정보보안개론 1주차 강의

시스템 : 하드웨어 + 소프트웨어

-> 하드웨어 뿐만 아니라 소프트웨어까지 매우 많은 것을 포함

데이터베이스 시스템 : 하드웨어 + 데이터베이서 소프트웨어

보안 시스템 : 하드웨어 + 보안 소프트웨어

한번 로그인이 되면 세션아이디를 발급

세션아이디를 가지고 확인한다.

시스템 보안

계정 관리 / 세션 관리 / 접근 제어 / 권한 관리 / 로그 관리 / 취약점 관리

계정 관리 : 식별과 인증

식별 : 로그인하려면 먼저 자신이 누구인지를 말함

인증 : 로그인을 허용하기 위한 확인

운영체제의 계정 관리

운영체제 : 시스템을 구성하고 운영하기 위한 가장 기본적인 소프트웨어

유닉스의 계정 관리

유닉스 계열의 시스템에서는 기본 관리자 계정으로 root가 존재

/etc/passwd 파일의 구성 – 시험!

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

root : 계정명

x : 패스워드가 암호화되어 shadow 파일에 저장됨

0 : 사용자 번호 ! 중복 안됨 !

0: 그룹 번호 ! 중복 가능 !

root : 실제 이름

//root : 홈 디렉터리의 위치

/bin/bash : 사용자의 쉘 정의로, 기본 설정은 bash 쉘이다.

유닉스에서 그룹은 /etc/group 파일에서 확인

데이터베이스의 계정 관리

데이터베이스에서도 운영체제처럼 계정이 존재

DB는 노출되면 안된다.

세션 관리

세션 : 지속적인 인증

매번 패스워드를 입력 할 수 없으므로 시스템은 이를 세션에 대한 타임아웃 설정

접근 제어

접근 제어: 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근하도록 통제

운영체제의 접근 제어

접근 가능한 인터페이스를 확인했으면 불필요한 인터페이스를 제거해야 함

데이터베이스의 접근 제어

데이터베이스 : 조직의 영업 및 운영 정보를 담고 있는 핵심 응용 프로그램

로그 관리

모든 시스템은 로그를 남긴다.

AAA 요소

시스템 사용자가 로그인한 후 명령을 내리는 과정에 대한 시스템의 동작

Authentication (인증)

Authorization (권한 관리)

Accounting

운영체제의 로그 관리

history : 명령 창에서 실행한 명령에 대한 기록은 history 명령으로 확인

응용 프로그램의 로그 관리

IIS 웹 서버의 로그 : IS 웹 서버의 로그 IIS 웹 서버의 로그는 [제어판]의 '로깅' 항목에서 확인