ARP deception and its prevention

Weiwei Lang
Professional Department
Beijing Information Technology College
Beijing，China
langww@bitc.edu.cn

***Abstract*—**ARP spoofing is a local area network (LAN) the most common and most dangerous viruses, this paper mainly from the principle of ARP protocol, ARP protocol existing vulnerabilities and security risks of analysis of ARP Spoofing principle and attack the phenomenon, and put forward effective solutions and prevention strategies.

Keywords- ARP protocol;ARP deception;preventive measures

I. INTRODUCTION

With the wide application of network technology in various fields, it can provide great convenience in improving working efficiency, realizing data sharing and information exchange. However, some with ARP Spoofing Trojan virus, not only of purloin network user accounts, passwords and other important information, but also by sending a large number of false ARP message, users in the Internet frequently dropped, resulting in network congestion and even large area network paralysis, maintenance of the network management and safe proposed a severe test. In many of the problems in the network application, ARP deception attack is also increasingly concerned by us. Below we start from the ARP agreement, to discuss the specific ARP deception and its preventive measures.

II. ARP PROTOCOL

A. ARP protocol profile

ARP (Resolution Protocol Address) is the abbreviation of the address resolution protocol, which works in the data link layer. Transmit data in a frame in a local area network, and address according to the MAC address of the target host in the frame [1]. In the Ethernet, a host to and the other a host for direct communication, it is necessary to know the MAC address of the destination host, because Ethernet switch equipment does not recognize the 32-bit IP address in the 48 bit Ethernet address (MAC address) to transmit data packets. And this MAC address is acquired through the ARP protocol.. The basic function of the ARP protocol is to complete the process of converting the IP address into the target address MAC address [2].

In addition, when the host and destination host and destination host are not in the same LAN, even if the MAC address of the destination host is known, the two cannot communicate directly, and must be forwarded before the route forwarding.. So at this point, the host through the ARP protocol will not be the real MAC address of the host, but a router to the router outside the router MAC address of a port. So then the host sends all the frames to the destination host and sends the router to the router, sending it out.. This is called ARP ARP (Proxy) [3].

B. ARP protocol vulnerabilities

Each host in the local area network contains a data structure called ARP buffer, which aims to reduce the number of data packets to improve the transmission performance of the network.. But have not perfect place in the ARP cache table in the realization mechanism, when the host receives an ARP reply packet, he did not to verify whether they sent the ARP request. Verify the ARP reply packet source is true to the topic they generate, only to the response is effective, the host will refresh the cache tables. Will direct the response packets in the MAC address and IP corresponding relationship to replace the original ARP cache table of the corresponding information of such an attack the host can at any time false ARP response messages to the target host sends, tampering with the address mapping of the cache table and intercept the data communication. ARP deception is the use of this vulnerability, to achieve the purpose of the network attack.

III. ARP DECEPTION

A. ARP deception

ARP deception, that is, the use of ARP protocol vulnerabilities, through the target host to send false ARP packets, to achieve a target host or intercept the target host communication data [4]. Using ARP spoofing, can in the network have a number of ARP traffic on the network congestion, the attacker lasts as long as the continuous a fake ARP packets will be able to respond to changes in the target host ARP cache IP-MAC entry, resulting in network outages or man in the middle attack.

ARP attack is mainly present in the local area network, local area network (LAN) if a person is infected with ARP Trojan, infection the ARP Trojan system will be trying to through "ARP spoofing" means to capture in the network where the other computer communication information, and thus caused the other computers in the net communication failures.

B. Two forms of ARP deception

According to the different objects, ARP deception is divided into two forms: one is the deception of the host, the other is the deception of the gateway.

The first ARP deception is: B wants to communicate directly with C, while A wants to steal the contents of B sent to A. At this time, C can send fraudulent ARP packets to the A, claiming that the MAC B address has become CC-CC-CC-CC-CC-CC. This will create the correspondence between the 192.168.1.2 and IP MAC addresses and CC-CC-CC-CC-CC-CC addresses in the ARP A cache. So A sends all the contents of B to the C card. C received and read the contents of the A issued to the B, in order not to be found after the two sides, you can then send data to B. As shown in Figure 1.

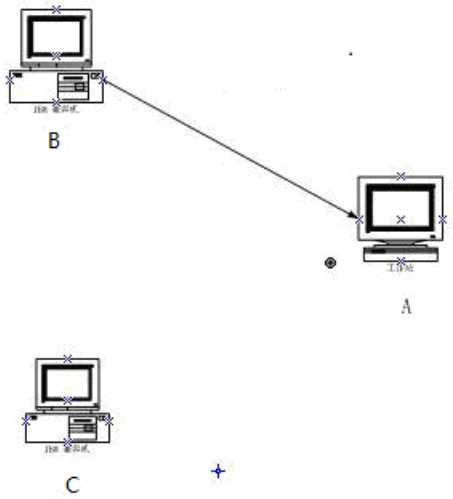

Figure 1 The same segment of ARP spoofing

Another disguise into gateway deception is if LAN host C in the ARP virus, C to send intercepted a message content, C need to sending a spoofed ARP packet, claiming that the MAC address of the gateway into the MAC address of the C, so a again to the gateway forwarding packets, packet was transferred to virus host C, virus host C won the contents of a communication, then the packet to be transferred to the real gateway. As shown in Figure 2.

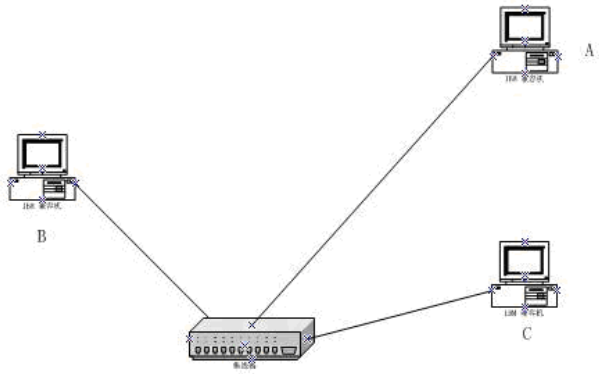

Figure 2 ARP spoofing in different segment

No matter what kind of deception, the identity of the master C, the identity of the middle man, A and B are successfully heard communications between the host and the data. Once the “middleman” ARP cheat for illegal purposes, the network users and the network will have an impact and damage to the network operation.

IV. ARP DECEIT DISCOVERY

Once there is an ARP attack in the LAN, will deceive all the hosts and gateways in the LAN, so that all the traffic must go through the Internet ARP attacker control hosts. Other users are directly through the gateway Internet, but now through the accused host forwarding Internet. Due to the impact of the host performance and program performance, this forwarding will not be very smooth. So the speed of the user can be slow or even break off frequently. In addition, ARP deception needs to send the ARP answer packet constantly, causing network congestion[5].

Expression of ARP spoofing Trojan poisoning phenomenon: use the LAN will suddenly dropped, after a period of time will return to normal. For example, the client state frequently changed red, frequent user disconnection, IE browser frequent mistakes, as well as some common software failure, etc. If the LAN is access to the Internet through authentication, sudden appearance of authentication, but (unable to Ping through the gateway) phenomenon can not access the Internet, restart the machine or in the MS-DOS window running ARP clear command arp-d and restore the Internet.

ARP cheat Trojan just successfully infected with a computer, it can lead to the entire LAN are unable to get the Internet, serious or even bring the entire network paralysis. The Trojan horse attack in addition to lead to other users in the same LAN Internet intermittent phenomenon, but also to steal user passwords. Such as steal QQ passwords, steal all network game password and account to make money trading, theft online bank accounts to do illegal trading activities and so on. This is the modus operandi of the Trojan, causing great inconvenience and huge economic losses to the user.

If there is a suspicion of ARP attack, we can use the corresponding capture tools (such as Sniffer Pro) to capture, if it is found that the LAN has a lot of ARP reply packet, and all of the IP addresses are pointing to the same MAC address, so that ARP spoofing attacks, and the MAC address is used to host MAC address of ARP spoofing attack, we can find out which corresponds to the real IP address, in order to take the corresponding control measures. In addition, we can also to a router or gateway switch to view the corresponding IP address and MAC address of the table, if you find a Mac corresponds to a large number of IP addresses, then also shows that presence of ARP spoofing attack, at the same time, through the MAC address found to ARP spoofing attack main machine on the switch corresponding to the physical port, so as to control.

V. THE COUNTERMEASURES OF ARP DECEPTION

ARP deception attacks the normal communication of network equipment, from the network management point of view, you can take some measures to prevent it.

A. empty ARP cache

Click on the "start" button - > Click to select the "run" - > input "arp-d" - > "OK" button. And then try again on the Internet, such as to be able to return to normal, then the drops may be by ARP spoofing by. This method can only temporarily solve the problem, and can not fundamentally solve the problem.

B. manual IP address and MAC address of the static binding

The most common way to prevent ARP deception is to do IP and MAC static binding, the host and Gateway within the network to do IP and MAC binding.

Because the deceiving is through the ARP dynamic real-time rules of deception machine within the network, so we put the ARP all set for static can solve the deception of Intranet PC, also at the gateway to static bind IP and MAC, so two-way binding is safer[6].

Run the following command under the MS-DOS window:

arp －s gateway IP gateway MAC

For example, suppose the computer network gateway 192.168.1.1, the machine address 192.168.1.5, on the computer running ARP - a command to view the MAC address table. Output is as follows:

Interface: 192.168.1.5 --- 0x2

Internet Address Physical Address Type

192.168.1.1 00-01-02-03-04-05 dynamic

Among them, 00-01-02-03-04-05 is the gateway 192.168.1.1 MAC address, the type is dynamic (dynamic), so it can be changed.

Manual binding commands for:

arp －s 192.168.1.1 00-01-02-03-04-05

The binding end, reusable ARP alpha view ARP cache:

Documents and Settings>arp –a

Interface: 192.168.1.5 --- 0x2

Internet Address Physical Address Type

192.168.1.100-01-02-03-04-05 static

At this time, type into static (static), you will no longer attack effect.

However, the need to explain that manual binding after the computer restart will fail, need to re bind. So the complete eradication of attack, only to find out in the network segment to be infected with the virus of computer, kill the virus, is the real solution to the problem.

C. Batch file

In the client to do the gateway ARP binding, the concrete steps are as follows:

Step 1:

Find the network address of the gateway, such as 192.168.1.1, following this case gateway. In the normal Internet access, "Start > Run > CMD > OK. Input: ARP alpha, enter, check the physical address corresponding to the gateway.

For example: The corresponding 00-01-02-03-04-05 gateway 192.168.1.1.

Step 2:

To write a batch file rarp.bat, as follows:

@echo off

arp －d

arp -s192.168.1.1 00－01－02－03－04－05

Save as: rarp.bat.

Step 3:

Run batch file to drag the batch file to the Windows - > Start - > boot - > startup, if you need to take effect immediately, run this file. Note: the configuration needs to be normal in the network.

D. using VLAN technology isolated port

LAN network administrator can according to need, the network planning a plurality of VLAN, when found to have illegal users in the malicious use of ARP spoofing attacks, or due to the legitimate user ARP virus infection because of the network, network administrator can first find the user in the switch port, then the port draw a separate VLAN, separate the user and other users, in order to avoid the impact of other users, of course, can also use will switch off the port to block the user on the network caused by impact [7].

E. Firewall and anti-virus software

Can install ARP firewall, open the LAN ARP protection, such as 360 security guards, antiARP and other software have ARP protection function. And it's free. Of course, there are a number of charges of software is also powerful. Or you can install ARP special tool, for example, Kingsoft ARP, ARP guards, XinXiang ARP etc. In addition, our timely download and install the system vulnerabilities patch, and timely update the virus library, enhance the ability of personal computer defense computer virus. In addition, the off unnecessary service can also effectively reduce the virus

attack.

VI. CONCLUSION

ARP protocol in TCP / IP network based on the widely used, although security vulnerabilities due to the inherent in the protocol, ARP Spoofing will lead to network operation and network users by the serious security threat, but through the analysis and grasp the principle of attack, we can adopt effective preventive measures, to the network implementation of protection and reduce the harm.

REFERENCES

[1]Xie Xiren, computer network [M]. Electronics Industry Press, 2007

[2]Richard Stevens. TCP/IP Illustrated Volume 1: The Protocols [M]. Machinery Industry Press, 2000

[3]E C. Douglas TCP/IP Internet (first volumes): principle, agreement and structure [M]. Electronics Industry Press, 2006

[4]Zhu Yanjing Liu Yi Chen array, local network environment ARP cheat attack and security strategy [J]. computer knowledge and technology. 2008

[5]Wang Qi, Ethernet ARP deceit principle and solution[J]. network security technology and application. 2007

[6]Li Jun,deception and prevention of ARP[J]. technology information. 2010

[7]Zhang Yuqing, cyber attack and defense technology[M]. Tsinghua University Press, 2011