1. 시스템 보안의 이해

시스템

- 시스템은 하드웨어뿐만 아니라 소프트웨어까지 매우 많은 것을 포괄
- 시스템과 관련된 보안 주제는 훨씬 큰 범위의 보안, 조직이나 국가 단위의 보안 요소를 다루는 일과 흡사

1. 정보 보안의 역사

시스템 보안 주제

1. 계정 관리(Account Management)
   - 사용자를 식별하는 가장 기본적인 인증 수단은 아이디와 패스워드
   - 이를 통한 계정 관리는 시스템 보안의 시작

2. 세션 관리(Session Management)
   - 일정 시간이 지나면 세션을 종료하고 비 인가자의 세션 가로채기를 통제하는 것

3. 접근 제어(Access Control)
   - 네트워크 안에서 시스템을 다른 시스템(해커 등)으로부터 적절히 보호할 수 있도록 접근을 통제하는 것

4. 권한 관리(Permission Management)
   - 시스템의 각 사용자가 적절한 권한으로 적절하게 정보 자산에 접근하도록 통제하는 것

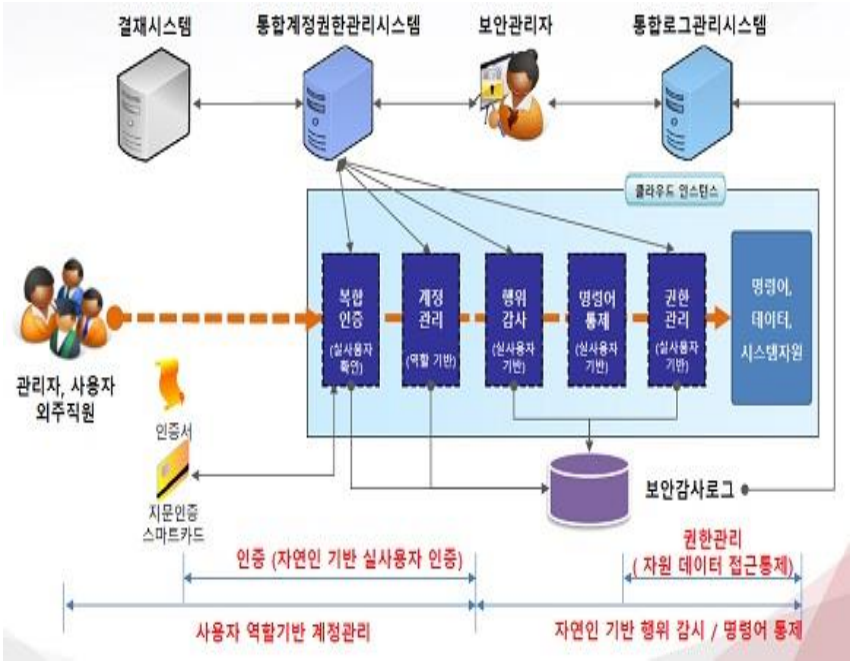
5. 로그 관리(Log Management)
   - 시스템 내부나 네트워크를 통해 외부에서 시스템에 어떤 영향을 미칠 경우 그 내용을 기록하여 관리하는 것

6. 취약점 관리(Vulnerability Management)
   - 시스템 자체의 결함을 체계적으로 관리하는 것

2. 계정 관리

계정관리

- 식별(**Identification**)과 인증(**Authentication**)
  - 식별: 시스템에 로그인하려면 자신이 누군지를 알림
    - 아이디 입력 및 중복 체크
  - 인증: 로그인(login)을 허용하기 위한 확인
    - 패스워드, 스마트 카드, 공인인증서 등
- 보안의 네 가지 인증 방법
  - 알고 있는 것
    - 머릿속에 기억하고 있는 정보를 이용하여 인증 수행
  - 가지고 있는 것
    - 신분증이나 OTP 장치 등으로 인증 수행
  - 자신의 모습
    - 홍채와 같은 생체 정보로 인증 수행
  - 위치하는 곳
    - 현재 접속을 시도하는 위치의 적절성을 확인하거나 콜백(Callback)을 사용해 인증 수행
    - 콜백: 접속을 요청한 사람의 신원을 확인, 미리 등록된 전화번호로 전화를 다시 걸어 접속을 요청한 사람이 본인인지 확인 (카톡 인증 등)



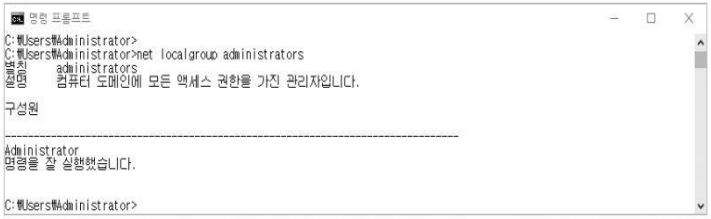
참고) 시큐브 클라우드 통합계정권한관리체계 프로세스와 적용되는 기술

2. 계정 관리

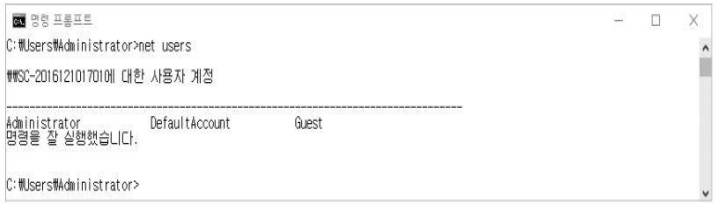
운영체제의 계정 관리

- 운영체제
  - 시스템을 구성하고 운영하기 위한 가장 기본적인 소프트웨어
    - 운영체제에 대한 권한을 가지게 되면 해당 시스템의 다른 응용 프로그램에 대해서도 어느 정도의 권한을 가질 수 있음
    - 일반 사용자 권한의 계정도 시스템의 상당 부분에 대한 읽기 권한을 가짐
    - 운영체제 내에서는 관리자 권한이 있는 계정 뿐 아니라 일반 사용자 권한이 있는 계정도 적절하게 제한

- 윈도우의 계정 관리
  - 관리자 계정: administrator / 시스템에 가장 기본으로 설치되는 계정
  - 관리자 그룹의 계정의 존재 형태를 확인하려면 윈도우에서 net localgroup administrators 명령을 사용



  - 사용자 계정을 모두 확인하려면 net users 명령을 사용



2. 계정 관리

■ 운영체제의 계정 관리

▪ 윈도우의 계정 관리

- 윈도우에서는 기본 그룹을 정의하는데, 시스템에 존재하는 그룹 목록은 net localgroup 명령으로 확인

2. 계정 관리

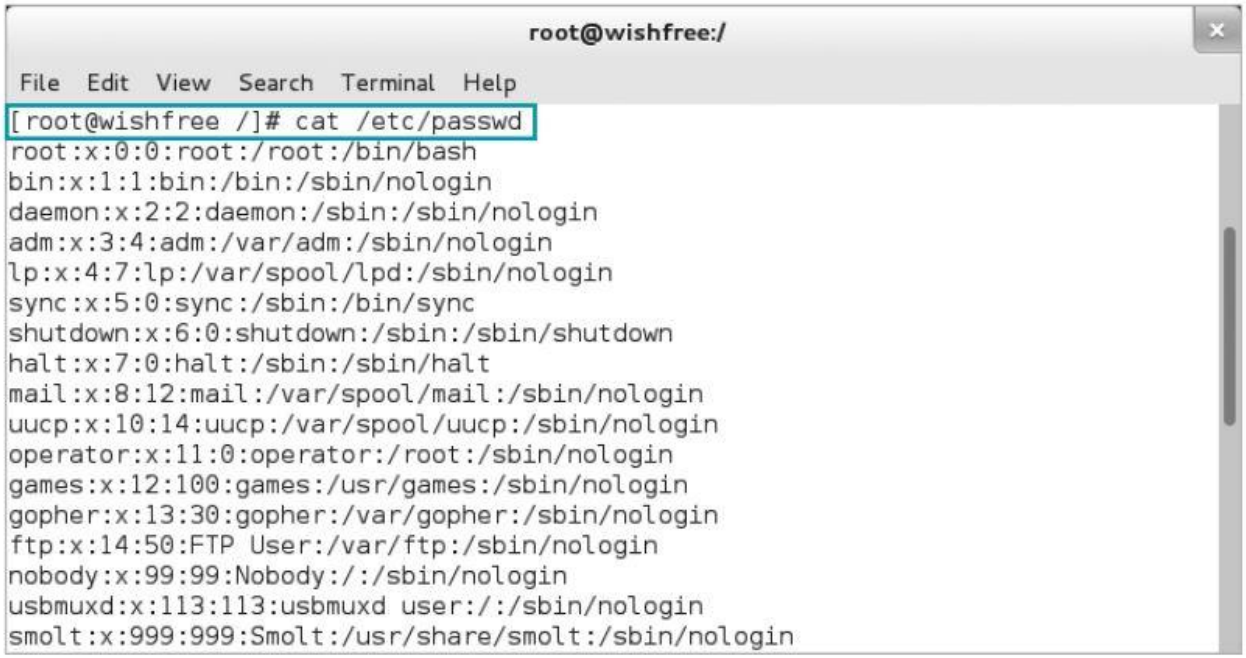
■ 운영체제의 계정 관리

▪ 윈도우의 계정 관리

그룹	특징
Administrators	• 대표적인 관리자 그룹으로 윈도우 시스템의 모든 권한을 가지고 있다. • 사용자 계정을 만들거나 없앨 수 있고 디렉터리와 프린터를 공유하는 명령을 내릴 수 있다. • 사용 가능한 자원에 대한 권한을 설정할 수 있다.
Power Users	• Administrators 그룹이 가진 권한을 대부분 가지지만 로컬 컴퓨터에서만 관리할 능력도 가지고 있다. • 해당 컴퓨터 밖의 네트워크에서는 일반 사용자로 존재한다.
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 구성 요소에 로그인할 수 있다. • 관리 계정에 비해 한정된 권한을 가지고 있다.
Guests	• 윈도우 시스템에서 Users 그룹과 같은 권한을 가지고 있다. • 두 그룹 모두 네트워크를 통해 서버에 로그인할 수 있으며 서버로의 로컬 로그인은 금지된다.

2. 계정 관리

- **유닉스의 계정 관리**
  - 유닉스 계열의 시스템(이후 유닉스)에서는 기본 관리자 계정으로 root가 존재
  - 유닉스에서는 /etc/passwd 파일에서 계정 목록을 확인



2. 계정 관리

■ 유닉스의 계정 관리

- /etc/passwd 파일의 구성

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

❶ 사용자 계정

❷ 패스워드가 암호화되어 shadow 파일에 저장되어 있음을 나타냄

❸ 사용자 번호

❹ 그룹 번호

❺ 실제 이름. 시스템 설정에 영향을 주지 않으며 자신의 이름을 입력해도 됨

❻ 사용자의 홈 디렉터리 설정. 위의 예에서는 관리자 계정이므로 홈 디렉터리가 /root 일반 사용자는 /home/ wishfree와 같이 /home 디렉터리의 하위에 위치

❼ 사용자의 셸 정의로, 기본 설정은 bash 셸이다. 사용하는 셸을 이곳에 정의

2. 계정 관리

유닉스의 계정 관리

- 유닉스에서 그룹은 /etc/group 파일에서 확인

- /etc/group의 내용

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

❶ 그룹 이름. 여기서는 root 그룹을 말함

❷ 그룹에 대한 패스워드. 일반적으로는 사용하지 않음

❸ 그룹 번호. 0은 root 그룹

❹ 해당 그룹에 속한 계정 목록. 이 목록은 완전하지 않으므로 패스워드 파일과 비교해보는 것이 가장 정확. **그룹 번호가 0인 그룹에 해당하는 계정은 root, sync, shutdown, halt, operator**

2. 계정 관리

데이터베이스의 계정 관리

- 데이터베이스에도 운영체제처럼 관리자 계정과 일반 사용자 계정이 존재
- MS-SQL의 관리자 계정은 sa(System Administrator), 오라클의 관리자 계정은 sys, system
  - 둘 다 관리자 계정이지만 sys와 달리 system은 데이터베이스를 생성할 수 없음
- 관리자 계정 (Admin Account)
  - 데이터베이스 관리자가 사용하는 계정으로, 데이터베이스의 모든 기능에 대한 접근 권한. 데이터베이스의 설정, 사용자 관리, 백업 및 복원 등의 작업을 수행

응용 프로그램의 계정 관리

- 취약한 응용 프로그램을 통해 공격자가 운영체제에 접근하여 민감한 정보를 습득한 뒤 운영체제를 공격하는 데 이용할 수 있음
  - **SQL 인젝션, 버퍼 오버플로우, 크로스 사이트 스크립팅 (XSS), 파일 업로드 취약점, 원격 코드 실행 (RCE)**
- TFTP처럼 인증이 필요치 않은 응용 프로그램은 더욱 세심한 주의가 필요

네트워크 장비의 계정 관리

- 네트워크 장비는 보통 패스워드만 알면 접근이 가능
- 시스코 장비의 계정 모드 구별
  - 네트워크 장비의 상태만 확인할 수 있는 사용자 모드
  - 네트워크에 대한 설정 변경이 가능한 관리자 모드
  - 처음 접속 시 사용자 모드로 로그인 되며 사용자 모드에서 관리자 모드로 로그인하려면 다시 별도의 패스워드를 입력
- 네트워크 장비에서도 계정을 생성하여 각 계정으로 사용할 수 있는 명령어 집합을 제한할 수 있음 (TACACS+)

3. 세션 관리

세션

- 세션의 개요
  - **'사용자와 시스템 사이 또는 두 시스템 사이의 활성화된 접속'**을 의미
  - **세션 유지의 예)** 줄 서고 있을 때 친구에게 자리 맡아달라고 부탁하기

- 세션관련 보안 문제
  - **세션 하이재킹, 네트워크 패킷 스니핑에 대응하기 위한 암호화, 지속적인 인증 필요**

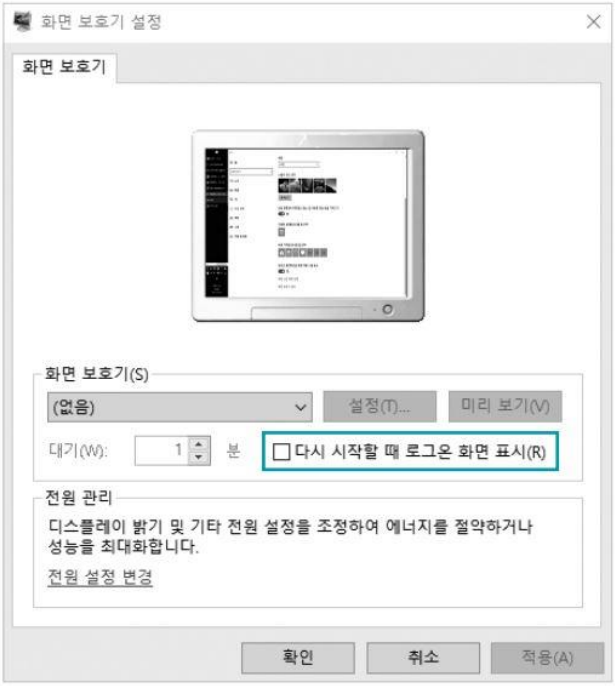
- 동화 〈해님 달님〉의 이야기
  - 일하러 나간 어머니를 기다리던 오누이는 호랑이의 손을 확인하고 문을 열어달라고 함
  - 이 과정은 오누이 입장에서 **어머니의 세션이 유효한지 확인**하기 위해 '손의 모양새'를 이용한 것
    - **세션 인증 과정의 예**

3. 세션 관리

세션

지속적인 인증 (Continuous Authentication)

- 세션을 유지하기 위한 보안 사항 중 하나
- 인증에 성공한 후 인증된 사용자가 처음의 사용자인지 지속적으로 재 인증 작업을 거치는 작업
- 매번 패스워드를 입력 할 수 없으므로 시스템은 이를 세션에 대한 타임아웃 설정으로 보완 (윈도의 화면보호기)
- 반면 유닉스는 원격에서 접속할 경우 패스워드를 다시 묻지 않고 세션을 종료한 후 재 접속 요구
- 시스템이 아닌 웹 서비스를 이용할 때도 '지속적인 인증'이 적용



4. 접근 제어

접근 제어(Access Control)

- 접근 제어: **적절한 권한을 가진 인가자 만이 특정 시스템이나 정보에 접근하도록 통제하는 것**
  - 사용자가 시스템 자원(파일, 프로세스, 네트워크 등)에 접근할 수 있는 권한을 설정하고, 이를 통해 보안을 유지하는 데 중요한 역할 수행
  - 시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트(Port)
- 운영체제에 대한 적절한 접근 제어를 수행하려면 가장 먼저 운영체제에서 어떤 관리적 인터페이스가 운영되고 있는지를 파악해야 함

운영체제의 접근 제어

- 시스템 자원에 대한 접근을 관리하고 제한하는 메커니즘을 의미
- 사용자가 시스템 자원(파일, 프로세스, 네트워크 등)에 접근할 수 있는 권한을 설정하고, 이를 통해 보안을 유지
  - 인증
  - 권한부여
  - 접근제어목록
  - 역할 기반 접근 제어

운영체제	서비스 이름	사용 포트	특징
유닉스 (리눅스 포함)	텔넷	23	암호화되지 않음
	SSH	22	SFTP 가능
	XDMCP	6000	유닉스용 GUI(XManager)
	FTP	21	파일 전송 서비스
윈도우	터미널 서비스	3389	포트 변경 가능
	GUI 관리용 툴		VNC, Radmin 등

운영체제 관리적 인터페이스

4. 접근 제어

운영체제의 접근 제어

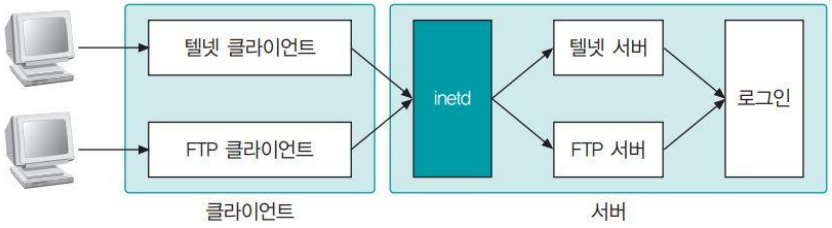
불필요한 인터페이스 제거

- 접근 가능한 인터페이스를 확인했으면 불필요한 인터페이스를 제거해야 함
- 불필요한 인터페이스를 제거할 때는 사용할 인터페이스에 보안 정책을 적용할 수 있는지를 판단해야 함
  - 유닉스에서 많이 쓰이는 Telnet(포트번호 23번)은 스니핑과 세션 하이재킹 공격 등에 취약하기 때문에 사용을 권고하지 않음
  - 가능하면 SSH (포트번호 22번) 나 XDMCP(UDP 포트번호 177)를 사용하는 것이 좋음
  - 윈도우의 GUI인 터미널 서비스는 운영체제의 버전에 따라 다른 수준의 암호화를 수행하므로 이를 고려하여 적용
- 운영체제에 대한 접근 목적의 인터페이스를 결정한 다음에는 접근 제어 정책을 적용해야 함
- 시스템에 대한 접근 제어 정책은 기본적으로 IP를 통해 수행
  - **IP 주소 기반 필터링**
  - **방화벽(Firewall)**
  - **VPN(가상 사설망)**
  - **접근 제어 목록(ACL)**
- 유닉스의 Telnet, SSH, FTP 등은 TCPWrapper를 통해 접근 제어가 가능

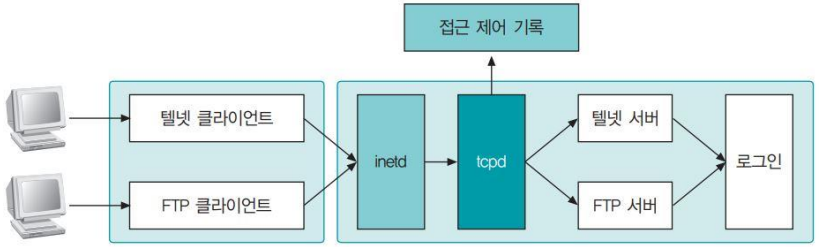
4. 접근 제어

운영체제의 접근 제어

- Inetd(Internet Daemon) : Unix 및 Unix 계열 운영 체제에서 사용되는 슈퍼 데몬, 네트워크 서비스 요청을 관리
  - 클라이언트로부터 텔넷이나 SSH, FTP 등에 대한 연결 요청을 받음
  - 해당 데몬을 활성화하여 실제 서비스를 함으로써 클라이언트의 요청을 처리(서비스 프로세스를 생성하여 처리)



  - TCPWrapper가 설치되면 inetd 데몬은 TCPWrapper의 tcpd 데몬에 연결을 넘겨줌
  - tcpd 데몬은 접속을 요구한 클라이언트에 **적절한 접근 권한이 있는지 확인한 후(접근 제어)** 해당 데몬에 연결을 넘겨줌. 이때 연결에 대한 로그를 실시할 수도 있음

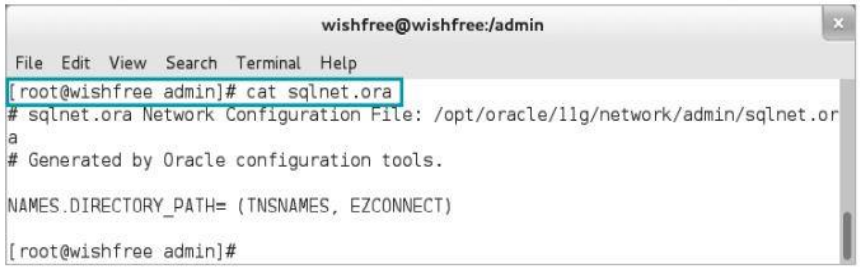


4. 접근 제어

■ 데이터베이스의 접근 제어

▪ 데이터베이스

- 조직의 영업 및 운영 정보를 담고 있는 핵심 응용 프로그램
- 적절한 접근 제어는 필수이지만 모든 데이터베이스가 적절한 접근 제어 수단을 제공하는 것은 아님
- 오라클은 $ORACLE_HOME/network/admin/sqlnet.ora 파일에서 접근 제어를 설정



- 200.200.200.100과 200.200.200.200이라는 두 IP의 접근을 허용하려면 다음을 추가

```
tcp.invited_nodes=(200.200.200.100, 200.200.200.200)
```

- 200.200.200.150의 접근을 차단하고 싶은 경우에는 다음과 같이 추가

```
tcp.excluded_nodes=(200.200.200.150)
```

- MySQL의 경우, 특정 IP와 계정에 대한 접근에 다음과 같이 권한을 부여

```
GRANT [권한] ON [데이터베이스].[테이블] TO [ID]@[IP 주소] IDENTIFIED BY [패스워드]
```

- GRANT ALL PRIVILEGES ON mydatabase.* TO 'myuser'@'192.168.1.100' IDENTIFIED BY 'mypassword';

4. 접근 제어

응용 프로그램의 접근 제어

- NGINX(Engine X) 웹 사이트 설정 파일에서는 다음과 같이 접근 제어를 수행
  - **NGINX: 고성능의 오픈 소스 웹 서버이자 리버스 프록시 서버, 로드 밸런서, HTTP 캐시, 그리고 메일 프록시 서버로 사용되는 웹 서버 소프트웨어 (/etc/nginx/nginx.conf)**

```
server {
listen        443 ssl;
   server_name    www.wishfree.com;
   location / {
deny  192.168.1.2;
       allow  192.168.1.1/24;
       allow  2001:0db8::/32;
     deny   all;
}
}
```

네트워크 장비의 접근 제어

- 네트워크 장비도 IP에 대한 접근 제어가 가능함
- 관리 인터페이스에 대한 접근 제어와 ACL(Access Control List)을 통한 네트워크 트래픽 접근 제어가 있음
- 네트워크 장비의 관리 인터페이스에 대한 접근 제어는 유닉스의 접근 제어와 거의 같음
- ACL을 통한 네트워크 트래픽 접근 제어는 방화벽에서 수행하는 접근 제어와 기본적으로 같음

5. 권한 관리

■ 운영체제의 권한 관리

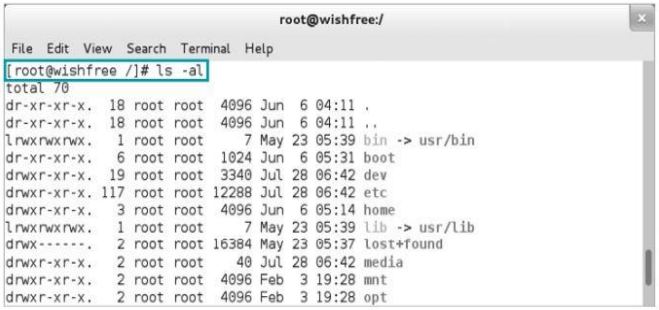
▪ 윈도우의 권한 관리

- 윈도우는 NT 4.0 이후 버전부터 NTFS를 기본 파일 시스템으로 사용
- 임의의 디렉터리를 만들고 마우스 오른쪽 버튼을 눌러 [등록정보]-[보안]을 선택하면 권한 설정 화면이 나타남
- NTFS에서 그룹 또는 개별 사용자에 대해 설정할 수 있는 권한의 종류
  - ❶ 모든 권한: 디렉터리 접근 권한과 소유권을 변경하고 하위 디렉터리와 파일 삭제 가능
  - ❷ 수정: 디렉터리 삭제가 가능하며 읽기, 실행, 쓰기 권한이 주어진 것과 동일
  - ❸ 읽기 및 실행: 읽기 수행, 디렉터리나 파일 옮기기 가능
  - ❹ 디렉터리 내용 보기: 디렉터리 내의 파일, 디렉터리 이름 보기 가능
  - ❺ 읽기: 디렉터리 내용 읽기만 가능
  - ❻ 쓰기: 해당 디렉터리에 하위 디렉터리와 파일 생성, 소유권이나 접근 권한의 설정 내용 확인 가능
- 권한의 규칙
  - **규칙 1: 접근 권한이 누적**
  - **규칙 2: 파일 접근 권한이 디렉터리 접근 권한보다 우선**
  - **규칙 3: '허용'보다 '거부'가 우선**

5. 권한 제어

■ 유닉스의 권한 관리

- 유닉스는 파일과 디렉터리에 대한 권한 설정 방법이 같음
- 임의의 디렉터리에서 ls -al 명령 으로 디렉터리의 내용을 확인



- etc 항목

```
drw-r-xr-x 117 root root 12288 Jul 28 06:42 etc
     ❶          ❷    ❸
```

❶ 파일의 종류와 권한
❷ 파일의 소유자
❸ 파일에 대한 그룹

- ❶은 다시 네 부분으로 세부화

```
- rw- r-- r--
ⓐ ⓑ  ⓒ  ⓓ
```

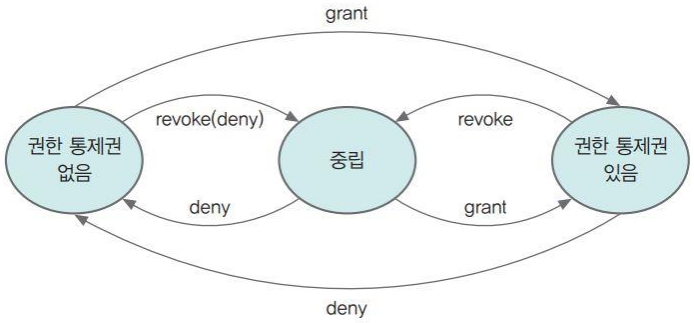
ⓐ 파일 및 디렉터리의 종류. -는 일반 파일을, d는 디렉터리를, l은 링크(link)를 나타냄
ⓑ 파일 및 디렉터리 소유자의 권한
ⓒ 파일 및 디렉터리 그룹의 권한
ⓓ 해당 파일 및 디렉터리의 소유자도 그룹도 아닌 제3의 사용자에 대한 권한

5. 권한 제어

■ 데이터베이스의 권한 관리

▪ 질의문에 대한 권한 관리

DDL(Data Definition Language): 데이터 구조를 정의하는 질의문이다. 데이터베이스를 처음 생성하고 개발할 때 주로 사용하고 운영 중에는 거의 사용하지 않는다.	
CREATE	데이터베이스 객체를 생성한다.
DROP	데이터베이스 객체를 삭제한다.
ALTER	기존 데이터베이스 객체를 다시 정의한다.
DML(Data Manipulation Language): 데이터베이스의 운영 및 사용과 관련해 가장 많이 사용하는 질의문으로 데이터의 검색과 수정 등을 처리한다.	
SELECT	사용자가 테이블이나 뷰의 내용을 읽고 선택한다.
INSERT	데이터베이스 객체에 데이터를 입력한다.
UPDATE	기존 데이터베이스 객체에 있는 데이터를 수정한다.
DELETE	데이터베이스 객체에 있는 데이터를 삭제한다.
DCL(Data Control Language) : 권한 관리를 위한 질의문이다.	
GRANT	데이터베이스 객체에 권한을 부여한다.
DENY	사용자에게 해당 권한을 금지한다.
REVOKE	이미 부여된 데이터베이스 객체의 권한을 취소한다.



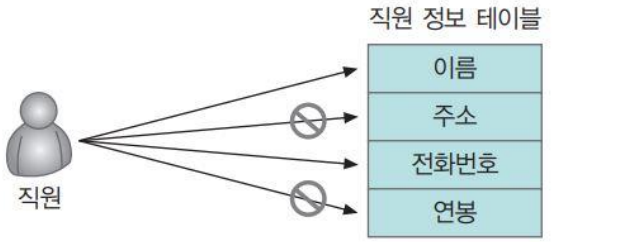
- DDL과 DML은 DCL에 의해 허용 또는 거부
  - GRANT SELECT, UPDATE ON employees TO user1
    - employees 테이블에 대해 user1이라는 사용자에게 SELECT 권한을 부여한다.
  - DENY DELETE ON employees TO user1
    - employees 테이블에 대해 user1이라는 사용자에게 DELETE 권한을 거부한다.

5. 권한 제어

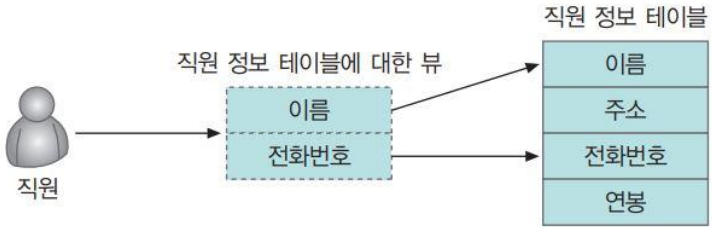
■ 데이터베이스의 권한 관리

▪ 뷰에 대한 권한 관리

- 뷰: 참조 테이블의 각 열에 대해 사용자의 권한을 설정하는 것이 불편해서 만든 가상 테이블
- 생성된 뷰에 대한 권한 설정은 테이블에 대한 권한 설정과 같음
- 뷰를 사용하지 않는 경우 테이블에 각각 접근 제한을 설정해야 함



- 뷰에 대한 권한만 할당



5. 권한 제어

응용 프로그램의 권한 관리

- 응용 프로그램은 응용 프로그램 내의 권한 관리보다 응용 프로그램 자체의 실행 권한이 더 중요
- 자신을 실행한 계정의 권한을 물려받으므로 보안상에 문제가 있는 취약한 응용 프로그램의 경우 해당 프로그램을 실행한 계정의 권한이 악용되는 문제가 발생
  - **아파치 웹 서버 서비스가 root 권한으로 실행되는 경우 공격자가 웹 취약점을 이용하여 root 권한을 획득**
- 윈도우의 IIS에서는 실행 프로세스 권한을 별도로 만들어 사용
  - 각 웹 애플리케이션이 특정 사용자 계정의 권한으로 실행되도록 구성 가능
- 유닉스에서는 nobody와 같이 제한된 계정 권한을 사용
  - nobody 계정은 일반적으로 제한된 권한을 가진 사용자 계정

6. 로그 관리

AAA 요소

- 시스템 사용자가 로그인한 후 명령을 내리는 과정에 대한 시스템의 동작
- 로그를 남기는 모든 시스템에 존재
- AAA에 대한 로그 정보는 해커나 시스템에 접근한 악의적인 사용자를 추적하는 데 많은 도움이 됨
  - 책임추적성(Accountability): 추적에 대한 기록의 충실도, 책임추적성이 높은 시스템일수록 로그가 충실하게 남아있음.
  - 감사 추적(Audit Trail): 보안과 관련하여 시간대별 이벤트를 기록한 로그

Authentication (인증)

- 자신의 신원을 시스템에 증명하는 것으로 아이디와 패스워드를 입력하는 과정
- 해당 시스템이 지문으로 신분을 확인하는 과정

Authorization (인가)

- 지문이나 패스워드 등을 통해 신원이 확인되어 인증받은 사용자가 로그인하는 과정
- 인증된 사용자가 특정 자원이나 서비스에 접근할 수 있는 권한을 결정하는 과정. 이는 사용자의 역할이나 정책에 따라 다르게 설정

Accounting(계정관리)

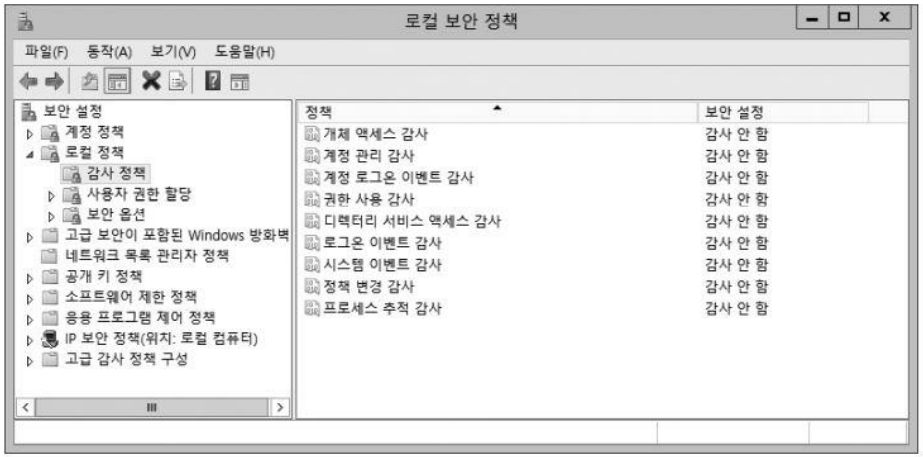
- 로그인했을 때 시스템이 이에 대한 기록을 남기는 활동
- 해당 객체나 파일에 대한 모든 접근 및 변경 사항을 기록하고 관리하는 과정. 이를 통해 누가, 언제, 어떤 작업을 수행했는지를 추적

6. 로그 관리

■ 운영체제의 로그 관리

▪ 윈도우의 로그

- 윈도우 서버 2012의 경우 로깅 항목과 설정 사항은 [로컬 보안 정책] 대화 상자의 [감사 정책] 메뉴에서 확인
- 로깅 정책 (감사 정책)은 기본적으로 수행하지 않게 설정되어 있으므로 필요할 경우 수행하도록 설정해야 함
- 설정 시 '성공'과 '실패'에 따라 선택적으로 로깅을 수행 할 수 있음



6. 로그 관리

■ 운영체제의 로그 관리

▪ 윈도우의 로그

- "Windows 키 + R" 키보드 단축기를 사용하여 "eventvwr.exe"를 입력하고 확인 버튼을 클릭하여 이벤트 뷰어를 확인, 이벤트 뷰어를 통하여 쌓이는 로깅 정보를 확인할 수 있음
- **"이벤트 ID"**를 통하여 문제를 해결하기 위한 추가적인 정보와 단계를 찾을 수 있음

- 개별 로그에서는 다음을 확인

항목	설명
종류	성공 감사와 실패 감사가 있다. 성공 감사는 어떤 시도가 성공했을 때, 실패 감사는 어떤 시도가 실패했을 때 남기는 로그다.
날짜, 시간	로그를 남긴 날짜와 시간
원본, 범주	로그와 관계있는 영역
이벤트	윈도우에서는 각 로그별로 고유한 번호를 부여한다. 로그를 분석할 때 이 번호를 알고 있으면 빠르고 효과적으로 분석할 수 있다.
사용자	관련 로그를 발생시킨 사용자
컴퓨터	관련 로그를 발생시킨 시스템

6. 로그 관리

■ 운영체제의 로그 관리

▪ 윈도우의 로그

- 윈도우가 제공하는 각 감사 정책은 다음 사항을 로깅

로그	설명
개체 액세스 감사	특정 파일이나 디렉터리, 레지스트리 키, 프린터 등과 같은 객체에 대해 접근을 시도하거나 속성 변경 등을 탐지한다.
계정 관리 감사	신규 사용자·그룹 추가, 기존 사용자·그룹 변경, 사용자 활성화·비활성화, 계정 패스워드 변경 등을 감사한다.
계정 로그인 이벤트 감사	로그온 이벤트 감사와 마찬가지로 계정의 로그인에 대한 사항을 로그로 남긴다. 이 둘의 차이점은 전자는 도메인 계정을 사용할 때 생성되고 후자는 로컬 계정을 사용할 때 생성된다는 것이다.
권한 사용 감사	권한 설정 변경이나 관리자 권한이 필요한 작업을 수행할 때 로깅한다.
로그인 이벤트 감사	로컬 계정의 접근 시 생성되는 이벤트를 감사하는 것이다. 계정 로그온 이벤트 감사에 비해 다양한 종류의 이벤트를 확인할 수 있다.
디렉터리 서비스 액세스 감사	시스템 액세스 제어 목록(SACL)이 지정되어 있는 액티브 디렉터리(active directory) 개체에 접근하는 사용자에 대한 감사 로그를 제공한다.
정책 변경 감사	사용자 권한 할당 정책, 감사 정책, 신뢰 정책의 변경과 관련된 사항을 로깅한다.
프로세스 추적 감사	사용자 또는 응용 프로그램이 프로세스를 시작하거나 중지할 때 해당 이벤트가 발생한다.
시스템 이벤트	시스템의 시작과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.

TIP 윈도우의 모든 이벤트 로그는 다음 URL에서 엑셀로 정리된 파일을 내려받을 수 있다.
http://www.microsoft.com/download/details.aspx?id=50034

6. 로그 관리

운영체제의 로그 관리

유닉스의 로그

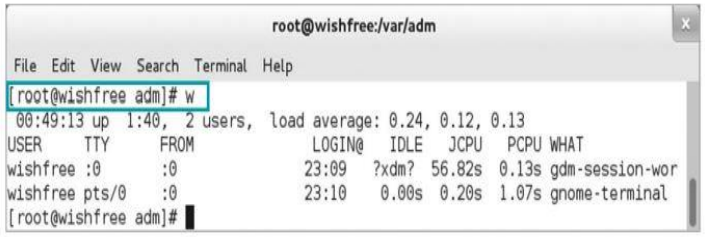
- 유닉스 시스템의 로그 저장 위치
  - /var/adm (최근 유닉스): 솔라리스, HP-UX 10.x 이후, IBM AIX
  - /var/log: FreeBSD, 솔라리스(/var/adm과 나누어 저장), 리눅스
  - /var/run: 일부 리눅스
  - 일반적으로 리눅스에서는 /var/log 디렉터리에 로그가 존재
- 일반적으로 리눅스에서는 /var/log 디렉터리에 로그가 존재

로그	설명
utmp	현재 로그인한 사용자의 아이디, 사용자 프로세스, 실행 레벨, 로그인 종류 등을 기록한다.
wtmp	사용자 로그인 · 로그아웃 시간, IP와 세션 지속 시간, 시스템 종료 · 시작 시간을 기록한다.
secure(sulog)	원격지 접속 로그와 su(switch user), 사용자 생성 등과 같이 보안에 직접적으로 연관된 로그를 저장한다.
history	명령 창에서 실행한 명령을 기록한다.
syslog	시스템 운영과 관련한 전반적인 로그다.

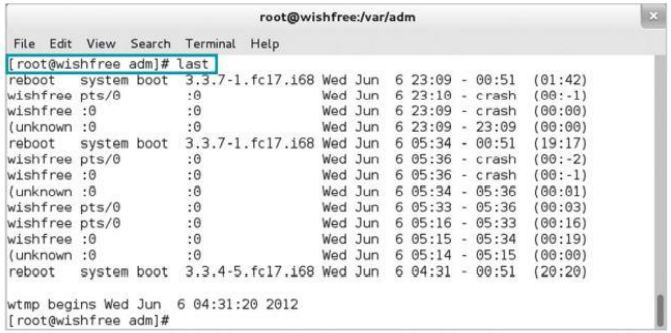
6. 로그 관리

운영체제의 로그 관리

- utmp(User Terminal Login Record)
  - utmp 파일은 **현재** 로그인한 사용자(현재 활성 세션)에 대한 정보를 저장.
  - 이 파일은 사용자가 시스템에 로그인할 때 생성되며, 사용자가 로그아웃하면 해당 정보가 삭제
  - utmp는 텍스트가 아닌 바이너리 형태로 로그가 저장
  - 로그 확인 명령어는 w, who, users, whodo, finger 등



- wtmp(Write User Terminal Login Record)
  - wtmp 파일은 **과거의** 로그인 및 로그아웃 기록을 포함하여 시스템의 모든 사용자 세션에 대한 정보를 저장
  - 이 파일은 사용자가 로그인할 때마다 새로운 기록을 추가하며, 로그아웃 시에도 기록이 남음.
  - wtmp는 시스템의 전체 로그인 기록을 보존하므로, 과거의 로그인 세션을 확인할 수 있음.
  - 내용 확인 명령어는 last



6. 로그 관리

운영체제의 로그 관리

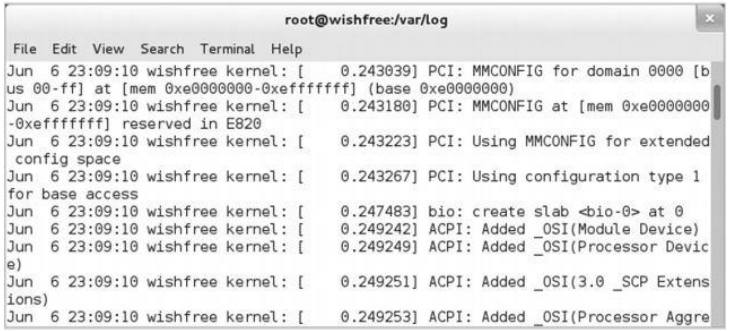
- secure(sulog)
  - 페도라, CentOS, 레드햇 등의 리눅스는 **secure 파일**에 원격지 접속 로그와 suswitch user, 사용자 생성 등과 같이 보안에 직접적으로 연관된 로그를 저장
  - 일반 유닉스에서 su 로그는 /var/adm/sulog 파일에 텍스트 형식으로 남음

6. 로그 관리

운영체제의 로그 관리

- history
  - 명령 창에서 실행한 명령에 대한 기록은 history 명령으로 확인

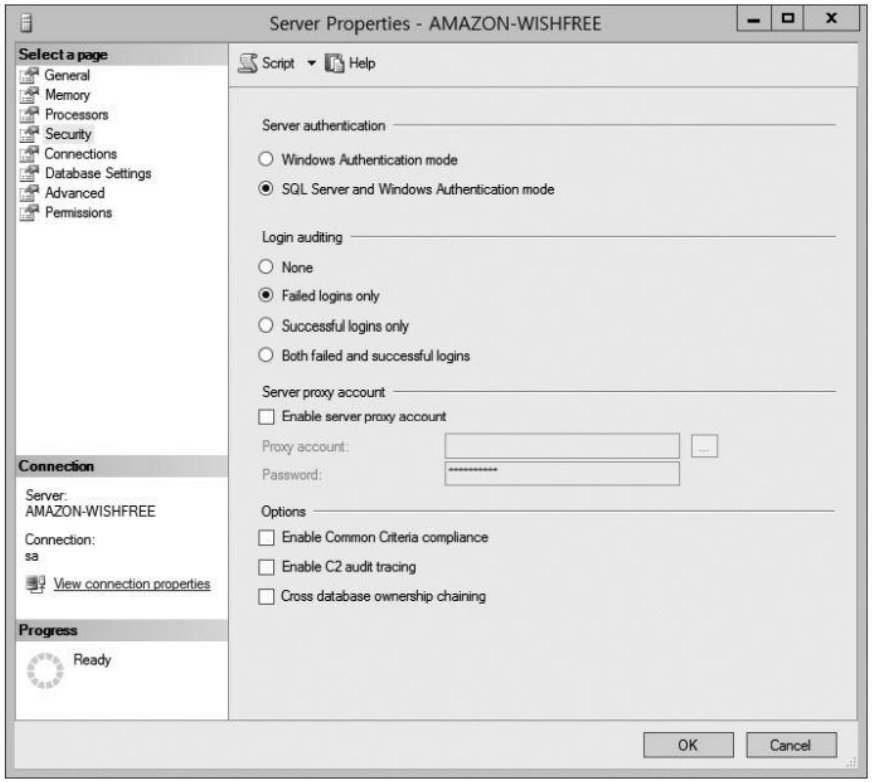
- syslog
  - 유닉스 시스템 내에서 사용하는 시스템 운영과 관련된 '로그 생성/관리' 도구
    - Syslog는 시스템 로그 메시지를 수집하고 전송하는 표준 프로토콜로, 다양한 시스템과 장치에서 발생하는 로그를 중앙에서 관리할 수 있도록 함
  - 다양한 소스(커널, 애플리케이션, 보안 시스템(네트워크 장비) 등)에서 발생하는 로그 메시지를 중앙에서 수집하고 저장
  - /var/log/messages 파일에 하드웨어의 구동, 서비스의 동작, 에러 등의 다양한 로그를 남김



6. 로그 관리

■ 데이터베이스의 로그 관리

- MS-SQL의 로그
  - Microsoft SQL Server Management Studio에서 서버를 선택한 뒤, 속성 대화 상자의 [보안] 메뉴에서 **'일반 로그인 감사'**와 **'C2 감사 추적'**을 설정할 수 있음
    - C2 감사 추적은 데이터베이스가 생성·삭제·변경되는지에 대한 자세한 정보를 로그로 남기는 것이므로 사용을 권고하지 않음



6. 로그 관리

데이터베이스의 로그 관리

- MySQL 로그

로그	설명
Error 로그	확장자 .err의 파일로 데이터 디렉터리에 생성된다. MySQL의 구동과 모니터링, 쿼리 에러에 관련된 메시지를 포함한 것으로, 별다른 설정 없이 기본적으로 남는 로그다.
General 로그	MySQL에서 실행되는 전체 쿼리를 저장한다.
Slow Query 로그	요청되는 전체 쿼리를 저장하는 General 로그와 달리, Slow Query 로그는 쿼리가 정상 완료된 시간, 즉 실행된 시간까지 입력하기 때문에 실행 도중 에러가 발생한 쿼리에 대해서는 로그로 남기지 않는다.
Binary 로그 & Relay 로그	Binary 로그는 데이터베이스 변경(테이블 생성, 삭제 등) 및 테이블 변경(insert, update, delete 등) 사항들이 기록되는 바이너리 형태의 파일로, MySQL의 복제를 구성하거나 특정 시점을 복구할 때 사용된다. 일반적으로 Binary 로그는 마스터에서, Rela 로그는 슬레이브에서 생성되며 포맷과 내용은 동일하다.

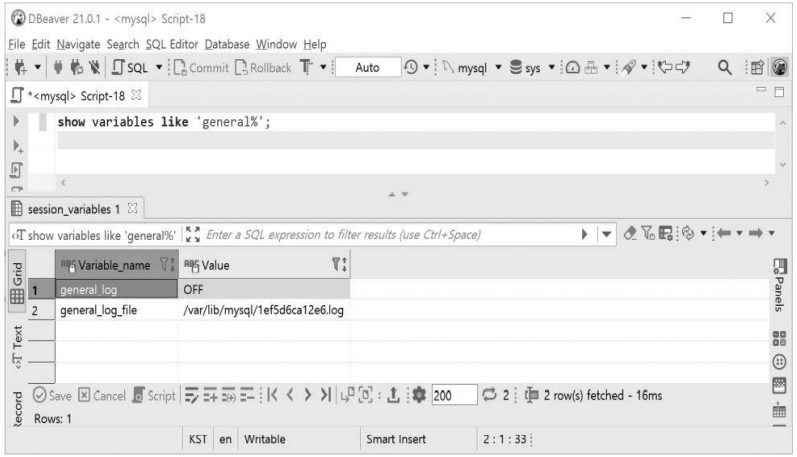
6. 로그 관리

데이터베이스의 로그 관리

MySQL 로그

- General 로그의 경우, 현재 설정을 확인할 수 있음

```
show variables like 'general%';
```



- General Log는 다음과 같이 설정 및 해제될 수 있음

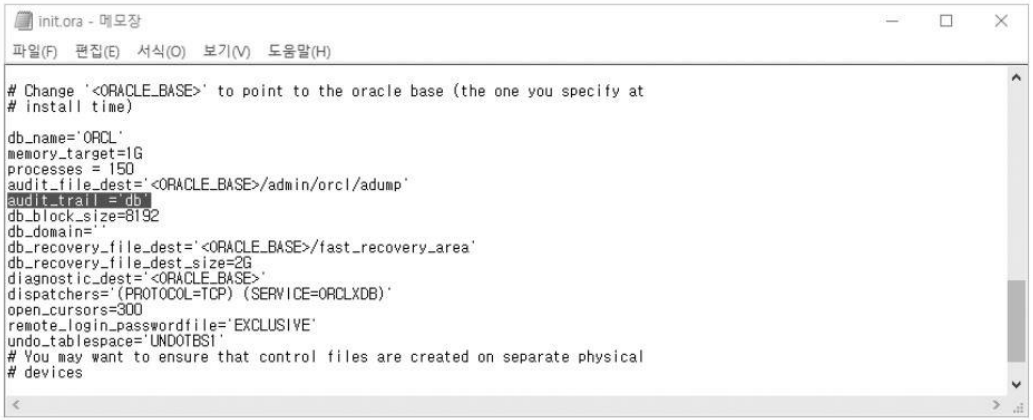
```
set global general_log = ON;    # 설정
set global general_log = OFF;    # 해제
```

6. 로그 관리

■ 데이터베이스의 로그 관리

▪ 오라클의 로그

- 오라클에서 감사 로그를 활성화하려면 먼저 오라클 파라미터 파일($ORACLE_HOME/dbs/ init.ora)의 AUDIT_TRAIL 값을 'DB' 또는 'TRUE'로 지정



설정 값	의미
NONE 또는 FALSE	데이터베이스 감사를 비활성화한다.
DB 또는 TRUE	데이터베이스 감사를 활성화한다.
OS	감사 로그를 OS상의 파일로 저장한다. 이때 경로명은 audit_file_dest에 의해 지정된다.

6. 로그 관리

■ 데이터베이스의 로그 관리

▪ 오라클의 로그

- 오라클에서 남길 수 있는 데이터베이스 감사의 종류로는 문장 감사, 권한 감사, 객체 감사가 있음

문장 감사	
설명	지정된 문장을 실행했을 때 기록을 남긴다.
예	AUDIT TABLE BY wishfree: 사용자 wishfree의 table에 대한 감사 활성화로 create table, drop table, truncate table, comment on table, delete from table 등의 작업이 수행된 경우 모두 audit trail을 남긴다. AUDIT SESSION BY wishfree, daniel: 사용자 wishfree와 daniel에 대한 세션 로그 감사를 활성화한다.
권한 감사	
설명	특정한 권한을 사용했을 때 기록을 남긴다.
예	AUDIT DELETE ANY TABLE BY ACCESS WHENEVER NOT SUCCESSFUL: 어떤 테이블이든 삭제하려는 시도에 대해 성공 유무와 관계없이 로그를 남긴다.
객체 감사	
설명	특정 객체에 대한 작업을 했을 때 기록을 남긴다.
예	AUDIT select ON wishfree.test BY session WHENEVER successful: 사용자 wishfree의 test 테이블에 대한 select가 실행되어 성공한 경우 세션별로 감사 로그를 생성한다.

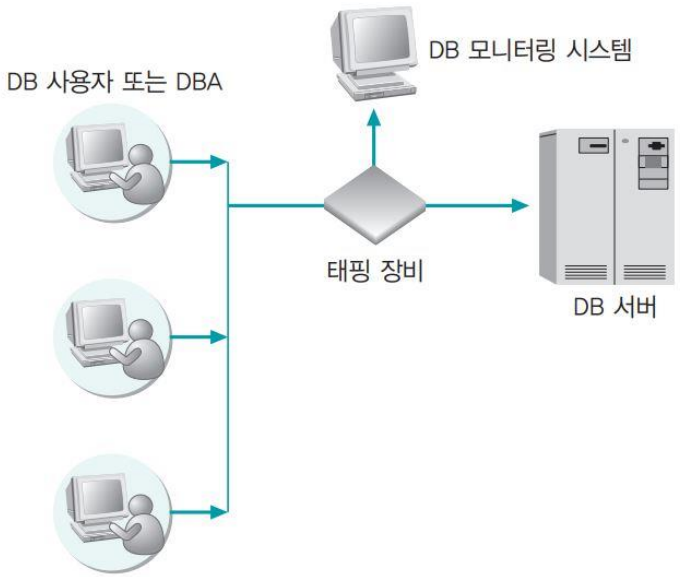
- 각각의 감사는 감사 뷰를 통해 확인 가능

뷰	설명
dba_stmt_audit_opts	문장 감사의 옵션을 확인한다.
dba_priv_audit_opts	권한 감사의 옵션을 확인한다.
dba_obj_audit_opts	객체 감사의 옵션을 확인한다.
dba_audit_trail	데이터베이스의 모든 감사 로그를 출력한다.
dba_audit_object	데이터베이스의 객체와 관련된 모든 감사 로그를 출력한다.
user_audit_object	현재 사용자의 객체와 관련된 모든 감사 로그를 출력한다.
dba_audit_session	사용자의 로그인·로그오프에 대한 감사 로그를 출력한다.
dba_audit_statement	문장 감사 로그를 출력한다.
dba_audit_object	객체 감사 로그를 출력한다.

6. 로그 관리

■ 데이터베이스의 로그 관리

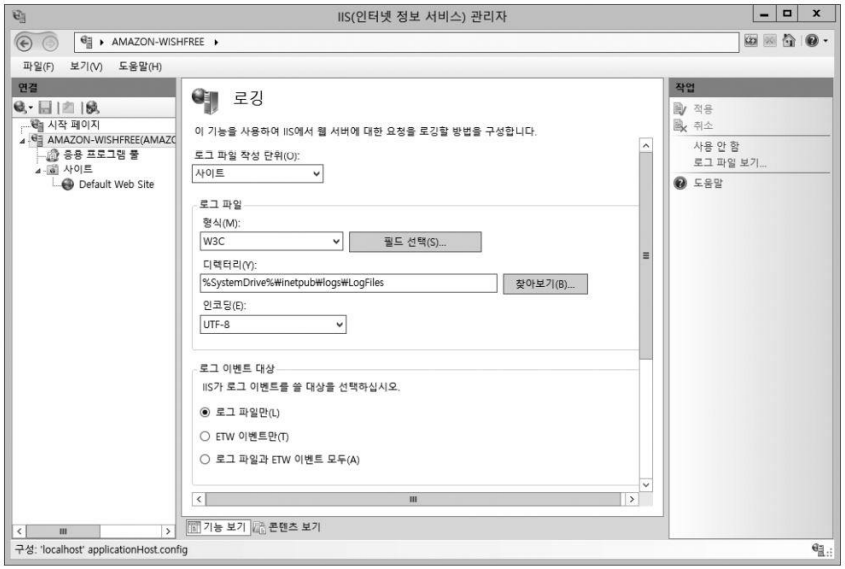
- 데이터베이스 모니터링
  - 네트워크 트래픽을 모니터링할 수 있는 태핑 장비를 네트워크에 설치
  - 네트워크 패킷 중에서 데이터베이스 질의문을 확인하여 이를 로그로 남김
  - 데이터베이스의 성능에 영향을 미치지 않으면서 잘못된 접근 시도와 질의문 입력을 모두 모니터링할 수 있음

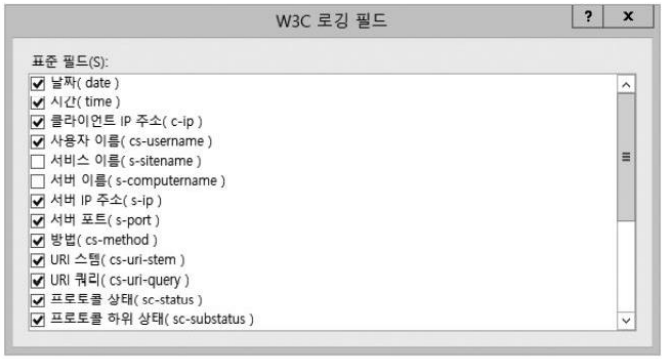


6. 로그 관리

응용 프로그램의 로그 관리

- IIS 웹 서버의 로그
  - IIS 웹 서버의 로그는 [제어판]의 '로깅' 항목에서 확인
  - 로그는 IIS 웹 서버의 기본 설정이면서 가장 널리 이용되는 'W3C 확장 로그 파일 형식'으로 설정되어 있음
  - NCSA, IIS, 사용자 지정 방식 로그 파일 형식을 사용할 수 있음





6. 로그 관리

응용 프로그램의 로그 관리

- IIS 웹 서버의 로그
  - 실제 로그는 '디렉터리'에 다음과 같은 형태로 남음

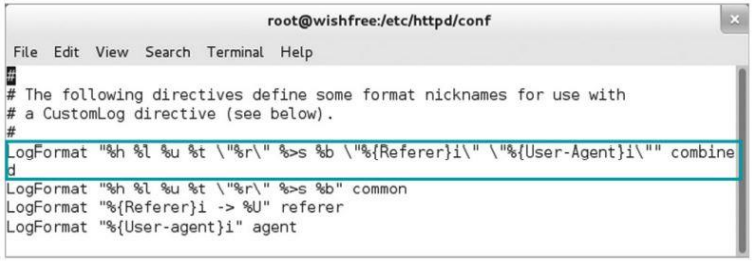
```
2021-06-03                    08:53:12                    192.168.137.128
GET/XSS/GetCookie.asp?cookie=ASPSESSIONIDQQ CAQDDA 80 - 192.168.137.1
Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;) 200 0 0 225
```

  - 샘플 로그의 실제 구성
    - **날짜와 시간**: 2021-06-03 08:53:12
    - **서버 IP**: 192.168.137.128
    - **HTTP 접근 방법과 접근 URL**: GET/XSS/GetCookie.asp?cookie=ASPSESSIO...
    - **서버 포트**: 80
    - **클라이언트 IP**: 192.168.137.1
    - **클라이언트의 웹 브라우저**: Mozilla/5.0+(compatible;+MSIE+9.0;+Windows...
    - **실행 결과 코드**: 200(OK)
    - **서버에서 클라이언트로 전송한 데이터의 크기**: 0
    - **클라이언트에서 서버로 전송한 데이터의 크기**: 0
    - **처리 소요 시간**: 225ms

6. 로그 관리

응용 프로그램의 로그 관리

- 아파치 웹 서버의 로그
  - 아파치 웹 서버에 대한 기본 접근 로그는 access_log에 남고 형식은 'combined'로 지정
  - httpd.conf 파일에서 combined 형식의 LogFormat을 확인할 수 있음



항목	설명
%a	클라이언트의 IP 주소
%A	서버의 IP 주소
%b	헤더 정보를 제외하고 전송된 데이터의 크기를 전송된 데이터의 크기가 0이면 '-'로 표시한다.
%c	응답이 완료되었을 때의 연결 상태 • X: 응답이 완료되기 전에 연결이 끊김 • +: 응답을 보낸 후에도 연결이 지속됨 • -: 응답을 보낸 후 연결이 끊김
%{Header}e	환경 변수 헤더의 내용
%f	요청된 파일 이름
%h	클라이언트의 도메인 또는 IP 주소
%H	요청 프로토콜의 종류
%l	inetd를 사용하고 있을 때 클라이언트의 로그인명
%m	요청 방식
%p	서버가 요청을 받아들이는 포트 번호
%P	요청을 처리하는 자식 프로세스의 아이디
%q	질의에 사용된 문자
%r	HTTP 접근 방법과 접근 URL
%s	HTTP 실행 결과 코드
%{format}t	웹 서버에 작업을 요구한 시간
%T	웹 서버가 요청을 처리하는 데 소요된 시간(초)
%u	클라이언트의 사용자
%U	요청된 URL 경로
%v	요청을 처리하는 서버의 이름
%i	클라이언트의 웹 브라우저

6. 로그 관리

응용 프로그램의 로그 관리

아파치 웹 서버의 로그

- access_log

```
192.168.137.1 - - [06/JUN/2017:05:48:28 +0900] "GET/HTTP/1.1" 403 4609 "-"
"Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)"
```

- access_log에서 샘플 로그의 구성
  - **클라이언트 IP(%h)**: 192.168.137.1
  - **클라이언트 로그인명(%l)**: -
  - **클라이언트 사용자명(%u)**: -
  - **날짜와 시간(%t)**: [06/JUN/2017:05:48:28 +0900]
  - **HTTP 접근 방법과 접근 URL(%r)**: GET/HTTP/1.1
  - **실행 결과 코드(%s): 403 Forbidden**
  - **서버에서 클라이언트로 전송한 데이터의 크기(%b)**: 4609바이트
  - **클라이언트의 웹 브라우저(%i)**: Mozilla/5.0 (compatible; MSIE 9.0; Windows...

6. 로그 관리

네트워크 장비의 로그 관리

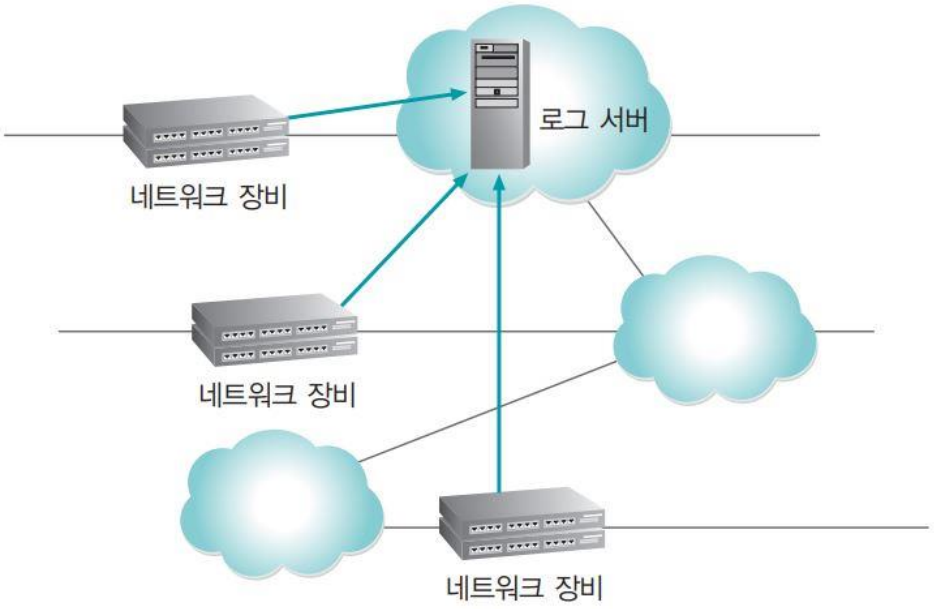
- 네트워크 보안 시스템의 로그
  - 침입 차단 시스템, 침입 탐지 시스템, 침입 방지 시스템 등 다양한 보안 시스템의 로그를 확인할 수 있음
  - 다양한 보안 시스템의 로그는 통합 로그 관리 시스템 (Security Information and Event Management, SIEM)에 의해 수집·관리되기도 함
- 네트워크 관리 시스템의 로그
  - 네트워크 트래픽 모니터링 시스템(Multi Router Traffic Grapher, MRTG)과 네트워크 관리 시스템(Network Management System , NMS)의 로그를 참고할 수 있음
  - NMS의 솔루션으로는 Splunk, IBM Qradar, Microsoft Sentinel 등이 있음
- 네트워크 장비 인증시스템의 로그
  - 대규모 네트워크를 운영하는 곳에서는 라우터나 스위치의 인증, 권한 부여, 계정관리 등을 일원화하기 위해 인증 서버로 TACACS+(Terminal Access Controller Access-Control System Plus)를 사용
  - 인증 서버를 통해 네트워크 장비에 대한 인증 시도 및 로그인 정보 등을 확인할 수 있음

6. 로그 관리

■ 네트워크 장비의 로그 관리

▪ 로그 서버

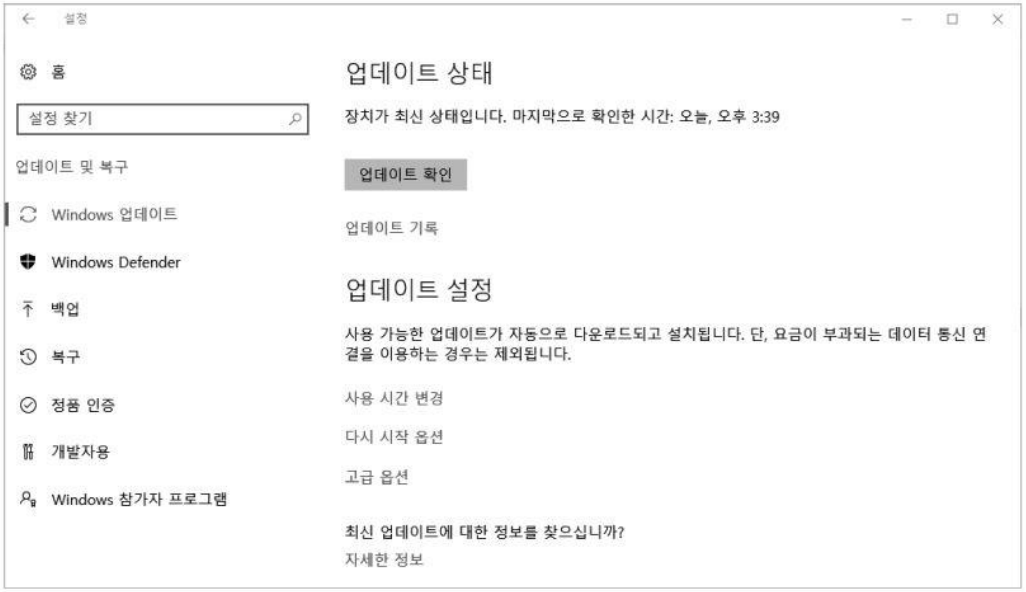
- 대부분의 네트워크 장비에는 하드디스크와 같이 로그를 저장할 저장 공간이 없어 로그 서버를 별도로 두고 운영
- 로그 서버를 운용하면 해커가 어떤 네트워크 장비에 침투하더라도 자신의 흔적을 지우기가 쉽지 않음
- 이 때문에 네트워크 장비 뿐만 아니라 운영체제 등을 관리할 때 로그 서버를 따로 운영



7. 취약점 관리

패치 관리

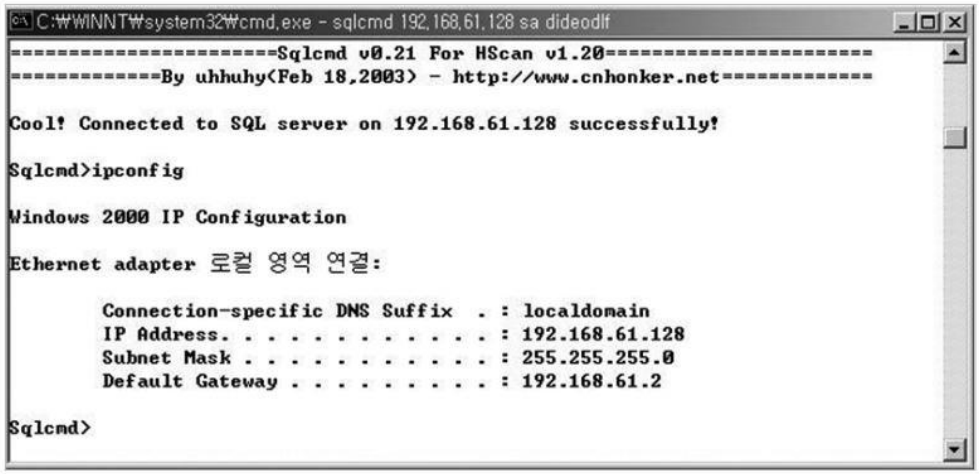
- 응용 프로그램을 만든 제작사가 배포하는 패치 또는 서비스 팩을 적용해 시스템 자체의 취약점을 보완
- 유닉스 시스템에도 내재된 취약점이 있지만 윈도우는 사용률이 훨씬 높고 접근하기도 쉬워 공격을 더 많이 받음
- 윈도우 업데이트를 통해 자동으로 보안 패치를 확인하고 적용할 수 있음



7. 취약점 관리

응용 프로그램 별 고유 위험 관리

- 응용 프로그램을 통해 운영체제의 파일이나 명령을 실행시킬 수 있는 것이 있음
- **MS-SQL의 xp_cmdshell**은 데이터베이스를 통해 운영체제의 명령을 실행하고, 파일 등에 접근할 수 있음
- 응용 프로그램의 동작과 관련하여 운영체제에 접근할 수 있는 함수나 기능이 있으면 적절성을 검토해야 함



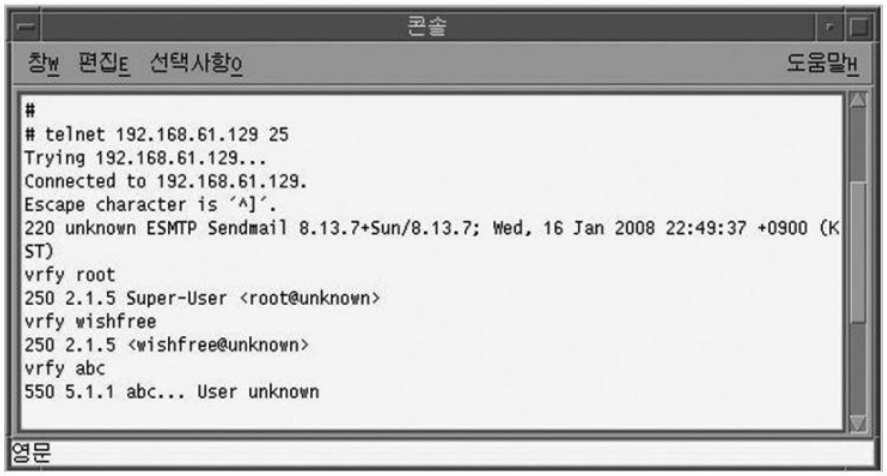
MS-SQL 2000에서 xp_cmdshell 툴을 이용한 명령 창 획득

7. 취약점 관리

■ 응용 프로그램의 정보 수집 제한

- 운영체제에 직접적인 영향을 미치지 않아도 응용 프로그램의 특정 기능이 운영체제의 정보를 노출시키기도 함
- 유닉스에서 이메일을 보낼 때 수신자가 있는 시스템의 sendmail 데몬에 해당 계정이 존재하는지 확인하는 과정으로 일반 계정은 vrfy 명령, 그룹은 expn명령을 시스템 내부에서 사용
- 일반 사용자는 텔넷을 이용해 시스템에 존재하는 계정 목록을 파악할 수 있음

```
telnet 192.168.61.129 25
vrfy root
vrfy wishfree
vrfy abc
```



sendmail 데몬에 접속하여 vrfy 명령을 실행한 결과