Enter the new value, or press ENTER for the default

طبق خط بالا شما یا باید مقادیر خودتان را وارد کنید و یا اینکه با زدن Enter مقدار پیش‌فرض را که داخل براکت های باز/بسته هستند را برای هر پرسش وارد کنید.

فهرست گزینه‌های دستور chage

l- یا list–: برای فهرست کردن جزئیات گذرواژه هر کاربر دلخواه به کار می‌رود:

ابتدا یک تغییر در گذرواژه کاربری به نام Mahdi می‌دهیم. (با دستور زیر گذرواژه کاربر را حذف یا Delete می‌کنیم.)

passwd -d Mahdi

حالا دستور زیر را اجرا می‌کنیم. در خروجی و در سطر Last password change تاریخ امروز را برای آخرین زمان تغییر نشان می‌دهد.

chage -l Mahdi

OUTPUT

Last password change : Jul 31, 2015

Password expires : never

Password inactive : never

Account expires : never

Minimum number of days between password change
: 0

Maximum number of days between password change
: 99999

Number of days of warning before password expires
: 7

هر کاربر مجوز اجرای دستور زیر را دارد. به جای username نام کاربری خودش را باید بنویسد و می‌تواند اطلاعات خودش را ببیند اما مجوز این کار را برای دیگر کاربران ندارد. این یک دلیل امنیتی است که حتی دیگر کاربران از آخرین به‌روزرسانی گذرواژه شما هم خبر ندارند چه برسد به دانستن خود گذرواژه؛ اما کاربر root می‌تواند اطلاعات همه را ببیند.

تنظیم تاریخ انقضا با گزینه M برای یک کاربر: کاربر ریشه قادر به تنظیم تاریخ انقضا گذرواژه برای تمام کاربران است. شکل کلی استفاده از این گزینه به‌صورت زیر است.

chage -M number-of-days username

number-of-days نشان دهنده تعداد روزهای بعد از آخرین تغییر که گذرواژه منقضی یا Expire می‌شود، می‌باشد. دستور زیر را اجرا کنید. پس از اجرای دستور زیر دوباره دستور chage -l username را اجرا کنید. (بجای username نام کاربری خودتان را وارد کنید.)

chage -M 10 Mahdi

تغییر در سطر دستور chage -l Mahdi

Maximum number of days between password change :
10

یک پیام هشدار دهنده به هنگام Login که مقدار پیش‌فرض آن ۷ روز است در هنگام وارد شدن به سیستم به کاربر نشان داده می‌شود؛

یعنی ۷ روز مانده به Expire شدن این پیام نشان داده می‌شود و روز بعد که ۶ روز مانده و الی آخر.

Warning: your password will expire in 3 days

پس از اینکه مهلت کاربر به زمان منقضی شدن گذرواژه‌اش رسید سیستم او را مجبور به ایجاد یک گذرواژه جدید می‌نماید.

You are required to change your password immediately (password aged)

WARNING: Your password has expired.

You must change your password now and login again!

Changing password for dhinesh

(current) UNIX password

Enter new UNIX password

Retype new UNIX password

تنظیم منقضی شدن حساب کاربری (Account Expire): با گزینه E- می‌توانید این کار را انجام دهید. فقط باید تاریخ را به فرمت YYYY-MM-DD به‌عنوان پارامتر دستور به همراه نام کاربر به دستور chage بدهید. شکل کلی به‌صورت زیر است:

chage -E YYYY-MM-DD username

پس از اجرای دستور بالا سطر Password expires از دستور chage -l username تغییر خواهد کرد.

بلاک کردن کاربرانی که به مدت X روز به سیستم وارد نشده‌اند: اگر بعد از اینکه گذرواژه کاربر منقضی شد و به مدت X روز به سیستم برای

ورود دوباره و ایجاد یک گذرواژه جدید تلاش نکرد خودبه‌خود سیستم اکانت آن کاربر را بلاک می‌کند.

این کار توسط گزینه I- انجام می‌گیرد. شکل کلی استفاده از آن به‌صورت زیر است:

chage -I number-of-days username

چگونه انقضای یک گذرواژه را غیرفعال کنیم: برای غیرفعال کردن انقضای گذرواژه یک کاربر باید مقادیر زیر را به‌صورت زیر مقداردهی کنید:

m 0-: به گزینه m مقدار صفر بدهید. این گزینه حداقل یا minimum زمان برای تغییر کلمه عبور را نشان می‌دهد و معادل سطر Minimum number of days between password change در خروجی دستور chage -l username است. شکل کلی استفاده از آن به‌صورت زیر است:

chage -m number-of-days username

M 99999-: این گزینه معرف حداکثر زمان برای تعویض گذرواژه است و معادل سطر Maximum number of days between password change در خروجی دستور chage -l username است. شکل کلی آن:

chage -M number-of-days username

مقدار حداکثر ۰ و حداقل ۹۹۹۹۹ یعنی هیچ وقت نمی‌خواهید گذرواژه را تغییر دهید.

I -1-: مقدار ۱- (منفی یک) یعنی حساب هرگز غیرفعال یا Inactive نمی‌شود. این مقدار در خروجی بالا معادل never برای سطر

Password inactive در خروجی دستور chage -l username است. شکل کلی آن به صورت زیر است:

chage -I number-of-days username

-1 E-: مقدار ۱- (منفی یک) یعنی اکانت هیچ گاه منقضی نمی‌شود. این مقدار در خروجی بالا معادل never برای سطر Account expires در خروجی دستور chage -l username است. شکل کلی آن:

chage -E number-of-days username

چگونگی تنظیم گذرواژه و غیرفعال کردن کاربران

دو فایل /etc/passwd و /etc/shadow دو فایل مرتبط با مدیریت کاربران و به ترتیب پایگاهی برای ذخیره نام کاربران (و دیگر اطلاعات) و گذرواژه‌های آن‌ها هستند که به‌صورت رمز شده در فایل /etc/shadow ذخیره می‌شوند. دستور passwd امکان ایجاد و تعویض گذرواژه را به هر کاربر می‌دهد به‌طوری‌که هر کاربر تنها مجاز به تغییر گذرواژه خودش است، اما کاربر root دسترسی کامل را به تمامی کاربران دارد. گاهی ممکن است دیگر نیازی به نام کاربری نباشد. تحت نام کاربری فایل‌ها و دایرکتوری‌هایی وجود دارند که غالبا در دایرکتوری خانگی همان کاربر ذخیره هستند و لازم است که آن‌ها را نگه داریم پس بجای حذف کاربر که منجر به پاک شدن تمامی این اطلاعات می‌شود بهتر است نام کاربری را غیرفعال کنیم.

هر خط فایل passwd برای یک کاربر است و دومین ستون هر خط اشاره گری به ستون دوم یک خط از فایل shadow است که نشان دهنده گذرواژه رمز شده است. ستون اول از هر خط فایل shadow نام کاربر را نشان می‌دهد. اگر ستون دوم فایل shadow خالی بود، یعنی هنوز برای کاربر گذرواژه ای تنظیم نشده است ولی کاربر Enable است. اگر ستون دوم علامت !! داشته باشد و بعد از این دو علامت هیچ کاراکتر

دیگری نباشد، یعنی کاربر هم گذرواژه ندارد و هم Disable است. ولی اگر علامت !! باشد و دنباله آن‌ها کاراکترهایی باشد (همان گذرواژه رمز شده)، یعنی کاربر Disable است ولی دارای گذرواژه می‌باشد. اگر ستون دوم فقط و فقط کاراکترهایی در هم و برهم داشته باشد و علامت !! در ابتدای آن نباشد، یعنی کاربر فعال بوده و دارای گذرواژه است.

خط زیر نشان دهنده این است که گذرواژه ای برای کاربر تنظیم نشده است ولی کاربر Enable می‌باشد. برای حذف گذرواژه یک کاربر با استفاده از سوئیچ d- دستور passwd می‌توانید گذرواژه را پاک کنید. بعد اجرای دستور زیر، ستون دوم مانند خروجی زیر خالی است.

```
passwd -d USERNAME

passwd -d user1

user1::15912:0:99999:7:::
```

خط زیر که ستون دوم علامت !! را دارد، یعنی کاربر نه گذرواژه دارد و نه فعال می‌باشد. (Disable است) و به این معنی است که کاربر Lock شده است. برای Lock کردن (غیرفعال کردن) کاربری از سوئیچ l- دستور passwd استفاده کنید.

```
passwd -l USERNAME

passwd -l user1

user1:!!:15912:0:99999:7:::
```

خط زیر یعنی کاربر گذرواژه دارد (کاراکترهای درهم‌برهم بعد از !!) ولی Lock یا غیرفعال (علامت !! در ابتدای رشته درون ستون دوم) می‌باشد.

```
::::
user1:!!$6$3peLgFul$HpcMYklxKse6Vj5q4YzfiJ36UyY
```

RvVv5cx3cRZD8KzFTvvUvKLAdhrEaFbZJbMmdPnoU
ATII7DW/giNKj1Hwk0:15912:0:99999:7

خط زیر یعنی کاربر هم گذرواژه دارد و هم اینکه Enable (فعال)می‌باشد، برای Unlock کردن یک کاربر از سوئیچ u- دستور passwd استفاده کنید.

passwd -u USERNAME

passwd -u user1

:::
user1:$6$3peLgFul$HpcMYklxKse6Vj5q4YzfiJ36UyYR
vVv5cx3cRZD8KzFTvvUvKLAdhrEaFbZJbMmdPnoUA
TII7DW/giNKj1Hwk0:15912:0:99999:7

Pluggable authentication module یا PAM چیست؟

PAM مخفف Pluggable authentication module است که فرایند Authorization پویایی را برای برنامه‌های کاربردی و سرویس‌ها در لینوکس فراهم می‌کند. در بحث مهندسی امنیت و امنیت رایانه، اجازه بخشی از سیستم‌عامل می‌باشد که وظیفهٔ تخصیص منابع سیستم را به وسیلهٔ دادن دسترسی به مصرف‌کنندگانی که مجاز هستند از آن‌ها استفاده کنند بر عهده دارد. منابع شامل فایل‌های شخصی یا آیتم‌های دیتا، برنامه‌های کامپیوتر، ابزارهای کامپیوتر و قابلیت عملکرد فراهم شده توسط برنامه‌های کاربردی کامپیوتر می‌باشد. کاربران کامپیوتر، برنامه‌های کامپیوتر و ابزارهای دیگر روی کامپیوتر، نمونه‌هایی از مصرف کنندگان منابع هستند. برنامه‌هایی که اجازه دسترسی کاربران به سیستم را می‌دهند از احراز هویت (Authentication) به منظور بررسی هویت کاربر استفاده می‌کنند. با احراز هویت بررسی می‌شود که آیا کاربری که خود را معرفی کرده است واقعا خود کاربر است یا یک کاربر غیر مجاز و

نامعتبر است. هر برنامه ای احراز هویت خودش را دارد، اما در توزیع‌های لینوکسی یک کتابخانه مرکزی به نام PAM برای استفاده برنامه‌های کاربردی و سرویس به منظور مجاز شناسی و احراز هویت به کار می‌رود. به‌طور مثال سرویس SSH می‌تواند از PAM به منظور احراز هویت استفاده کند و درصورتی‌که بیش از ۳ بار ورود ناموفق داشته باشیم، دیگر اجازه دسترسی داده نمی‌شود. با PAM مدیران سیستم قادر به استفاده و اعمال سیاست‌های احراز هویت به‌صورت متمرکز برای کلیه برنامه‌های کاربردی و سرویس‌ها هستند.

فایل‌های پیکربندی PAM

فایل etc/pam.conf/، فایل پیکربندی برای هر یک از سرویس‌ها است که استفاده نمی‌شود و به جای آن به ازای هر سرویس، در زیر دایرکتوری etc/pam.d/ یک فایل پیکربندی برای آن سرویس وجود دارد که تنظیمات در آن قرار می‌گیرد. به‌طور مثال سرویس sshd یک فایل به نام sshd در زیر این دایرکتوری دارد.

```
ls /etc/pam.d
atd          halt          pm-powersave          runuser
system-auth
authconfig   imap          pm-suspend            runuser-l
system-auth-ac
authconfig-tui  kbdrate    pm-suspend-hybrid     smtp
vmtoolsd
chfn         login         pop3                  sshd      vsftpd
chsh         newrole       poweroff              su
config-util  other         reboot                sudo
```

crond	passwd	remote	sudo-i
eject	pm-hibernate	run_init	su-l

در هر کدام از فایل‌های مربوط به هر سرویس ماژول‌های PAM استفاده شده برای احراز هویت، تعریف می‌شوند. هر فایل شامل چندین خط است که هر خط آن دارای فرمت کلی زیر است.

TYPE CONTROL MODULE_PATH
MODULE_ARGS

TYPE نوع ماژول PAM مورد استفاده را نشان می‌دهد. هر نوع ماژول هدف خودش را دارد و به‌طورکلی چهار دسته ماژول PAM وجود دارد که می‌توان استفاده کرد. به‌طور مثال یک ماژول گذرواژه (گذرواژه) را بررسی می‌کند و دیگری محلی که سیستم از آن مورد دسترسی قرار گرفته است را بررسی می‌کند.

- auth: درستی و اعتبار (authenticity) کاربر را بررسی می‌کند که به‌طور معمول توسط گذرواژه صورت می‌گیرد. (البته مکانیسم‌های دیگری برای تصدیق هویت و درستی کاربر وجود دارند).
- account: ماژول‌های مربوط به این دسته بررسی می‌کنند که آیا کاربر مجوز لازم برای دسترسی و استفاده از سرویس درخواستی را دارد. برای نمونه باید بررسی شود که هیچ کس نتواند با یک اکانت منقضی شده (expire) بتواند به سیستم لاگین کند.
- password: هدف از این ماژول برای قادر ساختن به تغییر authentication token است.
- session: ماژول‌های مربوط به این دسته مسئول پیکربندی و مدیریت جلسه‌های کاربر هستند. در جلسه کاری متغیرهای محیطی مربوط به کاربر مقداردهی اولیه می‌شوند؛ مانند

متغیرهای مربوط به دایرکتوری خانگی یا همچنین محدودیت‌های حساب کاربری مربوط به کاربری که لاگین کرده است.

موارد بالا چهار دسته‌بندی کلی از ماژول‌ها هستند که هر کدام ماژول‌های خاص خود را دارند. دومین فیلد از بالا CONTROL است که اشاره به رفتار ماژول دارد. هر ماژول می‌تواند رفتارهای کنترلی زیر را داشته باشد.

- required: ماژول‌های با این flag باید پیش از احراز هویت، به‌طور موفقیت آمیز پردازش شده باشند. پس از failure در ماژول‌هایی با این flag، تمامی ماژول‌های دیگر با flag مشابه پردازش خواهند شد، پیش از اینکه کاربر پیغامی مبنی بر failure دریافت کند.
- requisite: همانند رفتار required، ماژول‌هایی با این flag نیز باید پیش از احراز هویت پردازش شوند اما در این flag در صورت رخداد failure بلافاصله خطایی به کاربر اعلام کرده و دیگر هیچ ماژولی پردازش نخواهد شد. توجه کنید که پردازش ماژول‌ها به ترتیب از اولین خط است و به ترتیب از بالا به پایین تا آخرین خط پردازش می‌شوند. ماژول‌ها با رفتار requisite در صورت بروز failure در آن‌ها، در همان نقطه پردازش خاتمه و دیگر ماژول‌های زیرین پردازش نمی‌شوند؛ اما در ماژول‌ها با required ماژول‌های با flag مشابه در صورت بروز failure پردازش خواهند شد.
- sufficient: این flag کنترلی به این معنی است که اگر این خط به‌طور موفقیت آمیز پردازش شد، یک پیغام فوری مبنی بر موفقیت آمیز بودن احراز هویت صادر شده و دیگر ماژول‌های باقی مانده (ماژول‌های زیرین همین خط) دیگر پردازش نخواهند

شد. درصورتی‌که failure رخ دهد به سراغ خط بعدی خواهد رفت.

- optional: موفقیت یا عدم موفقیت ماژول‌ها با این flag، هیچ اثر و نتیجه مستقیمی ندارند. در واقع تنها برای اعلان یک پیغام، مناسب هستند و هیچ عکس‌العملی را انجام نمی‌دهند.

فیلد MODULE_PATH اشاره به مسیر و نام ماژول می‌کند. البته نیازی به تعیین مسیر کامل ماژول نیست و آوردن نام ماژول کافی است زیرا تمامی ماژول‌ها در دایرکتوری lib/security/ در سیستم‌های ۳۲ بیتی و lib64/security/ در توزیع‌های ۶۴ بیتی ذخیره شده‌اند. MODULE_ARGS آرگومان اختیاری است که به ماژول پاس داده می‌شود. گاهی لازم است که ماژول بداند چه عملی را در صورت موفقیت انجام دهد.

مثال اول از تنظیم PAM

هر خط آن شامل یک نوع ماژول به همراه رفتار و نام ماژول است. آرگومان MODULE-ARGS نیز اختیاری است.

OUTPUT

```
auth      required  pam_securetty.so
auth      required  pam_unix.so shadow nullok
auth      required  pam_nologin.so
account   required  pam_unix.so
password  required  pam_cracklib.so retry=3
password  required  pam_unix.so shadow nullok
use_authtok
```

```
session   required  pam_unix.so
```

در خروجی بالا، خطوط نخست، دوم و سوم برای احراز هویت ورود به سیستم استفاده شده‌اند. توجه کنید که هر سه خط از دسته auth و از نوع flag کنترلی required هستند. نام ماژول خط نخست، pam_securetty.so و نام ماژول خط دوم pam_unix.so است که دو آرگومان به آن پاس داده شده است و هر آرگومان با فاصله از نام ماژول و یکدیگر جدا شده‌اند. نام ماژول خط سوم pam_nologin.so است.

ماژول pam_securetty.so اطمینان حاصل می‌کند که اگر شخصی می‌خواهد به عنوان root به سیستم وارد شود، به یکی از ترمینال‌های موجود در فایل etc/securetty/ وارد شود (این در صورتی است که این فایل وجود داشته باشد).

ماژول pam_unix.so اعلانی را برای وارد کردن گذرواژه از سمت کاربر نشان می‌دهد و سپس گذرواژه را با اطلاعات ذخیره شده در فایل‌های etc/passwd/ و etc/shadow/ بررسی می‌کند. فایل passwd نام کاربری را در خود دارد و در دومین فیلد هر خط یک اشاره‌گر به خطی از فایل shadow است. به عبارتی، در فیلد نخست هر خط از فایل passwd نام کاربری و در دومین فیلد هم یک x وجود دارد که به خطی مشابه با نام کاربری در فایل shadow اشاره می‌کند که گذرواژه رمز شده را در خود دارد. می‌بینید که دو آرگومان nullok و shadow با یک فاصله از هم و از نام ماژول به ماژول پاس داده شده‌اند. آرگومان nullok برای ورود گذرواژه‌های خالی استفاده می‌شود.

ماژول pam_nologin.so در خطوط بالا آخرین گام احراز هویت است و بررسی می‌کند که آیا فایل etc/nologin/ وجود دارد یا خیر. در صورت وجود فایل و root نبودن کاربری (کاربری غیر از root) که برای ورود تلاش می‌کند، احراز هویت fail می‌شود؛ یعنی از ورود کاربران غیر root جلوگیری می‌کند.

سه دسته (سه خط) auth بالا همگی بررسی می‌شوند حتی اگر نخستین خط fail شود و این به خاطر ماهیت رفتار required است. به دلیل ماهیت required کاربر در هیچ گامی درصورتی‌که failure رخ دهد مطلع نخواهد شد (همان تفاوت با requisite که یک اعلان بلافاصله نشان داده می‌شد.)

خط چهارم از دسته account و از ماژول pam_unix.so برای تصدیق و تأیید حساب کاربری استفاده شده است. در خط دوم ماژول pam_unix.so و آرگومان‌های پاس داده شده به آن گذرواژه ورودی را بررسی کرد، اما در این خط ماژول pam_unix.so و با استفاده از نوع account حساب کاربری را برای مسائلی مانند اینکه آیا حساب کاربری expire شده و یا اینکه کاربر گذرواژه‌اش را در مدت زمانی تعیین شده از قبل تعویض کرده یا خیر بررسی می‌کند. توجه کنید که به‌طور مثال ماژول pam_unix.so دارای دو مؤلفه auth و account است که هر کدام وظیفه خاصی را انجام می‌دهند و رفتارهای کنترلی مانند require چگونگی رفتار آن‌ها را نشان می‌دهد.

خط پنجم و ماژول pam_cracklib.so از دسته (نوع) password و از flag کنترلی required است. ماژول pam_cracklib.so بررسی می‌کند که اگر کاربر expire شده باشد اعلانی برای وارد کردن گذرواژه جدید نشان داده شود. سپس بررسی (تست) می‌کند که آیا گذرواژه جدید وارد شده آیا بسیار ساده است یا خیر. اگر برای بار نسخت این تست fail شود، کاربر دو مرتبه دیگر می‌تواند برای وارد کردن گذرواژه تلاش کند که این امر توسط پاس دادن آرگومان retry=3 انجام می‌شود. توجه کنید که این عملیات توسط مؤلفه password از ماژول pam_cracklib.so انجام می‌شود.

خط ششم باز هم ماژول pam_unix است با سه آرگومان shadow، nullok و use_authtok که به آن پاس داده شده است و از مؤلفه password استفاده می‌کند. همان‌طور که گفته شد پردازش از بالا به

پایین است و این شبیه به یک stack یا پشته است. پشته ساختاری است که از بالای آن خوانده یا پردازش می‌شود تا به انتهای آن برسیم. آرگومان use_authok از ماژول برای این است که دیگر به کاربر اعلانی برای ورود گذرواژه نشان داده نمی‌شود و از گذرواژه‌های موفق وارد شده در بالای پشته یعنی در خطوط بالاتر، برای انتخاب گذرواژه به‌طور خودکار انجام می‌شود.

خط آخر و با استفاده از مؤلفه session از ماژول pam_unix.so برای مدیریت جلسه کاری کاربر استفاده می‌شود. این ماژول رخدادی از نام کاربری و نام سرویس را در فایل var/log/message/ در توزیع‌های مبتنی بر RHLE ثبت می‌کند؛ یعنی رکوردی ثبت می‌کند که زمان دسترسی موفق به سرویس و اینکه توسط چه کاربری صورت گرفته است را به همراه نام سرویس در فایل مربوطه درج می‌کند. این کار در ابتدا و انتهای جلسه (ورود به و خروج از جلسه) صورت می‌گیرد. خطوطی که با # شروع شوند توضیح یا Comment هستند.

مثال دوم از پیکربندی PAM

این مثال برای فایل پیکربندی دستور reboot در توزیع CentOS است.

```
less /etc/pam.d/reboot
```

OUTPUT

```
auth    sufficient    pam_rootok.so


auth    required    pam_console.so
#auth    include    system-auth
```