BackTrack Hard Drive Installation

BackTrack Development Team

jabra [at] remote-exploit [dot] org

Installing Backtrack
to a USB Stick or Hard Drive

Table of Contents

BackTrack Hard Drive Installation

Foreword

Before we begin, I'd like to stress that I am not responsible for anything that goes wrong with the installation. This document was created to aid in the installation process of Backtrack to a hard drive. I take no responsibility if things go wrong.

If you follow this documentation,

it *will* wipe all of the data on your hard drive!

History

For years, users have had to install and update the security and wireless tools to perform security assessments. However, Backtrack has a great feature which makes it easy to install on a USB or Hard Drive. By using this feature, it bypasses the hassle of having to install and update the tools manually.

Requirements

The requirements for the installation are either 700 MB or 2700 MB of hard drive space on a given device.

How do I install Backtrack to my hard drive ?

One of the cool features in Backtrack, is the ability to install onto your USB device or Hard Drive. The installer gives the choice of doing a minimal installation or a full installation. Obviously, with the number of tools included on Backtrack there are many times when this is an incredibly useful feature.

Booting Backtrack

The first step is to boot Backtrack using the cdrom. If you are using Vmware machine use the ISO as the cdrom. When the login prompt appears, login using:

username: root

password: toor

Creating the Partitions

Next, you will need to create the partitions and file systems. The device I am using is /dev/sda which is 3.75 gigs in size. I will create 3 partitions. The first partition will be /boot which I will allocate 50 MB which will be mounted as /boot. The second partition will be a swap partition which I will allocate 512 MB. The final partition will fill the rest of the disk and be mounted as /.

BT ~ # **fdisk /dev/sda**
Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel. Changes will remain in memory only,
until you decide to write them. After that, of course, the previous
content won't be recoverable.
Command (m for help):**n [enter]**
Command action
  e extended
  p primary partition (1-4)
p [enter]
Partition number (1-4): **1[enter]**
First cylinder (1-456, default 1):**[enter]**
Using default value 1
Last cylinder or +size or +sizeM or +sizeK (1-456, default 456): **+50M [enter]**
Command (m for help):**n [enter]**
Command action
  e extended
  p primary partition (1-4)
p [enter]
Partition number (1-4): **2 [enter]**
First cylinder (8-456, default 8):**[enter]**
Using default value 8
Last cylinder or +size or +sizeM or +sizeK (8-456, default 456): **+512M [enter]**
Command (m for help): **n [enter]**
Command action
  e extended
  p primary partition (1-4)
p [enter]

Partition number (1-4): **3 [enter]**

First cylinder (71-456, default 71):**[enter]**

Using default value 71

Last cylinder or +size or +sizeM or +sizeK (71-456, default 456): **[enter]**

Using default value 456

Command (m for help): **a [enter]**

Partition number (1-4): **1 [enter]**

Command (m for help): **t [enter]**

Partition number (1-4): **2 [enter]**

Hex code (type L to list codes): **82 [enter]**

Changed system type of partition 2 to 82 (Linux swap / Solaris)

Command (m for help): **p [enter]**

Disk /dev/sda: 3758 MB, 3758096384 bytes

255 heads, 63 sectors/track, 456 cylinders

Units = cylinders of 16065 * 512 = 8225280 bytes

Device	Boot	Start	End	Blocks	Id	System
/dev/sda1	*	1	7	56196	83	Linux
/dev/sda2		8	70	506047+	82	Linux swap
/dev/sda3		71	456	3100545	83	Linux

Command (m for help): **w [enter]**

The partition table has been altered!

Calling ioctl() to re-read partition table.

Syncing disks.

Creating the Filesystems

The next step is to create the filesystems on the partitions so that we will be able to write data to the devices. For this setup, we will use the Linux standard ext3 filesystem. We won't need to modify /dev/sda2, as it is already setup as Linux Swap.

```
BT ~ # mkfs.ext3 /dev/sda1
mke2fs 1.38 (30-Jun-2005)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
14056 inodes, 56196 blocks
2809 blocks (5.00%) reserved for the super user
First data block=1
7 block groups
8192 blocks per group, 8192 fragments per group
2008 inodes per group
Superblock backups stored on blocks:
        8193, 24577, 40961
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
This filesystem will be automatically checked every 25 mounts or 180 days, whichever
comes first.  Use tune2fs -c or -i to override.
```

```
BT ~ # mkfs.ext3 /dev/sda3
mke2fs 1.38 (30-Jun-2005)
Filesystem label=
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
387840 inodes, 775136 blocks
38756 blocks (5.00%) reserved for the super user
First data block=0
24 block groups
32768 blocks per group, 32768 fragments per group
16160 inodes per group
Superblock backups stored on blocks:
        32768, 98304, 163840, 229376, 294912
Writing inode tables: done
Creating journal (16384 blocks): done
Writing superblocks and filesystem accounting information: done
This filesystem will be automatically checked every 27 mounts or
180 days, whichever comes first.  Use tune2fs -c or -i to override.
```

Mount the Devices

The next step is to mount the devices onto the disk so we can install Backtrack. We will create directories in /tmp to mount them.

```
BT ~ # cd /tmp

BT tmp # mkdir boot

BT tmp #  mkdir bt2

BT tmp # mount /dev/sda1 boot

BT tmp # mount /dev/sda3 bt2
```

Backtrack Installer

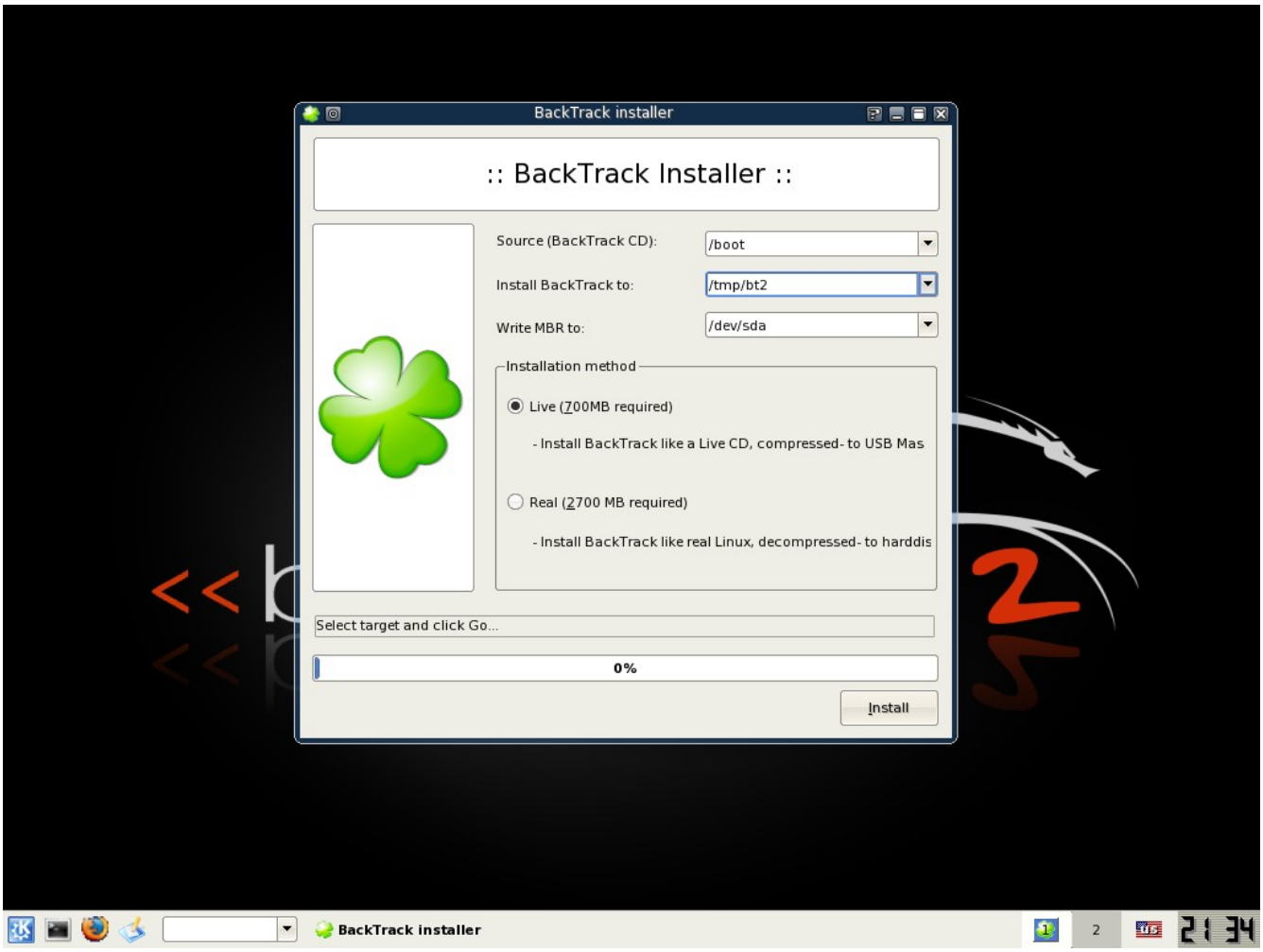
Now I will assume you have everything set up in terms of your hard drive, filesystems and partitions. Therefore, make sure you have started KDE. If you are still looking at a terminal prompt, start KDE with the following command:

```
BT ~ #  startx
```

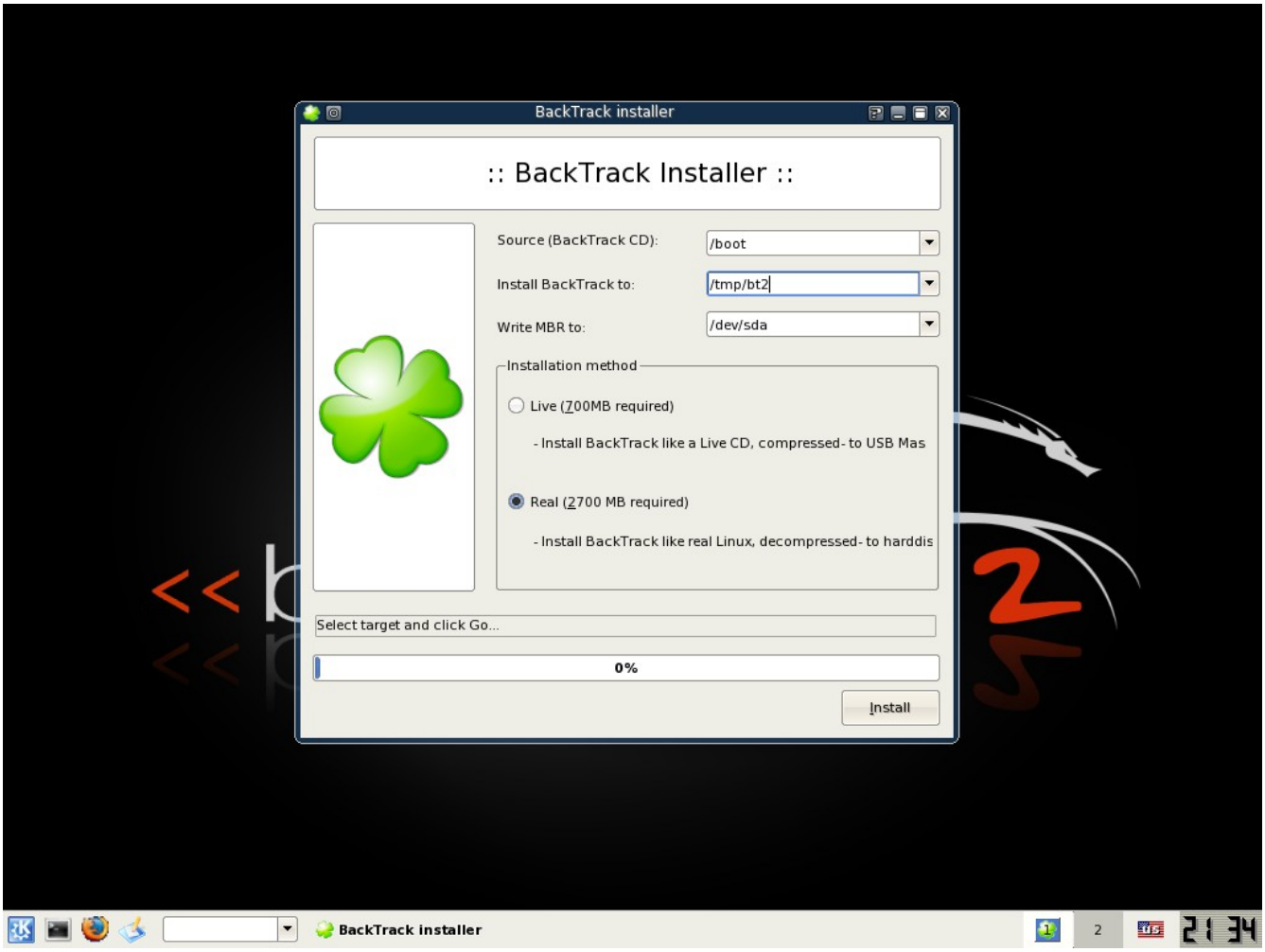
Once you are running KDE, click the K menu button on the lower left corner and follow the Menu:

K -> System -> Backtrack Installer

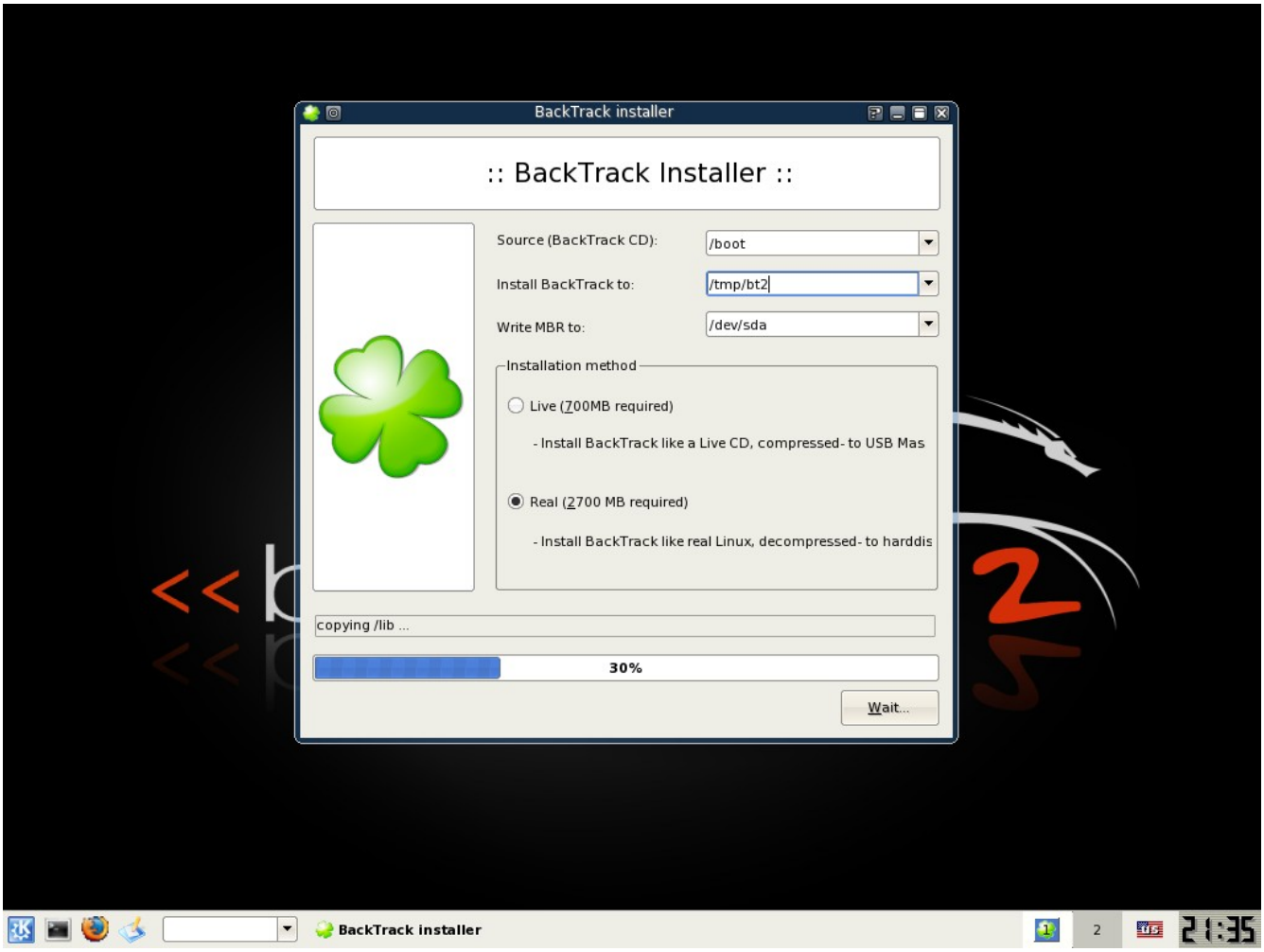
Once the Backtrack Installer comes up, first select the location that you would like to install Backtrack. I will be using /tmp/bt2 as that is the location of the where I have mounted the larger partition.



Next select the your Installation Method. The choices are either Live (700 MB required) or Real (2700 MB required). I have selected the Real Install because I have the space needed for it and it will be able to run faster without the compression. Obviously, if you are using a USB drive or hard drive which is smaller than 2700 MB you won't be able to do the Real Install.



After you have selected your method, click install and Backtrack will be installed on your hard drive.



Final Notes

The installation might seem to hang around 80%. This is normal. It is copying a huge **usr.mo**, which is not represented well in the in Installer.

Once the installation is over, reboot BackTrack. Don't forget to remove the CD / USB drive, and if all went well, Backtrack should now be installed on your hard disk.