Hardering via Sysctl

Sysctl (https://www.kernel.org/doc/Documentation/sysctl) is an mechanism for examining and even dynamically (that is: "on the fly") changing kernel parameters (which will applied immediately).. These parameters describe tunable limits (such as the size of a shared memory segment, the number of threads the operating system will use as an NFS client, the maximum number of processes on the system, etc) or describe, enable or disable behaviors (such as IP forwarding, security restrictions on the superuser, etc). All of this without having to rebuild the kernel or reboot the computer.

Sysctl provides an interface mechanism to interact with it which is implemented as a temporary virtual filesystem ("procfs") mounted under the "/proc/sys" directory. This means checking the value of some parameter requires opening a file in this virtual filesystem, reading its contents, parsing them and closing the file.The *sysctl* command (from "procps-ng" package) is used to view and set these kernel settings.

*Para ver todos los valores actuales (algunos de ellos solo están visibles si se es root): *sysctl -a*
NOTA:Se puede filtrar la salida anterior añadiendo el parámetro *-r expReg*
*Para ver el valor de una clave en concreto: *sysctl net.ipv4.icmp_echo_ignore_all*
*Si solo se quiere ver el valor, sin su nombre:*sysctl -n {net.ipv4.icmp_echo_ignore_all | -a [-r exp]}*
*Para modificar el valor de una clave en concreto por el indicado (solo algunas admiten ser modificadas): *sudo sysctl -w net.ipv4.icmp_echo_ignore_all=1*

In this case, "1" is on and "0" is off, so, with the above command we instructed the kernel to ignore all icmp echo requests. Related to this, you should know that all of the keys have a represention inside "/proc/sys" folder following the folder tree shown by its dotted name; that is: the value of the key *net.ipv4.icmp_echo_ignore_all* is "stored" inside the virtual "/proc/sys/net/ipv4/icmp_echo_ignore_all" file. So another way to see its value could be executing *cat /proc/sys/net/ipv4/icmp_echo_ignore_all* and another way to temporarily change it could be executing (as root): *echo 1 > /proc/sys/net/ipv4/icmp_echo_ignore_all*

Changes made by *sysctl -w* or similar commands are immediately applied, but they will only last ‘till the next boot because "/proc/sys" is a virtual filesystem, so it is not a permanent change. If you want to make a change permanent, or at least until you change it again, you will need to edit or create the file "**/etc/sysctl.conf**" and add the changes there editing/adding a line like this (you can see it contains a list of variable assignments, separated by newlines; empty lines and lines whose first non-whitespace character is "#" or ";" are ignored): *net.ipv4.icmp_echo_ignore_all=1*

Note, however, newer Systemd systems only apply settings from "**/usr/lib/sysctl.d/*.conf**" and "**/etc/sysctl.d/*.conf**" files. The naming and source directory decide the order of processing, which is important since the last parameter processed may override earlier ones. For example, parameters in a /usr/lib/sysctl.d/50-default.conf will be overriden by equal parameters in /etc/sysctl.d/50-default.conf and any configuration file processed later from both directories. Knowing this, and as vendors settings live in /usr/lib/sysctl.d/*.conf files, to override a whole vendor file, you should simply create a new file with the same in "/etc/sysctl.d" folder and put new settings there; to override only specific settings, instead, you should add a file with a lexically later name in "/etc/sysctl.d" folder and put new settings there.

At boot, the *systemd-sysctl* service reads all these configuration files from the above directories to configure that kernel parameters. But if you want to apply immediately the changes introduced in these configuration files without having to reboot the system, you can execute: *sudo sysctl --system* (or, if you only want to reload some changes made in a specific file, *sudo systctl -p /path/file.conf*)

NOTA: If the administrator wants to disable a configuration file supplied by the vendor, the recommended way is to place a symlink to "/dev/null" in "/etc/sysctl.d" folder with the same filename as the vendor configuration file (if the vendor configuration file was included in the initrd image, the image had to be regenerated, though).

NOTA: Many sysctl parameters can only be applied when certain kernel modules are loaded. For example parameters in /proc/sys/net/bridge/* depend on the br_netfilter module; if a module is not already loaded, referring sysctl parameters will then *silently* not be applied. Beware of modules are usually loaded on demand (when certain hardware is plugged in or network brought up); this means that *systemd-sysctl* service (which runs during early boot) will not configure such parameters if they become available after it has run. So, to set such parameters, it is recommended to add an Udev rule to

set those parameters when they become available. Alternatively, a slightly simpler and less efficient option is to add the module to "modules-load.d" folder, causing it to be loaded statically before sysctl settings are applied (see example below).

NOTA: *systemd-sysctl.service* is an early boot service that configures sysctl kernel parameters by invoking the */usr/lib/systemd/systemd-sysctl* binary. When invoked with no arguments, this binary applies all directives from configuration files listed in "sysctl.d" folders. If one or more filenames are passed on the command line, only the directives in these files are applied. In addition, --prefix= option may be used to limit which sysctl settings are applied.

Per veure una llista de paràmetres interessants implementats per defecte es pot consultar, a sistemes Fedora, l'arxiu "/usr/lib/sysctl.d/50-default.conf". Allà podem trobar, per exemple, els paràmetres *fs.protected_hardlinks* o *fs.protected_symlinks* (els quals, si valen 1, permeten crear links només si de l'arxiu original s'és el propietari i es tenen permisos de lectura i escriptura -en el cas del "hard links"- o si el procés que segueix el link n'és el propietari -en el cas del "soft links"-). Altres paràmetres estan relacionats amb el control de la xarxa, com ara *net.ipv4.icmp_echo_ignore_broadcasts*, *net.ipv4.conf.all.forwarding*, *net.ipv4.ip_forward*, *net.ipv4.conf.all.accept_redirects*, *net.ipv4.conf.all.accept_source_route* , etc. Per veure més informació, consulteu https://www.kernel.org/doc/html/latest/admin-guide/sysctl/index.html#introduction (i en el cas concret del control de xarxa, https://www.kernel.org/doc/Documentation/networking/ip-sysctl.txt)

NOTA: Alguns tutorials més"d'estar per casa" que mostren l'ús d'alguns dels paràmetres més habituals són, entre d'altres, https://www.cyberciti.biz/faq/linux-kernel-etcsysctl-conf-security-hardening o https://www.sysadmin.md/hardening-existing-linux-server-via-sysctl-parameters.html