Shielding The Networks Depending On Linux Servers Against Arp Spoofing

Ganga Rama Koteswara Rao¹, Dr. R.Satya Prasad²

¹Research Scholar, Department of CSE, Rayalaseema University, Kurnool, Andhra Pradesh, India.
²Research Guide, Assoc. Professor, Department of CSE, Acharya Nagarjuna University, Nagarjuna Nagar, Andhra Pradesh, India.

*Corresponding author E-mail: grkraoganga@gmail.com

Abstract

Escalating Internet-dependent business is giving rise to a corresponding growth to the threats on servers catering to this growing Internet usage. There is a need for research to secure the servers from attackers. Today, the most dangerous attack that can be performed inside the network is ARP Poisoning, which can provide fake identity to steal the authentic network traffic or modify the authenticated network traffic.

In the present scenario, any network can become an easy target of ARP spoofing which is highly difficult to detect and prevent. The aim of the research paper is to focus on detecting and preventing the ARP Poisoning attack, by using open source technologies.

Keywords: Address Resolution Protocol, ARP Cache, Device Manufacturer Address.

1. Introduction

Address Resolution protocol is used to determine the Device manufacturer address for a given IP address in the network. A number of the loopholes make the ARP quite exposed to dissimilar network assaults [12]. The ARP request is broadcasted when the Address Resolution Protocol table does not hold the Device manufacturer address of the recipient machine [2] and the recipient machine will respond with the Device manufacturer address after receiving the request query. Once the sender receives the reply, it stores the IP address and Device manufacturer address of the recipient in the ARP cache and the devices start communicating with each other. Under normal circumstances, the sender forwards the packets to a router with the recipient's address. The router is responsible for handling all communication between the two devices as shown in the figure below.

![Fig. 1. Communication between Sender and Receiver via router](image)

At layer2, the packet that needs to be forwarded to the router from the victim's device is spoofed with the attacker's device manufacturer address, thus the packet is forwarded to the attacker device.

When the hacker receives the packet, will forward the same packet to the router [16] and the victim's device manufacturer address is replaced with the hacker's device manufacturer address.

The reply from the router is logically forwarded to the attacker's system [6]. The same packet is forwarded to the victim's device by the hacker's device.

Impacts of the ARP spoofing attack are as follows:

- Causes of man-middle-attack.
- DNS spoofing
- Stealing of the cookie information.
- Session hijacking
- Examine the web pages visited by the victim
- Examining confidential information such as username and password.
- Listening to the network traffic
- Modify the network traffic, which can be used for various types of attacks such as replay, spoofing etc.

2. Review Of Literature

Different solutions for discovering ARP attacks have been proposed. But these solutions were not able to detect or discover a wide range of attacks. Further, the following solutions were proposed, but none of them completely solve the problem.

The Internet is designed to be dynamic and hence maintaining static ARP tables is impossible [1]. Distribution of such ARP tables may not be secure.
Often layer 2 devices offer little or no security features at all. Even the minuscule security features offered by high-end layer 2 devices such as port security can be easily compromised.

Every networked device cannot be virtualized. Virtual networks are proven to have their own security issues.

Securing communication between devices through encryption is possible only from the IP layer and upwards. Even an encrypted channel is susceptible to man-in-the-middle attacks [11].

Security features provided by firewalls cannot cover ARP spoofing [18]. Because firewalls can only decide whether to allow or disallow the network traffic to pass through them based on packet filtering rules [14].

Biju Issac [2] proposed to make the MAC address unicast, centralized and protected and also proposed a secure design of the DHCP protocol to mitigate MAC spoofing.

Nikhil Tripathi [12] probed several popular existing countermeasures to look for weaknesses in the proposed solutions. He predicted possible scenarios that could occur in a LAN when an ARP Poisoning attack is launched thereby allowing further studies to be more effective while designing new techniques to combat these attacks.

Seungpyo Hong [15] studied various prevention techniques. They suggested a protection method that does not require changes in the network protocol or costly devices. They suggested the implementation of static tables to guard against ARP poisoning attack.

3. Proposed Work

In the TCP/IP model, the Address Resolution Protocol functions between Internet and Network Interface layers. The Address Resolution Protocol is responsible for transmitting the Ethernet frame containing the sender and recipient addresses from source to destination. The Sender’s Ethernet address is retrieved from the kernel which obtains it from NVRAM on boot and ARP provides a Recipient’s address.

The attacker makes use of an ARP Poisoning on the target machines which is easy to implement and has a high impact on security. High critical threats to ARP spoofing are as follows.

An attacker can intercept traffic in two ways

(i) Simply examining the traffic and may expose confidential information such as login IDs and passwords.

(ii) Alter the traffic and can execute different types of assaults such as replay, spoofing etc.

This paper focuses on discovering and shielding Address Resolution Protocol Information. The structure of the ARP table depends on the operating system [9]. Some systems will accept the ARP packets and insert into the table. Some systems will not allow inserting the information into the table [8] if the information is already available on the table. Some systems wait for updates until the entries in the table are timed out.

This paper studies
- Mitigating man-middle-attack through ARP spoofing attack.
- Protecting ARP mapping.
- Checking unsolicited ARP replies.

• Checking duplicate use of MAC.
• Examining all the entries in the ARP table
• Examining the system log files.

![Fig. 2. Workflow diagram of the proposed detection and mitigation of ARP Spoofing attacks](image)

In this paper, the workflow diagram indicates the two important steps involved in mitigating the attack. The first step is the shell script program which runs in the background to examine the ARP traffic; it detects the duplicate MAC address and stores the duplicate MAC address and its IP address in the database known as the blacklist database [17]. The second step is the packet filtering rules which work at the firewall level to block the packet whose source address is already a duplicate MAC address. The packet filtering rules depend on the blacklist database stored by the detection algorithm.

4. Detection

The Ethernet traffic activity needs to be examined to identify suspicious ARP traffic and the network administrator is alerted with e-mail messages or SMS messages when IP and MAC address is changed. The controversial traffic needs to be monitored to detect the attack [4]. It is very difficult to identify ARP Poisoning attack [3]. The victim’s machine cannot verify the source IP/MAC mapping enclosed in Address Resolution protocol response [5]. IP to MAC pairing activity appearing on the network needs to be watched carefully. Administrators have to take appropriate actions when an ARP spoofing attack is detected [7]. Identifying malicious events often depends on the skills of the network administrator. Easiest and popular network attack method is an ARP poisoning attack, which may cause severe damage to the network. Before bringing loss to the organization, there is a need to detect ARP poisoning attack and source of attack as early as possible. This paper focuses on following points

1. Monitoring IP/MAC table.
2. Identifying ARP Spoofing attacks.
3. Detecting unidirectional and bidirectional attacks.
4. Capturing all inbound and outbound ARP packets.
5. Storing the activities in syslog file and sending an email when changes arise in syslog file.
6. Notifying the administrator when the new station is identified.
7. Testing for duplication of machines

All the incoming and outgoing packets are filtered to avoid inconsistencies
4.1 Algorithm for detecting ARP Spoofing attacks

Begin
examine each client in the network
if(client contains a valid IP address) then
  examine the MAC address of the client
  if(client is new) then
    update the ARP table with new client information
    Enable the client system to entrance into the network
  else
    update the ARP table with old client information
    Send alert message to administrator
    Block the client from accessing the network
endif
endif
Examine each record in the /var/log/syslog
if (changed in the MAC and IP is observed) then
  Block the IP address and MAC address.
  send email to the administrator
endif
end

There are a number of techniques to stop ARP poisoning assaults [15]. To prevent from ARP Spoofing attack, the script shown in the table below is useful to monitor the ARP entry in ARP table of the system. Before sending the message to the MAC layer, it is necessary to check the ARP cache [19]. The script is placed in the crontab that periodically monitors the MAC address of the gateway to check for possible ARP spoofing attack; it notifies the administrator and sends the mail to the administrator of the local system when duplicate MAC addresses are detected.

Table 1: Shell script to monitor the MAC address in ARP Table.

```bash
#!/bin/bash
arp -a | cut -d " " -f2,4 >f1;
exec < f1
while read line
  do
    list="(Sp [0])" "$line"
    done
for mac in $list [0]);
  do
    cut -d -f1 <- <grep -i $mac=f1> tmp
    read count &<tmp
    if [ count -gt 1 ];
      then
        echo "Hacked :: ARP Spoofed attack : $mac duplicated"
        Scount times
        subject="Your system was hacked!":
        mail -s Alert : hacked : ARP Spoofed Attack : $mac duplicate
        Scount times ":
        echo "$mac duplicated Scount times " | mail -s "Your System was hacked " grkrao@ubuntu
      fi
done
```

ARP spoofing can be detected by monitoring the network traffic for anomalies such as a huge amount of ARP packets coming from same source MAC address [13]. ARP spoofing can bedetected in two ways ARP flooding and besieged ARP Poisoning.

Configure the /etc/host.conf and etc/sysctl.conf with the following to prevent ARP spoofing attack

1. Enable no-spoof and spoofalert
2. In all interfaces, turn on source address verification.
3. Disable TCP Window Scaling.
4. Ignore ICMP broadcasts and bogus ICMP errors.
5. Reject IP source route packets.

6. Algorithm to Block The ARP Spoofing Attack.

```bash
begin
Examine the IP packet
if (package contain the valid IP address) then
  examine the type of packet
  if(IPCode = "redirect" or "Bogus icmp errors") then
    drop the packet
    Send an alert message to the administrator.
    Store the error in the log file
endif
Examine the MAC address of the source,
if (MAC address is in blacklist database) then
  Drop the packet
  Send an alert message to the administrator.
  Store the error in the log file
else
  allow the packet
endif
deny the packet
endif
end
```

7. Results

The attacker searches for the host on the network to attack it. A device in the internal network whose traffic is redirected other devices is called victim device. Before the hacker performs the attack, the attacker poisons the ARP cache of the victim machine. The ARP spoofing attack can be detected by examining the /var/log/syslog file and content of current arp table in the system as shown in figure 3 below.
Wireshark tool is used to detect the attack and gives information such as "Duplicate use of IP is detected for 192.168.17.2" which is a router IP address, when the attack is successful as shown in figure 4 below.

**Fig. 4.** Detection of ARP Spoofing attack using Wireshark

When the ARP spoofing attack is successful, the attacker gains the username and passwords of the victim as the victim login into the Moodle website in a typical ARP spoofing scenario depicted in this example as shown in figure 5 below.

**Fig. 5.** Examining the username and password of victim machine using Ettercap.

After the execution of the algorithm 5.1 to protect the targeted machine from ARP spoofing attack and the attacker fails to obtain the confidential information such as username and password of the targeted user as shown in figure 6 below.

**Fig. 6.** Failure of obtaining confidential information after applying prevention algorithm

### 7.1 On A Targeted Machine

The same failure of the attack can be shown in figure 7 below with the help of Wireshark tool after the implementation of the prevention algorithm 5.1.

**Fig. 7.** Failure of the attack after implementation of algorithm 5.1

After the execution of the shell script shown in table 1, it warns the administrator about the attack on the victim machine through themail as shown below.
8. Conclusion

The reliable server needs to provide 24/7 services to the public as they become increasingly dependent on online services for everyday functions. There is a need to protect the server from ARP Spoofing attack which leads to dangerous attacks like phishing, DoS, stealing of sensitive data and session hijacking etc. Different impacts of this attack are exposed in this paper with real-life examples. This attack is very simple to perform and yet very difficult to detect and prevent.

This paper focused on detection of the ARP spoofing by using bash shell script and protection from ARP spoofing attack using packet filtering rules implemented at the firewall to cleanse the network from ARP poisoning.

References