EnGarde Secure Linux Review

Juan van der Merwe

This review is on EnGarde Secure Linux which is a easy to use, out of the box Linux distribution built for what the name says, Secure (security).EnGarde Secure Linux does just that for your server with easy to setup user restrictions, Trusted hosts, Firewall protection etc via the GDWT (Guardian Digital WebTool)

Seeing the nature of EnGarde which is security it still allows you to do the basics like Setup and manage: local DNS, mail, web, ftp servers and backups.

EnGarde minimum system requirements

I have found that like any linux distribution the hardware requirements are minimal. EnGarde developers recommend at least a Pentium series processor, 32MB of RAM. A 2GB hard drive and an Ethernet (10/100/1000) adapter. To utilize the true potential of EnGarde I recommend 512MB of RAM and at least a 10GB hard drive.

Installation

A copy of the distribution can be downloaded from *http://www.EnGardelinux.org/*.

Registering your copy at *http://www.guardiandigital.com/register/* has its usual benefits mailing list, priority and instant access to new system and security updates as well as GDMS (Guardian Digital Master Support).

EnGarde also has a LiveCD option at the beginning of the installation which allows you to boot and run EnGarde without any changes on your hard drive, suggested for the *test* run for this distribution.

The LiveCD function is setup similar to other distributions with this feature. When doing a hard disk installation you will be asked general questions like language, the installation hard drive (automatic or manual partitioning) as well as basic packages to install, Firewall services, Web, Mail and DNS services and so forth. You will need to supply general network information regarding your install as IP address etc. You will have to remember the IP address as you need to configure the EnGarde server from any other PC on the same network.

Accessing your EnGarde server from another PC, simply type the IP address that you assigned it in the begin stages of the installation eg. *http://192.168.1.2:1023/* you will then need to accept the SSL certificate and proceed with the login.

You can now setup your Trusted hosts and passwords that can access your EnGarde`s Webtool (Figure 1).

Also setting up your startup services which will startup on bootup.

A nice feature with EnGarde is the Virtual Mail Domain Management, where you can create and maintain your needed mail boxes.

Setting up a FTP server is also very easy using the WebTool, but still maintains security regarding unencrypted logins and access control, which I found that EnGarde has made very easy for the server administrator.

Guardian Digital Secure Network (GDSN)

Guardian Digital created a free, basic, easy to use way of keeping up to date with the current system updates as well as piece of mind from the experts, like advice, usefull information and valuable services.

Making sure you are always protected against cyber attacks is one of (if not the most) important aspect to a multi computer network, seeing as data loss or corporate espionage can cost your business thousand of dollars in rectifying it by data recovery, system crashes or online asset theft.

Intruder Detection System

EnGarde comes with a full proactive intruder detection system, which basically does a real time scan as you go about your day to day administration operations with your EnGarde server, think of it as the same principal as a real time virus scan on a windows computer. The system scans individual ports for unwanted activity and any intruder attempts.

The scan is in a easy to read and understand attack graph form which allows you to get more info on your unexpected

Figure 1. Passwords and access control

guests, it lists attacks by multiple groups and orders like Protocol ,Class, Priority ,Common attacks and Port destinations (Figure 2).

Firewall Utility

Like any good and stable Linux distribution, ease of use is a big concern to the general Linux beginner.

With the EnGarde WebTool, setting up your firewall and firewall rule set is as easy as 1.2.3 Creating port forward rule sets can be done and maintained in a matter of seconds, obviously an understanding of ports is needed when using the Web Tool firewall setup.

Figure 2. Attack graphic

Setting up the trusted and un-trusted list on your server could never be easier.

EnGarde also allows you to use the blacklist function which is also very handy to have (Figure 3). Using the easy tick box style configuration to make and setup your EnGarde firewall rule set has never been easier. Click-click-click-click and you're done.

Alias utility for your Web and Email server

Manage and organize corporate websites and email communications quickly and easily. EnGarde's web server aliasing module allows server administrators to create thousands of virtual websites to distinctly display and organize all business-critical information from a single IP address. EnGarde also gives the administrator the ability to add email server aliases, allowing the creation of thousands of virtual email domains and providing simplified management for efficient office email communications.

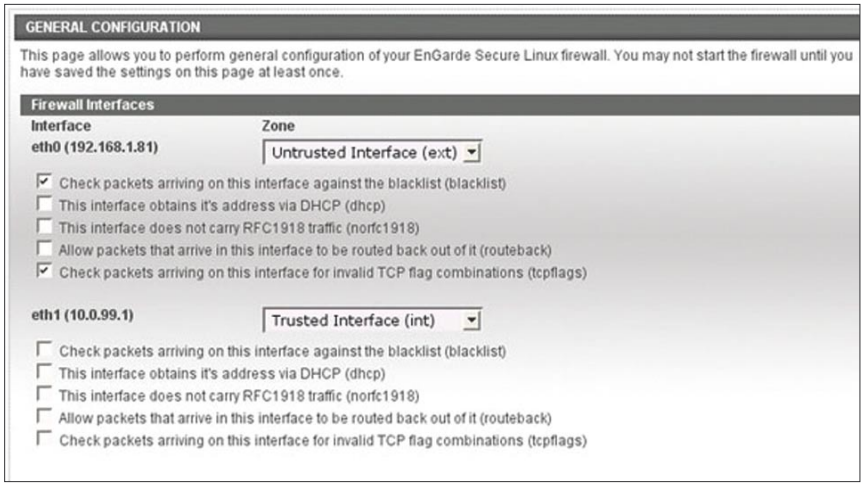

Figure 3. General configuration

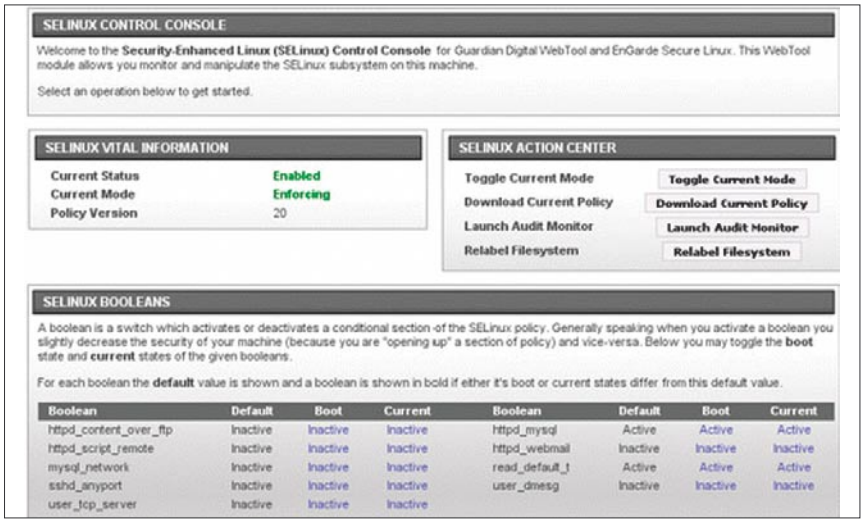

Figure 4. Selinux control

Netdiff Reporting Utility

Netdiff is for me, one of the quickest and easiest way to find out what has been happening on my EnGarde server, it monitors new hosts that have been added to your system, warns you about services that have been stopped as well as new ports that have been opened by a user.

Email protection and scanning on your EnGarde server.

As with most Linux security setups, scanning of emails are very important.

EnGarde, like other Linux distributions use ClamAV, SpamAssassin and Amavis to take care of the always irritating Spam.

The setup of the above mentioned packages are pretty simple to install on your EnGarde server and the configurations is the same like any other Linux distribution.

- ClamAV is used for scanning for viruses on your EnGarde mail server.
- SpamAssassin is basically just what the name says, scans for spam threats
- Amavisd-new is the content filter which sends the data to either the virus scanner or the spam scanner, which ever one is set to default.

Access control and SELinux

SELinux (Security-Enhanced Linux) is a security module that places all applications and processes under the control of the server administrator. The SELinux Control Console can be found on the WebTool and allows the administrator to define which working environment of processes and which recourses it may access (Figure 4).

Review Conclusion

After working with different Linux and Unix distributions in the past, I found that EnGarde is by far the most unique distribution to date.

I managed to setup my complete server in less than 30mins, there is more than enough documentation regarding EnGarde Secure Linux freely available on the net.

The security of EnGarde is of the highest level while still being able to perform the day to day functions of a normal Linux server.

EnGarde Secure Linux is a complete all in one, out of the box solution to suite any type of network.