IPCONFIG and ARP

1. Overview and Goal of Document

   Explain the commands Ipconfig and Arp in regards to what they are, what they do, and their association to the DNS Poisoning Application Project being conducted for VCU CMSC414

2. Associated program code

   Network_Retrieval.py

1. IPCONFIG

1.1. Overview

Ipconfig is a console application program of the Windows and MacOS operating systems. This command displays all Transmission Control Protocol / Internet Protocol (TCP/IP) network configuration values and is able to refresh all Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS) settings. In MacOS the ipconfig command is a wrapper for the IPConfiguration agent. The proper syntax of the Ipconfig command is ‘ ipconfig /parameterName ’

1.2. Purpose in Project

Ipconfig was used within the Network_Retrievel.py file to retrieve three pieces of information. These being the DNS-Suffix of the host connected network, the host assigned IP address, and the subnet mask of the connected network. These sources of info are utilized to determine the host connection to a network and which arp table will need to be examined to return the correct IPs and MACs.

2. ARP

2.1. Overview

Address Resolution Protocol (ARP) is a protocol for mapping Internet Protocol (IP) addresses to physical Media Access Control (MAC) addresses on a local area network (LAN). When two computers wish to communicate to each other over a network they would do so through a Layer 3 connection utilizing IPs. However, in order for the network’s Layer 2 devices to determine where the information of this communication needs to broadcasted the systems MAC address is used (MAC of a system is permanent). For this reason ARP is used to maintain a cache of all systems that have communicated over the network. This cache includes the IP assigned to the system and its corresponding MAC address. The proper syntax of the arp command is ‘ arp -flag ‘.

2.2. Purpose in Project

Arp was used within the Network_Retrieval.py file to retrieve the IP and MAC address of every system connected to the same network as the host. This information will be used in later parts of the project to allow for the host to conduct a Man in the Middle Attack on connected systems.