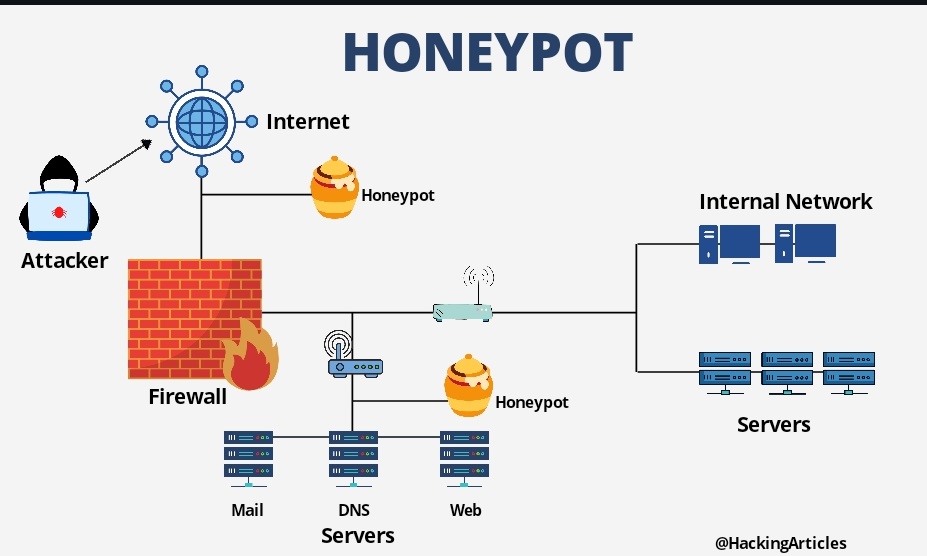
**Configuring a Raspberry Pi to be a “Honeypot” for Intrusion Detection Using Opencanary.**



**Background**

A great way to detect threats to you or your company’s network is the use of a “honeypot.” A “Honeypot” is a term for a vulnerable machine on your network, usually masquerading as a server with open ports. This is intended to entice hackers who may have already breached your network to attack it and thus notifying the person(s) in charge of securing the network.

**Prerequisites**

1. Raspberry Pi 3 or 4
2. PC
3. A Micro SD card
4. USB Keyboard & HDMI monitor
5. A Gmail Account

**Index**

**Part 1: Install Rasbian on an SD card.**

1. Download **Rasbian** from the official website**.**
2. Download **Balena Etcher**.
3. Flash the **Raspbian** ISO to the **SD card** with **Balena Etcher**.
4. **Insert** the **SD Card** into the Raspberry Pi and **Power On** the device.

**Part 2: Create Login credentials, Configure, and Update the OS.**

1. Plug a **USB keyboard** into the **RaspberryPi**. Follow the prompts to choose an **Account Name** and **Password**.
2. Create a **Bash Script** to change the MAC address of the Raspberry Pi.
3. **Enter** the root account with the command **sudo bash**. Now run this script using the command **source chadd.sh**. Type the command **exit** to leave the root file system. Type the command **cd ~** to return to the home directory.
4. **Update** the repositories of the OS by using the command **sudo apt update && sudo apt upgrade -y**.

**Part 3: Connect to the RaspberryPi remotely via SSH, “Secure Shell.”**

1. Find out the device’s **IP address** using the command **ifconfig**.
2. Connect remotely using **Linux**.
3. Connect remotely using **Windows**.

**Part 4: Install Python tools & Samba.**

1. Use the **apt-get** commandto install **python3-dev, pip, virtualenv, venv, scapy, libssl-dev,** and **libpcap-dev**.
2. Use the **apt** command to install **Samba**.

**Part 5: Create and name the Python virtual environment & activate the environment.**

1. Use the **python3 venv** command to create the virtual environment using the **–m** flagto name it.
2. Type **. canary/bin/activate** to activate the virtual environment.

**Part 6: Install OpenCanary, Scapy, Pcapy, and Markupsafe in the virtual environment.**

1. Use the **pip3** command to install **opencanary**.
2. Use the **pip3** command to install **scapy** and **pcapy**.
3. Use the **pip3** command to install **markupsafe** with the **-Iv** flag to select version **2.0.1**.

**Part 7: Setup a Gmail app password.**

1. Select **Accounts**. Select **Manage Your Google Account**.
2. Select **Security** on the **Top Bar**. Scroll down and select **2-Step Verification** under the sub menu called **Signing In To Google**.
3. Click **Get Started**. Enter your **Password** and click **Next**. Select a device to get prompts and click **Continue**.
4. Set up a **Backup Option** & click **Send**. Enter the **Verification Code** you recieved. Once verified click the return **Arrow**.
5. Scroll down and select **App Passwords**. Open the **Select App** drop down menu & Select **Other**.
6. Type **OpenCanary** in the app name field and click **Generate**. Copy the generated **App Password** to a **Text File** and return to the **Terminal**.

**Part 8: Copy & Modify the Configuration file. Add SMTP alerts.**

1. Use the **opencanaryd** command with the command line argument **copyconfig** to make a copy of the configuration file.
2. Open and edit the configuration file using **vi** or **nano**.
3. Change the **“device.node\_id”:** to **“SynologyFS”**. Ensure **“ftp.enabled”:** & **“http.enabled”:** are both **True**.
4. Ensure **“ssh.enabled”:** says **True**.
5. To enable **Email allerts** add **SMTP** under **“handlers”**.
6. Press **Ctrl+x**, **Ctrl-y**, and press **Enter** to save the changes.

**Part 9: Run OpenCanary and test event Logging.**

1. SSH services in the OS must be disabled before opencanary can run with it’s own SSH services. To **Disable** this use the command **sudo raspi-config**. Select **Interface options**, **SSH**, and **No**.
2. Use the **opencanaryd** command with the command line argument **start** to run opencanary.
3. Attempt an **ssh**, **ftp** and **https** connection with the device using any credentials.
4. Check **email** or the logging file **/var/tmp/opencanary.log**.

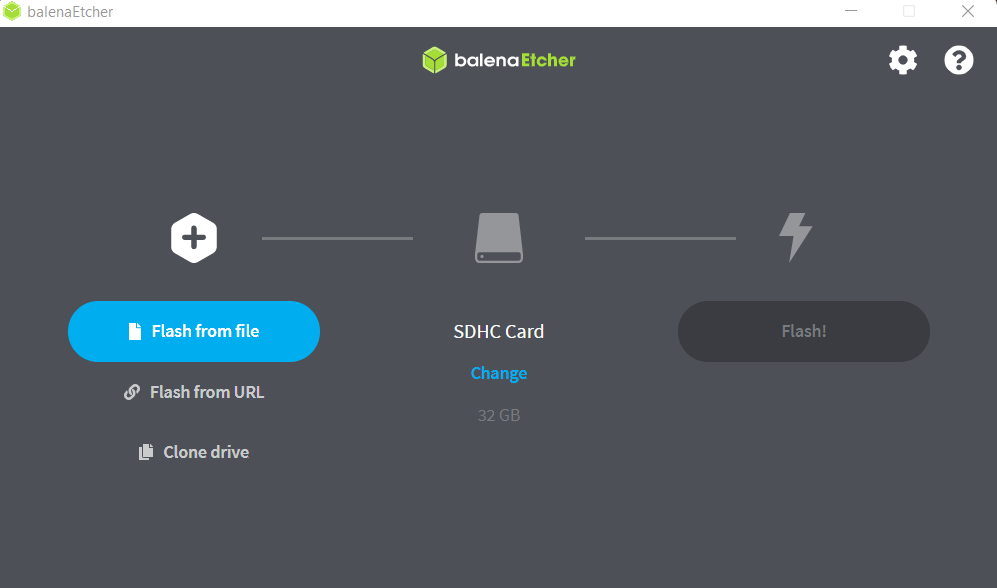
**Instructional**

**Part 1: Install Rasbian on an SD card.**

1. Download **Rasbian** from the official website: <https://downloads.raspberrypi.org/raspios_lite_armhf/images/raspios_lite_armhf-2022-04-07/2022-04-04-raspios-bullseye-armhf-lite.img.xz.>



1. Download **Balena Etcher** from: <https://www.balena.io/etcher/>.
2. Flash the **Raspbian** ISO to the **SD card** with **Balena Etcher**.



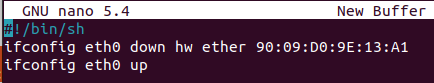
1. **Insert** the **SD Card** into the Raspberry Pi and **Power On** the device.

**Part 2: Create Login credentials, Configure, and Update the OS.**

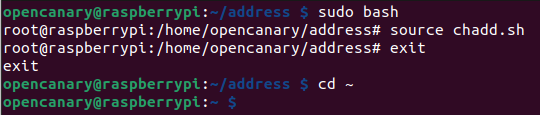
* 1. Plug a **USB keyboard** into the **RaspberryPi** and connect to an **HDMI** monitor. Follow the prompts choose **UK English**, a **Username** and a **Password**.
  2. Create a **Bash Script** to change the MAC address of the Raspberry Pi.
     + Make a new directory named address using the command **mkdir address**. Change your working directory to this new directory using the command **cd address**. Create a new text file in this directory by using the **nano** command.



* + - Enter the text shown below. Press **ctrl+x**, **ctrl+y**, type **chadd.sh**, and press **Enter**.



* 1. **Enter** the root account with the command **sudo bash**. Now run the file by using the command **source chadd.sh**. Type the command **exit** to leave the root file system. Type the command **cd ~** to return to the home directory.

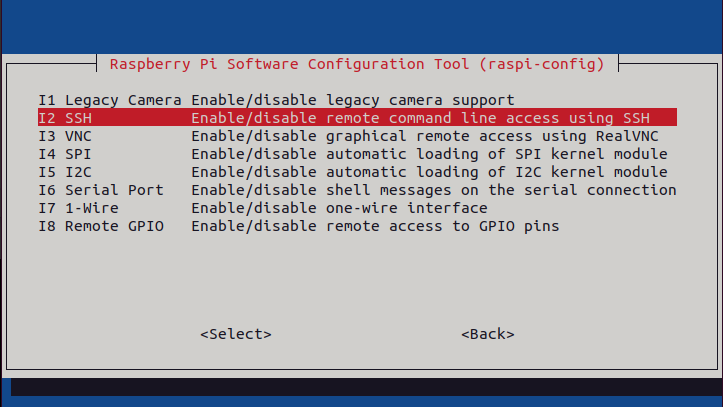
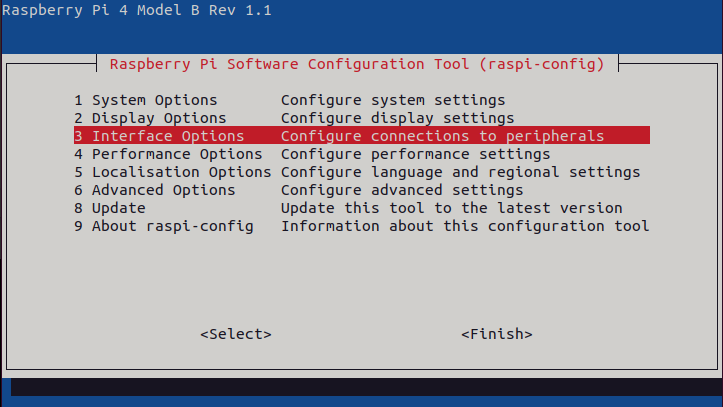


* 1. **Update** the repositories of the OS by using the command **sudo apt update && sudo apt upgrade -y**.

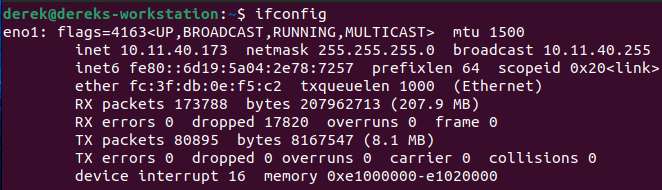


**Part 3: Connect to the RaspberryPi remotely via SSH, “Secure Shell.”**

* 1. SSH services in the OS must be **Enabled** before opencanary can run with it’s own SSH services. To **Enable** this use the command **sudo raspi-config**. Select **Interface options**, **SSH**, and **Yes**.



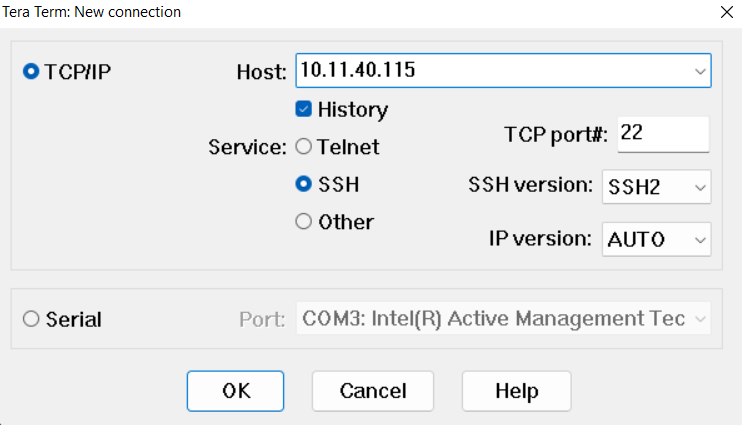
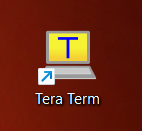
1. Find out the device’s IP address using the command **ifconfig**.



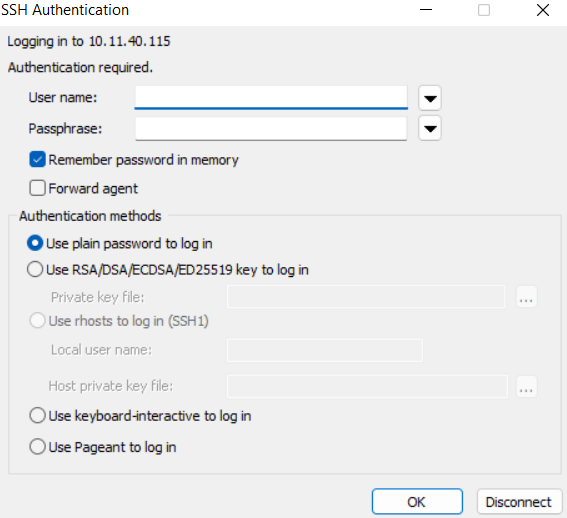
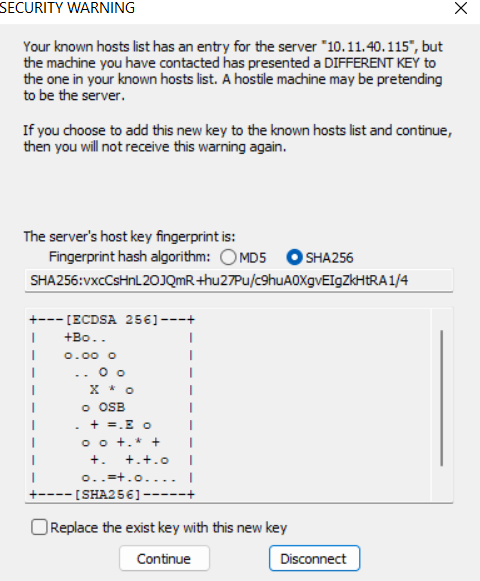
1. Connect remotely using Linux.
   * Open the terminal of a computer running linux. Use the **ssh** command in the format **username@ipaddress**.



1. Connect remotely using Windows.
   * Install and Load TerraTerm on a PC. Put the IP address you found into the Host section & click Okay.



* + Click Continue when prompted with a security warning. Type in the Username and the Password you set up. Click Okay.



**Part 4: Install Python tools & Samba.**

* 1. Use the **apt-get** commandto install **python3-dev, pip, virtualenv, venv, scapy, libssl-dev,** and **libpcap-dev**.



* 1. Use the **apt** command to install **Samba**.



**Part 5: Create and name the Python virtual environment & activate the environment.**

* 1. Use the **python3 venv** command to create the virtual environment using the **–m** flagto name it **canary**.



* 1. Type **. canary/bin/activate** to activate the virtual environment.



**Part 6: Install OpenCanary, Scapy, Pcapy, and Markupsafe in the virtual environment.**

* 1. Use the **pip3** command to install **opencanary**.



* 1. Use the **pip3** command to install **scapy** and **pcapy**.

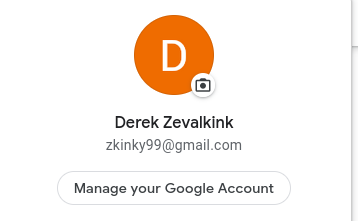


* 1. Use the **pip3** command to install **markupsafe** with the **-Iv** flag to select version **2.0.1**.

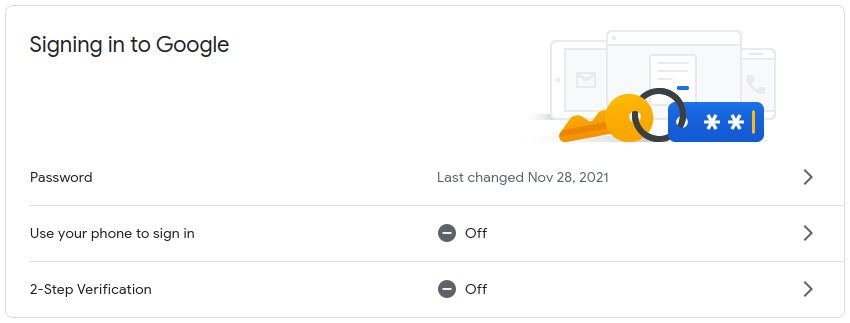
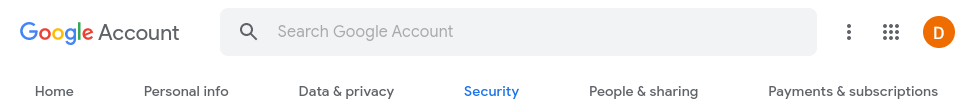


**Part 7: Setup a Gmail app password.**

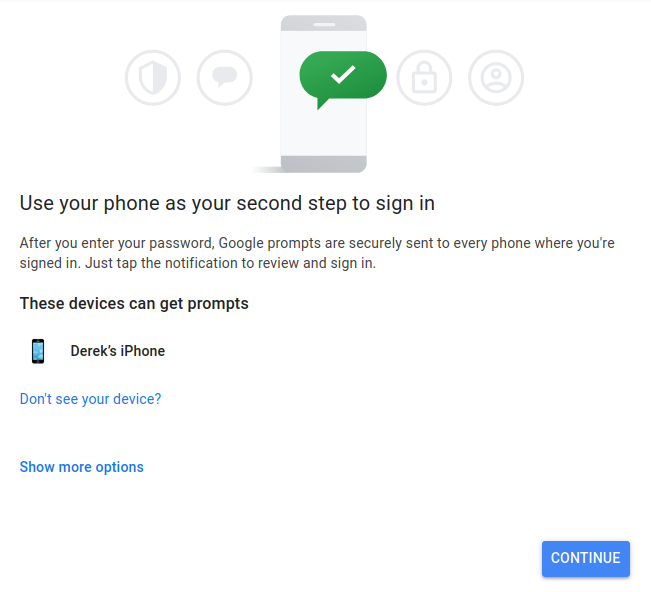
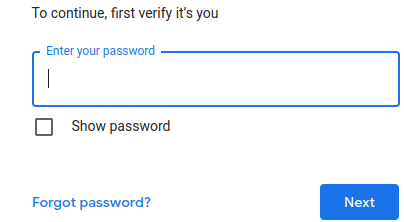
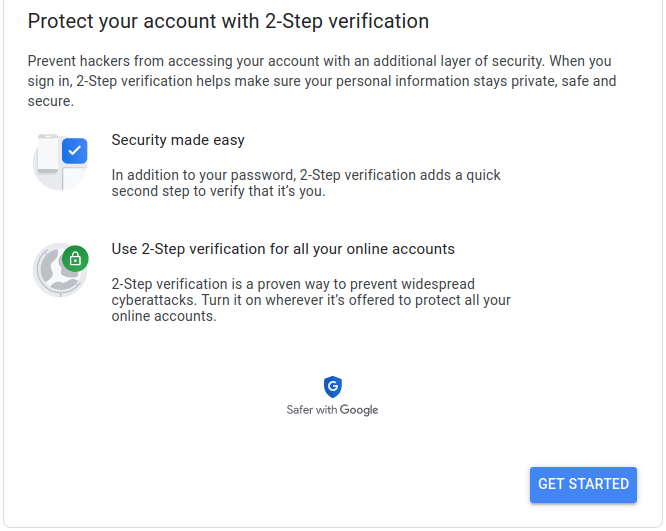
* 1. Select **Accounts**. Select **Manage Your Google Account**.



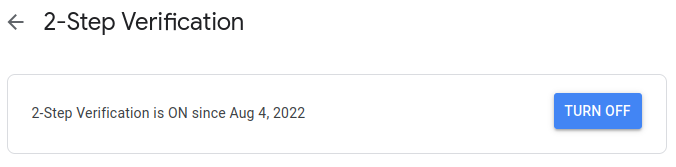
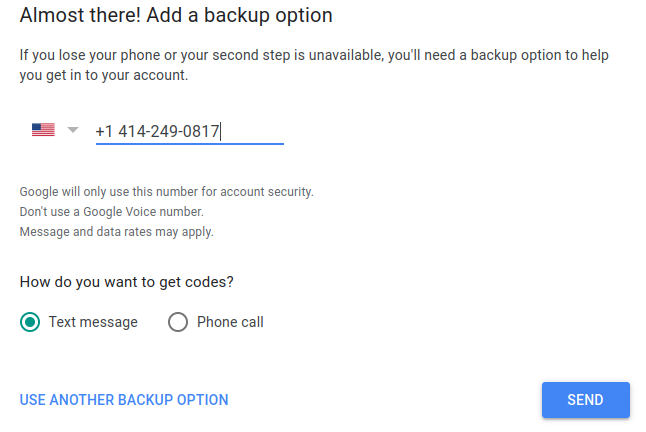
* 1. Select **Security** on the **Top Bar**. Scroll down and select **2-Step Verification** under the sub menu called **Signing In To Google**.



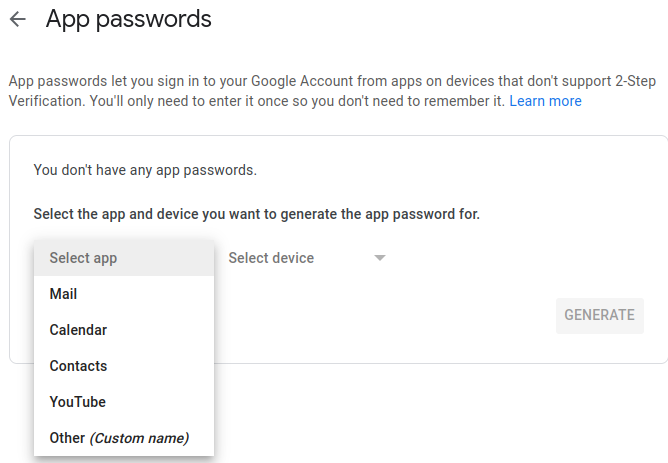
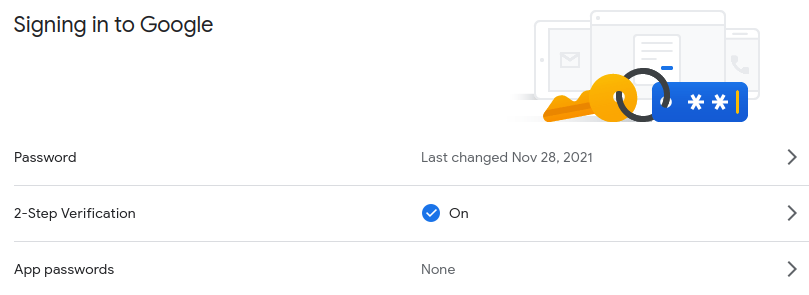
* 1. Click **Get Started**. Enter your **Password** and click **Next**. Select a device to get prompts and click **Continue**.



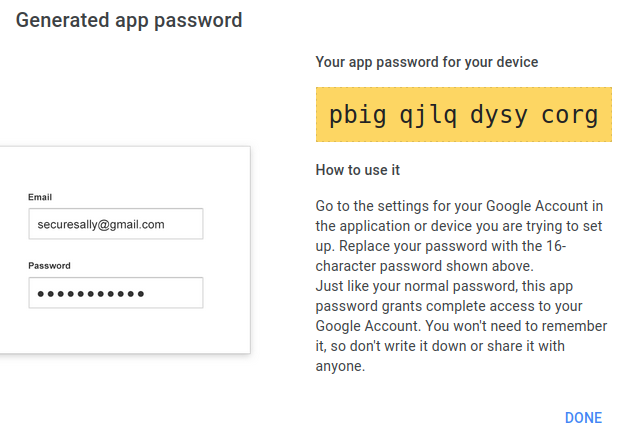
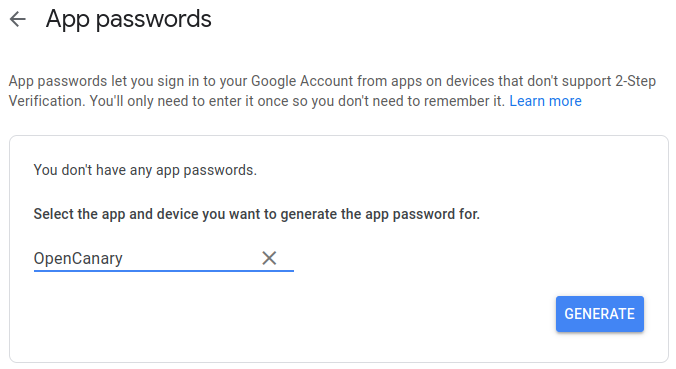
* 1. Set up a **Backup Option** & click **Send**. Enter the **Verification Code** you recieved. Once verified click the return **Arrow**.



* 1. Scroll down and select **App Passwords**. Open the **Select App** drop down menu & Select **Other**.



* 1. Type **OpenCanary** in the app name field and click **Generate**. Copy the generated **App Password** to a **Text File** and return to the **Terminal**.



**Part 8: Copy & Modify the Configuration file. Add SMTP alerts.**

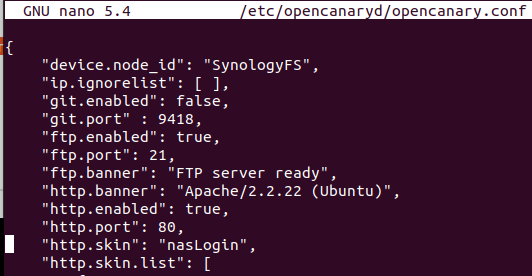
* 1. Use the **opencanaryd** command with the command line argument **copyconfig** to make a copy of the configuration file.



* 1. Open and edit the configuration file using **vi** or **nano.**



* 1. Change the **“device.node\_id”:** to **“SynologyFS”**. Ensure **“ftp.enabled”:** & **“http.enabled”:** are both **True**.



* 1. Scroll down and ensure **“ssh.enabled”:** also says **True**.



* 1. To enable **Email Alerts** add **this text** under **“handlers”**. <https://opencanary.readthedocs.io/en/latest/alerts/email.html>

**"handlers": {**

**"SMTP": {**

**"class": "logging.handlers.SMTPHandler",**

**"mailhost": ["smtp.gmail.com", 25],**

**"fromaddr": "noreply@gmail.com",**

**"toaddrs" : ["youraddress@gmail.com"],**

**"subject" : "OpenCanary Alert",**

**“credentials” : [“youraddress@gmail.com”, “apppassword”]**

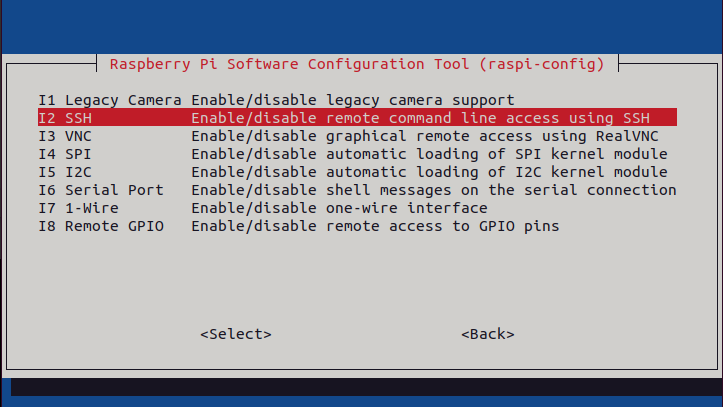
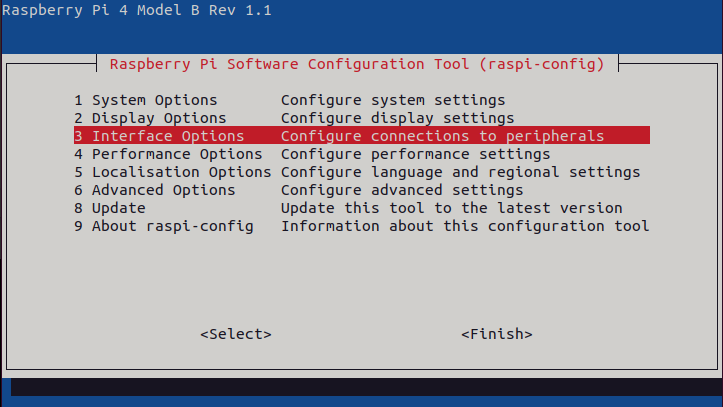
**“secure” : []**

**},**

* 1. Press **Ctrl+x**, **Ctrl-y**, and press **Enter** to save the changes.

**Part 9: Run OpenCanary and test event Logging.**

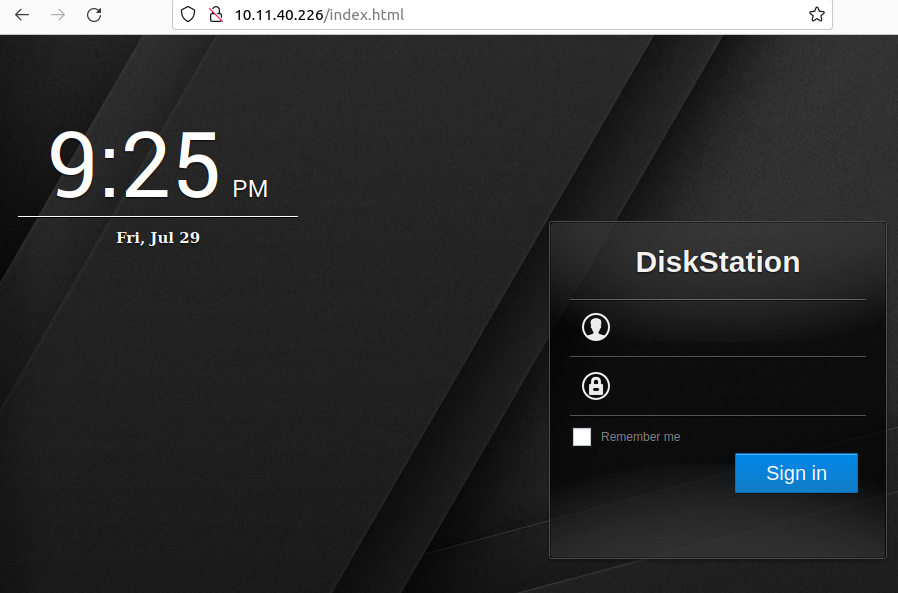
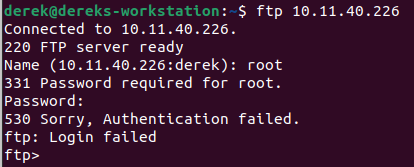
* 1. SSH services in the OS must be disabled before opencanary can run with it’s own SSH services. To **Disable** this use the command **sudo raspi-config**. Select **Interface options**, **SSH**, and **No**.



* 1. **Disconnect** from SSH and **Physically** access the Pi.
  2. Use the **opencanaryd** command with the command line argument **start** to run opencanary.



* 1. Attempt an **ssh**, **ftp** and **https** connection with the device using any credentials.



* 1. Check **email** or the logging file **/var/tmp/opencanary.log**.

