

ENGARDE SECURE LINUX

JUAN VAN DER MERWE

Engarde Secure Linux, 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 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 available at the beginning of the installation which allows you to boot and run Engarde without any changes on your hard drive. It's suggested you to use the LiveCD option to test run 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 such as IP address etc. You will have to remember the IP address as you need to configure the Engarde server from other PCs on the same network.

Access your Engarde server from another PC by simply typing the IP address

you assigned at the initial 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). You're also able to manage your startup services which will run on bootup. A nice feature with Engarde is the Virtual Mail Domain



Figure 1. Passwords and access control



Figure 2. Attack graphic

Management, where you can create and maintain your needed mail boxes.

Setting up a FTP server is also very easy using the WebTool. It contains all the

necessary security features regarding unencrypted logins and access control making it 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 thousands of dollars in online asset theft, lost productivity, and data recovery costs.

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. The system scans individual ports for unwanted activity and any intruder attempts. Think of it as the same principal as a real time virus scan on a windows computer.

The scan is easy to read and understand attack graph form which allows you to get more info on your unexpected 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 and maintianing port forward rule sets can be done in a matter of seconds; obviously an understanding of ports is needed when using the Web Tool firewall setup. 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). 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

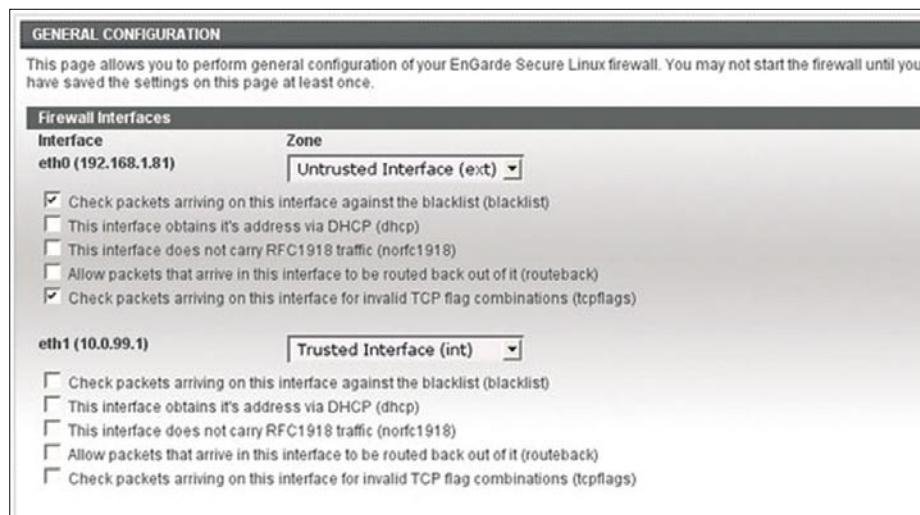


Figure 3. General configuration

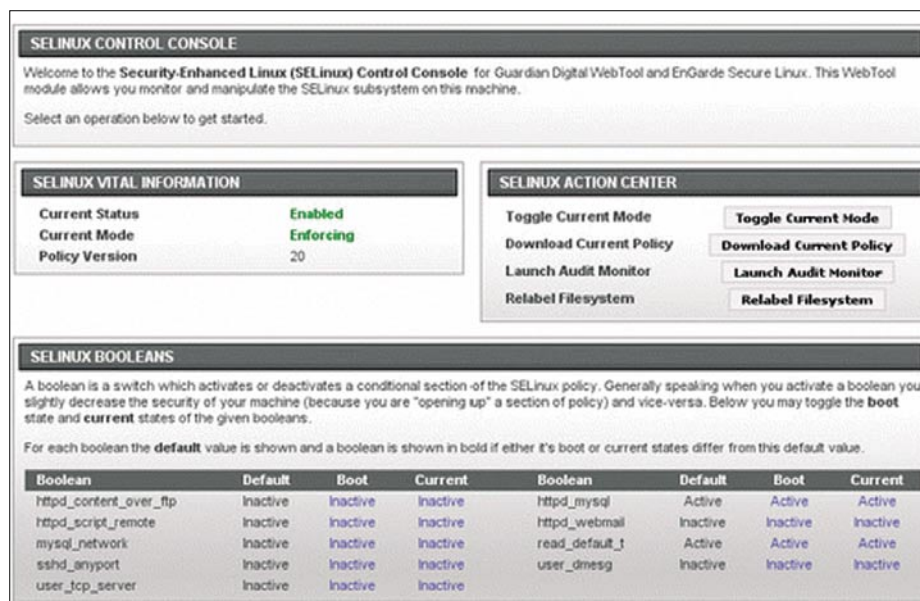


Figure 4. Selinux control

Network attacks

EnGarde Secure Linux also uses a variety of strategies to deal with attacks originating from the server's network. EnGarde's first line of defense to these attacks is to detect and report anomalous or suspicious network activity through the use of the Snort intrusion detection program. Snort examines network packets to look for the signatures of potential network threats and notifies the user when they are detected. Since Snort, an open source tool, is only effective when its set of rules is kept up-to-date, EnGarde, through the GDSN, keeps Snort supplied with the very latest rules.

EnGarde also helps reduce network vulnerabilities resulting from improper network configurations like inadvertently opened network ports by including its own network port status utility, NetDiff, which runs the Nmap port scanner at regular intervals, compares the results, and reports changes that could open EnGarde to network attacks. While these techniques cannot prevent network attacks like Denial of Service attacks that overload the server by exploiting flaws in the network protocols themselves, it does allow the EnGarde user to react quickly to potential or actual network attacks and prevent serious service interruptions.

Security at the Kernel and Security Enhanced Linux (SELinux)

EnGarde Secure Linux begins its defense in depth at the kernel, a level neglected by many supposedly secure systems, through the comprehensive application of security policies using *Security Enhanced Linux* (SELinux). Although released in its current form relatively recently, SELinux has a substantial heritage as part of a decades-long effort to develop inherently secure or "trusted" operating systems. This largely academic effort culminated in the development and subsequent public release by the *National Security Agency* (NSA) of SELinux. The release of this previously closely-guarded security framework was both a complete surprise to the open source community and a watershed in open source security development.

Guardian Digital was among the first in the open source community to realize the revolutionary potential of SELinux policies for building a truly secure operating system. Soon after the release of SELinux, Guardian Digital committed itself to the ambitious goal of applying SELinux policies to every element of its secure operating system and to every service it offered. Guardian Digital achieved this goal with the release of EnGarde Secure Linux 3.0, among the first and most thorough implementations of SELinux.

Snooping and Eavesdropping

Not all attackers are bent on causing damage to the system. Instead, many are attempting to steal private information by listening to the system's communications within the server or over the network. One common follow-up to rootkit intrusions, for example, is to install *keylogger* programs that record the system user's keyboard input to steal passwords. Another example is network *sniffing* commonly used to intercept passwords to outside systems as well as sensitive personal information like financial data and social security numbers. EnGarde presents several defenses to this kind of unauthorized listening. First, EnGarde makes it difficult or impossible for a would-be listener to install and run *snooping* software on the system by using the combination of detection and access restrictions described above. More important, though, EnGarde prevents the listener from finding anything intelligible to listen to by using encryption for every sensitive communication and every important service.

Feature Overview

EnGarde Secure Linux achieves its unique built-in security by drawing on the worldwide resources of the open source community, selecting *best of breed* open source security tools and then carefully configuring these tools for maximum security. These tools include:

SELinux kernel-level security

EnGarde Secure Linux uses SELinux, a system of kernel-level security tools originally developed by the NSA (*National Security Agency*) to control access by processes and programs to only those resources they need to do their jobs, thereby preventing the large-scale damage that intrusions and compromises can wreak on traditional computer systems.

Guardian Digital WebTool remote administration

EnGarde Secure Linux is designed for secure and convenient remote administration using Guardian Digital's custom-designed interface, the WebTool. The WebTool streamlines and simplifies all common system administration tasks, and guides the user in maintaining securely configured Internet services.

Guardian Digital Secure Network

Users of EnGarde Secure Linux receive program updates and security patches through the *Guardian Digital Secure Network* (GDSN) using the *Guardian Digital WebTool*, thereby ensuring that their EnGarde systems remain secure.

Intrusion Detection

EnGarde Secure Linux uses the best available open source tools to detect both actual system attacks and potential threats using the both local host-based detection systems and systems that detect network-based threats.

Secure Internet services

EnGarde Secure Linux selects the best available open source programs like Apache, Postfix, and vsFTPD and then configures them for maximum security, functionality, and productivity using the Guardian Digital WebTool.

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.

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 and 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 above mentioned packages are pretty simple to setup on your EnGarde server and the configuration is done the same as 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 resources it may access (Figure 4).

CONCLUSION

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

Security Distributions		
Arudius	Arudius is a Linux live CD. The CD consists of a Zenwalk Linux base on top of which a large collection of network security testing software has been installed.	http://www.fosstools.org/
BackTrack	BackTrack is Linux live distribution focused on penetration testing, based on SLAX. It's evolved from the Whax and Auditor Security Collection. BackTrack consists of more than 300 different up-to-date tools which are logically structured according to the work flow of security professionals.	http://www.remote-exploit.org/backtrack.html
Damn Vulnerable Linux (DVL)	DVL is a Linux-based tool for both novice and professional security personnel. It was initiated for training tasks and learning IT security knowledge domains such as web vulnerability, network security, or binary vulnerability such as exploitation or shellcodes.	http://www.damnvulnerablelinux.org
DEFT (Digital Evidence & Forensic Toolkit)	DEFT is a Xubuntu Linux-based Computer Forensics live CD. It is a very easy to use system that includes an excellent hardware detection and the best free and open source applications dedicated to incident response and computer forensics.	http://www.deflinux.net
FCCU	FCCU GNU/Linux Forensic Boot CD is based on Debian-live that contains a lot of tools suitable for computer forensic investigations, including bash scripts. The main purpose of the CD is to help the forensic analyze of computers.	http://www.lnx4n6.be
Frenzy	Frenzy is a portable system administrator toolkit based on FreeBSD. It generally contains software for hardware tests, file system check, security check and network setup and analysis.	http://frenzy.org.ua/eng
grml	grml is a bootable CD (Live-CD) originally based on Knoppix and nowadays based on Debian. grml includes a collection of GNU/Linux software especially for system administrator and users of texttools. grml provides automatic hardware detection.	http://www.grml.org
Helix	Helix is a customized distribution of the Knoppix Live Linux CD. Helix is more than just a bootable live CD. You can still boot into a customized Linux environment that includes customized linux kernels, excellent hardware detection and many applications dedicated to Incident Response and Forensics.	http://www.e-fense.com/helix
Knoppix-NSM	Knoppix-NSM is to learn about Network Security Monitoring or to deploy a NSM capability in your network based on KNOPPIX Technology.	http://www.securixlive.com/knoppix-nsm/
Network Security Toolkit (NST)	NST is bootable ISO live CD based on Fedora. The toolkit was designed to provide easy access to best-of-breed Open Source Network Security Applications and should run on most x86 platforms.	http://www.networksecuritytoolkit.org
OSWA Assistant	The OSWA-Assistant is a self-contained, freely downloadable, wireless-auditing toolkit for both IT-security professionals and End-users alike.	http://oswa-assistant.securitystartshere.org
OWASP Labrat	The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. The OWASP Live CD (LabRat) is a bootable CD akin to knoppix but dedicated to Application Security.	http://www.owasp.org
Protech	Protech is a specially designed Linux distribution for security technicians and programmers, although it can be used normally as your default desktop system. Protech ONE comes with a great variety of the best security tools for your use.	http://www.techm4sters.org
Samurai	The Samurai Web Testing Framework is a live linux environment that has been pre-configured to function as a web pen-testing environment. The CD contains the best of the open source and free tools that focus on testing and attacking websites.	http://samurai.inguardians.com