# Intrusion Detection systems

## Part 1

Complete the lab titled “Palo Alto Networks VM-Series Advanced Threat Detection” on pluralsight. I couldn’t get the very last step to work. Other than that, you should be able to screenshot your first checkpoint completion. Take a screenshot of the last http analysis using palo alto website.

## Part 2

In this project you will experiment with an Intrusion Detection System (IDS). Clone the vm named `onion`. Boot with 2 nics (ie. `citv bootvm foo c dualnic`)

Follow these instructions to do the install (start at step 7). My first nic was selected as the management network, my second as the one to sniff. It may prompt you to reboot a few times.

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. (If you had everything setup correctly you could potentially capture live traffic, but we will just analyze some precaptured ones)

## TO pass off

In a single pdf:

- Put screenshot from part 1
- 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?