PETER BAER GALVIN

Pete's all things Sun (PATS): the security sheriff

Peter Baer Galvin (www.galvin.info) is the Chief Technologist for Corporate Technologies, a premier systems integrator and VAR (www.cptech.com). Before that, Peter was the systems manager for Brown University's Computer Science Department. He has written articles and columns for many publications and is coauthor of the *Operating Systems Concepts* and *Applied Operating Systems Concepts* textbooks. As a consultant and trainer, Peter teaches tutorials and gives talks on security and system administration worldwide.

pbg@cptech.com

SECURITY IS A CONSTANT, ONGOING activity for most system administrators. While installations, patches, problems (fire fighting), and upgrades are usually in the sysadmin foreground, security is that constant background companion, at least at many facilities. In fact, the best sysadmins have a mental checklist they execute before hitting the <return> key on the command line, or pressing the <apply> button in a GUI (which brings up the question of whether the best sysadmins use any GUIs, but let's leave that for another time). The mental checklist is:

Checklist #1: Use before making a change.

- Is the syntax of the command correct?
- Is the command the right one to make the change?
- Is there a better way to make the change?
- Are the right options entered or selected?
- Is today Friday?
- Is today some other day on which it would be exceptionally bad to break something (such as the day before leaving for a vacation or conference)?
- What are the chances that executing this will break something?
- If this change would break something, can I undo the action?
- Is this a documented way to accomplish the task?
- If this is a new way to make a change, should I document it?
- And finally, what effect might this action have on security?

Only after this mental checklist is run would this mythical best sysadmin execute the action. Of course the best sysadmins would modify this list to suit their circumstances, site policies, and abilities.

If you care about security, and you are a good sysadmin, then not only do you consider your actions in a security context but you keep an eye open for ways to improve security without increasing your workload—which brings us to this month's topic.

The CIS Solaris Benchmark

Now, since you are the mythological "best sysadmin" that I've been talking about, you are already

going through another mental checklist. This is the one you execute when a new tool is proposed to you:

Checklist #2: Use before trying a new tool.

- Do I already have a better tool?
- Is it multiplatform or one-off?
- Does it work, or just cause more work?
- Is it kept up-to-date?
- Does it change too often, causing more work?
- How much does it cost?
- Do I already know it or is it at least easy to learn?
- Is it likely to break or break something? (Go back to checklist #1.)

In the case of the Center for Internet Security (CIS) [1], the answers to these questions are all the right ones. CIS publishes "benchmarks" for many operating systems and applications. They are reasonably priced for many uses and easy to use, and I believe they are among the best security tools that you can apply to your environment.

CIS is a nonprofit organization, but it does need funds to support its various activities. Membership is one form of funding and well worth considering. Organizations such as CIS are doing their part to improve the overall security of computing infrastructure. Many people feel security is too lax in general, and that lax core security wastes time and money as security is monitored and breaches are detected and mitigated. Membership in CIS provides you or your organization with a chance to help improve the state of security—in other words, a way to stop complaining and start helping. The benchmark documents are only for noncommercial use, but commercial use licenses are available. The benchmark tool is currently available for trial use; full use requires membership.

Each benchmark is platform-specific. For this column I will stick to the Solaris 10 Benchmark, but there are many others. Each benchmark comes as a document describing recommended security steps, plus an appendix including variations and more advanced security steps that are not recommended for all sites or all circumstances. Many benchmarks also come with a tool that runs an audit of a given system and calculates a security score. The resulting score can be compared to the score of the same system from a previous run, to the scores of other systems, or to the theoretical best score.

The tool included with the benchmark is "read-only" in that it should not make changes to the system. Rather, the benchmark documents and tools recommend changes that should be considered for improving security. Sun has taken the unusual step of supporting the use of the Solaris CIS Benchmark, in that any changes it recommends are supported by Sun. You can call Sun support if you have questions or problems regarding any changes you made based on the benchmark recommendations. (Glenn Brunette, a security-centric Sun Distinguished Engineer, has a nice blog posting about all of this [2].)

First Steps

CIS has many benchmarks available. Navigate the site to find the ones you are interested in. Before you can download any of the CIS assets, you must agree to its license and also fill out a form about you and your organization.

For Solaris, there are several available files to chose from. For Solaris 10 11/06 and 8/07, the best starting place is CIS_Solaris_Benchmark_v4.0. Included is the benchmark document containing recommendations and an

appendix with an overview of Solaris 10 security controls. Carole Fennelly edited the document with input from many security experts, and it is an excellent Solaris 10 security resource. (Full disclosure: Carole and I have worked together on projects, and I was among the beta reviewers of this document.)

The 89-page document is one of the best security documents available. It includes many recommendations on how to improve the out-of-the-box security of Solaris 10. Even though Solaris 10 is initially fairly secure, there are many steps recommended to improve that security. For each recommendation there is information about what hardware platforms it pertains to, if it is the OS default, if the change applies to zones or just the global zone, and if the Solaris Security Toolkit can be used to make the change. Also included is information on how the recommendation affects the security score of the system, how to implement the recommendation, and any notes regarding the recommendation. This completeness of information helps both novice and advanced sysadmins decide whether to implement the recommendation and, if so, how to do so.

Another tool to run through your mental checklists is "The Solaris Security Toolkit" [3], a freely available and supported tool from Sun. This tool not only audits but also can implement configuration changes. Its execution and configuration can be scripted to allow groups of systems to be configured similarly and checked for differences from that security configuration. For another useful site see [4], where custom scripts built around the toolkit are collected together.

You can obtain the Solaris Security Toolkit 4.2 documentation from [5] (assuming you are one of the mythical sysadmins who read documentation before mucking around with a tool!). Another nice guide to the toolkit comes in the form of Sun blueprints [6].

The Benchmark Tool

On the Solaris page of CIS, there are several older tools designed for specific Solaris releases. These tools are not supported by CIS and tend to be out of date and buggy. Rather than use those, head to the CIS front page [1] and navigate to CIS-CAT. This tool is written in Java, and it parses an XML file containing the tests to run for a given platform. The ux-xml tarball that comes with the benchmark holds the XML files. Using the same tool and the appropriate XML file gives you the flexibility to run multiple tests on multiple systems from this starting point. At the time of this writing the tool benchmarks the following platforms:

- SuSE
- Slackware
- Red Hat Enterprise Linux
- Solaris 10
- AIX
- Oracle 9i/10g (for Windows)
- Oracle 9i/10g (for UNIX)
- Windows XP
- Windows Server 2003

For my testing I used Solaris Nevada x86 build 81 (running within a VMware virtual machine on top of Mac OS X Leopard). Use of the tool is very easy, and it is well documented by CIS. Start the tool with the provided shell script, use the "file" menu to load the appropriate XML file, and again use

the "file" menu to run the benchmark (Figure 1). A few minutes later (even in this virtualized environment) a report is generated showing the results of the run. The result is reported in XML and HTML. One feature not working in my testing was the "file->browse results" menu item in the benchmark tool. Rather, I manually viewed the results files in /SYS-CAT_Results/.

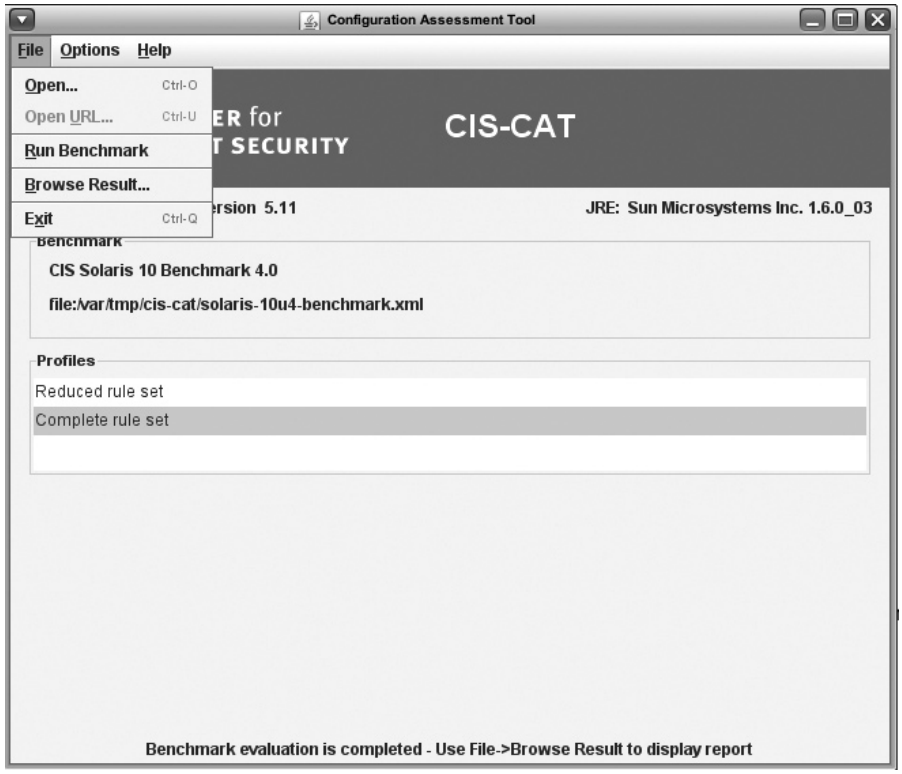

FIGURE 1: THE INITIAL SCREEN OF CIS-CAT

A tool is only as good as the usefulness of its results, and in the case of the CIS benchmark tool, the results are invaluable. Figure 2 shows the top of the report including summary information. Notice that on a generic current Solaris Nevada installation, the benchmark score is only 30%. Further down in the report are details on each test run, the results of the test, and a link to an explanation of the test, a link to the XML code that was executed, and recommendations to improve the security of the system based on the aspect tested (Figure 3). In essence, the report is a roadmap and how-to guide for improving security on a given system. Further, by being able to rerun the test and rescore the system, any changes made can be evaluated for their correctness and efficiency. This is a useful tool indeed.

Description	Items					Flat Model		
	P	F	E	U	i	Actual	Max	Score
1 Install Patches and Additional Software	0	0	0	0	2	0.0	0.0	0%
2 Restrict Services	10	12	0	0	13	10.0	22.0	45%
2.1 Establish a Secure Baseline	0	0	0	0	1	0.0	0.0	0%
2.2 Disable Unnecessary Local Services	1	6	0	0	0	1.0	7.0	14%
2.3 Disable Other Services	9	5	0	0	0	9.0	14.0	64%
2.4 Enable Required Services	0	0	0	0	12	0.0	0.0	0%
2.5 id-2.5g (untitled)	0	1	0	0	0	0.0	1.0	0%
3 Kernel Tuning	0	5	0	0	0	0.0	5.0	0%
4 Logging	1	8	0	0	0	1.0	9.0	11%
5 File/Directory Permissions/Access	3	5	0	0	0	3.0	8.0	38%
6 System Access, Authentication, and Authorization	2	10	0	0	1	2.0	12.0	17%
7 User Accounts and Environment	8	8	0	0	0	8.0	16.0	50%
8 Warning Banners	0	7	0	0	0	0.0	7.0	0%
9 Appendix A: File Backup Script	0	0	0	0	0	0.0	0.0	0%
10 Appendix B: Service Manifest for /var/svc/method/cis_netconfig.sh	0	0	0	0	0	0.0	0.0	0%
11 Appendix C: Additional Security Notes	0	0	0	0	6	0.0	0.0	0%
12 References	0	0	0	0	0	0.0	0.0	0%
Total	24	55	0	0	22	24.0	79.0	30%

FIGURE 2: THE CIS-CAT REPORT SUMMARY TABLE

⊠	A	B	w	Benchmark Item	Result
1 Install Patches and Additional Software					
?	+	+		1.1 Apply Latest OS Patches	~~notchecked~~
?	+	+		1.2 Install Solaris 10 Encryption Kit	~~notchecked~~
2 Restrict Services					
2.1 Establish a Secure Baseline					
?	+	+		2.1.1 Establish a Secure Baseline	~~notchecked~~
2.2 Disable Unnecessary Local Services					
F	+	+	1.0	2.2.1 Disable Local CDE ToolTalk Database Server	fail
F	+	+	1.0	2.2.2 Disable Local CDE Calendar Manager	fail
F	+	+	1.0	2.2.3 Disable Local Common Desktop Environment (CDE)	fail
F	+	+	1.0	2.2.4 Disable Local sendmail Service	fail
F	+	+	1.0	2.2.5 Disable Local Web Console	fail
F	+	+	1.0	2.2.6 Disable Local WBEM	fail
P	+	+	1.0	2.2.7 Disable Local BSD Print Protocol Adapter	pass
2.3 Disable Other Services					
P	+	+	1.0	2.3.1 Disable RPC Encryption Key	pass
P	+	+	1.0	2.3.2 Disable NIS Server Daemons	pass
P	+	+	1.0	2.3.3 Disable NIS Client Daemons	pass
P	+	+	1.0	2.3.4 Disable NIS+ daemons	pass
P	+	+	1.0	2.3.5 Disable LDAP Cache Manager	pass
F	+	+	1.0	2.3.6 Disable Kerberos TGT Expiration Warning	fail
F	+	+	1.0	2.3.7 Disable Generic Security Services (GSS) daemons	fail
F	+	+	1.0	2.3.8 Disable Volume Manager	fail
P	+	+	1.0	2.3.9 Disable Samba Support	pass
F	+	+	1.0	2.3.10 Disable automount daemon	fail
P	+	+	1.0	2.3.11 Disable Apache services	pass
P	+	+	1.0	2.3.12 Disable Solaris Volume Manager Services	pass
P	+	+	1.0	2.3.13 Disable Solaris Volume Manager GUI	pass
F	+	+	1.0	2.3.14 Disable Local RPC Port Mapping Service	fail
2.4 Enable Required Services					
?	+	+		2.4.1 Enable Kerberos server daemons	~~notchecked~~
?	+	+		2.4.2 Enable NFS server processes	~~notchecked~~
?	+	+		2.4.3 Enable NFS client processes	~~notchecked~~
?	+	+		2.4.4 Enable telnet access	~~notchecked~~

FIGURE 3: A CIS-CAT REPORT DETAILS SECTION

Conclusions

Security is a necessary part of most sysadmins' lives. Generally, security is a complicated annoyance, involving keeping an eye open for frequently changing security recommendations and trying to make those changes on all of the systems within a facility. Multiply this challenge by the number of platforms, applications, and versions of all of the above, and even the best system administrators have a difficult time keeping up.

One way to improve the security situation is to apply a tool to the problem. The best sysadmins consider all aspects of the tool and its impact on their environment before going down that path. Certainly sites and priorities vary, but for most sites and most administrators, a tool such as the Center for Information Security benchmark (both the benchmark document and the Java tool) is a clear improvement over the status quo:

- It is low-cost or free.
- It covers many platforms.
- It is easy to install and use.
- Its results are very useful.
- It effects no changes to the system.
- It is written by experts on the subject.
- It comes with documentation that teaches improved security.
- It is updated frequently.

The CIS organization and its documentation and tool benchmarks get my highest recommendation for utility, practicality, and overall ability to help sysadmins improve site security and maintain that improved security.

As an aside, the best sysadmins tend to be an opinionated group. Feel free to send me your own mental checklists or improvements to the ones I included in this column. A future column collecting these checklists could be very enlightening.

Next Time

Given that the theme of the next *;login:* issue is storage, and Solaris 10 comes with a free, open source, breakthrough file system, it seems fitting that ZFS should be the topic of PATS. As ZFS has been discussed previously in *;login:*, I'll start by updating the status and features list, then discuss field experiences and use cases, and finish with a look into the future of ZFS.

REFERENCES

[1] http://www.cisecurity.org/.

[2] http://blogs.sun.com/gbrunett/entry/cis_solaris_10_security_benchmark1.

[3] Available at http://www.sun.com/security/jass.

[4] http://www.ip-solutions.net/jass/.

[5] http://www.sun.com/products-n-solutions/hardware/docs/Software/\enterprise_computing/systems_management/sst/index.html.

[6] http://www.sun.com/software/security/blueprints/index.html.