CPRE 431

Group 11

# Redirect Traffic to a Fake Site with ARP Spoofing

## Overview

An attacker can utilize a technique called ARP (address resolution protocol) spoofing to get a victim to do various tasks such as leaking data or downloading malware. ARP spoofing occurs when an attacker sends false ARP messages over a LAN (local area network) that links an attacker's MAC address with the IP address of the legitimate server. This allows the attacker to intercept, modify, or block communication between the victim and the legitimate server, which is why ARP spoofing can be used in a "man-in-the-middle" attack. In the simulated system, there's the attacker, the legitimate server, and any users or victims on the attacker's LAN. The attacker uses ARP spoofing to impersonate the legitimate DNS server in the eyes of the victim, so the attacker has access to all data being sent to what the victim believes is the real server rather than the attacker's simulated, "fake" version. This includes potential login information like a username and password, which would be devastating if the attacker was posing as a bank's website for example.

## Introduction and Techniques

The internet protocol (IP) uses ARP to link the IP network addresses with the MAC addresses used by a data link protocol. When devices are on a LAN, the destination IP address must be changed to a MAC address for transmission across the data link layer. A specific device on the LAN is in charge of this conversion task. This same device sends out an ARP request to all devices on the LAN when it receives a request from an external network to communicate with one of the other devices on the LAN. The request from the external network

will contain the intended receiver's IP address. The intended receiver sends an ARP reply to the ARP request which contains the MAC address for the IP.

However, there is not a way that the protocol can authenticate which peer the packet originated from. This is what the attacker takes advantage of to utilize ARP spoofing as explained previously. Recall that the attacker sends falsified ARP messages over a LAN that links an attacker's MAC address with the IP address of the legitimate server. An attacker can use ARP spoofing to gather sensitive data from the victim (like usernames and passwords) that was intended for the legitimate server. ARP spoofing is mainly used to steal sensitive information, but it can also be used in DoS attacks, session hijacking, and man-in-the-middle attacks.

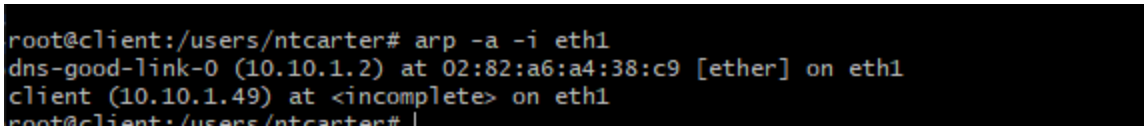
## The Attack

We attacked using ARP spoofing. ARP spoofing is an attack technique that uses ARP messages to intercept data packets from the other party in the middle under the LAN. This is an attack that can only be used in close-range communications because it uses the ARP protocol. First, the attacker approaches the client before the server approaches the client and pretends to be the server. How does an attacker pretends to be a server? An attacker is an attack that deceives a client or server with a MAC address. In other words, use a protocol that changes IP addresses to MAC addresses. When an attacker intentionally sends an ARP message that responds to a specific IP address and its MAC address, the client that receives the message recognizes the IP address as the attacker MAC address and sends the packet to that IP address as the attacker.

In this attack, first, use command like tcpdump -i eth1 -n -e "udp port 53", makes DNS traffic using UDP port 53 and ethernet headers. by this one, client uses server for both DHCP

and DNS lookups. use arp -a -i eth1 command, check the client's ARP table for checking the MAC address currently associated with server's IP address.

Figure 1: Client arp table pre spoofed




The next step is to make the client recognize the attacker as the server and the server recognize the attacker as the client. we need to enable packet forwarding first using command "sysctl -w net.ipv4.ip_forward=1". and then get IP address of client from the server. then arpspoof -i eth1 -t TargetGatewayAddress IPAddress makes the attacker sends ARP to client impersonating the server and send ARP to server impersonation the client.

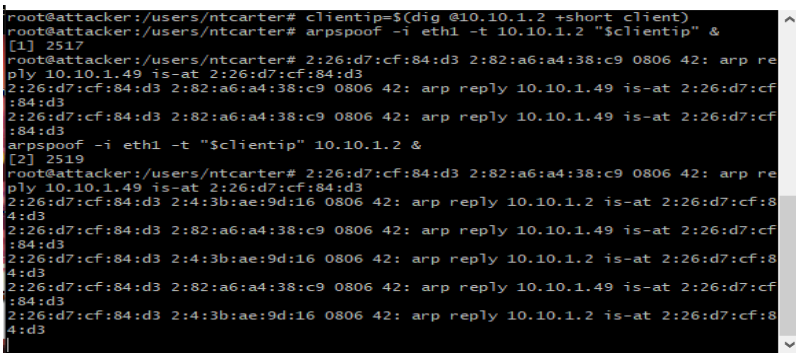



Figure 2. Setting up spoofing

The is a method of sending an attacker's MAC value to the ARP cache table on the gateway, so that the MAC address of the target's IP address is replaced by the attacker's MAC value, and all data sent to the target is sent to the attacker. Here, you can check ARP table with arp -a command and the MAC address value of the target has become the attacker MAC address value. To compare the figure 1 and figure 3, can check the differences of client arp table before and after spoofed.

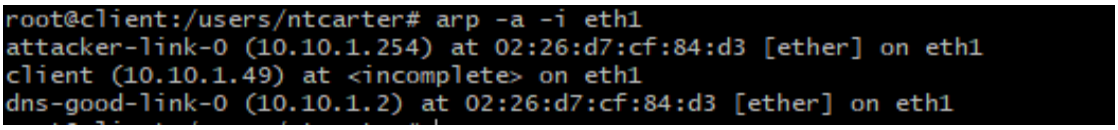
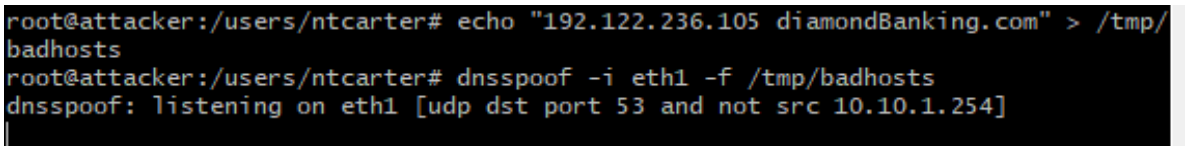


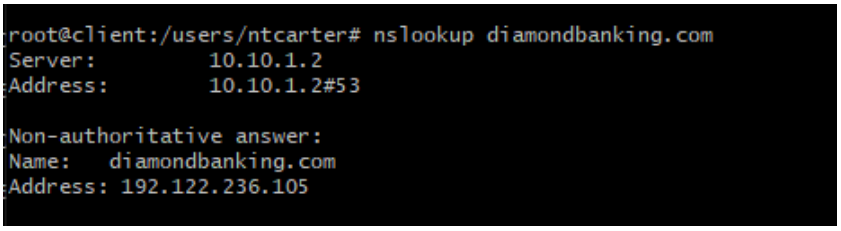

Figure 3. Client arp table after spoofed

Then, the attacker creates the fake site by impersonating the bank's name and IP address, and the client believes that the fake site is the real bank's site and communicates. By using command from figure 4, attacker put fake site on bank node. After that, get an IP address of bank by wget -q0- https://ipinfo.io/ip 192.122.236.105 commands.


(Figure.4)

Client sends a DNS query to server, but client using attacker's MAC address. And attacker sends query to server pretending to be client. Figure 5 shows the attacker's spoofing and Nslookup spoofed.

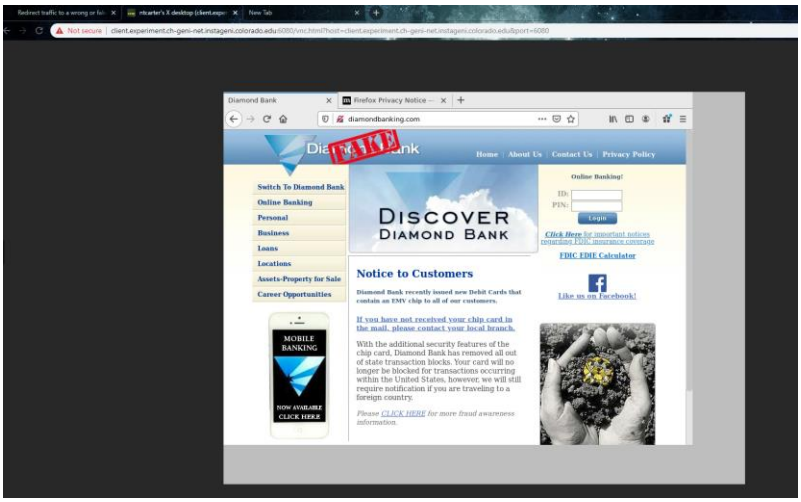



(Figure 5)

Therefore, attacker can find actual IP address associated with hostname. After attacker finds out actual IP address of client, sends response to client using fake site's IP address. The client will communicates with the fake site, but thinks they communicates with real bank site.

Because server sent the bank's real address to the client, but attacker's MAC address is used. Figure 6 shows is a final result of spoofed site on browser.




(Figure 6)

Detecting and Defending

There are several ways to detect and defend against ARP spoofing. One of the simplest ways is to use windows command prompt to check your ARP table. As discussed before ARP spoofing involves attackers connecting their MAC address to the IP that the user is trying to access. When you use the command arp -1 on a windows command prompt, you will be able to see what IP addresses are associated to what MAC addresses in your ARP table. If two different IP addresses are associated with a single MAC address it is very likely those IP addresses are being spoofed and you are under an ARP spoof attack. That MAC address is highly likely to be the attackers MAC address.

There are also many tools available on the internet that specialize in detecting attacks like ARP spoofing. Some of these tools are WireShark and XArp. These tools detect arp spoofing attacks by analyzing packets.

There are also several ways to prevent ARP spoofing. One basic solution is to map each machine on a network on each computer. This will allow your computer to disregard ARP replies

since all IP and MAC addresses will already be known. Another common way to prevent ARP spoofing is to use encryption. Both HTTPS and SSH make it difficult to ARP spoof on a network. With many websites using HTTPS today arp spoofs are becoming less prevalent and more complex. Just like with using HTTPS and SSH a VPN also make it difficult for an attacker to ARP spoof attack you. This is due to the fact that VPN's also encrypt all of your data between your client and a VPN server. For all of these encryption techniques an attack would have to somehow either break the encryption algorithm (infeasible) or make your client or browser believe they received legitimate traffic which is also incredibly difficult/infeasible. LAstly, like mentioned before you can use various tools, like Wireshark and XArp to detect and prevent ARP spoofing by analyzing and detecting potentially spoofed packets.

## Conclusion

The largest lesson we learned from the perspective of an attacker is to spend a lot of time looking for vulnerable targets. Today with a lot of websites using HTTPs and a lot of internet users using encryption, like a VPN, it becomes incredibly difficult to launch a successful ARP spoofing attack against a system with competent security. This might make targeted arp spoofing attacks not very viable. However, it seems possible and not too difficult to run an opportunistic ARP spoof attack if a random user is vulnerable. We also learned that running a successful ARP spoof attack is simple. This means that as attackers we could feasibly target many different systems at once looking for any vulnerable machines. The more complex part of an ARP spoof would be infecting a machine with a virus to act as a zombie for us to get onto a systems LAN.

There are a lot of things we learned from a system administrator's perspective. The main thing we learned was that arp spoofing is very easy, especially at its simplest level. It took us just a few hours to run a successful ARP spoof attack on a vulnerable system. This means that it is very important to have relevant security for this issue. If you overlook this type of attack

even novice attackers will be able to ARP spoof your system. Since there are a lot of tools available online to help detect and prevent ARP spoofing it becomes fairly easy to protect your system from this kind of attack. We also learned that it's important to know how to detect an ARP spoof attack. A lot of the material we covered with this topic were ARP spoofing on a simpler level. It possible for more experienced attackers to have more complex attacks that normal prevention techniques won't be able to pick up and detect. Because of this it is important to be able to detect potential ongoing ARP spoofing attacks. Having your system configured correctly or having detection software installed on your system could mean detecting an attack sooner.

Sources


https://doubleoctopus.com/security-wiki/threats-and-tools/address-resolution-protocol-poisoning/

https://witestlab.poly.edu/blog/redirect-traffic-to-a-wrong-or-fake-site-with-dns-spoofing-on-a-lan/

https://www.veracode.com/security/arp-spoofing

https://www.iplocation.net/arp-spoofing

https://www.comparitech.com/blog/vpn-privacy/arp-poisoning-spoofing-detect-prevent/

https://www.ionos.com/digitalguide/server/security/arp-spoofing-attacks-from-the-internal-network/