The Solaris™ Security Toolkit - Quick Start

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.: 816-1468-10
Revision 01, 05/31/01
Edition: June 2001

Please
Recycle

The Solaris™ Security Toolkit - Quick Start

Updated for Toolkit version 0.3

Overview

This Sun BluePrints™ OnLine article is for those individuals wanting to get started with the Solaris™ Security Toolkit as quickly as possible. Only the bare essentials in getting the Toolkit downloaded and installed will be addressed. Downloading and installation instructions for the `tar` and package format Toolkit distributions, in addition to a section discussing standalone and JumpStart™ modes, are also included.

Much of the material in this article has been summarized from the more in-depth coverage in the *The Solaris Security Toolkit - Installation, Configuration, and Usage Guide: Updated for Toolkit version 0.3* and *The Solaris Security Toolkit - Internals: Updated for Toolkit version 0.3* Sun BluePrints OnLine articles. Refer to the Bibliography or the Toolkit `Documentation` directory for the appropriate PDF files.

Installation

With the release of Toolkit version 0.3, the source is being distributed in Solaris™ Operating Environment (Solaris OE) package format, in addition to the traditional compressed `tar` archive. The same source is included in both archives. When downloading the Toolkit, be sure to always select the most recent version. Downloading and installing these two different archive types are discussed separately:

Compressed Tar Archive

These instructions use filenames which only apply to version 0.3 of the Toolkit. Use the following procedure to download and install the Toolkit:

1. **Download the source file** (jass-0.3.tar.Z)**.**

   The source file is located at:

   http://www.sun.com/blueprints/tools/license.html

2. **Extract the source file into a directory on the server using the** zcat **and** tar **commands as shown**:

```
# zcat jass-0.3.tar.Z | tar -xvf -
```

   Executing this command creates the subdirectory, jass-0.3, in the current working directory. This subdirectory will contain all the Toolkit directories and associated files.

   Throughout the rest of this document, the $JASS_HOME_DIR environment variable will be used to refer to the root directory of the Toolkit. When the Toolkit is installed from the tar archive, $JASS_HOME_DIR is defined to be the path up to, and including, jass-0.3. If the previous command is issued in the /opt directory, the $JASS_HOME_DIR environment variable would be defined as /opt/jass-0.3.

Package Format

The instructions included use filenames which are only correct for this release of the Toolkit. Use the following procedure to download and install the Toolkit:

1. **Download the source file** (SUNWjass-0.3.pkg).

   The source file is located at:

   http://www.sun.com/blueprints/tools/license.html

2. **Extract the source file into a directory on the server**.

   Use the pkgadd command as shown:

```
# pkgadd -d SUNWjass-0.3.pkg SUNWjass
```

Executing this command creates the SUNWjass directory in /opt. This subdirectory will contain all the Toolkit directories and associated files. The script make-pkg, included in version 0.3 of the Toolkit administrators can create custom packages using a different installation directory. After installation of the Toolkit, $JASS_HOME_DIR is defined to be /opt/SUNWjass.

Configuration and Usage

Standalone Mode

When using standalone mode, the Toolkit can be run directly from the $JASS_HOME_DIR directory by executing the following command:

```
# ./jass-execute -d secure.driver
```

Please note that this will execute all of the hardening scripts included in secure.driver. This may not be appropriate for all environments. Evaluate what security modifications are required before executing the Toolkit.

The secure.driver script will disable all remote access capabilities, such as TELNET, FTP, and RLOGIN. Do not reboot the system without at least one of those services being enabled, having serial or console access to the system, or having an alternate remote access mechanism installed, such as Secure Shell.

None of the other configuration steps required for jumpstart mode are require for standalone mode. The standalone Toolkit mode is one of the best options to harden a system as quickly as possible.

Additional information on the secure.driver, and other drivers in the Toolkit, can be found in the *The Solaris Security Toolkit - Internals: Updated for Toolkit version 0.3* Sun BluePrints OnLine article.

Note – A Toolkit standalone run, on a pre-existing system, should only be performed after the machine has been rebooted and backed up to verify that it is in a known and consistent configuration.

JumpStart Mode

Readers interested in, but not familiar with, JumpStart technology are referred to the Sun BluePrint OnLine article titled *Building JumpStart™ Architectures* for detailed instructions on how to set up a JumpStart server and environment. Refer to the Bibliography or the Toolkit `Documentation` directory for the appropriate PDF files.

For use in a JumpStart environment, the Toolkit source in `$JASS_HOME_DIR` should be copied into the base directory of the JumpStart server. Frequently, this is `/jumpstart` on the JumpStart server. Once this is done, `$JASS_HOME_DIR` should become the base directory of the JumpStart server.

This section assumes that the reader is familiar with JumpStart technology and already has an existing JumpStart environment available. If these assumptions are not correct, refer to the *Building JumpStart Architectures* Sun BluePrints OnLine article.

Only a few steps are required to integrate the Toolkit into a JumpStart architecture.

First, the Toolkit source must be copied into the root directory of the JumpStart server. For example, if the Toolkit archive was extracted to `/opt/jass-0.3`, and the JumpStart server root directory is `/jumpstart,` the following command would copy the Toolkit source:

```
# pwd
/opt/jass-0.3
# cp -r * /jumpstart
```

The second step is to copy the `$JASS_HOME_DIR/Drivers/user.init.SAMPLE` to `$JASS_HOME_DIR/Drivers/user.init`. This can be done with the following command:

```
# pwd
/jumpstart/Drivers
# cp user.init.SAMPLE user.init
```

Now that a `user.init` file is available, the two entries for `JASS_PACKAGE_MOUNT` and `JASS_PATCH_MOUNT` must be changed to the IP address of the JumpStart server.

Note – These IP addresses will be used by the JumpStart client to NFS mount the Toolkit directories during the JumpStart installation process.

Failure to modify these two IP addresses will result in an error similar to the following:

```
NOTICE: Mounting 192.168.11.33:/jumpstart/Packages on /a//tmp/jass-packages.
nfs mount: 192.168.11.33:/jumpstart/Packages: No such file or directory
NOTICE: Mounting 192.168.11.33:/jumpstart/Patches on /a//tmp/jass-patches.
nfs mount: 192.168.11.33:/jumpstart/Patches: No such file or directory
```

Once these modifications have been made, a Toolkit driver should be either selected (i.e., the Toolkit default: `Drivers/secure.driver`) or created, and then added to the JumpStart servers `rules` file for the host to be secured. If all the scripts listed in the `hardening.driver` and `config.driver` are to be used, then the `Drivers/secure.driver` should be added to the `rules` file. Otherwise, copies of these files should be made, modified, and then the appropriate entry made in the `rules` file.

Note – Modifications should never be made to the scripts included with the Toolkit, as this will make migrating to a new release of the Toolkit much more difficult.

One other modification may be required to successfully integrate the Toolkit into the existing JumpStart environment. If the `sysidcfg` files provided with the Toolkit are to be used to automate the JumpStart client installation, they should be reviewed for correctness. If the JumpStart server encounters any errors while parsing the `sysidcfg` file, the entire contents of the file will be ignored.

At this point, if all the other JumpStart server specific steps have been performed, it should be possible to jumpstart the client and successfully harden or minimize the OS during the installation process.

Undo

One of the most significant enhancements available in version 0.3 of the Toolkit is the capability to undo a Toolkit installation or series of installations. This feature has been added to provide administrators with an automated mechanism by which a system can be returned to its state prior to the Toolkit's execution.

The undo feature is only available through the `jass-execute` command in `$JASS_HOME_DIR`. It can not be used during a JumpStart installation, nor can it be used if the creation of backup file copies has been disabled by setting `$JASS_SAVE_BACKUP` to `0`. To undo a specific Toolkit run, or series of Toolkit runs, the following command would be used from $JASS_HOME_DIR:

```
# ./jass-execute -u
```

On a system where several Toolkit runs have been performed, output similar to the following will be displayed:

```
./jass-execute: NOTICE: Executing driver, undo.driver
Please select a JASS run to restore through:
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)
Choice?
```

The administrator can select one of these runs as the final run to be un-done. All system modifications performed in that selected run, and any runs made after that, will be undone. There are two important limitations to keep in mind with this feature. First, if the Toolkit option to not create backup files is selected, either through jumpstart or standalone modes, the undo feature will not be available. Secondly, a run can only be undone once. Once it is undone, all the files backed up by a Toolkit run are restored to their original locations and are not backed up again.

The Toolkit information needed for the undo feature is logged under the `/var/opt/SUNWjass` directory hierarchy. The package name, `SUNWjass`, is the official Sun package name of the Toolkit. In this directory, there is a `runs` directory. For each Toolkit run, a new sub-directory in the `/var/opt/SUNWjass/runs` directory is created. This directory stores the necessary log information for the Toolkit.

Note – The contents of the files in the `/var/opt/SUNWjass/runs` directory should never be modified by an administrator.

When a Toolkit run is undone, the associated `/var/opt/SUNWjass/runs` directory is not removed. Instead, a new file is created in the directory indicating that it has been undone, and correspondingly will not be listed the next time `jass-execute -u` is executed.

Note – A Toolkit undo run should only be performed, as with a Toolkit hardening run, after the machine has been rebooted and backed up.

Frequently Asked Questions

This section discusses some of the questions frequently asked of the Toolkit development team.

What Is The Root Password Set To?

When the Toolkit is run using the `secure.driver` driver, the `set-root-passwd.fin` script is run. This script sets the root password to be `t00lk1t`.

Does the Undo Feature Undo All Changes?

Generally speaking the undo feature can undo all modifications which didn't involve running a script. Of the 70+ scripts in the Toolkit only a handful execute scripts. Specifically - those Toolkit finish scripts which call other scripts are: `enable-bsm.fin`, `install-fix-modes.fin`, `install-jass.fin`, `install-openssh.fin`, `install-recommended-patches.fin`, and `install-strong-permissions.fin`. These finish scripts cannot be undone by the Toolkit undo feature.

JumpStart Installations Not In $SI_CONFIG_DIR?

Typically, the Toolkit is installed in the `$SI_CONFIG_DIR` of the JumpStart server. Once installed, the `$JASS_HOME_DIR` environment variable will automatically be set correctly.

If the Toolkit is installed under a subdirectory of `$SI_CONFIG_DIR`, such as `$SI_CONFIG_DIR/path/to/JASS`, then the following should be added to the `$JASS_HOME_DIR/Drivers/user.init` file:

```
if [ -z "${JASS_HOME_DIR}" ]; then
    if [ "${JASS_STANDALONE}" = 0 ]; then
        JASS_HOME_DIR="${SI_CONFIG_DIR}/path/to/JASS"
    fi
fi
export JASS_HOME_DIR
```

The appropriate Toolkit driver can then be added to either the rules file or existing JumpStart server finish scripts.

Remember to also define `$JASS_HOME_DIR` in the `user.init` file if the Toolkit code is not located in `$SI_CONFIG_DIR`.

Is The Toolkit Supported By Sun?

No. The Toolkit itself is not something about which a Service Order call can be made to Sun's Resolution Center. However, the configuration resulting from the Toolkit is supported. So, if a security feature enabled by the Toolkit is not behaving as advertised, a Service Order can and should be opened.

There are, however, unofficial support mechanisms for the Toolkit. Refer to *The Solaris Security Toolkit - Configuration, Installation, and Usage Guide: Updated for Toolkit version 0.3* Sun BluePrints OnLine article section titled *Support Forums* for details.

Why Is The `primary` Keyword, In The `syidcfg`, Being Ignored While Jumpstarting Solaris 2.6 OE?

In order to successfully automate a JumpStart installation of Solaris 2.6 OE, patch `106193-05` or later must be applied to the Solaris 2.6 OE image on the JumpStart server. The Solaris OE image, on the JumpStart server, can be patched with the `patchadd -C` command. Refer to the `patchadd(1m)` man page for additional information.

Conclusion

This article provides the administrator with the minimal information required on how to find, download, and use the Toolkit to harden Solaris OE systems. To facilitate that, this article discussed the different packaging solutions for the Toolkit, where to download them from, how they are installed, and what must be done to run them in either standalone or jumpstart modes. Additionally, the new version 0.3 undo feature is discussed, as are support options and some frequently asked questions.

Bibliography

Noordergraaf, Alex, *Building a JumpStart™ Infrastructure*, Sun BluePrints OnLine, April 2001,
`http://www.sun.com/blueprints/0401/BuildInf.pdf`

Noordergraaf, Alex and Brunette, Glenn, *The Solaris™ Security Toolkit - Configuration, Installation, 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`

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`

Author's Bio: Alex Noordergraaf

Alex Noordergraaf has more than 9 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: Solaris OE Minimization for Security, Solaris OE Network Settings, and Solaris OE Security.

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 8 years experience in the areas of computer and network security. Glenn currently works with in the Sun Professional Services organization where he is the Lead Security Architect for the North Eastern 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, ISP, 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.