General Linux Security

1. **Pengamanan Boot Sistem**

   Hal yang terpenting dalam masalah security atau keamanan adalah kemananan secara fisik, maka dari itu ada beberapa hal yang dapat kita maksimalkan diantaranya adalah dengan memberikan password pada grub, berikut adalah cara untuk memberikan password pada grub boot loader, tambahkan opsi berikut pada baris konfigurasi grub hingga seperti contoh berikut

```
default=0
timeout=5
splashimage=(hd0,0)/boot/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.18-128.el5)
root (hd0,0)
kernel /boot/vmlinuz-2.6.18-128.el5 ro root=LABEL=/
initrd /boot/initrd-2.6.18-128.el5.img
password rifqi
```

   Selain dengan menembahkan password pada grub kita juga dapat mendisable kombinasi CtrlAltDelete, sehingga sistem tidak akan restart ketika kompinasi tombol keyboard tersebut di aktifkan, untuk menonaktifkan fungsi CtrlAltDelete edit file /etc/inittab dan beri tanda komen (#) pada opsi dibawah

```
# Trap CTRL-ALT-DELETE
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
```

   Salah satu cara yang lain untuk lebih memberikan tingkat keamanan sistem linux adalah dengan memodifikasi konfigurasi file /etc/fstab, yaitu dengan menambahkan opsi nodev, nosuid dan noexec

```
LABEL=/var              /var                    ext3
defaults,nosuid,noexec,nodev        1 2
LABEL=/tmp              /tmp                    ext3
defaults, nosuid,noexec,nodev        1 2
```

2. **Pengaturan Service**

   Salah satu metode untuk mengamankan sistem adalah dengan menonaktifkan layanan-layanan (service) yang tidak diperlukan, untuk mengecek service apa saja yang dijalankan oleh sistem kita maka kita dapat menggunakan tools chkconfig berikut

```
/sbin/chkconfig --list | grep on
```

   dengan menjalankan perintah diatas maka kita akan tau service-service mana saja yang di jalankan oleh sistem seperti pada tampilan berikut

```
acpid                   0:off     1:off     2:on 3:on 4:on 5:on 6:off
anacron                 0:off     1:off     2:on 3:on 4:on 5:on 6:off
apmd                    0:off     1:off     2:on 3:on 4:on 5:on 6:off
atd                     0:off     1:off     2:off     3:on 4:on 5:on
     6:off
auditd                  0:off     1:off     2:on 3:on 4:on 5:on 6:off
autofs                  0:off     1:off     2:off     3:on 4:on 5:on
     6:off
avahi-daemon            0:off     1:off     2:off     3:on 4:on 5:on
     6:off
avahi-dnsconfd          0:off     1:off     2:off     3:off     4:off
     5:off     6:off
bluetooth               0:off     1:off     2:on 3:off     4:on 5:on
     6:off
conman                  0:off     1:off     2:off     3:off     4:off
     5:off     6:off
cpuspeed                0:off     1:on 2:on 3:on 4:on 5:on 6:off
crond                   0:off     1:off     2:on 3:on 4:on 5:on 6:off
cups                    0:off     1:off     2:on 3:off     4:on 5:on
6:off
```

Untuk mematika service yang tidak di perlukan, agar setiap kali sistem kita di jalankan dan service tersebut tidak otomatis di jalankan maka kita perlu mematikanya dengan [erintah berikut

```
/sbin/chkconfig nama_service off
```

sebagai contoh kita akan ennaktifkan service bluetooth, maka perintahnya adalah

```
/sbin/chkconfig bluetooth off
```

gunakan perintah diatas untuk menonaktifkan service-service lain yang tidak kita perlukan.

3. Super User Do (SUDO)

Sudo (super user do) merupakan tools di Unix/Linux yang mengizinkan user biasa agar dapat mengeksekusi perintah-perintah yang seharusnya hanya dapat di jalankan oleh user root, dan agar user biasa dapat menjalankan perintah root maka user yang akan kita berikan hak root harus kita dftarkan dulu pada file /etc/sudoers, berikut adalah contohnya

```
## Allow root to run any commands anywhere
root,rifqi,testing ALL=(ALL)       ALL
```

perintah diatas akan mengakibatkan user rifqi dan user testing dpat menjalankan perintah-perintah root, kita juga dapat mberikan ijin agar user-user yang kita daftarkan pada file /etc/sudoers dapat menjalankan perintah root tanpa ditanyai password, yaitu dengna menggunakan opsi berikut

```
rifqi,testing   ALL=NOPASSWD: ALL
```

dan kita juga dapat hanya memberikan hak kepada suatu user untuk hanya dapat menjalankan perintah-perintah tertentu saja

```
rifqi,testing   ALL=NOPASSWD: /sbin/ifconfig, /sbin/halt, /sbin/reboot
```

dengan opsi diatas maka user rifqi dan user testing hanya dapat menjalankan beberapa perintah-perintah root yang di izinkan saja, yaitu /sbin/ifconfig, /sbin/halt, /sbin/reboot.

4. Pengamanan SSH

SSH merupakan port komunikasi yang paling sering digunakan untuk melakukan maintenance server secara remote, walaupun openssh sendiri tergolong aplikasi dengan tingkat keamanan tinggi namun bukan berarti 100% aman, ketidak amanan bisa saja terjadi dari banyak hal, semisal dari kelengahan administrator dalam memberikan password, brute force dan lain sebagainya, untuk itu ada banyak solusi yang dapat kita lakukan untuk lebih mengamankan sistem kita dengan, berikut adalah beberapa hal yang dapat kita lakukan untuk lebih meingkatkan kemananan system. Salah satu yng dapat kita lakukan adalah dengan memodifikasi file konfiguasi OpenSSH, berikut adalah beberpa parameter konfigurasi OpenSSH yang dapat kita sesuaikan untuk lebih meningkatkan sisi keamanan

PermitRootLogin no **,** Aktifkan opsi ini agar user root tidak di perbolehkan login menggunakan port ss
AllowUsers rifqi, opsi ini hanya akan mengizinkn user rifqi yang boleh login ke sistem
ListenAddress 192.168.1.254, apabila kita memiliki beberapa IP Address maka kita dapat menentukan dari IP Address mana kita boleh login
Port 7676, salah satu metode untuk "menipu" adalah dengan mengubah port standar yang digunakan oleh ssh ke port lain, tentunya dengan syarat port tersebut belum digunakan.
LoginGraceTime 2m, opsi ini digunakan untuk membatsi waktu otentifikasi maksimal setelah promt otentifikasi dan sebelum user login
MaxAuthTries 2, ini digunakan untuk membatasi "N" kali user melakukan koneksi gagal maka ssh akan menutup koneksinya.

Cara lain untuk meminimalisir menyalahgunaan penggunaan port sshadalah dengan membatasi koneksi ssh hanaya diperbolehkan dari host tertentu, dengan menggunakan IPtables seperti rules berikut

```
/sbin/iptables -A INPUT -p tcp -s ! 10.55.1.20 --dport 22 -j
DROP
```

Dengan menggunakan perintah iptables diatas maka semua host tidak di izinkan melakukan keksi ke port ssh kecuali host dengan ip 10.55.1.20

5. Pengunaan TCP Wrapers

Secara default sistem kita akan membuka service-service ke semua host tanpa batasan, sehingga ini dapat menjadi celah kemanan di sistem kita, dan untuk membatasinya kita dapat

menggunakan aplikasi tcp wrappers, biasanya aplikasi ini telah terinstall secara default di sistem ketika kita menginstall CentOS linux, atau apabila kita ingin mengeceknys terleih dahulu mak kita dapat menggunakan perintah rpm berikut

```
#rpm -qa | grep wrappers
tcp_wrappers-7.6-40.6.el5
```

apabila anda menemui output seperti di atas berarti aplikasi tcp wrappers telah terinstall di sistem kita, file konfigurasi tcp wrappers ada dua file, yaitu /etc/hosts.allow dan /etc/host.deny, dan format penulisanya adalah

```
service_name : ip/host
```

berikut adalah contoh konfigurasi dari tcp wrappers, isikan beris berikut pada /etc/host.deny

```
ALL:ALL
```

kemudian isikan baris berikut pada file /etc/hosts.llow

```
sshd : 10.55.1.50
```

dengan menggunakan konfigurasi diatas berarti semua layanan akan di tutup oleh sistem dan hanya mengizinkan service ssh dari host 10.55.1.50, contoh diatas berarti sama dengan perintah berikut, etc/hosts.allow

```
ALL:10.55.1.50: ALLOW
ALL:ALL: DENY
```

atau sebaliknya, kita izinkan semua host dan tolak satu host tertentu, /etc/hosts.allow

```
ALL:10.55.1.50 : DENY
ALL:ALL : ALLOW
```

6. Analisa Log System

Sebagai administrator tentunya adalah tugas kita untuk senantiasa memantau kondisi sistem kita, tidak terkecuali sisi keamanan sistem kita, di linux ada beberapa file log (catatan) yag bisa digunakan untuk menganalisa sistem kita dari bahaya keamanan, diantaranya adalah file /var/log/messages yang menampung log-log sistem, berikut adalah isinya

```
tail /var/log/messages
Oct 23 04:30:24 centos avahi-daemon[2623]: Registering new
address record for fe80::201:2ff:fe44:6a1b on eth1.
Oct 23 06:10:24 centos dhclient: DHCPREQUEST on eth0 to
10.55.1.91 port 67
Oct 23 06:10:24 centos dhclient: DHCPACK from 10.55.1.91
Oct 23 06:10:24 centos dhclient: bound to 10.55.1.50 -- renewal
```

```
in 10538 seconds.
Oct 23 09:06:02 centos dhclient: DHCPREQUEST on eth0 to
10.55.1.91 port 67
Oct 23 09:06:02 centos dhclient: DHCPACK from 10.55.1.91
Oct 23 09:06:02 centos dhclient: bound to 10.55.1.50 -- renewal
in 9888 seconds.
Oct 23 11:50:50 centos dhclient: DHCPREQUEST on eth0 to
10.55.1.91 port 67
Oct 23 11:50:50 centos dhclient: DHCPACK from 10.55.1.91
Oct 23 11:50:50 centos dhclient: bound to 10.55.1.50 -- renewal
in 10020 seconds.
```

file lain yang perlua kita cek secara berkala adalah /var/log/secure yang berisi catatan keamanan sistem, berikut adalah contoh isi dari file /var/log/secure

```
#tail /var/log/secure
Oct 23 11:56:08 centos sshd[6634]: Accepted password for rifqi
from 10.55.1.194 port 53934 ssh2
Oct 23 11:56:08 centos sshd[6634]: pam_unix(sshd:session):
session opened for user rifqi by (uid=0)
Oct 23 11:56:13 centos sudo:    rifqi : TTY=pts/0 ;
PWD=/home/rifqi ; USER=root ; COMMAND=/bin/su
Oct 23 11:56:13 centos su: pam_unix(su:session): session opened
for user root by rifqi(uid=0)
Oct 23 12:39:42 centos sudo:    rifqi : TTY=pts/0 ;
PWD=/home/rifqi/rkhunter-1.3.4 ; USER=root ;
COMMAND=./installer.sh --layout custom /usr/local --install
Oct 23 12:49:59 centos sshd[13982]: pam_unix(sshd:auth):
authentication failure; logname= uid=0 euid=0 tty=ssh ruser=
rhost=10.55.1.194  user=rifqi
Oct 23 12:50:01 centos sshd[13982]: Failed password for rifqi
from 10.55.1.194 port 60012 ssh2
Oct 23 12:50:06 centos last message repeated 2 times
Oct 23 12:50:06 centos sshd[13983]: Connection closed by
10.55.1.194
Oct 23 12:50:06 centos sshd[13982]: PAM 2 more authentication
failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=10.55.1.194
user=rifqi
```

selain file-file log diatas tentunya masih banyak file-file log yang harus kita cek secara berkala, diantaranya adalah log file httpd, file log squid dan file log lain tergantung dari service apa saja yang kita jalankan.

7. Instalasi rkhunter

srkhunter merupakan aplikasi yang digunakan untuk mendeteksi apakah di sistem kita terpsang aplikasi *rootkit*, *backdoor* dan sejenisnya, apabila komputer kita tidak terhubung dengan jaringan internet pastinya kita tidak akan memerulukan aplikasi ini, akan tetapi apabila

komputer kita terhuung dengan jaringan internet dan membuka layanan public, semisal web server, maka tidak ada salahnya kita menginstall aplikasi ini, untuk menginstall rkhunter pertama download terlebih dahulu rkhunter di webnya

```
wget
http://sourceforge.net/projects/rkhunter/files/rkhunter/1.3.4/rk
hunter-1.3.4.tar.gz/download
```

ekstrak rkhunter dan masuk ke direktori hasil ekstrak

```
tar xvzf rkhunter-1.3.4.tar.gz
cd rkhunter-1.3.4
```

kemudian install dengan menjalankan script install.sh

```
./installer.sh --layout custom /usr/local --install
```

maka kita akan mendapatkan output seperti berikut

```
Installing WISHLIST: OK.
Installing language support files: OK.
Installing rkhunter: OK.
Installing rkhunter.conf: OK.
Installation finished.
```

Berarti instalasi telah berjalan dengan benar, dan untu menjalankanya gunakan perintah berikut

```
/usr/local/bin/rkhunter -check
```

hasil scaning rkhunter akan di letakan di /var/log/rkhunter, untuk melihatnya kita bisa menggunakan perintah less

```
less /var/log/rkhunter.log
```

8. Instalasi Portsentry

Portsentry merupkan adalah apikasi yang digunakan untuk memblok koneksi dari client yang di anggap membahayakan, sebagai contoh apabila ada client yang melakukn *scanning* ke server kita maka otomatis komputer client tersebut akan di blok dengan membuat rules iptables baru untuk menolak koneksi dari client tersebut, untuk proses instalasi portsentry, pertama download paket *rpm* untuk CentOS disini

```
wget
ftp://ftp.pbone.net/mirror/ftp.falsehope.net/home/tengel/centos/
4/te/i386/RPMS/portsentry-1.2-1.te.i386.rpm
```

kemudian install dengan perintah rpm

```
rpm -ivh portsentry-1.2-1.te.i386.rpm
```

setelah itu sesuaikan konfigurasi portsentry dengan kebutuhan anda, file konfigurasi portsentry ada di

```
/etc/portsentry/portsentry.conf
```

file konfigurasi ini merupakan file konfigurasi utama dari portsentry

```
/etc/portsentry/portsentry.modes
```

file ini merupakan file pengaturan mode dari portsentry

```
/etc/portsentry/portsentry.ignore
```

masukan host-host yang tidak akan di blok disini agar host tersebut melakukan scanning ke server.
Berikut adalah conoh log dari portsentry ketika ada host yang melakukan *scanning*

```
PortSentry is now active and listening.
Oct 24 09:59:32 centos portsentry[3191]: attackalert: UDP scan
from host: 10.55.1.25/10.55.1.25 to UDP port: 631
Oct 24 09:59:32 centos portsentry[3191]: attackalert: Host
10.55.1.25 has been blocked via dropped route using command:
"/sbin/iptables -I INPUT -s 10.55.1.25 -j DROP"
Oct 24 10:00:17 centos portsentry[3189]: attackalert: TCP
SYN/Normal scan from host: 10.55.1.35/10.55.1.35 to TCP port: 23
Oct 24 10:00:17 centos portsentry[3189]: attackalert: Host
10.55.1.35 has been blocked via dropped route using command:
"/sbin/iptables -I INPUT -s 10.55.1.35 -j DROP"
```

dan berikut adalah tampilan dari client yng melakukan *scanning*

```
nmap 10.55.1.50

Starting Nmap 5.00 ( http://nmap.org ) at 2009-10-24 17:00 EDT
Interesting ports on 10.55.1.50:
Not shown: 642 filtered ports, 352 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
443/tcp  open  https
3306/tcp open  mysql
```

```
MAC Address: xx:xx:xx:xx:xx:xx (Asiarock Incorporation)
```

dan berikut adalah tampilan ketika client melakukan *scanning* lagi, sesaat setelah *scanning* pertama

```
nmap 10.55.1.50

Starting Nmap 5.00 ( http://nmap.org ) at 2009-10-24 17:02 EDT
All 1000 scanned ports on 10.55.1.50 are filtered
MAC Address: xx:xx:xx:xx:xx:xx (Asiarock Incorporation)

Nmap done: 1 IP address (1 host up) scanned in 22.19 seconds
```

dari output diatas terlihat bahwa setelah client melakukan scanning maka IP ddress client akan langsung di blok oleh server