

# CLI Magic: Trojan Scan

By *srlinuxx*

Created *17/10/2005 - 9:25am*

Submitted by srlinuxx on Monday 17th of October 2005 09:25:11 AM Filed under [HowTos](#) [1]

We're all about security this week. Not the security you get from being all wrapped up in a baby-blanket, coddling, gratuitous GUI, but the kind that comes from knowing who is connected to your machine, and why. Trojan Scan is a simple but effective tool that monitors connections and alerts you to unauthorized activity of the sort that a rootkit, trojan, or other bad-to-the-bone-ware might engage in. Jump down out of that hi-tech hammock you're in and let's take a look.

Trojan Scan is crafted in the finest Unix tradition, building on and combining existing tools to scratch a particular itch. Most of the work is done by the `lsof` command, which lists open files. What good is that, you ask, when checking for connections? Remember, in Unix, everything is a file, so the answer is that it's plenty good. Trojan Scan invokes `lsof` like this:

[Full Article](#) [2].

[HowTos](#)

---

**Source URL:** <http://www.tuxmachines.org/node/3094>

## Links:

[1] <http://www.tuxmachines.org/taxonomy/term/98>

[2] <http://enterprise.linux.com/enterprise/05/10/14/1539210.shtml?tid=89>