CSCI 530 - Lab-8

Rishit Saiya (rsaiya@usc.edu)

1. A router called Node 0 links two subnets together. Due to the fact that they are in two distinct subnets, Node 1 cannot directly ARP poison Node 4. ARP can only function within a subnet. Node 1 must acquire access to the router, which is Node 0 in our case, if it wishes to ARP poison Node 4.

2. Node 1 is operating maliciously under the conditions described in this section by using ARP spoofing to conduct a man-in-the-middle attack against Node 0. In the aforementioned situation, Node 1 will receive traffic from Node 2, which Node 1 can either change or send to Node 0 in its original form.

3. Node 1 is doing a man-in-the-middle attack in this instance. As a result, any packets sent between Nodes 4 and 2 can be intercepted by Node 1. Traffic has to go through Node 0 as communication can only happen that way, because of existence in different subnets. Using the sniffer Ettercap, an attacker can extract passwords from packets that contain plaintext. FTP, an insecure protocol, is utilized for transfer between Node 4 and Node 2. Passwords are either transferred in plaintext or perhaps with a weak encryption method using this protocol. The Ettercap sniffer can readily detect these username and password. As a result, Node 1 can quickly determine the user password provided by Node 2.

4. Due to ARP spoofing, a man-in-the-middle attack has occurred in this case. The ARP cache and ARP table entries should be cleared as a result. Static ARP is another defense against such an assault. Additionally, there are tools available for detecting ARP spoofing. Another choice is to communicate with other systems using authentication and data encryption methods. To stop malicious packets from entering, packet filtering technologies may also be used. ARP spoofing can potentially be avoided with the use of a VPN. Additionally, software programs that check websites for malicious code are available.