Setting up Kali 1.1.0 on the new Raspberry Pi 2

Posted on March 7, 2015

My new Raspberry Pi 2 arrived, and I wanted to install Kali on it. I was preparing to follow the steps of Richard Brain, but before I started, the folks at Kali tweeted that there was now a download available.

I downloaded the image, checked the hash, and burned it onto a 32GB SD card using

```
sudo dd if=kali-1.1.0-rpi2.img of=/dev/mmcblk0  bs=4M
```

I placed the SD card into my RPi2 and booted it up. Of course I generated new ssh keys

```
rm /etc/ssh/ssh_host_*
dpkg-reconfigure openssh-server
service ssh restart
```

I changed the root password

```
passwd
```

I updated the software

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

Extending the root partition on Kali Raspberry Pi 2

Normally one you execute raspi-config to extend the root file system. However, Kali didn't have it. Following the lead from rageweb, I use the following commands to install the necessary files

```
wget http://archive.raspberrypi.org/debian/pool/main/r/raspi-config/raspi-config_20150131-1_all.deb
wget http://http.us.debian.org/debian/pool/main/t/triggerhappy/triggerhappy_0.3.4-2_armhf.deb
wget http://http.us.debian.org/debian/pool/main/l/lua5.1/lua5.1_5.1.5-7.1_armhf.deb
dpkg -i triggerhappy_0.3.4-2_armhf.deb
dpkg -i lua5.1_5.1.5-7.1_armhf.deb
dpkg -i raspi-config_20150131-1_all.deb
raspi-config
```

The information from the above link was out of date. So if these files don't exist, go to the parent directory and search for the appropriate file with the correct revision number. Also note that with a RPi 2, you need the **armhf** instead of the **armel** files.

Once I started raspi-config, I selected the resize root partition option, and rebooted, and that problem was solved.

Improving the security of remote access on Kali

The next steps are obvious to experts, but I can't tell how experienced the readers are. So feel free to skip this part if you are experienced. Advanced users should look into this post on setting up an encrypted filesystem (LUKS) on a Raspberry Pi.

I wanted to make sure that password-based root access was not allowed. Instead, to gain access, the user has to access the device physically (an attached monitor and keyboard, a serial interface, etc.) or else the user has to place public key into the account.

I copied my account's public key onto the device

```
cd ~/.ssh
scp id_rsa.pub root@rpi2kali:/tmp
```

I had to type the password of course. Then I logged onto the machine

```
ssh -l root rpi2kali
Password: XXXXXXXX
```

Setting up a non-root account on Kali

It's generally a bad idea to allow someone to get root access directly. I recommend that you create a new user, (I used the user ID of 'kali'), grant them sudo access, and set their password:

```
useradd -m -s /bin/bash -d /home/kali kali
adduser kali sudo
passwd kali
```

Now we have to set up this account to allow ssh key-based remote access, using the public key that was copied to this device previously. (I prefer this, because copying and pasting text can modify the string).

```
su - kali
mkdir ~/.ssh
chmod 700 ~/.ssh
cp /tmp/ida_rsa.pub ~/.ssh/authorized_keys
```

Now test all this out. Make sure you can remotely log into the system, and execute the sudo command. It's a good idea to have several remote windows open, so you can correct errors in one window, and test things out in the other.

Disabling remote root access and preventing password-based remote access on Kali

Once this is done, you can disable remote root access by changing yes to no in the line in */etc/ssh/sshd_config*. You can also disable remote access that uses passwords.

Change the lines to be the following

```
#PermitRootLogin yes
PermitRootLogin no
#PasswordAuthentication yes
PasswordAuthentication no
```

Then restart ssh

```
service ssh restart
```

Then make sure this all works. Try to log onto the root account remotely and you should see something like

```
ssh -l root rpi2kali
Permission denied (publickey).
```

Then make sure that password-based remote access to the kali account is not allowed. You should get a similar error when trying to log onto the kali account from an account that isn't in the *authorized_keys* file

Just remember to keep a window logged onto the machine while you test this, and to experiment by renaming the authorized_keys file. Also – you can use the **ssh -vvv** option to debug your remote ssh connection.

There's a lot more you can do, like

- Move the ssh service to a different port
- add the *ufw* firewall package
- Limit the remote access to specific IP ranges
- Limit access to the built-in Ethernet port only, and prevent WiFI access
- etc.

I'll fill in more later. But that's enough to get you started.

References

http://www.debian-administration.org/article/87/Keeping_SSH_access_secure

Related

Setting up the 900 Mhz Freakduino board o... Kali Linux
In "Hacking"

Cataloging SDHC Cards on Ubuntu using a bash script
In "Linux"

Scanning for confidential information on external web servers
In "Linux"

This entry was posted in Hacking, Linux, Security, System Administration and tagged kali, raspberry Pi 2, ssh. Bookmark the permalink.

One Response to *Setting up Kali 1.1.0 on the new Raspberry Pi 2*

rscalliwag07 *says:*
November 1, 2015 at 11:31 am

!Updated! Thanks for original post. Thought I'd help.

wget http://archive.raspberrypi.org/debian/pool/main/r/raspi-config/raspi-config_20151019_all.deb

wget http://http.us.debian.org/debian/pool/main/t/triggerhappy/triggerhappy_0.3.4-2_armhf.deb

wget http://http.us.debian.org/debian/pool/main/l/lua5.1/lua5.1_5.1.5-8_armhf.deb

dpkg -i triggerhappy_0.3.4-2_armhf.deb
dpkg -i lua5.1_5.1.5-8_armhf.deb
dpkg -i raspi-config_20151019_all.deb
raspi-config

Reply