Network Monitors

There are two types of network monitors: those that monitor your own system's network settings and those that monitor network traffic. The latter includes security tools (that can also be used as hackers tools) for exposing security weaknesses in a network. Be aware and be safe! A list of available tools is at [Top Ubuntu Security Tools](http://www.ubuntu-unleashed.com/2008/06/top-security-tools-in-ubuntu.html).

**Netstat**

[http://ubuntuguide.org/images/thumb/f/f6/Prefapp1.png/18px-Prefapp1.png](http://ubuntuguide.org/wiki/File:Prefapp1.png) [Netstat](http://www.faqs.org/docs/linux_network/x-087-2-iface.netstat.html" \o "http://www.faqs.org/docs/linux_network/x-087-2-iface.netstat.html) is the Linux command-line tool to monitor network status and functions. There are many usage parameters. See the manual for help.

netstat

**Etherape (Network monitoring)**

[http://ubuntuguide.org/images/thumb/f/f6/Prefapp1.png/18px-Prefapp1.png](http://ubuntuguide.org/wiki/File:Prefapp1.png) [EtherApe](http://etherape.sourceforge.net/" \o "http://etherape.sourceforge.net/) is a graphical utility that allows you to see (in real-time) where connections are being made on your network, or between your network (or computer) and the Internet. If you are experiencing unexpected network activity on your computer or LAN and wish to see where the activity is occurring, this is an easy tool to use. Both "local" user and "root user" installations are created; in general you must use the root user installation to see all your network traffic.

sudo apt-get install etherape

**List open files**

[http://ubuntuguide.org/images/thumb/f/f6/Prefapp1.png/18px-Prefapp1.png](http://ubuntuguide.org/wiki/File:Prefapp1.png) Sometimes you will see your network slowing and want to know which files are sending data over ports. Use this command:

lsof -i -n -P

**Nmap**

[http://ubuntuguide.org/images/thumb/f/f6/Prefapp1.png/18px-Prefapp1.png](http://ubuntuguide.org/wiki/File:Prefapp1.png) [Nmap](http://nmap.org/" \o "http://nmap.org/) is a free open source utility for network exploration (including showing open ports and running services) and security auditing. Install:

sudo apt-get install nmap

Scan your own PC:

nmap localhost

(Once you have found out which ports are open, use a [firewall](http://ubuntuguide.org/wiki/Ubuntu_Precise_Network_Management#Firewall) to close the ones you don't want open.)

**Nmap GUI**

Install:

sudo apt-get install nmapfe

or you can try Zenmap:

sudo apt-get install zenmap

**Nessus**

[Nessus](http://www.nessus.org/) is a proprietary comprehensive vulnerability scanning suite that is free for personal, non-enterprise usage. See the website for details.

**Snort**

[Snort](http://www.snort.org/) is the de facto open source standard for intrusion detection. Install:

sudo apt-get install snort

It can be used with an MySQL database (sudo apt-get install snort-mysql) or with a PostgreSQL database (sudo apt-get install snort-pgsql).

**AcidBase**

[AcidBase](http://secureideas.sourceforge.net/) is an intrusion detection / basic analysis and security engine that uses Snort. Install:

sudo apt-get install acidbase

**AppArmor**

[AppArmor](http://en.opensuse.org/AppArmor) is a set of security enhancements developed by Novell for SUSE Linux. It is installed in (K)ubuntu by default.

**Disable AppArmor**

AppArmor can prevent some services from running as expected and cannot be used in conjunction with SELinux. To disable it:

/etc/init.d/apparmor stop

update-rc.d -f apparmor remove

apt-get remove apparmor apparmor-utils

**SELinux**

[SE Linux](http://en.wikipedia.org/wiki/Security-Enhanced_Linux) (Security Enhanced Linux) is an NSA (US National Security Administration) recommended set of tools for enhanced security in Linux systems. It enforces strict access controls (privileges) and is meant for mission-critical installations. It is not suitable for the casual desktop user. It was first available in Hardy Heron and is being updated for Intrepid Ibex. It is not compatible with AppArmor (which must first be removed).

sudo apt-get install selinux

**Knockd (Port security)**

[http://ubuntuguide.org/images/thumb/f/f6/Prefapp1.png/18px-Prefapp1.png](http://ubuntuguide.org/wiki/File:Prefapp1.png) [Knockd](http://www.zeroflux.org/projects/knock" \o "http://www.zeroflux.org/projects/knock) is a small server that listens for a pre-defined sequence of port opening attempts (a "knock") before opening an otherwise closed firewall port for communications. Install:

sudo apt-get install knockd