Basic Linux system
==========
Oleh hari-huhui (h4ri@telkom.net)
Alhamdulillahirabbil 'aalamiin, segala puji bagi Allah yang telah menciptakan ilmu ini ....

Sebuah server linux yang aman tergantung bagaimana administrator membuat server tersebut. Berikut ini akan dijelaskan hal-hal yang berkaitan dengan masalah keamanan. i) Keamanan BIOS
Berilah boot password pada BIOS anda, karena orang lain bisa saja mem-boot system anda dengan menggunakan boot disk khusus.
ii) Set-lah panjang minimum password bagi user agar sulit untuk ditebak.
Kita bisa melakukan hal ini dengan cara mengedit file /etc/login.defs. Contoh:
vi /etc/login.defs
Editlah baris PASS_MIN_LEN 5
menjadi PASS_MIN_LEN 8
iii) Untuk alasan keamanan, jangan pernah login sebagai root kecuali memang sedang membutuhkan akses root. Dan jangan pernah meninggalkan login root begitu saja dari komputer kita tanpa logout terlebih dahulu.
iv) Mengeset login time out untuk account root
Editlah file /etc/profile dan tambahkan baris TMOUT setelah baris HISTSIZE. Contoh:
vi /etc/profile
tambahkan baris berikut:
TMOUT=7200
v) Disable servis-servis yang ada pada /etc/inetd.conf
vi /etc/inetd.conf
matikanlah servis-servis yang masih terbuka pada /etc/inetd.conf dengan memberikan tanda #. Sehingga file /etc/inetd.conf akan menjadi seperti:

```
# To re-read this file after changes, just do a 'killall -HUP inetd
#
#echo stream tcp nowait root internal
#echo dgram udp wait root internal
#discard stream tcp nowait root internal
#discard dgram udp wait root internal
#daytime stream tcp nowait root internal
#daytime dgram udp wait root internal
#chargen stream tcp nowait root internal
#chargen dgram udp wait root internal
#time stream tcp nowait root internal
#time dgram udp wait root internal
#
# These are standard services.
#
#ftp stream tcp nowait root /usr/sbin/tcpd in.ftpd -l -a
#telnet stream tcp nowait root /usr/sbin/tcpd in.telnetd
#
# Shell, login, exec, comsat and talk are BSD protocols.
```

```
#
#shell stream tcp nowait root /usr/sbin/tcpd in.rshd
#login stream tcp nowait root /usr/sbin/tcpd in.rlogind
#exec stream tcp nowait root /usr/sbin/tcpd in.rexecd
#comsat dgram udp wait root /usr/sbin/tcpd in.comsat
#talk dgram udp wait root /usr/sbin/tcpd in.talkd
#ntalk dgram udp wait root /usr/sbin/tcpd in.ntalkd
#dtalk stream tcp wait nobody /usr/sbin/tcpd in.dtalkd
#
# Pop and imap mail services et al
#
#pop-2 stream tcp nowait root /usr/sbin/tcpd ipop2d
#pop-3 stream tcp nowait root /usr/sbin/tcpd ipop3d
#imap stream tcp nowait root /usr/sbin/tcpd imapd
#
# The Internet UUCP service.
#
#uucp stream tcp nowait uucp /usr/sbin/tcpd /usr/lib/uucp/uucico -l
#
# Tftp service is provided primarily for booting. Most sites
# run this only on machines acting as "boot servers." Do not uncomment
# this unless you *need* it.
#
#tftp dgram udp wait root /usr/sbin/tcpd in.tftpd
#bootps dgram udp wait root /usr/sbin/tcpd bootpd
#
# Finger, systat and netstat give out user information which may be
# valuable to potential "system crackers." Many sites choose to disable
# some or all of these services to improve security.
#
#finger stream tcp nowait root /usr/sbin/tcpd in.fingerd
#cfinger stream tcp nowait root /usr/sbin/tcpd in.cfingerd
#systat stream tcp nowait guest /usr/sbin/tcpd /bin/ps -auwwx
#netstat stream tcp nowait guest /usr/sbin/tcpd /bin/netstat -f inet
#
# Authentication
#
#auth stream tcp nowait nobody /usr/sbin/in.identd in.identd -l -e -o
#
# End of inetd.conf
```

Setelah itu restartlah inetd anda dengan mengetikkan perintah:
killall -HUP inetd
Setelah direstart, buatlah file /etc/inetd.conf immutable sehingga tidak akan dapat dimodifikasi atau direname.
chattr +i /etc/inetd.conf

vi) Pemanfaatan TCP_WRAPPERS
Dengan TCP_WRAPPERS kita dapat dengan mudah menolak atau mengijinkan user-user yang akan mengakses komputer kita.
Edit file /etc/hosts.deny (vi /etc/hosts.deny) sehingga menjadi:
Deny access to everyone.
ALL: ALL@ALL, PARANOID
Perintah di atas akan membuat semua servis dan semua lokasi ditolak secara default kecuali diijinkan melalui pendefinisian di hosts.allow.
Edit file /etc/hosts.allow (vi /etc/hosts.allow) sehingga host-host yang kita percayai dapat mengakses komputer kita. Contoh:
sshd: 203.132.134.123 testing.com
Maksud dari baris di atas adalah TCP_WRAPPERS mengijinkan akses ssh melalui IP 203.132.134.123 dan atau dari host testing.com.
vii) Edit file /etc/securetty, file ini mendefinisikan kebolehan root untuk akses di virtual terminal ke berapa. Contoh:
tty1
#tty2
#tty3
#tty4
#tty5
#tty6
#tty7
#tty8
Konfigurasi di atas akan membuat root hanya bisa login pada tty1 saja.
viii) Edit file /etc/lilo.conf dan tambahkan baris timeout=00, restricted, dan password. Contoh:
boot=/dev/sda
map=/boot/map
install=/boot/boot.b
prompt
timeout=00
Default=linux
restricted
password=
image=/boot/vmlinuz-2.2.12-20
label=linux
initrd=/boot/initrd-2.2.12-10.img
root=/dev/sda6
read-only

Lalu ubahlah mode file tersebut agar hanya root saja yang bisa membaca file tersebut. Ketikkan perintah:
chmod 600 /etc/lilo.conf. Setelah itu, aktifkan kembali lilo dengan setting baru;
lilo
ix) Menghilangkan akses shutdown melalui tombol Ctrl-Alt-Del.
Untuk bisa seperti itu, maka kita harus mengedit file /etc/inittab pada baris:
ca::ctrlaltdel:/sbin/shutdown -t3 -r now

sehingga menjadi:
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
lalu aktifkan perubahan tersebut dengan perintah:
init q

Sebetulnya masih banyak faktor keamanan lain yang bisa dilakukan. Anda dapat memperolehnya di buku-buku yang membahas tentang security atau dari internet.

Demikianlah tulisan yang singkat ini, semoga ada perbaikan dan koreksi dari pembaca. Terima kasih buat temen-temen #indolinux.

Note: *makasih oom atas artikel yang sangat bermanfaat ini.*
oom hary dapat ditemui di channel IRC #indolinux dalnet dengan nick hari-huhui :)