

Building a Bootable BackTrack 4 Thumb Drive with Persistent Changes and Nessus

Kevin Riggins



Last year I was in South America and needed to be able to perform some scans and tests on a network. There was one problem though. I was not allowed to connect my laptop to their network. However, I was allowed to use any software I wanted on one of their machines. BackTrack to the rescue.

BackTrack is a Linux distribution focused on penetration testing. The folks at www.remote-exploit.org gathered together a collection of over 300 open-source tools and created a Live CD/DVD that contains them all. You can boot the live CD/DVD in a few minutes and be ready to get to work.

While this is really handy, there is a one problem with the live CD distribution format. You can't save any information to the CDROM. In other words, once you have done some work, you have to figure out how to save that work to another medium.

Never fear! The BackTrack team kept this in mind when they created the distribution. They made it possible to fairly easily configure a USB thumb drive to save or persist changes.

At the time, the version of Backtrack available was version 3 and that was what I used. Since then, Backtrack 4 Beta has been released.

In the Backtrack 3 version of this how-to, which is still available on my website (www.infosecramblings.com), there were a few other issues I wanted to address in addition to making changes persistent. I wanted to add one tool and update two others to versions that were released after the release of BackTrack 3. The tool I wanted to add was Nessus. Nessus is a vulnerability scanning application. It scans for an ever increasing number of known vulnerabilities in systems and devices.

Building a Bootable BackTrack 4 Thumb Drive with Persistent Changes and Nessus

Kevin Riggins

The tools I wanted to update were Firefox and Nmap. We still need to add Nessus, but lucky for us, Backtrack 4 Beta already has the latest versions of Firefox and Nmap.

This article will walk through setting up a bootable BackTrack 4 Beta USB thumb drive with the following features:

- Persistent Changes
- Nessus and NessusClient installed.

Assumptions, Tools and Supplies

This guide is written with the following assumptions:

- You know how to partition and format disks.
- You are familiar with Backtrack.
- You are familiar with Nessus.
- You are familiar with Linux.
- You are familiar with Windows.

Tools and Supplies

- A USB thumb drive - minimum capacity 2GB
- A Backtrack 3 CDROM, Backtrack 4 DVD or an additional USB thumb drive (minimum 1GB in size) - Used to partition the thumb drive.
- UNetbootin (unetbootin.sourceforge.net) - A free tool to transfer an iso image to a USB drive.

Let's Get Started!

Partitioning the USB thumb drive

If you have a Backtrack 3 CD or Backtrack 4 DVD, you are in good shape. If you don't and are using an additional USB thumb drive, you are going to need to skip ahead to the 'Making a bootable Backtrack 4 thumb drive' first so you have something to use to partition the target drive. Return to here once you have some form of bootable Backtrack. I know this seems convoluted, but it's the easiest and most sure way I know to get us where we want to go.

First let's partition our thumb drive. I used a 4 GB drive as I read that we would need 1.2 GB for persistent changes. After I got everything working, it looks to me like we can get away with a 2 GB stick if we are careful about regular cleanup of log files. Nessus tends to be the main culprit here.

Regardless of the size thumb drive we use, we need to partition and format the drive as follows:

The first partition needs to be a primary partition of at least 1 GB and formatted as FAT32. The second Partition can be the rest of the thumb drive. It needs to be formatted as ext2.

If you try to use Windows to re-partition the drive, you will likely run into some problems.

Windows sees most USB thumb drives as removable media. As such, it does not support multiple partitions on them. It also does not allow us to delete the existing partition from the drive. This is because most thumb drives have the 'Removable Media Bit' set. One of the reasons for this is so that autorun will work.

Building a Bootable BackTrack 4 Thumb Drive with Persistent Changes and Nessus

Kevin Riggins

The easy way to get around the problem is to re-partition the drive using Linux. That's why we need the Backtrack CDROM, DVD or additional thumb drive although any Linux system will work. So go ahead and partition and format the drive according the layout above. Once I was done with this step, I switched back to a Windows system for the next few steps.

Make a Bootable Backtrack 4 USB Thumb Drive

Now we need to download the Backtrack 4 ISO. Here are the details about the distribution package and the location to download it from. As always, check the hash values to make sure you are getting what you expect.

In the last step we partitioned our USB thumb drive to have at least one 1 GB FAT32 partition on it.

The next step is to make it a bootable USB thumb drive. This used to be fairly complicated, but now there is a much easier way. We are going to use the UNetbootin tool mentioned above. It is super easy to use. Just start UNetbootin, select the Backtrack 4 ISO, select the USB drive and click okay. You may get a warning that files exist on your USB drive.

After making sure you picked the right one, tell it to go ahead and replace the files. It'll chug along and before you know it you will have a bootable thumb drive. Much easier than the rigmarole we had to go through before. In some cases, the thumb drive will may not be bootable after running UNetbootin. If this happens, from Windows, open a command window and do the following.

Change to the drive letter that your thumb drive is mounted on.

```
cd /boot execute bootinst.bat
```

Note: we need administrative privileges for this.

Enabling Persistent Changes

Once we have booted into Backtrack we need to configure the rest of the thumb drive if we haven't already done so. I used fdisk to create a second partition from the remainder of the drive and formatted it with mkfs.ext2. In my case my USB drive was /dev/sdb.

Once we have formatted a second partition, mount it and create a changes directory in the root of the file system. Open a terminal windows and execute the following commands:

```
mount /dev/sdb2 /mnt/sdb2 cd /mnt/sdb2 mkdir changes
```

Next we need to make some changes to how the system boots. Execute the following:

```
cd /boot/syslinux chmod +Xx lilo chmod +Xx syslinux
```

Open syslinux.cfg with your favorite editor and make the following change. Note: I copied the boot definition I wanted to change and created a new entry so I would have a fall back option if broke something beyond repair.

Find the line "LABEL BT4". Copy that line and the next three right after that section. Change the "LABEL BT4" to something you want like "LABEL BT4-persist" and description to something like "MENU LABEL BT4 Beta - Console - Persistent" Change the line that begins with APPEND in your copied section by adding changes=/dev/ sdx2 immediately after root=/dev/ram0 rw where the x is the drive appropriate for your system. In my case it looks like this,

Building a Bootable BackTrack 4 Thumb Drive with Persistent Changes and Nessus

Kevin Riggins

```
...root=/dev/ram0 rw changes=/dev/ sdb2...
```

Save your changes and exit the editor.

That should do it. Reboot and select the option you configured. To test it, create a file and reboot again. If your file is still there, everything is golden.

Installing Nessus

Now that our changes are saved from boot to boot, we can install things and they won't disappear on us.

First we need to get a copy of Nessus. Go to nessus.org and download the Ubuntu Nessus and NessusClient packages. I used the 32-bit 8.04 version which worked fine for me.

We had to jump through quite a few hoops to get Nessus running on Backtrack 3. Again, with Backtrack 4 things are little easier. To install the Nessus server, open a terminal window and simply execute the following command. This assumes you are in the same directory as the Nessus packages.

```
dpkg --install Nessus-3.2.1-ubuntu804_i386.deb
```

Things are little bit more complicated for the client. There are some dependencies that need to be installed first. Luckily, we have apt to help us with this. Execute the following command to install them. It is all one line.

```
apt-get install libqt4-core libqt4gui libqtcore4 libqt4-network libqt4-script libqt4-xml libqt4-dbus libqt4test libqtgui4 libqt4-svg libqt4opengl libqt4-designer libqt4assistant
```

After that, we can install the client package.

```
dpkg --install NessusClient-3.2.1.1-ubuntu804.i386.d eb
```

Finally it's time to configure Nessus. Execute each of the following and follow the prompts provided. /opt/nessus/sbin/nessus-mkcert /opt/nessus/sbin/nessus-adduser Nessus requires that you have a key in order to keep you plugins up-to-date. You can go to the following link (tinyurl.com/cfb6u) to register for a free home feed. Remember to use appropriately according to the licensing agreement.

Once you have your key, execute the following to update your plugins.

```
cd /opt/nessus/etc/nessus /opt/nessus/bin/nessus-fetch --register [you feed code here]
```

When that is done, and it is going to take a few minutes, you are ready to start the server and client.

```
/etc/init.d/nessusd start /opt/nessus/bin/NessusClient
```

There you have it, a bootable USB thumb drive with Backtrack 4, persistent changes and Nessus. Now you are fully equipped to go forth and perform penetration tests with the latest tools and without the fear of losing all the work you have done because it didn't get saved.