Hey Lynis, Audit This

By Russ McRee – ISSA Senior Member, Puget Sound (Seattle), USA Chapter

Prerequisites/dependencies

Unix/Linux operating systems

Happy Holidays to all readers, the ISSA community, and infosec tool users everywhere. As part of December's editorial theme for the *ISSA Journal*, Disaster Recovery/Disaster Planning, I thought I'd try to connect tooling and tactics to said theme. I'm going to try and do this more often so you don't end up with a web application hacking tool as part of the forensics and analysis issue. I can hear Thom (editor) and Joel (editorial advisory board chair) now: "Congratulations Russ, it only took you seven years to catch up with everyone else, you stubborn git." ☺

Better late than never I always say, so back to it. As cited in many resources, including Georgetown University's System and Operations Continuity page, *"Of companies that had a major loss of business data, 43% never reopen, 51% close within two years, and only 6% will survive long-term."*[1] Clearly then, a sound disaster recovery and planning practice is essential to survival. The three control measures for effective disaster recovery planning are *preventive, detective,* and *corrective*. This month we'll discuss Lynis, a security and system auditing tool to harden Unix/Linux (*nix) systems, as a means to facilitate both preventative (intended to prevent an event from occurring) and detective (intended to detect and/or discover unwanted events) controls. How better to do so than with a comprehensive and effective tool that performs a security scan and determines the security posture of your *nix systems while providing suggestions or warnings for any detected security issues? I caught wind of Lynis via ToolsWatch,[2] a great security tools site that provides quick snapshots on tools useful to infosec practitioners. NJ Ouchn (@ToolsWatch), who runs ToolsWatch and the Blackhat Arsenal Tools event during Blackhat conferences, mentioned a new venture for the Lynis author (CISOfy[3]), so it seemed like a great time to get the scoop directly from Rootkit.nl's Michael Boelen, the Lynis developer and project lead.

According to Michael, there is much to be excited about as a Lynis Enterprise solution, including plugins for malware detection, forensics, and heuristics, is under development. This solution will include the existing Lynis client that we'll cover here, a management and reporting interface, as well as related plugins. Michael says they're making great progress and each day brings them closer to an official first version. Specific to the plugins, while a work in progress, they create specialized hooks via the client. As an example, imagine heuristics scanning with correlation at the central node to detect security intrusions. Compliance checking for the likes of Basel II, GLBA, HIPAA, PCI DSS, and SOX is another likely plugin candidate. The short-term road map consists of finishing the web interface, followed by the presenting and supporting documents. This will include documentation, checklists, control overviews, and materials for system administrators, security professionals, and auditors in particular. This will be followed by the plugins and related services. In the meantime CISOfy will heavily support the development of the existing Lynis tool, as it is the basis of the enterprise solution. Michael mentions that Lynis is already being used by thousands of people responsible for keeping their systems secure.

A key tenet for Lynis is proper information gathering and vulnerability determination/analysis in order to provide users with the best advice regarding system hardening. Lynis will ultimately provide both auditing functionality as well as monitoring and control mechanisms; remember the above mentioned preventative and detective controls? For monitoring, there will be a clear dashboard to review the environment for expected and unexpected changes with light touch for system administrators and integration with existing SIEM or configuration management tools. The goal is to leverage existing solutions and not reinvent the wheel.

Lynis and Lynis Enterprise will ultimately provide guidance to organizations who can then more easily comply with regulations, standards, and best practices by defining security baselines and ready-to-use plans for system hardening in a more measurable and action-oriented manner.

One other significant advantage of Lynis is how lightweight it is and easy to implement. The requirements to run the tool are almost non-existent; and it is, of course, open source, allowing ready inspection and assurances that it's not overly intrusive. Michael intends to provide the supporting tools (such as the management interface) as a Software-as-as-Service (SaaS) solution, but he did indicate that, depending on

1 http://continuity.georgetown.edu/dr/.

2 http://www.toolswatch.org/2013/11/lynis-the-auditing-tool-for-unixlinux-v1-3-5-with-the-support-of-many-linux-flavors/.

3 http://cisofy.com/.

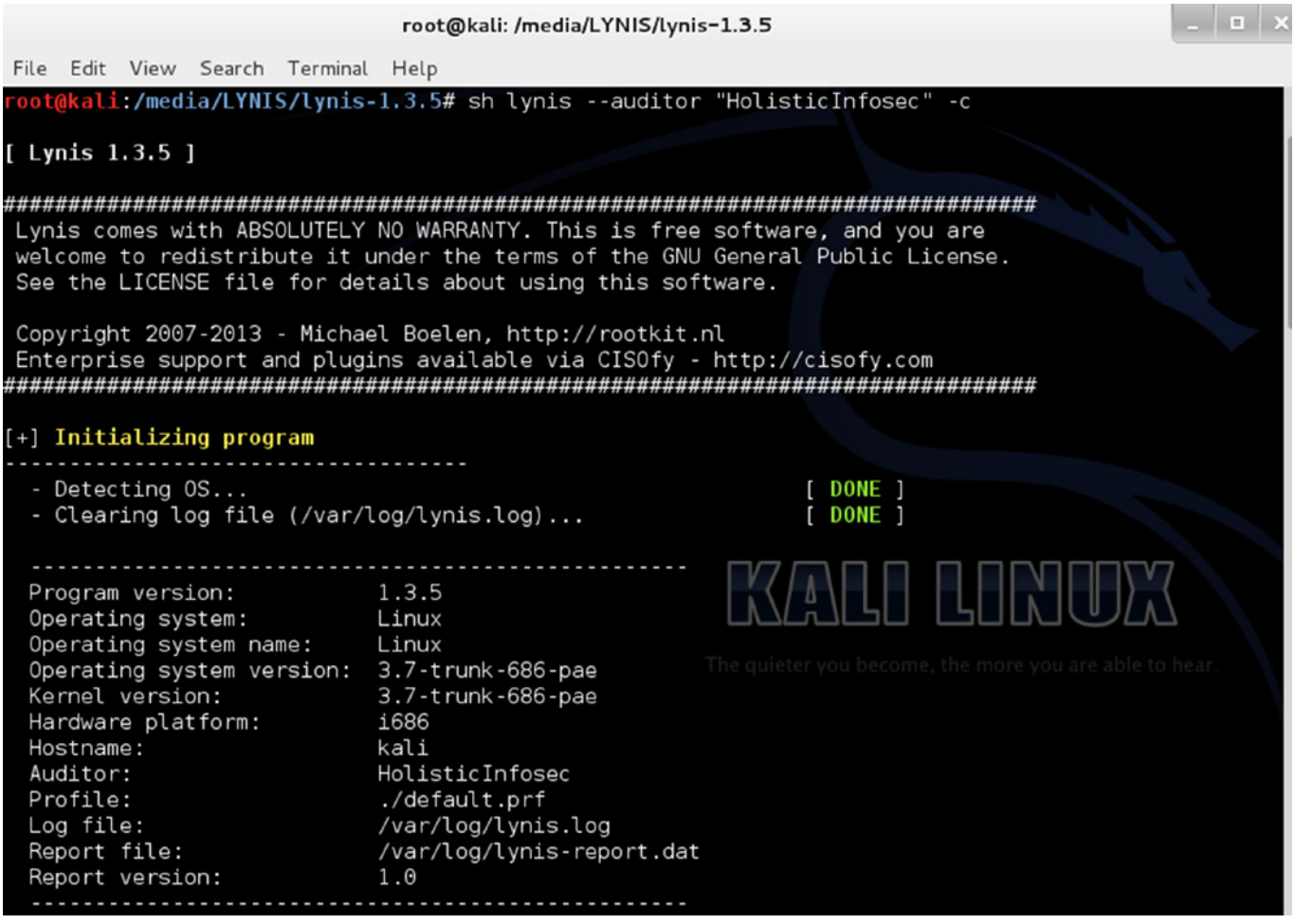

Figure 1 – Lynis kicking off

customer feedback and need, CISOfy might consider appliances at a later stage.

I conducted an interesting little study of three unique, security-centric Linux distributions running as VMWare virtual machines to put Lynis through its paces and compare results, namely, SIFT 2.1.4, SamuraiWTF2.1, and Kali 1.0. Each of these was assessed as pristine, new instances, as if they'd just been installed or initialized.

Setting Lynis up for use

Lynis is designed to be portable and as such is incredibly easy to install. Simply download and unpack Lynis to a directory of your choosing. You can also create custom packages if you wish; Lynis has been tested on multiple operating systems including Linux, all versions of BSD, Mac OS X, and Solaris. It's also been tested with all the package managers related to these operating systems, so deployment and upgrading is fundamentally simple. To validate its portability, I installed it on USB media as follows.

1. On a Linux system downloaded[4] lynis-1.3.5.tar.gz
2. Copied and unpacked it to /media/LYNIS/lynis-1.3.5 (an ext2-formatted USB stick)
3. In VMWare menu, selected *VM*, then *Removable Devices*, and checked *Toshiba Data Traveler* to make my USB stick available to the three virtual machines mentioned above.

You can opt to make modifications to the profile configuration (default.prf) file to disable or enable certain checks, and establish a template for operating system, system role, and/or security level. I ran my test on the three VMs with the default profile.

Using Lynis

This won't be one of those *toolsmith* columns with lots of pretty pictures; we're dealing with a command prompt and text output when using the Lynis client. Which is to say, change directories to your USB drive, `cd /media/LYNIS/lynis-1.3.5` on my first test instance, followed by `sh lynis –auditor HolisticInfoSec –c` from a root prompt as seen in figure 1.

You can choose to use the `–q` switch for quiet mode, which prompts only on warnings and doesn't require you to step through each prompted phase. Once Lynis is finished, you can immediately review results via `/var/log/lynis-report.dat` and grep for suggestions and warnings. You're ultimately aiming for a hardening index of 100. Unfortunately our first

4 http://cisofy.com/downloads/.

pass on the Kali system yielded only a 50. Lynis suggested installing auditd and removing unneeded compilers. Please note, I am not suggesting you actually do this with your Kali instance, fine if it's a VM snapshot; this is just to prove my point re: Lynis findings. Doing so did, however, increase the hardening index to a 51. ☺

Lynis really showed its stuff while auditing the SANS SIFT 2.1.4 instance. The first pass gave us a hardening index of 59 and a number of easily rectified warnings. I immediately correct the following and ran Lynis again:

```
warning[]=AUTH-9216|M|grpck binary found errors in
   one or more group files|
warning[]=FIRE-4512|L|iptables module(s) loaded,
   but no rules active|
warning[]=SSH-7412|M|Root can directly login via
   SSH|
warning[]=PHP-2372|M|PHP option expose_php is
   possibly turned on, which can reveal useful
   information for attackers.|
```

Running grpck told me that "sansforensics" is a member of the "ossec" group in /etc/group but not in /etc/gshadow. Easily fixed by adding `ossec:!::sansforensics` to /etc/gshadow.

I ran `sudo ufw enable` to fire up active iptables rules, then edited /etc/ssh/sshd_config with `PermitRootLogin no` to ensure no direct root login. Always do this as root will be bruteforce attacked, and you can sudo as needed from a regular user account with sudoers permissions. Finally changing `expose_php` to `Off` in /etc/php5/apache2/php.ini solves the PHP finding.

Running Lynis again after just these four fixes improved the hardening index from 59 to 69. Sweet!

Last but not least, an initial Lynis run against SamuraiWTF informed us of a hardening index of 47. Uh-oh, thank goodness the suggestion list per `sudo cat /var/log/lynis-report.dat | grep suggestion` gave us a lot of options to make some systemic improvements as seen in figure 2.

Updating just a few entries pushed the hardening index to 50; you can spend as much time and effort as you believe necessary to increase the system's security posture along with the hardening index.

The end of a Lynis run, if you don't suppress verbosity with the –q switch, will result in the like of figure 3, including your score, log and report locations, and tips for test improvement.

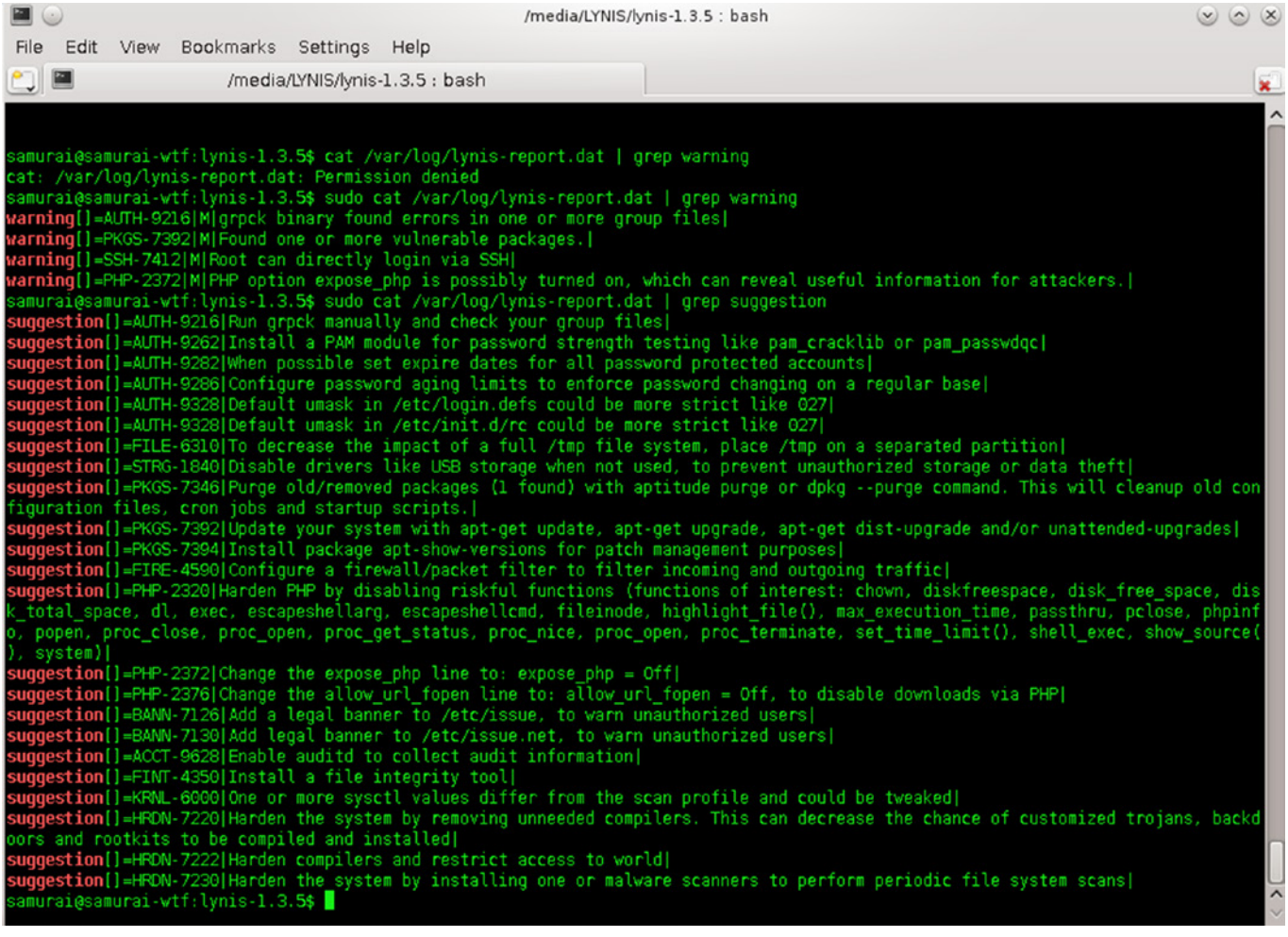

Figure 2 – Lynis suggests how the Samurai might harden his foo

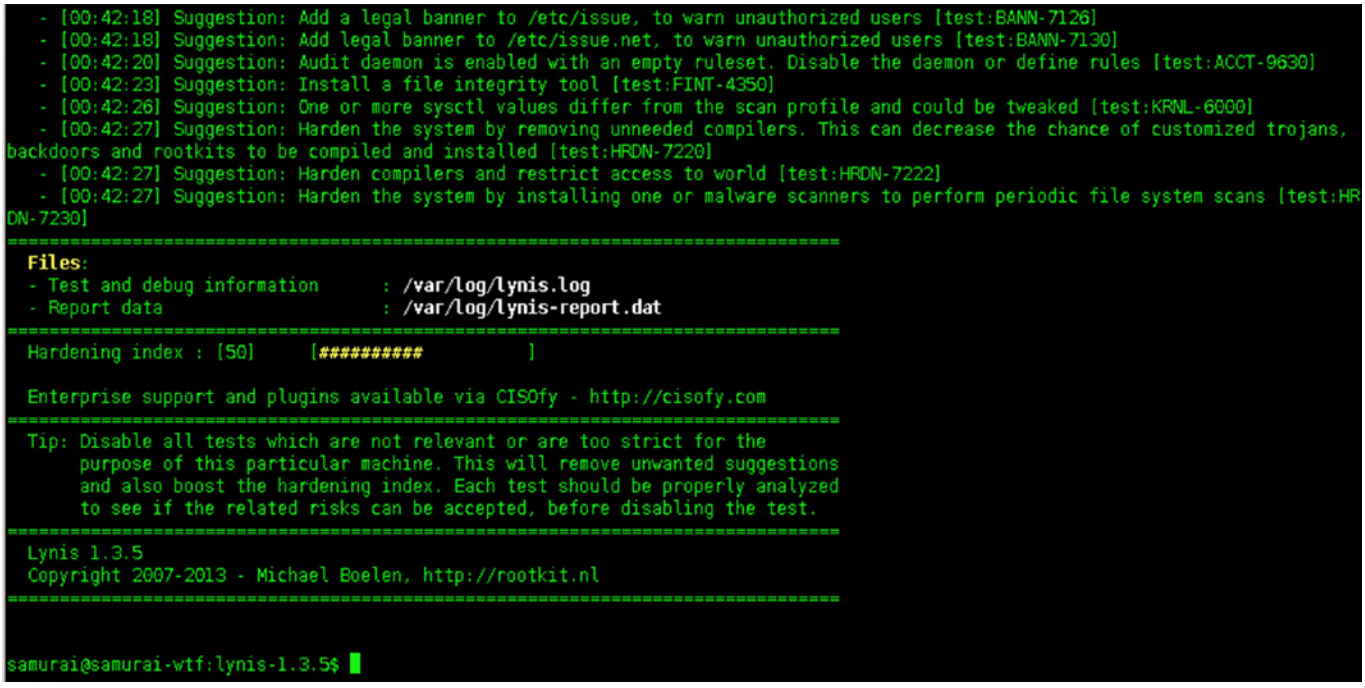

Figure 3 – The end of a verbose Lynis run

Great stuff and incredibly simple to utilize!

Conclusion

I'm looking forward to the Lynis Enterprise release from Michael's CISOfy and believe it will have a lot to offer for organizations looking for a platform-based, centralized means to audit and harden their *nix systems. Again, count on reporting and plugins as well as integration with SIEM systems and configuration management tools such as CFEngine. Remember too what Lynis can do to help you improve auditability against controls for major compliance mandates.

Good luck, and wishing you all a very Happy Holidays.

Stay tuned to vote for the 2013 Toolsmith Tool of the Year starting December 15th.

Ping me via email if you have questions (russ at holisticinfosec dot org).

Cheers…until next month.

Acknowledgements

—Michael Boelen, Lynis developer and project lead

About the Author

Russ McRee manages the Security Analytics team (security incident management, penetration testing, monitoring) for Microsoft's Online Services Security & Compliance organization. In addition to toolsmith, he's written for numerous other publications, speaks regularly at events such as DEFCON, Black Hat, and RSA, and is a SANS Internet Storm Center handler. As an advocate for a holistic approach to the practice of information assurance Russ maintains holisticinfosec.org. He serves in the Washington State Guard as the Cybersecurity Advisor to the Washington Military Department. Reach him at russ at holisticinfosec dot org or @holisticinfosec.