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