SIGURNOST OPERATIVNOG SUSTAVA DEBIAN

(Napisano na osnovi Securing Debian Manuala)

Mjere za zaštitu operativnog sustava Debian provode se prije, tokom i nakon instalacije sustava, tj. za vrijeme njegovog rada, a uključuju onemogućavanje izravnog pristupa sustavu i pristupa sustavu preko mreže. U te mjere spadaju:
- deaktiviranje/deinstaliranje nepotrebnih servisa (deamona) i postavljanje firewalla ili tcp-wrappera
- ograničavanje korisnika tj. njihovih ovlasti na sustavu
- osiguranje aktivnih servisa tako da u slučaju njihove kompromitacije utjecaj na sustav bude minimalan
- korištenje odgovarajućih alata koji omogućuju da eventualna kompromitacija sustava bude na vrijeme otkrivena, tako da se mogu poduzeti odgovarajuće mjere

Inače, najopćenitijeg recepta za osiguranja Debian sustava nema, pošto je svaki pojedinačni slučaj u određenoj mjeri specifičan. Razina sigurnosti tj. mjera i složenost njegovog osiguranja sustava treba biti prilagođena njegovoj važnosti tj. izloženosti informatičkim napadima. Za generalne probleme sigurnosti Debiana brine se Debian Security Team (http://security.debian.org/), a sigurnosno ažuriranje sistema predstavlja prioritet cijelog Debian projekta. Administratori trebaju pratiti izvještaje Security Teama i redovno provoditi ažuriranje vlastitog sustava.

Mjere zaštite pri instalaciji Debiana

Najvažnije mjere zaštite koje se provode prije početka i tokom instalacije Debiana su:

(1) Postavljanje BIOS passworda - za ulaz u BIOS Setup ili još bolje (ako je moguće) za pokretanje sustava. Nakon instalacije u BIOS postavkama treba onemogućiti bootanje sa bilo kojeg drugog medija osim hard diska na koji je instaliran sustav.

(2) Odvajanje dijelova filesystema tako da se stave na različite particije diska (radi izbjegavanja problema sa zauzećem root particije hard diska kao i za prevenciju napada pri kojima se koriste hard linkovi na exe fileove). Zgodno je odvojiti slijedeće direktorije:
- one na kojima korisnik ima ovlast upisivanja - /home/, /tmp/, /var/tmp/
- one čija veličina fluktuira (povećava se) - /var/ - obratiti pažnju na /var/log/ i /var/mail/spool ako stroj radi kao mail server
- one u koje se instalira software koji ne spada u Debian distribuciju /opt/, /usr/local/ (da se ovaj softver ne mora instalirati ponovno pri reinstalaciji Debiana)
- one koji sadržavaju podatke koji se ne mijenjaju - tu particiju može se mountati read-only

(3) Izbor prikladnog file sistema - najbolje da je uzeti journaling file sistem (ext3 je najbolje rješenje) - ovdje postoji manja vjerojatnost gubljenja podataka pri rušenju sustava, a manje je i vrijeme potrebno za recovery sustava. Ako se direktorij /tmp/ nalazi na posebnoj particiji, tu je zgodno uzeti ext2 filesystem.

(4) Tokom instalacije sustav ne bi trebao biti spojen na internet jer tako postaje izložen napadu prije nego se konfigurira na odgovarajući način. Također se ne preporučuje instalirati sustav direktno sa interneta - za takvo nešto može se koristiti Debian package mirror - drugi sustav na kojemu se preko interneta može kreirati Debian arhiva potrebna za instalaciju (korištenjem naredbi apt-proxy i apt-move).

(5) Postavljanje root passworda - treba biti dobro izabran - 6-8 alfanumeričkih znakova uz znakove interpunkcije. Pri instalaciji treba aktivirati shadow password (kriptirani password se zapisuje u fileu kojem može pristupati samo korisnik root i korisnička grupa shadow) - za naknadno aktiviranje koristi se naredba shadowconfig. Takodjer je pri instalaciji dobro aktivirati opciju MD5 password, čime se postiže bolja zaštita

passworda od dekripcije (mogu se koristiti i duži passwordi).

(6) Izbjegavanje nepotrebnih mrežnih servisa (deamona) - u slučaju da su instalirani treba ih deinstalirati ili deaktivirati. Kod deaktiviranja treba znati da se takvi servisi mogu se pokretati preko superdeamona inetd ili preko zasebnog programa kojim se spajaju na mrežu, a čije se pokretanje kontrolira preko skripti u /etc/init.d. Korištenje superdeamona inetd previše se ne preporuča (otvara mogućnost za DoS napade, pa je bolje koristiti recimo xinetd) - servisi se disabliraju komentiranjem odgovarajućih linija u /etc/inetd.conf ili pomoću naredbe update-inetd (--disable naziv_servisa). Ako se mrežni servis pokreće preko /etc/init.d, onda treba obrisati ili preimenovati startup linkove u /etc/rc(runlevel).d - to ide direktno (rm / mv) ili korištenjem naredbe update-rc.d (update-rc.d naziv_servisa stop broj_stop_akcije 2 3 4 5 .). Ovdje treba primijetiti da ne treba obrisati stop linkove u /etc/rc(runlevel).d odnosno ići sa opcijom remove u update-rc jer se tada pri reinstalaciji ili upgradeu paketa startup linkovi ponovno kreiraju.

(7) Instaliranje samo onog softvera koji je uistinu potreban - jer se koristeći sigurnosne propuste u pojedinom paketu može kompromitirati sustav. Posebno treba voditi računa o instaliranim razvojnim alatima jer pomoću njih uljez može (na lak način) doći do većih privilegija ili iskoristiti sustav a napad na druge sustave - u nekim verzijama Debiana razvojni alati se instaliraju u okviru base system instalacije.

Mjere zaštite nakon instalacije Debiana

Mjere zaštite koje se provode nakon instalacije Debiana ovise većim dijelom o samom instaliranom softveru. Generalno, te su mjere slijedeće:

(1) Prijavljivanje na Debian Security Announce mailing listu i praćenje "Debian Security Advisoryja" koje izdaje Debian Security Team - zgodno je pratiti i Debian Security mailing listu. Pri pojavi sigurnosnih updateova treba ih skinuti i instalirati. Za primjenu security updatea neposredno nakon instalacije treba podići firewall i konfigurirati ga tako da se sustav može spojiti samo na site security.debian.org (v. Dodatak 1). Od Debiana 3.0 (Woodyja) instalacijska procedura uključuje mogućnost konfiguracije automatskog sigurnosnog updatiranja sustava - to se može konfigurirati i naknadno (manualno) tako da se u file /etc/apt/sources.list doda redak
deb http://security.debian.org/ stable/updates main contrib {non-free}
Za update sustava mogu se koristiti razni GUI (update-notifier, synaptic, kpackage, adept) ili command-line (apt, dselect, aptitude) paketi - update sustava provodi se naredbama
apt-get update
apt-get upgrade
(ako se koristi aptitude treba samo apt-get naredbu zamijeniti s aptitude). Nakon security updatea često treba restartati updatirane servise, a ako se radili o updateu kernela, onda treba restartati stroj.

(2) Onemogućavanje bootanje s bilo kojeg drugog medija (diskete, CD, DVD) osim sa hard diska na koji je instaliran sustav (BIOS password treba biti postavljen da se to ne može promijeniti). Pritom treba voditi računa da se brisanjem CMOS-a (što je hardverski zahvat) briše i BIOS password, a postoje i softverske metode probijanja BIOS passworda.

(3) Postavljanje LILO ili GRUB passworda - bez toga uljez može doći na root-shell i promijeniti passworde (na boot promptu se napise naziv_bootimagea init=/bin/sh). Za postavljanje LILO passworda treba u /etc/lilo.conf dodati (uz druge boot opcije) - staviti ogranicenje na citanje toga filea
```
password=password
restricted
```
i nakon toga pokrenuti naredbu lilo. Za postavljanje GRUB passworda treba u /boot/grub/menu.lst dodati na pocetak filea
```
timeout 3
password password
```
Može se staviti i MD5 password (password --MD5 kriptirani_password) gdje kriptiranje passworda ide pomocu

naredbe grub-md5-crypt. Nakon toga treba pokrenuti naredbu update-grub

(4) Onemogućavanje pristupa root promptu u initramfs pri pojavi greške pri bootanju sustava (ovo se omogućava u nekim kernelima da bi administrator u slučaju greške mogao ući u rescue shell). U /boot/grub/menu.lst odnosno u /etc/lilo.conf u sekciju append dodati

```
panic=0
```

nakon toga treba pokrenuti naredbu lilo odnosno update-grub.

(5) Onemogućavanje root prompta na kernelu - nakon dizanja crampfs file sistema na 2.4 kernelima postoji mogućnost pristupa root promptu - može se pojaviti poruka - Press ENTER to obtain a shell (waits 5 seconds) - da bi se to onemogućilo treba u /etc/mkinitrd/mkinitrd.conf staviti

```
DELAY=0
```

(6) Ograničavanje logiranja roota na konzoli - može se staviti da se administrator mora logirati na konzolu kao neki "obični" korisnik, a da je root logiranje moguće samo s nekih terminala - to se postavlja u fileovima /etc/login.defs (varijabla CONSOLE definira terminale gdje je root login dozvoljen) ili /etc/securetty (dodaju se terminal devices koji dozvoljavaju root login). Pri korištenju PAM-a (Pluggable Authentication Modules) postoje još veće mogućnosti za kontrolu root logina.

(7) Onemogućavanje reboota sustava sa konzole - sa tipkama ctrl-alt-del svatko bi mogao rebootati sustav ako ima pristup tipkovnici - to se može omemogućiti tako da se u /etc/inittab stavi linija

```
ca:12345:ctrlaltdel:/sbin/shutdown -t1 -a -r now
```

Sada ctrl-alt-del pokreće shutdown sustava, a imena korisnika koji to mogu napravitti nalaze se u /etc/shutdown/ allow, pa ako niti jedan od takvih korisnika nije spojen na sustav, on se pri ctrl-alt-del neće rebootati.

(8) Mountanje particija tako da u /etc/fstab u za odgovarajuće particije stavimo opcije nosuid (ignorira setuid i setgid bitove), noexec (onemogućava izvršavanje programa) ili nodev (ignorira device fileove).
Za particiju na kojoj se nalazi /tmp može se staviti opcije nodev i noexec - neki programi mogu koristiti ovaj direktorij pri instalaciji, pa recimo apt treba iskonfigurirati tako da koristi neki drugi direktorij (varijabla APT::ExtractTemplates::TempDir u /etc/apt/apt.conf)
Za particiju na kojoj se nalazi /usr može se staviti opcije nodev i read-only - da bi se omogućila instalacija novih paketa, potrebno je u /etc/apt/apt.conf dodati (remountanje /usr particije read-write prije i read only poslije instalacije).

```
DPkg {
   Pre-Invoke { "mount /usr -o remount,rw" };
   Post-Invoke { "mount /usr -o remount,ro" };
};
```

Ako se na posebnim particijama nalaze direktoriji /var/tmp, /var/log i /var/account tu stavljamo opcije nodev, nosuid, noexec, a na particiju s direktorijem /var stavljamo nodev, usrquota, grpquota.

(9) Autentikacija usera u aplikacijama preko PAM-a (Pluggable Authentication Modules) - aplikacije trebaju imati (kompajliranu) podršku za PAM i biti konfigurirane u /etc/pam.d. PAM omogućava više koraka u autentikaciji i različite stupnjeve u ograničavanju pristupa.
Pri konfiguraciji PAM-a zgodno je učiniti slijedeće:
- omogućiti MD5 passworde i provjeru jačine passworda - u sve fileove u /etc/pam.d dodati

```
password required pam_cracklib.so retry=3 minlen=12 difok=3
password required pam_unix.so use_authtok nullok md5
```

- ograničiti root login samo na lokalne terminale - u sve fileove u /etc/pam.d dodati

```
auth requisite pam_securetty.so
```

pritom treba ažurirati listu terminala na kojima je omogućen root login u /etc/securetty (alternativa je aktivirati modul pam_access i modificirati /etc/security/access.conf - omogućava finiju kontrolu pristupa)
- omogućiti kontrolu korisničkih resursa (prema konfiguraciji u limits.conf) - /etc/pam.d/login staviti liniju

```
session required pam_limits.so
```

- ograničiti korisnike koji se mogu logirati kao root - kreirati novu grupu (wheel), tu dodati korisnika root i sve druge koji mogu preko su postati root - zatim dodati u /etc/pam.d/su liniju
  auth requisite pam_wheel.so group=wheel debug
- u slučaju potrebe da za neku aplikaciju preko PAM-a ide autentikacija samo nekih korisnika treba u /etc/pam.d/naziv_aplikacije staviti liniju
  auth required pam_listfile.so item=user sense=allow file=/etc/naziv_konfiguracijskog_filea (gdje se korisniku omogućava pristup aplikaciji)
- zbog raznih sigurnosnih propusta zgodno je instalirati libpam-tmpdir paket - u /etc/pam.d/common-session treba staviti liniju
  session optional pam_tmpdir.so
- kreirati defaultnu konfiguraciju za sve aplikacije sa podrškom za PAM - u /etc/pam.d/other staviti
  auth required pam_securetty.so
  auth required pam_unix_auth.so
  auth required pam_warn.so
  auth required pam_deny.so
  account required pam_unix_acct.so
  account required pam_warn.so
  account required pam_deny.so
  password required pam_unix_passwd.so
  password required pam_warn.so
  password required pam_deny.so
  session required pam_unix_session.so
  session required pam_warn.so
  session required pam_deny.so

(10) Limitiranje resursa dodijeljenih pojedinom useru (radi problema "iscrpljivanja resursa" sustava (CPU-a, memorije i dr.) korištenjem PAM-a - u fileu /etc/security/limits.conf (ranije u /etc/limits.conf) može se za svakog korisnika (ili sve korisnike) ograničiti broj procesa, veličina memorije za proces, broj istovremenih prijava na sustav, veličina core dumpa i sl. (naredbom ulimit mogu se vidjeti postavljeni limiti na sustav).

(11) Konfiguriranje postavki za logiranje korisnika u /etc/login.defs - ovaj konfiguracijski file odnosi se jedino na programe su i login. Treba staviti:
  FAIL_DELAY 10 - u slučaju neuspješnog logina, prompt se ponovno otvara nakon 10 sekundi
  FAILLOG_ENAB yes - neuspješni login se zapisuje u log file
  LOG_UNKFAIL_ENAB no - utipkano ime korisnika zapisuje se u log file
  SYSLOG_SU_ENAB yes - pokušaji logiranja preko su zapisuju se u log file
  MD5_CRYPT_ENAB yes - omogućavanje MD5 passworda (ako nema ove opcije to ide preko PAM-a)
  PASS_MAX_LEN 50 - maksimalna duljina passworda

(12) Ograničenje korištenja ftp-a - u fileu /etc/ftpusers navedeni su korisnici koji se ne mogu spajati preko ftp-a - korišenenje ftp-a treba izbjegavati zbog clear-text passworda. Za isto se može koristiti i konfiguracija PAM-a.

(13) Korištenje su i sudo - treba izbjegavati logiranje na sustav kao root - samo se po potrebi treba tako logirati korištenjem naredbe su ili sudo što je još bolje. Za korištenje naredbe sudo korisnik mora biti naveden u fileu /etc/sudoers gdje su definirane i naredbe koje može pokretati

(14) Onemogućavanje administratorskog pristupa preko mreže - u /etc/security/access.conf treba staviti liniju (za administratorsku grupu wheel)
  -:wheel:ALL EXCEPT LOCAL
Pritom pam-access modul treba biti aktiviran za sve servise (odnosno u defaultnoj konfiguraciji).

(15) Ograničavanje pristupa korisnicima - korisnicima kreiranim radi pokretanja mrežnih servisa (pop3, mail, ftp) treba dodijeliti null shell (/dev/null - treba biti definirano u /etc/shells), a ako im se hoće omogućiti pristup

dodjeljuje im se restricted shell (/bin/rbash). Može se koristiti pam_chroot modul ili chroot servisa koji omogućuju prijavu preko mreže. Podešavanje postavki za logiranje vrši se u /etc/security/access.conf

(16) Praćenje aktivnosti korisnika (auditing) - korištenje programa script koji bilježi sve naredbe koje korisnik izvrši na shell promptu, kao i rezultate tih naredbi - inicijalizacija shella mora sadržavati slijedeće naredbe

```
umask 077
exec script -q -a "/var/log/sessions/$USER"
```

Ovo je zgodno staviti u inicijalizacijske fileove korisnika - fileove u audit direktoriju var/log/sessions/ treba staviti da budu append-only (pomoću naredbe chattr).
Ako želimo vidjeti samo naredbe koje korisnik izvršava (bez njihovih rezultata), u inicijalizacijskom fileu /etc/profile može se environment konfigurirati tako da se sve izvršene naredbe zabilježe u history file. Primjer ove konfiguracije je slijedeći:

```
HISTFILE=~/.bash_history
HISTSIZE=10000
HISTFILESIZE=999999
# Don't let the users enter commands that are ignored in the history file
HISTIGNORE=""
HISTCONTROL=""
readonly HISTFILE
readonly HISTSIZE
readonly HISTFILESIZE
readonly HISTIGNORE
readonly HISTCONTROL
export HISTFILE HISTSIZE HISTFILESIZE HISTIGNORE HISTCONTROL
```

Pritom treba staviti da .bash_history bude append-only (pomoću naredbe chattr) - gornja skripta može se staviti i u korisnički .profile file koji u tom slučaju treba staviti da bude immutable.
Na kompleksnim sustavima gdje korisnici nemaju pristup shellovima može se koristiti program acct koji bilježi sve komande koje izvršavaju korisnici ili procesi na sustavu (u direktorij /var/account). U istom paketu nalaze se i neki alati za analizu ovih podataka (sa, ac, lastcomm).
Za još bolje praćenje aktivnosti korisnika mogu se koristiti programi ttysnoop (prati nove tty-eve i izlaz bilježi u file) ili snoop (wrapper za execve()) - sve izvršene komande bilježi u syslogd (preko authpriv utilityja).
Za praćenje aktivnosti korisnika pri loginu može se koristiti wtmp baza - pregledava se pomocu programa sac.

(17) Postavljanje defaultnih ovlasti na fileove koje kreira korisnik pomoću naredbe umask - obično se definira za cijeli sustav u /etc/profile (može se radi sigurnosti postaviti 077). Za konekcije koje koriste login umask se postavlja u fileu /etc/login.defs, a može se definirati i preko PAM-a - u /etc/pam.d/common-session stavi se
session optional pam_umask.so umask=077.

(18) Limitiranje podataka koje korisnik može vidjeti i pristupati im - ako korisnik može pokretati shell onda za defaultnu konfiguraciju Debiana ima pristup mnogim podacima na sustavu - u direktorijima /etc, /usr, /var - mogu se promijeniti ovlasti. Zgodno je također promijeniti ovlasti na korisničke direktorije u /home (750).

(19) Generiranje i provjera korisničkih passworda - radi sigurnosti zgodno je koristiti programe za generiranje korisničkih passworda za sustav kao što su makepasswd, apg, pwgen. Pošto korisnici mogu izabrati weak passworde (koje je lako crackirati) zgodno je koristiti programe za detektiranje takvih passworda (crackere) - john ili crack (zajedno s riječnikom odgovarajućeg jezika).

(20) Odlogiravanje neaktivnih korisnika - neaktivni korisnici predstavljaju opasnos za sustav jer uljez može pristupiti konzoli ako nije zaključana ili se može spojiti na sustav preko mreže ako remote shell nije enkriptiran kao u slučaju telneta. Automatsko odlogiranje neaktivnih korisnika može se postići postavljanjem shell varijable TMOUT ili instaliranjem i konfiguriranjem programa timeoutd tj. autolog.

(21) Upotreba tcpwrappera - tcpwrapperi registriraju pokušaj spajanja na sustav i na osnovi podataka u

odgovarajućim konfiguracijskim fileovima (hosts.access i hosts.deny) omogućavaju ili onemogućavaju spajanje, odnosno korištenje servisa za odredjeni host ili domenu - rade na nivou aplikacije (razvijeni su u vrijeme kad još nije bilo paketnih filtara). Procesi se mogu pokrenuti preko tcpwrapper servisa (tcpd) ili mogu imati ugrađenu podršku za tcpd (includan libwrap0) - koji paketi podržavaju tcpwrapper moze se vidjeti pomocu naredbe

apt-cache rdepends libwrap0

U /etc/hosts.deny može se staviti komanda kojom se rootu šalje mail o pokušajima spajanja koji je tcpwrapper registrirao (SPAWN).

(22) Upotreba logova i alerta - rad sa sistemskim logovima ide preko servisa syslogd (rsyslogd) čiji je konfiguracijski file /etc/(r)syslog.conf. Po defaultu sistemske poruke se ispisuju pomoću program xconsole. Logovi se mogu analizirati pomoću programa logcheck, log-analysis ili swatch. Logcheck može slati mailove s porukama koje se smatraju bitnim prema konfiguraciji u /etc/logcheck/logcheck.conf (može se definirati "razina" zaštite, a za neke pakete može se napraviti i specifično podešavanje).
Na mreži se može jedan stroj konfigurirati kao loghost - logovi sa svih strojeva na mreži šalju se njemu (što je zgodno u slučaju upada u sustav) - treba samo syslogd pokrenuti s opcijom -r tj. u /etc/default/syslogd staviti SYSLOGD="-r", dok na klijentima treba u /etc/syslog.conf staviti

<facility>.<level> @your_loghost

gdje facility i level moraju biti odgovarajući. Također je važno namjestiti odgovarajuće ovlasti za log fileove - posebno /var/log/lastlog(faillog) (chmod 660).

(23) Instaliranje kernel patcheva kojima se podiže razina sigurnosti - neki od značajnijih su:
- kernel-patch-2.4-lids (linux intrusion detection) omogućava kontrolu pristupa sustavu i bolju zaštitu
- paket trustees omogućava unaprijeđeni permission management
- paket selinux omogućava bolju kontrolu pristupa (vezano uz NSA Enhaced Linux)
- kernel-patch-exec-shield omogućava zaštitu od buffer overflowa
- kernel-patch-2.4-grsecurity i kernel-patch-grsecurity2 - omogućava obaveznu kontrolu pristupa, zaštitu od buffer overflowa, network randomness i druge opcije.

Još neki zanimljivi kernel patchevi su kernel-patch-adamantix, cryptoloop-source, linux-patch-openswan.

(24) Zaštita od buffer overflowa tj. izvršavanja koda pomoću programa čije varijable nisu prikladno ograničene - može se provesti patchiranjem kernela (tako da se spriječi pokretanje koda na stacku), popravljanjem izvornog koda programa ili rekompilacijom pri kojoj se provodi testiranje mogućih propusta sa buffer overflowom (SPP). Patchevi koji se koriste su oni navedeni pod (23), te kernel-patch-adamantix. Alati za testiranje izvršnih verzija programa su bfbtester, rats, pscan, flewfinder, splint.

(25) Limitiranje i kontrola upotrebe file sistema - limitiranje veličine filesistema koja stoji na raspolaganju korisniku ili korisničkoj grupi provodi se pomoću paketa quota, pri čemu kernel mora imati podršku za postavljanje quota na file sistemu. Kvote se postavljaju tako da za particije na koje korisnik ima potpune ovlasti u /etc/fstab u retku koji odgovara za pojedinoj particiji umjesto defaults staviti defaults,usrquota (grpquota), a u rootu te particije kreiramo fileove quota.user (group), restartamo quota servis i onda postavimo kvote naredbama

edquota -u <user> (<group>)

Za kontrolu pristupa fileovima i direktorijima mogu se osim uobičajenih permissiona koristiti i atributi specifični za ext2/ext3 filesisteme - i - immutable, a - append - fileove nitko ne može mijenjati (ni root) odnosno sadržaj im se može samo dodavati (analogno vrijedi za direktorije) - promjena atributa ide preko naredbe chattr, a pregled preko lsattr (iz e2fsprogs). Naredbom lcap CAP_LINUX_IMMUTABLE postiže se da više ni korisnik root ne može mijenjati atribute fileova/direktorija - ovo se može promijeniti samo u single-user modu (direktno sa stroja) - ovo nekad može biti zgodan način zaštite.
Kontrola integriteta fileova (posebice bitnih binaryja kao što je /bin/login) provodi se usporedbom aktualnih MD5 suma za te fileove s onim ranijim - koriste se paketi sxid, trpwire, aide, integrit - zgodno je da provjera ide svaki dan. Korištenje programa debsums nije preporučljivo jer se podaci iz debian package arhive lako mogu promijeniti.
Za indeksiranje fileova zgodno je radi sigurnosti koristiti program slocate (u paketu findutils) - pomoću njega se mogu pronaći programi vidljivi odgovarajućem useru (program locate defaultno pronalazi samo one koji su

vidljivi svakome).
Može se koristiti i digitalna signatura za binaryje - pomocu bsign ili elfsign. Pomocu paketa checksecurity vrši se provjera promjena u programu vezana uz setuid dozvole i sl.

(26) Osiguranje prijenosa fileova putem mreže - treba koristiti ssh (klijent scp) ili ftpd-ssl (kriptirani prijenos, klijent ftp-ssl). Za non-UNIX klijente koriste se winscp odnosno putty. Pritom se moze koristiti chrooting za ssh ili ftp.

(27) Osiguranje mrežnog pristupa - provodi se na slijedeće načine:
- Konfiguriranjem kernel parametara za mrežni pristup - postavljanjem parametara u fileu /etc/sysctl.conf ili u skripti koja se pokrece iz /etc/network/interfaces (pre-up <naziv_skripte> za odgovarajući interface) ili iz startup direktorija /etc/init.d. Primjer konfiguriranja nekih važnijih parametara:

```
echo 0 > /proc/sys/net/ipv4/conf/$IFACE/forwarding # IP forwarding disabled
echo 1 >/proc/sys/net/ipv4/conf/$IFACE/log_martians # Log strange packets.
 # (this includes spoofed packets, source routed packets, redirect packets but be careful with this on heavy loaded web servers.)
# IP spoofing protection.
echo 1 > /proc/sys/net/ipv4/conf/$IFACE/rp_filter
# Disable ICMP redirect acceptance.
echo 0 > /proc/sys/net/ipv4/conf/$IFACE/accept_redirects
echo 0 > /proc/sys/net/ipv4/conf/$IFACE/send_redirects
# Disable source routed packets.
echo 0 > /proc/sys/net/ipv4/conf/$IFACE/accept_source_route
```

- Konfiguriranje firewalla (iptables) - objašnjeno kasnije.
- Disabliranje weak-end hostova na LAN-u - ako imamo dvije povezane mreže (druga je internet) - obično se sustav konfigurira tako da su servisi dostupni samo s nekih IP adresa - nekad može biti problem je što to ne znači da su servisi dostupni samo s određenih hardverskih adresa - rješenje je u postavljanju firewalla, odgovarajućem routiranju i patchiranju kernela
- Zaštita od ARP (address resolution protocol) napada - pri slanju paketa na IP adresu vrši se address resolution i dobiva fizička (MAC) adresa - u ARP napadima nastoji simulirati da fizička adresa stroja uljeza odgovara IP adresi stroja s kojim želimo komunicirati (pa onda svoje pakete šaljemo uljezu, a ne tamo gdje treba). Za ovakve napade postoje i posebni programi (arpspoof i dsniff). Za zaštitu treba koristiti statički ARP cache (postavlja se naredbom arp -s <host_name> <hdwr_addr>), kontrolirati sumnjivi arp promet pomocu arpwatcha ili nekog IDS-a (snort) i implementirati IP filtriranje s validacijom fizičkih adresa.

(28) Kreiranje snapshota (snimke) sustava prije puštanja u produkciju (i nakon upgradeova) - koristeci paket md5sum i/ili sha1sum izračunaju se te sume za cijeli sustav i odredjene direktorije (/bin/, /sbin/, /usr/bin/, /usr/sbin/, /lib/, /usr/lib/) i snime na disketu ili CD. Istovremeno treba zbog mogućnosti trojaniziranja, programe md5sum i/ili sha1sum također snimiti na disketu ili CD, odakle se onda kasnije pokreću da bi se usporedile ove sume - za to se mogu se koristiti i ti isti programi na live-CD distribuciji, ako nije problem rebootati sustav. Preporuča se koristiti cron demona za svakonoćno testiranje (medij mora biti read-only).

(29) Ne koristiti softver koji ovisi o biblioteci svgalib jer je ona vrlo nesigurna (putem exploita za zgv uljez lako može postati root).

Ostale mjere odnose se na razne specifičnije izvore opasnosti za sigurnost informatičkog sustava, te na situacije koje mogu nastati u slučaju upada u sustav. Informacije o njima treba potražiti na internetu. (Odnose se na načine pojačanje zaštite sustava, upotrebu sigurnosnih alata, "dobre prakse" u osiguranju sustava, postupke u slučaju incidenta i sl.)