International Core Journal of Engineering Volume 10 Issue 1, 2024
ISSN: 2414-1895 DOI: 10.6919/ICJE.202401_10(1).0041

Security Analysis and Simulation Experiment of ARP Protocol Vulnerability

Hai Tong[1], Guangqun Zhou[2], and Shihua Liu[3,4,*]

[1] Ningbo branch of China Telecom Co., LTD, Ningbo 315000, China

[2] China United Network Communications Group Co., LTD. Ningbo branch 315000, China

[3] School of Artificial Intelligence, Wenzhou Polytechnic, Wenzhou 325000, China

[4] Wenzhou Network Security Detection and Protection Engineering Technology Research Center, Wenzhou 325000, China

[*]13267395@qq.com

Abstract

Although TCP/IP protocol is widely used, its security was not prioritized during its development. This paper primarily examines the fundamental workings of ARP protocol and its security vulnerabilities. Through network simulation, we demonstrate the process of ARP spoofing and flooding attacks while using Wireshark packet capture tool to analyze data packets in order to gain a deeper understanding of these attacks. Finally, we propose corresponding preventive measures. Conducting simulation experiments is an economical and practical method for analyzing network protocol vulnerabilities as it can identify security issues at a low cost and provide solutions.

Keywords

TCP/IP Protocol; ARP Protocol; ARP Flooding Attack; ARP Spoofing; Protocol Vulnerability.

1. Introduction

With the development of the Internet, the network brings convenience at the same time, network security incidents also occur from time to time, network attacks are deterring online users, and the security and confidentiality of information are greatly threatened. Internet security issues are increasingly concerned by experts and scholars all over the world. Every application field has put forward the urgent need for network security. As long as the Internet has been built on top of TCP/IP, it has been inherently insecure because it was not designed with security in mind. ARP (Address Resolution Protocol) is a kind of used to the network layer IP address resolution for the MAC address of the data link layer protocol. However, due to the design flaws of ARP protocol, there are some security issues[1]. Firstly, the mapping relationship between MAC and IP addresses in ARP protocol is static, that is, the MAC address of the same computer is fixed for a certain period of time[2]. This means that if a malicious user knows the MAC address of a computer, they can spoof an ARP response to intercept the computer's network traffic. This situation is often referred to as "ARP spoofing". Secondly, ARP protocol lacks authentication mechanism. This means that any user can send an ARP request without the need for authentication. If a malicious user sends a fake ARP request, then other computers may associate the malicious user's MAC address with the correct IP address, causing network traffic to be intercepted. This situation is often referred to as an "ARP man-in-the-middle attack". In order to solve these problems, some security measures can be adopted. For example, dynamic MAC address assignment can be used to avoid the problem of static MAC address mapping.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202401_10(1).0041

In addition, ARP request authentication or ARP encryption can be used to increase the security of ARP requests. Alternatively, network isolation and firewalls can be used to restrict network access, thereby reducing the possibility of ARP attacks. Based on the analysis of the working principle of the protocol, this paper uses kali Linux and ensp to arrange the experimental environment, and uses commands to attack other virtual machines on kali virtual machine. At the same time, Wireshark is used to capture and analyze packets to obtain experimental results. Through the way of simulation experiment analysis, we deeply understand the working principle of the attack, and finally put forward the corresponding preventive measures.

2. ARP Vulnerabilities and ARP Spoofing

2.1 ARP Protocol

ARP protocol stands for Address Resolution protocol, belongs to the network layer protocol, is a TCP/IP protocol according to the IP address to obtain the hardware address of the host. IP addresses change from time to time, but hardware addresses do not; they are unique, and the hardware address is the only way to send packets on the network to the destination host without causing address collisions. ARP protocol works before sending data packets, the IP address of the destination host is converted into the destination MAC address, to ensure the smooth progress of communication between hosts, and then data transmission will be carried out. If ARP address resolution fails, data transmission cannot be carried out. The destination host is all the online hosts in the broadcast domain. When all the other hosts receive the ARP request packet, they will match their IP addresses. If the requested IP address matches the local IP address, they will send the response packet of ARP. Sends data to the source MAC address in the response packet. The obtained IP-MAC mapping is then stored in the ARP cache and retained for a certain period of time. All hosts in the LAN can send ARP response packets and ARP request packets from time to time, while other hosts will not verify the authenticity of the received response packets when they receive it. As long as the response packets are received in the LAN, the IP-MAC will be mapped to the ARP cache, which gives an attacker a chance to take advantage of. The attacker will send a large number of incorrect ARP response packets to mask the correct mapping entry, the result is that the sent data information is intercepted by the attacker, or can not reach the target host, this is an ARP protocol attack[3,4].

2.2 Security Vulnerability of ARP Protocol

2.2.1 Security Vulnerability of ARP Cache

The function of ARP cache is that when the ARP request packet is sent for the first time and the response packet is received, the IP-MAC mapping in the response packet is directly added to the cache table, so that the cache table can be directly queried in the next send, and the IP address resolution is not needed again, which can save time and improve work efficiency. At the same time, there is an aging mechanism in the cache table. If a mapping entry is not used for a long time, this mechanism will automatically delete this entry. The purpose of this mechanism is also to ensure the timeliness of the mapping between IP address and MAC address, because most machines now use DHCP to automatically obtain IP address, IP address has a lease period, and it will change frequently. Can speed up the ARP cache table lookup. Because of this mechanism, the attacker can send a large number of forged ARP data packets when the cache is updated, then it can be written into the ARP cache table during the update period. When there is a forged mapping entry, the source host will not send a request packet to ask for the correct MAC address, and ARP spoofing will occur.

2.2.2 Vulnerability of ARP Broadcast

ARP requests are broadcast. When the source host in the LAN needs to communicate with the destination host, if there is no IP-MAC mapping of the destination host on the source host, it will be broadcast throughout the LAN, asking for the MAC address of the destination host. There are only a few correct response packets, but the attacker's forged response packets account for the majority, masking the correct response packets, the source host will receive a large number of wrong response

ISSN: 2414-1895 DOI: 10.6919/ICJE.202401_10(1).0041

packets, because the ARP protocol has no verification mechanism, it is impossible to distinguish the authenticity of the response packet, then the wrong IP-MAC entries will be generated in the cache table. If host 1 has the MAC address of destination host 2, the query can be unicast to host 2. When host 2 receives the request, it will update its ARP cache table. If an attacker joins the LAN at this time, he can forge the ARP request packet and send it to host 2. Due to the lack of authentication mechanism, the destination host mistakenly thinks that this is a correct request packet, so it writes to the cache table, and then the communication between the correct source host and the destination host is broken. Also, when the source host sends a request, the destination host sends a response packet first, because the ARP protocol does not stipulate that the response packet cannot be sent until the request packet is received. This also results in the generation of erroneous IP-MAC entries.

2.2.3 ARP Responses are Authentication-free and Stateless

The protocol design of ARP is not authentication mechanism, ARP works on the basis of mutual trust, because ARP is a stateless protocol, even if no ARP request packet is sent, the host can also receive ARP reply. Every host that receives an ARP reply packet unconditionally flusher its ARP cache according to the content of the reply packet. This provides the possibility of ARP spoofing, attackers can issue fake ARP packets to affect the communication of nodes in the LAN, and even can be a "man in the middle". Any ARP reply is legal and does not need authentication. As long as it is an ARP reply packet in the LAN, no matter whether it is a legitimate reply or not, the host will accept the ARP reply and modify its ARP cache with its IP-MAC information. This is a problem with ARP.

2.3 ARP Spoofing

The ARP spoofing attack exploits the operational mechanism of ARP protocol itself to attack hosts on LAN. It includes two forms: forging ARP request and ARP reply. The principle of ARP spoofing is to send a forged ARP reply to the target host, which is the forged mapping information between the source IP address and the MAC address. After the target host receives the IP-MAC mapping information in the reply packet, the target host updates the ARP cache, so that the target host sends the message to the wrong object. The ARP spoofing principle can be briefly described as the following process.see Figure 1.

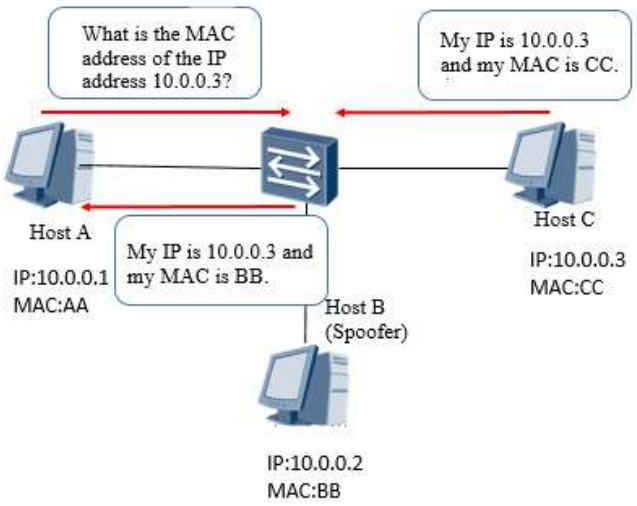

Figure 1. The ARP spoofing process

Suppose host B is an attacker who intercepts the communication data between host A and host C to perform ARP spoofing, and before the implementation of ARP spoofing, it can intercept the IP address and MAC address of the two hosts through ARP scanning. Then it can forge wrong ARP

ISSN: 2414-1895 DOI: 10.6919/ICJE.202401_10(1).0041

packets and send them to host A, and the source IP address in the packet is the IP address of host C. The source MAC address is the MAC address of host B. Upon receiving this ARP reply, host A will update the IP-MAC mapping in the ARP cache. Later, when host A sends a packet to host C, the destination MAC address will use host B's MAC address, and the switch will forward the packet to attacker B based on host B's MAC address. The above attack host B implements deception to intercept the communication process between host A and host C, the communication between host A and host C is not affected, but the data content of the communication between the two has been stolen by the attacker, if you want to complete an effective ARP spoofing, then it is necessary to cheat the host and the gateway at the same time, ARP spoofing is usually not easy to be detected. Because ARP itself did not receive ARP packets for verification, so the operating system will not tip error messages, many hackers will use this point, forge false ARP packets, attack a computer, so that you can manipulate whether the target host can network, if the gateway is attacked, then the whole LAN communication will be blocked, The network will be disconnected from time to time, affecting the normal communication of the network, so if it is attacked, it is not only difficult to find the source of the attack but also has a huge impact on the connectivity of the network.

3. The Simulation Experiment of ARP Spoofing Attack

3.1 Experimental Topology and Environment

As shown in Figure 2, it is a small LAN, three of which are clients and one is server, bridging a cloud on the central switch, and two network cards are bound to the cloud, one network card is connected to the local LAN, and the other network card is connected to the gateway of Kali, the attack host. After the LAN is set up, we will test the connectivity between Kali Linux and the hosts in the LAN to ensure access to the LAN. Then, we need to install the dsniff packet of ARP on Kali Linux. The arpspoof used for spoofing is an auxiliary tool of dsniff, which we can use with the command: apt-get install dsniff to install, if the installation fails, it may be the problem of the software source, you need to update the software source, after the installation is completed, the implementation of ARP spoofing environment is built.

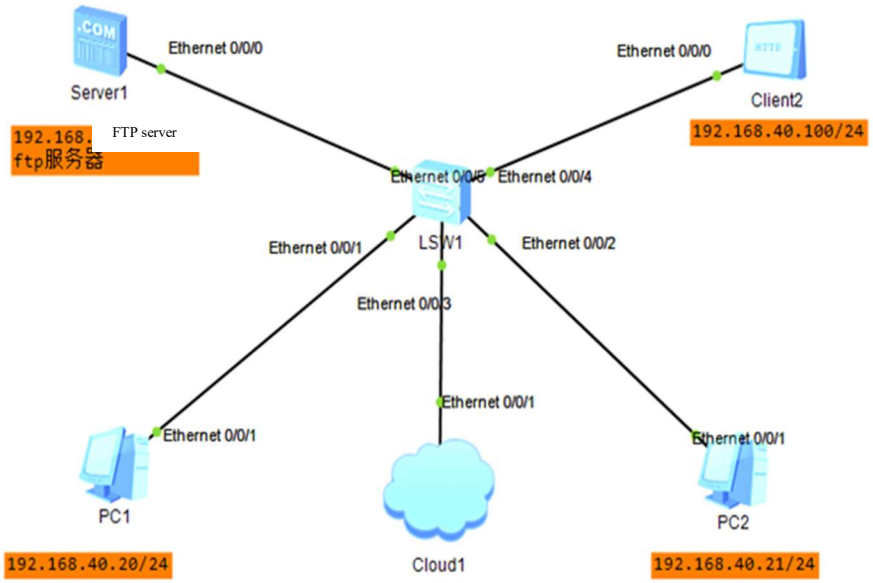

Figure 2. the Topology of the Experiment

ISSN: 2414-1895 DOI: 10.6919/ICJE.202401_10(1).0041

3.2 Experimental and Analysis

The ARP spoofing attack command requires Kali Linux root privileges to run. Before implementing the ARP spoofing attack, a simple host scan on the kali virtual machine is needed to determine the surviving hosts in the LAN. A simple fping command can be used to perform host scanning, and the command execution results are shown in Figure 3. Scan out the live hosts in the LAN to determine the IP address of the attack host.

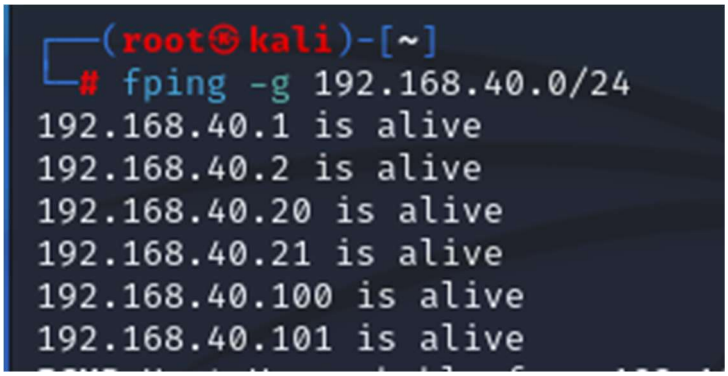

Figure 3. the fping command and the result

Then run the arpspoof command to implement ARP spoofing. The command format is as follows:

```
arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host
```

Figure 4. The command format of arpspoof

The main parameters of the command arpspoof is as in Table 1.

Table 1. The main parameters of the command arpspoof

Parameter	Description
-i	Specify the interface to use
-t	Specify a host that is poisoned by arp spoof
-r	Poison two hosts (target and host) to capture network traffic in both directions. (Valid only when used with the -t parameter)
host	The host that wants to intercept the packet

The attack process using the command “arpspoof -i eth0-t 192.168.40.100 192.168.40.101” is shown in Figure 5. At the beginning of the attack, if the traffic forwarding function is not enabled on the kali virtual machine, the internal network of the LAN will be disconnected and the communication between the two hosts will be interrupted. However, the communication packets between the two hosts still flow through the Kali host, and the packet capture is carried out on the Kali attacker. The packet capture results are shown in Figure 6 and Figure 7. It is found that the MAC address of the host in Kali is bound to the IP address of the spoof host and broadcast out, covering up the correct broadcast packet. All hosts in the LAN were subjected to erroneous broadcast packets, and the ARP cache table was successfully modified, resulting in the data flow through the Kali host when accessing the FTP server, resulting in the leakage of the user name and password.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202401_10(1).0041

Figure 5. The process and result of arpspoof

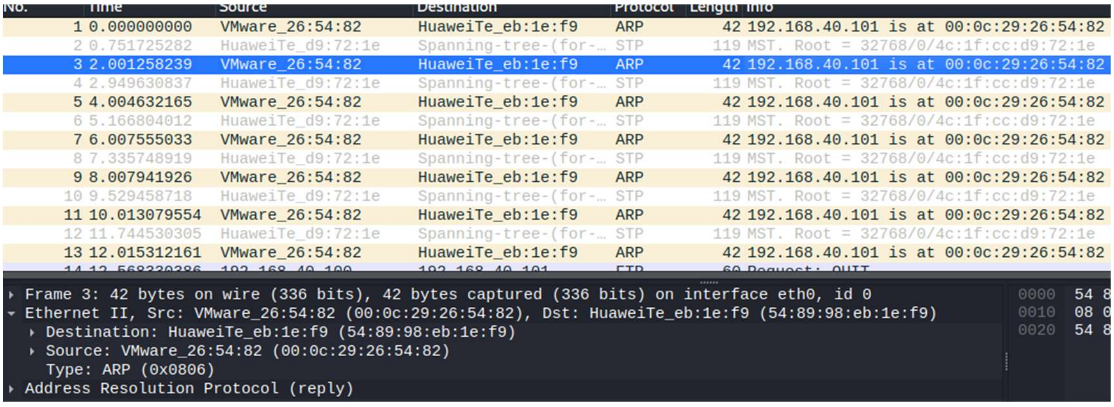

Figure 6. The capture result of arpspoof packages

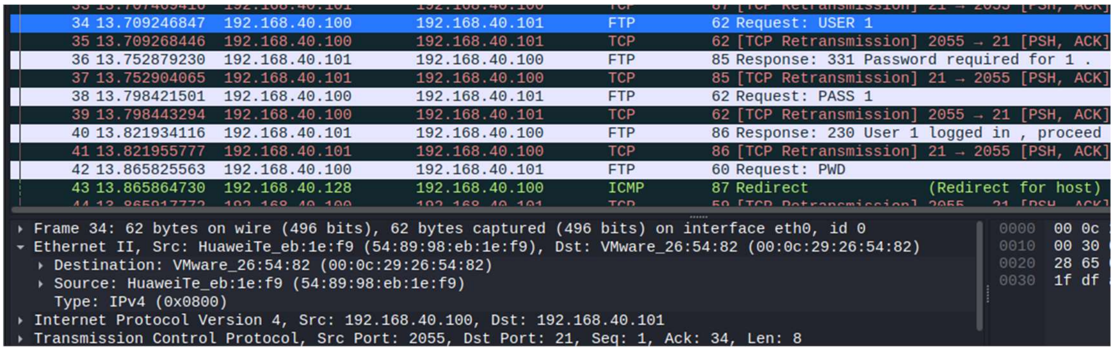

Figure 7. The capture result of FTP packages

3.3 Precautions Against ARP Spoofing

To prevent ARP spoofing attacks, we can start from the following aspects[5,6,7]:

(1) Use static ARP table: In the network, the commonly used IP address and MAC address are manually added to the static ARP table, so that the attacker can avoid using fake MAC address to deceive other devices in the network.

(2) Using dynamic ARP detection tools: Using ARP detection tools, you can monitor the ARP traffic in the network in real time, and find and prevent attackers from using spoofed MAC addresses in time.

(3) Enable port security: In a network, you can limit the number of MAC addresses allowed on each port by enabling port security, which prevents attackers from spoofing other devices on the port.

ISSN: 2414-1895 DOI: 10.6919/ICJE.202401_10(1).0041

(4) Use network layer encryption technology: Using network layer encryption technology (such as VPN), you can encrypt the data during transmission, thus avoiding the attacker to intercept and tamper with the data.

(5) Update your operating system and applications: Keeping your operating system and applications up to date fixes known vulnerabilities and security issues, thereby reducing the risk of attacks.

(6) Use security software: Using security software such as anti-virus and firewall can help detect and prevent network attacks and improve network security.

4. Conclusion

This paper starts with the analysis of the working principle of ARP protocol, analyzes the existing vulnerabilities and possible attack risks of ARP, and uses simulation software such as network simulator to reproduce the ARP protocol vulnerabilities and ARP flooding attack scenarios. Through packet capture analysis, this paper studies the principle of ARP and analyzes its possible consequences. The corresponding security measures are summarized.

Acknowledgments

This research was supported by Wenzhou Network Security Detection and Protection Engineering Technology Research Center.

Reerences

[1] Xu Shuang, Su Yu. Analysis of Network protocol [M]. China Water Resources and Hydropower Press, 2016.9.

[2] Li Long, Research and application of Attack and defense Technology based on TCP/IP protocol vulnerabilities [D]. Northeastern University,2013.

[3] Bian Jiang-hao, Research and implementation of ARP spoofing detection and defense method [D]. Yunnan: Kunming University of Science and Technology Press,2015,5.

[4] Zhao Mengna, Design and Implementation of ARP Attack System Based on Campus Network [D]. Guangdong: South China University of Technology Press,2013,11.

[5] Guo Jie, Research on ARP spoofing Attack and Prevention Strategy [J]. China Communications Tianjin Harbor Engineering Design Institute Co., LTD.,2018,5.

[6] Shan Guojie, Research on defense strategy based on ARP spoofing attack [D]. Shandong: Shandong Normal University Press,2011,6.

[7] Gu Yafen, Discussion on ARP Attack Principle and Defense Measures in LAN [J]. Gansu: Gansu Institute of Product Quality Supervision and Inspection,2021,5.