ARP Poisoning Attacks with Ettercap and Traffic Monitoring with Wireshark

Dept. of Computer Science and Engineering
Amrita School of Computing, Bengaluru
Amrita Vishwa Vidyapeetham, India
G. Vishwa Prakashini[1]
Chunduri Yoshitha[2]
Neha S[3]
Mr. Vishwas H. N[*]
bl.en.u4aie23007@bl.students.amrita.edu
bl.en.u4aie23003@bl.students.amrita.edu
bl.en.u4aie23022@bl.students.amrita.edu
hn_vishwas@blr.amrita.edu

***Abstract*—Address Resolution Protocol (ARP) Poisoning is a type of cyberattack that exploits the vulnerabilities of the ARP in local area networks (LANs). By sending falsified ARP messages, attackers redirect network traffic, allowing them to intercept, modify, or block communication between devices. This attack is a critical concern in cybersecurity due to its potential to compromise data integrity and confidentiality.**

In this study, we explore ARP poisoning using Ettercap in Kali Linux, a powerful network security tool designed for network protocol analysis and interception. Ettercap enables the execution of ARP poisoning by impersonating devices within a network. Through this impersonation, the attacker can act as a man-in-the-middle (MITM), gaining unauthorized access to sensitive data or injecting malicious payloads into communication streams. The paper details the setup and execution of an ARP poisoning attack within a controlled environment. Key steps include network discovery, ARP table manipulation, and traffic interception. We also demonstrate the monitoring of communication between the victim devices and the attacker's system using Ettercap's features. The implications of these attacks are examined, emphasizing their potential for unauthorized access to credentials, session hijacking, or denial-of-service (DoS).

***Index Terms*—Man-in-the-middle attack, ARP poisoning, Ettercap, Kali Linux**

I. Introduction

In the rapidly evolving landscape of cybersecurity threats, Man-in-the-Middle (MITM) attacks have emerged as one of the most insidious methods for compromising data integrity and confidentiality. A MITM attack occurs when an attacker intercepts communication between two parties, either passively eavesdropping on the data or actively altering it without the knowledge of the communicating parties. These attacks pose significant risks to secure communications, as they can lead to unauthorized access to sensitive information, data theft, and malicious modifications in transmitted messages.

One of the common techniques used to execute a MITM attack is Address Resolution Protocol (ARP) Poisoning. ARP, a foundational protocol in local area networks (LANs)[6], is responsible for mapping IP addresses to physical MAC addresses, ensuring proper communication within the network. However, ARP lacks authentication mechanisms, making it vulnerable to spoofing attacks. In ARP poisoning, an attacker sends falsified ARP messages to associate their MAC address with the IP address of a legitimate device on the network, such as a router or a client. This manipulation redirects the network traffic through the attacker's device, enabling interception, data tampering, or even denial-of-service (DoS) attacks.

ARP poisoning is particularly dangerous because it is difficult to detect and can compromise both individual users and entire networks. Tools like Ettercap make it easier for attackers to perform ARP poisoning by automating the process of discovering network devices[7], spoofing ARP packets, and capturing data in real time. As a result, understanding ARP poisoning and its role in MITM attacks is critical for both network administrators and cybersecurity professionals.

This paper focuses on ARP poisoning using Ettercap, exploring how attackers exploit this vulnerability and providing insights into mitigation strategies to secure networks against such threats.

II. Implementation Steps

A. Enable IP Forwarding

Open the terminal in Kali Linux and run the following command: sysctl net.ipv4.ipforward=1 This command enables traffic forwarding. Without it, the Windows 11 machine will assume that the MITM system is the gateway but will not forward the traffic to the actual gateway.

B. Retrieve Network Details

Run the following command to note the IP and MAC addresses of the active network interface: ifconfig

```
PS C:\Users\vishwa> arp -a

Interface: 192.168.56.1 --- 0x4
  Internet Address      Physical Address      Type
  192.168.56.255        ff-ff-ff-ff-ff-ff     static
  224.0.0.7             01-00-5e-00-00-07     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  224.0.0.253           01-00-5e-00-00-fd     static
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 172.30.16.188 --- 0xb
  Internet Address      Physical Address      Type
  172.30.16.1           9c-5a-80-b2-8b-00     dynamic
  172.30.16.9           04-0e-3c-e5-d0-02     dynamic
  172.30.16.13          6c-3b-e5-04-cc-47     dynamic
  172.30.16.52          40-b0-34-21-60-3d     dynamic
  172.30.16.113         3c-2a-f4-82-54-30     dynamic
  172.30.16.157         c0-18-03-54-8d-a7     dynamic
  172.30.16.172         14-07-08-1a-e8-80     dynamic
  172.30.16.199         f8-a2-6d-9d-07-80     dynamic
  172.30.16.204         88-b8-63-31-1d-dd     dynamic
  172.30.16.209         14-58-d0-3d-f9-00     dynamic
  172.30.16.226         c0-18-03-54-cb-4d     dynamic
  172.30.16.230         c0-18-03-54-cb-a7     dynamic
  172.30.16.234         c0-18-03-a3-81-90     dynamic
  172.30.16.252         00-1e-c9-2b-11-f3     dynamic
  172.30.17.25          28-c5-c8-1f-f7-65     dynamic
```

Fig. 1. Network details of victim system

C. Start Ettercap and Wireshark

Launch Ettercap for ARP poisoning. Open Wireshark in the background to monitor network traffic[1].

D. Search for Hosts

In Ettercap, click on the *Search* button to scan the network. This will list all active systems along with their IP and MAC addresses.

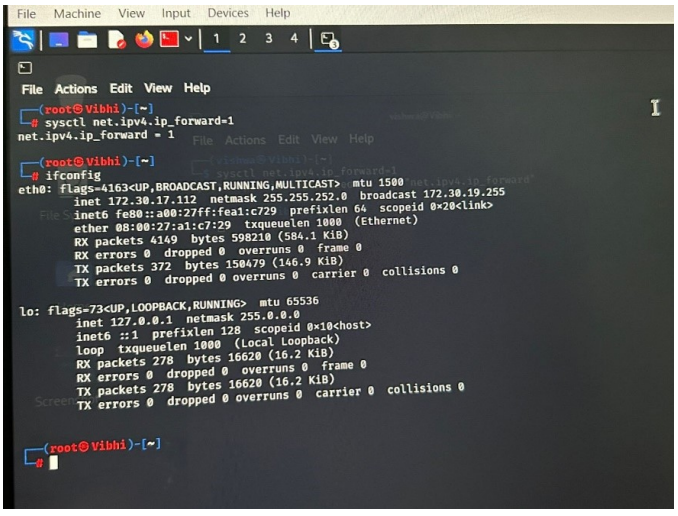

Fig. 2. Hosts visible to kali linux

E. Add Hosts to the Host List

Select the desired systems from the search results and add them to the host list.

F. Set Targets

Add the Windows 11 IP address as **Target 1** and its gateway as **Target 2**.

G. Enable ARP Poisoning

Go to the MITM menu in Ettercap and select *ARP Poisoning*[4].

H. Verify ARP Table on Windows

Open the Command Prompt on the Windows machine and run the following command: arp -a Observe that the MAC address of the default gateway has been replaced by the MAC address of the MITM machine (Kali Linux), indicating successful poisoning.

```
Interface: 172.30.16.188 --- 0xb
  Internet Address      Physical Address      Type
  172.30.16.1           08-00-27-a1-c7-29     dynamic
  172.30.16.9           04-0e-3c-e5-d0-02     dynamic
  172.30.16.13          6c-3b-e5-04-cc-47     dynamic
  172.30.16.52          40-b0-34-21-60-3d     dynamic
  172.30.16.113         3c-2a-f4-82-54-30     dynamic
  172.30.16.157         c0-18-03-54-8d-a7     dynamic
  172.30.16.158         00-68-eb-c8-e4-24     dynamic
  172.30.16.172         14-07-08-1a-e8-80     dynamic
  172.30.16.199         f8-a2-6d-9d-07-80     dynamic
  172.30.16.204         88-b8-63-31-1d-dd     dynamic
  172.30.16.209         14-58-d0-3d-f9-00     dynamic
  172.30.16.226         c0-18-03-54-cb-4d     dynamic
  172.30.16.230         c0-18-03-54-cb-a7     dynamic
  172.30.16.234         c0-18-03-a3-81-90     dynamic
  172.30.16.252         00-1e-c9-2b-11-f3     dynamic
  172.30.17.25          28-c5-c8-1f-f7-65     dynamic
  172.30.17.46          bc-5f-f4-f7-66-fb     dynamic
```

Fig. 3. ARP table

I. Capture ARP Packets in Wireshark

In Wireshark on Kali Linux, look at the first ARP packet. This is the packet used to initiate the attack.

J. Analyze Ethernet Packets

Examine the Ethernet details in Wireshark. Observe that the source IP is the Windows 11 machine, but the source MAC is that of the MITM machine.

K. Expand ARP Opcode Reply

Expand the ARP section in Wireshark. Notice an unsolicited ARP reply (Opcode 2) where the IP address belongs to Windows 11, but the MAC address belongs to the MITM machine (Kali Linux).

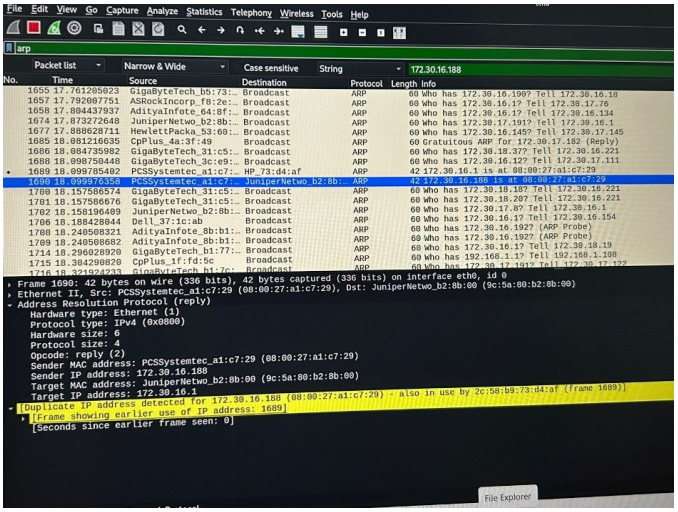

Fig. 4. wireshark

L. Ping a Website

From the Windows 11 machine, ping a website (e.g., https://www.google.com): ping www.google.com Observe the ping replies being forwarded through the MITM system[2].

M. Browse a Website

Open a browser on the Windows 11 machine and visit any website. Monitor the network traffic in Wireshark on Kali Linux.

N. Capture Sensitive Information

Use HTTP request inspection in Wireshark to observe confidential information such as passwords being transmitted over the network[3].

III. Capturing ARP Poisoning Attack Using Wireshark

A. Start Capturing ARP Packets

Start capturing ARP packets on Windows 11.

B. Click on Unsolicited Replies

Click on any unsolicited replies.

C. Filter Unsolicited ARP Replies

To filter out the unsolicited ARP replies, follow these steps: label=**Step 0:**

1) Prepare a filter as `selected` for `[Duplicate IP address configuration (duplicate_ip address)]`.
2) Create a new profile (e.g., `Security`).
3) Apply the filter for the sender IP address `[gateway's IP address]` as `selected`.
4) Apply the filter for Opcode as `and selected`.
5) Apply the filter for sender's MAC address of the legitimate ARP as `and not selected`.
6) Apply this filter, and you will see the spoofed MAC addresses.

D. Save the Filter

Save the filter and give it a label (e.g., `ARP Poison Attack`).

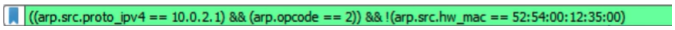

Fig. 5. Filter.

E. Use the Filter

Now you can use this filter to check for any unsolicited ARP replies.

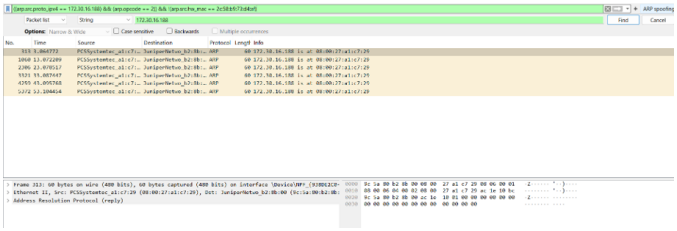

Fig. 6. Capturing ARP packets using Filter.

IV. Prevention of ARP Poisoning Attacks

ARP poisoning attacks can compromise the integrity and security of a network. Below are three key preventive measures to mitigate the risk of such attacks:

A. Use of Virtual Private Networks (VPNs)

Virtual Private Networks (VPNs) provide an encrypted tunnel for internet communication. When a VPN is used, all online activities and data transmissions are encrypted, making it significantly harder for attackers to execute ARP spoofing.

B. Static ARP Entries

Creating static ARP entries for frequently communicating hosts can provide an additional layer of protection. A static ARP entry creates a permanent mapping in the ARP cache, preventing malicious ARP responses from altering the communication route.

C. Use of Detection and Monitoring Tools

Detection tools, such as `XArp`, can help identify when an ARP spoofing attack is underway. In addition, robust monitoring tools should be employed to continuously track network activity and alert administrators to suspicious behavior.

V. Conclusion

ARP poisoning is a significant security threat in local networks that can lead to unauthorized access, data interception, and even complete network compromise. Understanding how this attack is carried out and the various methods to exploit it is crucial for safeguarding networked systems[9].

Our work has explored the attack's methodology and demonstrated the steps involved in executing it. By raising awareness of ARP poisoning and its consequences, we hope to emphasize the importance of implementing effective mitigation strategies such as using VPNs, creating static ARP entries, and deploying detection and monitoring tools. Through these measures, we can better protect networks from the dangers posed by ARP poisoning attacks.

References

[1] https://www.youtube.com/watch?v=cVTUeEoJgEg

[2] https://support.eset.com/en/kb2933-arp-icmp-or-dns-cache-poisoning-attack-in-eset-home-products-for-windows

[3] https://github.com/Ettercap/ettercap

[4] https://www.cisa.gov/resources-tools/services/ettercap

[5] Al Sukkar, G., Saifan, R., Khwaldeh, S., Maqableh, M., Jafar, I. (2016). Address resolution protocol (ARP): Spoofing attack and proposed defense.

[6] Galal, A. A., Ghalwash, A. Z., Nasr, M. (2022). A new approach for detecting and mitigating address resolution protocol (ARP) poisoning. International Journal of Advanced Computer Science and Applications, 13(6).

[7] Gouda, Mohamed G., and Chin-Tser Huang. "A secure address resolution protocol." Computer Networks 41.1 : 57-71.

[8] Bruschi, Danilo, et al. "Formal verification of ARP (address resolution protocol) through SMT-based model checking-A case study." Integrated Formal Methods: 13th International Conference, IFM 2017, Turin, Italy, .

[9] Stepanov, P. P., et al. "The problem of security address resolution protocol." Journal of Physics: Conference Series. Vol. 1791. No. 1. IOP Publishing, 2021.