Sentora-paranoid version 1.0.0
by: Mario Rodríguez Somohano
sentora-paranoid@open-source.tk

Official web site: http://sentora-paranoid.open-source.tk
Forum: http://forum.sentora-paranoid.open-source.tk

Document versión: 1.0.0-150202

Thanks for choosing sentora-paranoid for your sentora hosting environment security solution

We've broken down the installation into many smaller steps. Don't worry if it looks daunting; if you need any help, just post a thread in the forum for the version you are running, and we will try to help you.

•Having trouble with sentora-paranoid? The support at the site forum is free and available to anyone using this software, supported by other members of the community!
•Must of sentora-paranoid packages are customizable to suit your site's needs, but please refer to the package documentation and package specific support for it.
•Best of all, sentora-paranoid is released under the GNU GPL Licence, and therefore it's enterily free! No forced advertisements, no cost, no sign-ups, no forced email subscriptions!
•You will require a web host to run your sentora panel secured by sentora-paranoid
•Your web host must satisfy a few basic requirements for sentora-paranoid to run properly.

Installation

Downloading the installers scripts

1. First, Install a new fresh linux distribution.
2. Execute the latest sentora installer from the sentora project web page
(you may need to install curl first)

```
>bash <(curl -Ss https://raw.githubusercontent.com/sentora/sentora-installers/master/sentora_install.sh)
```

3.Follow sentora installer instructions
4.Download or execute sentora-paranoid installer from the sentora-paranoid web page

```
>bash <(curl -Ss http://sentora-paranoid.open-source.tk/installers/1.0.0-yymmdd/sentora-paranoid.sh)
```

Replace *yymmdd* for a valid release number (or use the dev-snapshot for current development test)

You will see the installation welcome screen which asks for some usefull information for the server you are installing, as shown on figure 1, then you will be asked for start installation.

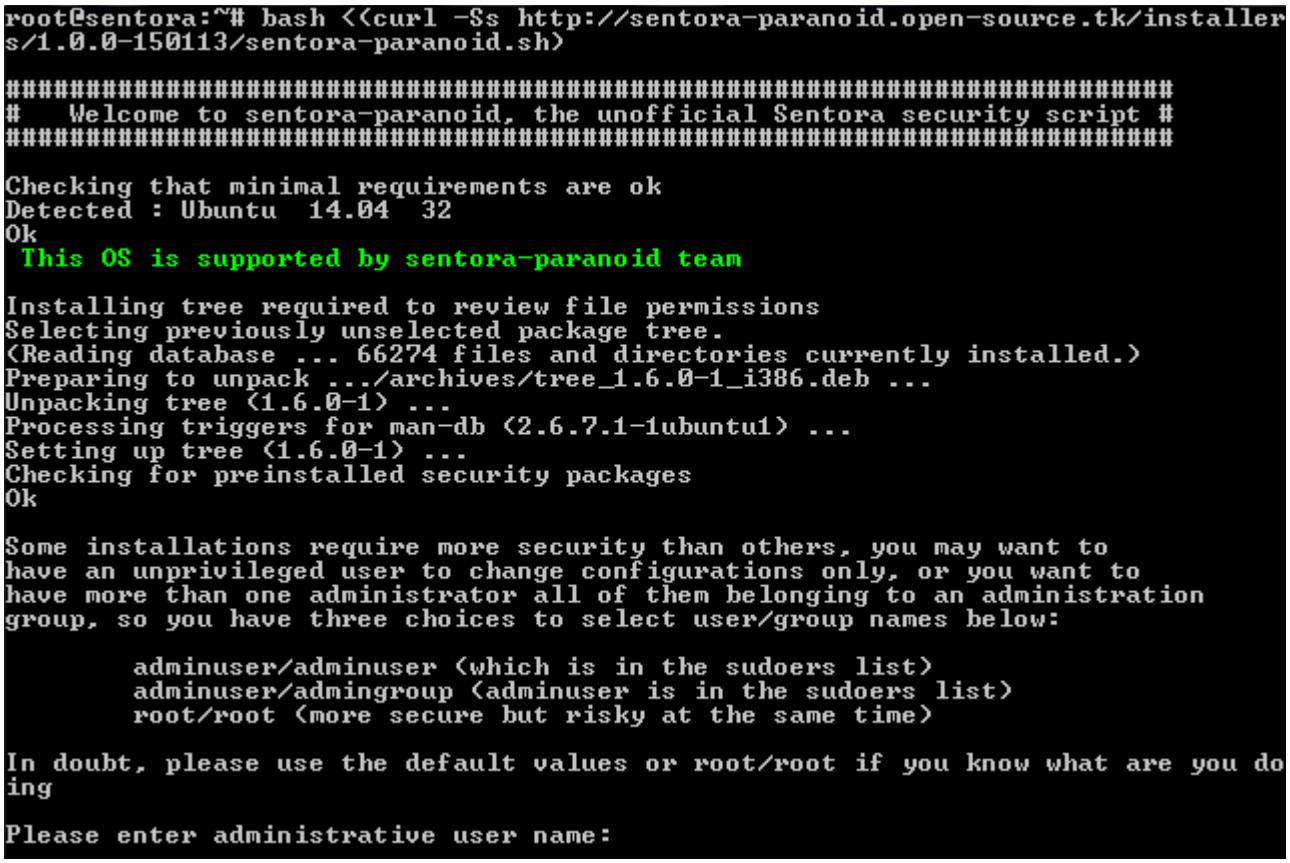

Figure 1: sentora-paranoid welcome screen

Administrative user/group:

The first thing that script will ask to you is the administrative user name and group you wish to use as administrative accounts, and there is three options:

> adminuser/adminuser: The user that perform sudo command (probably your user)
> adminuser/admingroup: The user that perform sudo command and sudoers group
> root/root: The root user

What is the appropiate selection? It depends on how you delegate administration, but here is a hint:

a) If you are the only administrator you can write your unprivileged user and group (default)
b) If there are more than one administrator and all of them belongs to an administrative group you need to write your username and the administration group
c) You can choose root account as the only administrator, but be advised, there is no need to risk your server for mistakes using this account just only by change a simple configuration file.

Unsecure PHP functions

The system, exec and eval PHP functions are dangerous. Some specific installations may not require this functios enabled, some others need them to operate effectively, Unfortunately, various content managment systems requires some of this functions. If you are unsure the best answer here is: NO, to keep enabled these php functions.

MTA virus scanner and content filters

Some hosting environments requires to handle a better mail security but we aware that virus scanners and content filters may require more CPU and RAM resources. You will be asked if you want to install a MTA virus scanner and content filters (not required for all installations).

MAC – Mandatory Access Control system (apparmor)

AppArmor is an effective and easy-to-use Linux security system, apparmor proactively protects the operating system and applications from external or internal threats by enforcing good behavior and preventing even unknown application flaws from being exploited. The main drawback is that this software may block legitimate applications and it's not quite user friendly for average user, for these reason this security feature will remain optional.

Sentora security modules

By default, modules can't be loaded without certain file system permissions, to allow modules installation you need to changes file system permissions manually, this will be improved in future sentora-paranoid script releases. By now the sentora-paranoid script has an experimental sentora module currently under development, you must not install security modules unless you were developing and testing this modules.

At this point the script is ready for installation.

Iptables-persistant configuration

It doesn't matter if you select yes or no, because proper iptables rules will be stored later during installation.

Note that you will be prompted for this twice, for ipv4 and for ipv6 settings.

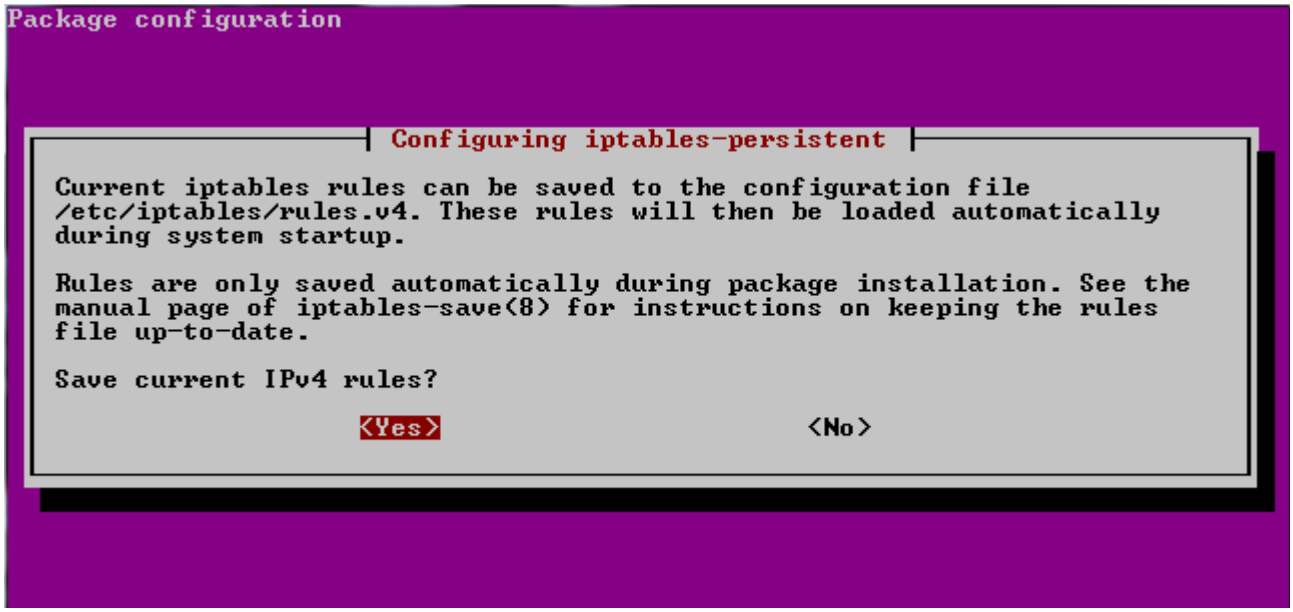

Figure 2: iptables-persistant rules

sentora-paranoid installed packages

You will see the instalation progress of the following packages:

Package	Version	Description
tree	1.6.0-1	Displays directory tree to check original and final file permissions
iptables	1.24.1-1	Administration tools for packet filtering and NAT (Firewall functions)
iptables-persistent	0.5.7	Boot-time loader for iptables rules
openssl	1.0.1f-1	Secure Sockets Layer toolkit - cryptographic utility
fail2ban	0.8.11-1	Ban hosts that cause multiple rule based authentication errors
apparmor	2.8.95~2430-0	User-space parser utility for AppArmor (Mandatory Access Control (MAC) system which is a kernel (LSM) enhancement to confine programs to a limited set of resources)
apparmor-utils	2.8.95~2430-0	Utilities for controlling AppArmor
libapache2-mod-apparmor	2.8.95~2430-0	Changehat AppArmor library as an Apache module to confine vhost scripts
ipset	6.20.1-1	Administration tool for kernel IP sets (hash tool to block unwanted ips)
opendkim	2.9.1-1	Milter implementation of DomainKeys Identified Mail
opendkim-tools	2.9.1-1	Set of command line tools for OpenDKIM
amavisd-new	1:2.7.1-2	Interface between MTA and virus scanner/content filters
spamassassin	3.4.0-1	Perl-based spam filter using text analysis
spamc	3.4.0-1	Client for SpamAssassin spam filtering daemon
clamav	0.98.5	anti-virus utility for Unix - command-line interface

clamav-base	0.98.5	anti-virus utility for Unix - base package
libclamav6	0.98.5	anti-virus utility for Unix - library
clamav-daemon	0.98.5	anti-virus utility for Unix - scanner daemon
clamav-freshclam	0.98.5	anti-virus utility for Unix - virus database update utility
sp-policyd	1.0.0	Postfix send rate limit per user/domain
libswitch-perl	2.16-2	Switch statement for Perl
libnet-dns-perl	0.68-1.2build1	Perform DNS queries from a Perl script
libmail-spf-perl	2.9.0-2	Perl implementation of Sender Policy Framework and Sender ID
pyzor	1:0.5.0-2fakesync1	spam-catcher using a collaborative filtering network
razor	1:2.85-4build2	spam-catcher using a collaborative filtering network
-decompressors-		arj bzip2 cabextract cpio gzip nomarch pax rar unrar unzip zip

See log files for preinstalled packages configurations changes.

temporary SSL certificates

The script generates two temporary certificates, one for CAroot and one for the server name you provided earlier. This certificates are used to provide SMTP, POP3, sFTP and HTTPS security.

Figure 3: Temporary SSL CA private key

CAroot password will be saved and will be recorded in /root/passwords.txt.

Remember CA and server certificates are temporary, you are encouraged to generate your own certificates and replace these ones.

Completed installation

Once the script ends a completed installation screen will be showed to you with relevant information, plese take note of:

- Name of the log file and where is located
- MySQL user account and password (for sentora-paranoid proccesses)
- OpenSSL Caroot password (for sign temporary certificates)

Figure 4: Reboot screen

There is a lot of important changes to the server configurations, you can review the script notices executing the grep command as follow:

```
> grep "NOTICE" <path of the log file>
```

And last, you need to reboot your server to changes take effect.

Troubleshooting

If you have any trouble please consider the forum to check for community solutions.
http://forum.sentora-paranoid.open-source.tk/