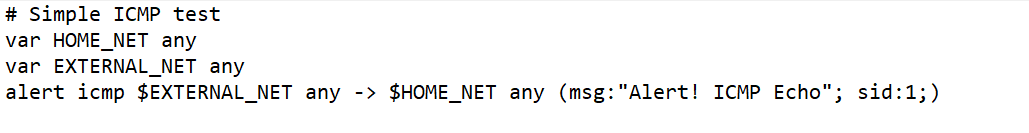
Snort Assignment

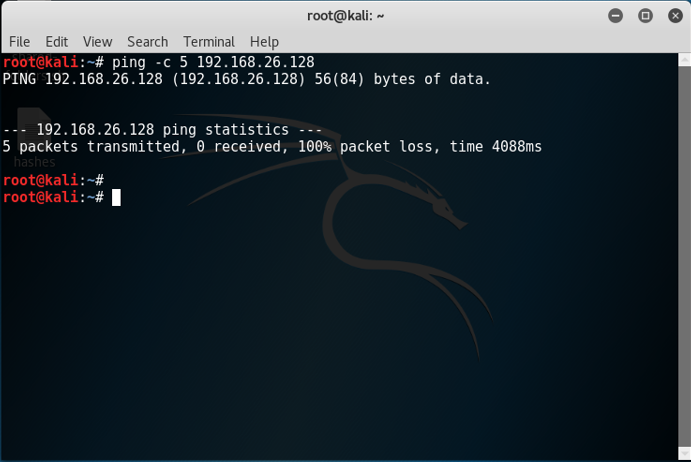
|  |
| --- |
| * This is an individual/group assignment, and is worth 20 points. You can find one partner for this. * The due date and time is Tuesday, 1:00 pm (sec01) / 5:30 pm (sec76), October 29. * Apply the usual naming convention. Use the file “Snort-Outcome.docx” for submission. |

**Task 1.**

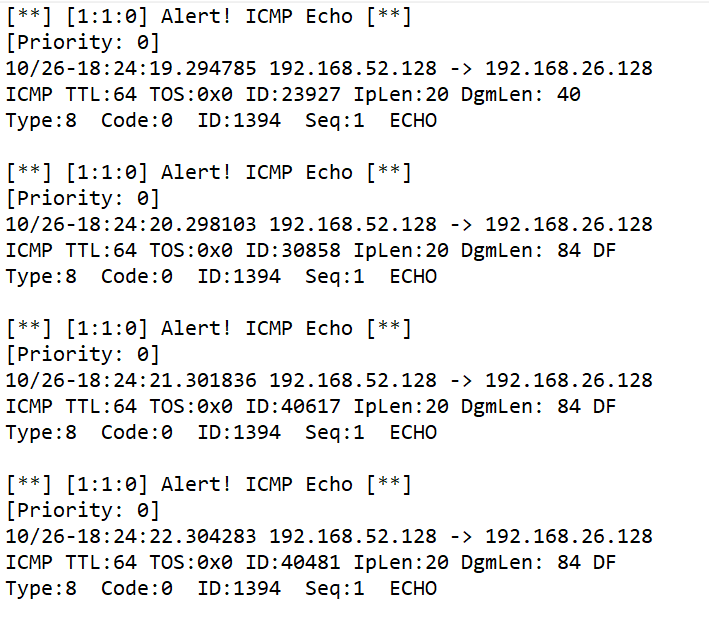
* Display your Snort rule.



* Display the hping3 command you have used.

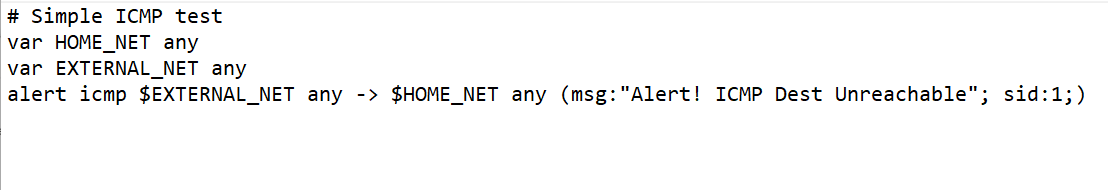


* Go to **c:\snort\log** and find the **alert.ids** file. Open it with **Wordpad**. Provide a screenshot like below for the ICMP alerts. After the screenshot, remove all the files in the log directory.

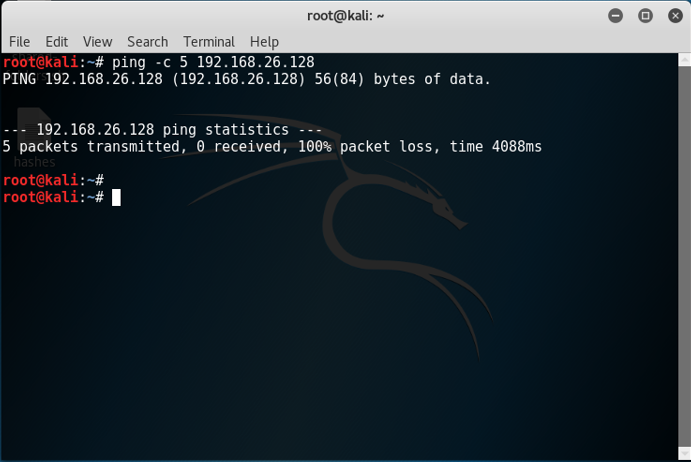


**Task 2.**

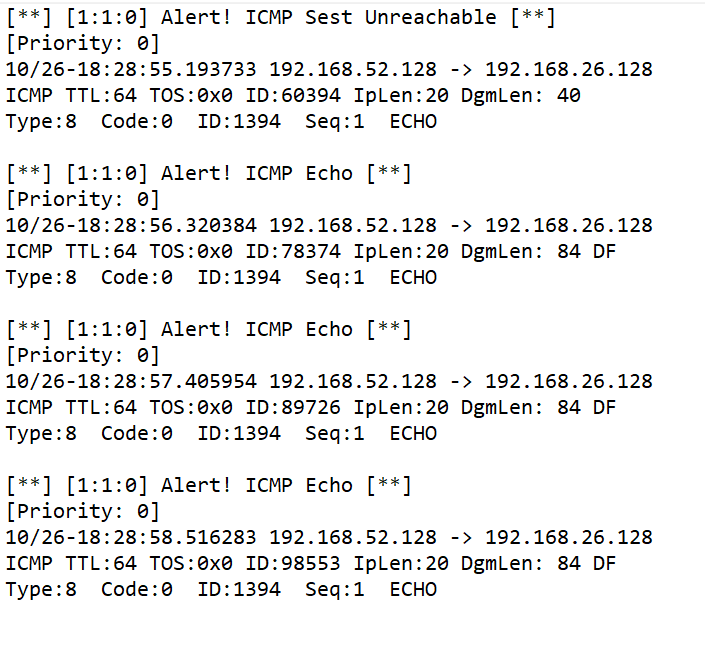
* Display your Snort rule.



* Display the hping3 command you have used.

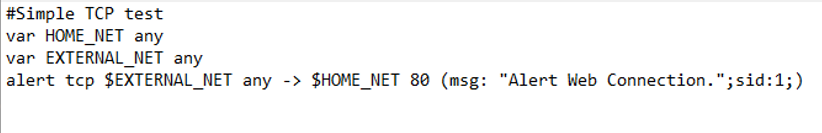


* Go to **c:\snort\log** and find the **alert.ids** file. Open it with **Wordpad**. Provide a screenshot for the ICMP alerts. After the screenshot, remove all the files in the log directory.

****

**Task 3.**

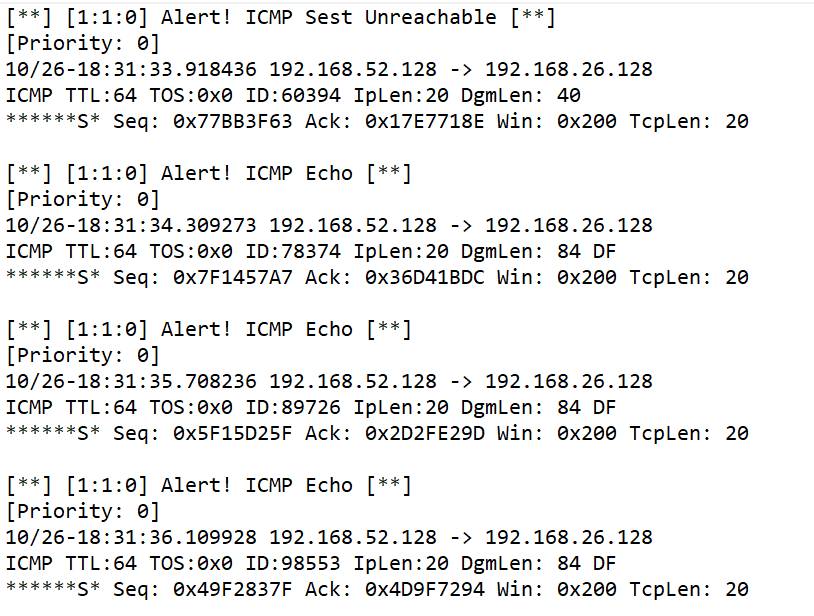
* Display your Snort rule.



* Display the hping3 command you have used.

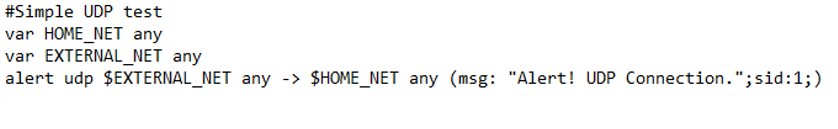


* Go to **c:\snort\log** and find the **alert.ids** file. Open it with **Wordpad**. Provide a screenshot for the TCP alerts. After the screenshot, remove all the files in the log directory.

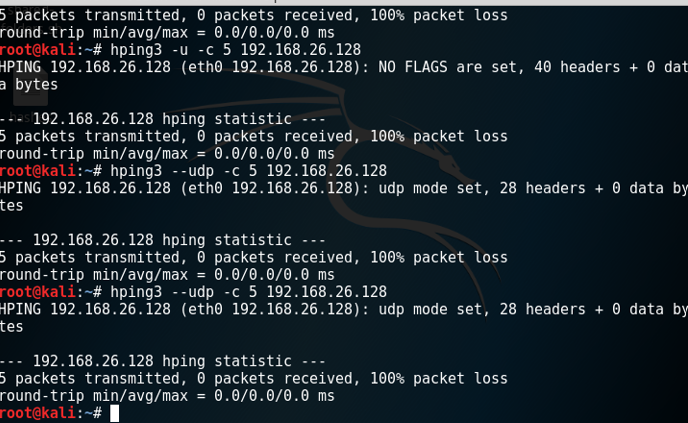


**Task 4.**

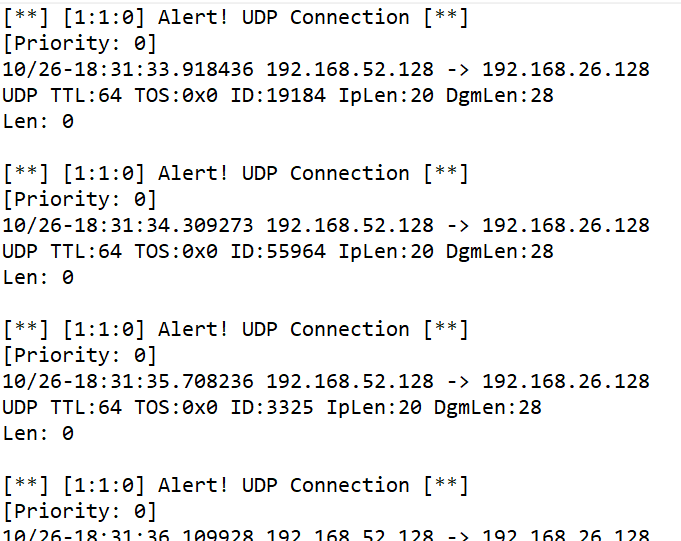
* Display your Snort rule.



* 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. After the screenshot, remove all the files in the log directory.



**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 packet matches this rule, rule sends output to the location specified |
| msg | Send message when rule is met |
| flow | Output should go to established server |
| uricontent | Universal resource identifier |
| nocase | Removes case sensitive |
| reference | Reference to log file |
| classtype | Attack category |
| sid | Snort ID |
| rev | Revisions to the rules |