Snort Lab Assignment

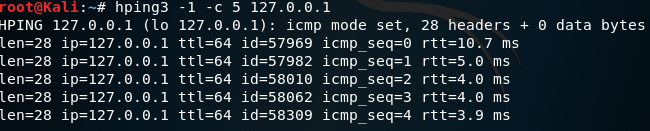
|  |
| --- |
| * This is an individual assignment. * The due date is Saturday, November 11th midnight. * For this assignment, you use Snort on Windows host and Kali. * Follow the usual naming convention. Use the file “Snort-Assignment-Outcome.docx” for submission. |

**Task 1.**

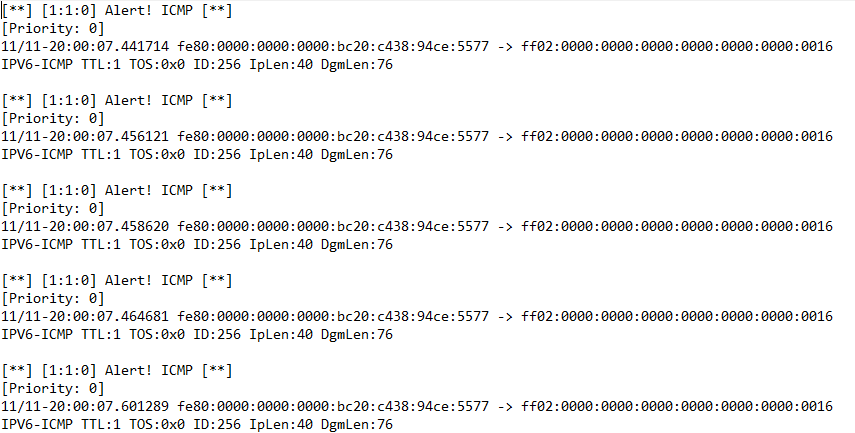
* Display your Snort rule.



* 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 | Someone on external net is going to http servers on http specified ports. |
| msg | The msg rule option tells the logging and alerting engine the message to print along with a packet dump or to an alert. |
| flow | It allows rules to only apply to certain directions of the traffic flow. |
| uricontent | Searches the normalized request URI field. |
| nocase | Deactivate case sensitivity. |
| reference | Reference external attack identification systems. |
| classtype | Categorize a rule as detecting an attack that is part of a more general type of attack class. |
| sid | Uniquely identify snort rules. |
| rev | Uniquely identify revisions of snort rules. |