

## Menginstal Slackware dan Mengamankannya

By [Cezary M Kruk](#)

*Artikel ini diterjemahkan dari bahasa Polandia oleh penulisnya. Artikel aslinya akan diterbitkan pada edisi musim panas [CHIP Special Linux](#).*

Ketika muncul versi baru dari distribusi yang anda sukai, anda akan selalu mendapatkan dilema yang sama: menginstal segalanya dari awal atau mencoba untuk mengupdate sistem atau meneruskan apa yang telah anda gunakan selama ini?

Mari kita ambil dua kemungkinan ekstrim: menginstal dan mengkonfigurasi sistem dari awal memungkinkan anda menemukan dan menggunakan segala hal baru yang ada padanya, dan tetap bertahan dengan apa yang telah anda punya akan memberikan anda keyakinan bahwa anda tetap dapat melanjutkan proyek anda tanpa mengalami kesulitan. Apa yang sedang anda hadapi ini adalah pertentangan biasa antara inovasi dan stabilisasi.

Konfigurasi dasar sistem tidaklah sukar. Namun semakin banyak yang anda butuhkan, semakin keras usaha yang harus anda berikan. Apakah mungkin menyederhanakan instalasi dan konfigurasi sistem agar lebih mudah? Sebuah data yang lengkap dan didesain dengan jelas yang berisi informasi mengenai perubahan-perubahan yang anda ketahui bisa bekerja pada sistem versi sebelumnya akan semakin memudahkan pengaturan sistem dengan versi yang baru. Cara ini tidak terlalu rumit ketika anda mengumpulkan data tetapi anda harus banyak bekerja ketika mengembalikan ulang konfigurasi. Bagaimana anda mengotomasi dan menyederhanakannya?

Untungnya Linux menyimpan informasi mengenai konfigurasi untuk setiap service pada file-file teks. Terlebih lagi ia memberi anda tool-tool yang sangat bagus untuk melakukan pemrosesan file. Jadi anda cukup hanya menyiapkan script-script yang tepat dan menggunakannya ketika anda menginstal sistem sekali lagi.

### 1.1. Dari instalasi menuju keamanan

Artikel ini menjelaskan dua kelompok script: yang pertama digunakan untuk menginstal dan menghapus paket program, dan yang kedua digunakan untuk mengamankan sistem dari kemungkinan serangan. Keduanya didesain untuk Slackware Linux. Tool-tool untuk menginstal dan menghapus paket tidak terlalu rumit seperti program dari paket SlackPkg atau Packware, namun tool-tool tersebut memberikan anda kendali penuh atas sistem anda. Hal yang sama juga berlaku pada script untuk mengamankan sistem. Mereka hanya menjalankan operasi-operasi dasar. Kedua set tool-tool tersebut dikumpulkan dalam `slack*more`.

Anda juga dapat mempersiapkan tool-tool lain untuk mengotomasi proses konfigurasi servis atau program. Jika anda memutuskan untuk sama sekali tidak melakukan tuning secara manual tetapi menambahkan script yang sesuai dengan prosedur, maka anda akan segera mendapatkan sebuah kit program anda sendiri untuk mengkonfigurasi sistem.

Terlebih lagi, karena anda akan mempersiapkan sendiri script-script tersebut, maka mereka akan benar-benar sesuai dengan apa yang anda butuhkan.

Kita telah mendiskusikannya dengan menggunakan contoh Slackware Linux karena distribusi tersebut secara alami mengharuskan pengguna menyentuh file-file konfigurasi secara langsung. Linux-linux yang lain, menawarkan program-program yang kompleks untuk melakukan hal tersebut, dan memisahkan pengguna dari file-file yang berisi informasi mengenai konfigurasi. Program-program tersebut membuat mereka malas atau memaksa mereka untuk melakukan penyelidikan yang rumit untuk menemukan apa dan dimana yang berubah pada sistem mereka oleh program-program yang *friendly* tersebut.

Slack\*more dibagi dalam dua bagian. INSTALL.tgz yang berisi tool-tool untuk melakukan instalasi, menghapus atau mengupgrade program, dan SECURE.tgz yang berisi tool-tool untuk melakukan pengamanan pada sistem.

```
mc...003.2/kruk/install/piki/INSTALL/Slackware-9.0 X
bin86: ADD
binutils: ADD
bison: ADD
flex: ADD
gcc: ADD
kernel-headers: ADD
make: ADD

cvs: REC
gcc-g++: REC
gdb: REC
gettext-tools: REC
m4: REC
perl: REC
pkgconfig: REC
pmake: REC
strace: REC

autoconf: OPT
automake: OPT
byacc: OPT
ccache: OPT
distcc: OPT
gcc-g77: OPT
gcc-gnat: OPT
gcc-java: OPT
gcc-objc: OPT
gcl: OPT
guile: OPT
indent: OPT
libtool: OPT
nasm: OPT
p2c: OPT
python: OPT
rcs: OPT

~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
~
Read d, 36 lines, 397 cha s
```

Gambar 1. Dengan script SCRIPT.sh dari direktori ./Slackware-9.0 anda akan mendapatkan daftar paket dari grup-grup individual. Gambar diatas menunjukkan daftar paket dari grup d (development).

## 1.2. Menginstal dan menghapus paket

Komponen terpenting dari paket INSTALL.tgz adalah script INSTALL.sh dan direktori ./Slackware-9.0, berisi script SCRIPT.sh dan file Slackware.

Untuk mendapatkan tool-tool tersebut, anda harus melakukan mount CD instalasi Slackware menuju direktori /mnt/cdrom, dan kemudian menjalankan SCRIPT.sh dari direktori ./Slackware. Script ini akan melihat direktori-direktori yang ada di CD-ROM, dan dengan dibimbing oleh file-file tagfiles yang ada di sana, ia akan membuat file-file

yang berisi informasi mengenai paket-paket yang ada (Gambar 1.). Setiap file akan memiliki nama sesuai dengan nama grup. Sebagai contoh, pada file e, yang berisi paket-paket yang membangun Emacs, anda akan menemukan diantaranya entri berikut ini:

```
emacs: ADD
emacs-misc: REC
emacs-nox: OPT
```

Pengguna yang mengenal Slackware Linux pasti tahu bahwa kategori ADD menunjukkan paket-paket utama untuk digunakan pada program, kategori REC berarti paket-paket yang direkomendasikan, dan kategori OPT berarti paket-paket optional.

Jika anda telah memiliki informasi dasar mengenai paket-paket, anda dapat memutuskan komponen mana yang anda inginkan dan mana yang tidak berguna bagi anda. Sehingga jika anda memodifikasi isi dari file e yang disebutkan di atas seperti di bawah ini:

```
emacs: ADD
#emacs-misc: REC
!emacs-nox: OPT
```

Paket emacs akan diinstal, paket emacs-misc akan diabaikan, dan paket emacs-nox tidak hanya akan diabaikan, tetapi juga -- jika paket tersebut sebelumnya telah terinstal pada sistem -- akan dihapus.

Pada file Slackware yang terdapat pada direktori ./Slackware-9.0 terdapat beberapa informasi mengenai grup-grup paket:

```
a
ap
d
e
f
...
```

Berdasarkan informasi tersebut script akan memilih grup dari paket mana yang akan diputuskan. Jika anda mengkustomasi file tersebut seperti berikut ini:

```
a
ap
#d
!e
f
...
```

maka grup d akan diabaikan, dan setiap paket dari grup e yang sebelumnya telah terinstal pada sistem, akan dihapus.

Sehingga: jika anda menambahkan pada nama paket atau nama grup dengan: # , maka mereka akan diabaikan, dan jika anda menambahkan nama tersebut dengan ! , maka komponen yang bersangkutan akan dihapus dari sistem. Jika sebuah paket atau sebuah

grup belum terinstal, maka arti dari # dan ! adalah sama. Entri dari file-file yang berisi nama grup memiliki prioritas yang lebih tinggi daripada entri pada file-file yang berisi nama paket. Sehingga jika anda memutuskan untuk mengabaikan keseluruhan isi grup atau untuk menghapus paket-paket yang berada di dalamnya, maka script akan melakukannya tanpa menghiraukan informasi yang tertulis pada file-file yang berisi nama-nama paket.

Jika anda telah mempersiapkan file Slackware dan file-file yang berisi informasi mengenai paket-paket individual, anda harus menjalankan script INSTALL.sh. Script ini akan menambah atau mengurangi komponen-komponen yang sesuai pada sistem. Jika ini adalah instalasi Slackware yang pertama kalinya, dan belum dilakukan tuning pada sistem, adalah ide bagus untuk mengoptimalkan kerja hard drive yang digunakan sebagai platform dari distribusi yang baru. Anda dapat menggunakan salah satu dari -- script INSTALL.hda atau INSTALL.hdb. Dengan script tersebut proses instal atau hapus paket akan menjadi semakin cepat.

INSTALL.sh didesain untuk banyak penggunaan. Jika tidak ada yang dapat dilakukan, ia tidak akan melakukan apa-apa. Dengan menggunakan script tersebut anda juga dapat melakukan instalasi dasar Slackware. Cukup menginstal paket dari grup a menggunakan program setup Slackware, dan kemudian meletakkan script tersebut pada sistem, memberikan tanda pada nama paket atau grup yang tidak anda butuhkan, dan untuk menginstal paket-paket berikutnya, jalankan INSTALL.sh.

### **1.3. Informasi mengenai paket**

Pada direktori ./Packages terdapat script SCRIPT.sh yang lain. Jika anda melakukan mount pada CD-ROM Slackware, dan menjalankan script tersebut, ia akan membuat sebuah struktur direktori yang berisi file-file informasi mengenai paket individual pada sistem. Database referensi mengenai paket-paket tersebut akan bermanfaat karena anda tidak harus melakukan mount pada CD instalasi tiap kali ingin melakukan pengecekan untuk mengetahui apa kegunaan dari paket yang terpilih. Anda dapat membuat database tersebut hanya jika anda belum memutuskan untuk menginstal keseluruhan Slackware Linux. Sebaliknya anda akan menemukan informasi mengenai keseluruhan paket pada direktori /var/log/packages.

### **1.4. Patch**

Direktori ./Patches terdiri dari dua script. Jika anda ingin menggunakannya, terlebih dahulu jalankan 0.check. Ia akan melakukan pengecekan pada server [sunsite.icm.edu.pl](http://sunsite.icm.edu.pl) dan melihat apakah tersedia update untuk Slackware 9.0 dan akan membuat file Packages.html yang berisi informasi mengenai update dan file Packages.txt yang berisi nama-nama paket:

```
mutt-1.4.1i-i386-1  
sendmail-8.12.9-i386-1  
sendmail-cf-8.12.9-noarch-1
```

script 1.get akan menggunakan file yang terakhir untuk mendapatkan paket-paket yang diperlukan, file .txt yang sesuai, dan file .tgz.asc. Untuk melakukannya, script ini

menggunakan perintah `wget -c -t0` sehingga tidak ada resiko anda akan mendapatkan file yang sama berulang kali. Di sisi lain melakukan pengecekan apakah file tersebut sudah berhasil didapatkan akan membutuhkan waktu, sehingga sebaiknya anda melihat ke dalam file `Packages.txt` sebelum anda memulai `1.get`, dan menghapus nama paket yang telah berhasil anda dapatkan atau yang tidak anda butuhkan. Namun hal ini tidak harus dilakukan.

Anda dapat merubah perintah untuk mendapatkan file-file tersebut dengan `wget -c -t0 -b`. Sehingga keseluruhan file akan diambil dari server pada satu waktu yang bersamaan -- pada background. Tetapi tidak semua server mengijinkan anda untuk melakukan koneksi secara simultan. Jika server **sunsite.icm.edu.pl** tidak memenuhi kebutuhan anda, anda dapat mendaftarkan host lain pada script `0.check` dan `1.get`. Kemudian anda harus menyesuaikan isi perintah yang membentuk file `Packages.txt` dari file `Packages.html`. Ini adalah perintah aslinya:

```
cat Packages.html | grep ".tgz.asc" | sed 's/.tgz.asc//g' | sed \
's/.*A HREF="//' | sed 's/">.*//' > Packages.txt
```

script `1.get` hanya mendaftarkan informasi mengenai paket-paket casual. Kumpulan update yang besar dari Slackware diletakkan pada direktori yang terpisah (`kde`, `kdei`, `dll`). Jika anda ingin mendapatkannya, anda harus melakukannya secara manual atau dengan memodifikasi script aslinya sesuai dengan kebutuhan anda.

### **1.5. Direktori `./usr/local/bin`**

Pada direktori `./usr/local/bin` terdapat script `catpkg` yang memudahkan pengamatan file-file yang terdapat pada direktori `/var/log/packages` untuk mendapatkan informasi mengenai keseluruhan paket yang terinstal pada sistem. `INSTALL.sh` menyalin keseluruhan isi dari direktori lokal `./usr/local/bin` ke sistem yang sesuai. Sehingga anda dapat meletakkan script yang berbeda di sini untuk digunakan selama bekerja dengan sistem.

```
mc - ~/DATA/CHIP/2003.2/kruk/install/pliki/SECURE
c_kruk@home1:~/DATA/CHIP/2003.2/kruk/install/pliki/SECURE$ cat 0.nosuid.home1

Removed SUID or SGID:

Removed SUID:
-rwx--x--x 1 root bin /usr/bin/at
-rwx--x--x 1 root bin /usr/bin/crontab
-rwxr-x--- 1 root floppy /usr/bin/fdmount
-rwx--x--x 1 root bin /usr/bin/chage
-rwx--x--x 1 root bin /usr/bin/chfn
-rwx--x--x 1 root bin /usr/bin/chsh
-rwx--x--x 1 root bin /usr/bin/expiry
-rwx--x--x 1 root bin /usr/bin/gpasswd
-rwx--x--x 1 root bin /usr/bin/newgrp
-rwx--x--x 1 root bin /usr/bin/passwd
-rwx--x--x 1 root bin /usr/bin/rcp
-rwx--x--x 1 root bin /usr/bin/rlogin
-rwx--x--x 1 root bin /usr/bin/rsh
-rwx--x--x 1 root bin /usr/bin/traceroute
-rwx--x--x 1 root bin /usr/X11R6/bin/xterm
-rwxr-xr-x 1 root root /usr/libexec/pt_chown
-rwx--x--x 1 root bin /bin/su
-rwxr-xr-x 1 root bin /bin/mount
-rwxr-xr-x 1 root bin /bin/umount
-r-xr-xr-x 1 root bin /bin/ping
-rwxr-xr-x 1 root root /opt/kde/bin/kcheckpass
-rwxr-xr-x 1 root root /opt/kde/bin/konsole_grantpty
-rwxr-xr-x 1 root root /opt/kde/bin/kppp
-rwxr-xr-x 1 root root /opt/kde/bin/fileshareset
-rwx--x--x 1 root root /usr/libexec/ssh-keysign
-rwxr-xr-x 1 root bin /usr/X11R6/bin/xscreensaver
-rwxr-xr-x 1 root bin /usr/X11R6/bin/xcardinfo
-rwxr-xr-x 1 root root /usr/local/bin/thotswap
-rwxr-xr-x 1 root bin /sbin/cardctl
-rwx--x--x 1 root bin /usr/X11R6/bin/xlock

Removed SUID and SGID:
-rwxr-xr-x 1 root root /usr/X11R6/bin/wmapm
c_kruk@home1:~/DATA/CHIP/2003.2/kruk/install/pliki/SECURE$ █
```

Gambar 2. Script SECURE.sh menghapus bit-bit SUID dan SGID dari file yang terpilih dan menampilkan informasi tentangnya

## 1.6. Mengamankan

Script utama pada SECURE.tgz adalah SECURE.sh. Ia melakukan tugas-tugas berikut:

- Melakukan pengesetan pada file /etc/login.defs untuk variabel `PASS_MAX_DAYS` menjadi bernilai 182. Dengan demikian waktu validasi password untuk pengguna baru akan dibatasi selama enam bulan.
- Melakukan pengesetan pada file /etc/profile file untuk variabel `HISTFILESIZE` menjadi bernilai 100. Dengan demikian file untuk sejarah perintah akan dibatasi menjadi seratus baris.

- Melakukan pengesetan pada file `/root/.bashrc` file untuk variabel `TMOUT` menjadi bernilai 900. Dengan demikian sesi root yang tidak aktif akan di-kill setelah limabelas menit.
- Memberikan tanda komentar pada file `/etc/inetd.conf` untuk semua servis jaringan yang tidak diberi komentar namun berpotensi membahayakan.
- Meletakkan entri pada file `/etc/hosts.deny` berupa `ALL: ALL@ALL` ,untuk memblok keseluruhan akses dari luar menuju mesin.
- Meletakkan entri pada file `/etc/hosts.allow` berupa `ALL: ALL@127.0.0.1 : ALLOW` , yang memberikan akses menuju ke resources pada mesin lokal.
- Mengubah kalimat `order hosts, bind` pada file `/etc/host.conf` menjadi `order bind, hosts` yang lebih aman dan menambahkan `nospoof on`
- Melakukan pengeblokan pada file `/etc/securetty` untuk akses root menuju semua console kecuali `/dev/tty1`.
- Menghapus grup `news` dan `uucp` dari file `/etc/group` yang dalam kebanyakan kasus, lebih dari yang dibutuhkan. Hal ini sama dengan memberikan perintah `groupdel news` dan `groupdel uucp`
- Menghapus user `news`, `uucp`, `operator`, `sync`, dan `shutdown` dari file `/etc/passwd`. Hal ini sama dengan memberikan perintah `userdel` dengan parameter yang sesuai.
- Melakukan aksi paralel dengan referensi dari file `/etc/shadow`.
- Memberikan tanda komentar pada file `/etc/inittab` untuk baris `ca::ctrlaltdel:/sbin/shutdown` . Dengan demikian shortcut `Ctrl-Alt-Delete` tidak akan menyebabkan mesin melakukan reboot.
- Menghilangkan hak baca atau eksekusi oleh grup atau user lain pada semua script yang ada pada direktori `/etc/rc.d`.
- Menambahkan beberapa perintah untuk mematikan atau menghidupkan beberapa servis pada file `/etc/rc.d/rc.local`. Agar perintah-perintah tersebut dapat bekerja, anda harus menambahkan modul *IP: TCP syncookie support* pada kernel.
- Melakukan test pada beberapa program yang bermasalah dan menghilangkan bit-bit SUID darinya. Informasi mengenai modifikasi tersebut disimpan pada file `log` (Gambar 2.).
- Melakukan hal yang sama dengan referensi beberapa program tersebut, dan menghilangkan bit-bit SUID dan SGID-nya.
- Meletakkan entri pada file konfigurasi `/etc/mail/sendmail.cf` o `PrivacyOptions=noexpn` dan `O PrivacyOptions=novrfy` . Hal tersebut mencegah pengecekan secara remote pada account-account sistem.
- Menyalin script `remove` ke direktori `/etc/cron.daily`. Script tersebut digunakan untuk menghapus secara otomatis direktori dan file-file temporary dari sistem.
- Menyalin beberapa script yang berguna pada direktori `/root/bin`.

Hal-hal tersebut akan meningkatkan keamanan sistem secara signifikan, walaupun itu hanya merupakan permulaan dalam mengamankan sistem dari gangguan yang mungkin terjadi. Script `SECURE.sh` ditulis dengan suatu cara sehingga dapat dijalankan berulang kali. Sehingga anda dapat menambahkan prosedur apapun ke dalam script tersebut dan menerapkannya tanpa mengalami masalah apapun.

Script tersebut akan memodifikasi beberapa servis, namun tidak akan melakukan overload. Untuk membaca `/etc/inetd.conf` kembali, gunakan perintah `killall -HUP inetd` . Untuk mengeksekusi `/etc/inittab` yang sudah dimodifikasi, jalankan perintah



init q . Untuk merestart sendmail gunakan perintah `/etc/rc.d/rc.sendmail restart` atau `kill -HUP `head -1 /var/run/sendmail.pid`` .

Anda bisa saja memasukkan perintah-perintah tersebut ke dalam script, namun terdapat potensi resiko yang harus anda pertimbangkan. Jika anda melakukan kesalahan kecil pada pemanggilan program sed, bukannya modifikasi file `/etc/inittab` yang akan anda dapatkan, melainkan sebuah file kosong. Sebagai akibatnya, setelah anda melakukan reboot pada init maka anda akan kehilangan akses menuju sistem, dan anda diharuskan untuk melakukan restore `/etc/inittab` dengan menggunakan sistem Linux yang terinstal pada partisi yang lain pada harddisk. Hal itu tidak selalu menyenangkan, terutama jika anda tidak mempunyai partisi lain yang berisi Linux.

```
mc - ~/DATA/CHIP/2003.2/kruk/install/pliki/SECURE
c_kruk@home1:~/DATA/CHIP/2003.2/kruk/install/pliki/SECURE$ head -n46 3.huge.home
1
Huge files:
1359696 Feb 14 01:51 /bin/rpm
1170308 Apr 3 21:29 /boot/vmlinuz
1170308 Mar 18 07:03 /boot/vmlinuz-ide-2.4.20
1435624 Mar 5 06:57 /lib/libc-2.3.1.so
1169241 Apr 2 07:00 /opt/OpenOffice.org1.0.3/help/en/common.jar
5008330 Apr 2 07:00 /opt/OpenOffice.org1.0.3/help/en/picture.jar
5472256 Apr 12 00:07 /opt/OpenOffice.org1.0.3/program/applicat.rdb
1030449 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libbasctl641li.so
3427013 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libcfgmgr2.so
2799427 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libcnt641li.so
2850166 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libdba641li.so
1519306 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libdbtools2.so
4384335 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libdbu641li.so
2510465 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libfrm641li.so
1315556 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libfwk641li.so
2569660 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/liblocaledata_ascii.so
3942878 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libmozabdrv2.so
1924855 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsal.so.3.0.1
1074944 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsb641li.so
1065462 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libtbl641li.so
10785364 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsc641li.so
2265379 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsch641li.so
4431058 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsd641li.so
1484385 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libset641li.so
5104660 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsfx641li.so
1903423 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libstdc++.so.3.0.4
1087721 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libstlport_gcc.so
1506595 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsvl641li.so
4385355 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsvt641li.so
13318396 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsvx641li.so
14054696 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libsw641li.so
2631714 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libtk641li.so
4135742 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libvcl641li.so
5033106 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libxo641li.so
1054900 Apr 2 07:00 /opt/OpenOffice.org1.0.3/program/libxpcorn.so
1114512 Jul 1 2002 /opt/OpenOffice.org1.0.3/share/dict/ooo/de_DE.dic
1173085 Mar 29 2002 /opt/OpenOffice.org1.0.3/share/dict/ooo/fr_FR.dic
1413535 Apr 8 2002 /opt/OpenOffice.org1.0.3/share/dict/ooo/pl_PL.dic
3344716 Apr 2 07:00 /opt/OpenOffice.org1.0.3/share/dict/ooo/th_en_US.dat
2318336 Apr 2 07:00 /opt/OpenOffice.org1.0.3/share/gallery/sg16.sdv
1156560 May 10 2001 /opt/RealPlayer8/Common/rmacore.so.6.0
1247004 May 10 2001 /opt/RealPlayer8/realplay
1996378 Apr 16 03:03 /opt/games/pingus/games/pingus
2137588 Mar 16 06:36 /opt/kde/bin/kmail
c_kruk@home1:~/DATA/CHIP/2003.2/kruk/install/pliki/SECURE$
```

Gambar 3. Daftar file-file dengan ukuran besar. Seperti yang dapat anda lihat, tempat tertinggi diduduki oleh file-file OpenOffice.org yang terinstal di direktori /opt, beserta file-file RealPlayer dan Pingus.

### 1.7. Test

script TEST-SECURE.sh mencari file-file berikut ini pada sistem:

- File-file yang bit-bit SUID dan SGID-nya diset.
- File-file besar dan tua (file yang lebih dari 1 MB, terakhir dimodifikasi atau digunakan lebih dari tiga bulan yang lalu).
- Khusus file-file yang berukuran besar (Gambar 3.).
- File-file yang tidak memiliki asosiasi kepada user atau grup apapun yang ada pada sistem.

Informasi mengenai tiap kategori file dicatat dalam file log yang terpisah. TEST-SECURE.sh memanfaatkan hasil kerja dari script SECURE.sh, menampilkan isi dari file log yang berisi informasi mengenai program-program tanpa bit SUID atau SGID.

Karena anda tidak selalu ingin melakukan test tersebut secara bersamaan, pada direktori /root/bin anda akan menemukan script 1.suid, 2.huge+old, 3.huge, dan 4.nobody. Setiap script hanya akan melakukan satu test khusus.

### 1.8. Dan seterusnya...

Hasil pengembangan script SECURE.sh bersama prosedur-prosedur lain akan bertanggung jawab terhadap konfigurasi dan instalasi untuk perlindungan yang lebih jauh. Dengan mengikuti prosedur yang digunakan dalam script ini, anda akan dapat menulis script berikutnya untuk melakukan tuning pada servis-servis yang lain: mengkonfigurasi account user, melakukan setting servis dan klien jaringan, email dan WWW, lingkungan X Window, dan lain-lain. Satu-satunya batasan adalah imajinasi anda sendiri karena dengan cara tersebut Linux memungkinkan anda untuk mengatur hampir segalanya. Sehingga ketika anda selesai membuat script-script tersebut anda akan dapat melakukan konfigurasi pada keseluruhan sistem benar-benar seperti yang anda inginkan, dengan hanya beberapa kali menekan Enter.

### 1.9. Sumber-sumber

Slack\*more:

[freshmeat.net/projects/slackmore](http://freshmeat.net/projects/slackmore)

SlackPkg:

[freshmeat.net/projects/slackpkg](http://freshmeat.net/projects/slackpkg)

Packware (Polish site):

[hacking.pl/packware.php](http://hacking.pl/packware.php)

*Cezary lives in Wroclaw, Poland. He is an editor in the Polish-language quarterly [CHIP Special Linux](#).*



Copyright © 2003, Cezary M Kruk. Copying license  
<http://www.linuxgazette.com/copying.html>  
Published in Issue 91 of *Linux Gazette*, June 2003

---

Diterjemahkan oleh Triyan W. Nugroho <[ivan\\_kid\[at\]yahoo.com](mailto:ivan_kid@yahoo.com)>