فصل دوم

امنیت برنامه‌ها

راهکارهایی برای ایمن‌سازی سیستم‌عامل (OS Hardening)

۱. سیستمتان را به‌صورت Minimal نصب کنید.
۲. روی grub تان حتماً پسورد بگذارید.
۳. زمان نصب و بعد از نصب، سیستمتان را به اینترنت متصل نکنید.
۴. Update ها را از DVD نصب کنید.
۵. ssh را به root ببندید و به کاربر عادی باز کنید.
۶. همیشه آخرین نسخه kernel را در grub بگذارید و kernel قبلی را comment کنید یا حذف نمایید.

```
vi /etc/grub.conf
# grub.conf generated by anaconda
#
# Note that you do not have to rerun grub after making changes to this file
# NOTICE:  You have a /boot partition.  This means that
#          all kernel and initrd paths are relative to /boot/, eg.
#          root (hd0,0)
#          kernel /vmlinuz-version ro root=/dev/sda3
```

```
#       initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.18-194.el5)
      root (hd0,0)
      kernel /vmlinuz-2.6.18-194.el5 ro root=LABEL=/
      initrd /initrd-2.6.18-194.el5.img
```

۷. روی بایوس دستگاهان حتماً گذرواژه قرار دهید.
۸. کاری کنید که multiboot از hard بوت شود نه از CDROM.
۹. grub-md5-crypt می‌تواند روی سیستم شما password قرار دهد. به help این دستور توجه نمایید.

```
grub-md5-crypt --help
Usage: grub-md5-crypt [OPTION]
Encrypt a password in MD5 format.

 -h, --help              print this message and exit
 -v, --version           print the version information and exit
 --grub-shell=FILE       use FILE as the grub shell

Report bugs to <bug-grub@gnu.org>.
```

پس از اجرای این دستور یک گذرواژه مانند ۱۲۳۴۵۶ وارد نمایید. خروجی دستور عبارتی encrypt شده می‌باشد. به اجرای دستور توجه نمایید.

```
grub-md5-crypt
Password:
```

Retype password:
1yckvZ$p7Q52tDy4Hb9aBE5BkcYS1
فایل grub.conf را ویرایش کرده و بعـد از timeout عبـارت زیـر را وارد نمایید.
password --md5 1yckvZ$p7Q52tDy4Hb9aBE5BkcYS1
در لیست زیر به فایل ویرایش شده آن توجه نمایید.
vi /etc/grub.conf
grub.conf generated by anaconda
#
Note that you do not have to rerun grub after making changes to this file
NOTICE: You have a /boot partition. This means that
all kernel and initrd paths are relative to /boot/, eg.
root (hd0,0)
kernel /vmlinuz-version ro root=/dev/sda3
initrd /initrd-version.img
#boot=/dev/sda
default=0
timeout=5
password --md5 1yckvZ$p7Q52tDy4Hb9aBE5BkcYS1
splashimage=(hd0,0)/grub/splash.xpm.gz
hiddenmenu
title CentOS (2.6.18-194.el5)
root (hd0,0)
kernel /vmlinuz-2.6.18-194.el5 ro root=LABEL=/
initrd /initrd-2.6.18-194.el5.img

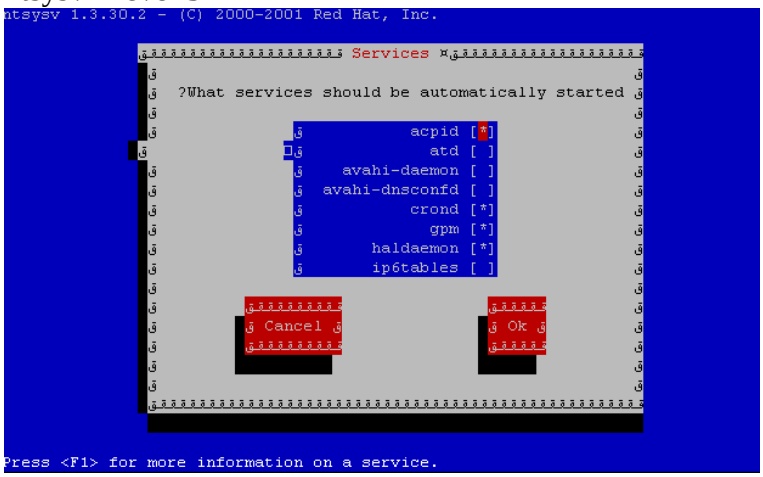
۱۰. بعد از grub مسئله مهم run level است. تا جایی که می‌توانید بهتر است از run level 3 استفاده کنید و از run level گرافیکی استفاده نکنید.

vi /etc/inittab

id:3:initdefault:

۱۱. همچنین تمام سرویس‌های که از آن‌ها استفاده نمی‌کنید را غیرفعال نمایید و تیکشان را بردارید. سایت http://www.mjmwired.net اطلاعات خوبی برای هر سرویس ارائه داده است.

ntsysv --level 3



۱۲. سیستم برای بوت شدن سراغ inittab می‌رود.

vi /etc/inittab

#

inittab This file describes how the INIT process should set up

the system in a certain run-level.

#

Author: Miquel van Smoorenburg, <miquels@drinkel.nl.mugnet.org>

```
#               Modified for RHS Linux by Marc Ewing and Donnie Barnes
#

# Default runlevel. The runlevels used by RHS are:
#   0 - halt (Do NOT set initdefault to this)
#   1 - Single user mode
#   2 - Multiuser, without NFS (The same as 3, if you do not have networking)
#   3 - Full multiuser mode
#   4 - unused
#   5 - X11
#   6 - reboot (Do NOT set initdefault to this)
#
id:3:initdefault:

# System initialization.
si::sysinit:/etc/rc.d/rc.sysinit

l0:0:wait:/etc/rc.d/rc 0
l1:1:wait:/etc/rc.d/rc 1
l2:2:wait:/etc/rc.d/rc 2
l3:3:wait:/etc/rc.d/rc 3
l4:4:wait:/etc/rc.d/rc 4
l5:5:wait:/etc/rc.d/rc 5
l6:6:wait:/etc/rc.d/rc 6

# Trap CTRL-ALT-DELETE
```

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

# When our UPS tells us power has failed, assume we have a few minutes
# of power left.  Schedule a shutdown for 2 minutes from now.
# This does, of course, assume you have powerd installed and your
# UPS connected and working correctly.
pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"

# If power was restored before the shutdown kicked in, cancel it.
pr:12345:powerokwait:/sbin/shutdown -c "Power Restored; Shutdown Cancelled"


# Run gettys in standard runlevels
1:2345:respawn:/sbin/mingetty tty1
2:2345:respawn:/sbin/mingetty tty2
3:2345:respawn:/sbin/mingetty tty3
4:2345:respawn:/sbin/mingetty tty4
5:2345:respawn:/sbin/mingetty tty5
6:2345:respawn:/sbin/mingetty tty6

# Run xdm in runlevel 5
x:5:respawn:/etc/X11/prefdm –nodaemon
```

خط زیر در این فایل عنوان می‌کند که کاربری که درون tty قـرار دارد و کنسول را در اختیار دارد، اگر Ctrl+Alt+Delete زد، سیستم پس از ۳ ثانیه reboot شود.

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

این خط را comment کنید یا به کاربری خاص تخصیص دهید.

vim /etc/shutdown.allowed

root

hossein

hadi

خط زیر در این فایل می‌گوید که اگر ups تان powerfail شـد، پـس از دو دقیقه سیستم را خاموش کن.

pf::powerfail:/sbin/shutdown -f -h +2 "Power Failure; System Shutting Down"

به بخش tty در این فایل توجه نمایید:

Run gettys in standard runlevels

1:2345:respawn:/sbin/mingetty tty1

2:2345:respawn:/sbin/mingetty tty2

3:2345:respawn:/sbin/mingetty tty3

4:2345:respawn:/sbin/mingetty tty4

5:2345:respawn:/sbin/mingetty tty5

6:2345:respawn:/sbin/mingetty tty6

از لحاظ امنیتی بهتر است تعداد tty تان را کـم کنیـد (۲ عـدد مناسـب است.)

نکته: وقتی inittab را تغییر دادیم برای اعمال تغییـرات دسـتور زیـر را می‌نویسیم:

init q

می‌خواهیم یک user وقتی به tty شماره یک وصل شود نتواند login کند مثلاً یک برنامه خاص مثل top اجرا شود. به‌صورت زیر باید عمل نماییم:

1:2345:wait:/user/bin/top

با استفاده از Alt+ctrl+F1 وارد tty1 می‌شوید.

یا حتی می‌توانید به‌صورت مستقیم با یک user، login شوید

2: respawn:/sbin/mingetty autologon test tty2

۱۳. امن کردن Run Level:

~~:S:wait:/sbin/sulogin

S عبارت است از Run Level 1 یا Single که به‌صورت پیش‌فرض به شما دسترسی می‌دهد ولی شما کاری کرده‌اید که پسورد از شما طلب نماید.(sulogin)

۱۴. ترتیب بوت سرویس‌ها مهم است (Boot Sequencing). نگاهی به Level 3 بیندازیم:

```
ls -l /etc/rc.d/rc3.d
total 112
lrwxrwxrwx 1 root root 22 Dec  5  2010 K02avahi-daemon -> ../init.d/avahi-daemon
lrwxrwxrwx 1 root root 24 Dec  5  2010 K02avahi-dnsconfd -> ../init.d/avahi-dnsconfd
lrwxrwxrwx 1 root root 13 Dec  5  2010 K05atd -> ../init.d/atd
lrwxrwxrwx 1 root root 16 Dec  5  2010 K10psacct -> ../init.d/psacct
lrwxrwxrwx 1 root root 14 Dec  5  2010 K10tcsd -> ../init.d/tcsd
lrwxrwxrwx 1 root root 17 Dec  5  2010 K35winbind -> ../init.d/winbind
```

lrwxrwxrwx 1 root root 20 Dec 5 2010 K44rawdevices -> ../init.d/rawdevices
lrwxrwxrwx 1 root root 20 Dec 5 2010 K50netconsole -> ../init.d/netconsole
lrwxrwxrwx 1 root root 15 Dec 5 2010 K75netfs -> ../init.d/netfs
lrwxrwxrwx 1 root root 18 Dec 5 2010 K87mcstrans -> ../init.d/mcstrans
lrwxrwxrwx 1 root root 20 Dec 5 2010 K87multipathd -> ../init.d/multipathd
lrwxrwxrwx 1 root root 17 Dec 5 2010 K87portmap -> ../init.d/portmap
lrwxrwxrwx 1 root root 21 Dec 5 2010 K87restorecond -> ../init.d/restorecond
lrwxrwxrwx 1 root root 18 Dec 5 2010 K89netplugd -> ../init.d/netplugd
lrwxrwxrwx 1 root root 15 Dec 5 2010 K89rdisc -> ../init.d/rdisc
lrwxrwxrwx 1 root root 19 Dec 5 2010 K92ip6tables -> ../init.d/ip6tables
lrwxrwxrwx 1 root root 15 Dec 5 2010 K95kudzu -> ../init.d/kudzu
lrwxrwxrwx 1 root root 22 Dec 5 2010 S02lvm2-monitor -> ../init.d/lvm2-monitor
lrwxrwxrwx 1 root root 22 Oct 22 2012 S03vmware-tools -> ../init.d/vmware-tools
lrwxrwxrwx 1 root root 18 Dec 5 2010 S08iptables -> ../init.d/iptables

```
lrwxrwxrwx 1 root root 17 Dec  5  2010 S10network -> ../init.d/network
lrwxrwxrwx 1 root root 16 Dec  5  2010 S12syslog -> ../init.d/syslog
lrwxrwxrwx 1 root root 15 Dec 11  2010 S13named -> ../init.d/named
lrwxrwxrwx 1 root root 20 Dec  5  2010 S22messagebus -> ../init.d/messagebus
lrwxrwxrwx 1 root root 15 Dec  5  2010 S26acpid -> ../init.d/acpid
lrwxrwxrwx 1 root root 19 Dec  5  2010 S26haldaemon -> ../init.d/haldaemon
lrwxrwxrwx 1 root root 14 Dec  5  2010 S55sshd -> ../init.d/sshd
lrwxrwxrwx 1 root root 13 Dec  5  2010 S85gpm -> ../init.d/gpm
lrwxrwxrwx 1 root root 15 Dec  5  2010 S90crond -> ../init.d/crond
lrwxrwxrwx 1 root root 11 Dec  5  2010 S99local -> ../rc.local
```

همیشه iptables و syslog قبل از همه سرویس ها باید بالا بیایند.

۱۵. کاری کنیم اگر کاربری پشت سیستم می‌نشیند نفهمد که درون کدام tty ها login کرده است.

```
cat /etc/securetty
console
vc/1
vc/2
vc/3
```

vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11

لیست ترمینال‌ها یا device هایی که root می‌تواند در آن‌ها login کند، نوشته شده است. مثلاً می‌توانیم tty3 و tty4 را حذف کنیم.

Login یا root را فقط روی یک tty باز بگذارید مثلاً روی tty5.

۱۶. کلاً login کاربر root را به‌صورت مستقیم از طریق ssh می‌بندیم تا اگر کاربر root، broute force شد کسی از طریق کاربر root نتواند login شود.

vi /etc/ssh/sshd_config
PermitRootLogin no
:wq

/itc/init.d/sshd restart

۱۷. به خودتان ssh کنید.

cat /etc/security/console.apps/authconfig

USER=root

PROGRAM=/usr/share/authconfig/authconfig.py

هر فایلی که در مسیر /etc/security/console.apps تعریف شده است، نام یک دستور است.

در مورد reboot این‌گونه نیست که پسورد بپرسد. اگر می‌خواهید user معمولی نتواند reboot کند فایلش را حذف کنید. Power off نیز همین‌طور.

rm-f /etc/security/console.apps/reboot

۱۸. قابلیت این را باید داشته باشید که tty تان را lock کنید از vlock استفاده نمایید.

yum install vlock

System → lock screen

vlock -c: tty را lock می‌کند.

vlock -a: تمام کنسول‌ها را lock می‌کند ولی task شما را اول اجرا می‌کند.

۱۹. کاربر lp برای print گرفتن است. می‌توانید آن را حذف نمایید.

cat /etc/passwd | grep ^lp

البته قبل از پاک کردن از passwd و shadow پشتیبان تهیه نمایید.

۲۰. وقتی کلیدهای Ctrl+Alt+F1..N را برای تعویض ترمینال می‌زنید، نسخه سیستم‌عامل نمایش داده می‌شود و این مسئله از لحاظ امنیتی مناسب نیست. پیغامی که قبل از Login به کاربر نشان داده می‌شود در مسیر /etc/issue قرار دارد:

cat /etc/issue

CentOS release 5.5 (Final)

Kernel \r on an \m

پیغامی که بعد از Login بـه کـاربر نشـان داده مـی‌شـود در مسـیر /etc/motd قرار دارد:

[root@mx1 ~]# cat /etc/motd

پیغامی که قبل از telnet کردن کاربر نشان داده مـی‌شـود در مسـیر /etc/issue.net قرار دارد:

cat /etc/issue.net

CentOS release 5.5 (Final)

Kernel \r on an \m

می‌توانید محتوای این فایل‌ها را حذف نماییـد و فقـط \t \d at قـرار دهید تا تاریخ و ساعت را نمایش دهد.

برای ssh هم این مسئله وجود دارد:

```
vi /etc/ssh/sshd_config
Banner /etc/issue

/etc/init.d/sshd reload
```

۲۱. پورت‌هایی که در حالت Listen قرار گرفته‌اند را ببندید.

```
netstat -ntlp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address               Foreign
Address         State       PID/Program name
tcp        0      0 192.168.0.17:110            0.0.0.0:*
LISTEN      3849/tcpserver
tcp        0      0 127.0.0.1:783               0.0.0.0:*
LISTEN      3713/spamd.pid
tcp        0      0 0.0.0.0:465                 0.0.0.0:*
LISTEN      3850/tcpserver
tcp        0      0 0.0.0.0:21                  0.0.0.0:*
LISTEN      3699/vsftpd
```