Sentry: a multipourpose GNU/Linux...

[In this short article I'll try to explain how to made a good use of Sentry: an useful GNU/Linux distribution that can be considered like a swiss-knife tool. I'll also describe my setup experience with this distro (followed by a case-study to solve an inusual need).]

What's sentry:

As described in product's FAQ the "Sentry Firewall CD" is a bootable GNU/Linux based CD-ROM, useful for a number of different needs: from firewall to application server.
What is meant for bootable CD-ROM is a media that contains an Operative System full installation and has a boot sector so, if PC BIOS allow it (and most recent ones do), it is possible to start PC directly from CD-ROM.
The advantage to operate from CD is due, before all, to the unchangeability of the media and the consequent fast recovery of system. And therefore is impossible for a cracker (not "haker" as some newspaper define those informatical intruders) to destroy the system itself in a definitive way.
One of preferred activities of cracker is, infact, the installation of a rootkit as soon as an host ahs been compromised.
A root kit is, in simple words, a kit of modified programs and system utilities that allow an easy access to compromised system masking, at the same time, crackers activities.
As You can understand these programs were, usually, installed on the compromised system hard disk and are very hard to remove so often is required to reinstall all system to gain a new safe situation.
With Sentry the O.S. is burned in a CD so it's impossible to change. To recover a compromised system is easy: it's necessary to reboot PC and to give it a better security level.
Another great advantage is given from the fact that the O.S: is not in the hard-disk that is one of the PC components tath more frequently breackdown.
To this point a flame can born about fact that also CD-player is a component with a mechanical part and therefore can easily breackdown (sometimes more frequently than an hard-disk). I would only to point out that You can have a great number of copies of the CD and CD-players at the cost of a single HD.

The original distribution on wich Sentry was based on was Slackware and this was also the version I used. Nowaday a Red Hat based Sentry is at Your disposal.

Preparing CD:

Some of following steps are keept from Sentry How-to.

1. Download ISO image of CD from www.SentryFirewall.com.
   File that You download come in a .gz or .bz2 compressed format; so You must
2. decompress it in a directory You chose:

   ```
   gzip -d sentrycd.iso.gz
   ```

3. Beeing a product that can be used as firewall (but it shoul be done every time) it's better to verify file integrity as follow:

   ```
   md5sum -b sentrycd.iso
   ```

4. Then You can burn it on a CD

   ```
   cdrecord -v -data speed=XXX dev=YYY sentrycd.iso
   ```

   Where XXX is burning speed and YYY Your CD-recorder device path.

It'is possible that You have not near You a GNU/Linux PC or (like me) You have not a cd-recorder in Your Linux box.
So You can uncompress your ISO image in Win with a program like Freezip (freeware) and then to burn CD with a Windows CD-recording program.

Hardware requirements and configuration

Once You get the CD You'll need a PC with, at least, two nics (network adapters). The PC should be able to boot from CD (older BIOS don't do it). At least 32Mb RAM are required but 64Mb are confortable. It's useful a floppy so save Your personal configuration. It's, instead, suggested to disconnect the HD drive, if present, (You can recycle it in another PC) so it could'nt be the base for an attacker to modify Your system.
PC must be configured (eventually setting BIOS) to boot from CD as 1st device and floppy as 2nd device, with no boot from hard-disk.To note that original how-to requires, as minimal configuration, the *"easy access to coffee, tea, soda or any other equivalent stimulant"* :-). In my opinion a good quantity of patience is better... and I 'll explain why later on.

Configuration e personalizzation

The requirement of a floppy is obvious: it reppresents and contains the personal configuration and specializzation of Your SENTRY system respect to standard one in the iso image of CD.
Floppy is detected at boot time, then mounted in `/floppy` and a file named `sentry.conf` is searched. If it's present it's configuration contains some commands thath overvrites CD configurations files with those ones that comes in the floppy itself. detailled instructions on possible command are in the original How-to thet's on the site and in the CD.
If any configuration problem occour You can restart from scratch simply booting from CD and then mounting floppy to modify it.

Once the system is started from CD You must Login as `root` with password `sentry`.
From here You should remember that every modification to system that is unsaved on floppy is lost as soon as You restart the system. That's why You're working with a ramdisk that is a volatile memory.
I assure that I forget to save a lot of times and that means I restarted my work every time so my suggest to provide a lot of patience.
Let's now modify default passwords for two standard users that are root and sentry: commands are:

```
passwd root
```

and

```
passwd sentry
```

as soon as the system ask You must supply new password and then re-enter it to validate input.
Then it's necessary to format floppy to write in it configuration files:
let's format:

```
fdformat /dev/fd0
```

and create filesystem:

```
mkfs -t ext2 /dev/fd0
```

from this point we can use the utility that allow to create floppy configuration file:

```
mkconfig
```

Configuration files written in floppy will contain password file

```
passwd
```

with users and passwords updated.
It's also possible to write by hand configuration files copying default structure with:

```
cp ~/SENTRY/scripts/cd-config/sentry.conf /floppy/
```

You should ever remember to copy files as soon as they're modified so, as example, once You modify users or passwords it'll became necessary to copy related files from ramdisk (the filesystem) to floppy:

```
cp /etc/passwd /floppy/config/passwd
cp /etc/shadow /floppy/config/shadow
```

It's necessary to specify that not all floppy files are read at boot and they don't go automatically to overwrite CD informations, but only those ones specified in file `/floppy/sentry.conf`. So it'll be useful to immediatly specify, to system, to read new users and passwords. Let's open the file with an editor:

```
vi /floppy/sentry.conf
```

. and insert following modifications:

```
--------
passwd= /floppy/config/passwd
shadow= /floppy/config/shadow
--------
```

Network configuration

Let's pass to configure first nic.It'll be necessary to modify file `/etc/rc.inet1` to insert appropriate data at following rows:

```
IPADDR=
NETMASK=
NETWORK=
BROADCAST=
```

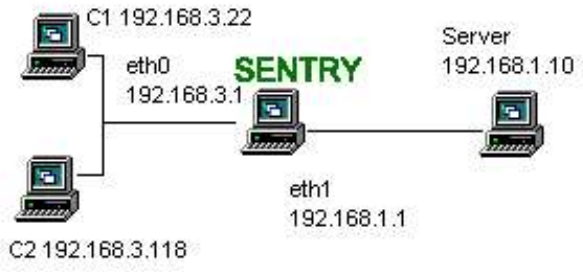
that are IP adresses of host, network, netmask, etc.
then is needed to copy file `/etc/rc.inet1` from ramdisk to floppy and to configure file `/floppy/sentry.conf` adding the row

```
--------
rc.inet1= /floppy/config/rc.inet1
--------
```

You must repeat operation for every nic that is for every file `/etc/rc.inet2` etc.

An application...

As pointed out in the introduction SENTRY CD is supplied with a good number of applications/services that can be useful.
Personally I used it in a situation where I need to control in detail the access to an application server from a network segment to another of my intranet.
Following scheme can be useful to explay the whole thing:



It was necessary to me to limit number of users that can connect to server, to control network traffic and in necessity case to drop (on fly) the service. It was also required that users can use the application only at a determinated time of the day.

With those specifications I found useful to connect between server and the rest of net a PC with "filtering" functions. I've heard about SENTRY and it seems to me useful to verify as it runs.
So I break intranet in two areas and I used SENTRY PC as router. One area is represented only from application server but to divide it from network means to regulate better the access.

Then I verified that SENTRY PC didn't had active unneeded services. I don't want to trust myself with a "read config and be peaceful" method so I used a good network scanner as (NESSUS) to test system. Good news are that SENTRY don't activate any default service (that is "if You need a service You must configure it").
In my case I need only routing and no other service and I already had configured nics as I explained.
Just to give a name to stuffs, my clients side corresponded to SENTRY network adapter eth0 configured as follows:

```
IPADDR=192.168.3.1
NETMASK=255.255.255.0
NETWORK=192.168.3.0
BROADCAST=192.168.3.255
```

while server side was SENTRY eth1 configured as:

```
IPADDR=192.168.1.1
NETMASK=255.255.255.0
NETWORK=192.168.1.0
BROADCAST=192.168.1.255
```

d server has `IPADDR=192.168.1.10` and two test clients was:
C1 with `IPADDR=192.168.3.22` and C2 with `IPADDR=192.168.3.118`

To this point it's necessary to activate routing between networks. On SENTRY PC let's add following rules:

```
route add 192.168.1.10 eth1
route add default 192.168.1.0
route add 192.168.3.22 eth0
route add 192.168.3.118 eth0
```

that shown to PC as to reach other hosts and only those ones. In addiction we imposed that default routing for outgoing packets is eth1 where no ather rules indicate otherwise.
I go on in remembering thet modifications go away on reboot. So to avoid flame'n'fury after positive tests ever remember to save modifications on floppy. I chose to write routing rules at the end of file `rc.inet1= /floppy/config/rc.inet1` where a default network rule was already present.
Let's add in hosts tables the due specifications: in `/etc/hosts` rows related to clients and server...

```
---------
C1 192.168.3.22
C2 192.168.3.118
Server 192.168.1.10
---------
```

In table `/etc/hosts.deny` is useful to add the row:

```
deny ALL:ALL
```

that deny access to any service for any host that is not in table `/etc/host.allow` where we write:

```
192.168.1.10 ALL
192.168.3.22 ALL
192.168.3.118 ALL
```

also in this case remember to copy files from directory /etc/ to floppy (in `/floppy/config/`) and to configure file `/floppy/sentry.conf` to allow files to be read at boot time.

To avoid in a drastic way access I chose a simple solution: I scheduled (with cron) two commands that at a determinate time "disable" network:

```
ifconfig eth0 down
ifconfig eth1 down
```

I should have scheduled two other command to restart network but I preferred to schedule a `reboot` 5 minutes before work time begin. Naturally I provided to overwrite default cron table with the one saved on floppy.
About this I must report that my version of SENTRY has an error in substitution command for cron table so I need some scripts to recover bug. In new SENTRY versions this bug is not present.

The result of operation described is a PC that allows only determinated clients to connect to server. In necessity case I can modify route and hosts tables to allow or remove the permissions to ather PC's or to limit only some network protocols. tanks to a copy of CD and an updated backup of floppy I can activate in case of fall a PC with same functions in some minutes (it's required only to transfer nics or to find some compatible ones). If I need it nothing can avoid me to use firewalling services in CD to "hardening defence".
As last node I want to report about an utility (`netwatch`) that allow to view (in text mode) some counters of packets travelling in the network segments.
Who has capabilities can also to mount CD iso image, copy it in a disk and modify parts that he needs to get a personalized system ready to use that can be re-converted in a CD.
For possible applications the limit is Your fantasy...

di Rudi Giacomini Pilon