**ARP Cache Poisoning**

•What is ARP?

Address Resolution Protocol

You remember we use DNS to map hostnames to IP addresses

We use ARP to map IP addresses to MAC addresses

**•What is a MAC address?**

Media Access Control

The address of a network interface

•Normally a host will broadcast a request like:

Which computer has 192.168.1.15?

•Then, the host with that IP will respond

I do and my MAC is A1:B1:C1:D1:E1:F1!

•Every computer has an ARP cache that holds these IP to MAC address mappings

•Run the following command in Windows:

arp-a

•However, ARP allows any host to send a response even if no request was initiated

This is called Gratuitous ARP

•Therefore, an attacker could poison the ARP cache to direct traffic however they want!

•Attacker mustbe on the same network as the victim to poison the ARP cache

•Attacker sends two Gratuitous ARP responses:

First one to update Victim’s ARP cache

oHey, the Gateway’s IP is at attacker’s MAC address!

Second one to update Gateway’s ARP cache

oHey, the Victim’s IP is at attacker’s MAC address!

•Attacker enables IP forwarding on their host to intercept and forward all incoming and outgoing traffic

•Attacker can now intercept all incoming and outgoing transmissions between the Victim and any other host on the Internet!