Hardening di un sistema Debian GNU/Linux

Principali passi per la configurazione e l'ottimizzazione in ottica di sicurezza (hardening) di un server basato su Debian GNU/Linux per fornire i servizi più comuni.

Verranno analizzate le principali modifiche da apportare rispetto ad un'installazione "by-default", espresse alcune considerazioni e valutazioni in ottica di sicurezza, analizzati alcuni strumenti utili per rafforzare le difese e monitorare lo stato del sistema.

copia & incolla (molto)

commentato (poco) di

“Securing Debian Manual”

apt-get install harden-doc

26 Novembre 2004

Security Day, Cesena

27 Novembre 2004

Linux Day, Rimini

Igor Falcomatà - koba@sikurezza.org

Hardening

From Wikipedia, the free encyclopedia

“In computing, **hardening** is the process of securing a system. This work is especially done to protect systems against attackers.

This would typically include removal of unnecessary usernames or logins and the disabling or removal of unnecessary services. On a typical Windows server, one example would be the disabling of the "print spooler" as this may not be needed.

There are various methods of hardening Unix and Linux systems. This may involve, among other measures, applying a patch to the kernel such as Exec Shield or PaX; closing open network ports; and setting up intrusion-detection systems (such as firewalls) and intrusion-prevention systems.

See also: Computer Security, Computer Network Security, Security Policy, Linux: Security Enhanced Linux”

Disclaimer

"Please (don't) try this at home"

- Alcune o tutte le procedure ed i suggerimenti riportati potrebbero danneggiare irreparabilmente i vostri dati, il vostro sistema, il vostro tostapane ed il vostro conto in banca...
- MAI (ho detto MAI) eseguire operazioni di hardening su un sistema 'in produzione' senza sapere esattamente cosa si sta facendo
- Provate e riprovate i singoli passi su sistemi di prova e cmq procedete per passi graduali
- Tenete traccia di tutte le operazioni che effettuate ("diario di bordo") in modo da poter tornare facilmente sui vostri passi (man script)
- Alcuni software e procedure (anche relativi al sistema operativo stesso) potrebbero non funzionare correttamente
- Casco ben allacciato in testa e prudenza, sempre!

Securing Debian Manual rev 2.99

Javier Fernández-Sanguino Peña <jfs@computer.org>

“This document describes security in the Debian project. Starting with the process of securing and hardening the default Debian GNU/Linux distribution installation. It also covers some of the common tasks to set up a secure network environment using Debian GNU/Linux, gives additional information on the security tools available and talks about how security is enforced in Debian by the security team.”

“One of the hardest things about writing security documents is that every case is unique. Two things you have to pay attention to are the threat environment and the security needs of the individual site, host, or network. For instance, the security needs of a home user are completely different from a network in a bank.”

“Securing Debian is not very different from securing any other system; in order to do it properly, you must first decide what you intend to do with it. After this, you will have to consider that the following tasks need to be taken care of if you want a really secure system.”

http://www.debian.org/doc/manuals/securing-debian-howto/

Perché Debian GNU/Linux?

- “Debian problems are always handled openly, even security related. Security issues are discussed openly on the debian-security mailing list. Debian Security Advisories are sent to public mailing lists (both internal and external) and are published on the public server. As the Debian Social Contract (http://www.debian.org/social_ contract) states:

  We Won t Hide Problems

  We will keep our entire bug-report database open for public view at all times. Reports that users file on-line will immediately become visible to others.”

- “Security updates are the first priority. When a security problem arises in a Debian package, the security update is prepared as fast as possible and distributed for our stable and unstable releases, including all architectures.”

- “Information regarding security is centralized in a single point, http://security. debian.org/.”

Chi ben comincia...

- “Before you install any operating system on your computer, set up a BIOS password. After installation (once you have enabled bootup from the hard disk) you should go back to the BIOS and change the boot sequence to disable booting from floppy, cdrom and other devices that shouldn t boot. Otherwise a cracker only needs physical access and a boot disk to access your entire system.” **[più in generale, valutare il “Layer 0” :)]**
- “Disabling booting unless a password is supplied is even better. This can be very effective if you run a server, because it is not rebooted very often. The downside to this tactic is that rebooting requires human intervention which can cause problems if the machine is not easily accessible.” **[sconsigliabile]**
- “Note: many BIOSes have well known default master passwords, and applications also exist to retrieve the passwords from the BIOS. Corollary: don t depend on this measure to secure console access to system.” **[avendo accesso fisico al sistema, è possibile 'resettare' la password del BIOS, oppure accedere fisicamente ai dischi]**

Partizionamento dei dischi

“An intelligent partition scheme depends on how the machine is used. A good rule of thumb is to be fairly liberal with your partitions and to pay attention to the following factors:”

- “Any directory tree which a user has write permissions to, such as e.g. /home, /tmp and /var/tmp/, should be on a separate partition. This reduces the risk of a user DoS by filling up your / mount point and rendering the system unusable (Note: this is not strictly true, since there is always some space reserved for root which a normal user cannot fill) as well as avoiding hardlink attacks”
- “Any partition which can fluctuate, e.g. /var (especially /var/log) should also be on a separate partition. On a Debian system, you should create /var a little bit bigger than on other systems, because downloaded packages (the apt cache) are stored in /var/cache/apt/archives.”

Partizionamento dei dischi

- “Any partition where you want to install non-distribution software should be on a separate partition. According to the File Hierarchy Standard, this is /opt or /usr/local. If these are separate partitions, they will not be erased if you (have to) reinstall Debian itself.”
- “From a security point of view, it makes sense to try to move static data to its own partition, and then mount that partition read-only. Better yet, put the data on read-only media. See below for more details.”

“In the case of a mail server it is important to have a separate partition for the mail spool. Remote users (either knowingly or unknowingly) can fill the mail spool (/var/mail and/or /var/spool/mail). If the spool is on a separate partition, this situation will not render the system unusable. Otherwise (if the spool directory is on the same partition as /var) the system might have important problems: log entries will not be created, packages can not be installed, and some programs might even have problems starting up (if they use /var/run).”

Scelta del filesystem

"During the system partitioning you also have to decide which file system you want to use. The default file system selected in the Debian installation for Linux partitions is ext2. However, it is recommended you switch to a journalling file system, such as ext3, reiserfs, jfs or xfs, to minimize the problems derived from a system crash in the following cases:"

- "for laptops in all the file systems installed. That way if you run out of battery unexpectedly or the system freezes due to a hardware issue (such as X configuration which is somewhat common) you will be less likely to lose data during a hardware reboot."
- "for production systems which store large amounts of data (like mail servers, ftp servers, network file systems. . .) it is recommended on these partitions. That way, in the event of a system crash, the server will take less time to recover and check the file systems, and data loss will be less likely."

Scelta del filesystem

“Leaving aside the performance issues regarding journalling file systems (since this sometimes can turn into a religious war), it is usually better to use the ext3 file system. The reason for this is that it is backwards compatible with ext2, so if there are any issues with the journalling you can disable it and still have a working file system. Also, if you need to recover the system with a bootdisk (or CDROM) you do not need a custom kernel. If the kernel is 2.4 ext3 support is already available, if it is a 2.2 kernel you will be able to boot the file system even if you lose journalling capabilities. If you are using other journalling file systems you will find that you might not be able to recover unless you have a 2.4 kernel with the needed modules built-in. If you are stuck with a 2.2 kernel in the rescue disk it might even be more difficult to have it access reiserfs or xfs.”

Non attaccare subito il sistema ad Internet.. oppure fatelo solo se protetto...

“The system should not be immediately connected to the Internet during installation. This could sound stupid but network installation is a common method. Since the system will install and activate services immediately, if the system is connected to the Internet and the services are not properly configured you are opening it to attack.

Also note that some services might have security vulnerabilities not fixed in the packages you are using for installation. This is usually true if you are installing from old media (like CDROMs). In this case, the system could even be compromised before you finish installation!

Since Debian installation and upgrades can be done over the Internet you might think it is a good idea to use this feature on installation. If the system is going to be directly connected to the Internet (and not protected by a firewall or NAT), it is best to install without connection to the Internet, using a local packages mirror for both the Debian package sources and the security updates.”

Password...
(avete visto "War Games"?)

"Setting a good root password is the most basic requirement for having a secure system. See passwd(1) for some hints on how to create good passwords. You can also use an automatic password generation program to do this for you (see Generating user passwords on page 53)."

"At the end of the installation, you will be asked if shadow passwords should be enabled. Answer yes to this question, so passwords will be kept in the file /etc/shadow."

"Furthermore, you are queried during installation whether you want to use MD5 hashed passwords. This is generally a very good idea since it allows longer passwords and better encryption. MD5 allows for passwords longer than 8 characters." "[Note: the default configuration in Debian, even when activating MD5 passwords, does not modify the previously set max value." [editare /etc/pam.d:]

"This, as a matter of fact, modifies all files under /etc/pam.d by substituting the password line and include md5 in it:

password required pam_unix.so md5 nullok obscure min=6 max=16" [max=64]

Servizi attivi

“Services are programmes such as ftp servers and web servers. Since they have to be listening for incoming connections that request the service, external computers can connect to yours. Services are sometimes vulnerable (i.e. can be compromised under a given attack) and are hence a security risk.

You should not install services which are not needed on your machine. Every installed service might introduce new, perhaps not obvious (or known), security holes on your computer.

As you may already know, when you install a given service the default behavior is to activate it. In a default Debian installation, with no services installed, the footprint of running services is quite low and it s even lower when talking about services offered to the network. The footprint in Debian 2.1 wasn t as tight as in Debian 2.2 (some inetd services were enabled by default) and in Debian 2.2 the rpc portmapper is enabled upon installation. Rpc is installed by defaultbecause it is needed for many services, for example NFS, to run on a given system. It can be easily removed, however, see Disabling daemon services ...”

Servizi attivi

“When you install a new network-related service (daemon) in your Debian GNU/Linux system it can be enabled in two ways: through the inetd superdaemon (i.e. a line will be added to /etc/inetd.conf) or through a standalone program that binds itself to your network interfaces. Standalone programs are controlled through the /etc/init.d files, which are called at boot time through the SysV mechanism (or an alternative one) by using symlinks in /etc /rc?.d/* (for more information on how this is done read /usr/share/doc/sysvinit /README.runlevels.gz).

If you want to keep some services but use them rarely, use the update-commands, e.g. update-inetd and update-rc.d to remove them from the startup process.”

Disabilitare i servizi

“Disabling a daemon service is quite simple. There are different methods:

- remove links from /etc/rc${runlevel}.d/ or rename the links (so that they do not begin with S)
- move the script file (/etc/init.d/_service_name_) to another name (for example /etc/init.d/OFF._service_name_)
- remove the execute permission from the /etc/init.d/_service_name_ file.
- edit the /etc/init.d/_service_name_ script to have it stop immediately.”

“Please note that, if you are not using file-rc, update-rc.d -f _service_ remove will not work properly, since all links are removed, upon re-installation or upgrade of the package these links will be re-generated (probably not what you wanted). If you think this is not intuitive you are probably right”

inetd? Nel 2004?

“You should stop all unneeded services on your system, like echo, chargen, discard, daytime, time, talk, ntalk and r-services (rsh, rlogin and rcp) which are considered HIGHLY insecure (use ssh instead). After disabling those, you should check if you really need the inetd daemon. Many people prefer to use daemons instead of calling services via inetd. Denial of Service possibilities exist against inetd, which can increase the machine s load tremendously. If you still want to run some kind of inetd service, switch to a more configurable inet daemon like xinetd or rlinetd.

You can disable services by editing /etc/inetd.conf directly, but Debian provides a better alternative: update-inetd (which comments the services in a way that it can easily be turned on again). You could remove the telnet daemon by executing this commands to change the config file and to restart the daemon (in this case the telnet service is disabled):

/usr/sbin/update-inetd --disable telnet”

Installare solo il software necessario

“Debian comes with a lot of software, for example the Debian 3.0 woody release includes almost 6 CD-ROMs of software and thousands of packages. With so much software, and even if the base system installation is quite reduced you might get carried away and install more than is really needed for your system.” [evitare tasksel]

“Since you already know what the system is for (don t you?) you should only install software that is really needed for it to work. Any unnecessary tool that is installed might be used by a user that wants to compromise the system or by an external intruder that has gotten shell access (or remote code execution through an exploitable service).”

[meglio adottare una politica di installazione minimale, aggiungendo solo le componenti che servono.. è ovviamente più faticoso. Potrebbe anche essere utile disabilitare l'accesso ai binari 'potenzialmente pericolosi' tramite i permessi sul file system (solo alcuni gruppi di utenti, etc.) o meccanismi di ACL vari]

Installare solo il software necessario

“The presence, for example, of development utilities (a C compiler) or interpreted languages (such as perl - but see below -, python, tcl. . .) may help an attacker compromise the system even further:

- allowing him to do privilege escalation. It s easier, for example, to run local exploits in the system if there is a debugger and compiler ready to compile and test them!
- providing tools that could help the attacker to use the compromised system as a base of attack against other systems

Of course, an intruder with local shell access can download his own set of tools and execute them, and even the shell itself can be used to make complex programs. Removing unnecesary software will not help prevent the problem but will make it slightly more difficult for an attacker to proceed (and some might give up in this situation looking for easier targets). So, if you leave tools in a production system that could be used to remotely attack systems [..] you can expect an intruder to use them too if available.”

Debian security mailing list

“It is never wrong to take a look at either the debian-security-announce mailing list, where advisories and fixes to released packages are announced by the Debian security team, or at mailto:debian-security@lists.debian.org, where you can participate in discussions about things related to Debian security.

In order to receive important security update alerts, send an email to debian-securityannounce-request@lists.debian.org with the word subscribe in the subject line. You can also subscribe to this moderated email list via the web page at http://www.debian.org/MailingLists/subscribe

This mailing list has very low volume, and by subscribing to it you will be immediately alerted of security updates for the Debian distribution. This allows you to quickly download new packages with security bug fixes, which is very important in maintaining a secure system.”

[altre liste interessanti: bugtraq (http:/www.securityfocus.com/archive), VulnWatch (http://www.vulnwatch.org/), Secunia Advisories (http://secunia.com/)]

Security update

“As soon as new security bugs are detected in packages, Debian maintainers and upstream authors generally patch them within days or even hours. After the bug is fixed, a new package is provided on http://security.debian.org.“

“To manually update the system, put the following line in your sources.list and you will get security updates automatically, whenever you update your system.

deb http://security.debian.org/ stable/updates main contrib non-free

apt-get update

apt-get upgrade”

[-u, --show-upgraded

Show upgraded packages; Print out a list of all packages that are to be upgraded. Configuration Item: APT::Get::Show-Upgraded.

-s, --simulate, --just-print, --dry-run, --recon, --no-act

No action; perform a simulation of events that would occur but do not actually change the system. Configuration Item: APT::Get::Simulate.”]

Password a LILO o GRUB

“Anybody can easily get a root-shell and change your passwords by entering <name-of-your-bootimage> init=/bin/sh at the boot prompt. After changing the passwords and rebooting the system, the person has unlimited root-access and can do anything he/she wants to the system. After this procedure you will not have root access to your system, as you do not know the root password.

To make sure that this cannot happen, you should set a password for the boot loader. You can choose between a global password or a password for a certain image.”

“Linux 2.4 kernels provide a way to access a root shell while booting which will be presented just after loading the cramfs file system. A message will appear to permit the administrator to enter an executable shell with root permissions, this shell can be used to manually load modules when autodetection fails. This behavior is the default for initrd s linuxrc.”

“The default MBR in Debian before version 2.2 did not act as a usual master boot record and left open a method to easily break into a system”

Considerazioni relative alla console

“Some security policies might force administrators to log in to the system through the console with their user/password and then become superuser (with su or sudo). This policy is implemented in Debian by editing the /etc/login.defs file or /etc/securetty when using PAM.”

“When using PAM, other changes to the login process, which might include restrictions to users and groups at given times, can be configured in /etc/pam.d/login. An interesting feature that can be disabled is the possibility to login with null (blank) passwords. This feature can be limited by removing nullok from the line:

auth required pam_unix.so nullok”

“If your system has a keyboard attached to it anyone (yes anyone) can reboot the system through it without login to the system. This might, or might not, adhere to your security policy. If you want to restrict this, you must check the /etc/inittab so that the line that includes ctrlaltdel calls shutdown with the -a switch (remember to run init q after making any changes to this file).”

Montare le partizioni

“When mounting an ext2 partition, there are several additional options you can apply to the mount call or to /etc/fstab. For instance, this is my fstab entry for the /tmp partition:

/dev/hda7 /tmp ext2 defaults,nosuid,noexec,nodev 0 2

You see the difference in the options sections. The option nosuid ignores the setuid and setgid bits completely, while noexec forbids execution of any program on that mount point, and nodev, ignores devices. This sounds great, but it

- only applies to ext2 file systems” [?!]
- “can be circumvented easily” [fixato nel 2.6]

Per esempio:

- noexec (/boot, /tmp, /var/tmp, /home, /var/log, ...)
- nodev (come sopra + /var, /usr/, /usr/local, /opt, ...)
- nosuid (/boot, /tmp, /var/tmp, /home, /var/log, ...)

e ovviamente tutti i mount controllabili dagli utenti (floppy, cd, usb, rete, etc.) (l'opzione “users” implica già noexec, nosuid, nodev)

Montare le partizioni

“The following is a more thorough example. A note, though: /var could be set noexec, but some software keeps its programs under in /var. The same applies to the nosuid option.”
[sconsigliabile avere /var nosuid e/o noexec, sotto Debian; apt non funzionerebbe correttamente]

“Be careful if setting /tmp noexec when you want to install new software, since some programs might use it for installation. Apt is one such program (see http://bugs.debian.org/116448) if not configured properly APT::ExtractTemplates::TempDir (see apt-extracttemplates(1)). You can set this variable in /etc/apt/apt.conf to another directory with exec privileges other than /tmp.”

Pluggable Authentication Modules

“PAM (Pluggable Authentication Modules) allows system administrators to choose how applications authenticate users. Note that PAM can do nothing unless an application is compiled with support for PAM.”

”PAM offers you the possibility to go through several authentication steps at once, without the user s knowledge. You could authenticate against a Berkeley database and against the normal passwd file, and the user only logs in if he authenticates correct in both. You can restrict a lot with PAM, just as you can open your system doors very wide. So be careful. A typical configuration line has a control field as its second element. Generally it should be set to requisite, which returns a login failure if one module fails.”

[le librerie PAM (ed i relaviti moduli) permettono di impostare numerose tipologie di autenticazioni (centralizzate, smartcard, one-time, etc.) nonché restrizioni, quali per esempio limiti sull'utilizzo delle risorse, limiti sull'accesso a programmi quali su e sudo, meccanismi di verifica della robustezza delle password, etc. etc. etc. etc. etc.]

[valutare anche la gestione delle risorse e dei limiti: limits.conf]

Gestione degli utenti

- creare ed abilitare solamente gli utenti necessari, rimuoverli o disabilitarli quando non servono; soprattutto gli account di test/prova/temporanei/etc.
- proibire password vuote, eventualmente forzare la robustezza (pam, cracklibs)
- impostare una scadenza sulle password (ad esclusione di root)
- in caso di reti complesse (più di due macchine :), utilizzare strumenti di autenticazione centralizzata
- impostare limiti sull'utilizzo delle risorse (limits, quota)
- negare l'accesso alla shell agli utenti (p. es. per gli utenti di sola posta attraverso funzionalità di “pop toaster”/virtualusers; oppure attraverso scponly o simile, restricted shells, etc.)
- abilitare funzioni di accounting/auditing per gli utenti locali con accesso alla shell
- abilitare strumenti per il logout automatico degli utenti

Gestione degli utenti

- permessi di accesso alle home directories /home/* e a /root (755 -> 700 o simile) [questo impedisce la visualizzazione delle homepages degli utenti via web, qualora si utilizzi mod_userdir]
- impostare umask restrittive di default (027 o 077)
- utilizzare directory tmp separate (p. es. /tmp/utente con permessi 700)
- non usare root per le attività 'normali' (vedi su e/o sudo)
- limitare l'accesso ad eventuali servizi da remoto agli utenti “di sistema” (p. es. /etc/ftpusers, ma voi non utilizzate ftp, vero?; oppure scp, etc.)
- modificare la shell e disabilitare gli account “by default” di Debian (vedi FAQ)

Gestione dei software e dei protocolli

- evitare software da fonti “non affidabili”
- rivedere e valutare le configurazioni di default
- software installati “a mano” vanno aggiornati e mantenuti “a mano” (e gli advisories?)
- utilizzare sempre software/protocolli che utilizzino traffico cifrato (telnet -> ssh, pop3 -> pop3s, imap -> imaps, http -> https, ftp -> ftp su ssl oppure sftp/scp, etc.)
- oppure le funzionalità di tunnel di ssh (p. es. per X11)
- oppure software di VPN (freeswan/superswan, openvpn, etc.)
- se proprio si inviano password in chiaro, è opportuno utilizzare meccanismi “one-time” o comunque password “dedicate” [ma ri-valutate i tre punti precedenti...]
- evitare di attivare servizi inutili (netstat -anp)
- se i servizi sono necessari alla stazione stessa (o nel caso di stazioni multihomed) abilitare il “binding” solo sull'interfaccia necessaria (localhost, lan, etc.) oppure filtrarne l'accesso con tcpwrappers e/o firewalling
- abilitare il firewalling del traffico in ingresso ed in uscita

Permessi sul filesystem

- di default Debian è poco restrittiva nella gestione dei permessi di accesso a directory, file ed eseguibili
- utenti con accesso locale o remoto (senza chroot) possono vedere gran parte dei file di configurazione, dei log, etc.
- possono anche accedere ad un gran numero di eseguibili “setuid” o “setgid” o in generale potenzialmente pericolosi (pensate agli utenti di sistema, p. es. quelli utilizzate per far girare i servizi)
- è opportuno restringere l'accesso ai software che vanno in esecuzione con privilegi particolari (p. es: restringendoli in lettura ed esecuzione solo ad un gruppo di utenti autorizzati)
- è difficile risolvere manualmente tutte queste problematiche...
- quando si aggiornano i software i permessi vengono ripristinati “al default”

Permessi sul filesystem

“FIXME: Content needed. Tell of consequences of changing packages permissions when upgrading (and admin this paranoid should chroot his users BTW).

If you need to grant users access to the system with a shell think about it very carefully. A user can, by default unless in a severely restricted environment (like a chroot jail), retrieve quite a lot of information from your system including:

- some configuration files in /etc. However, Debian s default permissions for some sensitive files (which might, for example, contain passwords), will prevent access to critical information. To see which files are only accessible by the root user for example find /etc -type f -a -perm 600 -a -uid 0 as superuser.
- your installed packages, either by looking at the package database, at the /usr/share /doc directory or by guessing by looking at the binaries and libraries installed in your system.
- some log files at /var/log. Note also that some log files are only accessible to root and the adm group (try find /var/log -type f -a -perm 640) and some are even only available to the root user (try find /var/log -type f -a -perm 600 -a -uid 0).”

Log di sistema

“It is easy to see that the treatment of logs and alerts is an important issue in a secure system. Suppose a system is perfectly configured and 99% secure. If the 1% attack occurs, and there are no security measures in place to, first, detect this and, second, raise alarms, the system is not secure at all.
Debian GNU/Linux provides some tools to perform log analysis, most notably swatch, logcheck or log-analysis (all will need some customisation to remove unnecessary things from the report). It might also be useful, if the system is nearby, to have the system logs printed on a virtual console. This is useful since you can (from a distance) see if the system is behaving properly.”

- aumentare la quantità di file di log mantenuti dal sistema (man logrotate)
- modificare i permessi di default dei log (vedi sopra)
- utilizzare strumenti di verifica dei log, per esempio logcheck

Log di sistema

“The logcheck package in Debian is divided into two packages logcheck (the main program) and logcheck-database (a database of regular expressions for the program). The Debian default (in /etc/cron.d/logcheck) is that logcheck is run daily at 2 AM and once after each reboot.

This tool can be quite useful if properly customised to alert the administrator to unusual events in the system. Logcheck can be fully customised so that it can send mails from events recovered from the logs that are worthy of attention. The default installation includes profiles for ignored events and policy violations for three different setups (workstation, server and paranoid). The Debian package includes a configuration file /etc/logcheck/logcheck.conf, sourced by the program, that defines which user the checks are sent to.”

Kernel patches

“Debian GNU/Linux provides some of the patches for the Linux kernel that enhance its security. These include:

- Linux Intrusion Detection (in package lids-2.2.19), by Huagang Xie and Philippe Biondi. This kernel patch makes the process of hardening your Linux system easier by allowing you to restrict, hide and protect processes, even from root. It also allows you to protect or hide certain files so that even root cannot modify them. Furthermore, you can also set capabilities for certain processes. A must for the paranoid system administrator. Homepage: http://www.lids.org
- POSIX Access Control Lists (ACLs) for Linux (in package kernel-patch-acl). This kernel patch adds access control lists, an advanced method for restricting access to files. It allows you to control fine-grain access to files and directory. This patch has been added to the 2.5 development kernel and will be included by default in the future 2.6 Kernel. Homepage: http://acl.bestbits.at/

Kernel patches

- “NSA Enhanced Linux (in package selinux also available from the developer s website (http://www.coker.com.au/selinux/))
- kernel-patch-2.2.18-openwall, by Solar Designer. This is a useful set of kernel restrictions, like restricted links, FIFOs in /tmp, a restricted /proc file system, special file descriptor handling, non-executable user stack area and other. Homepage: http: // www.openwall.com/linux/
- kernel-patch-2.4-grsecurity: The Grsecurity patch, for 2.4 kernels only 15 , which implements Mandatory Access Control, provides buffer overflow protection, ACLs, network randomness (to make OS fingerprinting more difficult) and many more features (http://www.grsecurity.net/features.php).” [deprecated...]

kentrino:~$ apt-cache show kernel-patch-grsecurity2

[..] Furthermore, 2.4.2x versions of this patch will not apply to Debian kernels 2.4.20 and above. You will have to use vanilla kernel sources to apply this patch. Reasons are documented in README.2.4.2x contained within the package.

Integrità del sistema

“Are you sure /bin/login on your hard drive is still the binary you installed there some months ago? What if it is a hacked version, which stores the entered password in a hidden file or mails it in cleartext version all over the Internet?

The only method to have some kind of protection is to check your files every hour/day/month (I prefer daily) by comparing the actual and the old md5sum of this file. [..] You really should consider this auditing of your binaries as very important, since it is an easy way to recognize changes at your binaries. Common tools used for this are sXid, AIDE (Advanced Intrusion Detection Environment), TripWire (non-free; the new version will be GPL), integrit and samhain.

Installing debsums will help to check the file system integrity, by comparing the md5sums of every file against the md5sums used in the Debian package archive. But beware, those files can easily be changed.” [Nota: non tutti i pacchetti contengono gli hash MD5]

Controllo binari setuid

“Debian provides a cron job that runs daily in /etc/cron.daily/standard. This cron job will run the /usr/sbin/checksecurity script that will store information of this changes.

In order for this check to be made you must set CHECKSECURITY_DISABLE= FALSE in / etc /checksecurity.conf. Note, this is the default, so unless you have changed something, this option will already be set to FALSE .

The default behavior does not send this information to the superuser but, instead keeps daily copies of the changes in /var/log/setuid.changes. You should set the CHECKSECURITY_ EMAIL (in /etc/checksecurity.conf) to root to have this information mailed to him. See checksecurity(8) for more configuration info.”

Alcune risorse...

(oltre a quelle contenute nella guida stessa)

http://www.bastille-linux.org/

“The Bastille Hardening System attempts to "harden" or "tighten" Unix operating systems. It currently supports the Red Hat, Debian, Mandrake, SuSE and TurboLinux Linux distributions along with HP-UX and Mac OS X. We attempt to provide the most secure, yet usable, system possible.”

http://www.debian-hardened.org/

“Hardened Debian/Debian Hardened is a project that brings to Debian GNU/Linux high security & hardening features, hardened kernels, packages and enhanced toolchain, the DHKP kernel patches and other cryptography & security related enhancements.”

http://d-sbd.alioth.debian.org/www/

“'Debian: Secure by Default' is a project to examine various security feauters available to the open source community and bring those which do not cause end user complications to Debian's standard distribution. The goal is to make Debian GNU/Linux a simple but effective example of excellence in security, without sacrificing any of Debian's current or future ease of use.”

Alcune risorse...

(oltre a quelle contenute nella guida stessa)

http://www.backports.org/

“You are running Debian stable, because you prefer the stable Debian tree. It runs great, there is just one problem: the software is a little bit outdated compared to other distributions. That is where backports come in.

Backports are recompiled packages from testing (mostly) and unstable (in a few cases only, e.g. security updates), so they will run without new libraries (wherever it is possible) on a stable Debian distribution.”

http://www.grsecurity.net/

“grsecurity is an innovative approach to security utilizing a multi-layered detection, prevention, and containment model. It is licensed under the GPL. It offers among many other features: an intelligent and robust Role-Based Access Control (RBAC) system that can generate least privilege policies for your entire system with no configuration; change root (chroot) hardening; /tmp race prevention; extensive auditing; prevention of entire classes of exploits related to address space bugs (from the PaX project); additional randomness in the TCP/IP stack; a restriction that allows a user to only view his/her processes; every security alert or audit contains the IP address of the person that caused the event.”

Domande?

<free advertising>

http://www.sikurezza.org – Italian Security Mailing List

ci vediamo a webb.it 2005

</free advertising>