***ARP and IP Spoofing Report***

***Introduction***

ARP (Address Resolution Protocol) and IP spoofing are critical techniques in the realm of cybersecurity, particularly in the context of network attacks and defense mechanisms. ARP spoofing enables an attacker to intercept network traffic by sending false ARP messages, thus associating their MAC address with the IP address of another device. IP spoofing, on the other hand, involves sending packets from a forged IP address, which can be used for various attacks, including denial of service and network reconnaissance. This report explores the methodologies of ARP and IP spoofing using tools available in Kali Linux, as well as techniques for detecting and defending against these types of attacks.

***Purpose***

The purpose of this lab is to demonstrate the practical application of ARP and IP spoofing, highlighting the potential vulnerabilities in network environments and how attackers can exploit them. Additionally, the lab aims to showcase the tools and techniques used for detecting these attacks, thus contributing to the development of robust security measures.

***Scope***

The lab consists of three primary parts:

ARP Spoofing with arpspoof: Intercepting network traffic between two devices by poisoning ARP caches.

IP Spoofing with hping3: Crafting and sending forged packets with a fake IP address to test network resilience against IP spoofing.

Detecting and Defending Against Spoofing Attacks: Utilizing tools like Wireshark and arpwatch to monitor and defend against spoofing attacks.

***Overview***

The evaluation covered the critical aspects of ARP and IP spoofing and their implications for network security. In Part 1, the ARP spoofing technique was implemented, demonstrating how attackers can redirect traffic and potentially capture sensitive data. Part 2 involved IP spoofing using hping3, illustrating how forged packets can confuse target systems. Finally, in Part 3, methods for detecting and defending against these attacks were discussed, highlighting the importance of proactive security measures.

***Results:***

***Part 1: ARP Spoofing With Arpspoof***

A screenshot of a computer

Description automatically generated

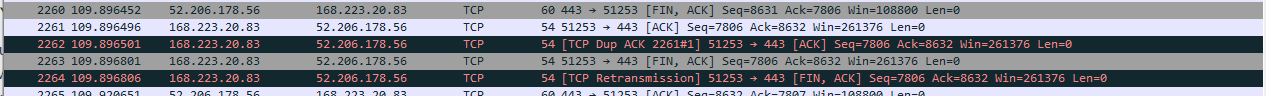


A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated



A screenshot of a computer program

Description automatically generated

***Part 2: IP Spoofing With Hping3***

A screen shot of a computer

Description automatically generated

A screen shot of a computer

Description automatically generated

***Part 3: Detecting and Defending Against Spoofing Attacks***

A screenshot of a computer program

Description automatically generated

A screenshot of a computer

Description automatically generated