. The software uses WINPCAP driver to capture original packets from the data link layer of the TCP/IP protocol stack[6], then analyzes the header and data of one packet, matches the keywords, suspicious QQ numbers or URL parameters. Once matched the conditions, the contents of the packet's, such as source IP address, MAC address and so on will be displayed. Thus it locates the source host accurately.

We use modular method to design the software. It is divided into several modules, including initialization module, NIC capture module, the ARP spoofing module, data packets capture module, packets filtering module, data packet forwarding module and packet analysis module. As shown in Figure 2.

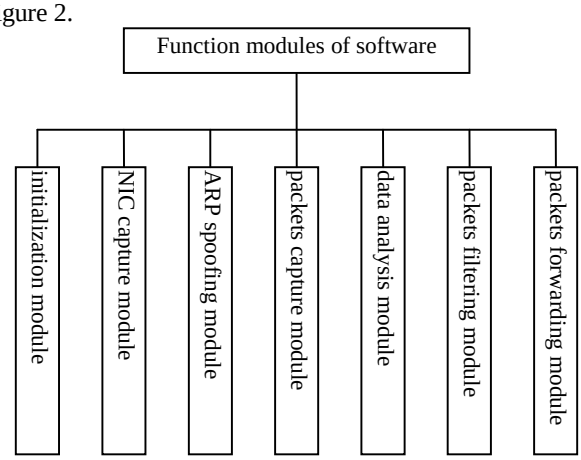

Figure 1 Function Modules of the Software

1) Initialization module

The initialization module is used for initializing the environment and loading dynamic-link libraries, including "Packet.dll", "WanPacket.dll" and "wpcap.dll" to start the software.

1) Network card capture module

WinPcap is used to in the software. First we must get all information about the NIC and gateway of the running computer in the LAN, including the IP address, subnet mask and MAC address, as well as the IP address, MAC address and NIC description of the gateway. This function is implemented by performing the thread named TMonForm.btn_NetDeviceClick (Sender: TObject) of the NIC capture module.

2) ARP Spoofing module

This module executes ARP spoofing in the LAN by implementing the TNBtScanThread.Execute. It uses WinPcap API function, to open the appropriate ports, to disguises the monitor host as the gateway and send ARP reply packets to the hosts in LAN. On the one hand, after getting the ARP APPLY, the hosts will automatically update their ARP caches, so the other hosts in LAN will take the listener host's MAC address as the gateway address; on the other hand, the listener host will get the response packets from the host deceived to get IP address, and MAC address, host name and work group information of the target host. The communication packets will pass through the listening host, so that we can capture the communication packets of target host in the LAN, and prepare for the packet analysis. Because routers will regularly send the ARP packets to correct ARP routing table, ARP spoofing thread keep in working, and send ARP spoofing packets frequently[4].

3) Data packets capture module

Software sets NIC card in promiscuous mode by calling the function named pcap_open_live, and start monitor service. Then all data packets pass through network will be sent to the monitor host.

```
/ / ********** Packets Capture thread *********
procedure TPcapThread.Execute;
var bp:Pbpf_program;
begin
   if NOT Assigned (FMonitorPcap) then exit ;
   if FMonitorPcap.FPcapHandle = Nil then exit ;
   PacketSetReadTimeout
(FMonitorPcap.FPcapHandle.Adapter, 100) ;
      while NOT Terminated do
   begin
      GetPackets ;
   end;
end ;
```

4) Data packets filter module

In the real network, the data traffic in the LAN is very heavy. Besides capturing the LAN transmission packet, the monitoring host analysis the received data packets. The monitoring host may overload and stop working. Therefore, the software provides filtering rules setting window to filter out irrelevant data packet, and only concerns about the related subnet, QQ number, FTP address or other critical

information, thus reduces pressure of packets analysis module, improving the software performance. This function is achieved by calling data packet filter module.

5) Data packets analysis module

The module analyzes the packets intercepted in the LAN by calling the function named TMonForm.PacketEvent (Sender: TObject; PacketInfo: TPacketInfo). The main task includes filtering UDP and TCP port, dissembling QQ, HTTP and FTP packets and so on, on condition that matching packet header or content with configured rules and keywords. If matched, it will display information source in the LAN or IP address, MAC address and computer name of the destination host.

6) Data packets processing module

As shown in Figure 3, it is assumed that the host C is listening host in the LAN, A and B communicate through the switch. By ARP spoofing, host C disguises as a false gateway, so that A and B communication data packets are sent to host C. Besides analyzing the data packets, host C must forward packets of host A and B at the same time so that they don't feel the network anomaly in order to hide host C. For example, A sends packets to B, after listening host getting data packets, it changes the source MAC address (before unmodified it's the A's MAC address) to MAC address of host C, and replaces the MAC address of the host B (before unmodified it's the monitor host MAC address) with the MAC address of host B, then starts routing function to forward the packet to the real gateway.

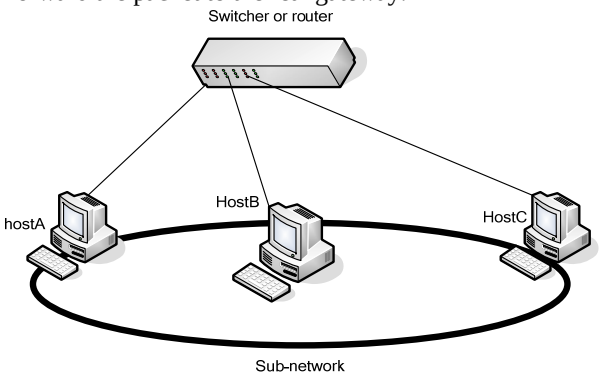

Figure 2 Principle of Monitoring

III. SYSTEM TESTING

A. Test environment and conditions

The software is tested in Little Ant Network Bar with 67 users online. The topological structure of net bar showed as Figure 1. And the host computer is Lenovo Erazer T430, with configuration: Inter G640 2.8GHz CPU, 4GB memory and Microsoft Windows XP operating system.

B. Test case and result

In the network bar one host is selected as silent monitoring site at random, which IP address is 24.86.116.200. After installing the software, configuring the target subnet, choosing NIC card, and setting filtering rules, the system starts tracing information source. The parameters are set as follows:

(1)The range of filtering IP network segment address is from 24.86.116.197 to 24.86.116.255.

(2)The filtering rules of QQ number is "4485375521".

(3)The filtered web site is "http://24.86.121.216/ index.htm".

(4)The filtering FTP keyword is "mounting".

1) Testing method

In the net bar, we use a host with IP address 24.86.1164.198 to login QQ server with QQ number "4485375521", visit "http://24.86.121.216/ index.htm" and create a document called "Beautiful mounting" on ftp server.

2) Testing result

The network security monitoring system captures the sensitive information immediately, and lists " FTP keyword, QQ number and web site" in "filtering rules name" table with values "mounting", "4485375521" and "http://24.86.121.216/ index.htm", and the "positioned MAC" and "positioned IP" are 00-23-89-D6-A2-DF, and "24.86.1164.198".

3) Result analysis

After one month continuous running, the software's capturing and analysis are proved. The time to scan the whole LAN is within one minute. There is no leakage in detecting the configured keywords, and the system running stable. The software didn't occur crashing or stopping suddenly. The other hosts didn't feel the monitor host, and the network performance is not affected obviously. The software's function and performance satisfy the designed goal.

IV. CONCLUSION

Passing the test, the software satisfies the design requirements such as intercepting LAN-sensitive information, data analysis, positioning the information source host accurately and timely, fills blank of security monitoring area in the LAN. It's already promoted in network security administration departments, and now it plays a deterrent role to network crime.

REFERENCES

[1] W , Richard Stevens. TCP/IP detailed description[M], Beijing Machine Press, 2000,124-128.

[2] The WinPcap Team, The Chinese version of the WinPcap 4.0.1 manual, http://www.coffeecat.net.cn/WinPcap/html/index.html, 2008.03.

[3] R Fielding, RFC2616, Hypertext Transfer Protocol-HTTP/1.1, 1999.06.

[4] Douglas E. Comer. Internet Working with TCP/IP Vol I(4thed)[M], Prentice Hall, 2004.

[5] ARP spoofing,http://en.wikipedia.org/wiki/Arp_spoofing.

[6] WinPcap documentation,http://www.winpcap.org/docs/default.htm.

Published by Atlantis Press, Paris, France.