Logo

Description automatically generated

Clemson University

**Lab-2: ICMP Redirect Attack Lab.**

**CPSC:8570**

**Spring- 2022**

Course Instructor: Dr. Long Cheng

**Lab by:**

**Sai Vinay Nandigam**

**CUID: C17742253**

**Task-1: Launching ICMP Redirect Attack**

**Graphical user interface, text, application, email

Description automatically generated**

**Question-1:** Can you use ICMP redirect attacks to redirect to a remote machine? Namely, the IP address assigned to icmp.gw is a computer not on the local LAN. Please show your experiment result, and explain your observation.

**Question-2:** Can you use ICMP redirect attacks to redirect to a non-existing machine on the same network? Namely, the IP address assigned to icmp.gw is a local computer that is either offline or non-existing. Please show your experiment result, and explain your observation.

**Question-3:** If you look at the docker-compose.yml file, you will find the following entries for the malicious router container. What are the purposes of these entries? Please change their value to 1, and launch the attack again. Please describe and explain your observation.

**Task-2: Launching the MITM Attack**

**Question-4:** In your MITM program, you only need to capture the traffics in one direction. Please indicate which direction and explain why.

**Question-5:** In the MITM program, when you capture the nc traffics from A (10.9.0.5), you can use A’s IP address or MAC address in the filter. One of the choices is not good and is going to create issues, even though both choices may work. Please try both, and use your experiment results to show which choice is the correct one, and please explain your conclusion.