**ARP Poisoning**

The interception of the vulnerability for the time it takes for a router to make an arp response with its MAC addr to a target machine where the arp table updates

Trick the target into thinking you’re the router and tricking the router into thinking you are the target machine

The MITM will send out arp response at a much quicker rate than the router sends out requests

* So when the router finally sends out the request, it’ll have already seen our response and accepted it before the real response even gets through

Telling the target that we are the router

* Arpspoof -i eth0 -t 192.168.0.9 -r 192.168.0.1
  + -i # ethernet device
  + -t # target
  + -r # router

Telling the router that we are the target

* Arpspoof -i eth0 -t 192.168.0.1 -r 192.168.0.9

With these both running, open up wireshark and make sure eth0 is selected

* The traffic from 192.168.0.9 should be viewable

Forwarding must be set up on the MITM in order to allow internet traffic to flow seamlessly

**HW – Try using ettercap**