Safeguarding the XT3

Katherine Vargo

Pittsburgh Supercomputing Center

katie@psc.edu

"The boss is worried about information security, so he sends his messages one alphabet letter at a time in random sequence.'

Tools for System Assessment and Inspection

Assessment:

- Benchmarks
- Patch Management

Inspection:

- Monitoring System Configuration
- Integrity Checking

Safeguarding the XT3

- Systems covered:
  - Management server
  - Service nodes

- OS Versions:
  - 1.4a17 and 1.4a20

Tools for System Assessment and Inspection

Assessment:

- Benchmarks
- Patch Management

Inspection:

- Monitoring System Configuration
- Integrity Checking

Benchmark tools - Bastille

- Assess a system's current state of hardening, granularly reporting on each of the security settings with which it works.
- Remove bastille-2.1.1-32.11 and install Bastille-3.0.8-1.0
- Generate an assessment report with

```
# bastille --assessnobrowser
```

Bastille

==== Bastille Hardening Assessment Completed ====

You can find a report in HTML format at:
file:///var/log/Bastille/Assessment/assessment-report.html

You can find a report in text format at:
/var/log/Bastille/Assessment/assessment-report.txt

You can find a more machine-parseable report at:
/var/log/Bastille/Assessment/assessment-log.txt

Assessment Report

Bastille Hardening Assessment Report

Score	Weights File
6.98 / 10.00	Bastille Default Weights

Contract all Modules | Expand all Modules

(*contract*)FilePermissions

Item	Question	State	Weight	Score Contrib
generalperms_1_1	Are more restrictive permissions on the administration utilities set?	No	0	0.00
suidmount	Is SUID status for mount/umount disabled?	No	1	0.00
suidping	Is SUID status for ping disabled?	No	1	0.00
suiddump	Is SUID status for dump and restore disabled?	Yes	1	1.00
suidcard	Is SUID status for cardctl disabled?	Yes	1	1.00
suidat	Is SUID status for at disabled?	No	1	0.00

Bastille

Baseline scoring

- SMW 6.98/10.00
- Boot node 7.36/100
- Login 7.17/10.00
- SDB 7.17/10.00

Installation on SIO nodes.

- Use Xtopview to touch /usr/share/Bastille/.nodisclaimer after installation of rpm

Bastille

Differences between SWM/boot/login scores:

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

Running Bastille

- 'bastille -c' to start the tool using the text interface implemented via Perl/Curses
- Bastille has an ‘undo’ option.
- Things to consider:
  - SUID status for Xwrapper
  - disallow root login on tty's 1-6
  - Enable LAUS (Linux Audit-Subsystem User Space Tools)
  - Disable r-tools, rsh etc

Tools for System Assessment and Inspection

Assessment:

- Benchmarks
- Patch Management

Inspection:

- Monitoring System Configuration
- Integrity Checking

Patch Management

Software:

- Fou4s
- SPident

Issues:

- License for updates
- 60 day evaluation

Patch Management - Fou4s

- fou4s - Fast Online Update for SuSE

- Designed for usage in cron jobs
- Provides full description and comparison of installed packages and updates

Fou4s

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

Fou4s - example

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.

Fou4s - example

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

Patch Management -SPident

- **SPident** compares the packages currently on the system with a database of which packages belong to each Service Pack.
- Package is included with Service Packs

SPident


```
$ SPident -v
Summary          (using 487 packages)
Product / Service 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
```

SPident


```
$ 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"
```

Spident - example

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

Tools for System Assessment and Inspection

Assessment:

- Benchmarks
- Patch Management

Inspection:

- Monitoring System Configuration
- Integrity Checking

Monitoring System Configuration

- Seccheck - SuSE Security Checker
- Security analysis on a daily, weekly and monthly basis.

Seccheck

- Emailed reports
- Daily - lists differences from last report
  - Bound Processes
  - empty passwd field
  - .rhost/.shost files
  - ownership of home directories
  - loaded kernel modules

Daily Seccheck

Changes (+: new entries, -: removed entries):

+ pbs_serve root UDP 128.199.99.999:47707

+ sshd root UDP 128.199.99.999:47705

+ sshd root UDP 128.199.99.999:47706

Seccheck

- Weekly - lists differences from last report
  - unused accounts
  - executables are group/world writeable
  - program md5 checksum
  - local passwd security

Seccheck Weekly

- Warning: user wu2738 has got a password and a valid shell but never logged in.

Seccheck Monthly

- Monthly - full report
  - Bound sockets,
  - changed rpm files,
  - world writable files

Seccheck Monthly

- Checking the /etc/shadow file:

  Login wna7654 has an unusual password

  field length

- The following loadable kernel modules are currently installed:

  Module

  E1000

  qla2300

Seccheck

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

Seccheck setup

- Enable mail on boot and SMW nodes
- Enable cron for other SIO nodes
- Enable seccheck for other SIO nodes, sdb, etc.

Edit /etc/sysconfig/seccheck via xtopview and set START_SECCHK="yes"

Tools for System Assessment and Inspection

Assessment:

- Benchmarks
- Patch Management

Inspection:

- Monitoring System Configuration
- Integrity Checking

Integrity Checking

- AIDE (Advanced Intrusion Detection Environment)
- Creates a database from the regular expression rules that it finds from the config file.
- Once this database is initialized it can be used to verify the integrity of the files.

Aide setup

- Remove old version: aide-0.9-194 installed in /usr/bin/aide and uses /etc/aide.conf due to segmentation errors.
- Monitoring /rr/current tree for SIO nodes
- Install mhash and aide version 0.11

Better IDS systems

- Samhain and Prelude

  http://la-samhna.de/samhain/index.html

  http://prelude-ids.org/
- Tripwire

  http://www.tripwire.com

Tools for System Assessment and Inspection

Assessment:

- Benchmarks
- Patch Management

Inspection:

- Monitoring System Configuration
- Integrity Checking

Questions?