msec [Mandrake SECurity tools]

Camille Bégnis <camille@mandrakesoft.com>

22/12/1999

Contents

1 Introducing msec

While Linux is being used for a very wide range of applications, from basic office work to high availability servers, came the need for different security levels. It is obvious that constraints inherent to highly secured servers do not match the needs of a secretary. In the other hand a big public server is more sensitive to malicious people than my isolated Linux box.

It is in that aim that were designed the msec package. It is made of two parts:

1. Scripts that modify the whole system to lead it to one of the six security levels provided with msec. These levels range from very poor security and ease of use, to paranoid config, suitable for very sensitive applications, managed by experts.

2. Cron jobs, that will periodically check the integrity of the system upon security level configuration, and eventually detect and warn you of possible intrusion of the system or security leak.

Note that the user may also define his own security level, adjusting parameters to his own needs.

2 Installation

msec is a base rpm. That means that if you previously installed Linux-Mandrake, msec is already installed on your system.

Installing the rpm will create a msec directory into /etc/security, containing all is needed to secure your system.

Then just login as root and type "/etc/security/msec/init.sh x", x being the security level you want or "custom" to create your own security level. The script will begin to remove all modifications made by a previous security level change, and apply the features of the chosen security level to your system. If you choose "custom", then you will be asked a series of questions for each security feature msec proposes. At the end, these features will be applied to your system.

Note that whatever the level you chose, your configuration will be stored into "/etc/security/msec/security.conf".

2.1 Level 0

This level is to be used with care. It makes your system more easy to use, but very sensitive at the same time. In particular, you shouldn't use this security level if you answer yes to at least one of the following questions:

- Is my computer connected to the Internet?
- Is my computer connected to other computers by a network?
- Does this computer will be used by someone else than me?
- Is there some confidential stuff on my computer I don't want others have access?
- I don't know Linux enough and I could harm it by myself?

As we see, this security level shouldn't be set by default because it may result in big problems for your data.

2.2 Level 1

The main security improvement compared with level 0 is that now, the access to one user's stuff is granted via user-name and password. So it may be used by various people, and it is less sensitive to bad maneuvers. However it shouldn't be used for a connected computer whether by modem or to a LAN (Local Area Network).

2.3 Level 2

Few improvements for this security level, the main one is that there are more security warnings and checks. It is more secure for multi-users use.

2.4 Level 3

This is the standard security recommended for a computer that will be used to connect to the Internet as a client. Most of security checks are periodically run, specifically one that check for open ports on the system. However, these open ports are kept opened and access to them is granted to everyone. So this security level is not really suited for a system permanently connected to the Internet.

From the user's point of view, the system is now a little bit more closed, so it'll need some basic knowledges of the Linux system to achieve some special operations. The security here offered is comparable with the one of a standard RedHat or previous Mandrake distribution.

2.5 Level 4

With this security level, the use of this system as a server becomes possible. The security is now high enough to use the system as a server which accept connections from many clients. Connections from the computer itself only will be granted. Howether advanced services have been disabled, and the system administrator will have to activate the desired ones by hand in config files. He also will have to define from whom the access is granted.

Security checks will warn system administrator of possible security holes or intrusions on the system.

2.6 Level 5

We take level 4 features, but now the system is entirely closed. Security features are at their maximum. The system administrator has to activate ports, and grant connections to give other computers access to services offered by this machine.

3 Security levels features

Follows the description of the different security features each level brings to the system. These features are of various types:

- file permissions,
- warnings dispatching,
- periodicall security checks:

  - on files: suid root, writeable, unowned;
  - listening ports: active, promiscuous;
  - passwords files.

- X display connections,
- listening port check,
- services available,
- boot password,
- authorized clients.

Feature \ Security level	***0***	***1***	***2***	***3***	***4***	***5***
Global security check		*	*	*	*	*
umask users	002	002	022	022	077	077
umask root	002	002	022	022	022	077
shell without password	*					
authorized to connect to X display	all	local	local	none	none	none
User in audio group	*	*	*			
. in $PATH	*	*				
Warning in /var/log/security.log		*	*	*	*	*
Warning directly on tty			*	*	*	*
Warning in syslog			*	*	*	*
Warning sent by mail to root			*	*	*	*
Suid root file check			*	*	*	*
Suid root file md5sum check			*	*	*	*
Writeable file check			*	*	*	*
Permissions check				*	*	*
Suid group file check				*	*	*
Unowned file check				*	*	*
Promiscuous check				*	*	*
Listening port check				*	*	*
Passwd file integrity check				*	*	*
Shadow file integrity check				*	*	*
System security check every midnight				*	*	*
All system events additionally logged to /dev/tty12				*	*	*
Only root can shutdown					*	*
Services not known disabled					*	*
Boot password					*	*
Grant connection to	all	all	all	all	local	none

Note that six out of the ten periodical checks can detect changes on the system. They store into files located in "/var/log/security/" the configuration of the system during the last check (one day ago), and warn you of any changes occurred meanwhile. These checks are:

- Suid root file check
- Suid root file md5sum check
- Writeable file check
- Suid group file check
- Unowned file check
- Listening port check

3.1 Global security check

- NFS filesystems globally exported. This is regarded as insecure, as there is no restriction for who may mount these filesystems
- NFS mounts with missing nosuid. These filesystems are exported without the "nosuid" option.
- Host trusting files contains "+" sign. That means that one of the files "/etc/hosts.equiv /etc/shosts.equiv /etc/hosts.lpd" is containing hosts which are allowed to connect without proper authentication.
- Executables found in the aliases file. It issues a warning naming the executables run through files "/etc/aliases" and "/etc/postfix/aliases".

3.2 umask users

Simply sets the umask for normal users to the value corresponding to the security level.

3.3 umask root

The same but for the root.

3.4 shell without password

Access to the consoles is granted without asking for a password.

3.5 authorized to connect to X display

- all : Everybody from everywhere can open an X window on your screen.
- local : Only people connected at localhost may open an X window on your screen.
- none : Nobody can do that.

3.6 User in audio group

Each user is a member of the "audio" group. That means that every user connected to the system is given access to sound card.

3.7 . in $PATH

the "." entry is added to $PATH environment variable, allowing execution of programs within the current working directory.

3.8 Warning in /var/log/security.log

Each warning issued by msec is logged into "/var/log/security.log".

3.9 Warning directly on tty

Each warning issued by msec is directly printed on current console.

3.10 Warning in syslog

Warnings of msec are directed to syslog service.

3.11 Warning sent by mail to root

Warnings issued by msec are also sent by mail to root.

3.12 Suid root file check

Check for new or removed suid root files on the system. If such files are encountered a list of these files is issued as a warning.

3.13 Suid root file md5sum check

Checks the md5sum signature of each suid root file that is on the system. If the signature has changed, it means that a modification has been made to this program, probably a backdoor. A warning is then issued.

3.14 Writeable file check

Check wether files are world writable on the system. If so, issues a warning containing the list of these naughty files.

3.15 Permissions check

This one checks permissions for some special files such as .netrc or user's config files. It also checks permissions of users home dir. If their permissions are too loose or owners unusual, it issues a warning.

3.16 Suid group file check

Check for new or removed suid group files on the system. If such files are encountered, a list of these files is issued as a warning.

3.17 Unowned file check

This check searches for files owned by users/groups(or more accurately by uids/gids) not known into /etc/password, If such files are found, the owner is automatically changed to user/group "nobody".

3.18 Promiscuous check

This test checks every ethernet card to determine wether they are in promiscuous mode. This mode allows the card to intercept every packet received by the card, even those that are not directed to it. It may mean that a sniffer is running on your machine.

Note that this check is setted up to be run every minute.

3.19 Listening port check

Issues a warning with all listening ports.

3.20 Passwd file integrity check

Verify that each user has a password (no blank password) and if it is shadowed.

3.21 Shadow file integrity check

Verify that each user into the shadow file has a password (no blank password).

3.22 System security check every midnight

All previous checks will be performed everyday at midnight. This relies on the addition of cron scripts in crontab file.

3.23 All system events additionally logged to /dev/tty12

All system messages directed to syslog are copied to tty12 console.

3.24 Only root can shutdown

You must be root (or referenced into /etc/shutdown.allow) and logged into a console to be able to shutdown or reboot the machine.

3.25 Services not known disabled

All services not contained into "/etc/security/msec/init-sh/server.4" for level 4 or "server.5" for level 5 will be disabled. They are not removed, but simply not started when loading a runlevel. If you need some of them, just add them again with the "chkconfig" utility (you might also need to restart them with init scripts in /etc/rc.d/init.d/).

3.26 Boot password

Allows you to setup a password for Lilo. Prevents (unexperienced) people from rebooting the machine, but in the other hand, the machine won't be able to reboot by itself.

3.27 Grant connection to

- all : All computers are allowed to connect to open ports.
- local : Only the localhost is allowed to connect to open ports.
- none : No computers are allowed to connect to open ports.

4 ToDo

- Automatic tty locking (unlock by passwd) after X time of inactivity.

- In high security level, only user having access to group "sugrp" can use the su command.

5 Author

Vandoorselaere Yoann <yoann@mandrakesoft.com>