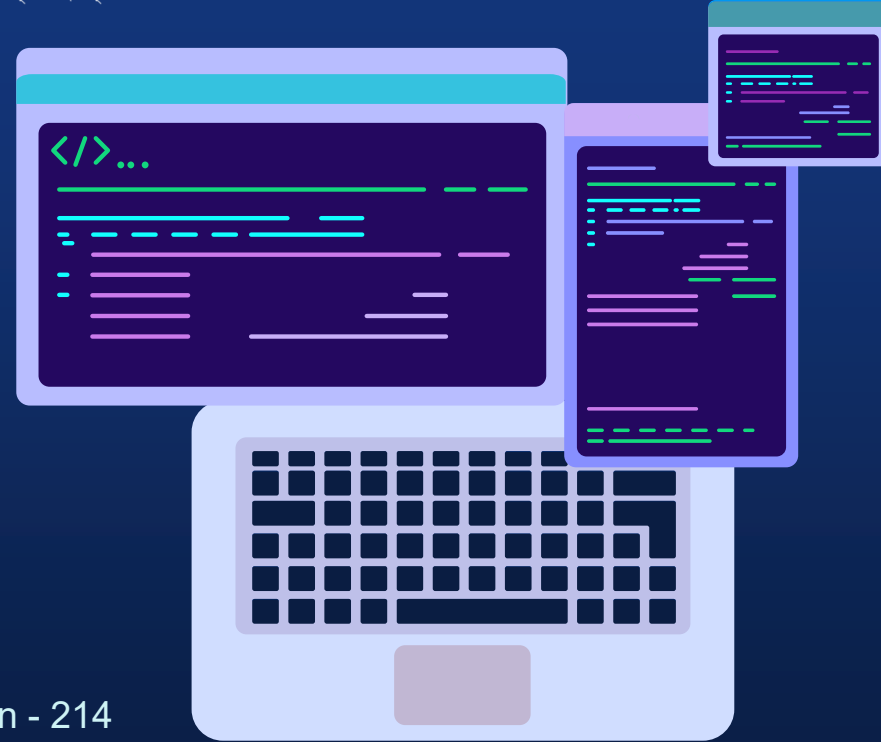




AMRITA
VISHWA VIDYAPEETHAM

Detection & Prevention of ARP Spoofing Attacks in Local Area Networks



Team 7 :
G Prajwal Priyadarshan - 214
Kabilan K - 224
Kishore B - 227
Rahul L S - 248

TABLE OF CONTENTS

- 01 Introduction
- 02 Problem Statement
- 03 Methodology
- 04 Expected Outcomes





Introduction :

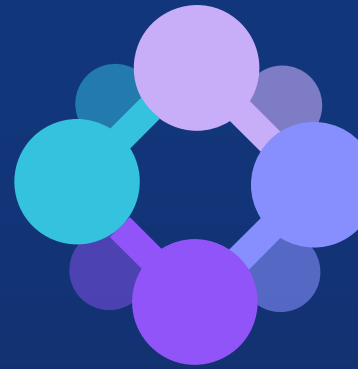

In today's digital world, networks form the backbone of communication between devices, whether it's checking emails, browsing the internet, or sharing files

One of the major security risks in local networks is something called **ARP spoofing**. It's a type of attack where a malicious device pretends to be someone. It is not, like tricking our computer and sending sensitive data to the wrong person.

ARP (Address Resolution Protocol),
It helps devices in a local network map **IP addresses** to **MAC addresses**. ARP has **no security or authentication**.

It helps devices talk to each other doesn't check whether the information it receives is actually true.

Spoofing (in networking) means **pretending to be someone else** to trick devices or people.



IP: 192.168.1.37

MAC - CC:CC:CC:CC:CC:CC

ARP SPOOFING



IP: 192.168.1.23

MAC - BB:BB:BB:BB:BB:BB



IP: 192.168.1.1

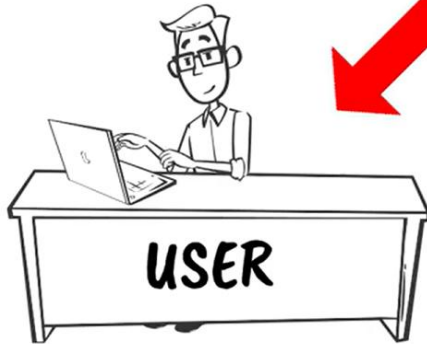
MAC - AA:AA:AA:AA:AA:AA



**WORLD WIDE WEB
(WWW)**

IP: 192.168.1.1 IP: 192.168.1.23
MAC - CC:CC:CC:CC:CC:CC

ARP SPOOFING



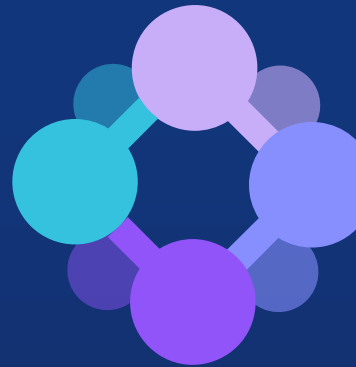

IP: 192.168.1.23
MAC - BB:BB:BB:BB:BB:BB




IP: 192.168.1.1
MAC - AA:AA:AA:AA:AA:AA



WORLD WIDE WEB
(WWW)



We will be proceeding like, how ARP spoofing can be detected and stopped, and how simple encryption tools can make a big difference in keeping networks secure.



PROBLEM STATEMENT



- **ARP (Address Resolution Protocol)** is used in LANs to map IP addresses to MAC addresses.
- **ARP is inherently insecure** because it does not authenticate messages.
- An attacker in the same LAN can send **fake (spoofed) ARP replies** to associate their MAC address with the IP of another device (e.g., the router).
- This allows the attacker to:
 - Intercept sensitive data (Man-in-the-Middle attack)
 - Modify or block network traffic
 - Hijack sessions or credentials
- These attacks are **hard to detect manually** and can compromise the privacy, integrity, and availability of the network.
- Hence, there is a need for an **automated system** to:
 - **Detect** abnormal or spoofed ARP activity
 - **Prevent** such attacks in real-time to secure the LAN



Methodology

A. Network Environment Setup

- Simulate a LAN using virtual machines or physical systems.
- Deploy legitimate clients and a malicious attacker to mimic real-world ARP spoofing behavior.

B. Detection Techniques

- Monitor ARP tables for frequent or unusual MAC-IP mappings.
- Use tools like **Wireshark** and **ARPWatch** to log ARP traffic and identify anomalies.
- Develop or integrate a custom script to detect multiple IPs mapping to a single MAC address or vice versa.





Methodology

C. Prevention Techniques

- Implement **Static ARP entries** for critical devices (e.g., gateway, servers).
- Use **Packet filtering** with firewalls to restrict ARP traffic.
- Employ **Dynamic ARP Inspection (DAI)** in managed switches for hardware-level protection.
- Optionally, test the use of **SSH tunneling or VPN** to secure sensitive communications even in the presence of spoofing.

D. Testing and Evaluation

- Conduct spoofing attacks in the test LAN.
- Measure detection accuracy, response time, and data protection effectiveness before and after implementing the proposed countermeasures.






Goal & Predicted Output

- ❑ **Practical Demonstration** : Perform an ARP spoofing attack in a virtual LAN using tools like Ettercap, then capture and study how the attacker can intercept or change the communication between devices.
- ❑ The goal is to
 - Intercept or modify data going between two devices on the network.
 - Capture packets and study how an attacker can watch or tamper with communication.

Expected Results :

- ❑ Show that ARP poisoning is a major threat in LANs.
 - ❑ Demonstrate how attackers can intercept or block data.
 - ❑ Analyze how network traffic can be exploited.
 - ❑ Recommend simple methods to prevent such attacks.
 - ❑ Enhance the overall security of LAN communication.
- 

Thank You !

