**Crafting man-in-the-middle founded on arp**

1. After looking at the topology, we see that node4 is out of the network, resulting in all the packets which it needs to send/receive happening through node 0. So if we poison the ARP cache of node0 from node1 for all valid IP addresses in the subnet of 10.1.1.0, all packets which node4 can possibly send to any host in the 10.1.1.0 subnet are intercepted by node1.
2. The packet route from node2 to node 0 is mapped by the following sequence- node2 sends a packet to the hardware address corresponding to node0’s IP address. This is node1’s hardware address. After receiving this packet, Node1 sends it to node0’s hardware address.
3. Node1 has poisoned the ARP cache of both node2 and node0. That is how it was able to figure out the username and password given by node2 to node4. Examining/forwarding the packets from and to node0 and node 2. All packets to node4 must flow through node2 since that is the only connection node4 has to the network. During the FTP login process node2 sent a packet containing the username and password to node0’s IP address which is then forwarded to node4. However the hardware address to which node2 sends the packet to belong to node1 and not node0 (because of cache poisoning). Since the username and password were sent as clear-text and node0 was filtering all packets it receives for these keywords, it was able to intercept and recover them.
4. Rebuilding after flushing all the contents of the ARP cache would be a quick fix. The images are restored back on the website correctly because of the proper entries in the ARP cache. An option of preventing someone from remounting an ARP poisoning attack would entail :
5. Moving the web server to the edge of the network so that a man in the middle ARP attack would not be physically possible. How this helps – the incoming requests are directly handled by the web server and are not passed through other hosts on the LAN.
6. Another option would be disabling processing of incoming ARP replies, which means - we only process ARP reply messages which correspond to outstanding ARP requests.