Optimasi Linux

Mohammad Safii
karebet_asli@telkom.net
http://sapitenk.cjb.net

Linux mewarisi keamanan unix. Itulah sebuah kalimat yang menjadi panduan seseorang mengapa memilih linux sebagai sistem operasi pada sebuah PC. Beberapa orang menyukai keamanan dari pada kemudahan penggunaannya. Mereka berfikir dengan tingkat sekuritas yang tinggi file-file pribadi aman. Unix identik dengan keamanannya. Tapi siapa sangka jika kita lalai saja, contohnya linux, maka tidak di sangka linux pun bisa tertembus keamanannya. Banyak webserver-webserver yang menggunakan sistem operasi Linux yang sering kali di jadikan sasaran deface. Baik dari salahnya konfigurasi Linux sebagai server atau bug yang terdapat dalam program web servernya.

Untuk menangani dan memanfaatkan keamanan dari unix di Linux ini, sebenarnya linux mempunyai beberapa penanganan dini yang berasal dari sistem linux sendirr. Tanpa ada software tambahan maka di bawah ini akan di jabarkan bagaimana memanfaatkan keamanan linux.

A. LILO

Langkah pertama ketika ingin mengoptimalkan linux ialah membuat secure lilo. Lilo begitu sangat penting dan perlu diamankan ketika secara default linux di set untuk memasukkan opsi ketika pertama boot. Keadaan ini tentu saja akan mengenakkan para cracker ketika waktu linux boot dan muncul

LILO boot :

Secara default linux akan memberikan wewenang kepada siapapun untuk login sebagai root. Caranya ketika menghadapi prompt seperti diatas ketikkan linux single. Yang artinya sistem akan di boot dengan Run Level 1 yaitu sebagai super user (root). Keadaan ini akan sangat berguna ketika super user sendiri lupa password root dan dapat

login dengan cara diatas tanpa harus memasukkan password root. Tapi jika prompt diatas tetap ditampilkan maka dengan mudah sistem bisa di acak-acak. Jadi terdapat berbagai macam tipe pengamanan diantarnya :

1. Mendisable linux single.

   Langkah pertama yaitu mendisable linux single yaitu tidak ada tipe boot dengan Run Level 1 atau linux single. Buka /etc/inittab, cari skrip di bawah ini

   id:3:initdefault:
   setelah itu tambahkan skrip dibawah ini tepat di bawahnya

   ~~:S:wait:/sbin/sulogin

   Penambahan tersebut akan meminta user yang login dengan linux single untuk memasukkan password root terlebih dahulu.
   Setelah menambah baris diatas jalankan perintah di bawah ini:

   # /sbin/init q

2. Mengubah konfigurasi lilo.conf

   Buka file /etc/lilo.conf
   Pada redhat 6.2 lilo.conf nampak seperti dibawah ini:

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
prompt
timeout=50
linear
default=linux
image=/boot/vmlinuz-2.2.14-5.0
        label=linux
        read-only
        root=/dev/hda1
```

   2.a Timeout

   Lilo seperti diatas mempunyai timeout=50; artinya bahwa sistem akan menunggu inputan dari user selama 50 detik. Dengan waktu tunggu seperti ini kemungkinan untuk login dengan linux single sangat besar. Oleh karena itu langkah sederhana menghilangkan waktu tunggu. Isikan timeout = 00.

   2.b Passsword lilo

   Selain memberikan waktu tunggu yang kecil lilo juga dapat di password. Dengan cara memberikan opsi **restricted** dan **password**.

Dibawah baris
Default=linux ; tambahkan
restricted
password=masukkan_passwordnya

Penambahan password diatas memberikan maksud bahwa walaupun tidak login sebagai linux single atau user yang lain lilo akan meminta password root.

2.c Menghilangkan prompt

Ketika linux booting maka muncul

LILO boot :

Kata tersebut muncul karena pada file lilo.conf tertulis kata **prompt.** Untuk menghilangkan prompt agar tidak ada opsi booting hapus kata tersebut.

Jika sudah ditambahkan semuanya maka lilo yang telah dimodifikasi seperti dibawah ini:

```
boot=/dev/hda
map=/boot/map
install=/boot/boot.b
timeout=00
linear
default=linux
restricted
password=masukkan_password
image=/boot/vmlinuz-2.2.14-5.0
        label=linux
        read-only
        root=/dev/hda1
```

Jika sudah dikonfigurasi seperti diatas keluar dari editor dan save. Untuk memberikan kepemilikan hanya kepada root maka jalankan :

```
# chmod 600 /etc/lilo.conf
    #  /sbin/lilo.conf
    LILO version 21, Copyright 1992-1998 Werner Almesberger

        Reading boot sector from /dev/hda
        Merging with /boot/boot.b
        Boot image: /boot/vmlinuz-2.2.14-5.0
     Added linux *
        /boot/boot.0300 exist – no backup copy made.
        Writing boot sector.
```

Konfigurasi diatas menggunakan redhat 6.2, untuk distro yang lain sama.
Jika langkah diatas sudah dijalankan dengan benar maka lilo dijamin aman. Namun ada satu hal yang penting ialah kepemilikan file /etc/lilo.conf. Tentu saja file tersebut dengan owner root. Tapi bagaimana jika suatu waktu root ceroboh atau salah konfigurasi lilo.conf maka bis saja linux tidak bisa booting karena konfigurasi lilo salah.Untuk mengatasi hal tersebut ada perintah di linux yang mengamankan file atau direktory sehingga hanya *read-only* saja termasuk root sendiri.

```
# chattr +i /etc/lilo.conf
```

Perintah diatas memberikan imunitas file lilo.conf untuk dapat di read-only saja oleh root. Jadi tidak bisa diedit atau dimodifikasi. Untuk menghilangkan imunitas file tersebut perintahnya :

```
# chattr –i /etc/lilo.conf
```

B. Disable ctrl+alt+del

Seperti yang telah diketahui untuk shutdown di linux *hotkey*-nya ctrl+alt+del. Selain menggunakan hotkey juga dapat menggunakan printah /sbin/reboot, /sbin/halt. Tapi jika ingin linux aman perintah shutdown dengan keyboard harus didisable karena bisa saja orang lain yang dengan tidak sengaja menekan ctrl+alt+del sedangkan Anda sedang mengkonfigurasi sistem tentu ini tidaklah mengenakkan dan langkah preventif ialah jawabannya.
Buka file /etc/inittab

```
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

Pada baris diatas berikan tanda # di depan baris agar perintah diatas dianggap komentar oleh linux (# merupakan simbol komentar pada bahasa C).

```
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

keluar dari editor dan save jalankan perintah di bawah ini

```
# /sbin/init q
```

C. /etc/services

File /etc/services berisi nomor port yang digunakan untuk koneksi dengan server atau dengan klien. File tersebut digunakan oleh klient untuk meresolv antara port dengan tipe service masing-masing port. Misal apabila klient atau server request smtp maka akan melihat pada file /etc/services smtp menggunakan nomor port berapa. Oleh karena sangat pentingnya maka perlu diberi imunitas file.

```
# chattr +i /etc/services
```

D. /etc/securetty

File /etc/securetty memberikan konfigurasi tty dan vc (virtual console) kepada root atau user yang lain. Maka perlu di disable tty yang tidak digunakan. Buka file /etc/securetty

```
tty1
tty2
tty3
tty4
tty5
```

Jika konfigurasinya seperti diatas maka cukup menggunakan tty1 saja caranya tambahkan # pada tty2-tty5

```
tty1
#tty2
#tty3
#tty4
#tty5
```

Begitu juga dengan vc cukup gunakan vc/1 saja.

E. Menghapus account yang tidak perlu

Maksud account yang tidak perlu ialah account yang dibuat otomatis oleh vendor dari paket yang telah diinstall ataupun tidak. Terkadang terdapat sebuah account tapi paket tersebut tidak diinstall. Gunanya account otomatis tersebut ialah memudahkan pengecekan untuk melihat update paket (software). Contoh sederhana dalam file contoh file /etc/passwd terdapat account ftp namun server tersebut tidak memberikan layanan ftp maka account tersebut harus dihapus begitu juga dengan account yang lain. Namun pada intinya semakin banyak account pada /etc/passwd semakin mudah untuk mengakses sistem dan tentu saja tidak menyenangkan. Isi file /etc/passwd :

```
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:
daemon:x:2:2:daemon:/sbin:
adm:x:3:4:adm:/var/adm:
lp:x:4:7:lp:/var/spool/lpd:
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:
```

```
news:x:9:13:news:/var/spool/news:
uucp:x:10:14:uucp:/var/spool/uucp:
operator:x:11:0:operator:/root:
games:x:12:100:games:/usr/games:
gopher:x:13:30:gopher:/usr/lib/gopher-data:
ftp:x:14:50:FTP User:/home/ftp:
nobody:x:99:99:Nobody:/:
xfs:x:43:43:X Font Server:/etc/X11/fs:/bin/false
named:x:25:25:Named:/var/named:/bin/false
postgres:x:26:26:PostgreSQL Server:/var/lib/pgsql:/bin/bash
pii:x:500:500:pii:/home/pii:/bin/bash
ipin:x:501:501::/home/ipin:/bin/bash
```

untuk menghapus user gunakan

```
# userdel nama_account
```

Account yang dihapus

```
# userdel adm
# userdel lp
# userdel shutdown
# userdel halt
# userdel news
# userdel mail
# userdel uucp
# userdel operator
# userdel games
# userdel gopher
# userdel ftp
```

Setelah menghapus username maka grup juga harus dihapus. Caranya menghapus

```
#groupdell nama_grup
```

Buka file /etc/group

```
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
```

```
mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
man:x:15:
games:x:20:
gopher:x:30:
dip:x:40:
ftp:x:50:
nobody:x:99:
users:x:100:
floppy:x:19:
xfs:x:43:
named:x:25:

# groupdel adm
# groupdel lp
# groupdel shutdown
# groupdel halt
# groupdel news
# groupdel mail
# groupdel uucp
# groupdel operator
# groupdel games
# groupdel gopher
# groupdel ftp
```

Kesimpulan dari penghapusan user dan grup ialah menghapus account dimana tidak dibutuhkan dan tidak terdapat service dalam server atau linux. Seperti contoh diatas tidak menyediakan ftp maka user dan grup ftp dihapus, begitu juga dengan news, gropher dll. Semakin sedikit account yang terdapat di /etc/passwd, /etc/group, /etc/passwd semakin secure linux.

Selain mengatur account juga memberikan imunitas terhadap file /etc/passwd, /etc/group, /etc/shadow, /etc/gshadow

```
# chattr +i /etc/passwd
# chattr +i /etc/shadow
# chattr +i /etc/group
# chattr +i /etc/gshadow
```

Shell Logging

Jika user sering berinteraksi dengan shell maka cara singkat untuk menampilkan perintah yang sudah dijalankan ialah dengan cara menekan tombol panah bawah dan atas. Karena setiap user mempunyai file .bash_history. Dimana dalam file tersebut

terdapat history command. Kasus sederhana ketika user meninggalkan Pcnya untuk sementara waktu misalnya ke kamar mandi maka shell akan mudah melihat perintah yang telah diketikkan user. Untuk menanggulangi keadaan tersebut bagi user atau root sekalipun edit file /etc/profile

```
HOSTNAME=`/bin/hostname`
HISTSIZE=1000
```

Ubah HISTSIZE (history size) dengan nilai 0
Sehingga menjadi

```
HOSTNAME=`/bin/hostname`
HISTSIZE=0
```

Dengan demikian setiap user ataupun root sekalipun tidak mempunyai histroy command lagi. Tentu ini cara yang terbaik menjaga agar system aman.

Keamanan Log

Salah satu pertimbangan keamanan yang paling utama adalah menjaga keamanan file dibawah
/var/log/. Di dalam direktory tersebut tercatat semua aktivitas system baik yang dilakukan user atau root. Sehingga jika system telah di crack maka langkah terakhir ialah menjaga /var/log/ karena pengawasan system terdapat di bawah direktory /var/log/. Setiap aktivitas yang terjadi di catat dalam sebuah log berdasarkan aplikasi masing-masing. Oleh karena itu sebuah file log seharusnya hanya bias di tulis dan tidak untuk di hapus isinya. Untuk memberi hak akses agar file log hanya bias di tulis saja maka tambahkan perintah
#chttr +a nama_log

jika seseorang masuk ke system, pastinya untuk tidak meninggalkan jejak dia harus menghapus file log terlebih dahulu, namun dengan hak akses diatas file log hanya bisa di tulis (append).

Daftar Pustaka

Red Hat Linux 8.0 The Official Red Hat Linux Security Guide. 2002 by Red Hat, Inc.