Sniffing/Spoofing Attacks (CS 915)

Post-Lab Assignment (100 marks)

1. Task 1: Explain how you use Scapy, Wireshark and tcpdump to sniff packets. Present sniffing attack results with screenshots. [10]

2. Task 2: Explain how you modify the provided code to spoof ICMP packets and the rationale for the modification. Present spoofing attack results with screenshots. [20]

3. Task 3: Explain how you do the sniff-then-spoof attack in Task 3. Present the attack results with screenshots. [20]

4. Answer the following two questions in Task 3. [10]

    - In the sniffing and then spoofing experiment in the lab, why can you get the echo reply from 1.2.3.4 which does not exist on the Internet? [5]

    - In the above experiment, why can't you get the echo reply from 10.9.0.99? [5]

5. As we have learned for a program to turn on the promiscuous mode or to simply be able to sniff packets on the local machine, the program needs to have a special privilege; normal users do not have that privilege. With this in mind, we checked the privilege of the Wireshark process like the following:

```
$ pgrep wireshark
7598
$ ps  -fp 7598
UID   PID   PPID  C STIME TTY  TIME     CMD
seed  7598     1  0 10:01 ?    00:00:01 /usr/bin/wireshark
```

    From the result, we can see that the UID (effective user ID) of the Wireshark process is seed. We also know that Wireshark can capture all the packets on the local network, regardless of whether a packet is from/to where the program runs. This does not seem possible based on the knowledge that a sniffer program requires the root privilege for sniffers to work. Please conduct an investigation to explain why Wireshark is still able to sniff packets. (40 marks)

    Hint: start packet capturing in Wireshark, and then show what child process is launched by Wireshark. You can use the "pstree -p 7598" command to get the IDs of process 7598's child processes. Focus on the program executed by the child processes. You can use **getcap** to find out what special Linux capabilities a program has. Include screenshots of the commands and outputs when necessary in your explanation.