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
```

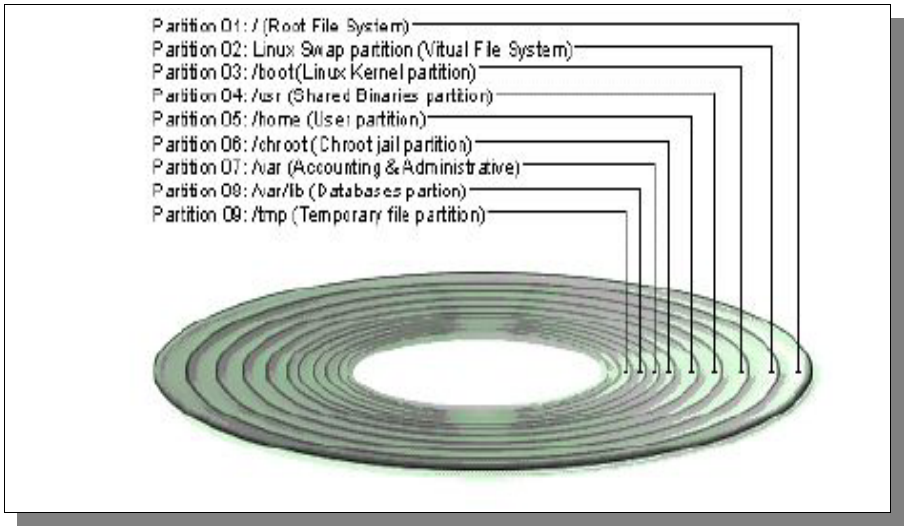
گزینه هایی که در فایل fstabبرای درایو ها و ابزارهای مانت شده میتوان استفاده کرد

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