**CNA 432/532: OSI Layer Security**

**Instructor: Dr. Tirthankar Ghosh**

**Lab 2: ARP vulnerability: poisoning ARP cache and Person-in-the-middle attack**

**Submission due date: September 22, 2014 (in class)**

**Group Lab: In groups of 2**

1. Login to your Kali machine
2. Find IP and MAC addresses of two computers, A and B (as shown in the figure)
3. Enable packet forwarding on the Kali machine
4. Start Wireshark on the Kali machine, and start packet capture in the appropriate interface
5. Ping either machine A or B, and capture an ARP reply
6. Save the captured packet as a binary file (select the entire frame and select Export Selected Packet Bytes)
7. Open the saved file with a hex editor (hexedit –b <filename>)
8. Modify the file to create a forged ARP reply spoofing A’s MAC address, save it with a different name (say, arp\_reply\_A)
9. Modify the file to create a forged ARP reply spoofing B’s MAC address, save it with a different name (say, arp\_reply\_B)
10. Send arp\_reply\_A to B, and send arp\_reply\_B to A (use file2cable to send the packets)
11. Write a script to send these forged ARP reply packets to both A and B every 2 seconds
12. Start ftp server at B
13. From A: try to login to B using ftp using any made-up username and password
14. Run dsniff on the Kali machine, and sniff the username and password
15. Write a report of your analysis of ARP vulnerability explaining ARP cache poisoning and describing the attack

Network topology:

Switch

Kali machine

Host B

Host A