Ch 7: Linux Snort IDS Lab

1. Start and login to your Kali Linux virtual machine as user kali with a password of **kali**.

2. Ensure snort is installed/updated by typing **sudo apt-get install snort**. If prompted to continue, press **y** for yes and accept any other default settings.

3. View the snort main configuration file by typing **sudo nano /etc/snort/snort.conf**. This is where you can tweak snort, such as specifying a network IP address for variables such as HOME_NET.

4. Press **CTRL+X** to exit the nano text editor.

5. Type **cd /etc/snort/rules**, then **ls**. Snort include many preconfigured rule files that look for suspicious activity.

6. Create some custom snort rules by typing **sudo nano /etc/snort/rules/local.rules**.

7. You will create a snort rule that checks for ICMP network traffic, and another that checks for port 23 Telnet usage.

8. Enter (or copy and paste) the following rule taking careful note of colons versus semicolons:

   alert icmp any any -> $HOME_NET any (msg: "Testing ICMP"; sid: 1000001; rev:1; classtype: icmp-event;)

   alert tcp any any -> $HOME_NET 23 (msg: "Telnet connection attempt"; sid : 1000002; rev:1;)

9. Press **CTRL+X**, **Y**, then press **ENTER**.

10. Type **sudo snort -T -I eth0 -c /etc/snort/snort.conf** (-T means test).

11. To run snort, type **sudo snort -A console -i lo-q -c /etc/snort/snort.conf**. -A means print alerts to stdout, -q means quiet mode which don't show banner or status report. We are using the lo (local loopback) interface here for testing purposes only.

12. Open another terminal emulator windows in Kali Linux (go to the menu in the upper left, then choose Favorites). Type **ping 127.0.0.1**.

13. Switch back to the terminal window where snort is running. You will see messages related to "Testing ICMP" as per our custom snort rule.

14. Press CTRL+C to exit snort, or close the terminal window.