Snort Lab Assignment

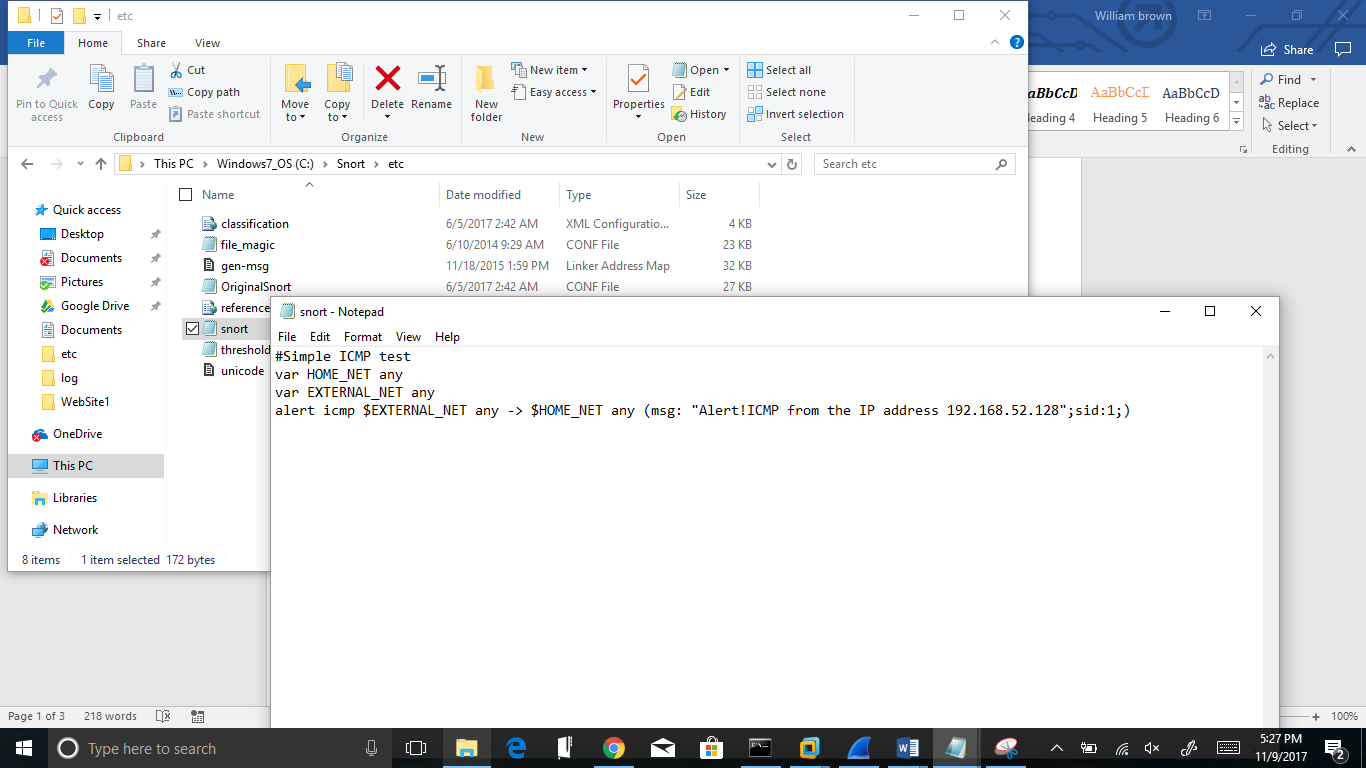
|  |
| --- |
| * This is a group assignment, and you may work with another student. * The due date is Saturday, November 4th midnight (after Test 2). * For this assignment, you use Snort on Windows host and Kali. * Follow the usual naming convention. Use the file “Snort-Assignment-Outcome.docx” for submission. |

**Task 1.**

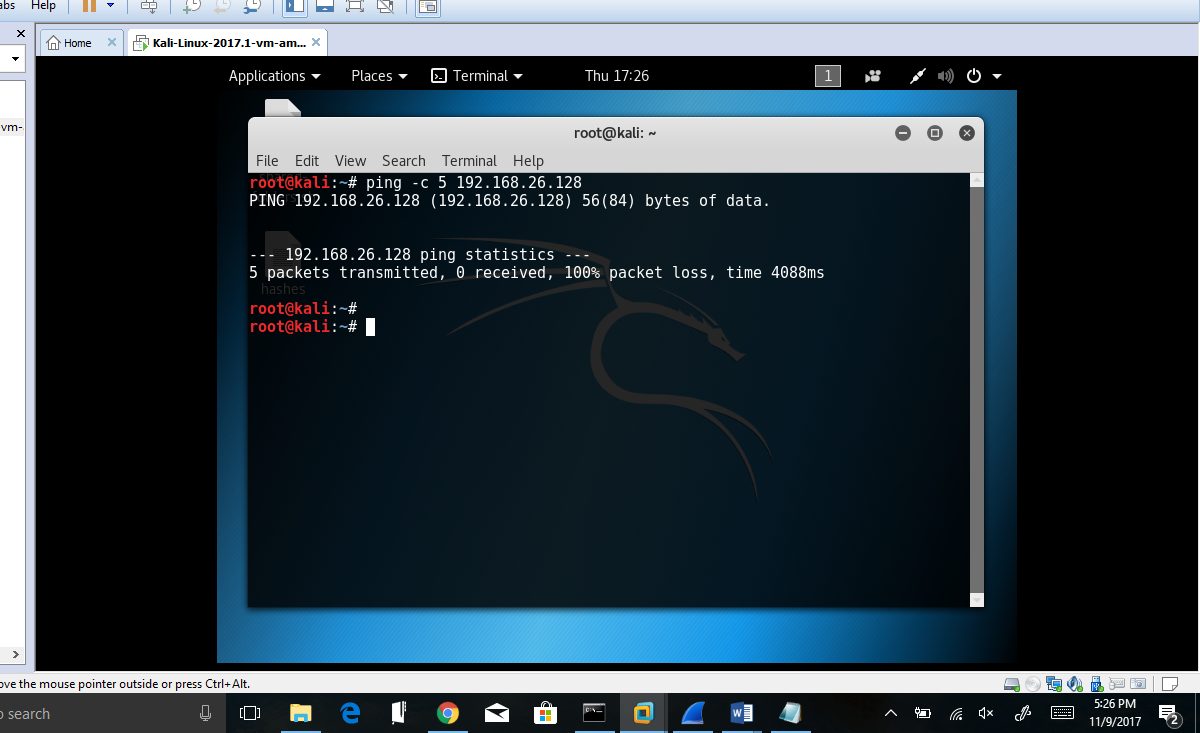
* Display your Snort rule.
* Display the hping3 command you have used.
* Go to **c:\snort\log** and find the **alert.ids** file. Open it with **Wordpad**. Provide a screenshot like below for the ICMP alerts. Provide your own screenshot.

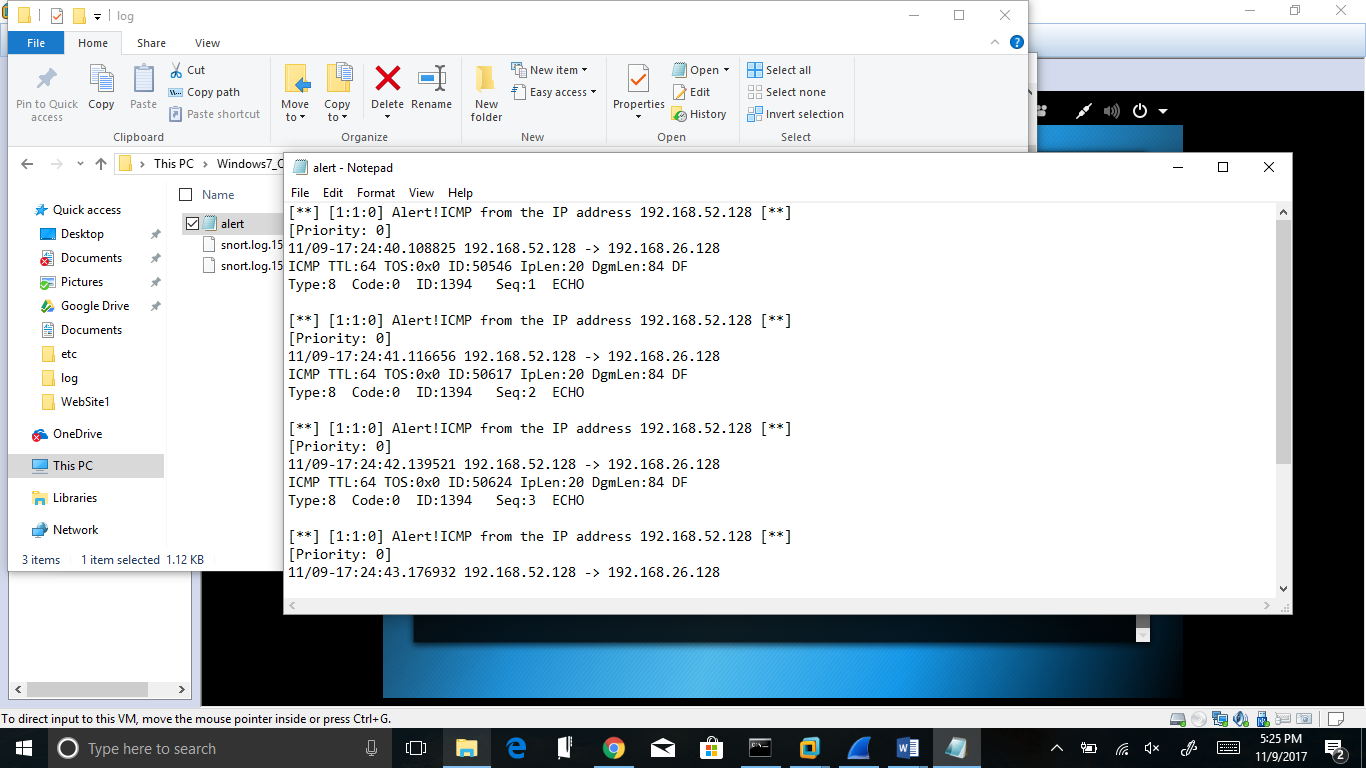
**Task 2.**

* Display your Snort rule.



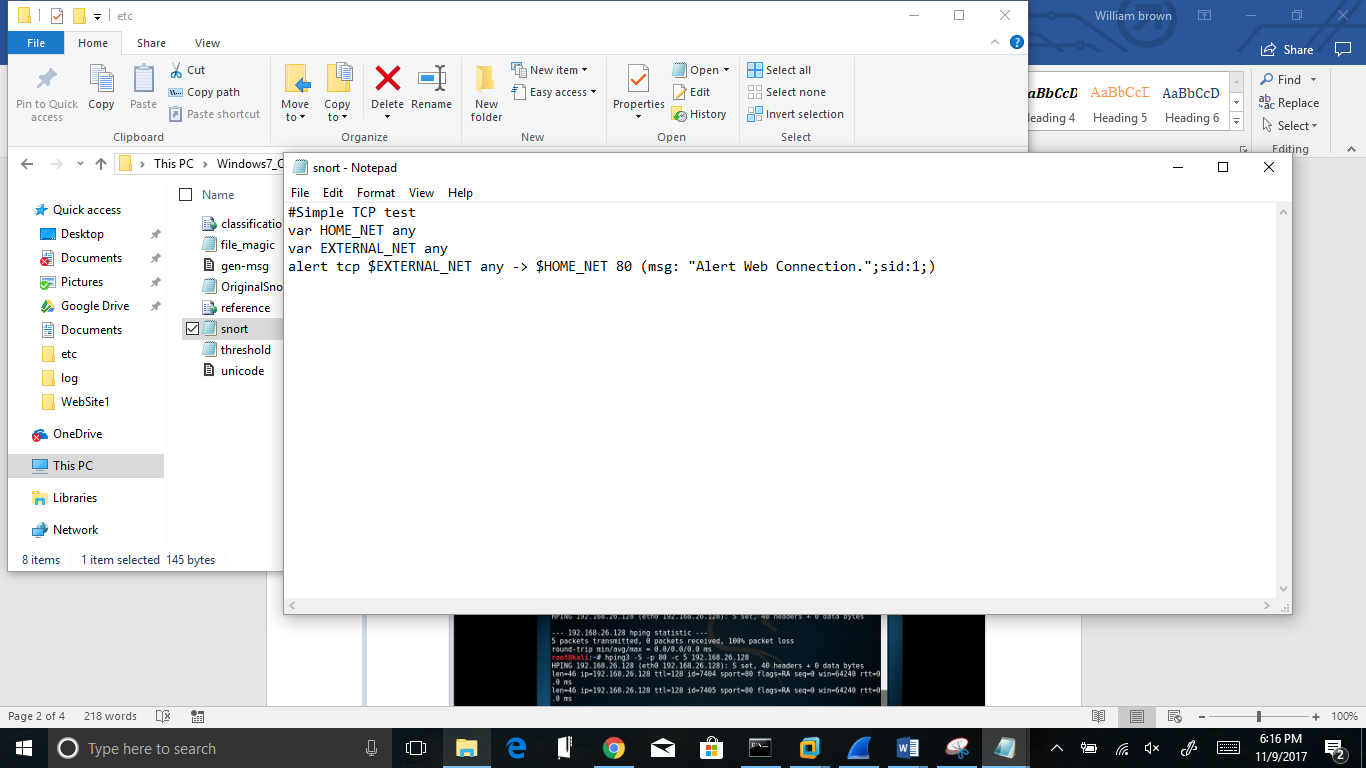
* Display the hping3 command you have used.



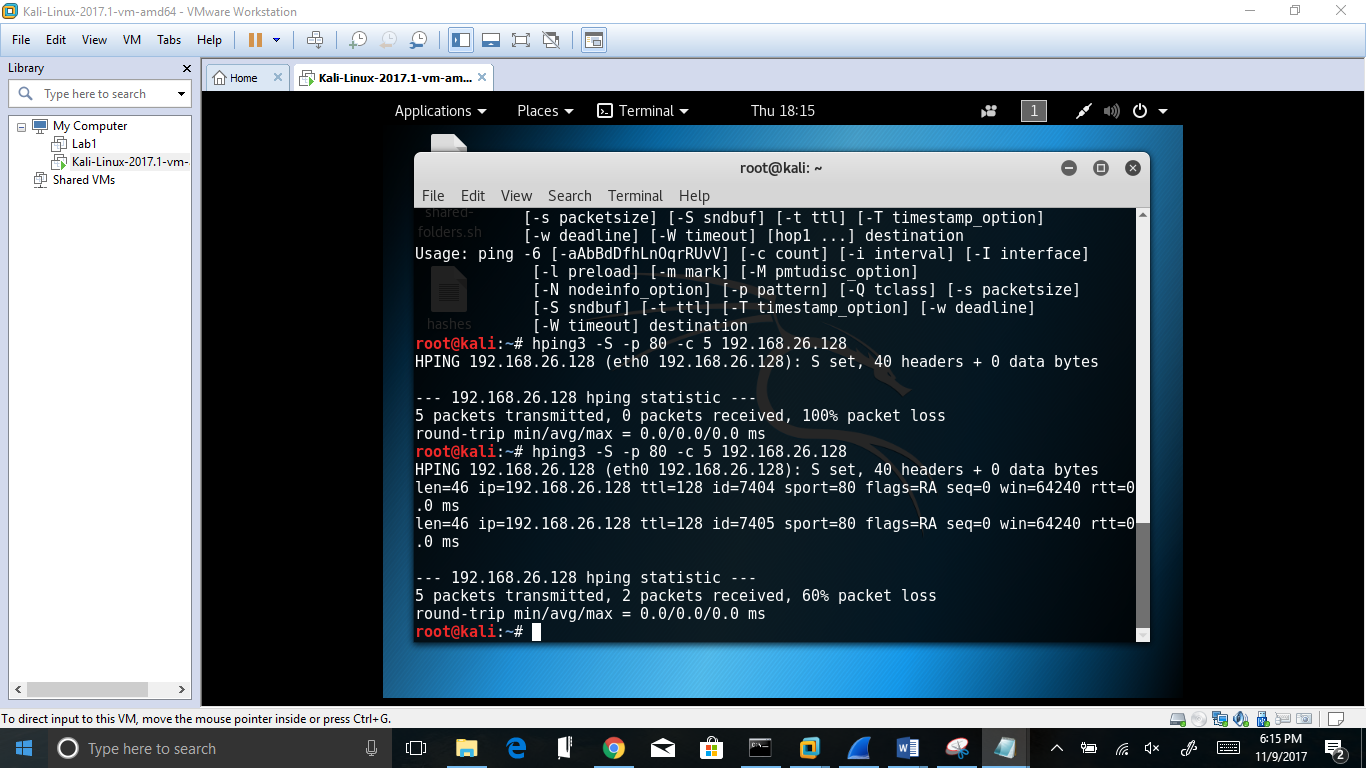
* Go to **c:\snort\log** and find the **alert.ids** file. Open it with **Wordpad**. Provide a screenshot for the ICMP alerts.
* 

**Task 3.**

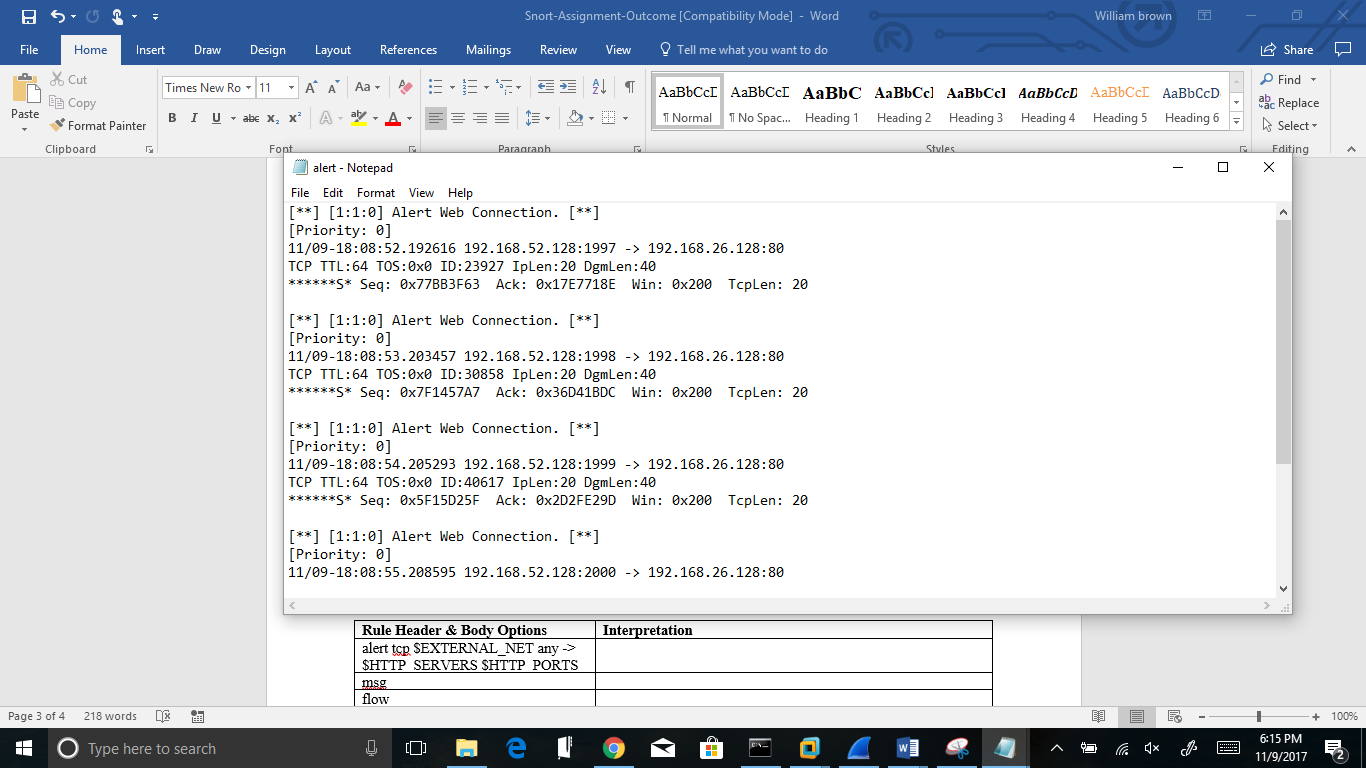
* Display your Snort rule.



* Display the hping3 command you have used.

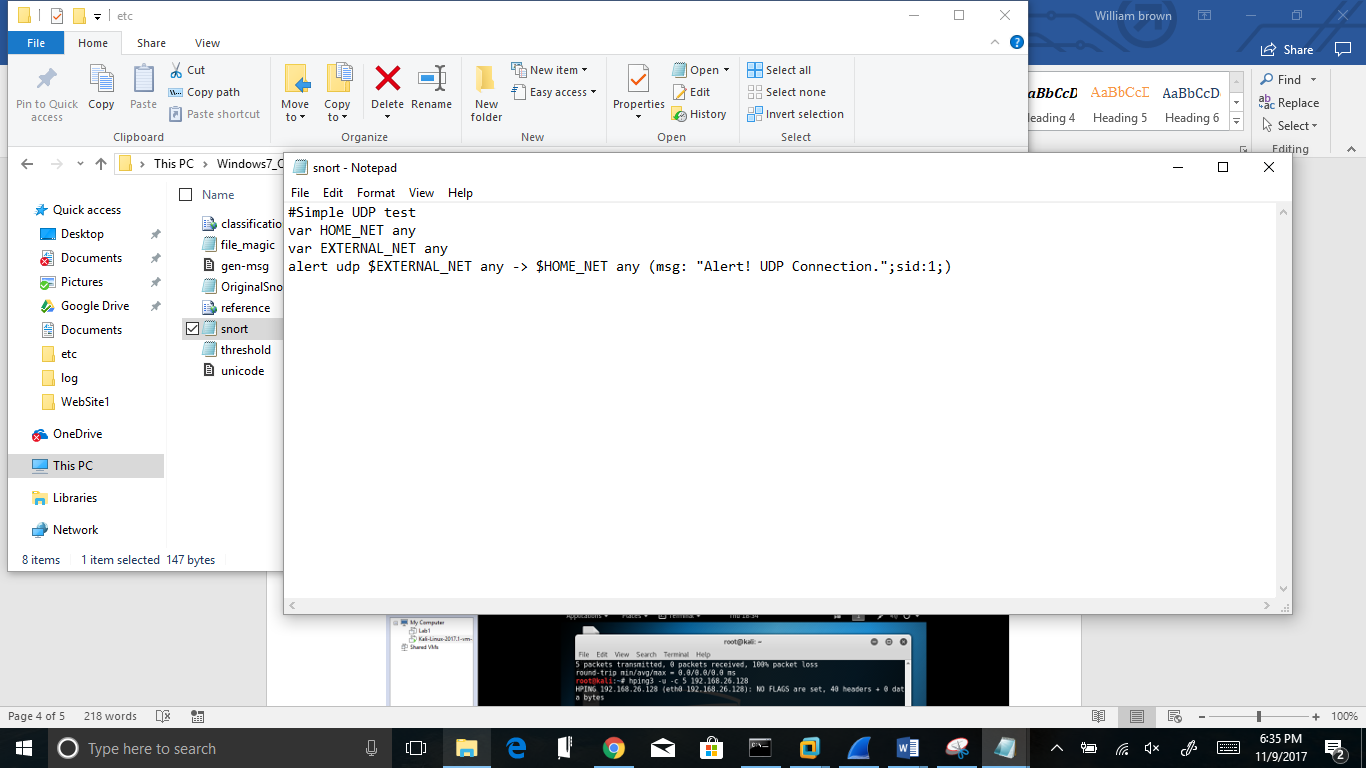


* Go to **c:\snort\log** and find the **alert.ids** file. Open it with **Wordpad**. Provide a screenshot for the TCP alerts.

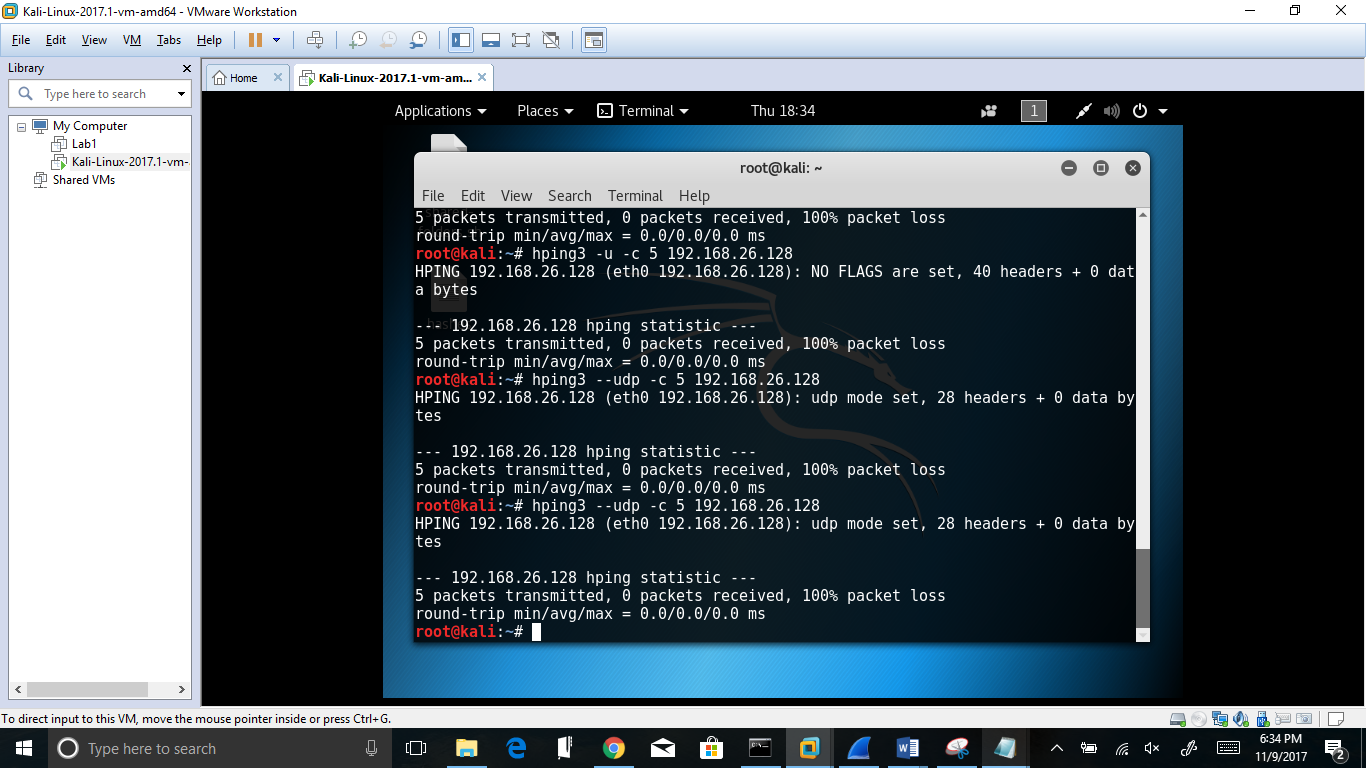


**Task 4.**

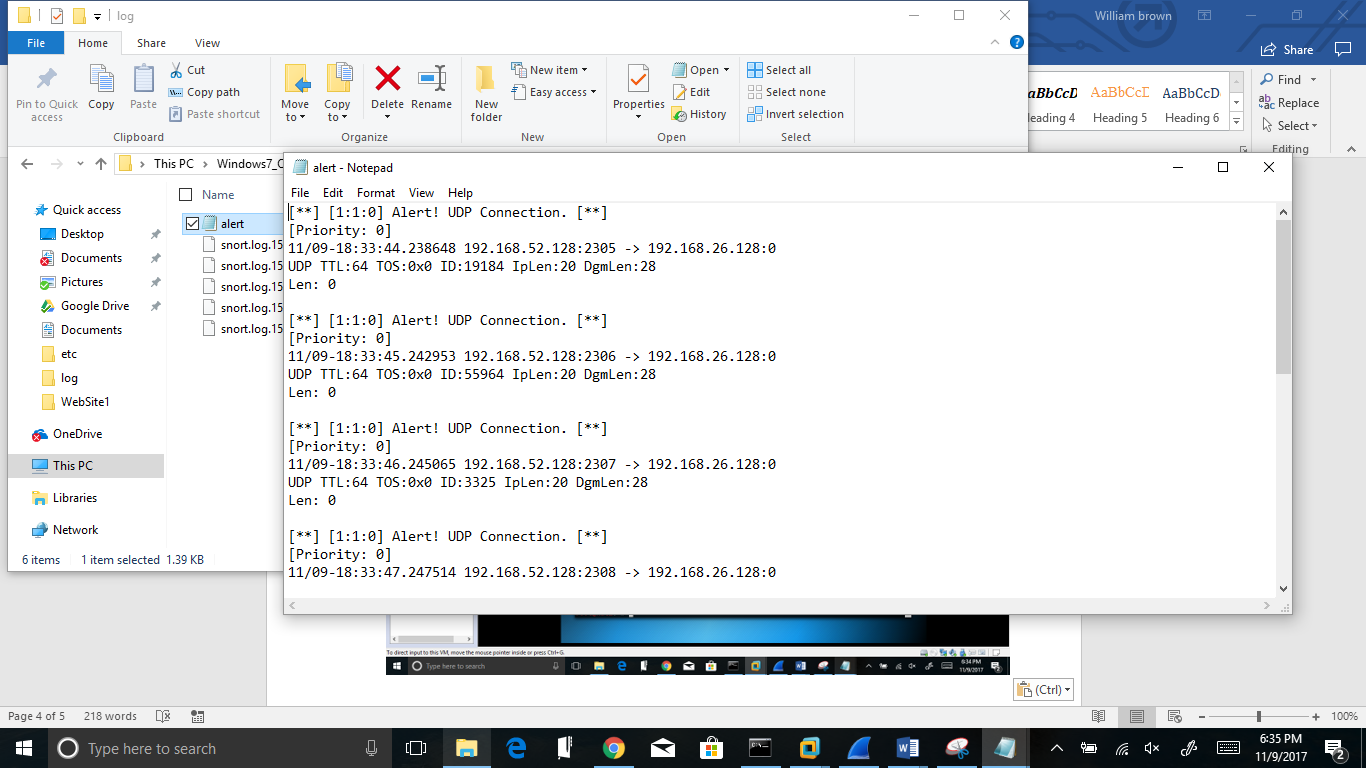
* Display your Snort rule.



* Display the hping3 command you have used.



* Go to **c:\snort\log** and find the **alert.ids** file. Open it with **Wordpad**. Provide a screenshot for the UDP alerts.



**Task 5. Snort Rule Interpretation**

Provide your interpretation of this rule in the table below.

|  |  |
| --- | --- |
| **Rule Header & Body Options** | **Interpretation** |
| alert tcp $EXTERNAL\_NET any -> $HTTP\_SERVERS $HTTP\_PORTS | If the packet matches the rule, then the rule sends its output to that location |
| msg | Gives the message that should be displayed when rule occurs |
| flow | Further defines rule. Says the output should go to an established server. |
| uricontent | Further refines the rule; Universal Resource Identifier |
| nocase | Deactivates case sensitivity |
| reference | Gives a referral to a log regarding information about the attack |
| classtype | Defines the category that the attack falls under |
| sid | Unique identifications to Snort; Snort Identification, this field is set to 1256 |
| rev | Identifies revisions to Snort rules |