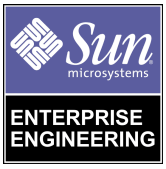
The Solaris™ Security Toolkit - Release Notes

Updated for Toolkit version 0.3

By Alex Noordergraaf - Enterprise Engineering and Glenn Brunette - Sun Professional Services

Sun BluePrints™ OnLine - June 2001



http://www.sun.com/blueprints

Sun Microsystems, Inc.
901 San Antonio Road
Palo Alto, CA 94303 USA
650 960-1300 fax 650 969-9131

Part No.: 816-1469-10
Revision 01, 06/13/01
Edition: June 2001

Please
Recycle

The Solaris™ Security Toolkit - Release Notes

Updated for Toolkit version 0.3

Overview

This Sun BluePrints™ OnLine article describes the changes made to the Toolkit as it has evolved between releases. The contents of this article are based on the `CHANGES` file included with the Toolkit source, but each entry has been expanded to provide more information about the modification or enhancement.

Update

This Sun BluePrints OnLine article has been updated to reflect changes in the newly released version (0.3) of the Solaris™ Security Toolkit for the Solaris™ Operating Environment (Solaris OE). The documentation for this release of the Toolkit 0.3 has been re-written into the following four parts:

- *Quick Start* focuses on the minimal set of required information needed in order to get the Toolkit up and running as quickly as possible. The setup and configuration requirements for the Toolkit are quite different, depending on whether or not it is being run in standalone or JumpStart modes—this document has a section for each.
- *Release Notes* discusses the changes and enhancements included in the new release.
- *Installation, Configuration, and Usage Guide* focuses on advanced configuration and installation information not contained in the Quick Start guide.

- *Internals* focuses on the actual components of the Toolkit. All of the internal scripts are individually listed and discussed.

Version 0.2 to Version 0.3 Changes

The following modifications and enhancements have been made to the Toolkit since the release of version 0.2 in November of 2000:

- Undo capability
- Updated framework
- Changes to profiles
- New driver scripts
- Changes to driver scripts
- New finish scripts
- Changes to finish scripts
- New file templates
- Miscellaneous changes

Each of these is discussed in greater detail.

Undo Capability

One of the most frequently requested enhancement added to Toolkit version 0.3 is the addition of undo functionality, which will allow administrators to undo the effects of a Toolkit run or runs on a given system. This feature allows administrators to backout or undo individual runs, or all Toolkit runs, completed on a system.

To use this feature, an option has been added to the `jass-execute` program. This option, `-u` instructs the program that a previous run of the Toolkit is to be removed. Because the `jass-execute` program is used to access the undo feature, this feature

is only available in standalone mode and not in JumpStart mode. On a system where several Toolkit runs have been performed, output similar to the following will be displayed:

```
# ./jass-execute -u
./jass-execute: NOTICE: Executing driver, undo.driver
Please select from one of these backups to restore to
1. May 04, 2001 at 18:25:04 (//var/opt/SUNWjass/run/
20010504182504)
2. May 04, 2001 at 18:22:50 (//var/opt/SUNWjass/run/
20010504182250)
3. Restore from all runs
Choice?
```

During a Toolkit undo run, the files are restored to their state before that particular Toolkit run. Toolkit modified and backed up files that were manually modified after a Toolkit run are restored automatically, and the manual changes lost.

The undo operation can be used for Toolkit runs that were initiated in either standalone or JumpStart mode. Only runs that were initiated with version 0.3 of the Toolkit can be undone.

The following files were added or modified in the drivers directory to support this functionality:

- `driver.run`
- `driver.funcs`
- `undo.driver`
- `undo.funcs`
- `undo.run`

In order to ensure correct execution of this functionality, these files should not be altered. If upgrading to version 0.3 from a previous Toolkit release, these files must be used in their entirety.

Updated Framework

Quite a few modifications were made to the Toolkit framework with the release of version 0.3. Each of these modifications is briefly discussed:

Functions that existed originally in the `driver.run` script were separated into a new file, `driver.funcs`, to allow sharing of common functions between Toolkit runs and Toolkit undo operations.

The Toolkit variable, JASS_CONFIG_DIR, has been renamed to JASS_HOME_DIR to provide a clearer meaning as to its use. The JASS_HOME_DIR is defined as the directory location in which the Toolkit is installed.

The SCRIPTS* and FILES* variables now use the JASS_ prefix (i.e., JASS_SCRIPTS and JASS_FILES) for consistency. Driver and finish scripts developed using older versions of the Toolkit will need to be updated to use the JASS_ prefix in order to function properly.

SUNWjass is now a reserved name for the Toolkit software package format distribution. The Toolkit is now available in this format, as well as in the original compressed tar format. The same source is distributed in both distributions. Administrators can also now make their own packages using the supplied make-pkg script.

Introduced in this release is a new data repository in the directory, /var/opt/SUNWjass. This repository, added to support undo operations, saves data on how each Toolkit run was executed, a manifest of files modified by the Toolkit, and the execution log. The undo feature mentioned previously relies on the information stored in these directories.

Note – This hierarchy is used to store information for each Toolkit run on a system.

The copy_files function in the driver.run script was enhanced to support the copy of Solaris OE specific files. Also, the copy_files function was updated to support being called by finish scripts. This allows a finish script to install files in the same manner as drivers using the JASS_FILES variable. A list of files to be installed is still the only argument to this function.

A new configuration file, finish.init, has been added to handle all finish script configuration variables. These variables still can be overridden by the user in the user.init file. This file was heavily commented to explain each variable, its impact, and its use in finish scripts.

Most of the finish scripts can now be customized to suit an organization's security policy using variables found in the finish.init script. At this point, nearly every aspect of the Toolkit can be customized using variables (without needing to alter the core script code). The use of this configuration file is strongly recommended so as to minimize migration issues with new Toolkit releases.

Changes to Profiles

The sendmail package listing was removed from the minimal-iPlanetWS-Solaris8-64bit.profile, as those packages are included in the SUNWCreq meta-cluster by default.

The SUNWcslu package was removed from the minimal-iPlanetWS-Solaris8-64bit.profile, as it was a typographical error. This package does not exist.

New Driver Scripts

The Driver script, hardening-jumpstart.driver, was added to provide a template for securing JumpStart servers. Some services will be automatically re-enabled by add_install_client. Proper use of add_install_client and rm_install_client to only have JumpStart clients available when necessary will help to keep these services to a minimum.

Changes to Driver Scripts

In order to support finish scripts in this release, the following entries were added to the JASS_HOME_DIR/Drivers/hardening.driver script:

- enable-process-accounting.fin
- install-shells.fin
- set-power-restrictions.fin
- set-ftpd-umask.fin
- set-sadmind-options.fin
- set-sys-suspend-restrictions.fin
- update-cron-log-size.fin

In addition, an entry for Files/.profile was added to the JASS_FILES environment variable in the Driver script, config.driver. This allows the installation of the /.profile file from the Files/.profile source location onto the target system when the Toolkit is configured to use the config.driver script.

New Finish Scripts

In a continuing effort to provide enhanced functionality, the following finish scripts have been added to the Toolkit. Each script is outlined with a brief explanation.

disable-ipv6.fin	This script disables the definition of IPv6 compatible network interfaces.
disable-vold.fin	This script disables the volume management daemon.

enable-process-accounting.fin	This script enables Solaris OE Process Accounting. Note that the following Solaris OE packages must be present on the system: SUNWaccr, SUNWaccu
install-shells.fin	This script updates the /etc/shells file with the standard shell definitions applicable for the specific version of the Solaris OE used. This file will be created if it does not already exist.
set-power-restrictions.fin	This script restricts use of power management functions to only the root user by default or the user(s) defined by the variables, JASS_POWER_MGT_USER and JASS_CPR_MGT_USER.
set-ftpd-umask.fin	This script sets the default file creation mask for use during FTP. The default value is 022, but this can be changed using the JASS_FTPD_UMASK variable.
set-sadmind-options.fin	This script configures the System Administration daemon to use strong authentication (AUTH_DES).
set-sys-suspend-restrictions.fin	This script restricts the ability to perform system suspend functions using the variable: JASS_SUSPEND_PERMS. The default Toolkit value for this is - which restricts access to the root user only.
update-cron-log-size.fin	This script increases the size of CRON facility log files from 0.5 MB by default to 10MB. This setting can be changed using the JASS_CRON_LOG_SIZE variable.

Changes to Finish Scripts

A variety of modifications and enhancements have been performed on finish scripts. Each modification is discussed:

The list of accounts that should be disabled on the system (by disable-system-accounts.fin) are now explicitly enumerated in the JASS_ACCT_DISABLE variable. Previously, user accounts that were added manually were also disabled.

The `tmpfs` partition size default limit has been increased from 100 MBytes to 512 MBytes in this release of the Toolkit. Also, the default profiles for each system (in the `Profiles/` directory) now have at least 768M devoted to swap space. The `set-tmpfs-limit.fin` finish script has also been updated to not run under version 2.5.1 of the Solaris OE where this functionality is not supported.

The `disable-system-accounts.fin` finish script was modified to use a copy of the `/sbin/noshell` that is installed from the `JASS_HOME_DIR/Files/` directory structure. The `/sbin/noshell` script is now installed using `copy_files` called from `disable-system-accounts.fin`.

The `disable-rlogin-rhosts.fin` finish script has been renamed to `disable-rhosts.fin` to be more indicative of its actions. In addition, both `rsh` and `rlogin` entries are now commented out in the `/etc/pam.conf` file to ensure that `rhosts` authentication is not enabled for either service.

The `install-strong-permissions.fin` finish script was updated to set stronger permissions on the `/var/cron` directory. Currently, this directory is set to mode 700. The permissions on the `/var/adm/loginlog` file were changed from mode 0640 to mode 0600, and its group was changed from `sys` to `root`.

Note – This file is not used by the SYSLOG facility if the default `/etc/syslog.conf`, supplied by the Toolkit, is installed.

Duplicate entries in the `EvilList` parameter in the `update-inetd-conf.fin` finish script were removed. This script was altered to provide better display and processing of the services that are disabled.

Formatting was improved for the output of the `print-jass-environment.fin` finish script. This allows better display of all of the variables used by the Toolkit, along with their respective values.

The symbolic links used in the `set-system-umask.fin` finish script were changed to hard links.

All of the finish scripts have been reviewed and their code improved in an effort to remove code redundancy. This is an ongoing effort and will take place with each update of the Toolkit.

Support was added to optionally prevent "kill" scripts from being disabled (in the `disable-*.fin` scripts). The default policy is to disable these kill scripts. This option allows kill scripts to remain on the system to stop services that may have been manually started. This option is controlled by the `JASS_KILL_SCRIPT_DISABLE` environment variable. By default, it is set to `1` in the `finish.init` script. If kill scripts should not be disabled, then the defined value should be changed to `0` in the `finish.init` script.

New File Templates

The file, `/etc/default/sendmail`, from the *Solaris™ Operating Environment Security - Updated for Solaris 8 Operating Environment* (April 2001) Sun BluePrints Online article was added to the `Files/` directory tree. This file will only be installed by the Toolkit on Solaris 8 OE systems. The file instructs `sendmail` to operate in queue processing mode only. The original method, from Toolkit version 0.2, still applies for Solaris OE versions 2.5.1, 2.6, and 7.

Added in this release are the `/etc/security/audit_*` files from the *Auditing in the Solaris™ Operating Environment* (February 2001) Sun BluePrint Online article. These files will only be installed by the Toolkit on Solaris 8 OE systems.

Both of these Sun BluePrints OnLine articles are included in the `Documentation` directory of the Toolkit.

Miscellaneous Changes

A variety of miscellaneous changes were made to the Toolkit which do not fit into any of the previous categories. These modifications include:

Changes to system files during a Toolkit run are now logged more completely to the `JASS_MANIFEST` file. Additional changes now logged include creation of intermediate directories, permission and ownership modifications, and the generation of checksums for each modified file.

Files and directories specified through symbolic links are handled more completely.

The processing and display of extraneous leading slashes in absolute paths have been cleaned up to promote better presentation.

A bug was fixed relating to processing of user variables, as the Toolkit was behaving differently between JumpStart client and standalone installations. Now user specified variables and code, from `user.init` and `user.run`, are processed properly in both modes.

The helper application, `add-client`, no longer depends on the Toolkit being installed in the directory `/jumpstart`. A list of available JumpStart server IP addresses will now be provided if not specified. The code was reviewed and revised where necessary, in order to provide clarity and documentation.

The default `le0` entry in the `sysidcfg` files distributed with Toolkit version 0.2 for Solaris 2.6, 7, and 8 OE was changed to `primary` for increased hardware portability.

Note – The `sysidcfg` files for Solaris 2.5.1 OE must still be reviewed and changed to an appropriate value.

A bug was fixed involving host-specific `JASS_FILES` when in standalone mode.

A new variable, `JASS_HOSTNAME,` was created, and the `driver.init` and `driver.run` scripts were updated to utilize it.

Conclusion

This article presents a description of the modifications included in Toolkit version 0.3. These enhancements and modifications are presented so that administrators using Toolkit version 0.3 will be aware of new enhancements, while users new to the Toolkit get an overview of the latest enhancements.

Additional details on each of the enhancements can be found in *The Solaris™ Security Toolkit - Installation, Configuration, and Usage Guide: Updated for Toolkit version 0.3* or *The Solaris™ Security Toolkit - Internals: Updated for Toolkit version 0.3* Sun BluePrints OnLine articles released with Toolkit version 0.3.

Bibliography

Noordergraaf, Alex and Brunette, Glenn, *The Solaris™ Security Toolkit - Internals: Updated for Toolkit version 0.3*, Sun BluePrints OnLine, June 2001,
`http://www.sun.com/blueprints/0601/jass_internals-v03.pdf`

Noordergraaf, Alex and Brunette, Glenn, *The Solaris™ Security Toolkit - Quick Start: Updated for version 0.3*, Sun BluePrints OnLine, June 2001,
`http://www.sun.com/blueprints/0601/jass_quick_start-v03.pdf`

Noordergraaf, Alex and Brunette, Glenn, *The Solaris™ Security Toolkit - Installation, Configuration, and Usage Guide: updated for Toolkit version 0.3*, Sun BluePrints OnLine, June 2001,
`http://www.sun.com/blueprints/0601/jass_conf_install-v03.pdf`

Author's Bio: Alex Noordergraaf

Alex Noordergraaf has more than nine years experience in the area of Computer and Network Security. As a Senior Security Architect in the Enterprise Engineering group of Sun Microsystems, he is developing, documenting, and publishing security best practices through the Sun BluePrints OnLine program. Articles completed include recommendations on Solaris OE Security settings, Solaris OE Minimization, and Solaris OE Network settings.

Prior to his role in Enterprise Engineering, he was a Senior Security Architect with Sun Professional Services, where he worked with many Fortune 500 companies on projects that included Security Assessments, Architecture Development, Architectural Reviews, and Policy/Procedure review and development. In addition to providing billable services to customers, he developed and delivered an Enterprise Security Assessment methodology and training curriculum to be used worldwide by the Sun Professional Services™ organization. *His customers have included major telecommunication firms, financial institutions, ISPs, and ASPs.*

Author's Bio: Glenn Brunette

Glenn Brunette has more than eight years experience in the areas of computer and network security. Glenn currently works in the Sun Professional Services organization, where he is the Lead Security Architect for the Northeastern USA region. In this role, he works with many Fortune 500 companies to deliver tailored security solutions such as assessments, architecture design and implementation, as well as policy and procedure review and development. His customers have included major financial institutions, ISPs, New Media, and government organizations.

In addition to billable services, Glenn works with the Sun Professional Services Global Security Practice and Enterprise Engineering group on the development and review of new security methodologies, best practices, and tools.