2주차 2차시 계정과 패스워드 관리

【학습목표】

1. 계정관리의 개념을 설명할 수 있다.
2. 운영체제의 계정관리를 응용할 수 있다.

학습내용1 : 계정관리의 개념

1. 인증 수단

1) 계정은 시스템에 접근하는 가장 기본적인 방법
- 일반적으로 '시스템 접근 권한이 필요합니다'라는 메시지가 뜨면, 해당 시스템에 대한 계정을 생성하라는 요청으로 받아들이는 경우가 많다.
- 계정은 시스템에 접근하는 가장 기본적인 방법이다. 그리고 계정의 기본 구성 요소는 아이디와 패스워드이다.

2) 계정의 기본 구성 요소는 아이디와 패스워드

3) 식별(Identification)이란 아이디라는 문자열을 통해 그 자신이 누구인지 확인하는 과정

4) 아이디만으로는 정확한 식별이 어려워 인증(Authentication)을 위한 다른 무언가(패스워드)를 요청

2. 보안의 4가지

① 알고 있는 것(Something You Know) : 군대의 암호처럼 머릿속에 기억하고 있는 정보를 이용해 인증을 수행하는 방법
예) 패스워드

② 가지고 있는 것(Something You Have) : 신분증이나 OTP(One Time Password) 장치 등을 통해 인증을 수행하는 방법
예) 출입카드

③ 스스로의 모습(Something You Are) : 홍채와 같은 생체 정보를 통해 인증을 수행하는 방법
예) 지문 인식

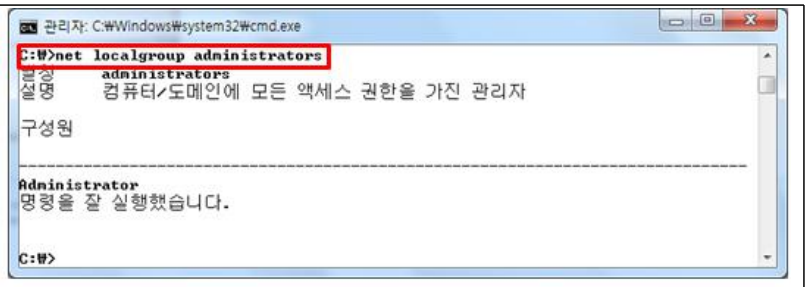
④ 위치하는 곳(Somewhere You Are) : 현재 접속을 시도하는 위치의 적절성을 확인하는 방법
예) 콜백

학습내용2 : 계정관리의 응용

1. 운영체제의 계정 관리

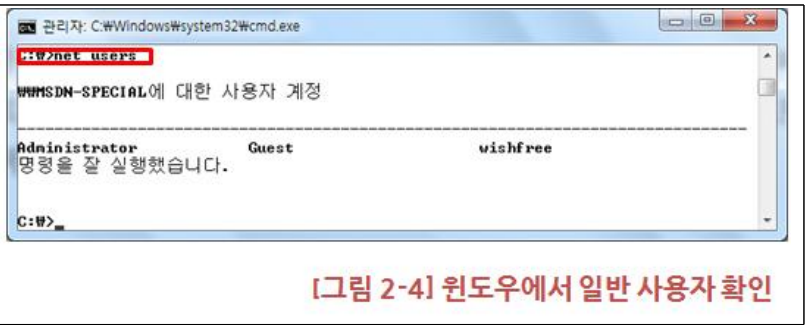
1) 윈도우의 계정 관리

- 윈도우에서는 운영체제에 대한 관리자 권한을 가진 계정을 administrator라고 하는데, 이는 시스템에 가장 기본으로 설치되는 계정



[그림 2-3] 윈도우에서 관리자 그룹에 속한 계정 목록 확인

- 일반 사용자를 확인하려면 net users라는 명령을 사용한다.



[그림 2-4] 윈도우에서 일반 사용자 확인

- 윈도우에서 시스템에 존재하는 그룹의 목록은 net localgroup 명령으로 확인할 수 있다.

2) [표 2-1] 윈도우의 주요 그룹

구분	특징
Administrators	• 대표적인 관리자 그룹으로, 윈도우 시스템의 모든 권한을 가지고 있다. • 사용자 계정을 만들거나 없앨 수 있으며, 디렉터리와 프린터를 공유하는 명령을 내릴 수 있다. • 사용할 수 있는 자원에 대한 권한을 설정할 수 있다.

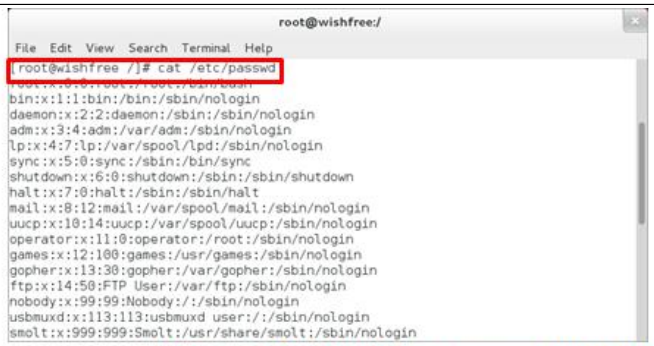
구분	특징
Power Users	• Administrators 그룹이 가진 권한을 대부분 가지지만, 로컬 컴퓨터에서만 관리할 능력도 가지고 있다. • 해당 컴퓨터 밖의 네트워크에서는 일반 사용자로 존재한다.

구분	특징
Backup Operators	• 윈도우 시스템에서 시스템 파일을 백업하는 권한을 가지고 있다. • 로컬 컴퓨터에 로그인하고 시스템을 종료할 수 있다.
Users	• 대부분의 사용자가 기본으로 속하는 그룹으로 여기에 속한 사용자는 네트워크를 통해 서버나 다른 도메인 구성요소에 로그인할 수 있다. • 관리 계정에 비해서 한정된 권한을 가지고 있다.

구분	특징
Guests	• 윈도우 시스템에서 Users 그룹과 같은 권한을 가진다. • 두 그룹 모두 네트워크를 통해서 서버에 로그인할 수 있으며 서버로의 로컬 로그인은 금지된다.

3) 유닉스의 계정 관리

- 기본 관리자 계정으로 root가 존재.
- 유닉스에서는 /etc/passwd 파일에서 계정 목록을 확인할 수 있다.



[그림 2-6] 유닉스에서 etc/passwd 파일 열람

* /etc/passwd 파일의 구성

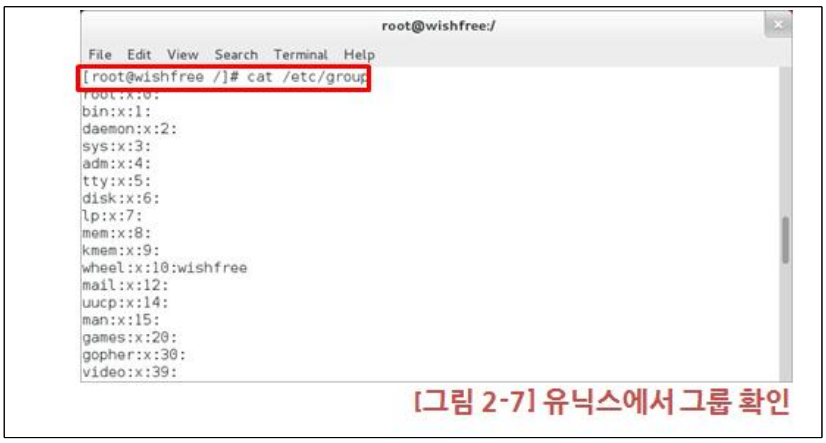
root : x : 0 : 0 : root : /root : /bin/bash
❶ ❷ ❸ ❹ ❺ ❻ ❼

① 사용자 계정

② 패스워드가 암호화되어 shadow 파일에 저장되어 있음을 나타낸다.

③ 사용자 번호
④ 그룹 번호
⑤ 실제 이름. 시스템 설정에 영향이 없으며, 자신의 이름을 입력해도 된다.
⑥ 사용자의 홈 디렉터리 설정. 위의 예에서는 관리자 계정이므로 홈 디렉터리가 /root이다.
- 일반 사용자는 /home/wishfree와 같이 /home 디렉터리 하위에 위치한다.
⑦ 사용자의 셸 정의로 기본 설정은 bash 셸이다.
- 사용하는 셸을 이곳에 정의해준다.

- 유닉스에서 그룹은 /etc/group 파일에서 확인할 수 있다.



[그림 2-7] 유닉스에서 그룹 확인

* /etc/group의 구조.

```
root : x : 0 : root
  ❶    ❷  ❸    ❹
```

① 그룹 이름. 여기서는 root 그룹을 말함.
② 그룹에 대한 패스워드. 일반적으로는 사용하지 않는다.
③ 그룹 번호. 0은 root 그룹
④ 해당 그룹에 속한 계정 목록
- 하지만 이 목록은 완전하지 않기 때문에 패스워드 파일과 비교해보는 것이 가장 정확함.

2. 데이터베이스의 계정 관리

1) MS-SQL에서 관리자 계정은 sa(system administrator)이고, 오라클에서 관리자계정은 sys, system이다.
- sys와 system은 둘 다 관리자 계정이지만, system은 sys와 달리 데이터베이스를 생성할 수 없음

2) 오라클은 Scott이라는 기본 계정이 존재하고, 솔루션을 설치하거나 테이블을 생성할 때 관련 계정이 자동으로 생성되는 경우가 많음.

3. 응용 프로그램의 계정 관리

1) 취약한 응용 프로그램을 통해 공격자는 운영체제에 접근해서 민감한 정보를 습득하여 운영체제를 공격하는데 이용할 수 있음.

2) TFTP(Trivial File Transfer Protocol)처럼 인증이 필요하지 않는 응용 프로그램은 더욱 세심한 주의가 필요함

4. 네트워크 장비의 계정 관리

1) 네트워크 장비에는 계정이라는 개념이 존재하지 않음

2) 그렇지만 네트워크 장비도 계정을 생성하여 각 계정으로 사용할 수 있는 명령어 집합을 제한할 수 있음

3) 네트워크가 대규모인 경우에는 계정 관리의 어려움 때문에 통합된 계정 관리를 위해 TACACS+와 같은 솔루션을 적용하기도 함

5. 패스워드 관리

1) 부적절한 패스워드의 예
① 길이가 너무 짧거나 널(Null)인 패스워드
② 사전에 나오는 단어나 이들의 조합
③ 키보드 자판의 일련 나열
④ 사용자 계정 정보로 유추 가능한 단어들

2) 좋은 패스워드란
① 기억하기 쉽지만 크래킹하기 어려운 패스워드

3) 패스워드와 관련된 주요 정책
① 패스워드 설정 정책
- 패스워드의 길이와 복잡도를 정해두는 것
- 패스워드 길이는 8자 이상, 복잡도는 연속된 숫자나 알파벳을 사용하지 못하게 하고 숫자와 알파벳, 특수문자를 섞어 설정하게 하는 식이다.

② 패스워드 변경 정책
- 일반적으로 60일 또는 90일 간격으로 패스워드를 변경하도록 하고 있다.

③ 잘못된 패스워드 입력 시 계정 잠금
- 잘못된 패스워드를 반복 입력할 경우 패스워드 크래킹 공격 또는 비인가자의 접근 시도로 판단하여 해당 계정을 사용하지 못하게 설정한다.

【학습정리】

1. 계정의 기본 요소는 아이디와 패스워드로 구성된다.

2. 패스워드 보안은 알고 있는 것(Something You Know), 가지고 있는 것(Something You Have), 스스로의 모습(Something You Are), 위치하는 곳(Somewhere You Are) 의 4가지 인증방법을 가진다.

3. 계정관리의 응용에는 운영체제 계정관리, 데이터베이스 계정관리, 응용프로그램 계정관리, 네트워크장비 계정관리, 패스워드 관리 등이 있다.