**Student Name:** Dustin McClure

**Lab Name:** Incoming Zero Day! Prepare The IDS/IPS!

**Documentation of Steps:**

* Open and sign in to **Security-Desk**
* Open Browser and navigate to **pfsense admin login** page at **172.16.20.250**
* Login to **pfsense admin panel**
* From **pfsense admin panel**
  + navigate to **System** **🡪 Package Manager**
  + select “**Available Packages**”
  + search for “**snort**”
  + click “**install**”
  + navigate to **Services 🡪 Snort**
  + On “**Snort Interfaces**” tab click “**add**”
  + **Set these options:**
    - **Interface:** SUBSCRN(em0.1)
    - **Description:** SUBSCRN
    - Check “**Send Alerts to System Log**”
    - Scroll to bottom and click “**Save**”
  + **Navigate to “Rules” tab (SUBSC RULES) and define custom rule below:**
    - alert tcp any any -> 172.16.10.100 80 (content:”GET”; content:”%3A%3A%28%29x0001%5E%28%3A%3A%29%28xFFFF%29”; msg:”LetMeCry Exploit”; sid:100)
    - Click “**Save”**
  + Navigate back to “**Snort Interfaces**” tab and click the **PLAY** button under **Snort Status** to activate the interface
  + Navigate to “**Alerts**” tab
  + Check “**Auto Refresh View**” check box, click “**Save**”, and verify that snort rule is capturing alerts as expected in the “**Entries in Active Log**” section

**Screenshots (2-6) with Description:**

**Graphical user interface, text, application, website

Description automatically generated**

**This is a screenshot of the pfsense firewall’s admin dashboard after signing in.**

**Graphical user interface, text, application

Description automatically generated**

**In this screenshot I had just searched for and installed the snort package for our pfsense firewall.**

**Graphical user interface, text, application, email

Description automatically generated**

**This is a screenshot of me configuring the snort rule to generate an alert any time there is incoming traffic toward port 80 on the prod-joomla server that matches the LetMeCry signature.**

**Graphical user interface

Description automatically generated**

**This is a screenshot of the alerts tab successfully listing entries in the active log file after configuring the snort interface and snort rule shown above.**

**What I Learned:**

Though I have seen logs generated by snort in the past and know what snort is, when I started this lab I had zero experience installing snort on a device or configuring snort.

First, in completing this lab I learned that pfsense has its own package manager that allows you to install from a repository of packages. I have poked around firewalls before, but have never noticed or explored this functionality. When I am trying to configure a package or service from my desktop to interface with my router, it can often be very arduous. The built in package manager here seems like it would make this process much more simple and seamless.

I also learned in a little more depth how snort works and how to configure rules for generating alerts. Exploring snort I found it to be very simple and intuitive to set up and use. I quickly learned how to create interfaces for use with snort; the program makes this process very simple by auto-detecting available interfaces that are then populated in the interface drop-down. The fact that the syntax is very similar to that of a firewall rule and is formatted much like JSON with key-value pairs made learning rule-creation equally as straightforward. I was able to create the necessary rule for this lab on the first attempt thanks to these similarities and Professor McEwen’s awesome video 😊.