



آزمایشگاه سیستم عامل دستور کار ۵: مدیریت کاربران

بخش اول: پیش نیاز

ویرایشگرها در لینوکس

انتخاب یک ویرایشگر متن مناسب برای کاربران لینوکسی، اهمیت زیادی دارد. زیرا در محیطی که تقریباً همه چیز به صورت دستوری کنترل می شود، شرایط با زمانی که از سیستم عامل دیگری استفاده می کنید متفاوت است. ویرایشگرهای متفاوتی برای سیستم عامل لینوکس پیاده سازی شده اند. از جمله این ویرایشگرها می توان به `vi`، `nano`، `pico`، `Emacs`، `gedit` و غیره اشاره کرد. در این دستور کار شما با ویرایشگر `vi` آشنا خواهید شد.

برای ورود به محیط ویرایشگر `vi` دستور زیر را تایپ می کنیم:

نام فایل <code>vi</code>

در صورت اینکه پس از `vi` نام فایل نیز بیاید اگر فایل مورد نظر قبلاً در سیستم نبوده باشد، فایل جدیدی با آن نام در سیستم ایجاد می شود و در صورتی که قبلاً در سیستم موجود بوده، محتویات آن در ویرایشگر `vi` نمایش داده می شود.

حالت های ویرایشگر `vi` :

هنگامی که وارد محیط ویرایشگر می شویم در حالت فرمان یا `command mode` قرار داریم.

در این حالت می توانیم مکان نما را حرکت داده و در سرتاسر متن جابه جا کنیم. در این شرایط تنها می توانیم متنی را حذف کنیم و امکان اضافه کردن متن وجود ندارد. برای اضافه کردن متن باید در حالت `Insert mode` قرار بگیریم. برای این منظور کلید `I` را می فشاریم و برای خروج از این حالت از کلید `Esc` استفاده می کنیم.

در زمانی که در حالت فرمان هستیم برای صدور فرمان ابتدا کاراکتر `:` را وارد نموده و پس از آن، فرمان مورد نظر را وارد می نماییم. برخی از فرمان های محیط فرمان به صورت زیر است:

- `W`: برای نوشتن روی فایل، پس از وارد نمودن همه دستورات و اعمال تغییرات لازم، برای ثبت نمودن همه تغییرات در فایل از این فرمان استفاده می شود.

- q: از ویرایشگر vi خارج شده و در shell سیستم عامل قرار می گیریم. (هنگامی که محتویات فایل تغییر نکرده باشد).
- !q: از ویرایشگر vi خارج شده و در shell سیستم عامل قرار می گیرد، با این تفاوت که در صورت اعمال تغییرات در فایل، تمامی این تغییرات نادیده گرفته می شوند.
- wq: ابتدا تغییرات اعمال شده روی فایل ثبت و ذخیره گردیده و سپس از محیط ویرایشگر vi خارج شده و در shell سیستم عامل قرار می گیریم.
- i: برای ورود به Insert mode در پایین صفحه نمایشگر واژه INSERT نوشته می شود که نشان دهنده این است که در Insert mode قرار داریم.
- a: برای ورود به Insert mode و اضافه نمودن متن به کار می رود. این حرف مخفف کلمه append است و بعد از محلی که مکان نما قرار دارد متن را به فایل اضافه می کند.
- \$: مکان نما را به آخرین کاراکتر خط می برد.
- ^: مکان نما را به اولین کاراکتر خط می برد.
- x: کاراکتری که مکان نما زیر آن قرار دارد را حذف می کند.
- X: کاراکتری که قبل از کاراکتری که مکان نما زیر آن قرار دارد را حذف می کند.
- dd: کل خط جاری را cut می کند.
- p: اطلاعات کپی یا بریده شده را در محل مکان نما می چسباند (paste).
- yy: کل خط جاری را کپی می کند.
- u: آخرین تغییر اعمال شده نادیده گرفته می شود (undo).
- شماره خط: مکان نما به شماره خط مورد نظر منتقل می شود.
- جستجو نمودن یک عبارت:

در حالی که در حالت فرمان هستیم دستور زیر را استفاده می نمایم.

عبارت مورد نظر برای جستجو / : عبارت مورد نظر را جستجو می نماید. کاربرد / قبل از عبارت مورد جستجو الزامی است.

بخش دوم: فایل های مربوط به مدیریت کاربران

در لینوکس نیز مانند بقیه سیستم های عامل کاربران دسته بندی می شوند و حوزه فعالیت و حقوق دسترسی متفاوتی را دارند. به عنوان مثال کاربران معمولی نمی توانند فایل های سیستم را پاک کنند یا ویرایش نمایند. اما مدیر سیستم (کاربر root) تقریباً هر کاری را می تواند روی سیستم انجام دهد و به همین دلیل توصیه می شود که به ندرت از حساب کاربری root استفاده نماییم. به این معنا که مدیر سیستم برای انجام کارهای روزمره خود از یک حساب کاربری معمولی استفاده کند و احتمال بروز حملات و خطرات را کاهش دهد.

برای مدیریت کاربران سه فایل /etc/passwd ، /etc/shadow و /etc/group را بررسی می کنیم:

/etc/passwd

احراز هویت کاربران توسط این فایل انجام می‌شود. در این فایل برای هر کاربر تعریف شده در سیستم، یک سطر اطلاعات وجود دارد. هر سطر این فایل دارای ۷ ستون (فیلد) است که ستون‌ها با جداکننده ':' از هم جدا شده‌اند. فیلدهای این فایل شامل موارد زیر هستند:

username:password:uid:gid:gecos:home_directory:login_shell
--

username: نام کاربری

password: اگر این ستون حاوی کاراکتر x باشد یعنی رمز عبور کاربر در فایل shadow به صورت رمز شده نگهداری می‌شود. اگر خالی باشد یعنی کاربر رمز عبور ندارد و اگر حاوی کاراکتر '*' باشد یعنی اکانت کاربر غیرفعال (disable) است.

uid: شماره شناسه کاربر که برای کاربران غیر سیستمی از ۱۰۰۰ شروع می‌شود و شناسه کاربر root صفر است.

gid: شماره شناسه گروه اصلی کاربر (gid) کاربران غیر سیستمی بالاتر از ۱۰۰ است.

gecos: به نوعی توضیحاتی در مورد کاربر مربوطه است.

home directory: دایرکتوری خانگی کاربر

login shell: پوسته پیش فرض کاربر که معمولاً /bin/bash است.

✓ برای این که بخواهیم که کاربری امکان لاگین به سیستم را نداشته باشد مقدار ستون login shell را برابر با /sbin/nologin قرار می‌دهیم.

/etc/shadow

در این فایل اطلاعات مربوط به رمز عبور کاربران نگهداری می‌شود. هر سطر این فایل دارای ۷ ستون (فیلد) است که ستون‌ها با جداکننده ':' از هم جدا شده‌اند. فیلدهای این فایل شامل موارد زیر هستند:

name:password:last_change:min:max:warn:inactive:expire
--

name: نام کاربری

password: حاوی رمز عبور به صورت رمز شده است.

last_change: آخرین زمان تغییر رمز عبور. (به صورت تعداد روز گذشته از تاریخ اول ژانویه ۱۹۷۰ نشان می‌دهد).

min: حداقل تعداد روزهایی که کاربر مجاز به تغییر رمز عبور نیست.

max: حداکثر مدتی که کاربر می‌تواند از رمز عبور استفاده کند و آن را تغییر ندهد.

warn: تعداد روز قبل از موعد زمان درج شده در فیلد max جهت اعلام خطر به کاربر برای تغییر رمز عبور.

inactive: اگر در زمان تعیین شده در فیلد max کاربر رمز عبورش را عوض نکند، اکانت کاربر غیر فعال (disable) خواهد شد.

expire: در زمان تعیین شده در این فیلد اکانت کاربر غیر فعال می‌شود.

/etc/group

در این فایل اطلاعات گروه‌ها قرار دارد و برای هر گروه یک سطر وجود دارد. این فایل دارای فیلدهای زیر است:

name:password:gid:members

name: نام گروه

password: به صورت کلی برای گروه‌ها رمز عبور نداریم که در این حالت از کاراکتر 'x' استفاده می‌شود.

gid: شماره شناسه گروه

members: اعضای گروه را مشخص می‌کند.

بخش سوم: دستورهای مربوط به مدیریت کاربران

- دستور passwd: برای تعویض رمز عبور کاربر استفاده می‌شود.
- دستور vigr: برای ویرایش فایل /etc/group
- دستور vipw: به طور پیش فرض برای ویرایش فایل /etc/passwd به کار می‌رود. اما می‌توانیم با پارامترهای زیر، از آن برای ویرایش فایل‌های دیگر نیز استفاده کنیم.

-s	برای ویرایش فایل /etc/shadow
-g	برای ویرایش فایل /etc/group

- دستور chage: با این دستور می‌توانیم مقادیر فیلدهای فایل /etc/shadow را تغییر دهیم.

-m	برای تغییر min
-M	برای تغییر max
-d	برای تغییر last_change
-E	برای تغییر expire
-I	برای تغییر inactive
-W	برای تغییر warn

(مثال)

chage -d 2021-04-12 test

- دستور useradd: برای ایجاد کاربر جدید

نام کاربری جدید useradd option

-d	دایرکتوری که در دستور مشخص شده را به عنوان دایرکتوری خانگی کاربر در نظر می‌گیرد.
-m	دایرکتوری خانگی برای کاربر جدید ایجاد می‌کند.
-s	پوسته پیش‌فرض کاربر را مشخص می‌کند.
-e	تاریخ انقضای حساب کاربری را مشخص می‌کنیم.
-g	گروه اصلی کاربر را مشخص می‌کنیم.
-u	شماره شناسه کاربر (uid) را مشخص می‌کند.

(مثال)

```
useradd user1 -d /home/user1
useradd user1 -s /bin/zsh
useradd user1 2021-4-18
useradd user1 -g head
```

- دستور userdel: حذف کاربر از سیستم توسط این دستور انجام می‌شود.

نام کاربری userdel option

با این دستور حساب کاربری حذف می‌شود اما هنوز دایرکتوری خانگی‌اش در مسیر /home/ وجود دارد.

- دستور usermod: برای تغییر خصوصیات کاربری

نام کاربری usermod option

-u	برای تغییر شماره شناسه کاربر (uid)
-e	برای تغییر تاریخ انقضای کاربر
-l	برای تغییر نام کاربری
-d	برای تغییر دایرکتوری خانگی کاربر
-g	برای تغییر گروه اصلی
-s	برای تغییر پوسته کاربر

- دستور groupdel: برای حذف گروه

نام گروه groupdel option

- دستور groupmod: برای تغییر خصوصیات گروه

نام گروه groupmod option

-g	برای تغییر شماره شناسه گروه (GID)
-n	برای تغییر نام گروه

- دستور gpasswd : برای انتساب یک کاربر معمولی به عنوان مدیر یک گروه

gpasswd -A user3 head

پس از این کاربر user3 مدیر گروه head است و می تواند با دستورهای زیر کاربر به گروه اضافه و یا حذف کند.
کاربر user5 را به گروه head اضافه می کند.

gpasswd -a user5 head

کاربر user5 را از گروه head حذف می کند.

gpasswd -d user5 head

تمرین:

- ۱- لیست و تعداد کاربرانی که نمی توانند به سیستم لاگین کنند را نمایش دهید.
- ۲- کاربری با نام کاربری test1 و کلمه عبور testpass و دایرکتوری خانگی /test1/ ایجاد نمایید.
- ۳- لیست کاربرانی را نمایش دهید که رمز عبور آنها به صورت رمز شده در فایل shadow قرار دارد.