**ATTACK**

**a) Syncan**

First resolve all the addresses. We can then see using conversations that Ciscois trying to attack by sending Syn packs across all ports of HP so as to see which all ports are open. After filtering it can be seen that only ports 22,80 and 53 sent back an ACK packet which means they are open. Ports 70,113,31337 and 25 sent RST packet saying its closed. The ones that didnt reply are basically protected by a firewall.

**b) Assgn5**

First we resolve the network, physical and transport addresses and find that:

* 172.16.0.107 belongs to Dell.
* 74.125.95.147 belongs to HP.
* 12.153.20.41 belongs to Cisco.

Using endpoints and conversations we find that HP and Cisco never had a direct conversation through their actual IP addresses. It can be seen that concersations are going on between 172.16.0.107 and 12.153.20.41, which should be Dell and Cisco , however from the MAC addresses its seen that its between Dell and HP. This means that HP is the attacker and via methods of ARP poisioning, has copied the IP address of Cisco and is hence obtaining information which is meant for Cisco from Dell.

**By**

**Nihal Haneef**

**16CO128**