NAME

bastille - system lockdown tool

SYNOPSIS

Path: **/usr/sbin** (Linux)

Path: **/opt/sec_mgmt/bastille/bin** (HP-UX)

bastille [**-b** | **-c** | **-x**] [**-f** *alternate_config_file*]
[**--os** [*version*]]

bastille [**-l** | **-r** | **--assess** | **--assessnobrowser**]

DESCRIPTION

b

Bastille is a system-hardening/lockdown program that enhances the security of a Unix host. It configures daemons, system settings and firewalls to be more secure. It can shut off unneeded services and r-tools like **rcp** and **rlogin**, and helps create "chroot jails" that help limit the vulnerability of common Internet services, like Web servers and DNS. This tool currently hardens Red Hat 6.0-8.0, Mandrake 6.0-8.1, HP-UX 11i v1, HP-UX 11i v2, and HP-UX 11i v3. It is currently being tested on Debian, SuSE, and Turbo Linux.

The utility includes a policy/configuration-selection interface, a configuration engine and a reporting module. The primary profile-building interface is an X interface via Perl/Tk. There is also a text-based Perl/Curses interface for Linux. The tool can be used interactively and non-interactively (when the policy-application engine is used directly). Used interactively, to build system-security configurations, Bastille has been designed to explain security issues to system administrators, then let them decide how to let the tool handle them. This both secures the system and educates the administrator. When the configuration engine is used directly, the utility is useful for duplicating a security configuration on multiple machines.

When used interactively (**bastille**, **bastille -x**, or **bastille -c**), the user interface guides you through a series of questions. Each step contains a description of a security decision involved in hardening a Unix system. Each question describes the cost/benefit of each decision. The Tk interface gives you the option to skip to another question module and return to the current module later. The X interface provides "Completed Indicators" to show you which question modules are complete. After you have answered all of the questions, the interface then provides automated support in performing lockdown steps. After performing the steps Bastille can perform automatically, the utility produces a "to-do" list that describes remaining actions you must perform manually to ensure the system is secure.

Security hardening can also be performed directly through the configuration engine (**bastille -b**) using the default or an alternate configuration (**bastille -b -f** *file*) (see the **config** file in the *FILES* section below for the default location). This method is useful for duplicating a particular security configuration on multiple machines. Before using the configuration engine directly, a configuration file must be created by using Bastille interactively. After the configuration file is created, copy it to the other systems, install Bastille Unix on those systems, then run the configuration engine on those systems.

Bastille draws from many major reputable sources on Unix Security. The initial development integrated Jay Beale's existing O/S hardening experience for Solaris and Linux with most major points from the SANS' *Securing Linux Step by Step* and Kurt Seifried's *Linux Administrator's Security Guide*. Later versions incorporated suggestions from the *HP-UX Bastion Host White-paper*, Center for Internet Security, and other sources.

To ensure that Bastille is used as safely as possible, please:

1) Let the developers know about any impacts you discover which aren't mentioned in the question text for possible inclusion in future revisions of the questions text.

2) Test Bastille configurations in a non-production environment first, with the application stack fully functionally tested after lockdown before deployment in a production environment. The characterization of consequences is known to be incomplete, especially for general purpose systems.

Options

bastille recognizes the following options

-b Run in batch mode. This option takes the answers that were created interactively and applies them to the machine.

-c Linux Only. Bring up the text interface of the interactive portion of Bastille. It is implemented with the Perl/Curses module, which must be installed separately if it did not come with your version of Perl.

-f *alternate_config_file*
Use an alternate config file versus the default location.

-l List applied configuration files. List the configuration files in the configuration file directory that matches the one last used.

-r Revert Bastille-modified system files to the state they were in before Bastille was run. Note that, if any changes to the system configuration were made in the interim, those changes should be reviewed again to make sure they (1) still work, and (2) have not broken the system or compromised its security.

-x The default option. Run the Bastille X interface. It is implemented with the Perl/Tk module, which must be installed separately if it did not come with your version of Perl.

--assess
Run Bastille in assessment-only mode so that it investigates the state of hardening, reports on such and generates a score. No changes are made to the system. It generates HTML and text reports and a Bastille configuration file.

For each question, Bastille generates one of the following results:

Yes The associated Bastille lockdown has been applied to the product or service shipped with HP-UX. Bastille may not always correctly detect the status of products or services that are not shipped with the HP-UX OE. Also, Bastille may not detect all variations of the possible ways to disable or enable a service or feature. It will detect if Bastille did so, and will likely detect configuration made in accepted, standard ways.

No The question configuration has not been applied.

User Action Pending
Bastille had performed a partial configuration; leaving the user with some actions needed to complete the configuration. These actions are listed in the TODO file listed below.

Inconsistent
Bastille can not tell the status. Usually, this is do to the system being in an inconsistent state. For example, Bastille would return this status of a service running in the process list, but configured on disk to be off. Note, there are some cases where inconsistent states that Bastille can not detect could be created on the system, so if the administrator has made changes to the system, and needs to rely on Bastille results, the system should be rebooted first to ensure the configuration is consistent. This caveat does not apply to Bastille initiated actions.

N/A: S/W Not Installed
This indicates that the relevant software is not installed, so there is no need to lock down the given item, but care should be taken when the software is installed to lock it down at that point.

Needed S/W Missing
This indicates that the item is not locked down since it needs software that is currently not available on the system.

Set to *value*
This indicates a non-boolean setting.

Not Defined
This indicates a non-boolean setting that has not been set yet. Thus the system default settings apply. In the case of later HP-UX versions, default account security settings are often found in the **/etc/security.dsc** file.

See the *FILES* section for location. The HTML version of the report is shown in a browser if either a graphical or text browser can be found.

--assessnobrowser
Same as **--assess**, except that the report is not displayed in a browser.

--os[*version*]
Explicitly set the operating system version while generating a configuration file. By setting the operating system version, all questions valid for that operating system will be asked and

configuration files can be generated for any version Bastille recognizes. For a complete list of operating system versions type **bastille -x --os**.

DIAGNOSTICS

$DISPLAY not set, cannot use X interface...
You explicitly asked for the X interface using the **-x** option, but the **DISPLAY** environment variable was not set. Set the environment variable to the desired display to correct the problem.

System is in original state...
You attempted to revert the files that Bastille changes with the **-r** option, but there were no changes to revert.

Must run Bastille as root
Bastille must run as the root user, since the changes it makes configure the machine.

Troubleshooting
Error messages that cite problems with opening, copying, or reading files usually relate to NFS file systems that do not trust the root user on the local machine. Please see the options parameter in the *fstab*(4) manpage for details. Errors that complain about individual configuration files indicate that a system has been too heavily modified for Bastille to make effective changes, or that the files, locations, or permissions of the Bastille installation directories have been changed.

If Bastille is unable to complete a lockdown, you should receive errors or warnings. Analyze the errors or warnings to determine if your lockdown was successfully applied. You may use the **--assess** option to aid in this diagnostic. Once the system state that caused the abort is fixed, run **bastille** again to complete the lockdown. This helps avoid cases where an incomplete lockdown can contribute to an inconsistent system configuration.

EXAMPLES

Example 1
Run the Bastille X interface. This will create a configuration file which can be run either immediately by Bastille after you have answered all of the questions, or saved for later use in a **config** file. See the *FILES* section below.

bastille

Example 2
Run Bastille in batch mode. This will take the answers that were created interactively and apply them to the machine.

bastille -b

Example 3
Perform an audit of the system to determine the state of the security settings on it, and place it in the audit log locations (specified below).

bastille --assessnobrowser

DEPENDENCIES

- Perl version 5.8.0 or greater, but recommend 5.8.8 or greater for best performance
- Perl/Tk version 8.00.23 or greater
- Perl/Curses version 1.06 or greater (on Linux only)

FILES

/etc/Bastille/config (Linux)

/etc/opt/sec_mgmt/bastille/config (HP-UX)

The **config** file contains the answers to the most recently saved session

/var/log/Bastille/error-log (Linux)

/var/opt/sec_mgmt/bastille/log/error-log (HP-UX)

The error log contains any errors that Bastille encountered while making changes to the system.

/var/log/Bastille/action-log (Linux)

/var/opt/sec_mgmt/bastille/log/action-log (HP-UX)

The action log contains the specific steps that Bastille took when making changes to the system.

/var/log/Bastille/TODO (Linux)

/var/opt/sec_mgmt/bastille/TODO.txt (HP-UX)

The to-do list contains the actions that remain for you to do to ensure the machine is secure.

/var/log/Bastille/Assessment/assessment-report.html (Linux)

/var/log/Bastille/Assessment/assessment-report.txt (Linux)

/var/log/Bastille/Assessment/assessment-report-log.txt (Linux)

/var/opt/sec_mgmt/bastille/log/Assessment/assessment-report.html (HP-UX)

/var/opt/sec_mgmt/bastille/log/Assessment/assessment-report.txt (HP-UX)

/var/opt/sec_mgmt/bastille/log/Assessment/assessment-report-log.txt (HP-UX)

These are the assessment report locations. They are formatted HTML, text, and a Bastille "config-file" respectively.

/var/log/Bastille/Assessment/Assessment/Drift.txt (Linux)

/var/opt/sec_mgmt/bastille/log/Assessment/Drift.txt (HP-UX)

This contains information about any configuration drift the system had experienced since the last Bastille run. This file will only be created when there has been an earlier Bastille-configuration applied to the system.

SEE ALSO

perl(1), bastille_drift(1M), fstab(4)

Here are some other references used during Bastille's development. Note that the websites and content are maintained by their domain owners. The domain owners are solely responsible for their own site and content:

The Linux Security HOWTO
Available at **http://www.linuxdoc.org/HOWTO/Security-HOWTO.html**. One of the best references regarding general Linux Security.

Security Quick-Start HOWTO for Linux
Available at **http://www.linuxsecurity.com/docs/LDP/Security-Quickstart-HOWTO/**. This is also a very good starting point for novice users (both to Linux and security).

The Linux Security Administrator's Guide
Available at **http://seifried.org/lasg/**.

Securing and Optimizing Linux: RedHat Edition
Available at **http://www.linuxdoc.org/links/p_books.html#securing_linux**.

Securing Debian Manual
Available at **http://www.debian.org/doc/manuals/securing-debian-howto**. It is provided for offline reading in several formats (Text, HTML and PDF) by installing the **harden-doc** package in Debian systems.