

3주차 1차시. 리눅스/유닉스의 계정과 권한

【학습목표】

1. 리눅스/유닉스 계정 및 권한에 대해 설명할 수 있다.

학습내용1 : 리눅스/유닉스 계정 체계

1. 로그인

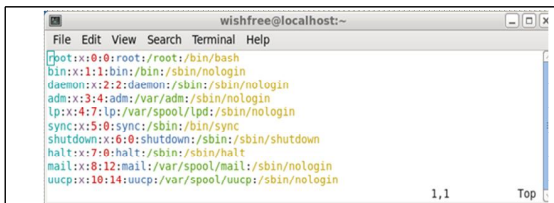
- * 계정 아이디와 패스워드로 자신이 누군지 알림
- * 계정에 따른 권한을 부여 받아 시스템에 대한 접근을 허가 받는 과정

2. 시스템 해킹

- * 사용자가 부여 받은 권한 이상의 권한을 획득하는 절차
- * 시스템 계정과 권한 체계 이해가 필수적으로 요구되는 작업

3. 리눅스 시스템의 계정과 권한 체계

- * root라고 불리는 관리자와 일반 사용자 계정이 존재
 - * 계정 목록을 /etc/passwd 파일에 저장
- \$ vi /etc/passwd



```
wishfree@localhost:~  
File Edit View Search Terminal Help  
root:x:0:0:root:/root:/bin/bash  
bin:x:1:1:bin:/bin:/sbin/nologin  
daemon:x:2:2:daemon:/sbin:/sbin/nologin  
adm:x:3:4:adm:/var/adm:/sbin/nologin  
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin  
sync:x:5:0:sync:/sbin:/bin/sync  
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown  
halt:x:7:0:halt:/sbin:/sbin/halt  
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin  
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
```

4. /etc/passwd 파일 내용

* 파일 내용 설명

root : x : 0 : 0 : root : /root : /bin/bash

① ② ③ ④ ⑤ ⑥ ⑦

① 사용자 계정

② 패스워드가 암호화되어 shadow 파일에 저장되어 있음

③ 사용자 번호(UID, User ID)

④ 그룹 번호(GID, Group ID) > 리눅스에서 관리자는 UID를 0번으로 부여 받음 > 일반 사용자는 그 외의 번호를 부여 받는데 보통 500번 이상을 부여

⑤ 사용자의 이름 > 자신의 이름 입력 가능

⑥ 사용자의 홈 디렉터리를 설정 > 관리자는 홈 디렉터리가 /root > 일반 사용자는 /home/wishfree와 같이 /home 디렉터리 하위에 위치

⑦ 사용자의 셸을 정의

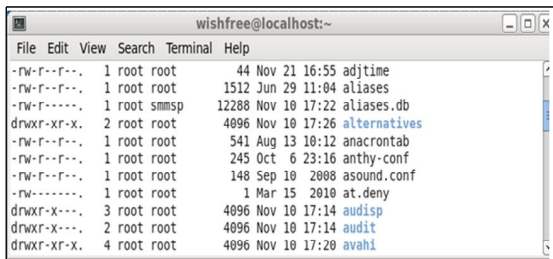
리눅스에서 권한 수준을 결정하는 중요한 항목

- 사용자 번호(UID, User ID)
- 그룹 번호(GID, Group ID)
- 파일의 접근 권한

5. /etc 폴더 내용

* 폴더 내용 설명

\$ ls -al /etc



① 파일에 대한 접근 권한을 표현

② 해당 파일에 링크(Link)되어 있는 파일의 개수를 표시

③ 해당 파일을 생성한 계정, 파일 생성자 또는 관리자가 수정 가능

④ 생성한 계정이 속한 그룹, 파일 생성자 또는 관리자가 수정 가능

6. 파일 속성

* 파일 속성 설명

drwxr-xr-x 2 root root 4096 Nov 10 17:26 alternatives

파일 속성	파일 소유자 권한	그룹 권한	일반(Others) 권한
d	rwX	r-X	r-X

* 파일의 종류에 대한 속성 문자

문자	파일 속성
d	디렉터리 파일(Directory File)
-	일반 정규 파일(Regular File)
l	링크되어 있는 파일(Symbolic Link File)
c	버퍼에 저장되지 않은 특수 파일(Character File) 예) 터미널
b	버퍼링된 특수 파일(Block File) 예) 디스크 드라이브
s	소켓 기능을 하는 파일(Socket File)
p	파이프 기능을 수행하는 파일(Pipe File)

7. 파일 소유자 권한

표기	의미	숫자
r	읽기(Read)	4(2진수 100)
w	쓰기(Write)	2(2진수 10)
x	실행(eXecution)	1(2진수 1)

rwX는 각각의 숫자 r(4) + w(2) + x(1)를 더한 수 7(2진수 111)로 읽음
접근 권한이 rwxr-xr-x인 경우 755로 읽음

학습내용2 : 리눅스/유닉스 파일 접근 권한 변경

1. 주제 / 참고

주제

리눅스/유닉스에서 파일에 대한 접근 권한 설정하기

참고

- 한빛미디어
- 정보 보안 개론과 실습: 시스템 해킹과 보안
- 140페이지
- 실습 3-1. 리눅스/유닉스에서 파일에 대한 접근 권한 설정하기

2. 파일 생성 시 기본 권한 확인

* 파일 생성

\$ touch a.txt

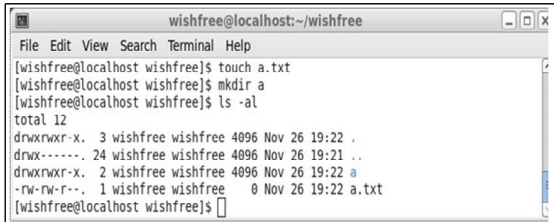
* 디렉터리 생성

\$ mkdir a

* 생성된 파일 및 디렉터리 접근 권한 확인

\$ ls -al

* 접근 권한 확인



```
wishfree@localhost:~/wishfree
File Edit View Search Terminal Help
[wishfree@localhost wishfree]$ touch a.txt
[wishfree@localhost wishfree]$ mkdir a
[wishfree@localhost wishfree]$ ls -al
total 12
drwxrwxr-x. 3 wishfree wishfree 4096 Nov 26 19:22 .
drwx----- 24 wishfree wishfree 4096 Nov 26 19:21 ..
drwxrwxr-x. 2 wishfree wishfree 4096 Nov 26 19:22 a
-rw-rw-r--. 1 wishfree wishfree 0 Nov 26 19:22 a.txt
[wishfree@localhost wishfree]$
```

* 파일 생성 시 기본 권한 부여

umask 값에 의해 결정

> /etc/profile에 설정

> 개별 계정 설정 : 사용자 계정의 .profile에 설정

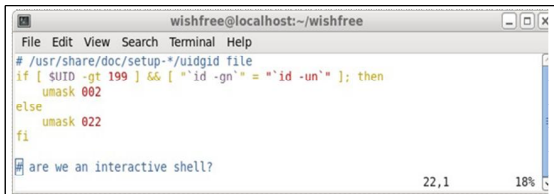
> bash shell : .bashrc에 설정

> C shell : .cshrc

페도라 14의 권한 설정

/etc/bashrc의 umask 값을 적용

\$ vi /etc/bashrc



```
wishfree@localhost:~/wishfree
File Edit View Search Terminal Help
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "$id -gn" = "$id -un" ]; then
    umask 002
else
    umask 022
fi
are we an interactive shell?
22,1 18%
```

* 기본 생성 최고 권한

파일 기본 생성 최고 권한 : 666

디렉터리 기본 생성 최고 권한 : 777

> 파일 기본 생성 최고 권한 : 666

> 디렉터리 기본 생성 최고 권한 : 777

파일 및 디렉터리 기본 생성 권한=최고 권한-umask

> 예) umask = 022

> 파일 생성 기본 권한 : 666 - 022 = 644

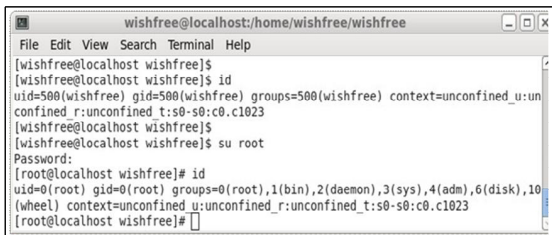
> 디렉터리 생성 기본 권한 : 777 - 022 = 755

3. 파일 및 디렉터리 기본 생성 권한 변경

- * /etc/bashrc의 umask 값을 통해 권한 변경 가능
- * /etc/bashrc는 관리자 소유의 파일
- * 관리자로 로그인 하거나 su(switch user) 명령을 사용하여 변경 가능

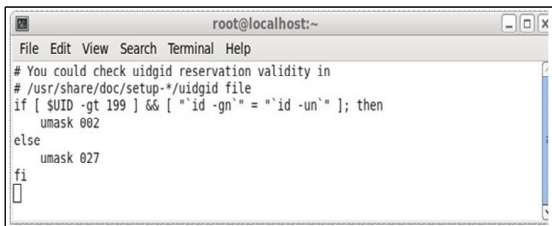
4. 파일 및 디렉터리 기본 생성 권한 변경

```
$ id
$ su root
# id
```



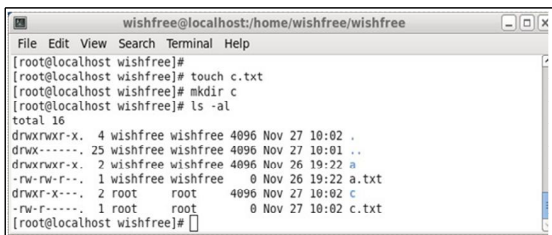
```
wishfree@localhost/home/wishfree/wishfree
[wishfree@localhost wishfree]$ id
[wishfree@localhost wishfree]$ id
uid=500(wishfree) gid=500(wishfree) groups=500(wishfree) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[wishfree@localhost wishfree]$ su root
Password:
[root@localhost wishfree]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@localhost wishfree]#
```

- * umask 변경
- # vi /etc/bashrc



```
root@localhost:~
File Edit View Search Terminal Help
# You could check uidgid reservation validity in
# /usr/share/doc/setup-*/uidgid file
if [ $UID -gt 199 ] && [ "`id -gn`" = "`id -un`" ]; then
    umask 002
else
    umask 027
fi
```

- * 파일 및 디렉터리 생성
- # touch c.txt
- # mkdir c



```
wishfree@localhost/home/wishfree/wishfree
[root@localhost wishfree]# touch c.txt
[root@localhost wishfree]# mkdir c
[root@localhost wishfree]# ls -al
total 16
drwxrwxr-x. 4 wishfree wishfree 4096 Nov 27 10:02 .
drwx----- 25 wishfree wishfree 4096 Nov 27 10:01 ..
drwxrwxr-x. 2 wishfree wishfree 4096 Nov 26 19:22 a
-rw-rw-r--. 1 wishfree wishfree 0 Nov 26 19:22 a.txt
drwxr-x---. 2 root root 4096 Nov 27 10:02 c
-rw-r----- 1 root root 0 Nov 27 10:02 c.txt
[root@localhost wishfree]#
```

* 파일의 권한 변경 : chmod 명령 사용

chmod 777 c.txt

```
wishfree@localhost:/home/wishfree/wishfree
File Edit View Search Terminal Help
[root@localhost wishfree]# chmod 777 c.txt
[root@localhost wishfree]# ls -al
total 16
drwxrwxr-x. 4 wishfree wishfree 4096 Nov 27 10:02 .
drwx----- 25 wishfree wishfree 4096 Nov 27 10:03 ..
drwxrwxr-x. 2 wishfree wishfree 4096 Nov 26 19:22 a.txt
-rw-rw-r--. 1 wishfree wishfree 0 Nov 26 19:22 a.txt
drwxr-x---. 2 root root 4096 Nov 27 10:02 c
-rwxrwxrwx. 1 root root 0 Nov 27 10:02 c.txt
[root@localhost wishfree]#
```

5. 파일 소유자/그룹 변경

* 파일 소유자 변경 : chown 명령 사용

* 파일 그룹 변경 : chgrp 명령 사용

chown wishfree c.txt

chgrp wishfree c.txt

```
wishfree@localhost:/home/wishfree
File Edit View Search Terminal Help
[root@localhost wishfree]#
[root@localhost wishfree]# ls -al c.txt
-rw-rw-r--. 1 wishfree wishfree 0 Nov 26 19:28 c.txt
[root@localhost wishfree]#
[root@localhost wishfree]# chown root c.txt
[root@localhost wishfree]# ls -al c.txt
-rw-rw-r--. 1 root wishfree 0 Nov 26 19:28 c.txt
[root@localhost wishfree]#
[root@localhost wishfree]# chgrp root c.txt
[root@localhost wishfree]# ls -al c.txt
-rw-rw-r--. 1 root root 0 Nov 26 19:28 c.txt
[root@localhost wishfree]#
```

【학습정리】

1. 리눅스/유닉스의 패스워드는 암호화되어 shadow 파일에 저장된다.

2. 리눅스/유닉스 파일 시스템 권한 표기법은 rwx로 나누어지며, r은 읽기(read), w는 쓰기(write), x는 실행(execution)을 의미한다.