Review: EnGarde Secure Linux (LiveCD)

Those of you who have followed my column know that I am a big fan of Linux. In addition to that, my column focuses on the trials and tribulations of getting my employers computing environment out of the Stone Age and rebuilt with security in mind from the get go. All of this while being hamstrung by an almost nonexistent budget. Therefore, a secure, easy-to-install Linux distro with efficient management capabilities would be a welcome addition to my arsenal of free software.

So when I was tasked with finding out a little bit about EnGarde Secure Linux and saw the description on their web site (quote below), I was immediately intrigued with the opportunity of giving it a trial run and letting EH-Net readers know whether or not it is worth their time.

Editor's Note: Guardian Digital announced the release of EnGarde Secure Community 3.0.18 (Version 3.0, Release 18) on Dec 4, 2007. This release includes many updated packages and bug fixes, some feature enhancements to Guardian Digital WebTool and the SELinux policy, and a few new features. This review was done with a prior release.

"EnGarde is the first truly secure, open source Internet operating platform. Simplified web-based management and enterprise scalability combine to deliver unprecedented security and a feature-rich Internet application environment.

EnGarde enables you to:

- Enforce robust SELinux policies with ease (provided it is installed not run from the LiveCD)

- Build and maintain secure Web sites

- Monitor networks using advanced Intrusion Detection

- Protect user with web and email content filtering

- Control access to Internet resources"

All good stuff, but it was that first bullet point that stuck with me. I am a huge fan of the NSA's open source efforts, but frankly, despite how long it has been around, adoption of SELinux has not been as widespread. I think that it all comes down to the learning curve of SELinux coupled with the way it is packaged. While it is not possible to draw a direct comparison, my hope was to highlight why EnGarde may be something EH-Net readers should get to know a little better..

Note: Please keep in mind that (as with installing SELinux from scratch) EnGarde must be fully installed to run SELinux. As described below, SELinux requires multiple reboots which is obviously not possible in a LiveCD environment. This article was written with EnGarde running in the LiveCD mode.

SELinux

SELinux was created by the NSA and designed to add an extra layer of security to a Linux distro that needed hardening beyond normal terms. SELinux is a series of packages which help to enforce Mandatory Access Control (MAC) and allows even more granular control of individual objects.

Installing SELinux:

-Install distro

-Update distro

-Run apt-get install selinux-basics selinux-policy-refpolicy-targeted1.

-Edit /boot/grub/menu.lst and add selinux=1 to your kernel command line (by adding it to the #kopt= line and then running update-grub). If you are using lilo, you must instead make similar changes to /etc/lilo.conf and run lilo.

-Fix dependencies listed. Below are the highlights. For a complete list please visit, http://wiki.debian.org/SELinux/Setup#package-specific):

- In /etc/pam.d/login uncomment the session required pam_selinux.so multiple" line. Do the same for /etc/pam.d/ssh

- In /etc/default/rcS set FSCKFIX=yes and add EDITMOTD=no. [Only important for 'strict' policy:] In /etc/init.d/bootmisc.sh search for "Update motd" and comment the two lines below that line. Then run rm /var/run/motd. Replace the symlink /etc/motd with a static "message of the day" file instead.

- Add no_static_dev="1" to /etc/udev/udev.conf to prevent udev from providing the /dev/.static directory.

- The cron package includes a daily cronjob to backup some system files, including /etc/shadow. For security reasons, you don't want cron to be able to read this file, so edit /etc/cron.daily/standard and disable the part making a backup of /etc/shadow and /etc/gshadow (bug #333837).

- "locate" is part of fileutils, and a useful tool for finding files on your system. To work it however needs to scan your whole filesystem for files - which would require rather extensive SELinux permissions and might be considered an "information leak". Currently there is no SELinux policy for regular locate to work flawlessly, so it is recommended to disable it on SELinux boxes. To do this, insert an exit 0 as the second line of /etc/cron.daily/find.

- Check that the /selinux directory exists and if not, create it with mkdir /selinux.

- Run touch /.autorelabel and reboot

- Run touch /.autorelabel and reboot again

- Run check-selinux-installation

Total time to install 20-25 minutes, this assumes that you are installing the OS from scratch. Please note that this install was a barebones, business card image and only security updates and packages necessary for the SELinux were installed.

Pros:

- There is a lot of documentation and it is flexible as far as the distro goes. A brief search on Google showed multiple "How-Tos" for Red Hat, Debian, etc.

- This is a secure approach and if your organization has vitally sensitive information, long term you may want to look into SELinux.

- When running nmap on this install it was slightly more secure, since there was no web interface

Cons:

- There is a rather large learning curve, and since SELinux is broken into multiple packages, harnessing SELinux's full potential will take quite a time commitment.

- Since there is no interface, it is a hard to jump right into this product.

- Multiple reboots are required which makes it near imposible to run SELinux on a LiveCD.

- SELinux cannot be run from a live CD and would needed to be deployed, after extensive testing

EnGarde

For this comparison, I used the most recent version of EnGarde Secure Community (there is an enterprise version of EnGarde that is not free) which was released on October 9, 2007. According to EnGarde, version 3.0.17 "includes several bug fixes and feature enhancements to the Guardian Digital WebTool and the SELinux policy, and several new packages available for installation."

Installing EnGarde:

- Select dhcp or enter manual ip

- Choose LiveCD or install (again please keep in mind if you run the LiveCD SELinux will be disabled)

- Click log in

- Open a browser and go to https://x.x.x.x:1023/. Login with username admin and whatever you set for the password.

- Use the WebTool's pulldown menus to select either a service or system you would like to use.

- Simply click on the modules to carry out your requests.

Total time to get EnGarde LiveCD running was only 7-10 minutes. This is as straightforward as it gets. Even a novice Linux user can easily navigate the GUI to leverage the WebTool for easy management of IDS, firewall, and even smtp/pop.

Total time to install EnGarde with SELinux is approx. 15-20 minutes (depending on your connection speed). Please note that a full install was not performed for this review. The concept was to see if EnGarde was a product that was worthwhile. Since EnGarde can run SELinux, it seemed that it would make sense to see everything else that was going on with EnGarde. To perform a full install of EnGarde for SELinux is beyond the scope of this article.

Pros:

- Fast to setup and use

- Can be used as a LiveCD without leaving a trace of its use

Cons:

- GUI opens an additional port that is not open in SElinux

Overall Impression

I would highly recommend downloading and running EnGarde. It gives you a very easy to use Web-based GUI with multiple, built-in security appliances like IDS and firewall, and you can easily leverage the added security benefits of SELinux (if you decide to install EnGarde as opposed to running the LiveCD). I do like SELinux and what the NSA is trying to do, but the bottom line is time, or lack thereof, and EnGarde is a server product that can be installed in much less time than it takes to install your favorite distro without SELinux, yet it offers this and so much more.

So in closing, here's your sound bite:

I can't stress enough how EnGarde is great for those of you whose most valuable commodity is time. Add in the fact that it's free and secure out of the box, and it becomes even more desirable in shops like mine.

Coming soon to a browser near you...
RichM gets his hands on a OLPC Machine. Let's see how secure it is!!