NSA Healthcare IoT Workout Instructions

Introduction

In this workout, you will be given a Raspberry Pi Zero, which is preloaded with various commands. You will interact with the device using a web application to gain a better understanding of securing IoT (Internet of Things) to cloud architecture.

Initial Setup

Your Raspberry Pi Zero device is configured to work with the UA Little Rock Cyber Arena. Follow these instructions to configure this device to work on your home network:

Step 1: Unpack everything and make sure you have the following materials.

RPI Zero with Sense Hat	
Power Supply	
HDMI Cable	

USB Extender	
Keyboard	

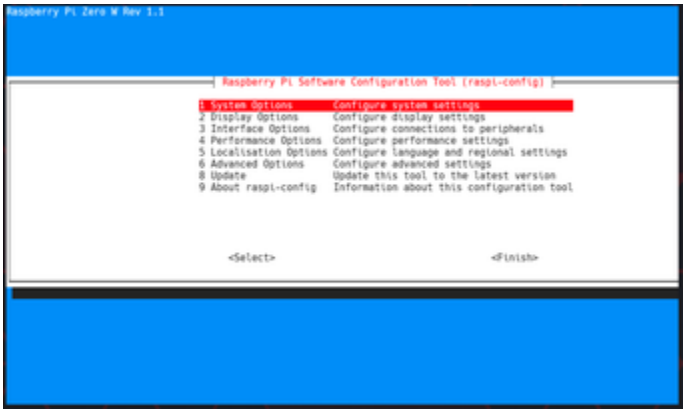
Step 2: Connect the HDMI Cable, USB Extender, and power supply. Also, the Bluetooth adapter in the Keyboard will be plugged into the USB Extender.

Step 3: Connect the HDMI cable to a monitor. It will take a few minutes to boot up, and then prompted for the username and password, use your wireless keyboard to type:

Username: *pi*

Password: *R3pr3$ent!*

Step 4: Run `sudo raspi-config` to configure wireless. You'll see a screen similar to the one below



Step 5: Select *System Options* > *Wireless LAN*, and enter the wireless network name and passphrase for your home wireless network.

Step 6: Restart your Raspberry Pi with `sudo reboot`. If the device makes a successful connection, you should see a rotating image display on your device screen.

Step 7: Go to https://cybergym-classified.labcyber.org/iot/. Enter the name of the device (e.g. cyber-arena-0001) on the bottom of your Raspberry Pi case. Then try sending a couple of commands to the device. If the device does not work, then please email cybergym@ualr.edu or go to the Slack channel and send the device ID with a screenshot or photo of the problem you experience.

Beginning your Workout

To begin, click on the link on your landing page to be taken to the web application. Here you will be asked to input the ID of your device, which is printed on the bottom of the Pi case (*cyber-arena-wxyz*). Afterwards, you will be taken to a page containing an interface from which you may send commands to the device. After the command is sent, look at the LED display attached to the device to see the effects of that particular command.

Mission

Your mission in this workout is to find vulnerabilities in the web application to manipulate the data being sent to the device. To do this, you will use the Inspect Element tool on your browser to view and edit the HTML and JavaScript code that makes up the page. The Elements tab will show the HTML content, and the JavaScript code can be found under the Sources tab.

There are two commands that you must find and send to the device. Once the appropriate command is sent, the device display will show a light configuration that is not available from the default commands, the page will refresh, and you will see a flag appear in the info section at the top of the page (it will look like CyberArena {flag_code}). Once these appear, you may copy and paste the inside text (flag_code) into the assessment portion of the landing page.