Security Onion

Your vm will need to be at least 10G in size to complete the below installation.

In this project you will experiment with an Intrusion Detection System (IDS). Begin by downloading an iso for security onion. Here is one or you can do a google search for one. Before installing, I created a vm with 2 nics, both of which are attached to the nat network. Make sure that at least the second nic can get promiscuous packets.

Follow these instructions to do the install. My first nic was selected as the management network, my second as the one to sniff.

After you have followed everything on that page, you can then use the desktop icons to view IDS stuff.

To generate some sample traffic, you can run `sudo so-replay`. It will replay some packet captures that have been taken to create some alerts.

With a second vm (maybe your ubuntu one) connect to the nat network.

**Some more tests**

From client machine:

- use `apt` to install something (or upgrade)
- use `curl` to do something (ie. `curl testmyids.com`)
- Look at rules and see if you can get others to fire (without actually generating malicious traffic) (Rules are located in `/etc/nsm/rules`.

It would be interesting to see if it can detect the rootkit traffic/RAT tool we installed a few weeks ago.

**TO pass off**

Choose 4 captures to analyze (either yours, or the pre-generated ones). Write a short paragraph on each. Identify what happened. Is it something to be concerned about. Try to find other information about the packet that you captured. Take a screenshot of the packet you viewed using either sguil or squert (or both).

Write a final paragraph about IDS. Why should you use one?