Snort Lab

|  |
| --- |
| * This is a lab assignment, and worth 5 points.
* The due date is the same day midnight.
 |

**Task 1.**

* Create a Snort rule that captures ICMP Echo Request from Kali and shows alerts with the message “Alert! ICMP”. (The *icode* and *itype* options are not necessary.)
* Send five (5) ICMP Echo Request messages from the Kali.
* Display your Snort rule.



* Go to **c:\snort\log** and find the **alert.ids** file. Open it with a text editor. Provide a screenshot for the five alerts you have captured. The following is an example.



