بنام خدا

امنیت سرور لینوکس

bl2k@rapmail.net

shabgard security Teams

تنظیمات بایوس سخت افزاری:
تنظیم بایوس برای جلوگیری از راه اندازی (بوت) سیستم از ابزار هایی مثل فلاپی یا سی دی رام یا هارد دوم
قرار دادن پسورد ورودی برای ورود به سیستم و تنظیمات بایوس

قبل از شروع هرگونه عملی ابتدا اتصال سرور رو از شبکه محلی قطع می کنیم چراکه هنوز کار تنظیمات به پایان نرسیده و هرآن ممکن هست که سرور مورد حمله قرار بگیره

```
#/etc/rc.d/init.d/network stop
Shutting down interface eth0 [OK]
Disabling Ipv4 packet forwarding [OK]
                                                    برای شروع
# /etc/rc.d/init.d/network start
 Setting network parameters [OK]
 Bringing up interface lo [OK]
 Bringing up interface eth0 [OK]
```

انتخاب پسورد مناسب:
بهترین پسوردها امروزه با روشهای جدید در عرض چند دقیقه شکسته شده پس انتخاب پسوردی با طول زیاد مثلا ۱۵ کارکتر با ترکیب حروف و اعداد و حروف غیر استاندارد حتما توصیه میشه بطور مثال

```
&bk@34%6<]fa%~
```

یوزر ریشه یا همون روت از خطرناک ترین یوزر های سیستم عامل لینوکس می باشدکه با دسترسی به این کاربر کل سیستم به خطر خواهد افتاد چه بسا بعد از انجام کاری محل کاره خود را ترک کنید و سیستم با این کاربر روشن بماند برا ی جلوگیری از این اتفاق خط زیر را مطابق دستورات وارد کنید

```
#vi /etc/profile
                                    بعداز کلمه HISTSIZE= خطوط زیر را وارد کنید
TMOUT=7200
```

با به کار گیری سیستم فایل NFSمیتوان سطح دسترسی به بعضی از هاست ها رو کنترل کرد
مطابق دستورات زیر در /etc/exports

```
#vi /etc/exports
                                    بطور مثال خطوط زیر را وارد کنید(ro=readonly ,root_squash=no access root)

 /dir/to/export host1.mydomain.com(ro,root_squash)
/dir/to/export host2.mydomain.com(ro,root_squash)
```

جلوگیری از را اندازی سرور در حالت single-user-mode
در این مود لینوکس که به صورت level 1 شروع به کار می کند حتی در صورت وجود پسورد سرور بدون پسورد وارد کاربر ریشه می شود برای جلوگیری از این حالت در صورت استفاده از دستور از بوت منو

```
LILO: linux single
```

موارد زیر را انجام میدهیم

```
#vi /etc/inittab
                                                این خط رو
id:3:initdefault:
                                            به شکل زیر تغییر می دهیم
id:3:initdefault:
~~:S:wait:/sbin/sulogin
                                                برای ثبت تغییرات
#/sbin/init q
```

با انجام موارد بالا با انتخاب این مود کاری از بوت منو بدون ورودپسورد دسترسی غیر ممکن خواهد بود

اعمال تغییرات لازم برای کارایی بهتر و امنیت بیشتر در به نمایش درآوردن گزینه های بوت لودر به صورت زیر در فایل مربوط

```
#vi /etc/lilo.conf
boot=/dev/sda
map=/boot/map
install=/boot/boot.b
prompt  برای حذف درخواست پسورد در ابتدای بوت این خط رو حذف کنید
Timeout=00  زمان نمایش انتخاب بوت لودر درصورت وجود صفر نمایش داده نمی شود
linear message=/boot/message  درصورت عدم نیاز به پنجره خوش آمدگویی حذف شود
default=linux restricted  درصورت نیاز به کنترل بیشتر و عدم دسترسی بدون پسورد در صورت بوت در حالت ریموت
password=<password>  پسورد خود را اینجا وارد کنید
image=/boot/vmlinuz-2.4.2-2
label=linux
initrd=/boot/initrd-2.4.2-2.img
read-only
root=/dev/sda6
```

برای عدم دسترسی کاربران بجز روت به فایل lilio.conf دستور زیر را وارد می کنیم

```
#chmod 600 /etc/lilo.conf
                                                    برای ثبت تغییرات
#/sbin/lilo -v
LILO version 21.4-4, copyright © 1992-1998 Wernerr Almesberger  lba32
 extentions copyright © 1999,2000 John Coffman
Reading boot sector from /dev/sda
had : ATAPI 32X CD-ROM drive, 128kB Cache Merging with /boot/boot.b Mapping message file /boot/message
Boot image : /boot/vmlinuz-2.2.16-22 Mapping RAM disk /boot/initrd-2.2.16-22.img
Added linux *
/boot/boot.0800 exists
no backup copy made.
Writing boot sector.
```

از کار انداختن کلید های معمول ری ست CTRL+ALT+DEL

```
#vi /etc/inittab
                                                    این خط رو
ca::ctrlaltdel:/sbin/shutdown -t3 -r now
                                                    به شکل زیر تغییر می دهیم
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
                                                    برای ثبت تغییرات
#/sbin/init q
```

امنیت بیشتر برای دسترسی به کنسول سیستم تغییرات به شکل زیر در فایل مربوطه انجام می پذیرد

```
#vi /etc/securetty
                                                    به شکل زیر تغییر می دهیم
```

```
vc/1                                                tty1
#vc/2                                               #tty2
#vc/3                                               #tty3
#vc/4                                               #tty4
#vc/5                                               #tty5
#vc/6                                               #tty6
#vc/7                                               #tty7
#vc/8                                               #tty8
#vc/9                                               #tty9
#vc/10                                              #tty10
#vc/11                                              #tty11
```

حذف گروه های کاربری و کاربران که به صورت پیش فرض وجود دارد

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

برای حذف گروه های بدون استفاده

```
# groupdel adm
# groupdel lp
# groupdel news
# groupdel mail
# groupdel uucp
# groupdel games
# groupdel dip
```

اضافه کردن یوزر های مورد نیاز سیستم بطور مثال

```
#useradd admin
تعریف پسورد برای یوز وارد شده
#passwd admin
خروجی به صورت زیر خواهد بود
Changing password for user admin
New UNIX password:
Retype new UNIX password:
passwd: all authentication tokens updated successfully
```

برا هشدار در صورت تغییرات در فایلهای مهمی چون...passwd,shadow
به صورت زیر عمل می کنیم

```
# chattr +i /etc/passwd
# chattr +i /etc/shadow
# chattr +i /etc/group
# chattr +i /etc/gshadow
در صورت نیاز به برگشت به حالت قبل -i استفاده شود
```

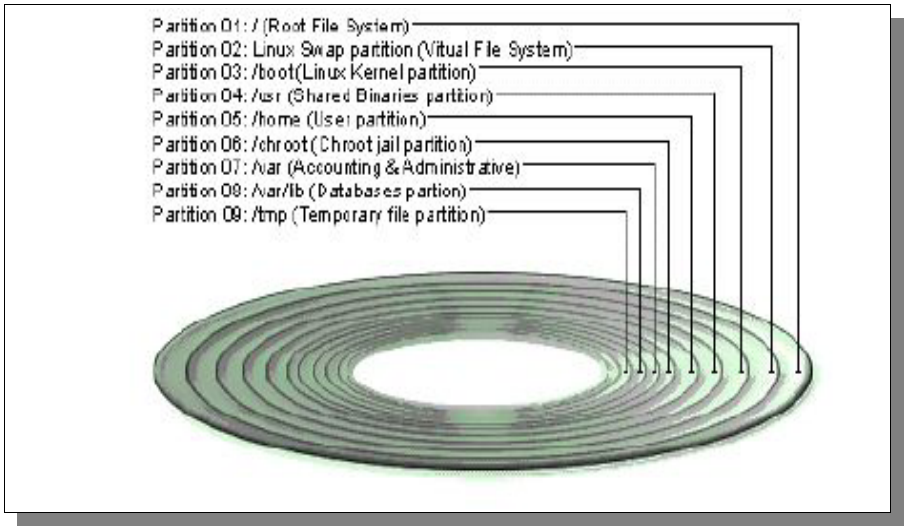
گزینه هایی که در فایل fstabبرای درایو ها و ابزارهای مانت شده میتوان استفاده کرد

defaults	دسترسی آزاد نوشتن خواندن ریشه
Noquota	Do not set users quotas on this partition.
nosuid	SUID/SGID عدم ایجاد دسترسی.
nodev	عدم دسترسی ابزارهای دیگر به این پارتیشن
noexec	عدم اجرای برنامه های باینری اجرا شدنی
quota	Allow users quotas on this partition.
ro	فقط خواندنی
rw	نوشت و خواندن
suid	SUID/SGID دسترسی با سطح

با در نظر گرفتن این پارتیشن بندی در نصب به صورت
حداقل ها به صورت زیر(این اعداد برای لینوکس ۷.۲ نوشته شده)

/boot	5	MB	All Kernel images are kept here.
<Swap>	512	MB	Our swap partition. The virtual memory of the Linux operating system.
/	256	MB	Our root partition.
/usr	512	MB	Must be large, since many Linux binaries programs are installed here.
/home	5700	MB	Proportional to the number of users you intend to host. (i.e. 100 MB per users * by the number of users 57 = 5700 MB)
/var	256	MB	Contains files that change when the system run normally (i.e. Log files).
/tmp	329	MB	Our temporary files partition (must always reside on its own partition).

/chroot	256	MB	If you want to install programs in chroot jail environment (i.e. DNS, Apache).
/var/lib	1000	MB	Partition to handle SQL or Proxy Database Server files (i.e. MySQL, Squid).



برای مثال یک نمونه از محتویات فایل/etc/fstab نشان داده می شود

For example change:

```
LABEL=/cache        /cache      ext2    defaults        1 2
LABEL=/home         /home       ext2    defaults        1 2
LABEL=/tmp          /tmp        ext2    defaults        1 2
```

To read:

```
LABEL=/cache        /cache      ext2    defaults,nodev      1 2
LABEL=/home         /home       ext2    defaults,nosuid     1 2
LABEL=/tmp          /tmp        ext2    defaults,nosuid,noexec      1 2
```

```
[root@deep /]# cat /proc/mounts
/dev/root /   ext2    rw 0 0
/proc /proc   proc    rw 0 0
/dev/sda1     /boot       ext2    ro 0 0
/dev/sda10    /cache      ext2    rw,nodev 0 0
/dev/sda9     /chroot     ext2    rw 0 0
/dev/sda8     /home       ext2    rw,nosuid 0 0
/dev/sda13    /tmp        ext2    rw,noexec,nosuid 0 0
/dev/sda7     /usr        ext2    rw 0 0
/dev/sda11    /var        ext2    rw 0 0
/dev/sda12    /var/lib    ext2    rw 0 0
none  /dev/pts    devpts  rw 0 0
```

جلوگیری از اجرای برنامه نصب کننده پکیج ها بجز مدیریت هاست

```
#chmod 700 /bin/rpm
```

مقدار زمان برای ورود به سیستم رو با اضافه کردن خطوط زیر به /etc/profile کم می کنیم

```
#vi /etc/profile
HISTSIZE=1000
                                                به این مقدار تغییرمیدیهم
HISTSIZE=10
                                  برای جلوگیری از ذخیره شده History در فایل bash_history.
HISTFILESIZE=0
```

پریینت گرفتن اتوماتیک از تمامlogفایلهای مهم درصورت ورود کرکر به سیستم که مورد هدف قرار می گیرد

```
#vi /etc/syslog.conf
                                                خطوط زیر اضافه
authpriv.*;mail.*;local7.*;auth.*;daemon.info /dev/lp0
                                                راه اندازی دوباره سیستم لوگ
#/etc/rc.d/init.d/syslog restart
                                                خروجی انجام دستور
Shutting down kernel logger: [OK]
Shutting down system logger: [OK]
Starting system logger: [OK]
Starting kernel logger: [OK]
```

تنظیم سطح دسترسی به شاخه اتواستارت اسکریپیت های اجرای سرویس ها و برنامه های سیستم

```
#chmod -R 700 /etc/init.d/*
```

بطور پیش فرض بعد از ورود به سیستم کرنل لینوکس نگارش و نوع خود را اعلام می کند که اطلاعات خوبی برای یک نفوذگر حساب میشود با اعمال تغییرات زیر مشکل فوق قابل حل است

```
#vi /etc/rc.local
```

```
--
# This will overwrite /etc/issue at every boot.  So, make any changes you
# want to make to /etc/issue here or you will lose them when you reboot.
#echo "" > /etc/issue
#echo "$R" >> /etc/issue
#echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue
#
#cp -f /etc/issue /etc/issue.net
#echo >> /etc/issue
--
```

با غیر فعال کردن خطوط موجود و حذف فایلهای issue.net , issue به صورت زیر

```
Then, remove the following files: issue.net and issue under /etc/ directory:
[root@deep /]# rm -f /etc/issue
[root@deep /]# rm -f /etc/issue.net
```

پیدا کردن فایلهایی که در یوزر root با فعال بودن خاصیت SUID (-r-xr-sr-x) SGID(-rwsr-xr-x) قابل اجرا هستن
دقت کنید این برنامه ها از طرف سیستم قابل اجرا هستت---محل اجرای این فایلها مهم می باشدکه در دسترس یوزرمعمولی نباشد

- To find all files with the 's' bits from root-owned programs, use the command:

```
[root@deep]# find / -type f \( -perm -04000 -o -perm -02000 \) -exec ls -
l {} \;

*-rwsr-xr-x   1 root     root        34220    Jul 18 14:13  /usr/bin/chage
*-rwsr-xr-x   1 root     root        36344    Jul 18 14:13  /usr/bin/gpasswd
-rwxr-sr-x    1 root     man         35196    Jul 12 03:50  /usr/bin/man
-r-s--x--x    1 root     root        13536    Jul 12 07:56  /usr/bin/passwd
-rwxr-sr-x    1 root     mail        10932    Jul 12 10:03  /usr/bin/suidperl
-rwsr-sr-x    1 root     mail        63772    Jul 12 10:03  /usr/bin/sperl5.6.0
-rwxr-sr-x    1 root     slocate     23964    Jul 23 17:48  /usr/bin/slocate
*-r-xr-sr-x   1 root     tty         6524     Jul 12 03:19  /usr/bin/wall
*-rws--x-x    1 root     root        13184    Jul 21 19:15  /usr/bin/chfn
*-rws--x-x    1 root     root        12640    Jul 21 19:15  /usr/bin/chsh
*-rws--x-x    1 root     root        5464     Jul 21 19:15  /usr/bin/newgrp
*-rwxr-sr-x   1 root     tty         8500     Jul 21 19:15  /usr/bin/write
*-rwsr-xr-x   1 root     root        6288     Jul 26 10:22  /usr/sbin/usernetctl
-rwxr-sr-x    1 root     utmp        6584     Jul 13 00:46  /usr/sbin/utempter
*-rwsr-xr-x   1 root     root        20540    Jul 25 07:33  /bin/ping
-rwsr-xr-x    1 root     root        14184    Jul 12 20:47  /bin/su
*-rwsr-xr-x   1 root     root        55356    Jul 12 05:01  /bin/mount
*-rwsr-xr-x   1 root     root        25404    Jul 12 05:01  /bin/umount
*-rwxr-sr-x   1 root     root        4116     Jul 26 10:22  /sbin/netreport
-r-sr-xr-x    1 root     root        14732    Jul 26 14:06  /sbin/pwdb_chkpwd
-r-sr-xr-x    1 root     root        15340    Jul 26 14:06  /sbin/unix_chkpwd
```

برای عیر فعال کردن این دسترسی با دستورات زیر این خاصیت رو از برنامه میگیریم

```
# chmod a-s /usr/bin/chage
# chmod a-s /usr/bin/gpasswd
# chmod a-s /usr/bin/wall
# chmod a-s /usr/bin/chfn
# chmod a-s /usr/bin/chsh
# chmod a-s /usr/bin/newgrp
# chmod a-s /usr/bin/write
# chmod a-s /usr/sbin/usernetctl
# chmod a-s /bin/ping
# chmod a-s /bin/mount
# chmod a-s /bin/umount
# chmod a-s /sbin/netreport
```

اجازه ندهید یک ماشین داخل شبکه آدرس MAC(Media access control) رو به سرور اعلام کنه

For each IP address of INTERNAL computers in your network, use the following command to know the MAC address associate with the IP address:

```
[root@deep /]# ifconfig
eth0      Link encap:Ethernet  HWaddr 00:50:DA:C6:D3:FF
          inet addr:207.35.78.3  Bcast:207.35.78.32  Mask:255.255.255.224
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1887318 errors:0 dropped:0 overruns:1 frame:0
          TX packets:2709329 errors:0 dropped:0 overruns:0 carrier:1
          collisions:18685 txqueuelen:100
          Interrupt:10 Base address:0xb000

eth1      Link encap:Ethernet  HWaddr 00:50:DA:C6:D3:09
          inet addr:192.168.1.11  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:182937 errors:0 dropped:0 overruns:0 frame:0
          TX packets:179612 errors:0 dropped:0 overruns:0 carrier:0
          collisions:7434 txqueuelen:100
          Interrupt:11 Base address:0xa800

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          UP LOOPBACK RUNNING  MTU:3924  Metric:1
          RX packets:7465 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7465 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
```

با این دستورات آدرس MACبه صورت دستی وارد می شود

```
# arp -s 207.35.78.3 00:50:DA:C6:D3:FF
# arp -s 192.168.1.11 00:50:DA:C6:D3:09
```

بعدازانجام تغییرات سیستم دوباره راه اندازی شود

پیداکردن حذف فایهای زاید و مخفی

```
find / -name ".. " -print -xdev
find / -name ".*" -print -xdev | cat -v
```

```
find / -type f \( -perm -2 -o -perm -20 \) -exec ls -lg {} \;
```

پیداکردن فایهایی که به گروه خاصی تعلق ندارند(توجه داشته باشید فایلهای شاخه/dev/ در نظر گرفته نمی شود)

```
#find -nouser -o -nogroup
```

End Part 1
Coming Soon Next Section...
bl2k@rapmail.net
Shabgard Security Teams

Pluggable Authentication Modules (PAM)
بهنیه سازی سیستم بررسی کننده هویت کاربران

طول پسورد

موقع نصب لینوکس حداقل طول پسورد ورودی به صورت پیش فرض ۵ کاراکتر در نظر گرفته شده است برای اطمینان از انتخاب کاربران با طول مناسب که امنیت نسبی رو ایجاد کنه می توانیم حداقل طول پسورد ورودی رو افزایش دهیم جهت انجام این کار :

#vi /etc/pam.d/passwd

خط زیر رو پاک می کنیم

password required /lib/security/pam_stack.so service=system-auth

مقادیر زیر به فایل /etc/pam.d/system-auth اضافه می کنیم

```
Password        required        /lib/security/pam_cracklib.so retry=3
password        sufficient      /lib/security/pam_unix.so nullok use_authtok md5 shadow
password        required        /lib/security/pam_deny.so
```

مقادیر زیر به فایل /etc/pam.d/passwd اضافه می کنیم

```
Password        required        /lib/security/pam_cracklib.so retry=3 minlen=12
Password        sufficient      /lib/security/pam_unix.so nullok use_authtok md5
shadow
password        required        /lib/security/pam_deny.so
```

غیر فعال کردن دسترسی برنامه ها به کنسول

```
# rm -f /etc/security/console.apps/halt
# rm -f /etc/security/console.apps/poweroff
# rm -f /etc/security/console.apps/reboot
# rm -f /etc/security/console.apps/shutdown
```

در صورت کاربرد این فرمان فقط یوزر ریشه حق دسترسی به محیط X را خواهد داشت

```
# rm -f /etc/security/console.apps/xserver
```

برای غیر فعال کردن کل دسترسی ها به کنسول می توان از اسکریپیت زیر سود جست

```
# !/bin/sh
cd /etc/pam.d
for i in * ; do
sed '/[^#].*pam_console.so/s/^/#/' < $i > foo && mv foo $i
done
```

که بنام disabling.sh ذخیره شه و بدین صورت اجرا شود

```
# chmod 700 disabling.sh
# ./disabling.sh
```

برای محدود کردن دسترسی به سیستم از راه دور

```
# vi /etc/security/access.conf
```

دسترسی ریشه به آی پی مورد نظر **207.35.78.2**

```
-:ALL EXCEPT root gmourani:207.35.78.2
-:ALL:LOCAL
```

و همچنین با تغییر فایل زیر برای اطمینان از اجرای مود sshd (مود با ضریب امنیت بالا)

```
# vi /etc/pam.d/login
```

account required /lib/security/pam_access.so

برای رسیدن به امنیت قابل قبول سیستم گرافیکی لینوکس نصب نمی شود یا در صورت امکان بایستی ابزار هایی مثل صدا... نصب نشوند برای رسیدن به منظور مراحل زیر دنبال می شود:

#vi /etc/security/console.perms

```
# file classes -- these are regular expressions
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
<xconsole>=:[0-9]\.[0-9] :[0-9]
# device classes -- these are shell-style globs
<floppy>=/dev/fd[0-1]*
<sound>=/dev/dsp* /dev/audio* /dev/midi* \
/dev/mixer* /dev/sequencer
<cdrom>=/dev/cdrom* /dev/cdwriter*
<pilot>=/dev/pilot
<jaz>=/dev/jaz
<zip>=/dev/zip
<scanner>=/dev/scanner
<fb>=/dev/fb /dev/fb[0-9]*
<kbd>=/dev/kbd
<joystick>=/dev/js*
<v4l>=/dev/video* /dev/radio* /dev/winradio* /dev/vtx* /dev/vbi*
<gpm>=/dev/gpmctl
<dri>=/dev/dri/* /dev/nvidia*
# permission definitions
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <sound> 0640 root.sys
<console> 0600 <cdrom> 0600 root.disk
<console> 0600 <pilot> 0660 root.tty
<console> 0600 <jaz> 0660 root.disk
<console> 0600 <zip> 0660 root.disk
<console> 0600 <scanner> 0600 root
<console> 0600 <fb> 0600 root
<console> 0600 <kbd> 0600 root
<console> 0600 <joystick> 0600 root
<console> 0600 <v4l> 0600 root
<console> 0700 <gpm> 0700 root
<xconsole> 0600 /dev/console 0600 root.root
<xconsole> 0600 <dri> 0600 root
```

با انجام تغییرات به صورت زیر

```
# file classes -- these are regular expressions
<console>=tty[0-9][0-9]* :[0-9]\.[0-9] :[0-9]
# device classes -- these are shell-style globs
<floppy>=/dev/fd[0-1]*
<cdrom>=/dev/cdrom* /dev/cdwriter*
<pilot>=/dev/pilot
<fb>=/dev/fb /dev/fb[0-9]*
<kbd>=/dev/kbd
<gpm>=/dev/gpmctl
<dri>=/dev/dri/* /dev/nvidia*
# permission definitions
<console> 0660 <floppy> 0660 root.floppy
<console> 0600 <cdrom> 0600 root.disk
<console> 0600 <pilot> 0660 root.tty
<console> 0600 <fb> 0600 root
<console> 0600 <kbd> 0600 root
```

<console> 0700 <gpm> 0700 root

محدود کردن منابع سیستم از کاربران

با انجام این عمل می توان در مقابل حملاتی مانند dos که منابع سیستمي رو به هدر میدهند مقابله کرد

#vi /etc/security/limits.conf

و با اضافه کردن خطوط زیر

*** hard core 0**
*** hard rss 5000** Memory used 5M
*** hard nproc 35** number process

و یا گروه خاصی از کاربران به صورت زیر

@users hard core 0
@users hard rss 5000
@users hard nproc 35

گام بعدی اضافه کردن خطوط زیر در فایل login به ترتیب زیر :

#vi /etc/pam.d/login

session required /lib/security/pam_limits.so

کنترل زمانی دسترسی به سرویس دهی

با این عمل می توان دسترسی یوزر ریشه رو به ساعات و یا روزهای خاصی از هفته محدود کرد

#vi /etc/security/time.conf

با ویرایش خط زیر

login ; tty* & !ttyp* ; !root !gmourani ; !Al0000-2400

بطور مثال دسترسی بین ساعات ۸ صبح تا ۶ عصر کاربر admin روز سه شنبه بطور هفتگی مجاز است:

login ; * ; !admin ; !Wd0000-2400 !Tu0800-1800

طام بعدی انجام مراحل زیر برای فعال سازی مدول زمانبندی است:

#vi /etc/pam.d/login

و اضافه کردن خطوط زیر

account required /lib/security/pam_time.so

بلوکه کردن دسترسی روت برای SU(Substitute User)

#vi /etc/pam.d/su

و اضافه کردن خطوط زیر

auth required /lib/security/pam_wheel.so use_uid

بدین معنی که کاربرانی که در گروه wheel با su امکان دسترسي به ریشه خواهند داشت لذا برای دسترسی یوزر ادمین ایجاد شده مراحل زیر باید انجام شود:

 # usermod -G10 admin

برای ورود کاربرانی که در گروه wheel قرار دارد بدون وارد کردن پسورد کاربر ریشه طبق مراحل زیر عمل می کنیم:

#vi /etc/pam.d/su

و اضافه کردن خطوط زیر

auth sufficient /lib/security/pam_wheel.so trust use_uid

End Part II
Bl2k@shabgarg.org
Shabgard Security Teams

Linux Kernel
کامپایل کرنل و بروز رسانی آن

استفاده از آخرین نسخه کرنل که قلب تپنده لینوکس محسوب می شود باعث افزایش امنیت و جلوگیری از حمله های نفوذگران خواهد شد که با استفاده از آسیب پذیری های کشف شده در سطح کرنل انجام می پذیرند.

برای دریافت آخرین نسخه های آن به سایت http://www.kernel.org مراجعه و نگارش پایدار کرنل مورد نظر و یا بسته های بروز رسان نسخه های پیشین را دریافت کنید.

در صورت استفاده از آخرین نگارش کرنل ممکن است برنامه های موجود روی لینوکس به درستی کار نکنند برای رفع این مشکل باید نسخه ای که ایراد پیدا میکند دوباره برای این نسخه از کرنل با استفاده از سورس برنامه مربوطه دوباره کامپایل شود یا از بسته های کامپایل شده جدید استفاده شود.

قبل از شروع کار از وجود بسته های نصب شده با استفاده از دستورات زیر اطمنیان حاصل کنید:

iptables (فایروال سیستم عامل لینوکس)

```
[root@tango /]# rpm -q iptables
package iptables is not installed
```

quota (محدودکننده و مونیتورینگ)

```
[root@tango /]# rpm -q quota
package quota is not installed
```

و برای نصب برنامه های فوق به صورت زیر عمل می کنیم:

ابتدا سی دی رام را بصورت زیر معرفی می کنیم(عمل مانت کردن)

```
[root@tango /]# mount /dev/cdrom /mnt/cdrom/
had: ATAPI 32X CD-ROM drive, 128kB Cache
mount: block device dev/cdrom is write-protected, mounting read-only
```

برای نصب Iptables

```
[root@tango /]# cd /mnt/cdrom/RedHat/RPMS/
[root@tango RPMS]# rpm -Uvh iptables-version.i386.rpm
iptables ########################################################
```

برای نصب quota

```
[root@tango /]# cd /mnt/cdrom/RedHat/RPMS/
[root@tango RPMS]# rpm -Uvh quota-version.i386.rpm
quota ########################################################
```

نحوه تنظیمات این دو برنامه در بخشهای بعدی مفصل توضیح داده خواهد شد.

تهیه نسخه پشتیبان از کرنل موجود بر رو فلاپی

با استفاده از دستور زیر مسیر و نگارش بوت لینوکس بدست می آوریم:

```
[root@tango /]# cat /etc/lilo.conf
boot=/dev/sda
map=/boot/map
install=/boot/boot.b
timeout=00
default=linux
restricted
password=mypasswd
image=/boot/vmlinuz-2.4.2-2   نگارش کرنل لینوکس
label=linux   the image we booted from
initrd=/boot/initrd-2.4.2-2.img
read-only
root=/dev/sda6
```

با استفاده از فرمان زیر یه کپی بر روی فلاپی از نسخه قدیمی تهیه می کنیم:

```
[root@tango /]# mkbootdisk --device /dev/fd0H1440 2.4.2-2
Insert a disk in /dev/fd0. Any information on the disk will be lost.
Press <Enter> to continue or ^C to abort:
```

در صورتیکه پارتشین بوت فقط خواندنی است با استفاده از خطوط زیر این مشکل را حل نمایید(بعد از انجام کار دوباره به حالت اول تغییر داده شود)

```
#vi /etc/fstab
LABEL=/boot /boot ext2 defaults,ro 1 2
To read:
LABEL=/boot /boot ext2 defaults 1 2
```

گام بعدی

```
[root@tango /]# mount /boot –oremount
```

براي صحت از انجام دستورات بالا

```
[root@tango /]# cat /proc/mounts
/dev/root / ext2 rw 0 0
/proc /proc proc rw 0 0
/dev/sda1 /boot ext2 rw 0 0
/dev/sda10 /cache ext2 rw,nodev 0 0
/dev/sda9 /chroot ext2 rw 0 0
/dev/sda8 /home ext2 rw,nosuid 0 0
/dev/sda13 /tmp ext2 rw,noexec,nosuid 0 0
/dev/sda7 /usr ext2 rw 0 0
/dev/sda11 /var ext2 rw 0 0
/dev/sda12 /var/lib ext2 rw 0 0
none /dev/pts devpts rw 0 0
```

برای کپی سورس کرنل جدید

```
[root@tango /]# cp linux-version.tar.gz /usr/src/
```

براي ورود به شاخه سورس

```
[root@tango /]# cd /usr/src/
```

برای پاک کردن نسخه قبلی به ترتیب

```
[root@tango src]# rm -f linux
[root@tango src]# rm -rf linux-2.4.x/
[root@tango src]# rm -f /boot/vmlinuz-2.4.x
[root@tango src]# rm -f /boot/System.map-2.4.x
[root@tango src]# rm -rf /lib/modules/2.4.x/
```

در صورتی که کرنل قبلی بصورت بسته نصب شده مراحل زیر را دنبال کنید :

```
[root@tango src]# rpm -qa | grep kernel
kernel-2.4.2-2
kernel-headers-2.4.2-2
```

برای حذف بسته کرنل به فورمت زیر عمل می کنیم که با جاگذاری نتیجه بالا در دستور زیر :

```
[root@tango src]# rpm -e –nodeps kernel-2.4.2-2 kernel-headers-2.4.2-2
```

برای خارج کردن سورس از حالت فشرده به صورت زیر:

[root@tango src]# **tar xzpf linux-version.tar.gz**

و براي حذف سورس به صورت فايل آرشيو

[root@tango src]# **rm -f linux-version.tar.gz**

برای دست یابی به بیشترین سازگاری کرنل جدید تغییرات زیر رو در فایلهای مربوطه به شکل زیر انجام دهید:

#vi +66 /usr/src/linux/include/linux/sem.h

پارامتر فوق

#define SEMMNI 128 /* <= IPCMNI max # of semaphore identifiers */

به شکل زیر

#define SEMMNI 512 /* <= IPCMNI max # of semaphore identifiers */

#vi +26 /usr/src/linux/kernel/printk.c

پارامتر زیر

#define LOG_BUF_LEN (16384)

به صورت

#define LOG_BUF_LEN (65536)

#vi +19 /usr/src/linux/Makefile

پارامتر فوق

HOSTCFLAGS = -Wall -Wstrict-prototypes -O2 -fomit-frame-pointer

به شکل زیر

HOSTCFLAGS = -Wall -Wstrict-prototypes -O3 -funroll-loops -fomitframe-Pointer

و همچنین

#vi +90 /usr/src/linux/Makefile

پارامتر زیر

CFLAGS := $(CPPFLAGS) -Wall -Wstrict-prototypes -O2 -fomit-frame-pointer -fno-strict-aliasing

به شکل زیر

CFLAGS := $(CPPFLAGS) -Wall -Wstrict-prototypes -O3 -funroll-loops -fomit-frame-pointer -fno-strict-aliasing

توجه :
براي مثال براي نصب يك **وصله امنيتي** **linux-2.4.5-ow1.tar.gz** به شكل زير عمل ميكنيم

[root@tango /]# **cp linux-2.4.5-ow1.tar.gz /usr/src/**
[root@tango /]# **cd /usr/src/**
[root@tango src]# **tar xzpf linux-2.4.5-ow1.tar.gz**
[root@tango src]# **cd linux-2.4.5-ow1/**
[root@tango linux-2.4.5-ow1]# **mv linux-2.4.5-ow1.diff /usr/src/**
[root@tango linux-2.4.5-ow1]# **cd ..**
[root@tango src]# **patch -p0 < linux-2.4.5-ow1.diff**
[root@tango src]# **rm -rf linux-2.4.5-ow1**
[root@tango src]# **rm -f linux-2.4.5-ow1.diff**
[root@tango src]# **rm -f linux-2.4.5-ow1.tar.gz**

پاک کردن کرنل بطور کامل

مراحل زیر را قبل از وارد شدن به مرحله تنظیم مدولهای کرنل با دستورات زیر انجام می دیهم توجه داشته باشید با این کار کل کرنل بطور کامل حتی فایلهای Header پاک می شوند

```
[root@tango src]# cd /usr/include/
[root@tango include]# rm -f asm linux
[root@tango include]# ln -s /usr/src/linux/include/asm-i386 asm
[root@tango include]# ln -s /usr/src/linux/include/linux linux

[root@tango include]# cd /usr/src/linux/
[root@tango linux]# make mrproper
```

در ترمینال با وارد کردن دستور make config وارد محیط متنی تنظیمات مدولی کرنل خواهیم شد

```
[root@tango /]# cd /usr/src/linux/ مطمئن شوید که در این شاخه قرار دارید؟
[root@tango linux]# make config
rm -f include/asm
( cd include ; ln -sf asm-i386 asm)
/bin/sh scripts/Configure arch/i386/config.in
#
# Using defaults found in arch/i386/defconfig
#
```

در این قسمت انتخاب های زیر رو می توان با انتخاب کلید های مورد نظر انجام داد

[y] برای کامپایل کرنل باز شده.
[m] برای استفاده از یک مدول
[n] برای عدم انتخاب یک قسمت و یا مدول

روشهای مختلفی مانند monolithic kernel و modularized kernel براي كامپايل كرنل موجود است كه در ادامه از روش monolithic kernel استفاده خواهد شد. در این روش درایور سخت افزار همراه با کد کرنل به صورت مجتمع کامپایل خواهد شد.
برای مثال سیستم فوق با مشخصات سخت افزاری زیر را در نظر میگیریم:

1 Pentium-III 667 MHz (i686) processor
1 Motherboard Asus P3V4X Pro 133Mhz EIDE
1 Hard Disk Ultra ATA/66 EIDE
1 Chipset Apollo Pro133A
1 CD-ROM ATAPI IDE
1 Floppy Disk
2 Ethernet Cards 3COM 3c597 PCI 10/100
1 Mouse PS/2

به جواب هایی که با y یا n در حالت پررنگ دقت کنید شما هم مراحل زیر رو دنبال می کنید

```
rm -f include/asm
( cd include ; ln -sf asm-i386 asm)
/bin/sh scripts/Configure arch/i386/config.in
#
# Using defaults found in arch/i386/defconfig
#
*
* Code maturity level options
*
Prompt for development and/or incomplete code/drivers (CONFIG_EXPERIMENTAL) [N/y/?]
*
* Loadable module support
*
Enable loadable module support (CONFIG_MODULES) [Y/n/?]
Set version information on all module symbols (CONFIG_MODVERSIONS) [Y/n/?] n
Kernel module loader (CONFIG_KMOD) [Y/n/?]
*
* Processor type and features
```

*
Processor family (386, 486, 586/K5/5x86/6x86/6x86MX, Pentium-Classic, Pentium-MMX, Pentium-Pro/Celeron/Pentium-II, Pentium-III, Pentium-4, K6/K6-II/K6-III, Athlon/K7, Crusoe, Winchip-C6, Winchip-2, Winchip-2A/Winchip-3) [Pentium-III] **Pentium-Pro/Celeron/Pentium-II**
defined CONFIG_M686
Toshiba Laptop support (CONFIG_TOSHIBA) [N/y/m/?]
/dev/cpu/microcode - Intel IA32 CPU microcode support (CONFIG_MICROCODE) [N/y/m/?]
/dev/cpu/*/msr - Model-specific register support (CONFIG_X86_MSR) [N/y/m/?]
/dev/cpu/*/cpuid - CPU information support (CONFIG_X86_CPUID) [N/y/m/?]
High Memory Support (off, 4GB, 64GB) [off]
defined CONFIG_NOHIGHMEM
Math emulation (CONFIG_MATH_EMULATION) [N/y/?] (NEW)
MTRR (Memory Type Range Register) support (CONFIG_MTRR) [N/y/?]
Symmetric multi-processing support (CONFIG_SMP) [Y/n/?] **n**
APIC and IO-APIC support on uniprocessors (CONFIG_X86_UP_IOAPIC) [N/y/?] (NEW) **y**
*
*** General setup**
*
Networking support (CONFIG_NET) [Y/n/?]
SGI Visual Workstation support (CONFIG_VISWS) [N/y/?]
PCI support (CONFIG_PCI) [Y/n/?]
PCI access mode (BIOS, Direct, Any) [Any]
defined CONFIG_PCI_GOANY
PCI device name database (CONFIG_PCI_NAMES) [Y/n/?] **n**
EISA support (CONFIG_EISA) [N/y/?]
MCA support (CONFIG_MCA) [N/y/?]
Support for hot-pluggable devices (CONFIG_HOTPLUG) [Y/n/?] **n**
System V IPC (CONFIG_SYSVIPC) [Y/n/?]
BSD Process Accounting (CONFIG_BSD_PROCESS_ACCT) [N/y/?]
Sysctl support (CONFIG_SYSCTL) [Y/n/?]
Kernel core (/proc/kcore) format (ELF, A.OUT) [ELF]
defined CONFIG_KCORE_ELF
Kernel support for a.out binaries (CONFIG_BINFMT_AOUT) [Y/m/n/?]
Kernel support for ELF binaries (CONFIG_BINFMT_ELF) [Y/m/n/?]
Kernel support for MISC binaries (CONFIG_BINFMT_MISC) [Y/m/n/?]
Power Management support (CONFIG_PM) [Y/n/?] **n**
*
*** Memory Technology Devices (MTD)**
*
Memory Technology Device (MTD) support (CONFIG_MTD) [N/y/m/?]
*
*** Parallel port support**
*
Parallel port support (CONFIG_PARPORT) [N/y/m/?]
*
*** Plug and Play configuration**
*
Plug and Play support (CONFIG_PNP) [Y/m/n/?] **n**
*
*** Block devices**
*
Normal PC floppy disk support (CONFIG_BLK_DEV_FD) [Y/m/n/?]
XT hard disk support (CONFIG_BLK_DEV_XD) [N/y/m/?]
Compaq SMART2 support (CONFIG_BLK_CPQ_DA) [N/y/m/?]
Compaq CISS Array support (CONFIG_BLK_CPQ_CISS_DA) [N/y/m/?]
Mylex DAC960/DAC1100 PCI RAID Controller support (CONFIG_BLK_DEV_DAC960) [N/y/m/?]
Loopback device support (CONFIG_BLK_DEV_LOOP) [N/y/m/?]
Network block device support (CONFIG_BLK_DEV_NBD) [N/y/m/?]
RAM disk support (CONFIG_BLK_DEV_RAM) [N/y/m/?]
*
*** Multi-device support (RAID and LVM)**
*

Multiple devices driver support (RAID and LVM) (CONFIG_MD) [N/y/?]
*
*** Networking options**
*
Packet socket (CONFIG_PACKET) [Y/m/n/?]
Packet socket: mmapped IO (CONFIG_PACKET_MMAP) [N/y/?] **y**
Kernel/User netlink socket (CONFIG_NETLINK) [N/y/?] **y**
Routing messages (CONFIG_RTNETLINK) [N/y/?] (NEW) **y**
Netlink device emulation (CONFIG_NETLINK_DEV) [N/y/m/?] (NEW) **y**
Network packet filtering (replaces ipchains) (CONFIG_NETFILTER) [N/y/?] **y**
Network packet filtering debugging (CONFIG_NETFILTER_DEBUG) [N/y/?] (NEW) **y**
Socket Filtering (CONFIG_FILTER) [N/y/?]
Unix domain sockets (CONFIG_UNIX) [Y/m/n/?]
TCP/IP networking (CONFIG_INET) [Y/n/?]
IP: multicasting (CONFIG_IP_MULTICAST) [Y/n/?] **n**
IP: advanced router (CONFIG_IP_ADVANCED_ROUTER) [N/y/?] **y**
IP: policy routing (CONFIG_IP_MULTIPLE_TABLES) [N/y/?] (NEW) **y**
IP: use netfilter MARK value as routing key (CONFIG_IP_ROUTE_FWMARK) [N/y/?] (NEW) **y**
IP: fast network address translation (CONFIG_IP_ROUTE_NAT) [N/y/?] (NEW) **y**
IP: equal cost multipath (CONFIG_IP_ROUTE_MULTIPATH) [N/y/?] (NEW) **y**
IP: use TOS value as routing key (CONFIG_IP_ROUTE_TOS) [N/y/?] (NEW) **y**
IP: verbose route monitoring (CONFIG_IP_ROUTE_VERBOSE) [N/y/?] (NEW) **y**
IP: large routing tables (CONFIG_IP_ROUTE_LARGE_TABLES) [N/y/?] (NEW) **y**
IP: kernel level autoconfiguration (CONFIG_IP_PNP) [N/y/?]
IP: tunneling (CONFIG_NET_IPIP) [N/y/m/?]
IP: GRE tunnels over IP (CONFIG_NET_IPGRE) [N/y/m/?]
IP: TCP Explicit Congestion Notification support (CONFIG_INET_ECN) [N/y/?]
IP: TCP syncookie support (disabled per default) (CONFIG_SYN_COOKIES) [N/y/?] **y**
*
*** IP: Netfilter Configuration**
*
Connection tracking (required for masq/NAT) (CONFIG_IP_NF_CONNTRACK) [N/y/m/?] (NEW) **m**
FTP protocol support (CONFIG_IP_NF_FTP) [N/m/?] (NEW) **m**
IP tables support (required for filtering/masq/NAT) (CONFIG_IP_NF_IPTABLES) [N/y/m/?] (NEW) **m**
limit match support (CONFIG_IP_NF_MATCH_LIMIT) [N/m/?] (NEW) **m**
MAC address match support (CONFIG_IP_NF_MATCH_MAC) [N/m/?] (NEW) **m**
netfilter MARK match support (CONFIG_IP_NF_MATCH_MARK) [N/m/?] (NEW) **m**
Multiple port match support (CONFIG_IP_NF_MATCH_MULTIPORT) [N/m/?] (NEW) **m**
TOS match support (CONFIG_IP_NF_MATCH_TOS) [N/m/?] (NEW) **m**
tcpmss match support (CONFIG_IP_NF_MATCH_TCPMSS) [N/m/?] (NEW) **m**
Connection state match support (CONFIG_IP_NF_MATCH_STATE) [N/m/?] (NEW) **m**
Packet filtering (CONFIG_IP_NF_FILTER) [N/m/?] (NEW) **m**
REJECT target support (CONFIG_IP_NF_TARGET_REJECT) [N/m/?] (NEW) **m**
Full NAT (CONFIG_IP_NF_NAT) [N/m/?] (NEW) **m**
MASQUERADE target support (CONFIG_IP_NF_TARGET_MASQUERADE) [N/m/?] (NEW) **m**
REDIRECT target support (CONFIG_IP_NF_TARGET_REDIRECT) [N/m/?] (NEW) **m**
Packet mangling (CONFIG_IP_NF_MANGLE) [N/m/?] (NEW) **m**
TOS target support (CONFIG_IP_NF_TARGET_TOS) [N/m/?] (NEW) **m**
MARK target support (CONFIG_IP_NF_TARGET_MARK) [N/m/?] (NEW) **m**
LOG target support (CONFIG_IP_NF_TARGET_LOG) [N/m/?] (NEW) **m**
TCPMSS target support (CONFIG_IP_NF_TARGET_TCPMSS) [N/m/?] (NEW) **m**
ipchains (2.2-style) support (CONFIG_IP_NF_COMPAT_IPCHAINS) [N/y/m/?] (NEW)
ipfwadm (2.0-style) support (CONFIG_IP_NF_COMPAT_IPFWADM) [N/y/m/?] (NEW)
*
*
*
The IPX protocol (CONFIG_IPX) [N/y/m/?]
Appletalk protocol support (CONFIG_ATALK) [N/y/m/?]
DECnet Support (CONFIG_DECNET) [N/y/m/?]
802.1d Ethernet Bridging (CONFIG_BRIDGE) [N/y/m/?]
*
*** QoS and/or fair queuering**

*
QoS and/or fair queuing (EXPERIMENTAL) (CONFIG_NET_SCHED) [N/y/?]
*
*** Telephony Support**
*
Linux telephony support (CONFIG_PHONE) [N/y/m/?]
*
*** ATA/IDE/MFM/RLL support**
*
ATA/IDE/MFM/RLL support (CONFIG_IDE) [Y/m/n/?] **m**
*
*** IDE, ATA and ATAPI Block devices**
*
Enhanced IDE/MFM/RLL disk/cdrom/tape/floppy support (CONFIG_BLK_DEV_IDE) [M/n/?]
*
* Please see Documentation/ide.txt for help/info on IDE drives
*
Use old disk-only driver on primary interface (CONFIG_BLK_DEV_HD_IDE) [N/y/?]
Include IDE/ATA-2 DISK support (CONFIG_BLK_DEV_IDEDISK) [M/n/?]
Use multi-mode by default (CONFIG_IDEDISK_MULTI_MODE) [N/y/?]
Include IDE/ATAPI CDROM support (CONFIG_BLK_DEV_IDECD) [M/n/?]
Include IDE/ATAPI TAPE support (CONFIG_BLK_DEV_IDETAPE) [N/y/m/?]
Include IDE/ATAPI FLOPPY support (CONFIG_BLK_DEV_IDEFLOPPY) [N/y/m/?]
SCSI emulation support (CONFIG_BLK_DEV_IDESCSI) [N/y/m/?]
*
*** IDE chipset support/bugfixes**
*
CMD640 chipset bugfix/support (CONFIG_BLK_DEV_CMD640) [Y/n/?] **n**
RZ1000 chipset bugfix/support (CONFIG_BLK_DEV_RZ1000) [Y/n/?] **n**
Generic PCI IDE chipset support (CONFIG_BLK_DEV_IDEPCI) [Y/n/?]
Sharing PCI IDE interrupts support (CONFIG_IDEPCI_SHARE_IRQ) [Y/n/?]
Generic PCI bus-master DMA support (CONFIG_BLK_DEV_IDEDMA_PCI) [N/y/?] **y**
Boot off-board chipsets first support (CONFIG_BLK_DEV_OFFBOARD) [N/y/?]
Use PCI DMA by default when available (CONFIG_IDEDMA_PCI_AUTO) [N/y/?] **y**
AEC62XX chipset support (CONFIG_BLK_DEV_AEC62XX) [N/y/?]
ALI M15x3 chipset support (CONFIG_BLK_DEV_ALI15X3) [N/y/?]
AMD Viper support (CONFIG_BLK_DEV_AMD7409) [N/y/?]
CMD64X chipset support (CONFIG_BLK_DEV_CMD64X) [N/y/?]
CY82C693 chipset support (CONFIG_BLK_DEV_CY82C693) [N/y/?]
Cyrix CS5530 MediaGX chipset support (CONFIG_BLK_DEV_CS5530) [N/y/?]
HPT34X chipset support (CONFIG_BLK_DEV_HPT34X) [N/y/?]
HPT366 chipset support (CONFIG_BLK_DEV_HPT366) [N/y/?]
Intel PIIXn chipsets support (CONFIG_BLK_DEV_PIIX) [N/y/?]
NS87415 chipset support (EXPERIMENTAL) (CONFIG_BLK_DEV_NS87415) [N/y/?]
PROMISE PDC20246/PDC20262/PDC20267 support (CONFIG_BLK_DEV_PDC202XX) [N/y/?]
ServerWorks OSB4 chipset support (CONFIG_BLK_DEV_OSB4) [N/y/?]
SiS5513 chipset support (CONFIG_BLK_DEV_SIS5513) [N/y/?]
SLC90E66 chipset support (CONFIG_BLK_DEV_SLC90E66) [N/y/?]
Tekram TRM290 chipset support (EXPERIMENTAL) (CONFIG_BLK_DEV_TRM290) [N/y/?]
VIA82CXXX chipset support (CONFIG_BLK_DEV_VIA82CXXX) [N/y/?]
Other IDE chipset support (CONFIG_IDE_CHIPSETS) [N/y/?]
IGNORE word93 Validation BITS (CONFIG_IDEDMA_IVB) [N/y/?] (NEW)
*
*** SCSI support**
*
SCSI support (CONFIG_SCSI) [Y/m/n/?]
*
*** SCSI support type (disk, tape, CD-ROM)**
*
SCSI disk support (CONFIG_BLK_DEV_SD) [Y/m/n/?]
Maximum number of SCSI disks that can be loaded as modules (CONFIG_SD_EXTRA_DEVS) [40]
SCSI tape support (CONFIG_CHR_DEV_ST) [N/y/m/?]

SCSI OnStream SC-x0 tape support (CONFIG_CHR_DEV_OSST) [N/y/m/?]
SCSI CD-ROM support (CONFIG_BLK_DEV_SR) [N/y/m/?]
SCSI generic support (CONFIG_CHR_DEV_SG) [N/y/m/?]
*
* Some SCSI devices (e.g. CD jukebox) support multiple LUNs
*
Enable extra checks in new queueing code (CONFIG_SCSI_DEBUG_QUEUES) [Y/n/?] **n**
Probe all LUNs on each SCSI device (CONFIG_SCSI_MULTI_LUN) [Y/n/?] **n**
Verbose SCSI error reporting (kernel size +=12K) (CONFIG_SCSI_CONSTANTS) [Y/n/?] **n**
SCSI logging facility (CONFIG_SCSI_LOGGING) [N/y/?]
*
*** SCSI low-level drivers**
*
3ware Hardware ATA-RAID support (CONFIG_BLK_DEV_3W_XXXX_RAID) [N/y/m/?]
7000FASST SCSI support (CONFIG_SCSI_7000FASST) [N/y/m/?]
ACARD SCSI support (CONFIG_SCSI_ACARD) [N/y/m/?]
Adaptec AHA152X/2825 support (CONFIG_SCSI_AHA152X) [N/y/m/?]
Adaptec AHA1542 support (CONFIG_SCSI_AHA1542) [N/y/m/?]
Adaptec AHA1740 support (CONFIG_SCSI_AHA1740) [N/y/m/?]
Adaptec AIC7xxx support (CONFIG_SCSI_AIC7XXX) [N/y/m/?] **y**
Enable Tagged Command Queueing (TCQ) by default (CONFIG_AIC7XXX_TCQ_ON_BY_DEFAULT) [N/y/?] (NEW) **y**
Maximum number of TCQ commands per device (CONFIG_AIC7XXX_CMDS_PER_DEVICE) [8] (NEW)
Collect statistics to report in /proc (CONFIG_AIC7XXX_PROC_STATS) [N/y/?] (NEW)
Delay in seconds after SCSI bus reset (CONFIG_AIC7XXX_RESET_DELAY) [5] (NEW)
AdvanSys SCSI support (CONFIG_SCSI_ADVANSYS) [N/y/m/?]
Always IN2000 SCSI support (CONFIG_SCSI_IN2000) [N/y/m/?]
AM53/79C974 PCI SCSI support (CONFIG_SCSI_AM53C974) [N/y/m/?]
AMI MegaRAID support (CONFIG_SCSI_MEGARAID) [N/y/m/?]
BusLogic SCSI support (CONFIG_SCSI_BUSLOGIC) [N/y/m/?]
Compaq Fibre Channel 64-bit/66Mhz HBA support (CONFIG_SCSI_CPQFCTS) [N/y/m/?]
DMX3191D SCSI support (CONFIG_SCSI_DMX3191D) [N/y/m/?]
DTC3180/3280 SCSI support (CONFIG_SCSI_DTC3280) [N/y/m/?]
EATA ISA/EISA/PCI (DPT and generic EATA/DMA-compliant boards) support (CONFIG_SCSI_EATA) [N/y/m/?]
EATA-DMA [Obsolete] (DPT, NEC, AT&T, SNI, AST, Olivetti, Alphatronix) support (CONFIG_SCSI_EATA_DMA) [N/y/m/?]
EATA-PIO (old DPT PM2001, PM2012A) support (CONFIG_SCSI_EATA_PIO) [N/y/m/?]
Future Domain 16xx SCSI/AHA-2920A support (CONFIG_SCSI_FUTURE_DOMAIN) [N/y/m/?]
GDT SCSI Disk Array Controller support (CONFIG_SCSI_GDTH) [N/y/m/?]
Generic NCR5380/53c400 SCSI support (CONFIG_SCSI_GENERIC_NCR5380) [N/y/m/?]
IBM ServeRAID support (CONFIG_SCSI_IPS) [N/y/m/?]
Initio 9100U(W) support (CONFIG_SCSI_INITIO) [N/y/m/?]
Initio INI-A100U2W support (CONFIG_SCSI_INIA100) [N/y/m/?]
NCR53c406a SCSI support (CONFIG_SCSI_NCR53C406A) [N/y/m/?]
NCR53c7,8xx SCSI support (CONFIG_SCSI_NCR53C7xx) [N/y/m/?]
NCR53C8XX SCSI support (CONFIG_SCSI_NCR53C8XX) [N/y/m/?]
SYM53C8XX SCSI support (CONFIG_SCSI_SYM53C8XX) [Y/m/n/?] **n**
PAS16 SCSI support (CONFIG_SCSI_PAS16) [N/y/m/?]
PCI2000 support (CONFIG_SCSI_PCI2000) [N/y/m/?]
PCI2220i support (CONFIG_SCSI_PCI2220I) [N/y/m/?]
PSI240i support (CONFIG_SCSI_PSI240I) [N/y/m/?]
Qlogic FAS SCSI support (CONFIG_SCSI_QLOGIC_FAS) [N/y/m/?]
Qlogic ISP SCSI support (CONFIG_SCSI_QLOGIC_ISP) [N/y/m/?]
Qlogic ISP FC SCSI support (CONFIG_SCSI_QLOGIC_FC) [N/y/m/?]
Qlogic QLA 1280 SCSI support (CONFIG_SCSI_QLOGIC_1280) [N/y/m/?]
Seagate ST-02 and Future Domain TMC-8xx SCSI support (CONFIG_SCSI_SEAGATE) [N/y/m/?]
Simple 53c710 SCSI support (Compaq, NCR machines) (CONFIG_SCSI_SIM710) [N/y/m/?]
Symbios 53c416 SCSI support (CONFIG_SCSI_SYM53C416) [N/y/m/?]
Tekram DC390(T) and Am53/79C974 SCSI support (CONFIG_SCSI_DC390T) [N/y/m/?]
Trantor T128/T128F/T228 SCSI support (CONFIG_SCSI_T128) [N/y/m/?]
UltraStor 14F/34F support (CONFIG_SCSI_U14_34F) [N/y/m/?]

UltraStor SCSI support (CONFIG_SCSI_ULTRASTOR) [N/y/m/?]
*
*** I2O device support**
*
I2O support (CONFIG_I2O) [N/y/m/?]
*
*** Network device support**
*
Network device support (CONFIG_NETDEVICES) [Y/n/?]
*
*** ARCnet devices**
*
ARCnet support (CONFIG_ARCNET) [N/y/m/?]
Dummy net driver support (CONFIG_DUMMY) [M/n/y/?]
Bonding driver support (CONFIG_BONDING) [N/y/m/?]
EQL (serial line load balancing) support (CONFIG_EQUALIZER) [N/y/m/?]
Universal TUN/TAP device driver support (CONFIG_TUN) [N/y/m/?]
General Instruments Surfboard 1000 (CONFIG_NET_SB1000) [N/y/m/?]
*
*** Ethernet (10 or 100Mbit)**
*
Ethernet (10 or 100Mbit) (CONFIG_NET_ETHERNET) [Y/n/?]
3COM cards (CONFIG_NET_VENDOR_3COM) [N/y/?]
AMD LANCE and PCnet (AT1500 and NE2100) support (CONFIG_LANCE) [N/y/m/?]
Western Digital/SMC cards (CONFIG_NET_VENDOR_SMC) [N/y/?]
Racal-Interlan (Micom) NI cards (CONFIG_NET_VENDOR_RACAL) [N/y/?]
DEPCA, DE10x, DE200, DE201, DE202, DE422 support (CONFIG_DEPCA) [N/y/m/?]
HP 10/100VG PCLAN (ISA, EISA, PCI) support (CONFIG_HP100) [N/y/m/?]
Other ISA cards (CONFIG_NET_ISA) [N/y/?]
EISA, VLB, PCI and on board controllers (CONFIG_NET_PCI) [Y/n/?]
AMD PCnet32 PCI support (CONFIG_PCNET32) [N/y/m/?]
Apricot Xen-II on board Ethernet (CONFIG_APRICOT) [N/y/m/?]
CS89x0 support (CONFIG_CS89x0) [N/y/m/?]
DECchip Tulip (dc21x4x) PCI support (CONFIG_TULIP) [N/y/m/?]
Generic DECchip & DIGITAL EtherWORKS PCI/EISA (CONFIG_DE4X5) [N/y/m/?]
Digi Intl. RightSwitch SE-X support (CONFIG_DGRS) [N/y/m/?]
EtherExpressPro/100 support (CONFIG_EEPRO100) [Y/m/n/?]
National Semiconductor DP83810 series PCI Ethernet support (CONFIG_NATSEMI) [N/y/m/?]
PCI NE2000 and clones support (see help) (CONFIG_NE2K_PCI) [N/y/m/?]
RealTek RTL-8139 PCI Fast Ethernet Adapter support (CONFIG_8139TOO) [N/y/m/?]
SiS 900/7016 PCI Fast Ethernet Adapter support (CONFIG_SIS900) [N/y/m/?]
SMC EtherPower II (CONFIG_EPIC100) [N/y/m/?]
Sundance Alta support (CONFIG_SUNDANCE) [N/y/m/?]
TI ThunderLAN support (CONFIG_TLAN) [N/y/m/?]
VIA Rhine support (CONFIG_VIA_RHINE) [N/y/m/?]
Winbond W89c840 Ethernet support (CONFIG_WINBOND_840) [N/y/m/?]
Sun Happy Meal 10/100baseT PCI support (CONFIG_HAPPYMEAL) [N/y/m/?]
Pocket and portable adapters (CONFIG_NET_POCKET) [N/y/?]
*
*** Ethernet (1000 Mbit)**
*
Alteon AceNIC/3Com 3C985/NetGear GA620 Gigabit support (CONFIG_ACENIC) [N/y/m/?]
Packet Engines Hamachi GNIC-II support (CONFIG_HAMACHI) [N/y/m/?]
SysKonnect SK-98xx support (CONFIG_SK98LIN) [N/y/m/?]
FDDI driver support (CONFIG_FDDI) [N/y/?]
PPP (point-to-point protocol) support (CONFIG_PPP) [N/y/m/?]
SLIP (serial line) support (CONFIG_SLIP) [N/y/m/?]
*
*** Wireless LAN (non-hamradio)**
*
Wireless LAN (non-hamradio) (CONFIG_NET_RADIO) [N/y/?]
*

*** Token Ring devices**
*
Token Ring driver support (CONFIG_TR) [N/y/?]
Fibre Channel driver support (CONFIG_NET_FC) [N/y/?]
*
*** Wan interfaces**
*
Wan interfaces support (CONFIG_WAN) [N/y/?]
*
*** Amateur Radio support**
*
Amateur Radio support (CONFIG_HAMRADIO) [N/y/?]
*
*** IrDA (infrared) support**
*
IrDA subsystem support (CONFIG_IRDA) [N/y/m/?]
*
*** ISDN subsystem**
*
ISDN support (CONFIG_ISDN) [N/y/m/?]
*
*** Old CD-ROM drivers (not SCSI, not IDE)**
*
Support non-SCSI/IDE/ATAPI CDROM drives (CONFIG_CD_NO_IDESCSI) [N/y/?]
*
*** Input core support**
*
Input core support (CONFIG_INPUT) [N/y/m/?]
*
*** Character devices**
*
Virtual terminal (CONFIG_VT) [Y/n/?]
Support for console on virtual terminal (CONFIG_VT_CONSOLE) [Y/n/?]
Standard/generic (8250/16550 and compatible UARTs) serial support (CONFIG_SERIAL) [Y/m/n/?]
Support for console on serial port (CONFIG_SERIAL_CONSOLE) [N/y/?]
Extended dumb serial driver options (CONFIG_SERIAL_EXTENDED) [N/y/?]
Non-standard serial port support (CONFIG_SERIAL_NONSTANDARD) [N/y/?]
Unix98 PTY support (CONFIG_UNIX98_PTYS) [Y/n/?]
Maximum number of Unix98 PTYs in use (0-2048) (CONFIG_UNIX98_PTY_COUNT) [256] **128**
*
*** I2C support**
*
I2C support (CONFIG_I2C) [N/y/m/?]
*
*** Mice**
*
Bus Mouse Support (CONFIG_BUSMOUSE) [N/y/m/?]
Mouse Support (not serial and bus mice) (CONFIG_MOUSE) [Y/m/n/?]
PS/2 mouse (aka "auxiliary device") support (CONFIG_PSMOUSE) [Y/n/?]
C&T 82C710 mouse port support (as on TI Travelmate) (CONFIG_82C710_MOUSE) [N/y/m/?]
PC110 digitizer pad support (CONFIG_PC110_PAD) [N/y/m/?]
*
*** Joysticks**
*
*
* Input core support is needed for joysticks
*
QIC-02 tape support (CONFIG_QIC02_TAPE) [N/y/m/?]
*
*** Watchdog Cards**
*
Watchdog Timer Support (CONFIG_WATCHDOG) [N/y/?]

Intel i8x0 Random Number Generator support (CONFIG_INTEL_RNG) [N/y/m/?]
/dev/nvram support (CONFIG_NVRAM) [N/y/m/?]
Enhanced Real Time Clock Support (CONFIG_RTC) [N/y/m/?]
Double Talk PC internal speech card support (CONFIG_DTLK) [N/y/m/?]
Siemens R3964 line discipline (CONFIG_R3964) [N/y/m/?]
Applicom intelligent fieldbus card support (CONFIG_APPLICOM) [N/y/m/?]
*
*** Ftape, the floppy tape device driver**
*
Ftape (QIC-80/Travan) support (CONFIG_FTAPE) [N/y/m/?]
/dev/agpgart (AGP Support) (CONFIG_AGP) [Y/m/n/?] **n**
Direct Rendering Manager (XFree86 DRI support) (CONFIG_DRM) [Y/n/?] **n**
*
*** Multimedia devices**
*
Video For Linux (CONFIG_VIDEO_DEV) [N/y/m/?]
*
*** File systems**
*
Quota support (CONFIG_QUOTA) [N/y/?]
Kernel automounter support (CONFIG_AUTOFS_FS) [N/y/m/?]
Kernel automounter version 4 support (also supports v3) (CONFIG_AUTOFS4_FS) [Y/m/n/?] **n**
DOS FAT fs support (CONFIG_FAT_FS) [N/y/m/?]
Compressed ROM file system support (CONFIG_CRAMFS) [N/y/m/?]
Simple RAM-based file system support (CONFIG_RAMFS) [N/y/m/?]
ISO 9660 CDROM file system support (CONFIG_ISO9660_FS) [Y/m/n/?] **m**
Microsoft Joliet CDROM extensions (CONFIG_JOLIET) [N/y/?]
Minix fs support (CONFIG_MINIX_FS) [N/y/m/?]
NTFS file system support (read only) (CONFIG_NTFS_FS) [N/y/m/?]
OS/2 HPFS file system support (CONFIG_HPFS_FS) [N/y/m/?]
/proc file system support (CONFIG_PROC_FS) [Y/n/?]
/dev/pts file system for Unix98 PTYs (CONFIG_DEVPTS_FS) [Y/n/?]
ROM file system support (CONFIG_ROMFS_FS) [N/y/m/?]
Second extended fs support (CONFIG_EXT2_FS) [Y/m/n/?]
System V and Coherent file system support (read only) (CONFIG_SYSV_FS) [N/y/m/?]
UDF file system support (read only) (CONFIG_UDF_FS) [N/y/m/?]
UFS file system support (read only) (CONFIG_UFS_FS) [N/y/m/?]
*
*** Network File Systems**
*
Coda file system support (advanced network fs) (CONFIG_CODA_FS) [N/y/m/?]
NFS file system support (CONFIG_NFS_FS) [Y/m/n/?] **n**
NFS server support (CONFIG_NFSD) [Y/m/n/?] **n**
SMB file system support (to mount Windows shares etc.) (CONFIG_SMB_FS) [N/y/m/?]
NCP file system support (to mount NetWare volumes) (CONFIG_NCP_FS) [N/y/m/?]
*
*** Partition Types**
*
Advanced partition selection (CONFIG_PARTITION_ADVANCED) [N/y/?]
*
*** Console drivers**
*
VGA text console (CONFIG_VGA_CONSOLE) [Y/n/?]
Video mode selection support (CONFIG_VIDEO_SELECT) [N/y/?]
*
*** Sound**
*
Sound card support (CONFIG_SOUND) [Y/m/n/?] **n**
*
(Security options will appear only if you are patched your kernel with the Openwall Project patch).
*** Security options**
*

Non-executable user stack area (CONFIG_SECURE_STACK) [Y]
Autodetect and emulate GCC trampolines (CONFIG_SECURE_STACK_SMART) [Y]
Restricted links in /tmp (CONFIG_SECURE_LINK) [Y] **n**
Restricted FIFOs in /tmp (CONFIG_SECURE_FIFO) [Y]
Restricted /proc (CONFIG_SECURE_PROC) [N] **y**
Special handling of fd 0, 1, and 2 (CONFIG_SECURE_FD_0_1_2) [Y]
Enforce RLIMIT_NPROC on execve(2) (CONFIG_SECURE_RLIMIT_NPROC) [Y]
Destroy shared memory segments not in use (CONFIG_SECURE_SHM) [N]
*
*** USB support**
*
Support for USB (CONFIG_USB) [Y/m/n/?] **n**
*
*** Kernel hacking**
*
Magic SysRq key (CONFIG_MAGIC_SYSRQ) [N/y/?]
*** End of Linux kernel configuration.
*** Check the top-level Makefile for additional configuration.
*** Next, you must run 'make dep'.

حال می رسیم به کامپایل بعد از مراحل بالا به شکل زیر:

[root@tango linux]# **make dep; make clean; make bzImage**

حال کرنل به صورت فشرده شده آماده نصب می باشد
توجه:
بعد از اتمام مرحله فوق در روش بعدی باید استفاده از مدولهای موجود برای کرنل را فعال سازیم در صورتی که به انتخاب

Enable loadable module support (CONFIG_MODULES)

در قسمت Modularized kernel جواب بلی داده اید.

[root@tango linux]# **make modules**
[root@tango linux]# **make modules_install**

برای نصب کرنل آماده شده مراحل زیر را دنبال می کنیم:

[root@tango /]# **cd /usr/src/linux/**
[root@tango linux]# **cp arch/i386/boot/bzImage /boot/vmlinuz-2.4.5**

گام دوم:

[root@tango /]# **cd /usr/src/linux/**
[root@tango linux]# **cp System.map /boot/System.map-2.4.5**

گام سوم:

[root@tango linux]# **cd /boot/**
[root@tango /boot]# **ln -fs vmlinuz-2.4.5 vmlinuz**
[root@tango /boot]# **ln -fs System.map-2.4.5 System.map**

گام پنجم:

[root@tango /]# **cd /boot/**
[root@tango /boot]# **rm –f module-info**
[root@tango /boot]# **rm –f initrd-2.4.x.img**

گام ششم:

[root@tango /]# **cd /usr/src/linux/**
[root@tango linux]# **cp -r include/asm-generic ../linux-2.4.5/include/**
[root@tango linux]# **cp -r include/asm-i386 ../linux-2.4.5/include/**
[root@tango linux]# **cp -r include/linux ../linux-2.4.5/include/**
[root@tango linux]# **cd ../**
[root@tango src]# **rm -rf /usr/src/linux**
[root@tango src]# **cd /usr/src/**
[root@tango src]# **ln -s /usr/src/linux-2.4.5 linux**

و در پایان فایل lilo رو به شکل زیر تغییر مي دهیم

[root@tango /]# **vi /etc/lilo.conf**

```
boot=/dev/sda
map=/boot/map
install=/boot/boot.b
timeout=00 default=linux
restricted
password=somepasswd

image=/boot/vmlinuz
label=linux read-only
root=/dev/sda6
```

برای ثبت تغییرات:

[root@tango /]# **/sbin/lilo -v**

```
LILO version 21.4-4, copyright © 1992-1998 Wernerr Almesberger 'lba32' extentions
copyright © 1999,2000 John Coffman

Reading boot sector from /dev/sda had : ATAPI 32X CD-ROM
drive, 128kB Cache Merging with /boot/boot.b Mapping
message file /boot/message Boot image : /boot/vmlinuz
Added linux * /boot/boot.0800 exists – no backup copy made.
Writing boot sector.
```

روش دوم در بخشهای بعدی توضیح داده خواهد شد

End Part 3
By : bl2k@shabgard.org
To be continue.....