

KillJoy ~ 0.1

Mobile remote session monitoring and management

KillJoy is a mobile TCP session monitor which allows for termination of specific sessions in addition to complete denial of service to a specific computer on the network. In its current implementation, KillJoy is designed to run for and has been tested on the Nokia n810 Internet Tablet, running Maemo 4 (Diablo); however, a minimalistic version also runs as a desktop application (this is a work in progress).



KillJoy's main strength and distinction is that it does its work as a normal computer on the network, without needing to redirect traffic through itself or act as a gateway in the form of an Intrusion Detection System (IDS). It accomplishes this via TCP and ARP packet injection. Furthermore, KillJoy is a flexible tool, allowing both interactive (manual) termination of sessions and automated control based on preset rules.

All of this, combined with portability in the form of a small, plant-able tablet, makes for a readily available tool to be used on any network without any special access.

Installation Instructions

KillJoy is written in Python and uses Scapy for its network deeds. As such, you will need to follow the steps below to get it to working on the Nokia n810 (other Maemo devices are probably similar):

1. Gain root privileges on the device. Note that you may need to enable the Extras repository. With a terminal open, type:

```
$ apt-get install rootsh
$ rootsh
```

2. From the terminal, install Python and the Python SDK (necessary for installing Scapy)

```
# apt-get install python2.5 python2.5-sdk python2.5-hildon
```

3. Next, install Scapy onto the device:

```
wget http://www.secdev.org/projects/scapy/files/scapy-latest.tar.gz
# tar -zxf scapy-latest.tar.gz
# cd scapy-2.1.0
# python setup.py install
```

4. At this point, if no errors were reported, test to ensure Scapy is installed correctly:

```
# scapy
INFO: Can't import python gnuplot wrapper . Won't be able to plot.
INFO: Can't import PyX. Won't be able to use psdump() or pdfdump().
INFO: No IPv6 support in kernel
WARNING: No route found for IPv6 destination :: (no default route?)
Welcome to Scapy (2.1.0)
>>> [Ctrl+D]
#
```

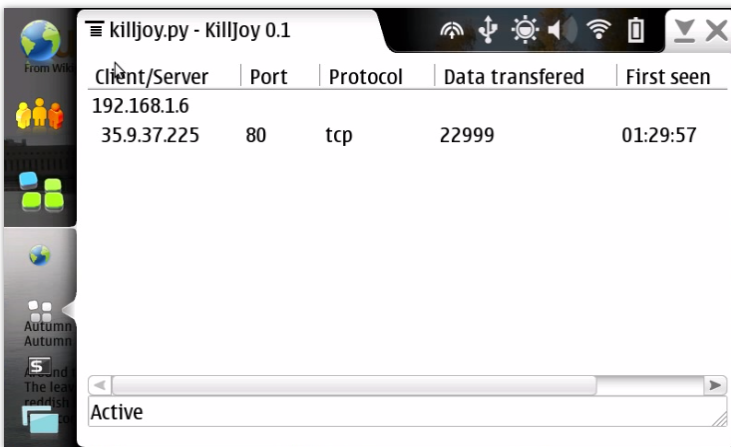
5. You're now set to run KillJoy. Just cd into its directory and launch the script:

```
# cd KillJoy
# chmod +x ./killjoy_nokia.py
# ./killjoy_nokia.py
```

Basic Usage

KillJoy's main window is simplistic, showing you a list of the active sessions going across the network. The scanner automatically starts with the program and terminates when the main window is closed.

Here's an example of how it might look on first launch:



Here, I'm downloading the latest copy of Audacity, although that's not immediately obvious since name resolution is disabled. You can change this by checking **Options > Enable name resolution**.

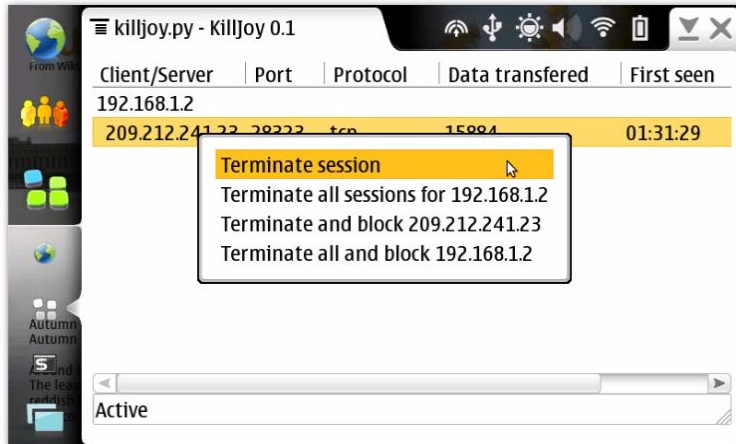
Terminating and Blacklisting Sessions

First, a clarification of the terminology:

- A *target* refers to a device on the local network.

- Each *target* may have multiple *sessions*, which are connections from it to the outside world. KillJoy shows all conversations over the TCP protocol in real time.

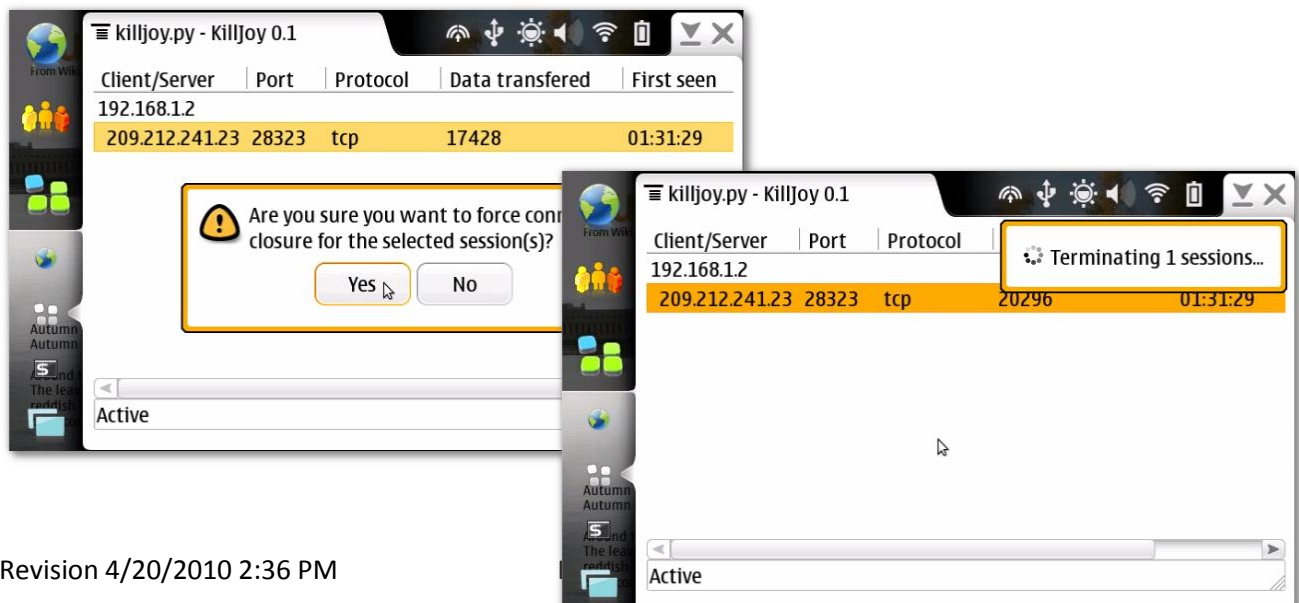
To terminate a specific session, highlight it and navigate to **Session** in the main menu (or right-click on the item to display a context menu).



This menu allows the following options:

- Terminate the session only
- Terminate the session, and then **block** future sessions matching:
`local_ip:local_port <--> remote_ip:remote_port`
- Terminate all sessions owned by the *target* (local device)
- Terminate all sessions owned by the target, and then **block** all future sessions for the target.
WARNING: this will effectively block all internet access over TCP from the device by terminating all sessions initiated by or intended for the local target when detected.

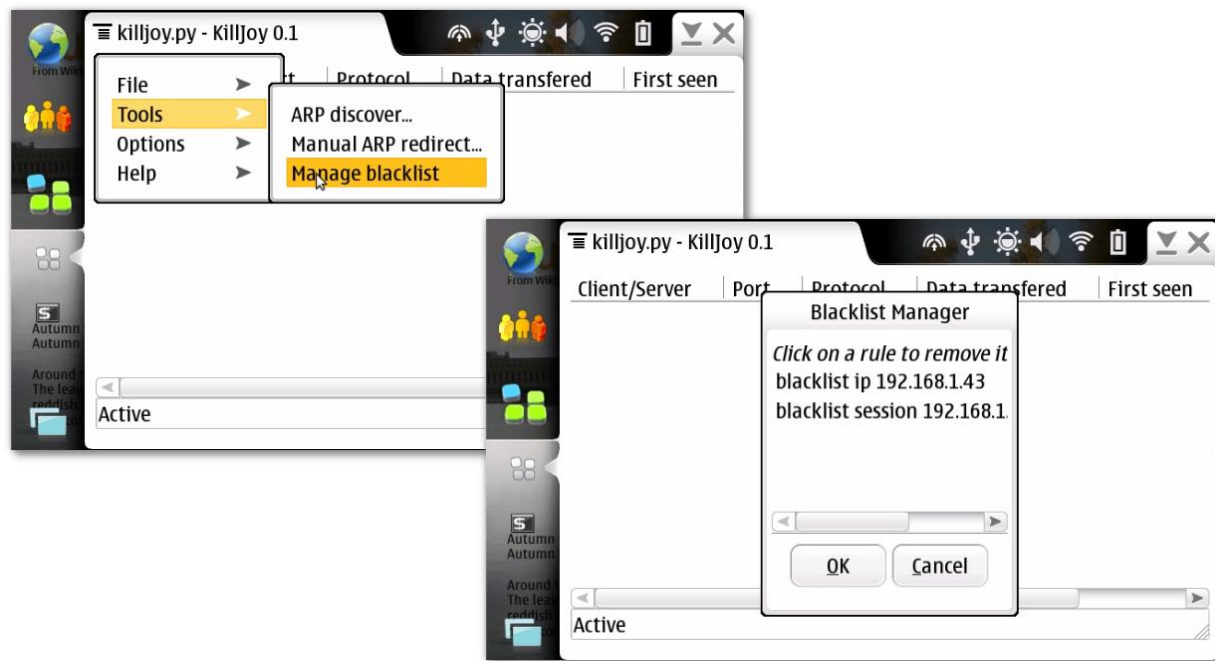
All actions take effect immediately.



Managing the Blacklist

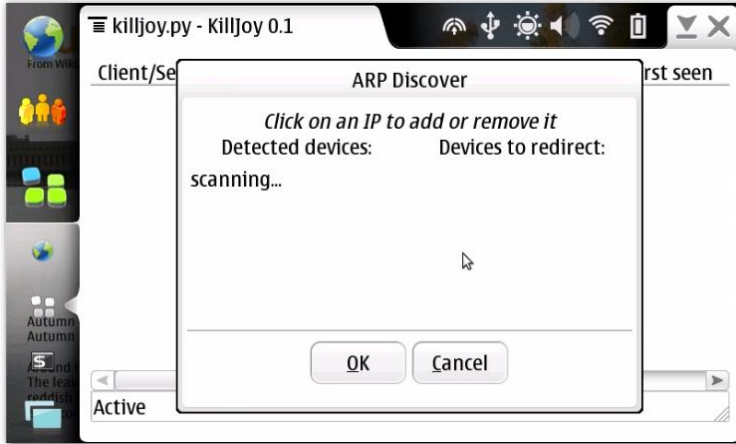
NOTE: This feature is experimental and may have instable results.

If you chose to blacklist a target or session, and later wish to remove the rule to allow the connections to persist, it is possible to remove the rules by selecting **Tools > Manage blacklist** from the main menu.

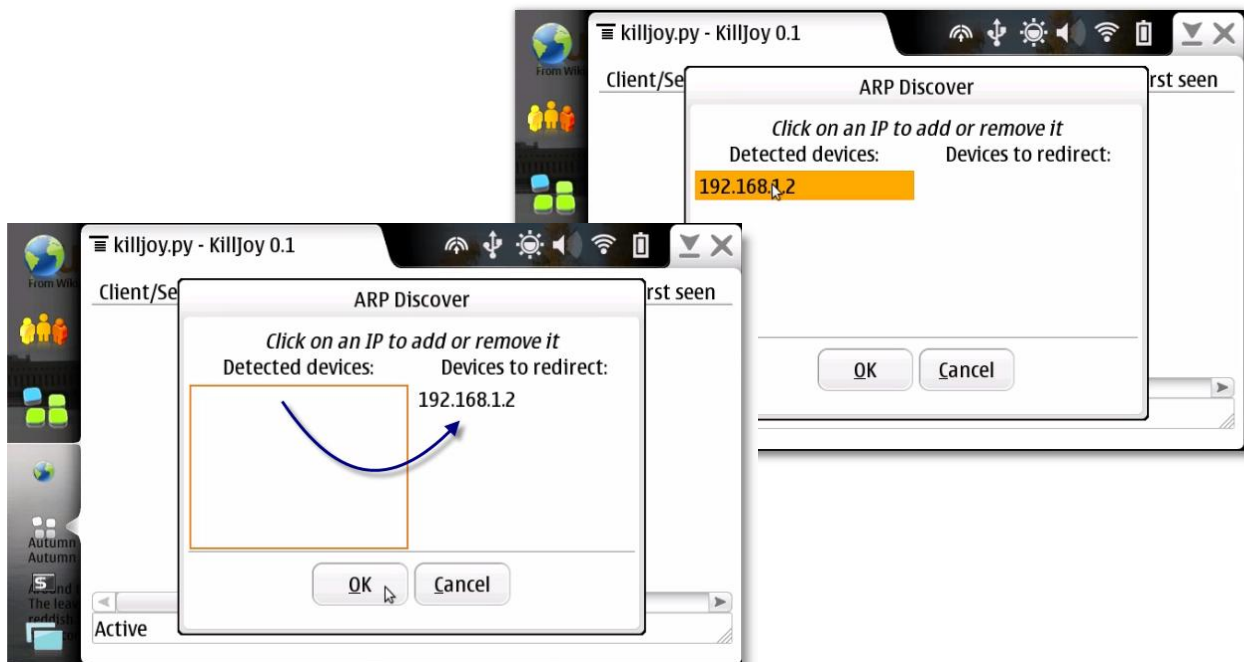


Advanced Usage

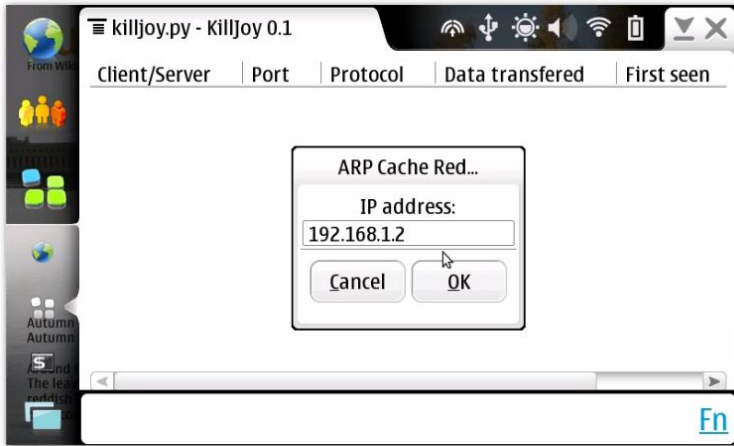
You may notice under some circumstances that only traffic from the device itself is being picked up. This can happen if the wireless card does not support true promiscuous mode, and certainly if the devices you wish to target are behind a switch. To provide a way around this, KillJoy allows the user to perform an ARP MiTM attack on a specific target so that its sessions can be seen and controlled.



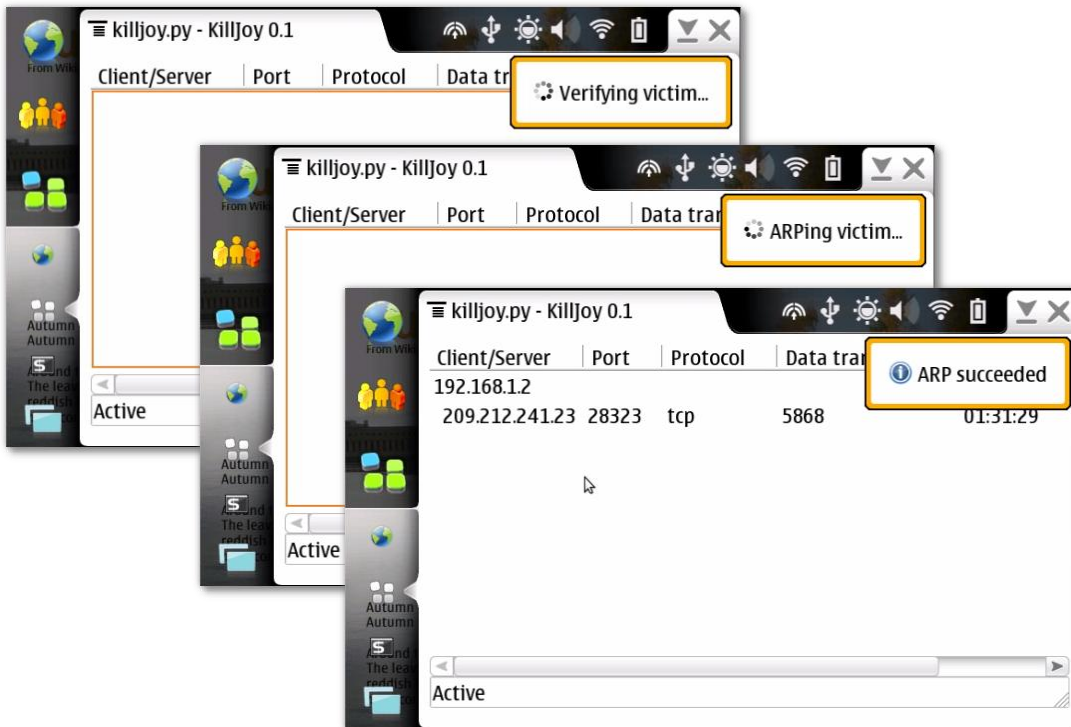
In this window, tapping on a list of detected IPs in the left pane will add them to the queue on the right (you can also tap on these to move them back). When you click OK, the ARP caches of all of the IPs listed in the right column will be poisoned and your device will be placed in between. KillJoy will maintain the MITM attack for each of these IPs so that it is not necessary to perform the attack again for the current session.



Alternatively, if you know the IP of the device you wish to target, select Tools > Manual redirect... from the main menu:



After selecting an IP from the list and clicking OK, with a little luck, one can now view the traffic for that machine:



Once the victim has been ARP'd, session management can continue as described previously. KillJoy will maintain the redirect and take care of re-ARPing when the application is shut down.

DISCLAIMER:

This product is in an unstable, beta-testing state. Use at your own risk and discretion; preferably on a network you own or have full permission for.