리눅스 2019년4월5일 5주차

교재 60p 참고

리눅스 사용자 관리는 숫자로 한다.

사용자 번호는 UID라고 한다.

UID 0~999 : 시스템계정 ( root권한의 일부를 부여 받은 계정 )

0 : root

64555: 추후 사용

1000~60000 : 일반 사용자

* /etc/passwd 라는 곳에 이러한 정보들이 저장된다.

교재 68p 참고

/etc/passwd : 계정의 일반 정보

/etc/shadow : 암호와 관련된 정보

/etc/login.defs : 사용자 계정 생성 시 필요한 기본 값이 들어있다.

차이점 : login에 관련된 내용만 저장.

교재 69p 참고

/etc/default/useradd : 계정 생성 시 필요한 기본값이 들어 있다.

차이점 : useradd와 관련된 내용만 저장.

Login.defs에 있는걸 useradd가 가져다가 쓴다.

useradd : 사용자 추가 명령어

실습) kim, lee 사용자 추가하고 패스워드는 kim, lee로 줘라. Kim의 Uid는 2500으로 설정

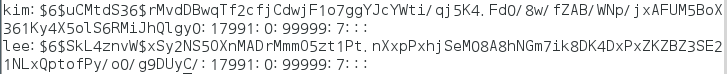
* useradd –u 2500 kim
* useradd lee
* passwd kim
* passwd lee

Q1. lee 사용자의 uid는 얼마인가? 2501

실습) shadow 파일을 화면에 출력하시오

* cat /etc/shadow

$를 기준으로 정보가 구분된다. /교재 73p 참고



$해시알고리즘표기값$솔트값(8자리)$해시값

해시 알고리즘 표기값 : 어떠한 해시 알고리즘을 사용했는지를 나타냄. 보통 1 또는 6으로 표시된다. ( 1: MD-5 해시알고리즘/ 리눅스 초창기부터 사용, 6 : SHA-512 / 현재 대부분의 리눅스 기본 )

## 리눅스는 같은 비밀번호를 넣어도 값이 다르도록 솔트값을 넣는다.

솔트값 : 암호의 복잡성을 높이기 위해 리눅스가 추가하는 임의값

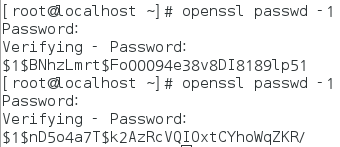
이 값을 다르게 하여 같은 password도 다른 암호문자로 저장한다.

해시값 : 솔트값 + 사용자패스워드를 1,6번의 해시 알고리즘을 적용하여 생성한 값

해시알고리즘표기값 1인지 6인지 알아보는 방법

1. cat /etc/shadow
2. cat /etc/login.defs -> encrypt\_method sha512 : sha-512로 설정되어있다.

실습 )

* openssl passwdl –1 : 암호 넣어라
* password : 1234 ( 패스워드 1234로 지정 )
* 
* 같은 비밀번호를 넣었지만 솔트값이 다르기 때문에 다른 암호문자가 된다.
* 암호 길이가 sha-512가 md5보다 길다.
* 74쪽 sha-512 암호 알고리즘 분석 실습 후 캡쳐해서 한글 파일 포함시키기 과제
* 
* egrep ‘kim|lee’ /etc/shadow (kim ,lee 값 출력)

사용자 패스워드 관리 : passwd

패스워드를 수정할 때 사용

passwd : root 가 사용할 때와 일반 사용자가 사용할 때가 다르다

root : passwd 계정명

관리자는 모든 계정 패스워드 변경 가능

일반사용자 : passwd

일반 사용자는 본인 패스워드만 변경 가능

<passwd 옵션>

-S : 패스워드 정보 출력

-l : 패스워드 잠금 ( 로그인 못함 )

-u : 잠긴 패스워드 풀기

-d : 사용자의 패스워드 제거한다. 패스워드 없이 로그인 가능

실습 )

* passwd kim
* kim (패스워드 kim 으로 설정)
* passwd –l kim ( 잠금 )
* passwd –u kim ( 잠금 풀기 )
* 
* alt + ctrl + f1 ~ f6 까지 사용 가능하다. ( 멀티쉘 제공 )
* 패스워드 규칙 81p 참고

계정 정보 변경 : usermod

<usermod 옵션>

useradd 명령어와 동일하다.

계정 삭제 : userdel

사용법 : userdel 계정명

실습) kim 계정 삭제

* userdel kim ( 홈 디렉터리 안 없어짐 )
* userdel –r kim ( 홈 디렉터리 같이 없어짐 )

<userdel 옵션>

-r : 홈디렉터리 같이 제거

-f : 로그인중이어도 강제 삭제

Q. lee 계정을 삭제하면서 홈디렉터리도 삭제하시오.

-> userdel –r lee

-> ls /home ( 홈 디렉터리에 lee 있는지 확인 )

\*\* 그룹 관리

설정 및 정보 파일

/etc/group : 그룹 정보 저장

* tail /etc/group ( (:)콜론 개수만큼 정보가 들어간다 / tail 은 끝에서 10줄 출력 )
* 그룹계정명 : x : gid : member\_list ( 84p 참고 )

/etc/gshadow : 그룹 암호 저장

* tail /etc/gshadow
* groupname(그룹계정명) : 패스워드(그룹 패스워드) : admin(그룹 관리자) : 멤버리스트
* admin 생략가능

그룹생성(root 만 사용가능) : groupadd

<groupadd 옵션>

-g : gid 설정

-o : gid 중복 허용

* groupadd terran
* groupadd –g 2500 student ( 그룹 아이디 지정해서 만들 수 있다. )

그룹 수정 : groupmod

그룹 삭제 : groupdel

그룹 패스워드 설정 : gpasswd

<gpasswd 옵션> 짱짱 중요

-A : 그룹 관리자 지정

-a : 그룹 관리자가 그룹에 멤버를 추가할 때 사용

-d : delete, 그룹의 멤버 제거

-M : root가 그룹 멤버를 지정할 때 사용한다.

실습 ) terran 그룹에 멤버 kim과 lee를 포함시키려고 한다. kim , lee 계정 생성하고 멤버를 포함시키시오.

* useradd kim
* useradd lee
* gpasswd –a kim terran
* gpasswd –a lee terran
* gpasswd –d kim terran ( 삭제 )

## 사용자 관리 및 보안 ( 현업에서의 시스템 관리 ) 교재 93p 참고

1. 조직별로 그룹을 생성
2. 조직원 계정을 해당그룹에 포함시킨다.
3. 모든 조직이 동일한 홈 디렉터리를 사용하도록 정책을 쓴다.

단 , 해당 조직의 자원이 여러 부서에서 공유되거나 사용자가 많으면 계정별로 홈 디렉터리를 운영할 수 있다.

실습 ) 인사부 직원 lee1, kim1, choi의 계정을 생성하고 이 직원들은 insa 그룹에 포함시킨다.

홈 디렉터리는 모두 /home/insa 를 사용하게 한다.

* groupadd insa ( 그룹 먼저 생성하기 )
* mkdir /home/insa ( 홈 디렉터리 생성 )
* useradd –g insa –d /home/insa lee1 ( 사용자 추가 : 옵션 이용 )
* tail /etc/passwd

사용자 정보 조회

1. 계정 조회 : id ( root 에 대한 계정 정보 보여줌 )

* id
* id centos

<id 옵션>

-g : 그룹 id 출력

-G : 사용자가 속한 모든 그룹의 id 출력

-u : uid 출력

-n : -u나 –g 와 같이 출력, 번호가 아닌 이름으로 출력

// 그룹정보 출력

* id –un centos
* groups [계정명] // 현재 사용자가 속한 그룹의 그룹명 출력
* groups centos : centos 의 그룹 출력

// 로그인한 사용자 관련 명령어

users : 시스템에 로그인 되어 있는 사용자 id를 출력

who : 로그인 된 사용자 출력

who am i : 지금 로그인된 id 정보 출력

who am I 는 실질적으로 사용중인 권한자를 출력해주는 명령이다.

w : 로그인된 사용자와 수행중인 작업을 출력해주는 명령

logname : 사용자의 로그인 계정