**LAB REPORT, DAY 3**

**NETWORK SNIFFING AND ATTACKS**

**Objective:** To explore network sniffing and different network layer attacks was our main goal on this lab day. The emphasis is laid on getting grip of how to use tools like Wireshark and TCPdump for network analysis as well as understanding these attacks.

**Network Sniffing**

**The Tools Used for this task was:**

**Wireshark**: A graphical tool used to capture and analyze network traffic.

**TCPdump**: A command-line tool for packet capturing and analyzing networks.

Process followed: Wireshark involves selecting the right network interface and starting the process of capturing. TCPdump by specifying network interfaces captures traffic.

**ARP Cache Poisoning**

**Overview**:ARP cache poisoning (also known as ARP spoofing) works by sending fake ARP messages to a network which make devices associate the attacker’s MAC address with IP address of another device e.g., a router; hence the attacker can intercept, modify or block data meant for the target device.

**Solutions**: on completion of the class we had a discussion about what should be done in order to protect our systems from such problems. From our conclusions, we need to do some things like: Use static ARP entries for critical devices. Enable port security on network switches. Regularly monitor network activity for unusual ARP traffic.

**DHCP Starvation & Spoofing**

**Overview**: DHCP Starvation: In this attack, an attacker floods the DHCP server with requests thereby exhausting the pool of available IP addresses leaving legitimate users without an IP address disrupting their access into networks.

**Conclusion**

We gained first hand experience about Network sniffing as well as various networking attacks in Lab Day 3.The knowledge of these techniques is crucial in network analysis and defense too.Issues stemming from these attacks can however be protected against through installation of adequate security measures such as enabling DHCP snooping, using static ARP entries and correctly configuring VLANs.