i-Guard
Graphical Installer Manual

iGuard includes a graphical setup that helps the installation process. In this manual you can read on how to build the installer and then setup **iGuard**.

Requirements

In order to setup **iGuard** you will need:

- GTK v1.2, a portable graphics library installed in various platforms. For portability reasons GTK v.1.2 was preferred as v2.0 does not come preinstalled in many Linux boxes. If GTK is not installed in your system (can be checked by running gtk-config command) you will find in the packages/ folder. For details check http://www.gtk.org
- libpcap, a library required to capture packets from network interfaces. Most systems come with libpcap installed. In other case, you can find a stable version under the packages/ folder. For further information, you can visit http://www.tcpdump.org

As **iGuard** requires access to the raw packet interface it must be installed by a user with sufficient priviledges (usually root).

Running the installer

iGuard comes with a precompiled version of the installer running on most Linux platforms (currently tested on Redhat and Debian). To run the installer simply type:

./setup

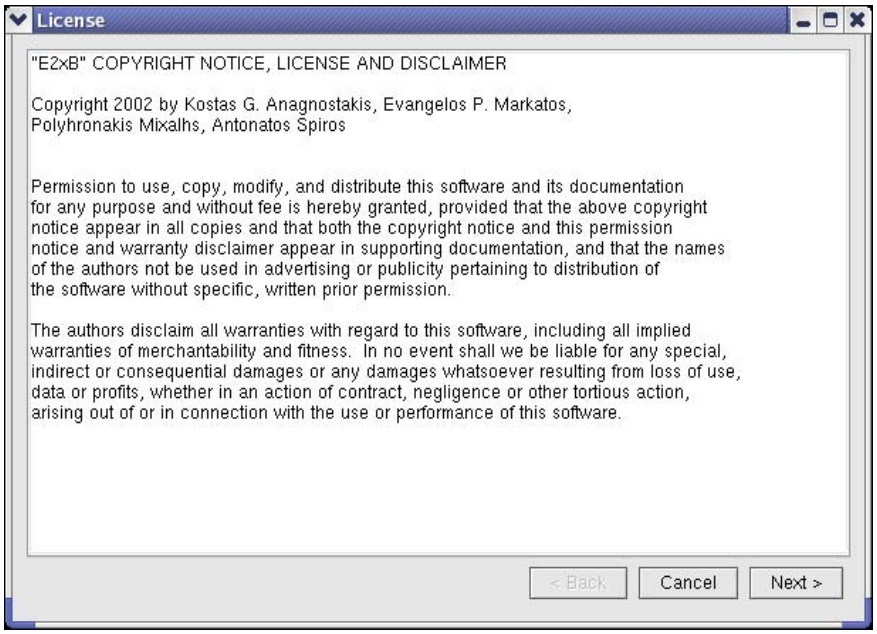
In case the installer does not run you can build it by typing *make* (assuming you have GTK installed). After the compilation is finished you can then run the installer.

Step by step process

iGuard installer is a simple tool, avoiding complex installation procedures.

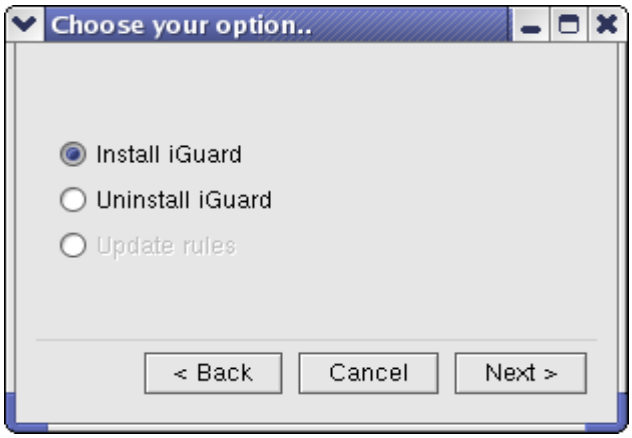
1. License and disclaimer

In the first screen, you will find the license and disclaimer screen. It is strongly recommended that you read this page.



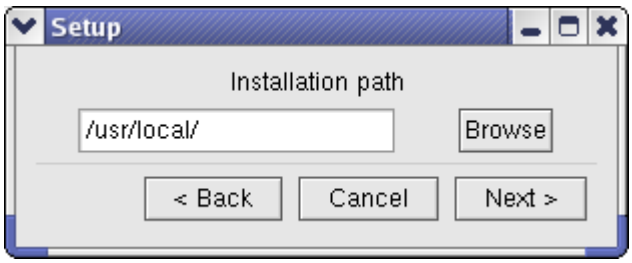
2. Choosing your option

In the next screen you can either choose to install or uninstall **iGuard**. The option of updating rules is currently unavailable (will be soon supported).

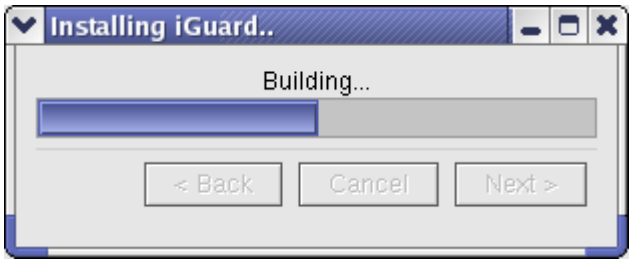


2.1 Installing iGuard

In case you want to install **iGuard** you should provide a path under which **iGuard** will be installed. In our example, we choose */usr/local*. The installer will create a directory *iguard/* under the directory provided and will install the binaries, configuration files and rules inside it. In our example, binaries will be placed inside */usr/local/iguard/*



The user should always provide a path. In case no path is provided the installation does not proceed. Relative paths can be also provided.
After this step, the configuration and compilation of **iGuard** follows. The installer stores the directory on which iGuard is installed at */etc/iguard.conf*



In case of a successful installation you should see the following screen

(The path depends on the directory selected by the user)

2.2 Uninstalling iGuard

Chosing to uninstall **iGuard** requires no further interaction from the user's side. The installer reads */etc/iguard.conf* to locate the directory on which **iGuard** is installed and removes it. The installer does not need to delete any other libraries or packages.

3. Using iGuard

Executing **iGuard** is exactly like running *Snort* (www.snort.org). The executable file is under $IGUARD_PATH/bin/ directory (where $IGUARD_PATH is the directory where iGuard is installed –in our previous example was /usr/local/iguard/-). A typical execution would be

./snort –i eth0 –c ../etc/snort.conf

where *eth0* is the network interface and *snort.conf* the Snort's configuration file. This execution examines all packets carriving ath the *eth0* interface and checks them against the default ruleset of Snort rules. For more details on the configuration settings you can find under *doc/* directory of the **iGuard** package.