

↳ Bastille Linux



The Bastille Hardening program:
increased security for your OS

[Resources](#) | [News & Updates](#) | [Credits & Sponsors](#) | [Quotes](#) | [Screenshot](#) | [Undoing Bastille](#) | [Assessment](#) | [Jay's Linux Security Page](#)

[Running Bastille On](#) | [Development Resources](#)

What Is It?

The Bastille Hardening program "locks down" an operating system, proactively configuring the system for increased security and decreasing its susceptibility to compromise. Bastille can also assess a system's current state of hardening, granularly reporting on each of the security settings with which it works.

Bastille currently supports the Red Hat (Fedora Core, Enterprise, and Numbered/Classic), SUSE, Debian, Gentoo, and Mandrake distributions, along with HP-UX. **Full Mac OS X is ready for download today.** Bastille's focuses on letting the system's user/administrator choose exactly how to harden the operating system. In its default hardening mode, it interactively asks the user questions, explains the topics of those questions, and builds a policy based on the user's answers. It then applies the policy to the system. In its assessment mode, it builds a report intended to teach the user about available security settings as well as inform the user as to which settings have been tightened.

NOTE: [Bastille Linux is now Bastille UNIX - read about this here.](#)

Bastille UNIX release coming January 14th, 2008.

Why Use It?

Bastille broke new ground by working to educate users about security, and help them make balanced, informed choices. Many users have found Bastille's secondary goal of educational just as useful as its primary goal of system hardening, leading some organizations to make an interactive Bastille hardening session part of their training regimen for new system administrators. In this spirit, Bastille can allow the user to run through the entire interactive portion without applying the chosen changes.

Who Uses It?

Bastille has become a vital part of the security hardening space. It's the most used hardening tool for Linux and HP-UX and is shipped by the vendor on SuSE, Debian, Gentoo and HP-UX. It is covered in all of the major books on Linux Security and has been the subject of a number of articles. Most recently, the [Center for Internet Security's](#) Linux Hardening Guide has recommended the use of Bastille to help harden systems.

Who Develops It?

Bastille was originally conceived of by a group of concerned system administrators at a conference organized by the [SANS Institute](#), an ally of the Bastille Project. [Jay Beale](#) wrote the initial program and now leads a number of developers, beta-testers and concept-creators in Bastille's development. For example, employees of [Hewlett Packard](#) have extended Bastille to HP-UX and shipped it with the latest versions of that operating system. Employees of [IBM](#) have helped port Bastille to SuSE and TurboLinux, while contractors at the Navy's [Space and Naval Warfare Systems Center](#), working under the funding of TSWG, have helped extend Bastille's functionality. Bastille also involves a number of unpaid volunteers, like Peter Watkins who created the firewall, Paul Allen who created the GUI, Mike Rash, who contributed the Port Scan Attack Detector (PSAD) and many others. We'll be updating the Credits file soon!

Please check back for updates!

Click on this ["Download"](#) link above to download, install and run Bastille.

Anti-SPAM

Anti-SPAM for Bastille Linux e-mail is provided by [No-Junkmail.com](#), home of the SPAM Zapper. This inline solution has been very effective for us. Jay's recommendation can be found [at his site](#).