Task 1 – ARP Poisoning Attack to Discover IP Addresses:

In this task, I will show how to discover the IP address of a victim device from an adversary device via an ARP poison attack. To start, both devices will be on the same network (CSE425 Wi-Fi). In this ARP spoofing attack, I will change the IP table of the victim device such that the IP of the network router will be mapped to the MAC address of my adversary device. To do this, I will use a tool called Ettercap. First, I begin the Ettercap session, selected the desired network, and click accept. I can now go to the host list in Ettercap and view the IP addresses of both the router and the victim device. From there, I will add the targets IP addresses to my target list, both the router (192.168.29.1) as target 2 and the victim device (192.168.29.133) as target 1. Then I will go to the man in the middle menu and select Arp poisoning. I will then start sniffing, which will proceed to poison the ARP and conduct the attack. Now, when the victim goes to ping the router IP address, the packets will be accessible to my adversary device. To prove this, I can check the Wireshark output after the victim device pings the router IP (192.168.29.1). In this ouput, when filtering for ICMP, I can see that the packets that victim device pinged to the router IP are viewable from the adversary device. I can also filter by ARP and see that the router IP is being mapped to the MAC address of my adversary device. With the method laid out above, I can discover the victim IP address as well as poison the ARP which is necessary for completing task 2.

Task 2 – DNS Spoofing Attack to Redirect Traffic:

In this task, I will show how to redirect a victim device’s request to <http://www.cse.msu.edu> to an adversary device using a DNS spoofing attack. Here is how the attack works; when the victim device goes to their browser and searches a link, it needs to first find the mapped IP address to that URL. To do this, it goes to the DNS server and asks for the address. In this scenario, when the victim device goes to ask the DNS server, it will instead be asking the adversary device. In turn, the adversary device will respond with a malicious IP address on their server, not the victim’s requested website. To complete this DNS spoofing attack, the first task needs to be completed using Ettercap (ARP poisoning task) and up and running. Then, I can edit the etter.dns file in the Ettercap application on the adversary device with the lines “cse.msu.edu A 192.168.29.178 \*.cse.msu.edu A 192.168.29.178” to redirect traffic the victim device sends to <http://www.cse.msu.edu> to my adversary IP address, where I am running a default MacOS Apache server that displays the text “It Works”. By entering this line, when the victim devices goes to access <http://www.cse.msu.edu> in the browser, the DNS server that the adversary device is spoofing is going to reroute the IP address of that link from its authentic address to my malicious one. Next, I will go into Ettercap and click the plugins menu, and click the “dns\_spoof” option, which will begin the DNS spoofing attack. Now when I type in <http://www.cse.msu.edu> into the victim device’s browser, the DNS server map that link to the IP address set by my adversary device. I can also verify this by viewing the Wireshark output, which shows that the DNS query response requested by the victim device is mapping <http://www.cse.msu.edu> to the malicious IP address With the DNS spoofing attack, you can easily redirect the victims request to the adversary device and their desired server.