به نام خدا

آزمایشگاه سیستم عامل

گزارش آزمایش شماره یک

محمد جواد زندیه 9831032

تمرین ها:

1. دایرکتوری داخل میز کاری (Desktop) بسازید و تمامی مجوزهای آن را به گونه ای تغییر دهید که فقط شما و اعضای گروه بتوانند بنویسند، بخوانند و در آن جستجو کنند.

```
javad@javad-virtual-machine:~$ ls
Desktop  Documents  Downloads  Music  Pictures  Public  Templates  Videos
javad@javad-virtual-machine:~$ cd Desktop
javad@javad-virtual-machine:~/Desktop$ mkdir test_dir
javad@javad-virtual-machine:~/Desktop$ ls
OS_LAB_InstructionManual_1398_v02.pdf  test_dir
javad@javad-virtual-machine:~/Desktop$ chmod 770 test_dir
javad@javad-virtual-machine:~/Desktop$ ls -l
total 832
-rw------- 1 javad javad 847650 07:54 4 اوکتوبر OS_LAB_InstructionManual_1398_v02.pdf
drwxrwx--- 2 javad javad   4096 20:53 10 اوکتوبر test_dir
```

ابتدا با دستور ls متوجه می شویم که فایل های موجود در دایرکتوری کنونی چیست، بعد از آن با استفاده از cd Desktop به دایرکتوری Desktop می رویم که در آنجا قرار است فایل مورد نظر ساخته شود.

با دستور mkdir test_dir دایرکتوری را می سازیم و با دستور chmod 770 test_dir به user , group مجوز های خواندن(r) و نوشتن(w) و جست و جو(x) در فایل را می دهیم.

7: 4(read) + 2(write) + 1(execute)

7(user) 7(group) 0(other)

با دستور ls -l می توان مطمئن شدن که تغییرات اعمال شده است. خروجی این دستور همان طور که در شکل هم هست به این صورت است:

drwxrwx---

رنگ قرمز معرف permission های داده شده به user یعنی javad است. (read, write, execute)

رنگ آبی معرف permission های داده شده به group است. (read, write, execute)

رنگ سبز هم معرف permission های داده شده به other هست. (هیچ مجوزی به آن برای این فایل داده نشده است)

2. گروه هایی که شما در آن عضو هستید، را لیست کنید، سپس مالکیت فایل قبلی را به یکی دیگر از گروه های خود بدهید.

```
javad@javad-virtual-machine:~/Desktop$ groups
javad adm cdrom sudo dip plugdev lpadmin lxd sambashare
javad@javad-virtual-machine:~/Desktop$ members adm
syslog javad
javad@javad-virtual-machine:~/Desktop$ sudo chown syslog test_dir
javad@javad-virtual-machine:~/Desktop$ ls -l
total 832
-rw------- 1 javad  javad 847650 07:54 4  اوکتوبر OS_LAB_InstructionManual_1398_v02.pdf
drwxrwx--- 2 syslog javad   4096 20:53 10 اوکتوبر test_dir
```

با دستور groups می توان گروه هایی را که owner که در اینجا javad می باشد را متوجه شد. از میان یکی از گروه ها، گروه adm را انتخاب کردیم و members آن را پیدا کردیم و سپس با دستور sudo chown مالکیت فایل test_dir را از مالک اولیه آن یعنی javad به هم گروهی آن در گروه adm یعنی syslog دادیم. با دستور ls -l می توان دید که مالک کنونی این فایل syslog است.

3. این دستور چه کاري انجام ميدهد؟ Chmod 4664 file.txt

```
javad@javad-virtual-machine:~/Desktop$ ls -l test_file.txt
-rw-rw-r-- 1 javad javad 0 21:37 10 اوکتوبر test_file.txt
javad@javad-virtual-machine:~/Desktop$ chmod 4664 test_file.txt
javad@javad-virtual-machine:~/Desktop$ ls -l test_file.txt
-rwSrw-r-- 1 javad javad 0 21:37 10 اوکتوبر test_file.txt
```

Permissions Breakdown

	User	Group	Other
Read	Yes ✔	Yes ✔	Yes ✔
Write	Yes ✔	Yes ✔	No ✘
Execute	No ✘	No ✘	No ✘

File	Directory
Yes ✔	No ✘

این دستور برای فایل ها استفاده می شود نه دایرکتوری ها.

Permission هایی که به هر یک از User, Group, Other داده می شود در جدول بالا آورده شده است.

Special

Confused by what theses special settings are used for? Read our article on the subject!

Sticky Bit	SGID	SUID
No ✘	No ✘	Yes ✔

S ای که در rwSrw-r- - دیده می شود به این معناست که از permission خاص SUID بهره می برد.

در کنار سه نوع اجازه نامه خواندن، نوشتن و اجرا کردن، سه نوع دیگر از اجازه نامه ها هستند که تاثیرشان بر روی دایرکتوریها و فایلها متفاوت است.

:Suid

فقط بر روی فایلهای با قابلیت اجرایی تاثیر دارند. اگر بر روی یک فایل با قابلیت اجرایی تنظیم شود، وقتی آن فایل اجرا شود، آن فایل با دسترسی صاحب فایل اجرا میشود و نه با دسترسی فردی که فایل را اجرا کرده. مثلا وقتی شما با دستور passwd پسوردتان را تغییر میدهید تغییراتی را داخل فایل shaddow ایجاد میکنید و از آنجایی که ایجاد تغییر در فایل shaddow فقط برای کاربر root میسر است، پس باید دستور passwd با دسترسی root اجرا شود، برای همین بر روی این دستور به طور پیش فرض suid تنظیم شده.

نکته: اگر suid بر روی دستوراتی مثل vi تنظیم شود، تمام کاربران به تمام فایلهای داخل سیستم دسترسی root خواهند داشت و یک مشکل امنیتی بزرگ به وجود میآید.

:Sgid

اگر بر روی یک فایل با قابلیت اجرایی تنظیم شود وقتی آن فایل اجرا شود، با دسترسی گروه فایل اجرا میشود و نه با دسترسی گروه فردی که فایل را اجرا میکند. اگر بر روی دایرکتوری ها تنظیم شود هر فایل یا دایرکتوری که داخل اون فایل ساخته شود، گروه همان فایل را به خود اختصاص میدهد و گروه فردی که فایل را ساخته، نمیگیرد.

:Sticky

فقط بر روی دایرکتوری ها قابل تنظیم کردن است. اگر بر روی یک دایرکتوری تنظیم شود، فایلهای داخل دایرکتوری را فقط صاحب دایرکتوری و صاحب فایل و کاربر روت میتواند تغییر اسم دهند و یا پاک کنند. این اجازه نامه به طور پیش فرض بر روی tmp/ وجود دارد. روی بعضی از سیستمهای قدیمی این اجازه نامه را میشود روی فایلهای معمولی هم تنظیم کرد.

نوع دسترسی	عدد اختصاص داده شده
suid	4000
sgid	2000
sticky bit	1000

4. درون کل دایرکتوری های موجود، فایل های خالی را پیدا کرده و پاک کنید (این کار باید در یک خط دستور انجام شود).

```
javad@javad-virtual-machine:~/Desktop$ cd test_dir
javad@javad-virtual-machine:~/Desktop/test_dir$ mkdir empty1, empty2, full1
javad@javad-virtual-machine:~/Desktop/test_dir$ ls
empty1,  empty2,  full1
javad@javad-virtual-machine:~/Desktop/test_dir$ cd full1
javad@javad-virtual-machine:~/Desktop/test_dir/full1$ touch text_file.txt
javad@javad-virtual-machine:~/Desktop/test_dir/full1$ cd ..
javad@javad-virtual-machine:~/Desktop/test_dir$ rmdir *
rmdir: failed to remove 'full1': Directory not empty
javad@javad-virtual-machine:~/Desktop/test_dir$ ls
full1
```

3 فایل را ایجاد کردیم که 2 تای آنها خالی و درون دیگری یک فایل قرار دادیم. با دستور rmdir * می توان تمام دایرکتوری های خالی را پاک کرد و دایرکتوری هایی که پر است با ارور مواجه می شوند و پاک نمیشود.