	Time[1]
1. Download hypervisor Windows: **VMware Player** (free), www.vmware.com/go/downloadplayer [2] Mac OS X: **VMware Fusion** (trial), http://www.vmware.com/products/fusion/ [3]	<1 min
2. Install hypervisor (reboot required on Windows; no reboot on Mac)	2 min
3. Download **BackTrack 4 R2 Release VMware Image** BackTrack 4 R2 from http://www.backtrack-linux.org/downloads/ Ver. 22.11.2010 is a big download, ~2400MiB (about half the size of a R/RW DVD)	14 min
4. Unpack the downloaded bt4-r2-vm.tar.bz2 file. This takes time as a big archive. On Windows you probably (unless done earlier) also need to get some tool to unpack bz2 archive files (e.g. WinRAR, http://www.win-rar.com/, shareware). (Mac OS X already has application for unpacking, Archive Utility.app)	10 min
5. Navigate to unpacked files and open the BT4R2.vmx file (VM configuration file).	<1 min
6. You now have the full power of BackTrack available at your fingertips!	28 min

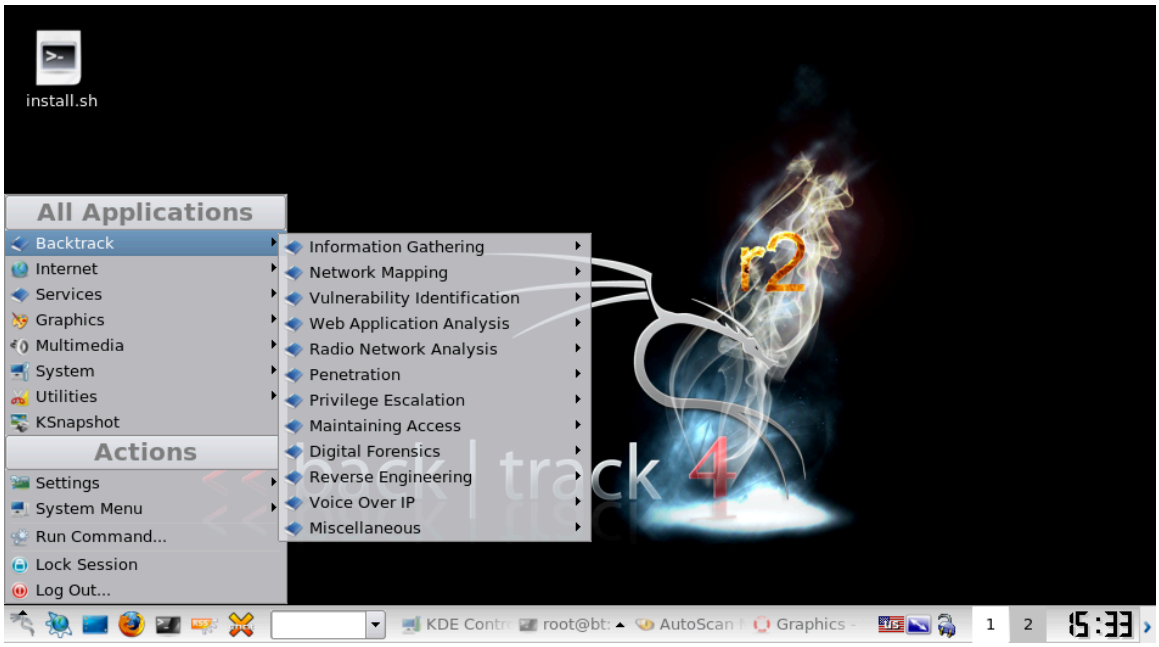

Figure 1: BackTrack 4 Release 2 (BT4R2)

[1] Download times based on a 24 Mbps connection. With a 3 Mbps connection, expect downloading BT to take up towards two hours.
[2] (Registration required) Version 3.1.3 for 32-bit and 64-bit Windows, 105MiB
[3] (Registration required) Version 3.1.2 for Intel-based Macs, 152MiB; 30-day trial

1 Using BackTrack

BackTrack starts in command line interface (CLI) but don't worry – you don't have to spend any time in this, unless you want to.

1. Login using user name **root** and password **toor**.
2. Start the graphical user interface (GUI) by the **startx** command (type startx and press return).

The GUI environment is as easy-to-use as both Mac OS X and Windows environments with the – for Windows users – familiar Start-menu at lower right corner. (Figure 1)

To enable networking (BT default is stealth-mode, no networking), in a terminal (one method):

```
$ ifconfig eth0 up
$ dhclient eth0
```

2 BackTrack, Huh?

For the non-initiated, BackTrack is a well-known software distribution with lots of tools for information security and (some) digital forensics.

The home page - http://www.backtrack-linux.org/ - has quite decent documentation on how to use the multitude of applications. The list of included software is comprehensive and the below is simply an overview of the categories:

- Information Gathering →
  - Archive →
  - DNS →
  - Route →
  - Seachengine →
  - Dradis Client, Dradis Server, Paterva Maltego CE
- Network Mapping →
  - Identify Live Hosts →
  - OS-Fingerprinting →
  - Portscanning →
  - Service Fingerprinter →
  - VPN →
- Vulnerability Identification →
  - Cisco →
  - Fuzzers →
  - OpenVas →
  - SMP Analysis →
  - SNMP Analysis
- Web Application Analysis →
  - Database (backend) →
    - MSSQL →
    - MYSQL →
    - Oracle →
  - Web (frontend) →
- Radio Network Analysis →
  - 80211 →
    - Cracking →
    - Misc →
    - Spoofing →
  - Bluetooth →
  - RFID →
    - RFIDIOt ACG →
    - RFIDIOt Frosch →
    - RFIDIOt PCSC →
- Penetration →
  - ExploitDB →
  - Fast Track →
  - Inguma →
  - Metasploit Exploitation Framework →
    - Framework Version 2 →
    - Framework Version 3 →
  - Social Engineering Toolkit →
  - Sapyto
- Privilege Escalation →
  - PasswordAttacks →
    - OfflineAttacks →
    - OnlineAttacks →
    - Chntpw
  - Sniffers →
  - Spoofing →
- Maintaining Access →
  - Backdoors and Rootkits →
  - Tunneling →
- Digital Forensics →
  - Anti Forensics →
  - File Carving →
  - Forensic Analysis →
  - Image Acquiring →
- Reverse Engineering →
- Voice Over IP →
  - VoIP Analysis → Signaling →
- Miscellaneous →

This is an extract from a more comprehensive guide into desktop virtualization.