Explore Address Resolution Protocol Vulnerabilities through MITM Attack: A Packet Sniffer Abstract:

Abstract:

In the world of computer networking, communication between devices is vital for the exchange of information. However, this communication can be intercepted by malicious individuals who seek to gain unauthorized access to sensitive data. One of the most common ways that attackers carry out such attacks is through the use of man-in- the-middle (MITM) attacks .

These attacks are often executed by exploiting vulnerabilities in network protocols that lack proper authentication mechanisms. One such protocol is the Address Resolution Protocol (ARP), which is responsible for mapping network addresses (such as IP addresses) to physical addresses (such as MAC addresses).

Unfortunately, ARP is vulnerable to spoofing attacks, which can be used to intercept network traffic and carry out MITM attacks.

To explore the vulnerability of the ARP protocol, I propose a packet sniffer that utilizes an ARP spoofer to intercept packets from another user on the network .

My approach will leverage the flaw in ARP to carry out a MITM attack, which will allow us to eavesdrop on and potentially modify network traffic. In the proposed approach, a Windows will be used as the environment and Python as the programming language. Additionally, I will utilize the Scapy library, which is a powerful packet manipulation tool, to implement the packet sniffer and ARP spoofer .

By evaluating the efficiency of ARP and exploring its vulnerabilities, I hope to shed light on the importance of secure network protocols and the need for proper authentication mechanisms to prevent MITM attacks