Getting Started with BackTrack, Your New Hacking System

In this tutorial, I will walk you through BackTrack, giving you a tour of the most salient features for the hacker-to-be.

NOTE: BackTrack Is No Longer Supported; Switch to Kali Linux

BackTrack is no longer supported by the developers, so we have stopped using it as our primary hacking system here on Null Byte. Instead, please check out **my guide on installing Kali Linux**, which is what we now use for most hacks in Null Byte. Of course, you can still read on below if you'd like to get a little information about what BackTrack was and how it worked.

As you can see in the screenshot above, I've installed the most recent version of BackTrack, version 5 release 3 (generally referred to BT5r3). My install is the 64-bit version with the KDE interface, but the GNOME interface works just as well and has all the same features. I just prefer the KDE.

The BackTrack Menu

Similar to Windows start button, we have a button with the BackTrack icon in the lower left-hand corner along the lower panel.

When you click on it, it opens up a collection of multi-nested menus just like Windows. Let's go through each of them from bottom to top.

Step 1 Leave Menu

The first menu we come to is titled "Leave." This is where we would go when we want to shutdown BackTrack.

The sub-menus here are all self-explanatory.

- **End Session**
- **Lock Screen**
- **Start a parallel session as a different user**

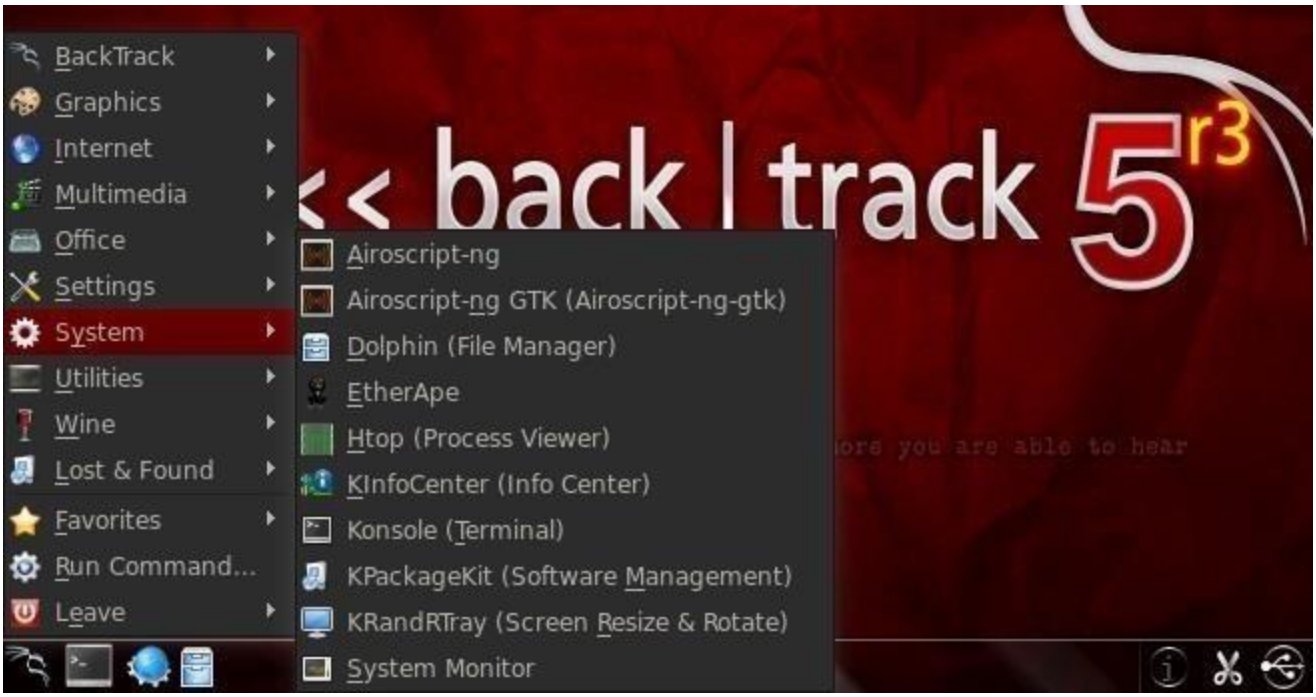
Step 2 Utilities Menu

We're going to skip over a few menu choices as they are not salient to our hacking tutorials, so go up to "Utilities."

- **Akonaditray** (a personal information manager)
- **Klipper** (a clipboard tool)
- **KWrite** (text editor similar to notepad),
- **Terminator** (a way of managing multiple terminals)
- **WBarConf** (a tool for managing your KDE bars)

Step 3 The System Menu

The next menu we'll look at is titled "System," which contains applications that are crucial to the hacker. When we hover over System we see **Airoscript-ng** and **Airoscript-ng GTK**. These are scripts for using Aircrack-ng to hack wireless. I'll do a tutorial on those in the near future, so stay tuned.



We also see

- **Dolphin** (a file manager similar to Windows Explorer)
- **EtherApe** (a graphical network model)
- **Htop** (a process viewer)
- **KinfoCenter** (an information center about your computer, i.e. CPU, memory, DMA, etc)

Below KinfoCenter we find probably the most important utility in any Linux system:

- **Konsole** (a terminal)

Any true hacker MUST become familiar with the terminal. For the remaining tools, we have:

- **KpackageKit** (download packages)
- **KRandRTray** (resizing windows)
- **System Monitor** (self-explanatory)

Step 4 The Internet Menu

Now we're going to jump up to the "Internet" menu and we can see **EtherApe** appears here again (it was also under "System").

Also, there's:

- **Firefox** (web browser)
- **Konqueror** (web browser)
- **Wicd** (for connecting to Wi-Fi)
- **Zenmap** (the network reconnaissance tool *nmap* overlaid with a nice GUI).

We'll be using nmap for target reconnaissance in a tutorial coming soon.

Step 5 BackTrack!

At the very top of the menu, we find the "BackTrack" menu! This is where we'll be spending most of our time as hackers. The BackTrack menu has shortcuts to the hundreds of hacking tools in BackTrack.

These tools are too numerous to list here, but as you can see BackTrack classifies them into the following:

- "Information Gathering"
- "Vulnerability Assessment"
- "Exploitation tools"
- "Privilege Escalation"
- "Mainataining Access"
- "Reverse Engineering"
- "RFID Tools"
- "Stress Testing"
- "Forensics"
- "Reporting Tools"
- "Services"
- "Miscellaneous"

Over the next several tutorials, we'll examine each of these set of tools.

Step 6 Exploitation Tools

If we hover over "Exploitation Tools," those of you who have following my earlier tutorials will see some familiar territory. Exploitation Tools opens a sub-menu of numerous types

of Exploitation Tools and if we hover over "Network Exploitation" we will see my favorite tool, "Metasploit Framework."

For those of you who are just getting started in hacking, **Metasploit** is a powerful network exploitation tool and I have a number Metasploit tutorials here, so take a look at them if you aspire to become an expert hacker.