



## Security Testing Live-CD – Quickstart Guide!

This package contains 2 security testing CDs. The latest version is marked 'BT2', we also supply an older version which should be used with older or BT2 incompatible machines, this CD is marked 'Audit'.

Both packages are designed to run directly from the CD and do not need to be installed directly on your hard drive – they should not affect your Windows installation at all. Both CDs are freely downloadable from the Internet and are open source, so you are free to copy them for friends (although they are each 700MB+ downloads, which need to be written to disc as .iso images).

To use the Live-CDs, you'll need to set your PC or Laptop to boot from CD. When your computer starts up you will see a message like 'Hit Del or Esc or Fxx for Bios/Setup', do this and look for an 'advanced' or 'boot sequence' menu, then set the CD as the 1<sup>st</sup> boot device. Now reboot your machine, and the PC should now boot from the CD. If you have a USB Bluetooth dongle or PCMCIA WiFi card, make sure it's inserted at startup time.

Assuming you inserted the BT2 CD, you will now be presented with a login menu, enter the following:

```
bt login: root
Password: toor
```

Now we'll start the Bluetooth service & scan for visible devices, assuming you have a USB Bluetooth Dongle plugged in and a Mobile phone in Bluetooth visible mode..

```
bt~ # hciconfig hci0 up
bt~ # hcitool scan
```

If that didn't work, it might be your Bluetooth dongle isn't recognised by this PC using Linux. In which case if you have a 2<sup>nd</sup> PC try it on that. Now we launch the desktop manager.

```
bt~# startx
```

When the desktop manager has launched you'll need to go click on the large 'K' in the bottom left of the screen to bring up the program manager menu. For wireless tools options, select Backtrack->Radio Network Analysis-> and then either -> Bluetooth or -> 80211 for Wifi.

Most of the Bluetooth tools run from the command line, so when you launch them you'll get a window running a text based terminal. The first Bluetooth tool is BDADDR – this changes the MAC address for your Bluetooth device. So as an example of how the command line works in Linux.

To get help with a command:

```
bt~ # bdaddr --help
```

To view the Bluetooth MAC address:

```
bt~ # bdaddr -i hci0
```

To change the MAC address to 00:00:00:FF:FF:FF

```
bt~ # bdaddr -t 00:00:00:FF:FF:FF
bt~ # hciconfig hci0 reset
bt~ # bdaddr
```

You'd use the above procedure to pretend to be another Bluetooth device. This is just one example of something that's made easy using Linux, but very difficult under Windows.