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.

- 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.

- 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.

```
[**] [1:1:0] Alert! ICMP [**]
[Priority: 0]
10/22-08:49:35.242148 192.168.199.142 -> 192.168.1.49
ICMP TTL:64 TOS:0x0 ID:41460 IpLen:20 DgmLen:28
Type:8  Code:0  ID:17416   Seq:1024  ECHO
```

Task 2.

- Create a Snort rule that captures ICMP Echo Request from the Kali and shows alerts with the message "Alert! ICMP from the IP address 192.168.199.142", where 192.168.199.142 is the IP address of the Kali. Your rule must incorporate the IP address of the Kali.
- Send five (5) ICMP Echo Request messages from the Kali using hping3.
- You should process this request in a single command line. Before you create a rule for this task, delete the rule for the previous task.

- 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.

- Create a Snort rule that captures TCP traffic to port 80 from the Kali and shows alerts with the message “Alert! Web connection”.
- Send five (5) SYN messages from the Kali using hping3.
- You should process this request in a single command line. Before you create a rule for this task, delete the rule for the previous task.

- 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.

- Create a Snort rule that captures UDP traffic and displays alerts with the message “Alert! UDP connection”.
- Send five (5) UDP messages from the Kali using hping3.
- You should process this request in a single command line. Before you create a rule for this task, delete the rule for the previous task.

- 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

Interpret the following Snort rule. For a Snort rules tutorial, go to the following.

http://manual.snort.org/node27.html

alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS (**msg**:”WEB-IIS CodeRed v2 root.exe access”; **flow**:to_server,established; **uricontent**:”/root.exe”; **nocase**; **reference**:url,www.cert.org/advisories/CA-2001-19.html; **classtype**:web-application-attack; **sid**:1256; **rev**:8;)

Provide your interpretation of this rule in the table below.

Rule Header & Body Options	**Interpretation**
alert tcp $EXTERNAL_NET any -> $HTTP_SERVERS $HTTP_PORTS	
msg	
flow	
uricontent	

nocase	
reference	
classtype	
sid	
rev	