ARP Poisoning Detection Tool

What is ARP and ARP Poisoning?

ARP is a protocol that makes it possible for network messages to get to a particular network device. ARP converts Media Access Control (MAC) addresses into Internet Protocol (IP) addresses and the other way around. Devices often utilize ARP to get in touch with the router or gateway that gives them access to the Internet.

ARP spoofing, sometimes referred to as ARP poisoning, is a Man in the Middle (MitM) attack that enables attackers to eavesdrop on network device traffic. It involves a threat actor sending fake ARP packets across a LAN. As a result, the IP address of an authorized computer or server on the network is linked to the MAC address of an attacker. The attacker will start receiving any data meant for that IP address as soon as the attacker's MAC address is linked to a genuine IP address.

Functioning of the Tool

This tool checks of ARP poisoning is happening or not by checking the ARP cache and looking for anomalies in the output file.

This tool is written in **Python** language and the following modules are used:

- *os*
- *itertools*
- *getpass*

Tool starts with running ***arp -a*** command on CMD and saving the output in a text file in ***C:\Users\Public*** directory. Then the output text file is formatted to ignore unnecessary string like “internet”, “interface”, etc. Now only IP Addresses and their corresponding MAC addresses are remaining and they are added as a key-value pair in a dictionary where key is IP Address and Value if MAC address.

The IP Addresses are unique and MAC Addresses are supposed to be unique. If any two IP Addresses have same MAC Address and ARP Poisoning is detected.

Two functions ***getPoisonedIPs(dict)*** and ***getPoisonedMACs(dict)*** are used to find these anomalies in the output file.

How to Install and Run the Tool

Simply download ***main.py*** file and run the tool on the victim machines.