Safeguarding the XT3

Katherine Vargo, *Pittsburgh Supercomputing Center*

ABSTRACT: *Service nodes and the management server provide critical services for the XT3 and its users. Using open-source software, these critical services can be monitored and safeguarded from common Linux attacks. Patch management, configuration verification, integrity checking, and benchmarking software provide a solid foundation for insulating services from assaults and enable system administrators to increase system availability and reliability.*

KEYWORDS: *XT3, security*

1. Introduction

Patch management, configuration verification, integrity checking, and benchmarking software provide a solid foundation for insulating services from assaults and enable system administrators to increase system availability and reliability. By obtaining a system baseline and continually monitoring system configuration changes, system administrators can safeguard the XT3 from common Linux attacks.

The assessment and monitoring tools used in this paper were installed on the management server and service nodes running version 1.4a17 and 1.4a20.

2. System Assessment

A solid baseline measure of a system is necessary before system administrators can implement system security changes. A baseline measurement of systems is easily obtainable using benchmark software to score the configuration and patch management software to identify out of date programs.

2.1 Benchmarks

Benchmarks are used across industries to set standards and compare functions and results. Computer configuration benchmarks help to compare operating system distributions and configurations. Bastille is a standard Linux benchmark to measure the security of an operating system and its configuration.

Bastille

Bastille, a tool included with most Linux distributions, provides a mechanism for reporting as well as modifying a system's current state of hardening and configuration. Version 2.1.1-32.11 of Bastille was included with the 1.4 distributions. The test results published in this paper were obtained using an updated version of Bastille, version 3.0.8-1.0.

Bastille's has assessment report provides an initial snapshot and score of the machine configuration. To generate a report with Bastille, use the assess option.

Bastille Hardening Assessment Report is generated in three formats: html, text, and machine-parse able text. The html report provides details about the tests that were performed, the weight of the test in the report, and the score of the configuration setting. The report provides a baseline for the initial configuration of the machine and an overall score.

To install a newer version of Bastille on the service nodes, you will need to use xtopview. In addition to installing the rpm, it is necessary to touch /usr/share/Bastille/.nodisclaimer. This is necessary because the file systems are read-only and it is not possible to accept the license agreement when Bastille is initially run. This is not an issue for the SMW because it has a writable file system.

Systems	Score
SMW	6.98 / 10.0
Boot	7.36 / 10.0
Login	7.17 / 10.0
SDB	7.17 / 10.0

Table 1: Service Node and SMW Score Card.

Generally, the systems rated high for disabling miscellaneous daemons such as snmpd and kudzu. Other unnecessary daemons, such as web and ftp services, were turned off by default as well. DNS and printing services are turned off by default too.

Table 2: Comparison of the SMW/Boot/SDB Scores.

System (Score)	DHCP Enabled	GRUB Passwd	Additional Logging
SMW (6.98)	Y	N	N
SDB/Login (7.17)	N	Y	N
Boot (7.36)	N	Y	Y

The systems are fairly compatible. The services node and SMW differ only by 0.19 points. The first difference between the SMW and service nodes is the enabling of DHCP. The SMW uses DHCP to boot the nodes and must remain enabled. The second difference between the SMW and service nodes is the grub password. The service nodes have no menu.lst file while the SMW has a menu.lst file without a password lock. There is only one difference between the boot node and services nodes; it accounts for the 0.19 point difference. The boot node has additional logging using local2-6 facilities.

Once you have reviewed the Bastille Hardening Assessment Report, you can use Bastille in interactive mode to make the changes to the system configuration. It is also possible to specify a configuration file for unattended installations. Bastille also has an 'undo' option in case you need to revert to the previous configuration.

Other configuration changes to consider include disabling r-tools, disabling root login on ttys1-5, disabling SUID status of Xwrapper, and enabling LAUS (Linux Audit-subsystem user space tools).

2.2 Patch Management

The next step in assessing the system baseline configuration is to determine the patch level for the machine. To get a list of available patches for SuSE Linux Enterprise Server, obtain a 60 day evaluation from Novell. This will enable access to patches and updates if you don't currently have a license.

Fou4s:

Due to the quantity of patches and updates released in a given period, it can be difficult to assess the patch level of the machine. Fou4s, a patch management software package, provides excellent reporting on the available patches not installed on the XT3.

Fou4s, Fast Online Update for SuSE, is designed for automatic updates via cron jobs as well providing full descriptions and comparisons of installed packages and patches.

The summary report provides a snapshot of the system and quick reference to what updates are required. In addition, fou4s provides detailed information about all required patches.

In the example below, there are a total of 198 updates including 19 security updates that are required to ensure the system is patched and up-to-date.

```
Update statistics for SUSE-CORE 9  (fou4s 0.13.1):
                                Size        After Upd.   To D/L
198 update(s), total        263018kB   +90036kB 263018kB
19 security update(s)  110725kB   +78575kB 110725kB
175 recommended update(s) 151660kB +16268kB
        151660kB
1 optional update(s)       633kB       0kB      633kB
 3 script(s)                  0kB       0kB       0kB
```

In addition to the total number of updates to download, there is information about each specific program update. In the quota example listed below, the latest patch version is 3.11-22.14 but 3.11-22.10 is the version installed on the machine. The updated version of quota includes a recommended patch that provides support for reiserfs mounted by label.

```
 Update Information for patch-10628 (2005-11-17)

 Recommended update for quota
  Applies to Package: quota Product(s):
    SUSE CORE 9 for x86
    SUSE CORE 9 for Itanium Processor Family
    SUSE CORE 9 for IBM POWER
    SUSE CORE 9 for IBM S/390 31bit
    SUSE CORE 9 for IBM zSeries 64bit
    SUSE CORE 9 for AMD64 and Intel EM64T
    Open Enterprise Server
    Novell Linux Desktop 9 for x86
    Novell Linux Desktop 9 for x86_64
  Patch: patch-10628
  Release: 20051205 Obsoletes: none
  Indications:  Everyone using quota on should update.
```

Contraindications: None.
Problem description: Adds support for reiserfs mounted by label.
Solution: Please install the updates provided at the location noted below.
Installation notes: This update is provided as an RPM package that can easily be installed onto a running system by using this command:
rpm -Fvh quota.rpm
==========
quota 3.11-22.14 (3.11-22.10) [dl] recommended 171kb

The reporting feature of fou4s provides a fast and convenient assessment of the system patches.

SPident

Another package for assessing the state of patches on the system is SPident. It is a SuSE supplied package that compares the packages currently installed on the system with a database of Support Pack packages; it is included with Support Pack updates.

The verbosity of Spident output is increased with additional –v flags.

_SPident -v gives a summary table showing whether or not there are any conflicts or updates.

SPident -vv gives the individual file names of conflicting packages. ***Note:*** *Conflicting packages arise when a newer version was expected but was never installed. This is indicated by a minus symbol (-) in front of the package name.*

SPident -vvv gives the individual file name of any updated packages. ***Note:*** *Updated packages arise when the installed version of a package is newer then the expected version. This is indicated by a plus symbol (+) in front of the package name*

The SPident output listed below details the percentage of packages in conflict with the original packages of Support Packs. SLES-9-SP2 has 1 conflict.

$ SPident -v
Summary (using 487 packages)
Product / Support PackSupport Pack conflict match update (shipped)
SLES_9_i386 0 0% 253 52.0% 8 (1486 17.0%)
SLES_9_i386_SP1 0 0% 77 15.8% 5 (481 16.0%)
SLES_9_i386_SP2 1 0.2% 224 46.0% 5 (647 34.6%)
Unknown 9 1.8%
CONCLUSION: System is NOT up_to_date!
found SLES_9_i386_SP1 + "online updates"
expected SLES_9_i386_SP2

Running SPident with additional verbosity, provides details about the package requiring an update. Once the conflicting package is updated and there are no conflicts, the system is considered up-to-date.

$ SPident -vv
Summary (using 487 packages)
Product / Service Pack conflict match update (shipped)
SLES_9_i386 0 0% 253 52.0% 9 (1486 17.0%)
SLES_9_i386_SP1 0 0% 76 15.6% 5 (481 15.8%)
SLES_9_i386_SP2 0 0% 224 46.0% 6 (647 34.6%)
Unknown 10 2.1%
CONCLUSION: System is up_to_date!
found SLES_9_i386_SP2 + "online updates"

The output for a XT3 1.4 system is shown below. It reports several packages out of date even though the version numbers are greater then expected. This is due to Cray customizing some programs and using their own numbering system when repackaging them. For example, the sudo package was modified to allow the /etc/sudoers file to be a symlink. Because the packages are not standard numbers, SPident considers it out of date.

Summary (using 901 packages)
Product/ServicePack conflict match update (shipped)
SLES-9-x86_64 5 0.3% 506 56.2% 62 (1597 31.7%)
- glib 2.4.2-8 < 1.2.10-586.1
- perl-DBD-mysql 2.9003-22.1.S9 < 2.9003-22.1
- perl-DBI 1.41-28.4.S9 < 1.41-28.1
- python-mysql 0.9.3b2-1 < 0.9.3b2-90.1
- sudo 1.6.8p11-4 < 1.6.7p5-117.1
SLES-9-x86_64-SP1 1 0.2% 112 12.4% 34 (524 21.4%)
- glib 2.4.2-8 < 1.2.10-586.2
SLES-9-x86_64-SP2 3 0.4% 311 34.5% 46 (700 44.4%)
- glib 2.4.2-8 < 1.2.10-586.2
- perl-DBI 1.41-28.4.S9 < 1.41-28.4
- sudo 1.6.8p11-4 < 1.6.7p5-117.4

SPident provides an assessment of the service nodes and SMW software in comparison to Support Pack packages.

3. System Inspection and Monitoring

After assessing the machine and modifying the system to adhere to the site's security policy, it is necessary to monitor the system to ensure it remains in compliance.

3.1 Monitoring System Configuration

Seccheck

Seccheck, SuSE Security Checker, provides security analysis on a daily, weekly, and monthly basis. It is standard on SuSE distributions and provides email reports of the system.

Daily seccheck tests examine user home directories, user accounting files, and file system export settings. The /etc/passwd, /etc/shadow, and /etc/group files are examined for accounting irregularities. The /etc/aliases file is checked for program executables listed as mail aliases. Home directories are examined to ensure proper permissions. NFS configuration is checked for global exports and suid options. The daily reports include the differences between the previous day report.

Weekly checks include file system modifications and configuration. Suid and sgid files are reported. Files that group and world writable are reported as well. The report includes a listing of all devices. Modified files in rpm packages are reported via the rpm md5 mechanism. The weekly reports include the differences from the previous week report.

Additional information about the rpm md5 check is available from the man page for rpm. In this example, configuration files have been modified.

```
S.5....T c /etc/printcap
..5..... c /etc/securetty

 S - file size differs
 5 - checksum differs
 T - last modified time changed
 c - config file
```

The monthly report is a full report of the daily and weekly tests. It does not contain any differences from the last monthly report.

Additional configuration steps are needed to receive the seccheck reports on XT3 systems. Mail must be enabled on the boot node and SMW. In addition, cron must be enabled for SIO nodes. By default, the boot node and SMW have seccheck enabled. To enable seccheck for other SIO nodes, use xtopview to modify /etc/sysconfig/seccheck and set START_SECCHK='yes'.

3.2 Integrity Checking

SuSE has several integrity checking packages installed by default. The default tripwire package installed on the XT3 is out of date and doesn't execute due to segmentation faults.

Aide (Advanced Intrusion Detection Environment) is another integrity checking package installed by default on SuSE installations. Aide creates a database from the regular expression rules that it finds from the config file. Aide version 0.9-194, which is installed by default on the system, exits with a segmentation fault. Remove version 0.9 and install version 0.11 of aide to remove the segmentation errors.

On the boot node, modify /usr/local/etc/aide.conf to monitor the /rr/current tree. It is not necessary to run it on the SIO nodes themselves. Monitoring the /rr/current tree provides notification of any of the SIO nodes in one report.

The aide package was functional but slow. Other integrity checking programs include commercially available Tripwire and freely available Samhain. These systems provide centralized monitoring and faster reporting.

4. Conclusion

By obtaining a system baseline and continually monitoring system configuration changes, system administrators can safeguard the XT3 from common Linux attacks. Patch management, configuration verification, integrity checking, and benchmarking software provide a solid foundation for insulating services from assaults and enable system administrators to increase system availability and reliability.

Acknowledgments:

This material is based upon work supported by the National Science Foundation under Cooperative Agreement No. SCI-0456541.

About the Author

Katherine Vargo is the Manager of Scientific Computing Systems at the Pittsburgh Supercomputing Center. The Scientific Computing Systems group administers the high performance computing systems and ensures availability of computing services for the scientific community at PSC. Before becoming Manager of Scientific Computing Systems at PSC, Katherine administered several Top 500 machines, including LeMieux which premiered at number two in November 2001. She received her Master's degree in Information System from The University of Pittsburgh. Katherine can be reached at the Pittsburgh Supercomputing Center, 300 South Craig Street, Pittsburgh, PA 15212 USA, Phone: 412-268-1596 E-mail: katie@psc.edu.