

정보보호와 시스템 보안

시스템 보안

전은아

목차

1. 시스템 보안에 대한 이해
2. 계정과 패스워드 관리
3. 세션 관리
4. 접근 제어
5. 권한 관리
6. 로그 관리
7. 취약점 관리

학습목표

- 시스템과 관련한 6가지 보안 주제를 이해한다.
- 계정과 패스워드의 중요성을 이해하고 적절한 패스워드 설정법을 익힌다.
- 세션의 의미와 관리 방법을 살펴본다.
- 사용자 및 클라이언트에 대한 접근 제어와 권한 관리 방법을 알아본다.
- 로그의 의미와 수행 가능한 로그의 범위를 살펴본다.

01 시스템 보안에 대한 이해

■ 시스템과 관련한 보안 기능

■ 계정과 패스워드 관리

- 적절한 권한을 가진 사용자를 식별하기 위한 가장 기본적인 인증 수단
- 시스템에서는 계정과 패스워드 관리가 보안의 시작

■ 세션 관리

- 사용자와 시스템 또는 두 시스템 간의 활성화된 접속에 대한 관리
- 일정 시간이 지날 경우 적절히 세션을 종료하고, 비인가자에 의한 세션 가로채기를 통제

■ 접근 제어

- 시스템이 네트워크 안에서 다른 시스템으로부터 적절히 보호될 수 있도록 네트워크 관점에서 접근을 통제

■ 권한 관리

- 시스템의 각 사용자가 적절한 권한으로 적절한 정보 자산에 접근할 수 있도록 통제

■ 로그 관리 해커들이 해킹하고 로그 지워야함

- 시스템 내부 혹은 네트워크를 통한 외부에서 시스템에 어떤 영향을 미칠 경우 해당 사항을 기록

■ 취약점 관리

- 시스템은 계정과 패스워드 관리, 세션 관리, 접근 제어, 권한 관리 등을 충분히 잘 갖추고도 보안적인 문제가 발생할 수 있음.
- 이는 시스템 자체의 결함에 의한 것으로 이 결함을 체계적으로 관리하는 것이 취약점 관리이다.

02 계정과 비밀번호 관리

■ 인증 수단

- 계정은 시스템에 접근하는 가장 기본적인 방법
- 기본 구성 요소는 아이디와 비밀번호
- 식별(Identification)이란 아이디라는 문자열을 통해 그 자신이 누구인지 확인하는 과정
- 아이디만으로는 정확한 식별이 어려워 인증(Authentication)을 위한 다른 무언가(비밀번호)를 요청

■ 비밀번호 보안의 4가지 인증 방법

- **알고 있는 것(Something You Know)** : 군대의 암호어처럼 머릿속에 기억하고 있는 정보를 이용해 인증을 수행하는 방법

EX) 비밀번호

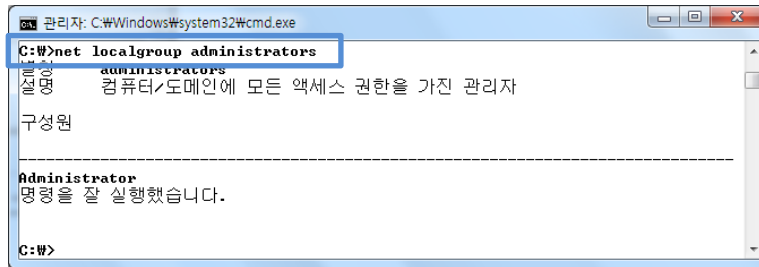
가지고 있는 것	인증의 유형	종류	통해 인증
증을 : EX) 출	알고 있는 것	비밀번호, 주민등록번호, I-PIN 등	
스스로 : EX) 지	가지고 있는 것	신분증, 여권, 신용카드, 인증서, OTP, Key, 스마트카드	1
	그 자체	홍채, 지문, 각막, 행동, 서명	
위치하 : EX) 콜백	위치해 있는 곳	지역, IP 주소	1

02 계정과 비밀번호 관리

■ 운영체제의 계정 관리

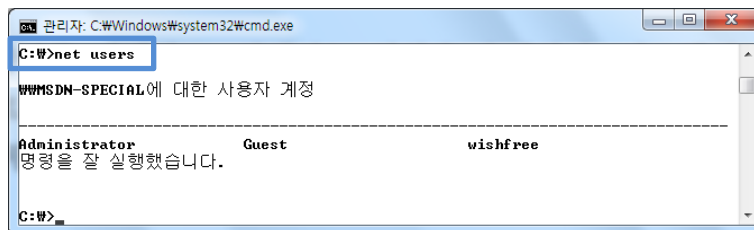
■ 윈도우의 계정 관리

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



[그림 3] 윈도우에서 관리자 그룹에 속한 계정 목록 확인

- 일반 사용자를 확인하려면 **net users**라는 명령을 사용한다.



[그림 4] 윈도우에서 일반 사용자 확인

- 윈도우에서 시스템에 존재하는 그룹의 목록은 [**net localgroup** 명령으로 확인

02 계정과 패스워드 관리

■ 운영체제의 계정 관리

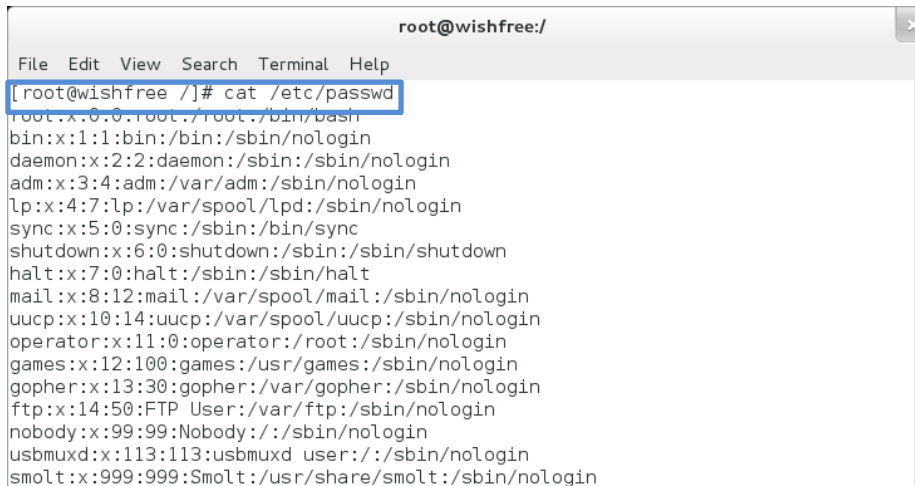
[표 1] 윈도우의 주요 그룹

구분	특징
Administrators	<ul style="list-style-type: none">• 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.
Power Users	<ul style="list-style-type: none">• Administrators 그룹이 가진 권한을 대부분 가지지만, 로컬 컴퓨터에서만 관리할 능력도 가지고 있다.• 해당 컴퓨터 밖의 네트워크에서는 일반 사용자로 존재한다.
Backup Operators	<ul style="list-style-type: none">• 윈도우 시스템에서 시스템 파일을 백업하는 권한을 가지고 있다.• 로컬 컴퓨터에 로그인하고 시스템을 종료할 수 있다.
Users	<ul style="list-style-type: none">• 대부분의 사용자가 기본으로 속하는 그룹으로 여기에 속한 사용자는 네트워크를 통해 서버나 다른 도메인 구성요소에 로그인할 수 있다.• 관리 계정에 비해서 한정된 권한을 가지고 있다.
Guests	<ul style="list-style-type: none">• 윈도우 시스템에서 Users 그룹과 같은 권한을 가진다.• 두 그룹 모두 네트워크를 통해서 서버에 로그인할 수 있으며 서버로의 로컬 로그인도 금지된다.

02 계정과 비밀번호 관리

■ 운영체제의 계정 관리

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



```
root@wishfree:/  
File Edit View Search Terminal Help  
[root@wishfree /]# cat /etc/passwd  
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  
operator:x:11:0:operator:/root:/sbin/nologin  
games:x:12:100:games:/usr/games:/sbin/nologin  
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin  
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin  
nobody:x:99:99:Nobody:/:/sbin/nologin  
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin  
smolt:x:999:999:Smolt:/usr/share/smolt:/sbin/nologin
```

[그림 6] 유닉스에서 etc/passwd 파일 열람

02 계정과 패스워드 관리

■ 운영체제의 계정 관리

- 유닉스의 계정 관리
 - /etc/passwd 파일의 구성

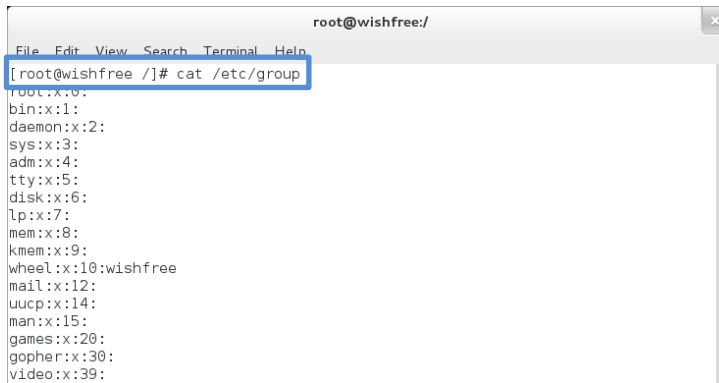
```
root : x : 0 : 0 : root : /root : /bin/bash
  ①  ② ③ ④ ⑤ ⑥ ⑦
```

- ① 사용자 계정
- ② 패스워드가 암호화되어 shadow 파일에 저장되어 있음을 나타낸다.
- ③ 사용자 번호 pid
- ④ 그룹 번호 gid
- 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.

02 계정과 비밀번호 관리

■ 운영체제의 계정 관리

- 유닉스의 계정 관리
 - 유닉스에서 그룹은 /etc/group 파일에서 확인할 수 있다.



```
root@wishfree:/  
[root@wishfree /]# cat /etc/group  
root:x:0:  
bin:x:1:  
daemon:x:2:  
sys:x:3:  
adm:x:4:  
tty:x:5:  
disk:x:6:  
lp:x:7:  
mem:x:8:  
kmem:x:9:  
wheel:x:10:wishfree  
mail:x:12:  
uucp:x:14:  
man:x:15:  
games:x:20:  
gopher:x:30:  
video:x:39:
```

[그림 7] 유닉스에서 그룹 확인

- /etc/group의 구조.

```
root : x : 0 : root  
① ② ③ ④
```

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

02 계정과 패스워드 관리

■ 데이터베이스의 계정 관리

- MS-SQL에서 관리자 계정은 sa(system administrator)이고, 오라클에서 관리자계정은 sys, system
 - sys와 system은 둘 다 관리자 계정이지만, system은 sys와 달리 데이터베이스를 생성할 수 없음.
- 오라클은 Scott이라는 기본 계정이 존재하고, 솔루션을 설치하거나 테이블을 생성할 때 관련 계정이 자동으로 생성되는 경우가 많음.

■ 응용 프로그램의 계정 관리

- 취약한 응용 프로그램을 통해 공격자는 운영체제에 접근해서 민감한 정보를 습득하여 운영체제를 공격하는데 이용할 수 있음.
- TFTP(Trivial File Transfer Protocol)처럼 **인증이 필요하지 않는 응용 프로그램은 더욱 세심한 주의가 필요함.**

■ 네트워크 장비의 계정 관리

- 네트워크 장비에는 계정이라는 개념이 존재하지 않음
- 그렇지만 네트워크 장비도 계정을 생성하여 각 계정으로 사용할 수 있는 명령어 집합을 제한할 수 있음.
- 네트워크가 대규모인 경우에는 계정 관리의 어려움 때문에 통합된 계정 관리를 위해 TACACS+와 같은 솔루션을 적용하기도 함

02 계정과 비밀번호 관리

■ 비밀번호 관리

- 부적절한 비밀번호의 예
 - 길이가 너무 짧거나 널(Null)인 비밀번호
 - 사전에 나오는 단어나 이들의 조합
 - 키보드 자판의 일련 나열
 - 사용자 계정 정보로 유추 가능한 단어들
- 좋은 비밀번호란?
 - 기억하기 쉽지만 크래킹하기 어려운 비밀번호
- 비밀번호와 관련된 주요 정책
 - **비밀번호 설정 정책**
 - 비밀번호의 길이와 복잡도를 정해두는 것
 - 비밀번호 길이는 8자 이상, 복잡도는 연속된 숫자나 알파벳을 사용하지 못하게 하고 숫자와 알파벳, 특수 문자를 섞어 설정하게 하는 식이다.
 - **비밀번호 변경 정책**
 - 일반적으로 60일 또는 90일 간격으로 비밀번호를 변경하도록 하고 있다.
 - **잘못된 비밀번호 입력 시 계정 잠금**
 - 잘못된 비밀번호를 반복 입력할 경우 비밀번호 크래킹 공격 또는 비인가자의 접근 시도로 판단하여 해당 계정을 사용하지 못하게 설정한다.

<http://www.passwordmeter.com>

<https://howsecureismypassword.net/>

03 세션 관리

■ 세션의 의미

- 사용자와 컴퓨터 또는 두 컴퓨터 간의 활성화된 접속



[그림 8] 서버 입장에서 세션을 유지하는 방법

03 세션 관리

■ 세션의 의미

- 세션을 유지하기 위한 보안 사항

- ① 세션 하이재킹(Session Hijacking)이나 네트워크 패킷 스니핑(Sniffing)에 대응하기 위해 암호화를 하는 것
- ② 세션에 대한 지속적인 인증(Continuous Authentication)을 하는 것



[그림 9] 윈도우 화면 보호기 설정

04 접근 제어

■ 접근 제어의 의미

- 접근 제어(Access Control)는 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근할 수 있도록 통제하는 것
- 시스템의 보안 수준을 갖추기 위한 가장 기본적 수단
- 시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트이다.

■ 운영체제의 접근 제어

- 운영체제에 어떤 관리적 인터페이스가 운영되고 있는지 알아보자.

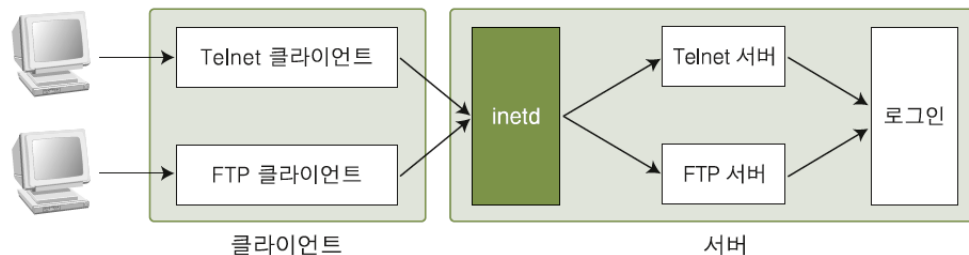
[표 2] 일반적으로 사용되는 관리 인터페이스

운영체제	서비스 이름	사용 포트	특징
유닉스(리눅스 포함)	텔넷(Telnet)	23	암호화되지 않음
	SSH	22	SFTP 가능
	XDMCP	5000	유닉스용 GUI(XManager)
	FTP	21	파일 전송 서비스
윈도우	터미널 서비스	3389	포트 변경 가능
	GUI 관리용 툴	-	VNC, Radmin 등

04 접근 제어

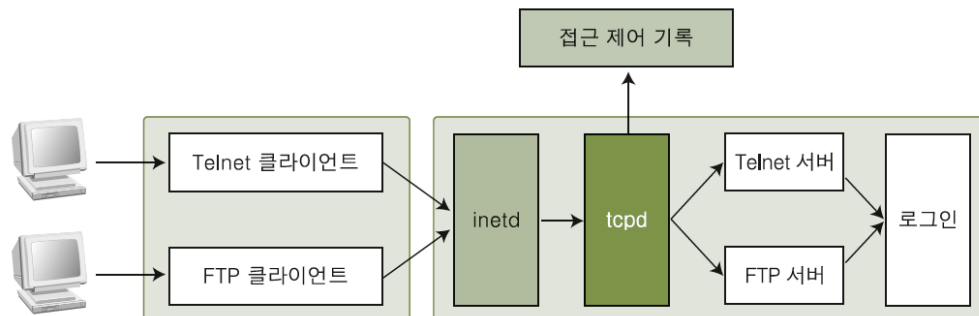
■ 운영체제의 접근 제어

- Inetd 데몬은 클라이언트로부터 inetd가 관리하고 있는 Telnet이나 SSH, FTP 등에 대한 연결 요청을 받은 후 해당 데몬을 활성화시켜 실제 서비스를 하는, 데몬과 클라이언트의 요청을 연결시켜주는 역할을 함.



[그림 10] inetd 데몬을 통한 데몬 동작도

- TCPWrapper가 설치되면, inetd 데몬은 연결을 TCPWrapper의 tcpd 데몬에 넘겨줌. tcpd 데몬은 접속을 요구한 클라이언트에 **적절한 접근 권한이 있는지 확인한 후** 해당 데몬에 연결을 넘겨주며, 이때 연결에 대한 로그도 실시할 수 있음.

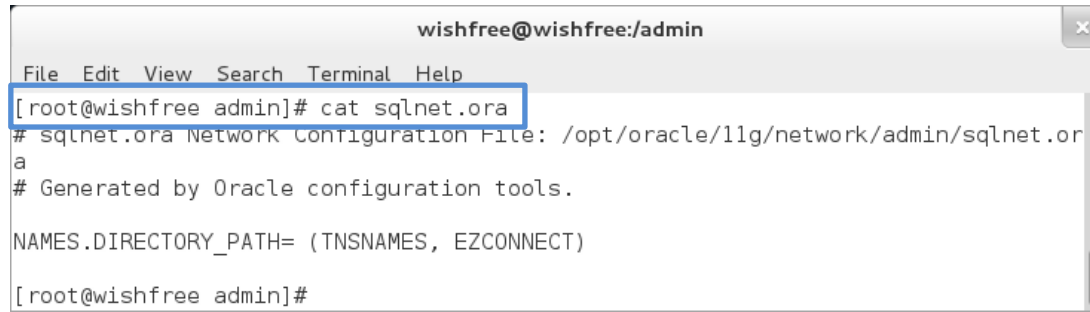


[그림 11] TCP Wrapper를 통한 데몬 동작도

04 접근 제어

■ 데이터베이스의 접근 제어

- 오라클은 \$ORACLE_HOME/network/admin/sqlnet.ora 파일에서 설정



```
wishfree@wishfree:/admin
File Edit View Search Terminal Help
[root@wishfree admin]# cat sqlnet.ora
# sqlnet.ora Network Configuration File: /opt/oracle/11g/network/admin/sqlnet.ora
# Generated by Oracle configuration tools.

NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)

[root@wishfree admin]#
```

[그림 12] 오라클의 sqlnet.ora 파일 내용

- 200.200.200.100과 200.200.200.200이라는 두 IP의 접근을 허용하고 싶으면 ❶과 같이, 200.200.200.150의 접근을 차단하고 싶으면 ❷와 같이 추가

- ❶ tcp.invited_nodes=(200.200.200.100, 200.200.200.200)
- ❷ tcp.excluded_nodes=(200.200.200.150)

- MS-SQL은 IP에 대한 접근 제어를 기본으로 제공하지 않음.

04 접근 제어

■ 응용 프로그램의 접근 제어

- 최근의 상용 응용 프로그램은 IP에 대한 접근 제어를 제공하는 경우가 많음.
 - 웹 서비스를 제공하는 IIS와 아파치 역시 IP에 대한 접근 제어를 제공

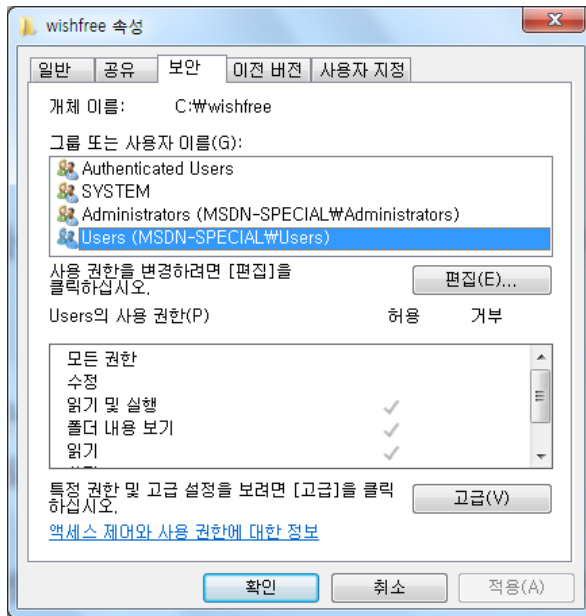
■ 네트워크 장비의 접근 제어

- 네트워크 장비에서 수행하는 IP에 대한 접근 제어로는 관리 인터페이스의 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 트래픽에 대한 접근 제어는 방화벽에서의 접근 제어와 기본적으로 같음.

05 권한 관리

■ 운영체제의 권한 관리

- 윈도우의 권한 관리
 - NTFS 권한의 종류



[그림 13] 임의 디렉터리의 권한 설정 창

- ❶ 모든 권한 : 디렉터리에 대한 접근 권한과 소유권을 변경할 수 있으며, 하위에 있는 디렉터리와 파일을 삭제할 수 있음.
- ❷ 수정 : 디렉터리를 삭제할 수 있음. 읽기 및 실행과 쓰기 권한이 주어진 것과 같음.
- ❸ 읽기 및 실행 : 읽기를 수행할 수 있으며, 디렉터리나 파일을 옮길 수 있음.
- ❹ 디렉터리 내용 보기 : 디렉터리 내의 파일이나 디렉터리의 이름을 볼 수 있음.
- ❺ 읽기 : 디렉터리의 내용을 읽기만 할 수 있다.
- ❻ 쓰기 : 해당 디렉터리에 하위 디렉터리와 파일을 생성할 수 있으며, 소유권이나 접근 권한의 설정 내용을 확인할 수 있음.

- 윈도우의 6가지 권한은 다음과 같은 규칙이 적용된다.
 - 규칙 1 : 접근 권한은 누적된다.
 - 규칙 2 : 파일에 대한 접근 권한이 디렉터리에 대한 접근 권한보다 우선한다.
 - 규칙 3 : '허용'보다 '거부'가 우선한다.

05 권한 관리

■ 운영체제의 권한 관리

- 유닉스의 권한 관리

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

① ② ③

- ① 파일의 종류와 권한으로, 다음과 같이 네 부분으로 세분화할 수 있다.

- rw- r-- r--
① ② ③ ④

- ① 파일 및 디렉터리의 종류이다. -표시는 일반 파일을, d 표시는 디렉터리를, l 표시는 링크(Link)를 나타냄.
 - ② 파일 및 디렉터리 소유자의 권한
 - ③ 파일 및 디렉터리 그룹의 권한
 - ④ 해당 파일 및 디렉터리 소유자도 그룹도 아닌 제3의 사용자에게 대한 권한
- 유닉스는 읽기(r: read), 쓰기(w: write), 실행(x : execute)과 같은 세 가지 권한을 부여.
 - 권한은 숫자로도 표현할 수 있음. 읽기는 4, 쓰기는 2, 실행은 1로 바꾸어 각 권한 세트별로 합치는 것.

```
rw- r-x r-x = 42- 4-1 4-1 → 655
```

- ② 파일에 대한 소유자
- ③ 파일에 대한 그룹

05 권한 관리

■ 데이터베이스의 권한 관리

■ 질의문에 대한 권한 권리

• DDL

- DDL(Data Definition Language)은 데이터 구조를 정의하는 질의문
- 데이터베이스를 처음 생성하고 개발할 때 주로 사용하고 운영 중에는 거의 사용하지 않음.
 - CREATE : 데이터베이스 객체를 생성한다.
 - DROP : 데이터베이스 객체를 삭제한다.
 - ALTER : 기존의 데이터베이스 객체를 다시 정의한다.

• DML

- DML(Data Manipulation Language)은 데이터베이스의 운영 및 사용과 관련해 가장 많이 사용하는 질의문
- 데이터의 검색과 수정 등을 처리
 - 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.

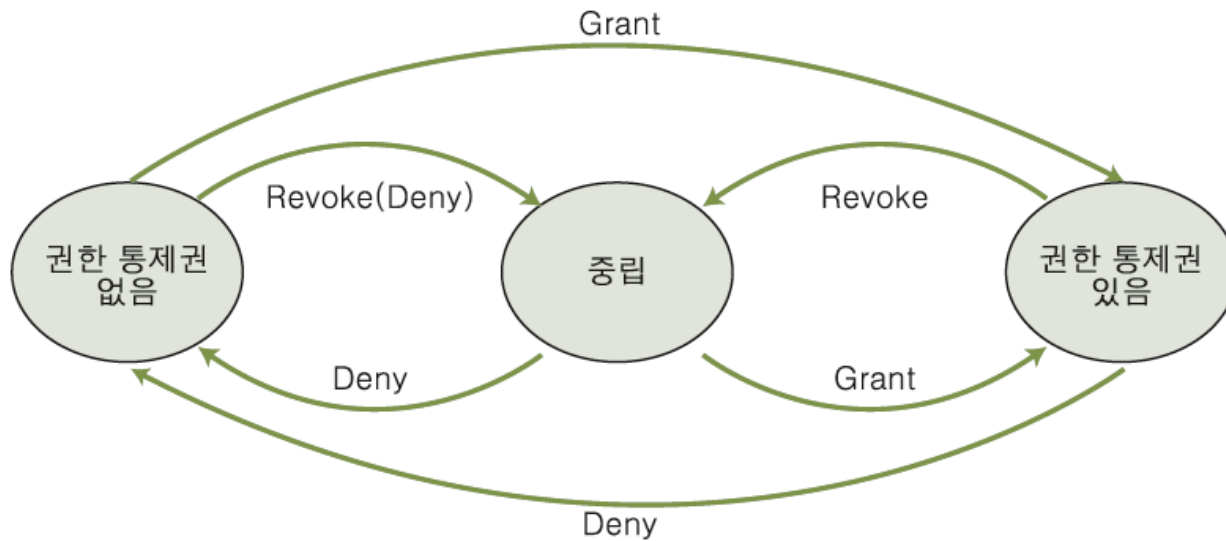
• DCL

- DCL(Data Control Language)은 권한 관리를 위한 질의문.
 - GRANT : 데이터베이스 객체에 권한을 부여한다.
 - DENY : 사용자에게 해당 권한을 금지한다.
 - REVOKE : 이미 부여된 데이터베이스 객체의 권한을 취소한다.

05 권한 관리

■ 데이터베이스의 권한 관리

- 질의문에 대한 권한 관리
 - DDL과 DML은 DCL에 의해 허용(Grant) 또는 거부(Deny)된다.

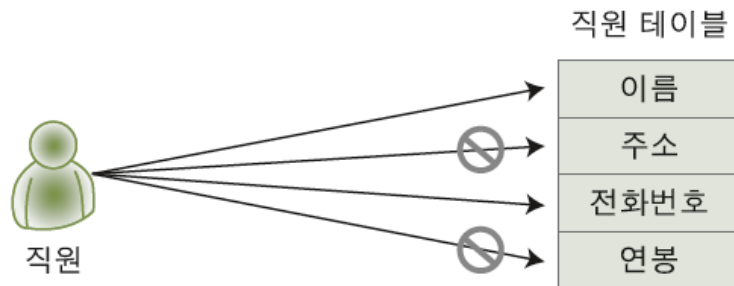


[그림 15] DCL 명령에 의한 권한 부여 구조

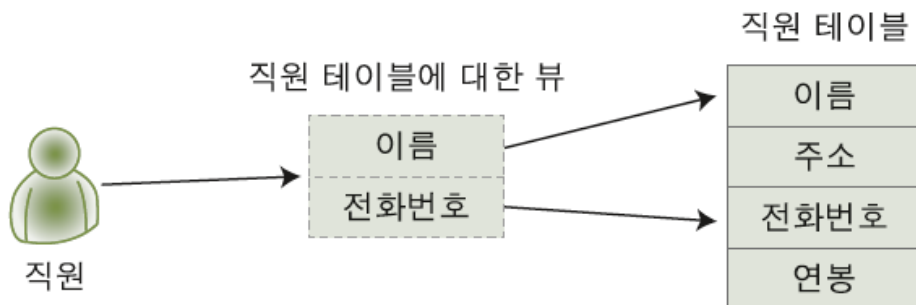
05 권한 관리

■ 데이터베이스의 권한 관리

- 뷰에 대한 권한 관리
 - 뷰는 각 사용자에게 대해 참조 테이블의 각 열에 대한 권한을 설정하는 것이 불편해서 만든 가상 테이블



[그림 16] 뷰를 사용하지 않는 테이블에 대한 접근 제어



[그림 17] 뷰를 사용한 테이블에 대한 접근 제어

05 권한 관리

■ 응용 프로그램의 권한 관리

- 응용 프로그램은 응용 프로그램 내의 권한보다 **응용 프로그램 자체의 실행 권한이 더 중요함.**
- 응용 프로그램은 자신을 실행한 계정의 권한을 물려받음
- 응용 프로그램이 보안상에 문제가 있는 취약한 프로그램일 때 해당 프로그램을 실행한 계정의 권한이 악용되는 문제가 발생
 - 윈도우의 IIS에서는 그 실행 프로세스 권한을 별도로 만들어 사용
 - 유닉스에서는 nobody와 같이 제한된 계정 권한을 사용

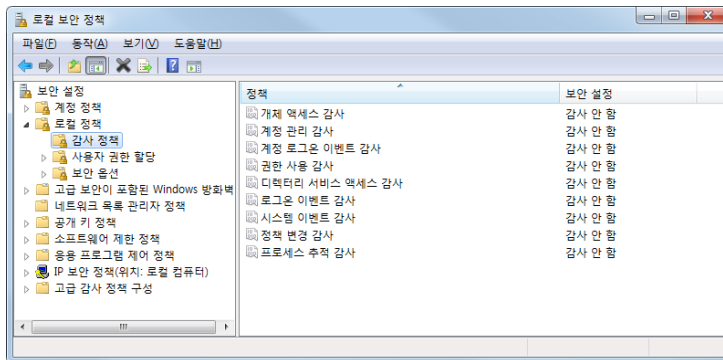
06 로그 관리

■ AAA

- **Authentication(인증)** : 자신의 신원(Identity)을 시스템에 증명하는 과정으로, 아이디와 패스워드를 입력하는 과정
- **Authorization(인가)** : 올바른 지문을 입력하거나 올바른 패스워드를 입력해 시스템에 로그인인 허락된 사용자라고 판명되어 로그인되는 과정
- **Accounting(계정관리)** : 시스템에 로그인한 후 시스템이 이에 대한 기록을 남기는 활동

■ 운영체제의 로그 관리

- 윈도우의 로그
 - 윈도우는 이벤트(Event)라고 불리는 중앙 집중화된 형태로 로그를 수집하여 저장
 - 윈도우에서 로깅 항목과 설정 사항은 [제어판]-[관리 도구]-[로컬 보안 정책]의 [로컬 정책]-[감사 정책] 메뉴에서 확인할 수 있음.



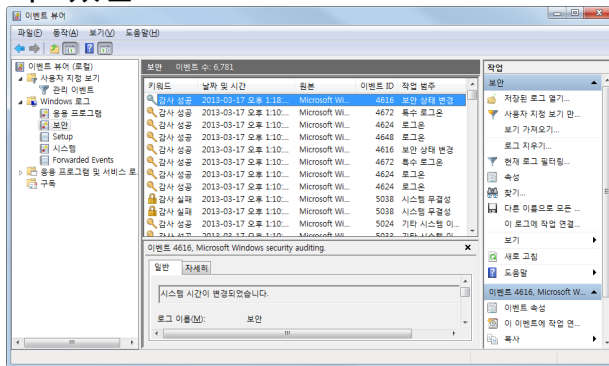
[그림 18] 로컬 정책 중 감사 정책에 대한 설정

06 로그 관리

■ 운영체제의 로그 관리

■ 윈도우의 로그

- 로깅 정책을 적용하면 [제어판]-[관리 도구]-[이벤트 뷰어]를 통해 쌓이는 로깅 정보를 확인할 수 있음



[그림 19] 이벤트 뷰어를 이용한 보안 로그 확인

[표 3] 이벤트 뷰어에 표시되는 내용

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

06 로그 관리

■ 운영체제의 로그 관리

■ 윈도우의 로그

[표 4] 윈도우의 로그 종류

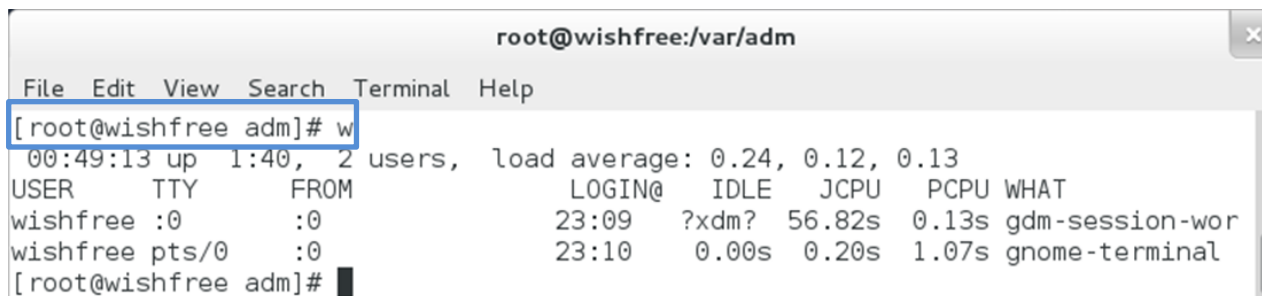
종류	설명
개체 액세스 감사	특정 파일이나 디렉터리, 레지스트리 키, 프린터 등과 같은 객체에 대하여 접근을 시도하거나 속성 변경 등을 탐지한다.
계정 관리 감사	신규 사용자, 그룹의 추가, 기존 사용자 그룹의 변경, 사용자의 활성화나 비활성화, 계정 패스워드 변경 등을 감사한다.
계정 로그인 이벤트 감사	로그온 이벤트 감사와 마찬가지로 계정의 로그인에 대한 사항을 로그로 남기는데 이들의 차이점은 전자는 도메인 계정의 사용으로 생성되는 것이며, 후자는 로컬 계정의 사용으로 생성되는 것이다.
권한 사용 감사	권한 설정 변경이나 관리자 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 또는 신뢰 정책의 변경과 관련된 사항을 로깅한다.
프로세스 추적 감사	사용자 또는 응용 프로그램이 프로세스를 시작하거나 중지할 때 해당 이벤트가 발생한다.
시스템 이벤트	시스템의 시동과 종료, 보안 로그 삭제 등 시스템의 주요한 사항에 대한 이벤트를 남긴다.

06 로그 관리

■ 운영체제의 로그 관리

■ 유닉스의 로그

- 리눅스(유닉스) 시스템은 윈도우와 달리 일반적으로 중앙 집중화되어 관리되지 않고, 분산되어 생성.
 - /usr/adm : (초기 유닉스) HP-UX 9.X, SunOS 4.x
 - /var/adm : (최근 유닉스) 솔라리스, HP-UX 10.x 이후, IBM AIX
 - /var/log : FreeBSD, 솔라리스(/var/adm 와 나누어 저장), 리눅스
 - /var/run : 일부 리눅스
- UTMP
 - 유닉스 시스템의 가장 기본적인 로그
 - 로그인 계정 이름, 로그인한 환경(initab id), 로그인한 디바이스(console, tty 등), 로그인한 셸의 프로세스 ID, 로그인한 계정의 형식, 로그오프 여부, 시간에 대한 저장 구조(structure)를 확인할 수 있음.
 - utmp는 텍스트가 아닌 바이너리 형태로 로그가 저장됨.



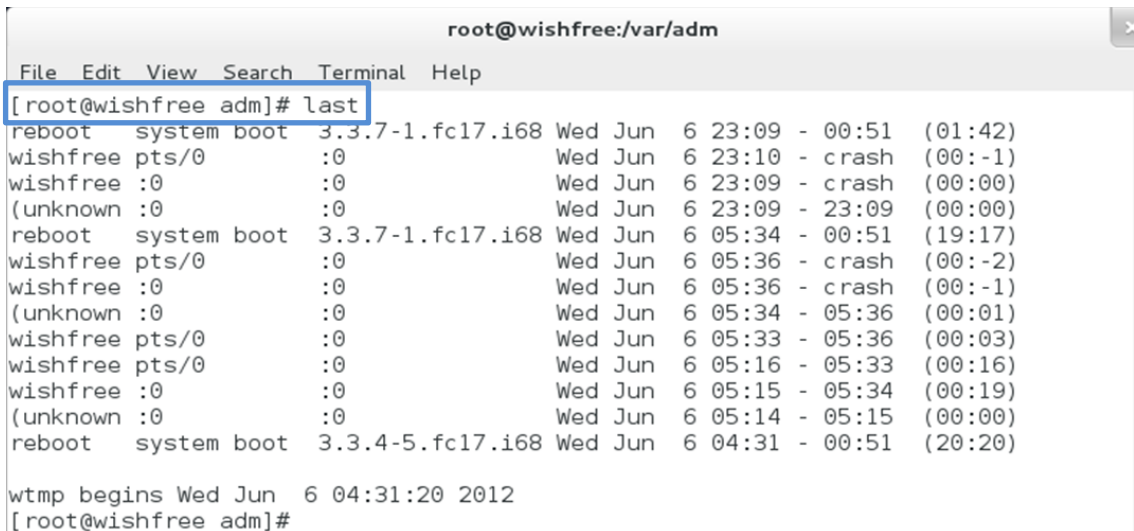
```
root@wishfree:/var/adm
File Edit View Search Terminal Help
[root@wishfree adm]# w
00:49:13 up 1:40, 2 users, load average: 0.24, 0.12, 0.13
USER      TTY      FROM          LOGIN@  IDLE   JCPU   PCPU WHAT
wishfree  :0        :0            23:09   ?xdm?  56.82s  0.13s gdm-session-wor
wishfree pts/0      :0            23:10   0.00s  0.20s  1.07s gnome-terminal
[root@wishfree adm]#
```

[그림 22] w 명령 실행 결과

06 로그 관리

■ 운영체제의 로그 관리

- WTMP
 - utmp 데몬과 비슷하게 사용자들의 로그인, 로그아웃, 시스템의 재부팅에 대한 정보를 담고 있음.
 - last 명령을 이용하여 내용을 확인할 수 있다.



```
root@wishfree:/var/adm
File Edit View Search Terminal Help
[root@wishfree adm]# last
reboot system boot 3.3.7-1.fc17.i68 Wed Jun 6 23:09 - 00:51 (01:42)
wishfree pts/0 :0 Wed Jun 6 23:10 - crash (00:-1)
wishfree :0 :0 Wed Jun 6 23:09 - crash (00:00)
(unknown :0 :0 Wed Jun 6 23:09 - 23:09 (00:00)
reboot system boot 3.3.7-1.fc17.i68 Wed Jun 6 05:34 - 00:51 (19:17)
wishfree pts/0 :0 Wed Jun 6 05:36 - crash (00:-2)
wishfree :0 :0 Wed Jun 6 05:36 - crash (00:-1)
(unknown :0 :0 Wed Jun 6 05:34 - 05:36 (00:01)
wishfree pts/0 :0 Wed Jun 6 05:33 - 05:36 (00:03)
wishfree pts/0 :0 Wed Jun 6 05:16 - 05:33 (00:16)
wishfree :0 :0 Wed Jun 6 05:15 - 05:34 (00:19)
(unknown :0 :0 Wed Jun 6 05:14 - 05:15 (00:00)
reboot system boot 3.3.4-5.fc17.i68 Wed Jun 6 04:31 - 00:51 (20:20)


wtmp begins Wed Jun 6 04:31:20 2012
[root@wishfree adm]#
```

[그림 23] last 명령 실행 결과

06 로그 관리

■ 운영체제의 로그 관리

- Secure
 - 페도라와 CentOS, 레드햇 등의 리눅스는 secure 파일에 원격지 접속 로그와 su(switch user) 및 사용자 생성 등의 보안과 직접적으로 연관된 로그가 저장됨.



```
root@wishfree:/var/log
File Edit View Search Terminal Help
[root@wishfree log]#
[root@wishfree log]# cat secure
Jun  6 05:14:58 wishfree gdm-welcome[847]: pam_unix(gdm-welcome:session): session opened for user gdm by (uid=0)
Jun  6 05:15:05 wishfree polkitd(authority=local): Registered Authentication Agent for unix-session:2 (system bus name :1.34 [gnome-shell --gdm-mode], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
Jun  6 05:15:13 wishfree gdm-password[941]: pam_unix(gdm-password:session): session opened for user wishfree by (unknown)(uid=0)
Jun  6 05:15:13 wishfree gdm-welcome[847]: pam_unix(gdm-welcome:session): session closed for user gdm
Jun  6 05:15:13 wishfree polkitd(authority=local): Unregistered Authentication Agent for unix-session:2 (system bus name :1.34, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)
Jun  6 05:15:19 wishfree polkitd(authority=local): Registered Authentication Agent for unix-session:3 (system bus name :1.61 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)
```

[그림 24] /var/adm/sulog 파일의 내용

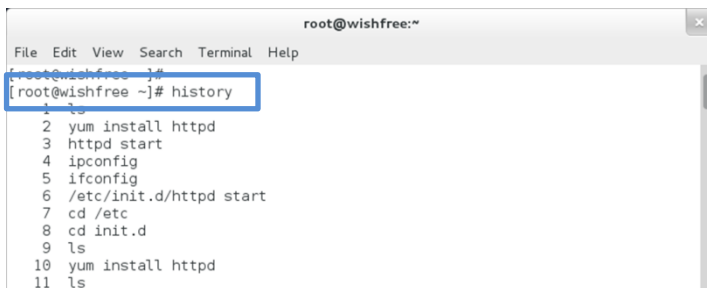
- 일반 유닉스에서 su 로그는 /var/adm/sulog 파일에 텍스트 형식으로 남음.

[날짜] [시간] [+ (성공) or - (실패)] [터미널 종류] [권한 변경 전 계정 - 변경 후 계정]

06 로그 관리

■ 운영체제의 로그 관리

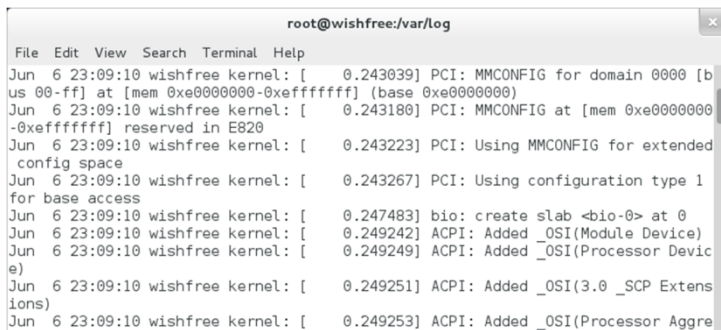
- History
 - 명령창에서 실행했던 명령에 대한 기록은 history 명령으로 확인할 수 있음.



```
root@wishfree:~  
[root@wishfree ~]# history  
1  ls  
2  yum install httpd  
3  httpd start  
4  ipconfig  
5  ifconfig  
6  /etc/init.d/httpd start  
7  cd /etc  
8  cd init.d  
9  ls  
10 yum install httpd  
11 ls
```

[그림 25] history 명령 실행 결과

- Syslog
 - 시스템의 운영과 관련한 전반적인 로그
 - /var/log/messages 파일에 하드웨어의 구동, 서비스의 동작과 에러 등 다양한 로그를 남김



```
root@wishfree:/var/log  
Jun  6 23:09:10 wishfree kernel: [ 0.243039] PCI: MMCONFIG for domain 0000 [bus 00-ff] at [mem 0xe0000000-0xffffffff] (base 0xe0000000)  
Jun  6 23:09:10 wishfree kernel: [ 0.243180] PCI: MMCONFIG at [mem 0xe0000000-0xffffffff] reserved in E820  
Jun  6 23:09:10 wishfree kernel: [ 0.243223] PCI: Using MMCONFIG for extended config space  
Jun  6 23:09:10 wishfree kernel: [ 0.243267] PCI: Using configuration type 1 for base access  
Jun  6 23:09:10 wishfree kernel: [ 0.247483] bio: create slab <bio-0> at 0  
Jun  6 23:09:10 wishfree kernel: [ 0.249242] ACPI: Added _OSI(Module Device)  
Jun  6 23:09:10 wishfree kernel: [ 0.249249] ACPI: Added _OSI(Processor Device)  
Jun  6 23:09:10 wishfree kernel: [ 0.249251] ACPI: Added _OSI(3.0 _SCP Extensions)  
Jun  6 23:09:10 wishfree kernel: [ 0.249253] ACPI: Added _OSI(Processor Aggre
```

[그림 26] syslog의 내용

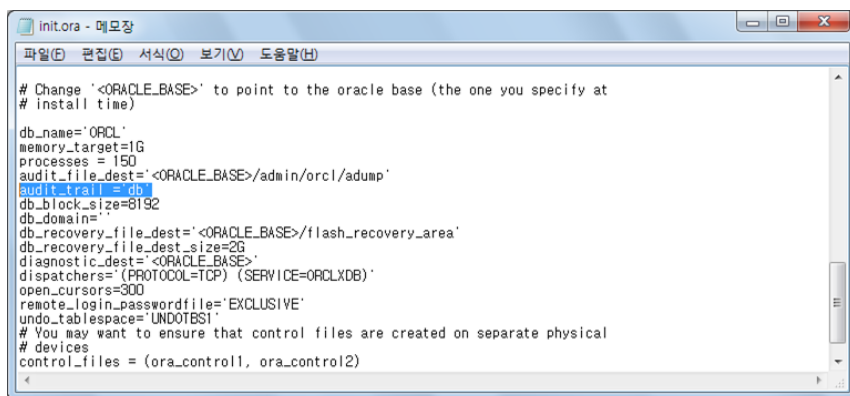
- C2 감사 추적은 데이터베이스가 생성.삭제.변경되는지에 대한 자세한 정보를 로그로 남기는 것.
- 빈번한 접속이 있는 데이터베이스의 경우 대량의 로그를 생성할 수 있음.

06 로그 관리

■ 데이터베이스의 로그 관리

■ 오라클의 로그

- 오라클에서 감사 로그를 활성화시키려면 먼저 오라클 파라미터 파일 (\$ORACLE_HOME/dbs/init.ora)의 AUDIT_TRAIL 값을 'DB' 또는 'TRUE' 값으로 지정해야 함.



[그림 28] 오라클 감사 로그 설정

[표 5] AUDIT_TRAIL 설정 값

AUDIT_TRAIL 값	AUDIT_TRAIL 내용
NONE 또는 FALSE	데이터베이스 감사를 비활성화시킴
DB 또는 TRUE	데이터베이스 감사를 활성화시킴
OS	감사 로그를 OS상의 파일로 저장 이때 경로명은 audit_file_dest에 의해 지정

06 로그 관리

■ 데이터베이스의 로그 관리

■ 오라클의 로그

- AUDIT_TRAIL 값을 지정한 후에는 '\$ORACLE_HOME\wrdbs\admin\cataudit.sql'를 실행시킴.
- 감사 로그가 활성화된 후 오라클에서 남길 수 있는 데이터베이스 감사의 종류는 문장 감사, 권한 감사, 객체 감사가 있음.
 - 문장 감사 (statement auditing) : 지정된 문장을 실행시켰을 경우 기록을 남김.
 - 권한 감사 (privilege auditing) : 특정한 권한을 사용했을 때 기록을 남김.
 - 객체 감사 (object auditing) : 특정한 객체에 대한 작업을 했을 경우 기록을 남김.

[표 6] 주요 오라클 감사 뷰

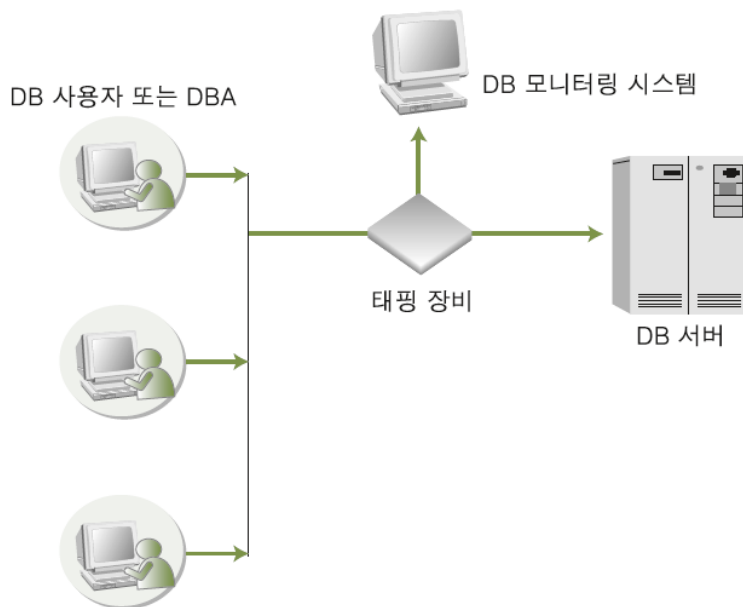
뷰	설명
dba_stmt_audit_opts	문장 감사의 옵션 확인
dba_priv_audit_opts	권한 감사의 옵션 확인
dba_obj_audit_opts	객체 감사의 옵션 확인
dba_audit_trail	데이터베이스의 모든 감사 로그를 출력
user_audit_trail	데이터베이스에 저장된 현재 사용자의 감사기록 조회
dba_audit_object	데이터베이스의 객체와 관련된 모든 감사 로그를 출력
user_audit_object	현재 사용자의 객체와 관련된 모든 감사 로그를 출력
dba_audit_session	사용자의 로그인 로그오프에 대한 감사 로그를 출력
dba_audit_statement	문장 감사 로그를 출력
dba_audit_object	객체 감사 로그를 출력

06 로그 관리

■ 데이터베이스의 로그 관리

■ 데이터베이스 모니터링

- 데이터베이스에 대한 로그를 남기는 가장 좋은 방법은 별도의 데이터베이스 모니터링 툴을 도입하는 것
- 네트워크에 네트워크 트래픽을 모니터링할 수 있는 태핑(Tapping) 장비를 설치하고, 네트워크 패킷 중 데이터베이스 질의문을 확인하여 이를 로그로 남김.



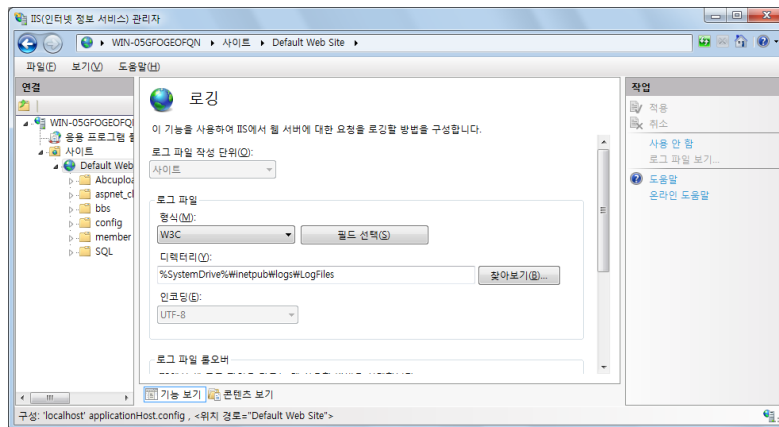
[그림 29] 모니터링 툴을 이용한 데이터베이스 로그 생성과 보존

06 로그 관리

■ 응용 프로그램의 로그 관리

■ IIS 웹 서버의 로그

- IIS(Internet Information Services) 웹 서버의 로그는 [제어판]-[관리 도구]-[IIS(인터넷 정보 서비스) 관리자]-[IIS] 창에서 '로깅' 항목을 통해 확인할 수 있음.



[그림 30] IIS 웹 서버 로깅 설정

- IIS 웹 서버에서 로그는 기본 W3C 형식으로 남도록 설정되어 있음.
- W3C 형식 이외에도 다음의 로그 파일 형식을 사용할 수 있음.
 - NCSA
 - IIS
 - 사용자 지정 방식

06 로그 관리

■ 응용 프로그램의 로그 관리

- IIS 웹 서버의 로그인
 - W3C 로그 형태

```
2012-06-03 08:53:12 192.168.137.128 GET
/XSS/GetCookie.asp?cookie=ASPSESSIONIDQQCAQDDA 80 – 192.168.137.1
Mozilla/5.0+(compatible;+MSIE+9.0;+Windows+NT+6.1;) 200 0 0 225
```

- 날짜와 시간 : 2012-06-03 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 데이터 크기 : 0
- 클라이언트에서 서버로 전송한 데이터의 크기 : 0
- 처리 소요 시간 : 225 밀리세컨드

06 로그 관리

■ 응용 프로그램의 로그 관리

- 아파치 웹 서버의 로그
 - 아파치 웹 서버에 대한 기본 접근 로그는 access_log에 남으며, 형식은 'combined'로 지정됨.

[표 7] Combined 형식 로그에 사용되는 인수

인자	내용	인자	내용
%a	클라이언트의 IP 주소	%A	서버 IP 주소
%b	헤더 정보를 제외하고서 전송된 데이터의 크기, 전송된 데이터의 크기가 0일 때 '-'로 표시	%c	응답이 완료되었을 때의 연결 상태 • X : 응답이 완료되기 전에 연결이 끊김 • + : 응답이 보내진 후에도 연결이 지속됨 • - : 응답이 보내진 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 ID
%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		

06 로그 관리

■ 응용 프로그램의 로그 관리

- 아파치 웹 서버의 로그
 - access_log 형태.

```
192.168.137.1 - - [06/JUN/2012:05:48:28 +0900] "GET / HTTP/1.1" 403 4609 "-"  
"Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0)"
```

- 클라이언트 IP(%h) : 192.168.137.1
- 클라이언트 로그인명(%l) : -
- 클라이언트 사용자명(%u) : -
- 날짜와 시간(%t) : [06/JUN/2012:05:48:28 +0900]
- HTTP 접근 방법과 접근 URL(%r) : GET / HTTP/1.1
- 실행 결과 코드(%s) : 403 Forbidden
- 서버에서 클라이언트로 전송한 데이터 크기(%b) : 4609 바이트
- 클라이언트의 웹 브라우저(%i) : Mozilla/5.0 (compatible; MSIE 9.0; Windows...

06 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 **통합로그관리시스템(SIEM, Security Information and Event Management)**에 의해 수집되고 관리되기도 함.

■ 네트워크 관리 시스템의 로그

- 네트워크 트래픽 모니터링 시스템(MRTG)과 네트워크 관리 시스템(NMS)의 로그를 참고할 수 있음.

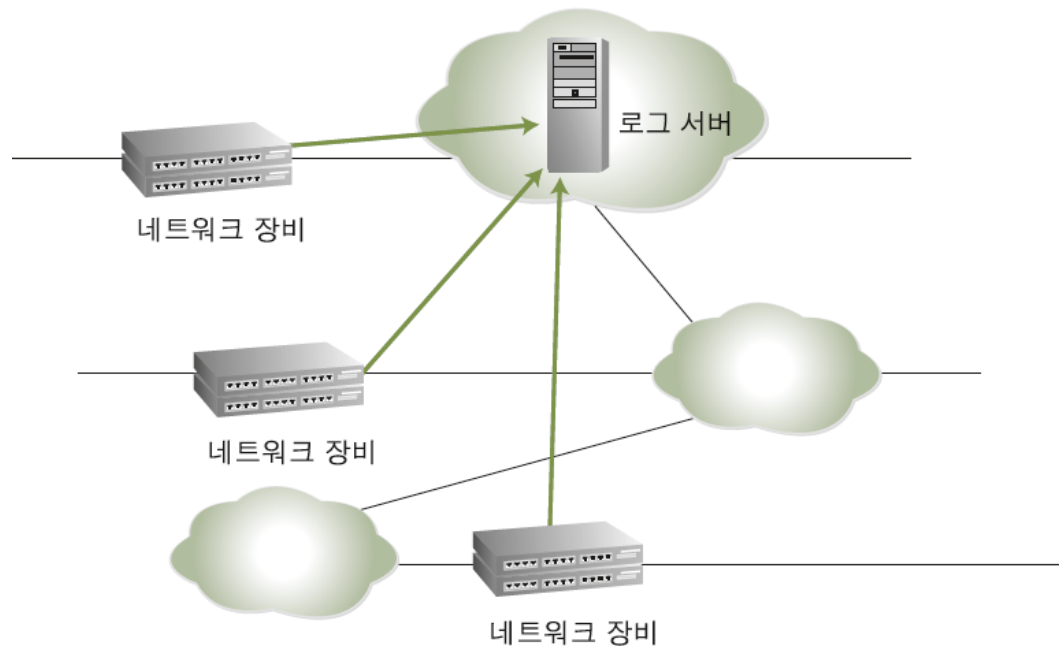
■ 네트워크 장비 인증 시스템의 로그

- 대규모 네트워크를 운영하는 곳에서는 라우터나 스위치의 인증을 일원화하기 위해 인증 서버로 TACACS+(Terminal Access Controller Access-Control System Plus)를 사용하기도 함.
 - 이 인증 서버를 통해서 네트워크 장비에 대한 인증 시도 및 로그인 정보 등을 확인할 수 있음.

06 로그 관리

■ 네트워크 장비의 로그 관리

- 라우터나 스위치는 자체적으로 로그를 남기는 저장공간이 없음. 각 네트워크 장비에서 생성되는 로그를 네트워크를 통해 **로그 서버에 전송**.
- 해커가 어떤 네트워크 장비에 침투하더라도 자신의 흔적을 지우기가 쉽지 않음.

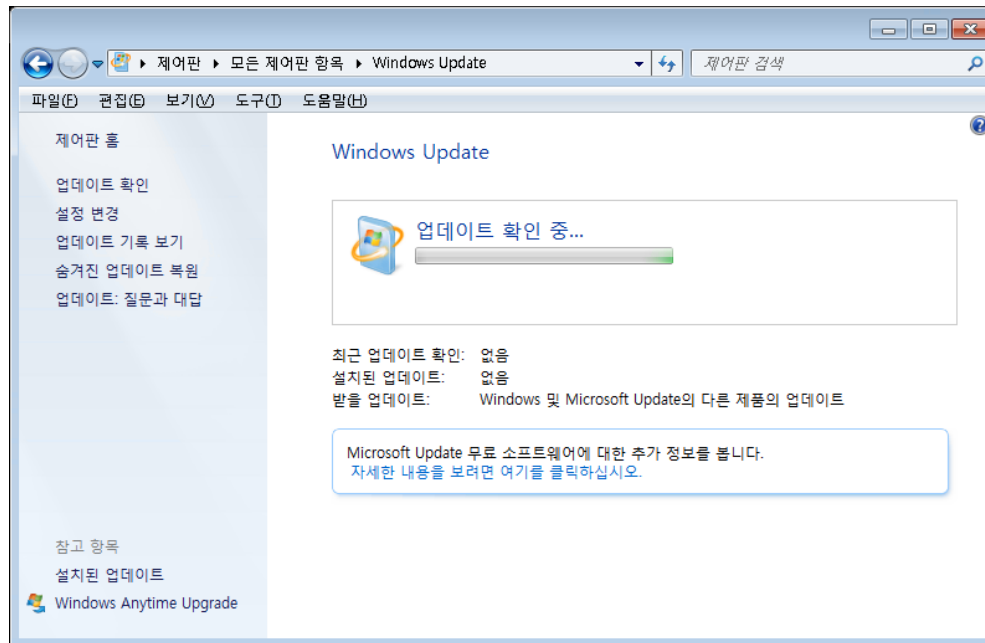


[그림 33] 네트워크 장비의 로그 생성과 보존

07 취약점 관리

■ 패치 관리

- 윈도우 업데이트를 통해 자동으로 보안 패치를 확인하고, 패치를 적용할 수 있다.

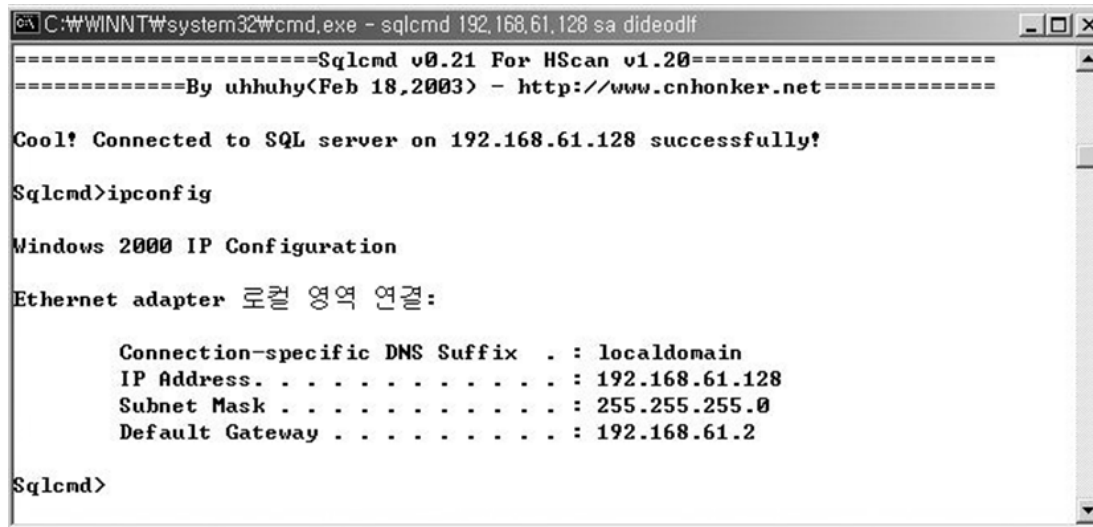


[그림 34] 윈도우 업데이트 항목 확인

07 취약점 관리

■ 응용 프로그램별 고유 위험 관리

- 응용 프로그램 중에는 해당 응용 프로그램을 통해 운영체제의 파일이나 명령을 실행시킬 수 있는 것이 있음.
- MS-SQL의 xp_cmdshell은 데이터베이스를 통해 운영체제의 명령을 실행하고, 파일 등에 접근할 수 있음.
- 응용 프로그램의 동작과 관련하여 운영체제에 접근할 수 있는 함수나 기능이 있으면 그 적절성을 검토해야 함.



```
C:\WINNT\system32\cmd.exe - sqlcmd 192.168.61.128 sa dideodlf

=====Sqlcmd v0.21 For HScan v1.20=====
=====By uhhuhy(Feb 18,2003) - http://www.cnhonker.net=====

Cool! Connected to SQL server on 192.168.61.128 successfully!

Sqlcmd>ipconfig

Windows 2000 IP Configuration

Ethernet adapter 로컬 영역 연결:

    Connection-specific DNS Suffix  . : localdomain
    IP Address. . . . .               : 192.168.61.128
    Subnet Mask . . . . .             : 255.255.255.0
    Default Gateway . . . . .         : 192.168.61.2

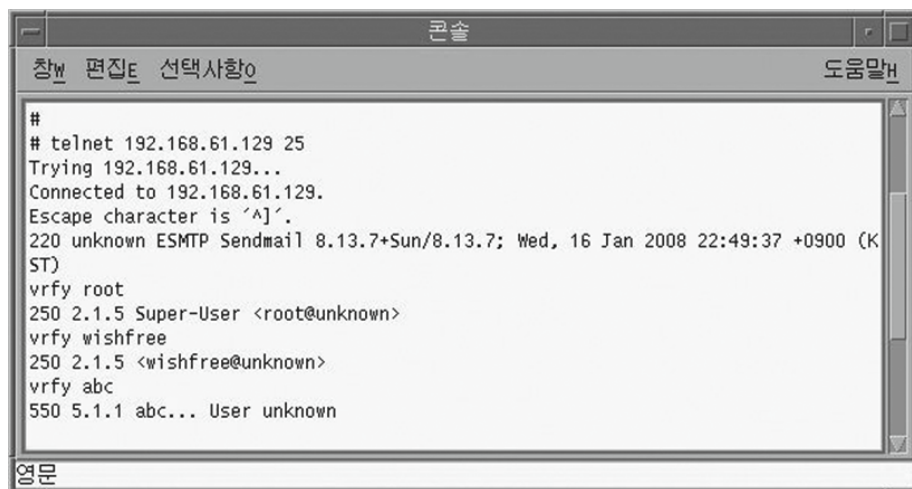
Sqlcmd>
```

[그림 35] MS-SQL 2000에서 xp_cmdshell 툴을 이용한 명령창 획득

07 취약점 관리

■ 응용 프로그램을 통한 정보 수집 제한

- 응용 프로그램이 운영체제에 직접적인 영향을 미치지 않아도 응용 프로그램의 특정 기능이 운영체제의 정보를 노출시키기도 함.
- 유닉스에서는 이메일을 보낼 때, 수신자가 있는 시스템의 sendmail 데몬에 해당 계정이 존재하는지 확인하기 위해 일반 계정은 vrfy(verify) 명령을, 그룹은 expn(expansion) 명령을 시스템 내부적으로 사용. 일반 사용자는 다음과 같이 Telnet을 이용해 시스템에 존재하는 계정의 목록을 어느 정도 파악할 수 있음.
- 이러한 응용 프로그램의 기능은 제한하는 것이 바람직함.



```
#
# telnet 192.168.61.129 25
Trying 192.168.61.129...
Connected to 192.168.61.129.
Escape character is '^]'.
220 unknown ESMTS Sendmail 8.13.7+Sun/8.13.7; Wed, 16 Jan 2008 22:49:37 +0900 (KST)
vrfy root
250 2.1.5 Super-User <root@unknown>
vrfy wishfree
250 2.1.5 <wishfree@unknown>
vrfy abc
550 5.1.1 abc... User unknown
```

[그림 36] sendmail 데몬에 접속하여 vrfy 명령을 실행한 결과

Q&A