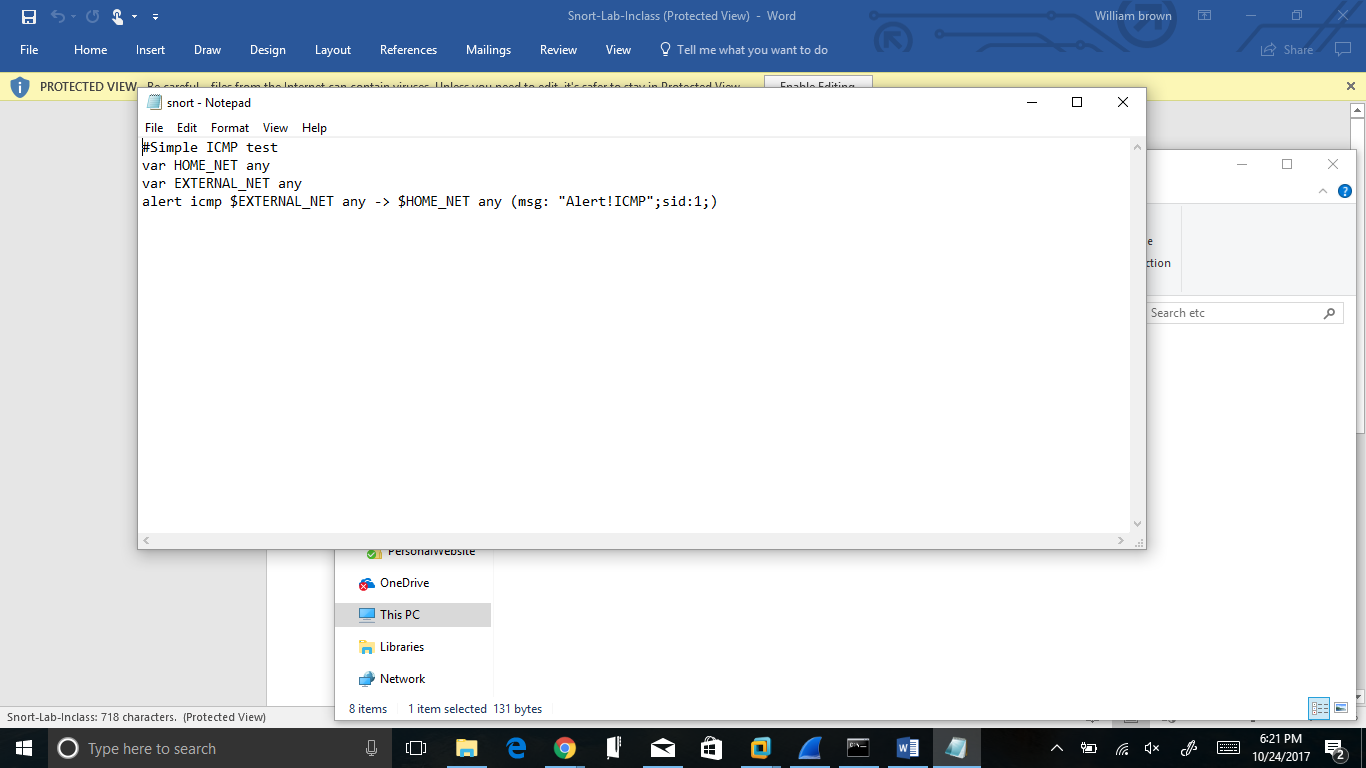
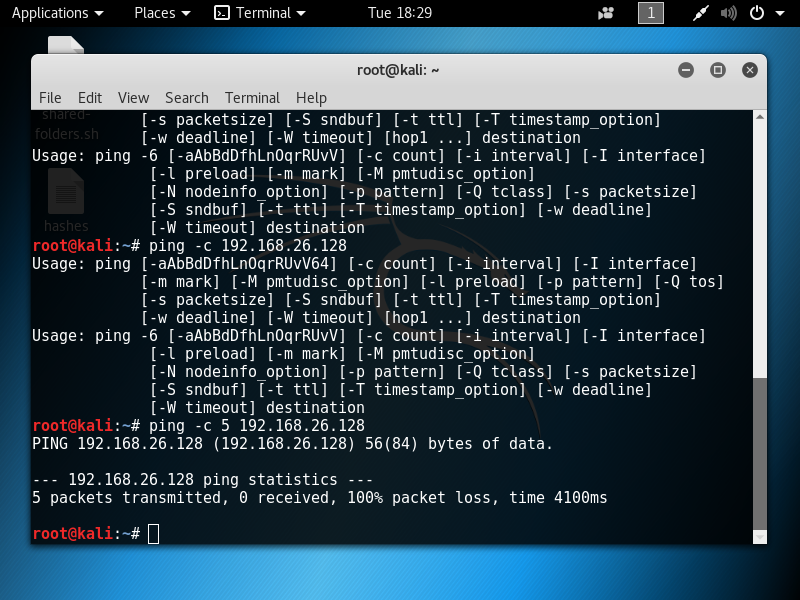
Snort Lab (In Class)

|  |
| --- |
| * This is an individual assignment, and you may collaborate with other students. * The due date and time is tonight. * For this assignment, you should use Snort on Windows host and Kali. * This is the first task of the Snort Lab Assignment. Finish it as much as you can and then submit. * Follow the usual naming convention. |

**Task 1.**

* Create a Snort rule that captures ICMP Echo Request from the 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 using hping3. You should process this request in a single command line.
* 
* Go to **c:\snort\log** and find the **alert.ids** file. Open it with **Wordpad**. Provide a screenshot like below for the ICMP alerts. Provide your own screenshot.

