**Homework #7 Setup Instructions**

In this assignment you will work on Snort [**www.snort.org**](http://www.snort.org) , an IDS/IPS host-based system. You will be writing rules to do the following:

1. Generate an alert when ICMP traffic occurs towards the HIS
2. Stop ICMP traffic to prevent ICMP flooding
3. Stop SSH traffic to prevent brute-force attacks

**Setup**:

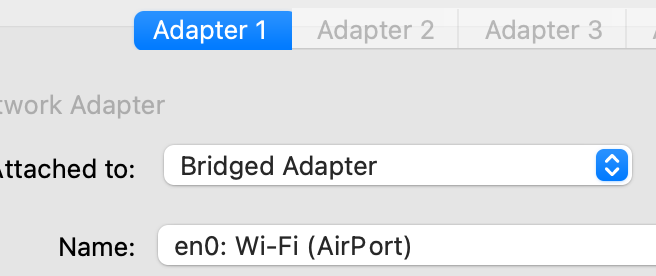
**Host**

**Snort**

KALI WINDOWS/MAC

**Snort Installation:**

* ﻿Change the network setting in the VirtualBox from NAT to Bridge Adapter



* Type **sudo vi /etc/apt/sources.list**
  1. Copy the lines from **SOURCES** (check the HW folder) file and paste it in **sources.list**
* Type **sudo apt-get update**
  1. Watch the output and keep notes of the pgp keys
  2. Type **sudo apt-key adv --recv-keys --keyserver keyserver.ubuntu.com xxxxxxxxxxxxxx**
  3. Repeat b above for the 2nd key
* Type **sudo apt-get update** (2nd time)
* Type snort --version to check if snort installed on your machine
* use ip addr command to know your ethernet interface ip address
* Install Snort using apt-get command <https://en.wikipedia.org/wiki/APT_(software)> :
  1. Type apt-get install snort
  2. Type your network IP address range when asked:
     1. If KALI ip address is 192.168.1.70 then type 192.168.1.0/24 as your ip address range
* Type snort --version to check if snort installed on your machine correctly
* The two main directories for snort:
  1. ﻿/etc/snort Which has the configuration and rules files
  2. ﻿/var/log/snort which has the log files

* Run snort in sniffing mode and observe how snort decode the packets
  1. snort -vde
* To start Snort: /etc/init.d/snort start
* To stop Snort: /etc/init.d/snort stop
* To view snort.log file: ﻿u2spewfoo snort.log

**SSH**

﻿

* Access kali using ssh: ssh yourid@kali\_Ip\_iddress

ssh: connect to host kali\_ip\_address1 port 22: Connection refused

* Check ssh process status: service ssh status
* ﻿Start ssh process: service ssh start
* Check ssh process status: service ssh status
* ssh yourid@kali\_Ip\_iddress
* Access kali using ssh: ssh yourid@kali\_Ip\_iddress