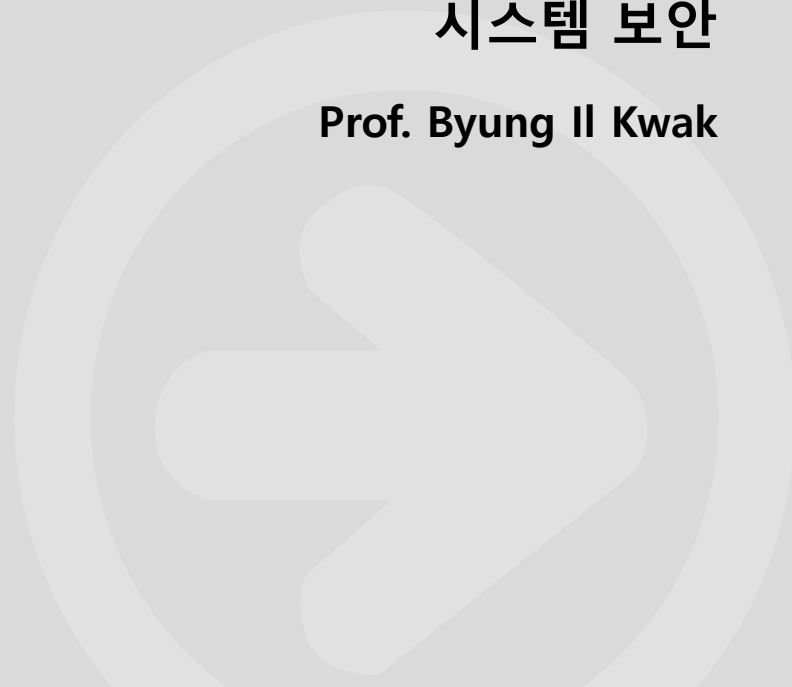




정보보호론 #6

시스템 보안

Prof. Byung Il Kwak



- 네트워크의 이해
- 서비스 거부 공격: DoS와 DDoS
- 스니핑 공격
- 스푸핑 공격
- 세션 하이재킹 공격
- 무선 네트워크 공격과 보안
- TLS
- IPSec

- 시스템 보안의 이해
- 계정 관리
- 세션 관리
- 접근 제어
- 권한 관리
- 로그 관리
- 취약점 관리

CONTENTS

▣ 시스템 보안의 이해

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



클라우드 환경에서의 시스템

정보 보안의 역사

▣ 시스템 보안 주제

▣ 계정 관리

- 사용자를 식별하는 가장 기본적인 인증 수단은 아이디와 패스워드이며, 이를 통한 계정 관리는 시스템 보안의 시작이라 할 수 있음

▣ 세션 관리

- 일정 시간에 대한 세션 종료와 비인가자의 세션 가로채기를 통제하는 것

▣ 접근 제어

- 네트워크 안에서 시스템을 외부로부터 적절히 보호할 수 있도록 접근을 통제하는 것

▣ 권한 관리

- 시스템의 각 사용자가 적절한 권한으로 적절하게 정보 자산에 접근하도록 통제하는 것

▣ 로그 관리

- 시스템에 영향을 미치는 경우, 그 내용을 기록하여 관리하는 것

▣ 취약점 관리

- 시스템 자체의 결함을 체계적으로 관리하는 것

CONTENTS

□ 계정 관리

□ 계정관리

▣ 식별과 인증

- 식별: 어떤 시스템에 로그인하려면 먼저 자신이 누구인지를 알림
- 인증: 로그인을 허용하기 위한 확인

▣ 보안의 인증 방법

- 알고 있는 것
 - 머릿속에 기억하고 있는 정보를 이용하여 인증 수행
- 가지고 있는 것
 - 신분증(ID card)이나 OTP (One Time Password) 장치 등으로 인증 수행
- 자신의 모습
 - 홍채와 같은 생체 정보(Biometric)로 인증 수행
- 위치하는 곳
 - 현재 접속을 시도하는 위치의 적절성을 확인 or 콜백을 사용해 인증 수행
 - 콜백(Callback): 접속을 요청한 사람의 신원을 확인
 - 예) 미리 등록된 전화번호로 연락하여 접속 요청한 본인을 확인

□ 운영체제의 계정 관리

▣ 운영체제

- 시스템 구성 및 운영을 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** 뿐만 아니라 **일반 사용자 권한이 있는 계정**도 적절하게 **적절한 제한**이 필요



Linux



□ 운영체제의 계정 관리

▣ 운영체제

- 윈도우의 계정 관리

그룹	특징
Administrators	<ul style="list-style-type: none">• 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	<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 구성 요소에 로그인할 수 있다.• 관리 계정에 비해 한정된 권한을 가지고 있다.
Guests	<ul style="list-style-type: none">• 윈도우 시스템에서 Users 그룹과 같은 권한을 가지고 있다.• 두 그룹 모두 네트워크를 통해 서버에 로그인할 수 있으며 서버로의 로컬 로그인도 금지된다.

윈도우의 주요 그룹

□ 운영체제의 계정 관리

▣ 운영체제

- 윈도우의 계정 관리

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



```
선택 명령 프롬프트
C:\Users\Administrator>net localgroup

SC-201612101701에 대한 별칭
-----
* _vmware_
* Access Control Assistance Operators
* Administrators
* Backup Operators
* Cryptographic Operators
* Distributed COM Users
* Event Log Readers
* Guests
* Hyper-V Administrators
* IIS_IUSRS
* Network Configuration Operators
* Performance Log Users
* Performance Monitor Users
* Power Users
* Remote Desktop Users
* Remote Management Users
* Replicator
* System Managed Accounts Group
* Users
명령을 잘 실행했습니다.

C:\Users\Administrator>
```

윈도우에서 그룹 목록 확인

□ 운영체제의 계정 관리

▣ 윈도우의 계정 관리

- 관리자 계정: 'administrator'(시스템에 기본으로 설치되는 계정)
- 윈도우 CMD 창에서 '> net localgroup administrators' 명령으로 관리자 그룹 계정의 존재를 확인할 수 있음



```
C:\Users\Administrator> net localgroup administrators
명칭      administrators
설명      컴퓨터 도메인에 모든 액세스 권한을 가진 관리자입니다.

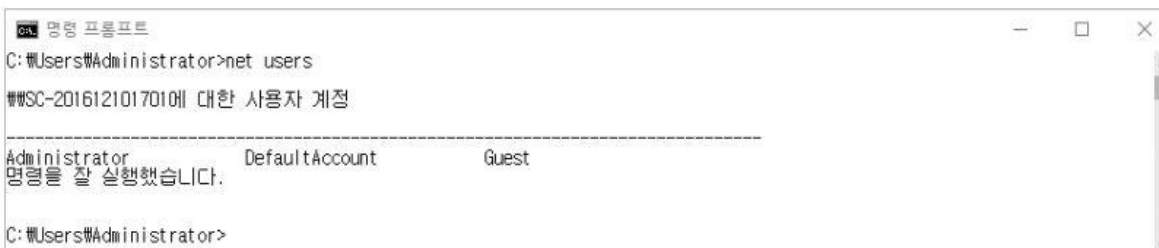
구성원

-----
Administrator
명령을 잘 실행했습니다.

C:\Users\Administrator>
```

윈도우에서 관리자 그룹에 속한 계정 목록 확인

- 사용자 계정을 모두 확인하려면 net users 명령을 사용



```
C:\Users\Administrator> net users

##SC-201612101701에 대한 사용자 계정

-----
Administrator      DefaultAccount      Guest
명령을 잘 실행했습니다.

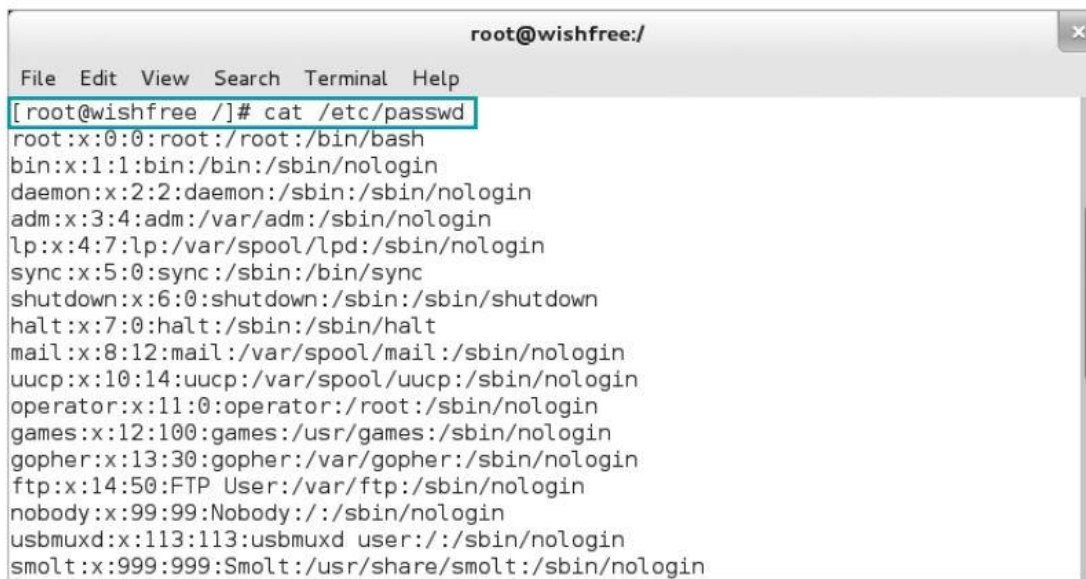
C:\Users\Administrator>
```

윈도우에서 일반 사용자 계정 확인

계정 관리

□ 운영체제의 계정 관리

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



```
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
```

유닉스의 /etc/passwd 파일 열람

계정 관리

□ 운영체제의 계정 관리

▣ /etc/passwd 파일의 구성

```
root : x : 0 : 0 : root : /root : /bin/bash
```

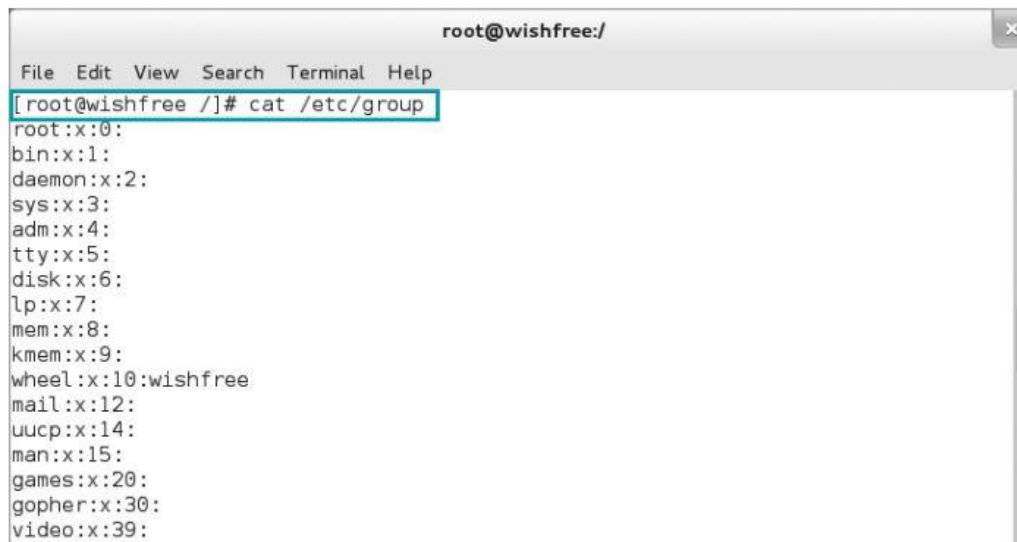
① ② ③ ④ ⑤ ⑥ ⑦

- ① 사용자 계정
- ② 패스워드가 암호화되어 shadow 파일에 저장되어 있음을 나타냄
- ③ 사용자 번호
- ④ 그룹 번호
- ⑤ 실제 이름
 - 시스템 설정에 영향을 주지 않으며 자신의 이름을 입력해도 됨
- ⑥ 사용자의 홈 디렉터리 설정.
 - 위의 예에서는 관리자 계정(root)을 나타냄.
 - 홈 디렉터리가 '/root' 이며, 일반 사용자는 '/home/wishfree'와 같이 '/home' 디렉터리 하위에 새롭게 구성됨
- ⑦ 사용자 셸 정의, 기본은 bash 셸이 적용됨. 사용하는 셸을 정의함

계정 관리

□ 운영체제의 계정 관리

- ▣ 유닉스에서 그룹은 '/etc/group' 파일에서 확인



```
root@wishfree:/  
File Edit View Search Terminal Help  
[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:
```

유닉스의 그룹 확인

- 그룹 번호가 0인 그룹에 해당하는 계정은 root, sync, shutdown, halt, operator
 - root 그룹에 속하는 계정

계정 관리

□ 운영체제의 계정 관리

▣ /etc/group의 내용

```
root : x : 0 : root
```

①

②

③

④

① 그룹 이름을 의미함.

- 여기서는 그룹의 이름이 'root'로 설정됨

② 그룹에 대한 패스워드를 의미함.

- 일반적으로는 사용하지 않음.

③ 그룹 번호를 의미함.

- 0은 root 그룹을 의미.

④ 해당 그룹에 속한 계정 목록.

- 이 목록은 완전하지 않으므로 패스워드 파일과 비교하여 확인 가능

❑ 데이터베이스의 계정 관리

- ❑ 데이터베이스에도 운영체제와 같이 계정이 존재
 - MS-SQL에서 관리자 계정은 **sa**, 오라클의 관리자 계정은 **sys**, **system**
 - 둘 다 관리자 계정이지만 sys와 달리 system은 데이터베이스를 생성할 수 없음

❑ 응용 프로그램의 계정 관리

- ❑ 취약한 응용 프로그램을 통해 공격자가 운영체제에 접근하여, 민감 정보를 습득한 뒤 운영체제를 공격하는 데 이용할 수 있음.
 - 습득한 민감 정보는 2차 공격을 유발할 수 있음
 - 운영체제의 관리자 권한을 얻으면, backdoor를 심어 추가적인 공격을 발생시킴

□ 네트워크 장비의 계정 관리

- ▣ 네트워크 장비는 보통 패스워드만 알면 접근이 가능
- ▣ 시스코 장비의 계정의 모드 구별 (User vs Admin)
 - User: 네트워크 장비의 상태만 확인 가능
 - Admin: 네트워크 상태 파악 및 설정 변경 가능
 - 네트워크 장비에 처음 접속할 경우
 - User mode로 로그인 되며, User mode에서 Admin mode로의 로그인은 별도 패스워드를 입력해야 함
- ▣ 네트워크 장비에서도 계정을 생성하여 각 계정으로 사용할 수 있는 명령어 집합을 제한할 수 있음
 - **TACACS+**: Cisco protocol로써, Cisco의 client와 server간의 통신을 위해 사용됨

CONTENTS

□ 세션 관리

□ 세션

▣ 세션의 개요

- 사용자와 시스템 사이 또는 **두 시스템 사이의 활성화된 접속**
- 예시) 동화 <해님 달님>의 이야기
 - 일하러 나간 어머니를 기다리던 오누이는 호랑이의 손을 확인하고 문을 열어달라고 함
 - > 오누이 입장에서 어머니의 세션이 유효한지 확인하기 위해 '손 모양'을 확인

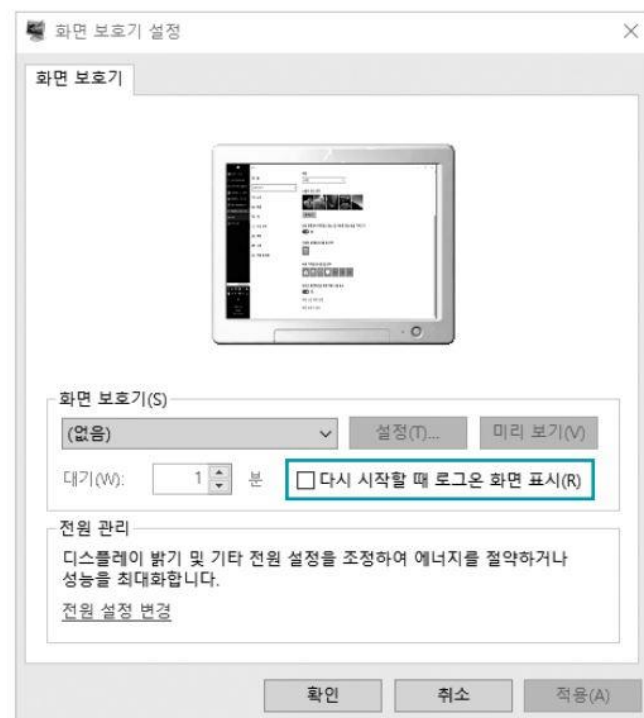


➔ 세션 관리

□ 세션

▣ 지속적인 인증

- 세션을 유지하기 위한 보안 사항 중 하나
- 인증에 성공한 후 인증된 사용자가 처음의 사용자인지 **지속적으로 재인증** 작업을 거치는 작업
- **하지만, 매번 패스워드를 입력 할 수 없음.**
시스템은 이를 세션에 대한 타임아웃 설정으로 보완 (**윈도의 화면보호기**)
- 반면 **유닉스**는 원격에서 접속할 경우 패스워드를 다시 묻지 않고 **세션을 종료한 후 재접속**을 요구
- 시스템이 아닌 웹 서비스를 이용할 때도 '지속적인 인증'이 적용



지속적인 인증 제공을 위한 윈도우의 화면 보호기 설정

CONTENTS

□ 접근 제어

□ 접근 제어

▣ 접근 제어

- **접근 제어**: 적절한 권한을 가진 **인가자만** 특정 시스템이나 정보에 **접근 가능**하게끔 통제하는 것
 - 시스템의 보안 수준을 갖추기 위한 가장 기본적인 수단
 - 시스템 네트워크 접근 제어의 기본적인 수단은 **IP와 서비스 포트**
 - 운영체제에 적절한 접근 제어를 수행하려면, 먼저 운영체제에서 다루는 실행중인 관리 인터페이스를 파악해야 함

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

일반적으로 사용되는 관리 인터페이스

□ 운영체제의 접근 제어

▣ 불필요한 인터페이스 제거

- 접근 가능한 인터페이스를 확인했다면, 불필요한 인터페이스를 제거
- 불필요한 인터페이스를 제거할 때는 사용할 인터페이스에 **보안 정책을 적용** 가능한지 **판단**이 필요함
 - 유닉스에서 많이 쓰이는 **텔넷**은 **스니핑과 세션 하이재킹 공격 등에 취약하기** 때문에 사용을 권고하지 않음
 - 접근 제어 정책은 기본적으로 IP 주소와 포트번호를 이용함
 - 불필요한 인터페이스를 사용하지 않도록, 가능하면 **SSH나 XDMCP를 사용**하는 것이 좋음 (Telnet 사용하고 있을 경우, 종료되지 않거나 에러가 발생할 수 있음)
 - 윈도우의 GUI인 터미널 서비스는 운영체제의 버전에 따라 다른 수준의 암호화를 수행하므로 이를 고려하여 적용

□ 운영체제의 접근 제어

▣ 불필요한 인터페이스 제거

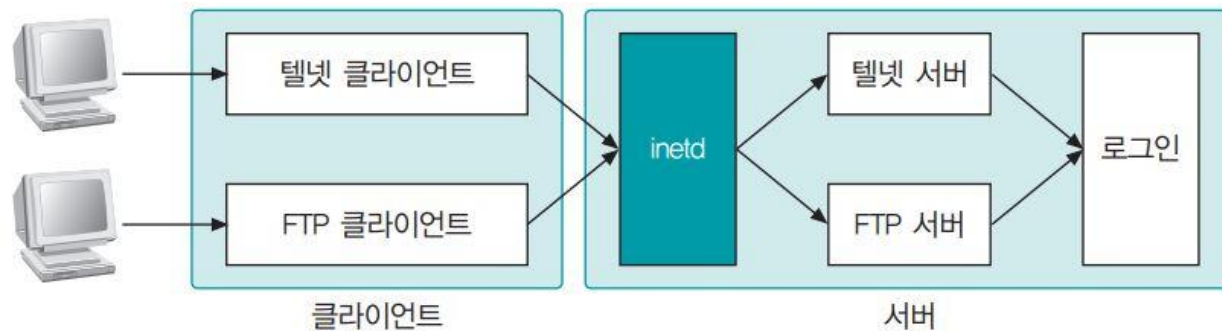
- 운영체제에 대한 접근 목적의 인터페이스를 결정한 다음에는 접근 제어 정책을 적용해야 함 (현재 내가 사용중인 인터페이스를 접근 차단 시키면 명령어 적용이 되지 않음)
- 유닉스의 텔넷이나 **SSH, FTP** 등은 TCPWrapper를 통해 접근 제어가 가능
 - TCPWrapper: FTP, Telnet, SSH 및 xinetd 기반의 서비스 관련 접근 제어(ACL) 설정을 적용하는 도구

➔ 접근 제어

□ 운영체제의 접근 제어

▣ inetd 데몬

- 클라이언트로부터 inetd가 관리하는 텔넷이나 SSH, FTP 등에 대한 연결 요청을 받음
 - 해당 데몬을 활성화하여 실제 서비스를 함으로써 데몬과 클라이언트의 요청을 연결



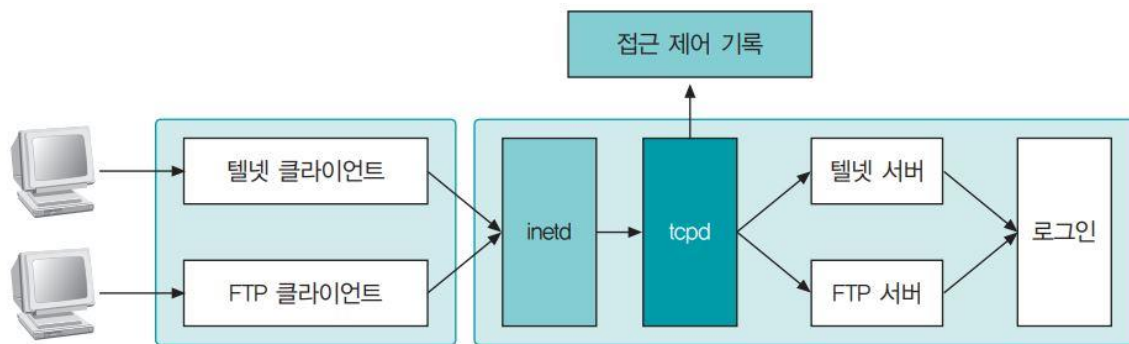
inetd 데몬을 통한 데몬의 동작

➔ 접근 제어

□ 운영체제의 접근 제어

▣ inetd 데몬

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

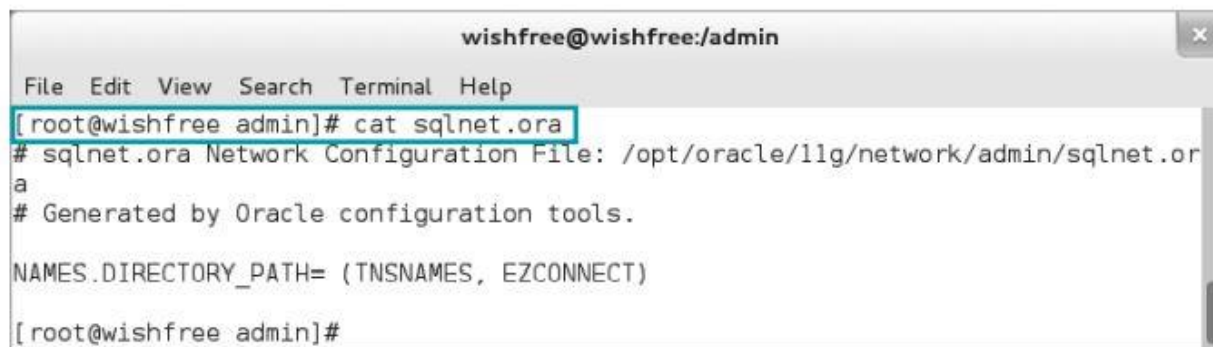


TCP Wrapper를 통한 데몬의 동작

□ 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



```
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]#
```

오라클 sqlnet.ora 파일 내용

접근 제어

□ 데이터베이스의 접근 제어

▣ 데이터베이스

- **200.200.200.100**과 **200.200.200.200**이라는 두 IP의 접근을 허용하려면 다음을 추가

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

- **200.200.200.150**의 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]
```

■ 응용 프로그램의 접근 제어

- NGINX 웹 사이트 설정 파일에서는 다음과 같이 접근 제어를 수행

```
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 ACL을 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

CONTENTS

□ 권한 관리

□ 운영체제의 권한 관리

□ 윈도우의 권한 관리

- 윈도우는 NT 4.0 이후 버전부터 NTFS를 기본 파일 시스템으로 사용
- 임의의 디렉토리를 만들고 마우스 오른쪽 버튼을 눌러 [등록정보]-[보안]을 선택하면 권한 설정 화면이 나타남

NTFS에서 그룹 또는 개별 사용자에게 설정할 수 있는 권한의 종류

- ① 모든 권한: 디렉터리 접근 권한과 소유권을 변경하고 하위 디렉터리와 파일 삭제 가능
- ② 수정: 디렉터리 삭제가 가능하며 읽기, 실행, 쓰기 권한이 주어진 것과 동일
- ③ 읽기 및 실행: 읽기 수행, 디렉터리나 파일 옮기기 가능
- ④ 디렉터리 내용 보기: 디렉터리 내의 파일, 디렉터리 이름 보기 가능
- ⑤ 읽기: 디렉터리 내용 읽기만 가능
- ⑥ 쓰기: 해당 디렉터리에 하위 디렉터리와 파일 생성, 소유권이나 접근 권한의 설정 내용 확인 가능

권한 규칙

규칙 1: 접근 권한이 누적

규칙 2: 파일 접근 권한이 디렉터리 접근 권한보다 우선

규칙 3: '허용'보다 '거부'가 우선

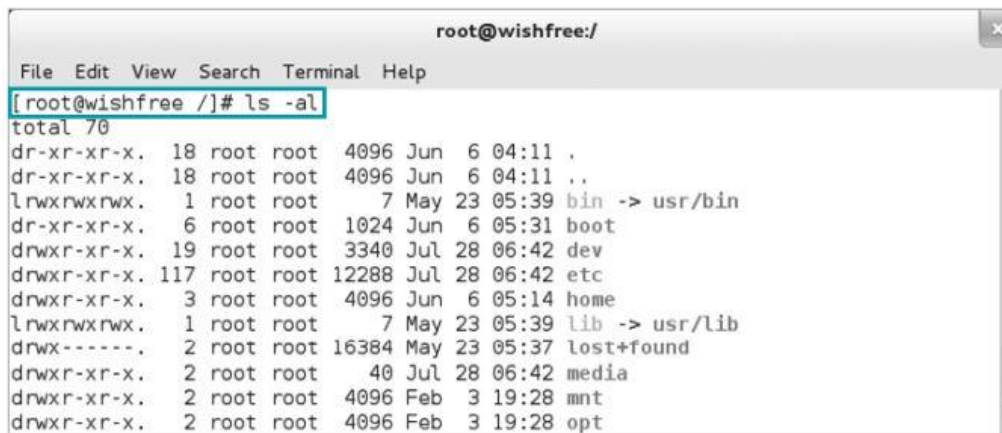
Q) 이유는??



□ 운영체제의 권한 관리

▣ 유닉스의 권한 관리

- 유닉스는 파일과 디렉터리에 대한 권한 설정방법이 같음
- 임의의 디렉터리에서 `ls -al` 명령으로 디렉터리 내용을 확인



```
root@wishfree:/  
File Edit View Search Terminal Help  
[root@wishfree /]# ls -al  
total 70  
dr-xr-xr-x. 18 root root 4096 Jun  6 04:11 .  
dr-xr-xr-x. 18 root root 4096 Jun  6 04:11 ..  
lrwxrwxrwx.  1 root root    7 May 23 05:39 bin -> usr/bin  
dr-xr-xr-x.  6 root root 1024 Jun  6 05:31 boot  
drwxr-xr-x. 19 root root 3340 Jul 28 06:42 dev  
drwxr-xr-x. 117 root root 12288 Jul 28 06:42 etc  
drwxr-xr-x.  3 root root 4096 Jun  6 05:14 home  
lrwxrwxrwx.  1 root root    7 May 23 05:39 lib -> usr/lib  
drwx-----.  2 root root 16384 May 23 05:37 lost+found  
drwxr-xr-x.  2 root root   40 Jul 28 06:42 media  
drwxr-xr-x.  2 root root 4096 Feb  3 19:28 mnt  
drwxr-xr-x.  2 root root 4096 Feb  3 19:28 opt
```

유닉스 디렉토리 열람

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 권한
- ② 파일의 소유자
- ③ 파일에 대한 그룹

- ①은 다시 다음과 같이 4개 부분으로 세부화

```
- rw- r-- r--
```

a b c d

- ① 파일 및 디렉터리의 종류
 - 는 일반 파일을, d는 디렉터리를, l은 링크(link)를 의미
- ② 파일 및 디렉터리 소유자의 권한
- ③ 파일 및 디렉터리 그룹의 권한
- ④ 제3의 사용자에게 대한 권한

□ 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.

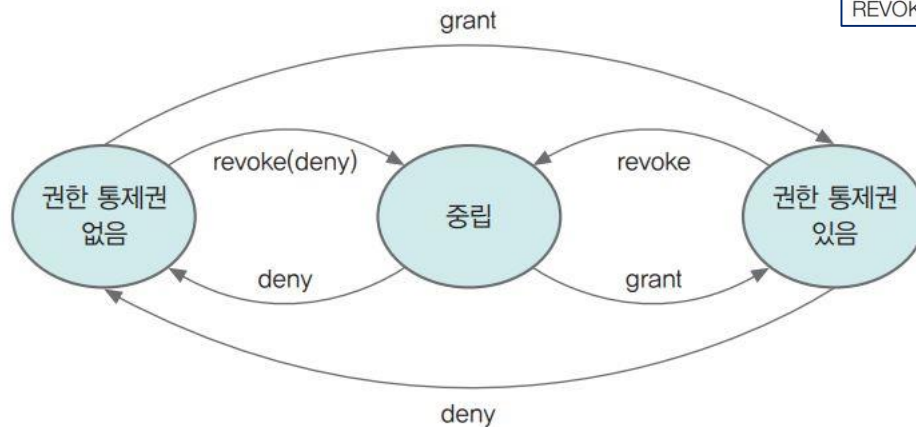
데이터베이스 질의문(Query) 종류

❑ 데이터베이스의 권한 관리

❑ 질의문에 대한 권한 관리

- DDL과 DML은 DCL에 의해 허용 또는 거부

GRANT	데이터베이스 객체에 권한을 부여한다.
DENY	사용자에게 해당 권한을 금지한다.
REVOKE	이미 부여된 데이터베이스 객체의 권한을 취소한다.

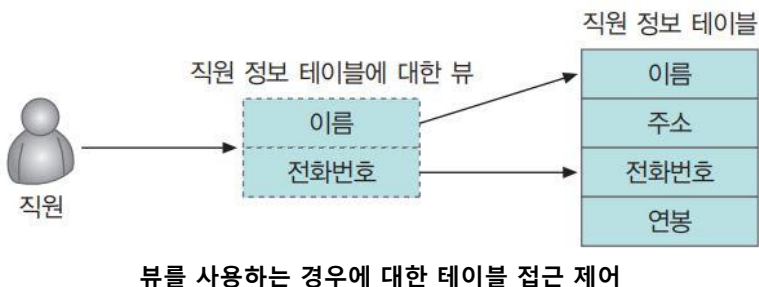
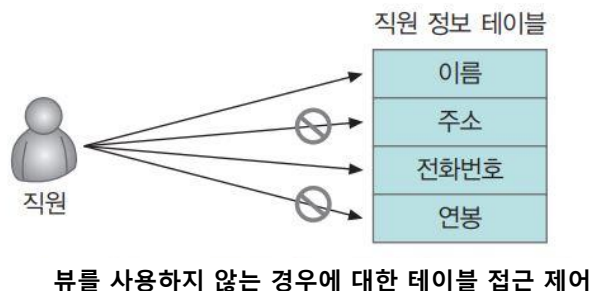


DCL 명령에 의한 권한 부여 구조

데이터베이스의 권한 관리

뷰에 대한 권한 관리

- 뷰(view): 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



□ 데이터베이스의 권한 관리

▣ 응용 프로그램의 권한 관리

- 응용 프로그램은 응용 프로그램 내의 권한 관리보다 **응용 프로그램 자체의 실행 권한이 더 중요**
- 자신을 실행한 계정의 권한을 물려받음.
 - 보안상에 문제가 있는 **취약한 응용 프로그램**의 경우 해당 프로그램을 실행한 계정의 **권한이 악용될 수 있는 문제**가 발생
- 이를 대비하기 위해, 윈도우의 IIS에서는 **실행 프로세스 권한을 별도로** 만들어 사용
- 유닉스에서는 **nobody**와 같이 **제한된 계정 권한**을 사용

CONTENTS

□ 로그 관리

로그 관련 기본 개념

□ 로그 데이터

- 실제 현실에서 발생하는 사건을 시간과 함께 데이터로 기록된 정보
- 운영체제, 응용 프로그램 등 서비스를 제공하는 주체에 따라 다양한 로그 데이터들이 존재함
 - 윈도우
 - 이벤트(Event)라는 중앙 집중화된 로그를 수집하여 저장함
 - 로그가 중앙 집중화되어 관리가 용이함
 - 공격자가 한 로그만 삭제하면 되므로, 로그 관리에 있어 보안 수준이 낮음
 - 유닉스
 - 로그를 여러 곳에 산발적으로 저장하며, 여러 곳에 저장된 유닉스 로그는 초보자들이 찾기가 어려움
 - 공격자도 로그를 모두 찾아 지우기 어려움

로그 관련 기본 개념

□ AAA (Authentication, Authorization, Accounting)

- 사용자가 시스템에 로그인하여 명령을 내리는 과정에 대한 시스템 동작을 구분 지을 수 있음
- 네트워크 및 시스템 접근 허용을 위한 인증을 통한 권한 부여와 사용자 대한 사용 정보를 관리하기 위한 프레임워크

- Authentication

- 자신의 신원(Identity)을 시스템에 증명하는 과정(아이디(id)와 패스워드(password) 입력)
 - 아이디가 신원을 나타내고, 정상 패스워드를 입력하면 인증됨

- Authorization

- 올바른 패스워드를 입력 시스템에 로그인한 사람의 권한 여부를 나타냄
 - 정상적으로 인증이 된 사람일지라도, 특정 서버로의 접근 권한은 없을 수 있음

- Accounting

- 사용자의 자원에 대한 사용 정보를 모아서 과금, 감사, 리포팅 등을 수행



Who is
the User



What User
Can Do



What the
User Did



로그 관련 기본 개념

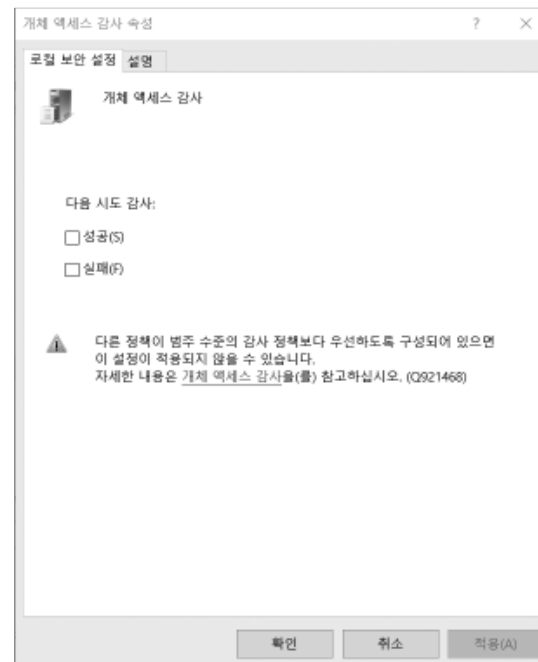
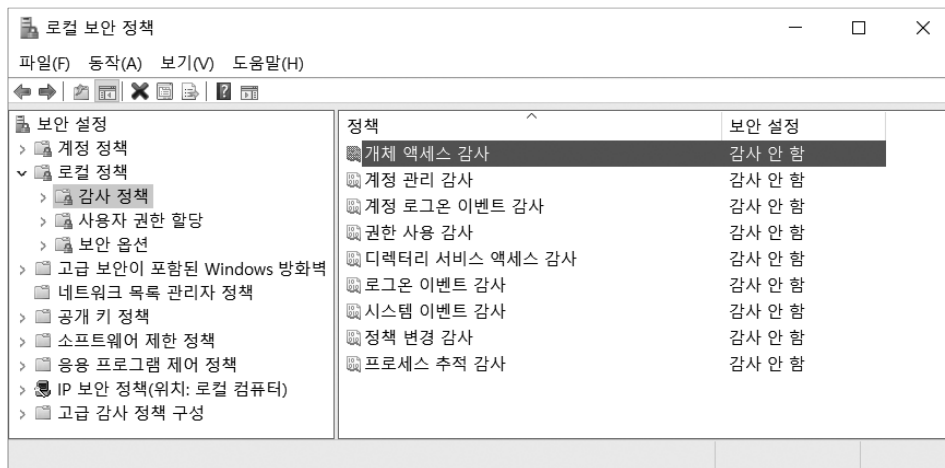
- AAA (Authentication, Authorization, Accounting)
 - ▣ 인증과 인가, Accounting은 일반 운영체제 뿐만 아니라 방화벽 등 모든 시스템에 해당
 - ▣ 책임 추적성(Accountability) : 추적에 대한 기록의 충실도
 - ▣ 감사 추적(Audit Trail) : Accounting을 하여 남긴 로그 정보를 통한 추적 그 자체

원도우의 로그 분석과 설정

로그 정책의 설정

윈도우 로그 정책

- [제어판]-[관리 도구]-[로컬 보안 정책] 메뉴 선택 [로컬 정책]-[감사 정책]에서 확인
- 윈도우에서는 로그 정책이 대부분 정보를 로깅하지 않게 설정 가능

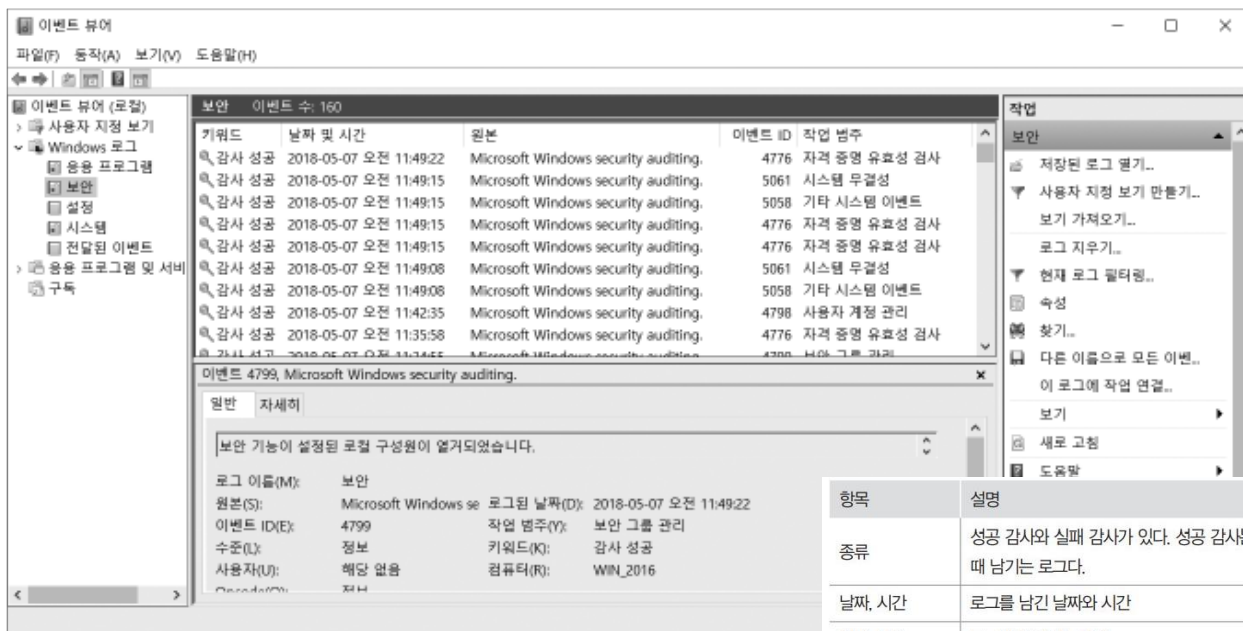


윈도우의 로그 분석과 설정

□ 로그 정책의 설정

■ 윈도우 로그 정책

- [제어판]-[관리 도구]-[이벤트 뷰어]에서 쌓이는 로깅 정보 확인
- 이벤트 뷰어를 통해 윈도우 보안 로그 확인 가능



이벤트 뷰어를 통한 보안 로그

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

이벤트 뷰어에서의 표시 항목

윈도우의 로그 분석과 설정

□ 로그 감사

- 파일이나 디렉토리, 레지스트리 키, 프린터 같은 객체에 접근을 시도하거나 속성을 변경하려는 행위 등을 탐지할 수 있음

이벤트 ID	내용
4656	개체에 대한 접근 요청
4657	레지스트리 값 변경
4658	개체에 대한 접근 종료
4660	개체 삭제
4663	개체에 대한 접근
4670	개체의 접근 권한 변경
4698	스케줄된 작업 생성
4699	스케줄된 작업 삭제
4700	스케줄된 작업 활성화
4701	스케줄된 작업 비활성화
5031	외부의 접근을 허용하는 응용 프로그램을 윈도우 방화벽이 차단
5140	네트워크 공유 개체 접근

윈도우의 로그 분석과 설정

□ 로그 감사

▣ 개체 관리 감사

이벤트 ID	내용
4739	도메인 정책 변경
4722	사용자 계정 활성화
4724	사용자 계정 패스워드 초기화 시도
4726	사용자 계정 삭제
4740	사용자 계정 잠금
4781	사용자 계정 이름 변경
4720	사용자 계정 생성
4723	사용자 계정 패스워드 변경 시도
4725	사용자 계정 비활성화
4738	사용자 계정 변경
4767	사용자 계정 잠금 해제

주요 계정 관리 감사 로그

윈도우의 로그 분석과 설정

□ 로그 감사

▣ 계정 로그인 이벤트 감사

※ 도메인 컨트롤러

- 윈도우 서버 도메인 안에서 보안 인증 요청에 응답하는 서버 컴퓨터 (로그인, 권한확인, 사용자 등록, 암호 변경 등)

이벤트 ID	내용
4776	도메인 컨트롤러에 대한 로그인 시도
4777	도메인 컨트롤러에 대한 로그인 시도 실패

주요 계정 로그인 이벤트 감사 로그

오류 코드	설명
C0000064	사용자 이름이 존재하지 않는다.
C000006A	사용자 이름은 맞으나 비밀번호가 일치하지 않는다.
C0000234	해당 계정이 현재 잠긴 상태이다.
C0000072	해당 계정이 현재 사용 중지된 상태이다.
C000006F	해당 계정이 허용되어 있지 않은 기간에 접근을 시도한다.
C0000070	로그인을 시도한 시스템에 접근이 허용되어 있지 않다.
C0000193	계정이 만료된다.
C0000071	만료된 비밀번호를 사용한다.
C0000224	다음 로그인할 때 사용자 비밀번호를 변경해야 한다.
C0000225	운영체제 오류로 로그인에 실패한다.

4776 이벤트 ID 오류 코드 리스트

윈도우의 로그 분석과 설정

□ 로그 감사

▣ 권한 사용 감사

- 권한 설정 변경 시, 관리자 권한이 필요한 작업 수행 시 로깅
- 공격자가 계정 생성하여 관리자 권한 부여, 이에 준하는 일 수행 시 로깅이 남음

이벤트 ID	내용
4672	권한 할당
4673	권한이 있는 서비스 호출
4674	권한이 있는 개체 작동

주요 권한 사용 감사 로그

윈도우의 로그 분석과 설정

□ 로그 감사

▣ 로그인 이벤트 감사

- 계정 로그인 이벤트 감사와 비슷함

■ 로컬 계정의 접근 시 생성되는 이벤트를 감사

이벤트 ID	내용
4624	성공적인 로그인
4634	로그오프
4778	윈도우 시스템에 세션 재생성
4800	시스템 잠금
4802	화면 보호기 실행
5632	무선 네트워크를 통한 인증 요청
4625	계정 로그인 시도 실패
4649	리플레이 공격 탐지
4779	윈도우 시스템에 세션 해제
4801	시스템 잠금 해제
4803	화면 보호기 해제
5633	유선 네트워크를 통한 인증 요청

윈도우의 로그 분석과 설정

□ 로그 감사

▣ 디렉토리 서비스 액세스 감사

- 디렉토리 서비스 운영에 대한 부분

▣ 정책 변경 감사

- 사용자 권한 할당 정책, 감사 정책, 또는 신뢰정책 변경과 관련된 사항을 로깅함

이벤트 ID	내용	이벤트 ID	내용
4719	시스템 감사 정책 변경	4714	암호화 데이터 복구 정책 변경
4907	개체에 대한 감사 설정 변경	4946	방화벽에 대한 예외사항 목록 변경 - 규칙 추가
4706	다른 도메인과의 신뢰 관계 형성	4947	방화벽에 대한 예외사항 목록 변경 - 규칙 변경
4707	다른 도메인과의 신뢰 관계 제거	4948	방화벽에 대한 예외사항 목록 변경 - 규칙 제거
4713	커버로스 정책 변경	4950	방화벽 설정 변경
4704	사용자 권한 할당	4670	개체에 대한 권한 변경
4705	사용자 권한 제거		

주요 정책 변경 감사 로그

윈도우의 로그 분석과 설정

□ 로그 감사

▣ 프로세스 추적 감사

- 프로세스 추적 감사 관련 이벤트 로그는 사용자나 응용 프로그램이 프로세스 시작, 중지 시 발생

이벤트 ID	내용
4688	새 프로세스 생성
4689	프로세스 종료
5712	RPC (Remote Procedure Call)이 시도됨

주요 프로세스 추적 감사 로그

※ RPC (Remote Procedure Call)

- 별도의 원격 제어를 위한 코딩 없이 다른 주소 공간에서 리모트의 함수나 프로시저를 실행 할 수 있게 해주는 프로세스간 통신

윈도우의 로그 분석과 설정

□ 로그 감사

▣ 시스템 이벤트

- 시스템의 서비스 시작과 종료, 보안 로그 삭제 등 시스템의 주요 사항에 대한 이벤트

이벤트 ID	내용
5024	방화벽 서비스 시작
5025	방화벽 동작 멈춤
5030	방화벽 시작 실패
4608	윈도우 시작
4609	윈도우 종료
4616	시스템 시간 변경
4697	시스템에 서비스 등록
4618	모니터링하고 있던 보안 이벤트에서 패턴 발생

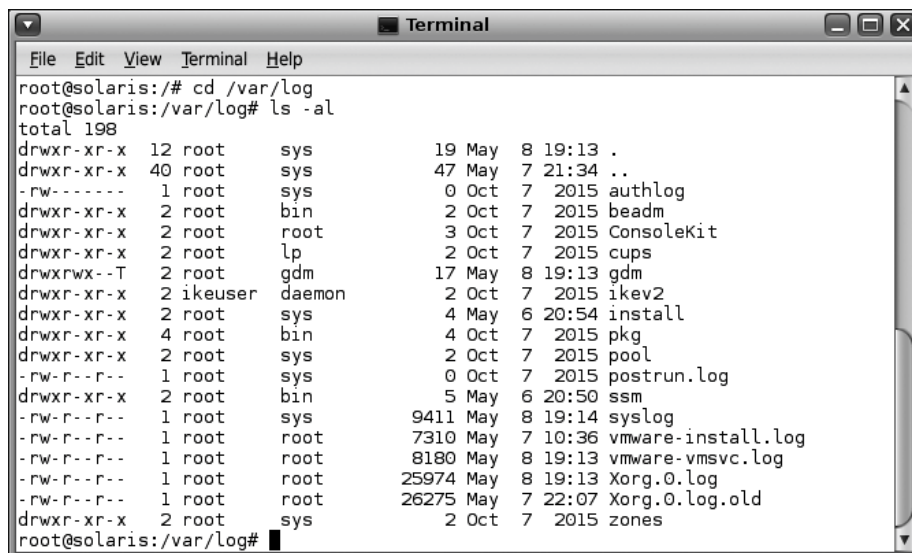
주요 시스템 이벤트 감사 로그

리눅스 로그 분석과 설정

□ 로그 디렉터리

경로	적용 시스템
/usr/adm	초기 유닉스, BSD 계열 : HP-UX 9.X, SunOS 4.x
/var/adm	최근 유닉스, SVR 계열 : 오라클 솔라리스, HP-UX 10.x 이후, IBM AIX
/var/log	일부 BSD 계열 : BSD, FreeBSD, 오라클 솔라리스, 리눅스
/var/run	일부 리눅스

```
cd /var/log
ls -al
```



```
root@solaris:~# cd /var/log
root@solaris:/var/log# ls -al
total 198
drwxr-xr-x 12 root  sys      19 May  8 19:13 .
drwxr-xr-x 40 root  sys      47 May  7 21:34 ..
-rw-r--r--  1 root  sys         0 Oct  7 2015 authlog
drwxr-xr-x  2 root  bin        2 Oct  7 2015 beadm
drwxr-xr-x  2 root  root       3 Oct  7 2015 ConsoleKit
drwxr-xr-x  2 root  lp         2 Oct  7 2015 cups
drwxrwx--T  2 root  gdm       17 May  8 19:13 gdm
drwxr-xr-x  2 ikeuser daemon    2 Oct  7 2015 ikev2
drwxr-xr-x  2 root  sys        4 May  6 20:54 install
drwxr-xr-x  4 root  bin        4 Oct  7 2015 pkg
drwxr-xr-x  2 root  sys        2 Oct  7 2015 pool
-rw-r--r--  1 root  sys         0 Oct  7 2015 postrun.log
drwxr-xr-x  2 root  bin        5 May  6 20:50 ssm
-rw-r--r--  1 root  sys     9411 May  8 19:14 syslog
-rw-r--r--  1 root  root    7310 May  7 10:36 vmware-install.log
-rw-r--r--  1 root  root    8180 May  8 19:13 vmware-vmvsc.log
-rw-r--r--  1 root  root   25974 May  8 19:13 Xorg.0.log
-rw-r--r--  1 root  root   26275 May  7 22:07 Xorg.0.log.old
drwxr-xr-x  2 root  sys        2 Oct  7 2015 zones
root@solaris:/var/log#
```

리눅스 로그 분석과 설정

□ utmp 로그

▣ utmp 데몬 : utmp 파일에 로그 남기는 프로그램

- utmp 데몬은 리눅스의 가장 기본적인 로깅을 제공하는 데몬(/etc/lib/utmpd) 현재 시스템에 로그인한 사용자의 상태 출력
- utmp 데몬에 저장된 로그를 출력하는 명령 : **w, who, users, whodo, finger** 등

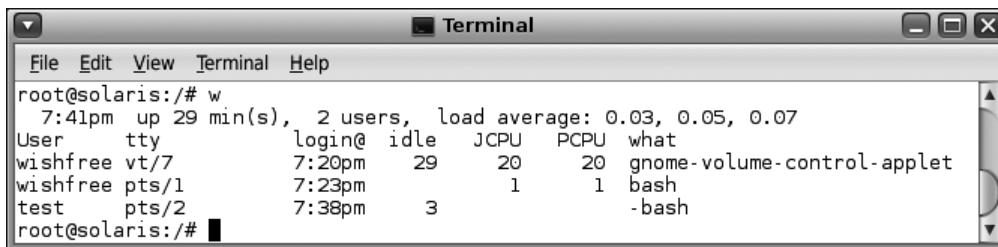
▣ w 명령

- 현재 시스템에 로그인된 사용자 계정과 로그인 셸 종류, 로그인 시간, 실행 중인 프로세스의 종류

리눅스 로그 분석과 설정

□ utmp 로그

w

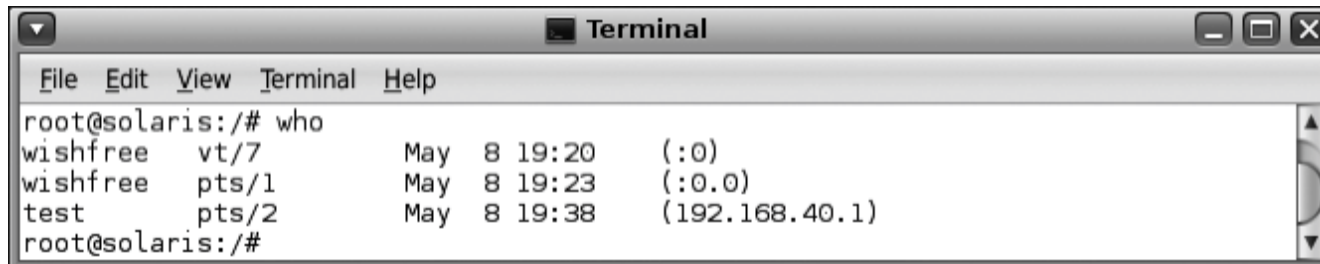


```
root@solaris:~# w
 7:41pm up 29 min(s),  2 users,  load average: 0.03, 0.05, 0.07
User      tty      login@   idle    JCPU    PCPU    what
wishfree  vt/7      7:20pm   29      20      20      gnome-volume-control-applet
wishfree  pts/1     7:23pm    1       1       1      bash
test      pts/2     7:38pm    3       -       -      -bash
root@solaris:~#
```

w 명령을 실행하여 현재 시스템에도 로그인한 사용자 목록 확인

□ who 명령 : 접속한 시스템의 IP 확인

who



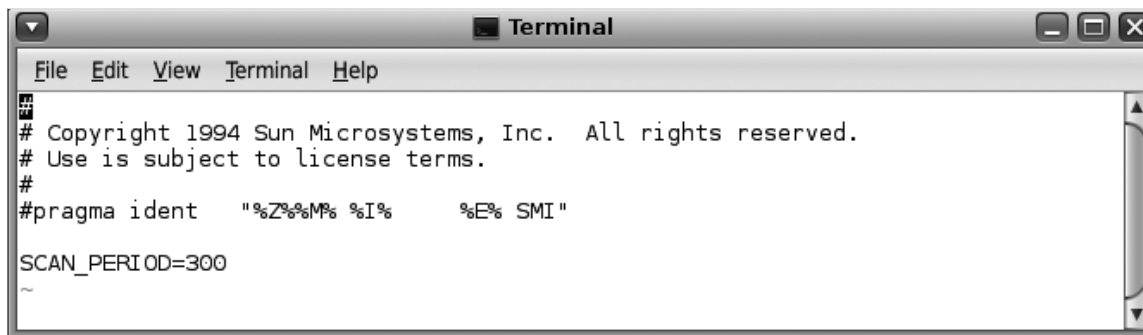
```
root@solaris:~# who
wishfree  vt/7      May  8 19:20    (:0)
wishfree  pts/1     May  8 19:23    (:0.0)
test      pts/2     May  8 19:38    (192.168.40.1)
root@solaris:~#
```

who 명령을 실행하여 시스템에 로그인한 사용자 IP확인

리눅스 로그 분석과 설정

□ utmp 로그

```
vi /etc/default/utmpd
```



```
Terminal
File Edit View Terminal Help
# Copyright 1994 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#pragma ident  "%Z%%M%  %I%      %E% SMI"

SCAN_PERIOD=300
~
```

/etc/default/utmpd 파일에서 스캔 주기 설정

리눅스 로그 분석과 설정

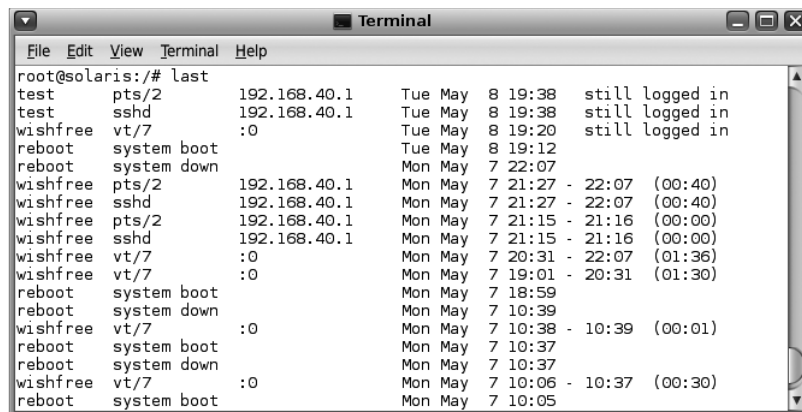
□ wtmp 로그

▣ wtmp 데몬

- wtmp 파일에 로그 남김, /usr/include/utmp.h 파일 구조체 사용
- utmp 데몬과 비슷한 역할, 사용자들의 로그인, 로그아웃, 시스템 재부팅 정보 수록

▣ last 명령 이용 확인

last



```
root@solaris:/# last
test pts/2 192.168.40.1 Tue May 8 19:38 still logged in
test sshd 192.168.40.1 Tue May 8 19:38 still logged in
wishfree vt/7 :0 Tue May 8 19:20 still logged in
reboot system boot Tue May 8 19:12
reboot system down Mon May 7 22:07
wishfree pts/2 192.168.40.1 Mon May 7 21:27 - 22:07 (00:40)
wishfree sshd 192.168.40.1 Mon May 7 21:27 - 22:07 (00:40)
wishfree pts/2 192.168.40.1 Mon May 7 21:15 - 21:16 (00:00)
wishfree sshd 192.168.40.1 Mon May 7 21:15 - 21:16 (00:00)
wishfree vt/7 :0 Mon May 7 20:31 - 22:07 (01:36)
wishfree vt/7 :0 Mon May 7 19:01 - 20:31 (01:30)
reboot system boot Mon May 7 18:59
reboot system down Mon May 7 10:39
wishfree vt/7 :0 Mon May 7 10:38 - 10:39 (00:01)
reboot system boot Mon May 7 10:37
reboot system down Mon May 7 10:37
wishfree vt/7 :0 Mon May 7 10:06 - 10:37 (00:30)
reboot system boot Mon May 7 10:05
```

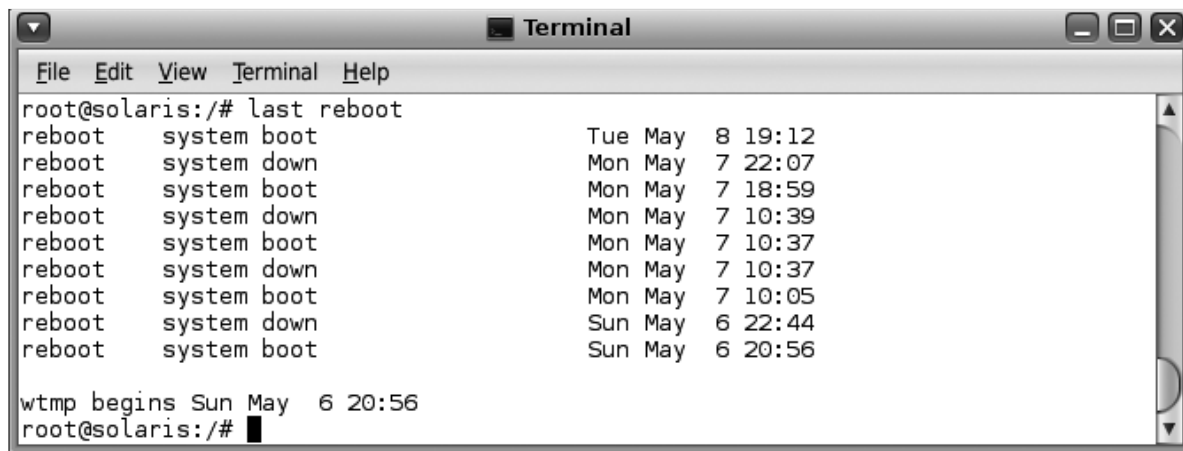
last 명령 실행하여 시스템에 로그인한 사용자의 최근 목록 확인

리눅스 로그 분석과 설정

□ wtmp 로그

- ▣ 특정 항목만 확인하고 싶으면 last 명령 뒤에 해당 문자열만 추가

```
last reboot
```



```
root@solaris:/# last reboot
reboot      system boot          Tue May  8 19:12
reboot      system down           Mon May  7 22:07
reboot      system boot          Mon May  7 18:59
reboot      system down           Mon May  7 10:39
reboot      system boot          Mon May  7 10:37
reboot      system down           Mon May  7 10:37
reboot      system boot          Mon May  7 10:05
reboot      system down           Sun May  6 22:44
reboot      system boot          Sun May  6 20:56

wtmp begins Sun May  6 20:56
root@solaris:/#
```

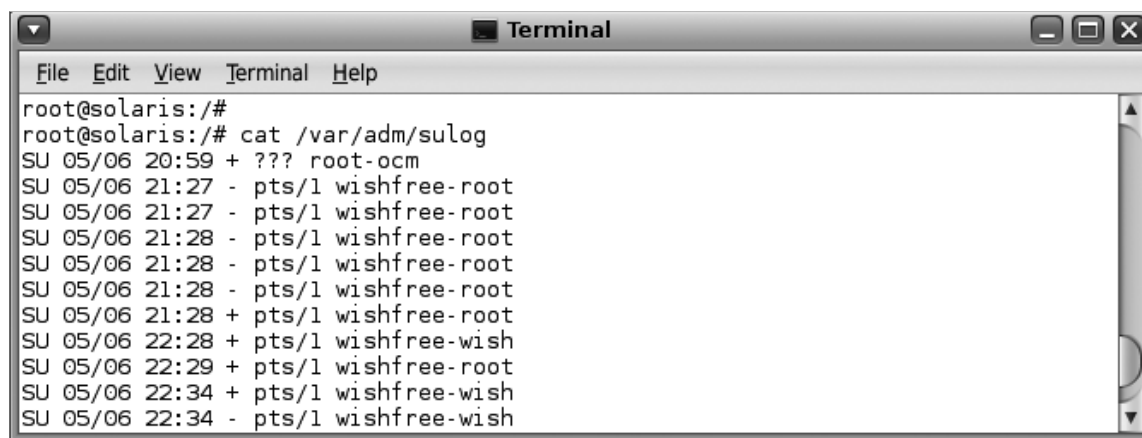
last reboot 명령 실행하여 시스템을 부팅/셧 다운한 최근 기록 확인

리눅스 로그 분석과 설정

□ su 로그

- su (switch user)는 권한 변경에 대한 로그

```
cat /var/adm/sulog
```



```
root@solaris:/#  
root@solaris:/# cat /var/adm/sulog  
SU 05/06 20:59 + ??? root-ocm  
SU 05/06 21:27 - pts/1 wishfree-root  
SU 05/06 21:27 - pts/1 wishfree-root  
SU 05/06 21:28 - pts/1 wishfree-root  
SU 05/06 21:28 - pts/1 wishfree-root  
SU 05/06 21:28 - pts/1 wishfree-root  
SU 05/06 21:28 + pts/1 wishfree-root  
SU 05/06 22:28 + pts/1 wishfree-wish  
SU 05/06 22:29 + pts/1 wishfree-root  
SU 05/06 22:34 + pts/1 wishfree-wish  
SU 05/06 22:34 - pts/1 wishfree-wish
```

□ 출력 형식

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

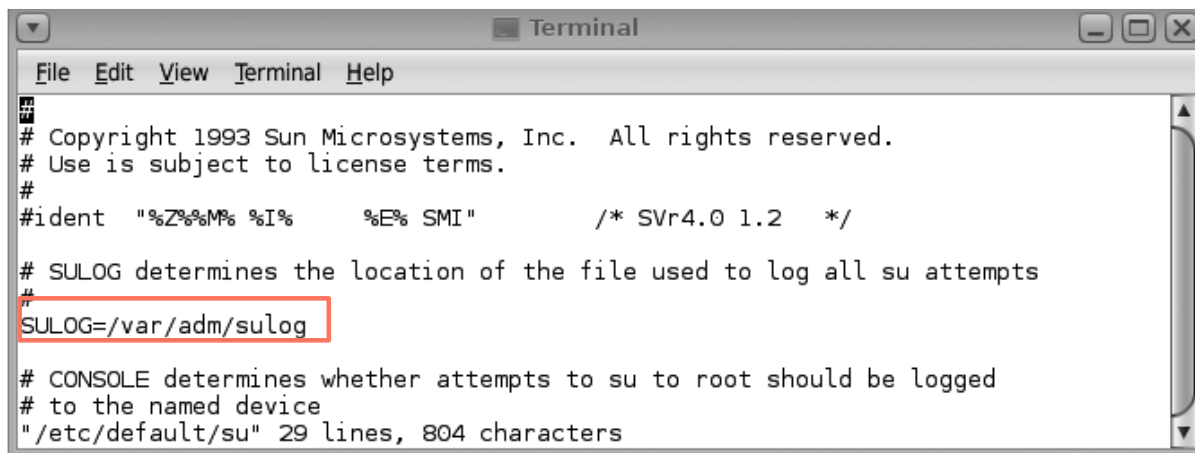
- su 로그에 대한 설정 파일 : `/etc/default/su`

리눅스 로그 분석과 설정

□ su 로그

▣ su 로그에 대한 설정 파일 : **/etc/default/su**

```
vi /etc/default/su
```



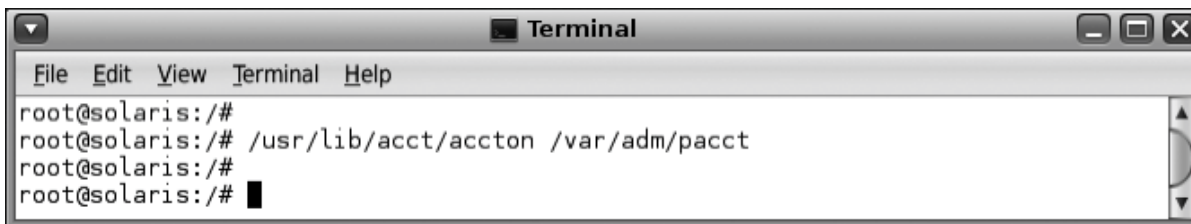
```
Terminal
File Edit View Terminal Help
# Copyright 1993 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "%Z%%M% %I%      %E% SMI"          /* SVr4.0 1.2 */
# SULONG determines the location of the file used to log all su attempts
#
SULONG=/var/adm/sulog
# CONSOLE determines whether attempts to su to root should be logged
# to the named device
"/etc/default/su" 29 lines, 804 characters
```

리눅스 로그 분석과 설정

□ pacct 로그

- ▣ 시스템에 로그인한 모든 사용자가 수행한 프로그램에 대한 정보 저장하는 로그

```
/usr/lib/acct/accton  /var/adm/pacct
```



```
Terminal
File Edit View Terminal Help
root@solaris:/#
root@solaris:/# /usr/lib/acct/accton /var/adm/pacct
root@solaris:/#
root@solaris:/# █
```

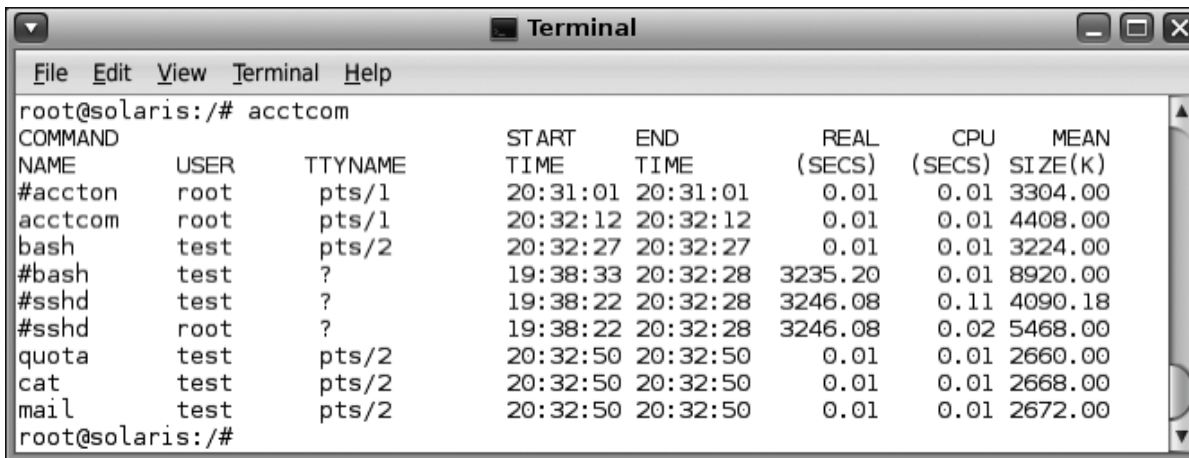
- ▣ pacct 로그도 utmp나 wtmp처럼 /usr/adm/pacct 파일에 텍스트가 아닌 바이너리 형태로 저장

리눅스 로그 분석과 설정

□ pacct 로그

- ▣ pacct 로그도 utmp나 wtmp처럼 /usr/adm/pacct 파일에 텍스트가 아닌 바이너리 형태로 저장
- ▣ 로깅 내용 확인 위한 acctcom 명령 실행

acctcom



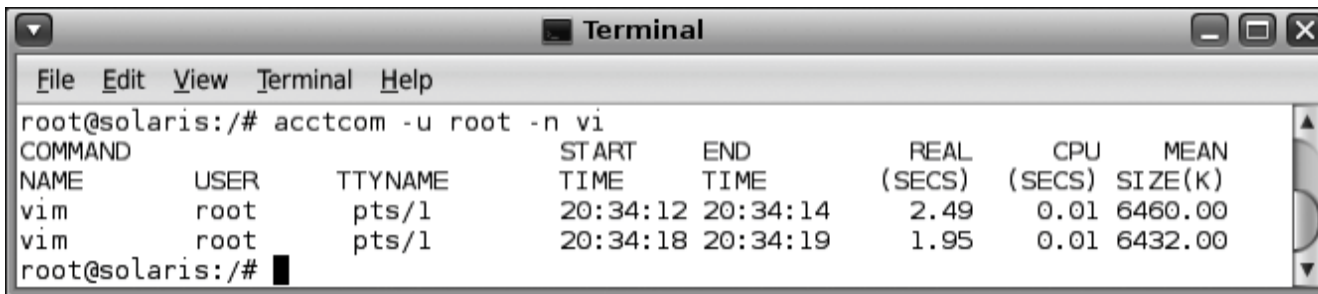
COMMAND	NAME	USER	TTYNAME	START TIME	END TIME	REAL (SECS)	CPU (SECS)	MEAN SIZE(K)
#accton		root	pts/1	20:31:01	20:31:01	0.01	0.01	3304.00
acctcom		root	pts/1	20:32:12	20:32:12	0.01	0.01	4408.00
bash		test	pts/2	20:32:27	20:32:27	0.01	0.01	3224.00
#bash		test	?	19:38:33	20:32:28	3235.20	0.01	8920.00
#sshd		test	?	19:38:22	20:32:28	3246.08	0.11	4090.18
#sshd		root	?	19:38:22	20:32:28	3246.08	0.02	5468.00
quota		test	pts/2	20:32:50	20:32:50	0.01	0.01	2660.00
cat		test	pts/2	20:32:50	20:32:50	0.01	0.01	2668.00
mail		test	pts/2	20:32:50	20:32:50	0.01	0.01	2672.00

리눅스 로그 분석과 설정

□ root 계정으로 vi 에디터 실행한 기록 출력하는 명령

▣ acctcom을 통해 root 계정이 vim 에디터를 실행한 내역 확인이 가능

acctcom -u root -n vi



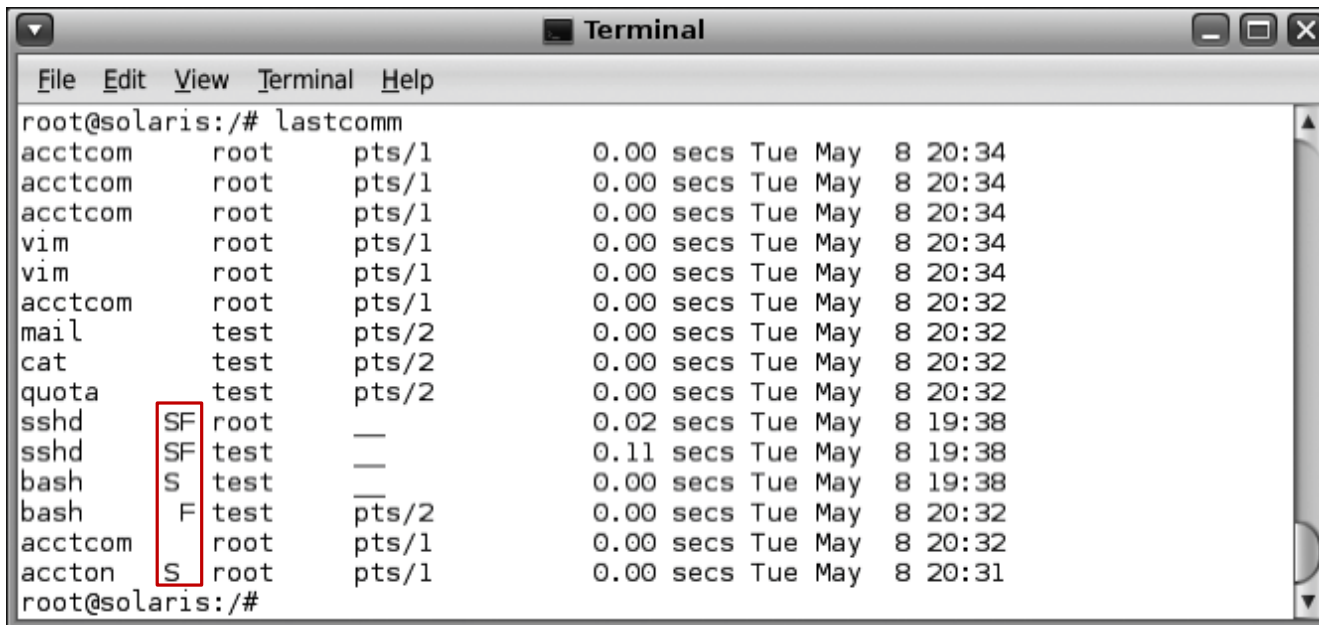
COMMAND							
NAME	USER	TTYNAME	START TIME	END TIME	REAL (SECS)	CPU (SECS)	MEAN SIZE(K)
vim	root	pts/1	20:34:12	20:34:14	2.49	0.01	6460.00
vim	root	pts/1	20:34:18	20:34:19	1.95	0.01	6432.00

리눅스 로그 분석과 설정

□ lastcomm

▣ 실행된 날짜 출력

```
lastcomm
```



```
root@solaris:/# lastcomm
acctcom    root    pts/1    0.00 secs Tue May 8 20:34
acctcom    root    pts/1    0.00 secs Tue May 8 20:34
acctcom    root    pts/1    0.00 secs Tue May 8 20:34
vim        root    pts/1    0.00 secs Tue May 8 20:34
vim        root    pts/1    0.00 secs Tue May 8 20:34
acctcom    root    pts/1    0.00 secs Tue May 8 20:32
mail       test    pts/2    0.00 secs Tue May 8 20:32
cat        test    pts/2    0.00 secs Tue May 8 20:32
quota      test    pts/2    0.00 secs Tue May 8 20:32
sshd       SF root    0.02 secs Tue May 8 19:38
sshd       SF test   0.11 secs Tue May 8 19:38
bash       S  test   0.00 secs Tue May 8 19:38
bash       F  test    pts/2    0.00 secs Tue May 8 20:32
acctcom    root    pts/1    0.00 secs Tue May 8 20:32
accon      S  root    pts/1    0.00 secs Tue May 8 20:31
root@solaris:/#
```


리눅스 로그 분석과 설정

□ lastcomm

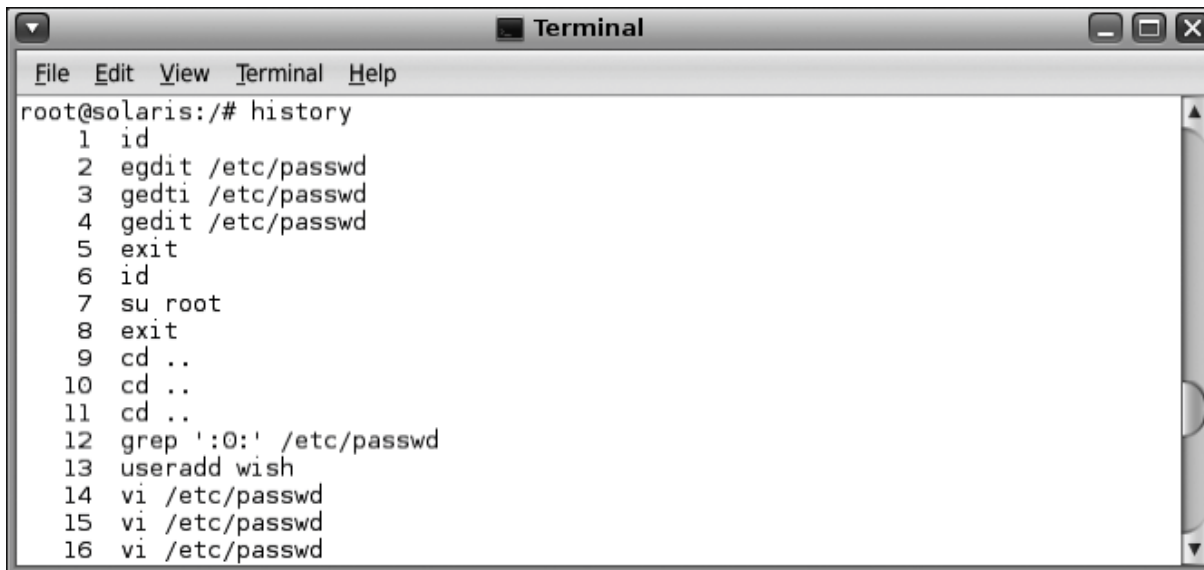
- ▣ lastcomm 명령 이용하면 실행한 명령과 S, F, D, X가 각 프로세스 간략한 상태 표시
 - S : Superuser가 사용한 명령
 - F : Fork 후에 사용된 명령
 - D : Core를 덤프하고 종료된 명령
 - X : Signal에 의해 종료된 명령

```
/usr/lib/acct/accton
```

리눅스 로그 분석과 설정

- .sh_history 또는 .bash_history
 - ▣ 리눅스에서는 실행 명령 기록
 - .sh_history, .csh_history, .bash_history 에 저장됨
 - ▣ '[셸의 종류]_history 파일' 형식으로 각 계정의 홈 디렉터리에 저장

history



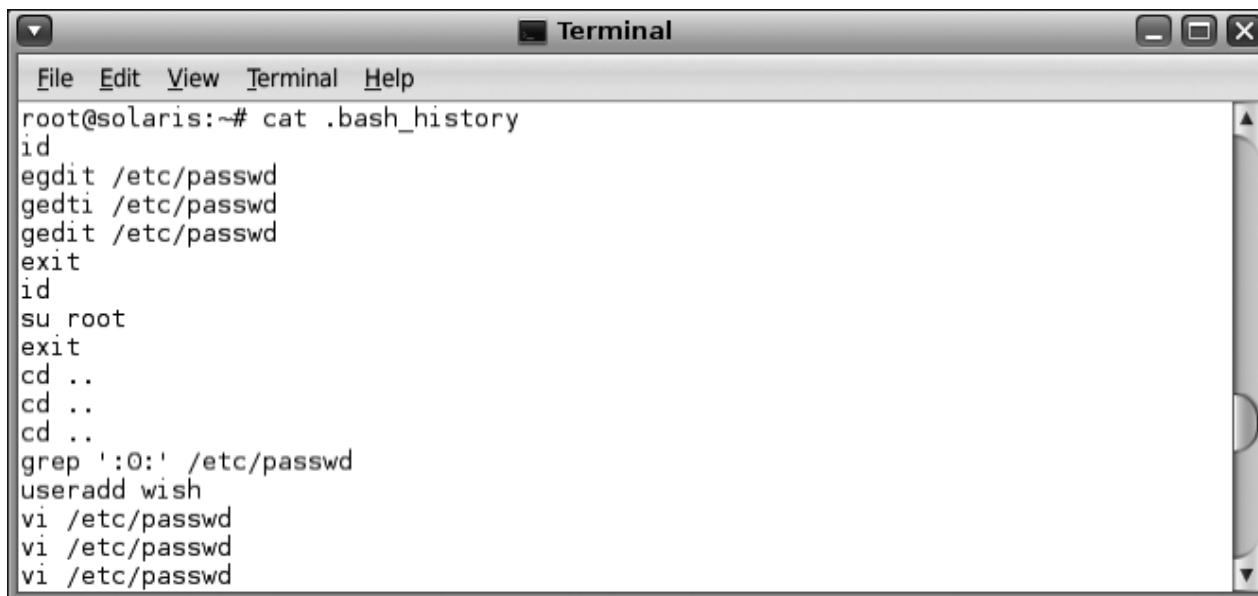
```
root@solaris:/# history
 1 id
 2 egdit /etc/passwd
 3 gedti /etc/passwd
 4 gedit /etc/passwd
 5 exit
 6 id
 7 su root
 8 exit
 9 cd ..
10 cd ..
11 cd ..
12 grep ':0:' /etc/passwd
13 useradd wish
14 vi /etc/passwd
15 vi /etc/passwd
16 vi /etc/passwd
```

리눅스 로그 분석과 설정

❑ .sh_history 또는 .bash_history

- ▣ history 내용은 .bash_history에 텍스트 형태로 저장
- ▣ cat이나 more 명령으로 확인

```
cat .bash_history
```



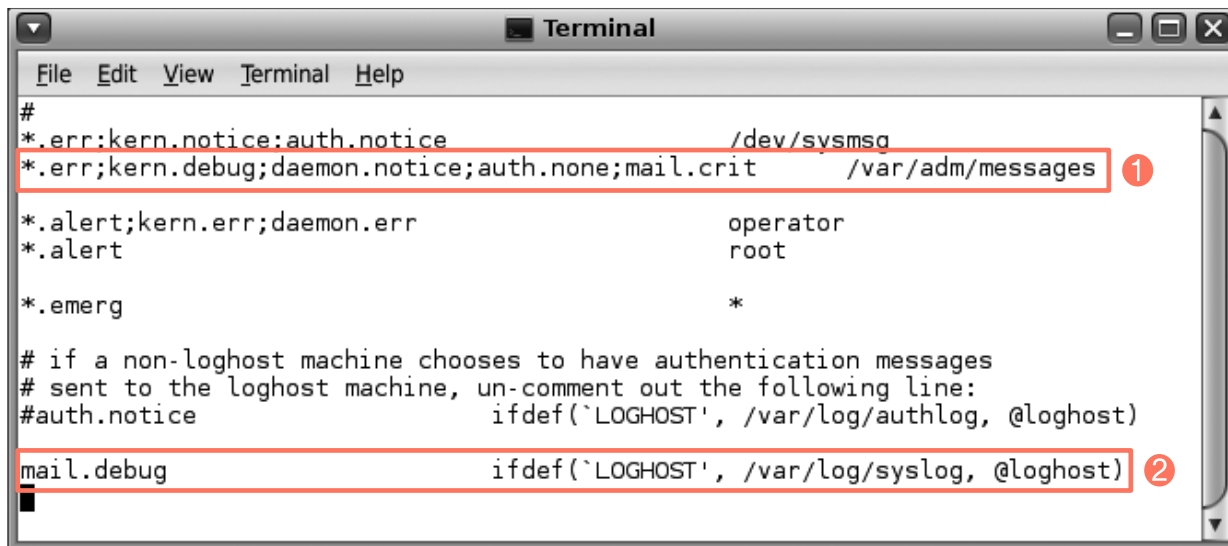
```
Terminal
File Edit View Terminal Help
root@solaris:~# cat .bash_history
id
egdit /etc/passwd
gedti /etc/passwd
gedit /etc/passwd
exit
id
su root
exit
cd ..
cd ..
cd ..
grep ':0:' /etc/passwd
useradd wish
vi /etc/passwd
vi /etc/passwd
vi /etc/passwd
```

리눅스 로그 분석과 설정

□ syslog

- ▣ 시스템의 로그 정보를 대부분 수집하여 로깅
- ▣ 해당 로그의 종류와 로깅 수준은 /etc/syslog.conf 파일에서 확인

```
vi /etc/syslog.conf
```



```
File Edit View Terminal Help
#
*.err;kern.notice:auth.notice          /dev/sysmsg
*.err;kern.debug;daemon.notice;auth.none;mail.crit    /var/adm/messages  1
*.alert;kern.err;daemon.err             operator
*.alert                                       root
*.emerg                                       *
# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
#auth.notice          ifdef('LOGHOST', /var/log/authlog, @loghost)
mail.debug             ifdef('LOGHOST', /var/log/syslog, @loghost)  2
█
```

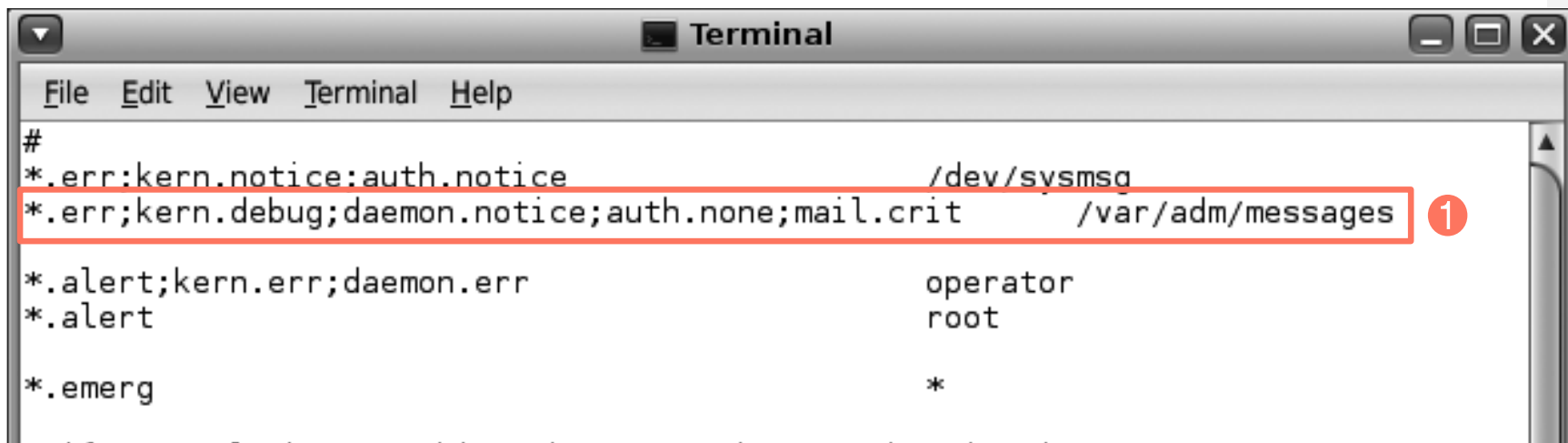
리눅스 로그 분석과 설정

□ syslog

□ ① *.err;kern.debug;daemon.notice;mail.crit

/var/adm/messages

- 모든 에러(*.err)와 커널의 디버그 시 남는 로그(**kern.debug**)
- 각 데몬의 동작에 대한 일반 정보(**daemon.notice**)
- 메일 서비스에 심각한 오류가 있는 경우 (**mail.crit**)
- **/var/adm/messages** 파일에 관련 로그를 저장(로깅)



```
#
*.err:kern.notice:auth.notice /dev/sysmsg
*.err;kern.debug;daemon.notice;auth.none;mail.crit /var/adm/messages ①
*.alert;kern.err;daemon.err operator
*.alert root
*.emerg *
```

리눅스 로그 분석과 설정

□ syslog

▣ ② mail.debug ifdef(`LOGHOST', /var/log/syslog, @loghost)

- 해석: 메일에 대한 디버깅 정보(mail.debug)를 **`LOGHOST'**가 정의되어 있을 경우
- (ifdef) loghost 시스템의(@loghost) **/var/log/syslog** 파일에 메시지 저장

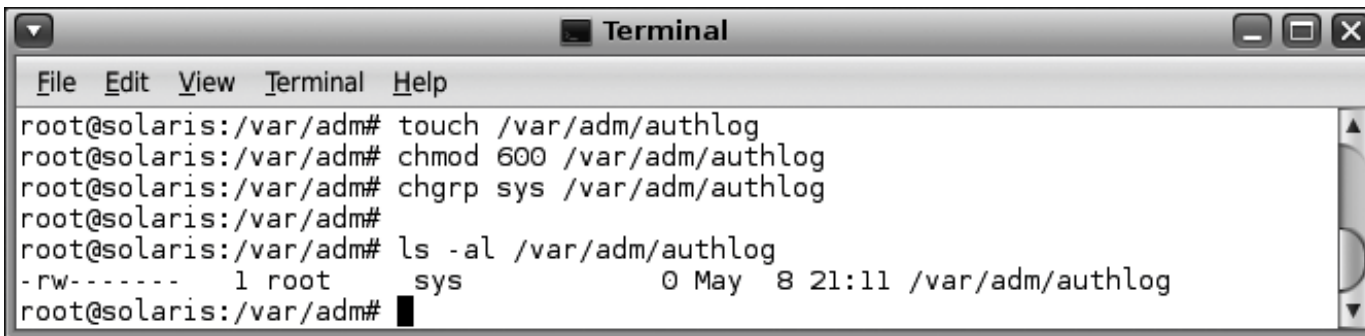
```
# if a non-loghost machine chooses to have authentication messages
# sent to the loghost machine, un-comment out the following line:
#auth.notice                ifdef(`LOGHOST', /var/log/authlog, @loghost)
mail.debug                   ifdef(`LOGHOST', /var/log/syslog, @loghost) ②
```

리눅스 로그 분석과 설정

□ authlog / loginlog

- ▣ loginlog는 실패한 로그인 시도에 대한 로깅 수행
- ▣ loginlog 파일에 실패한 로그인 기록이 저장되도록 설정
- ▣ 이 설정은 /etc/default/login 파일에 저장, 시스템 재부팅할 때 적용

```
touch /var/adm/authlog
chmod 600 /var/adm/authlog
chgrp sys /var/adm/authlog
```



```
Terminal
File Edit View Terminal Help
root@solaris:/var/adm# touch /var/adm/authlog
root@solaris:/var/adm# chmod 600 /var/adm/authlog
root@solaris:/var/adm# chgrp sys /var/adm/authlog
root@solaris:/var/adm#
root@solaris:/var/adm# ls -al /var/adm/authlog
-rw-----  1 root    sys      0 May  8 21:11 /var/adm/authlog
root@solaris:/var/adm#
```

리눅스 로그 분석과 설정

□ 시스템별 로그 상세 경로

로그 파일	리눅스(레드햇)	솔라리스	HP-UX (10.x 이상)	IBM-AIX
utmp, wtmp	/var/run(utmp) /var/log(wtmp)	/var/adm	/var/adm	/var/adm
utmpx, wtmpx	존재하지 않음	/var/adm	존재하지 않음	존재하지 않음
btmp	/var/log	존재하지 않음	/var/adm	존재하지 않음
syslog	존재하지 않음	/var/log	/var/adm/syslog/syslog.log	/var/adm
secure	/var/log	존재하지 않음	존재하지 않음	존재하지 않음
sulog	존재하지 않음	/var/adm	/var/adm	/var/adm
pacct	/var/log	/var/adm	/var/adm	/var/adm
authlog	존재하지 않음	/var/log	존재하지 않음	존재하지 않음
messages	/var/log	/var/adm	/var/adm	/var/adm
loginlog	존재하지 않음	/var/adm	존재하지 않음	존재하지 않음
lastlog	/var/log	/var/adm	/var/adm	/etc/security
access_log	/var/log/httpd	/var/log/httpd	/usr/local/etc/httpd/logs	/usr/local/etc/httpd/logs
error_log	/var/log/httpd	/var/log/httpd	/usr/local/etc/httpd/logs	/usr/local/etc/httpd/logs
shutdownlog	존재하지 않음	존재하지 않음	/etc/shutdownlog	존재하지 않음
failedlogin	존재하지 않음	존재하지 않음	존재하지 않음	/etc/security

데이터베이스 로그 관리

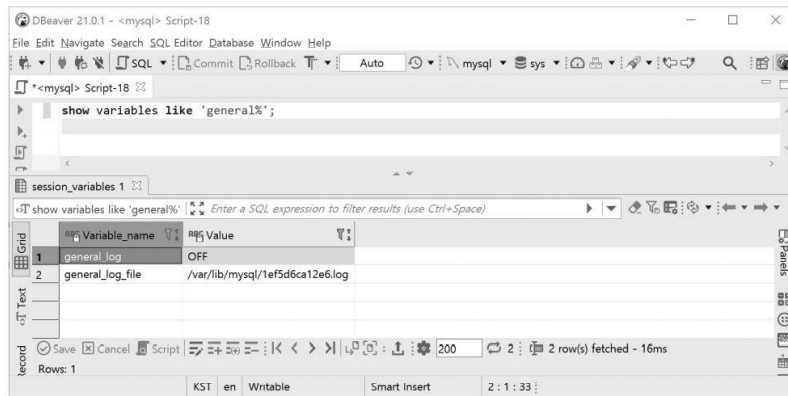
MySQL 로그

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, Relay 로그는 슬레이브에서 생성되며 포맷과 내용은 동일하다.

MySQL 로그 종류

General 로그의 경우, 현재 설정을 확인할 수 있음

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



MySQL General Log 설정 확인

데이터베이스 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



```
# Change '<ORACLE_BASE>' to point to the oracle base (the one you specify at
# install time)

db_name='ORCL'
memory_target=1G
processes = 150
audit_file_dest='<ORACLE_BASE>/admin/orcl/adump'
audit_trail = db
db_block_size=8192
db_domain=
db_recovery_file_dest='<ORACLE_BASE>/fast_recovery_area'
db_recovery_file_dest_size=2G
diagnostic_dest='<ORACLE_BASE>'
dispatchers='(PROTOCOL=TCP) (SERVICE=ORCLXDB)'
open_cursors=300
remote_login_passwordfile='EXCLUSIVE'
undo_tablespace='UNDOTBS1'
# You may want to ensure that control files are created on separate physical
# devices
```

오라클 감사 로그 설정

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.

데이터베이스 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.

오라클 데이터베이스 감사 종류 및 예

데이터베이스 로그 관리

□ 오라클의 로그

▣ 각각의 감사 종류는 감사 뷰를 통해 확인 가능

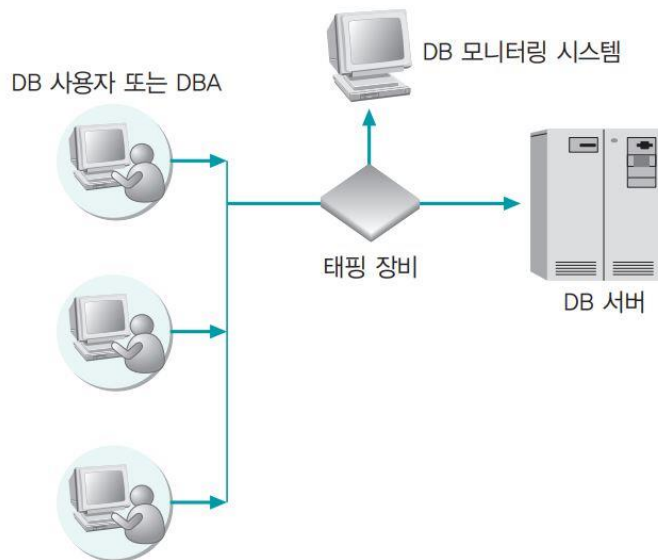
뷰	설명
dba_stmt_audit_opts	문장 감사의 옵션을 확인한다.
dba_priv_audit_opts	권한 감사의 옵션을 확인한다.
dba_obj_audit_opts	객체 감사의 옵션을 확인한다.
dba_audit_trail	데이터베이스의 모든 감사 로그를 출력한다.
dba_audit_object	데이터베이스의 객체와 관련된 모든 감사 로그를 출력한다.
user_audit_object	현재 사용자의 객체와 관련된 모든 감사 로그를 출력한다.
dba_audit_session	사용자의 로그인·로그오프에 대한 감사 로그를 출력한다.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

오라클의 주요 감사 뷰

➔ 데이터베이스 로그 관리

❑ 데이터베이스 모니터링

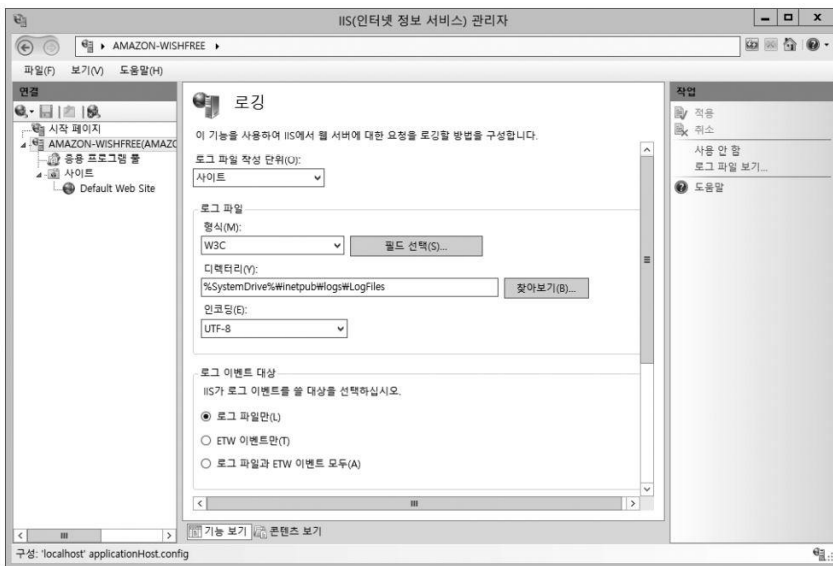
- ❑ 네트워크 트래픽을 모니터링할 수 있는 태핑(tapping) 장비를 네트워크에 설치
- ❑ 네트워크 패킷에서 질의문(Query)을 로그로 남김
 - 데이터베이스의 성능에 영향을 미치지 않으면서 잘못된 접근 시도와 질의문 입력을 모두 모니터링할 수 있음



응용 프로그램 로그 관리

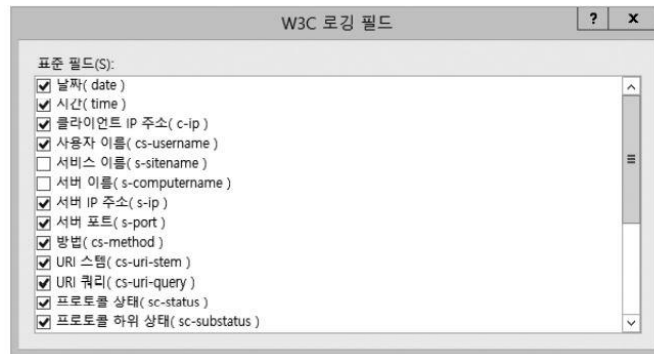
■ IIS 웹 서버의 로그

- IS 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



IIS 웹 서버 로깅 설정

※ W3C: MS 계열의 IIS 기본 설정에서 사용하는 로그



W3C 로깅 필드

■ IIS 웹 서버의 로그

- 실제 로그는 '디렉토리' 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
```

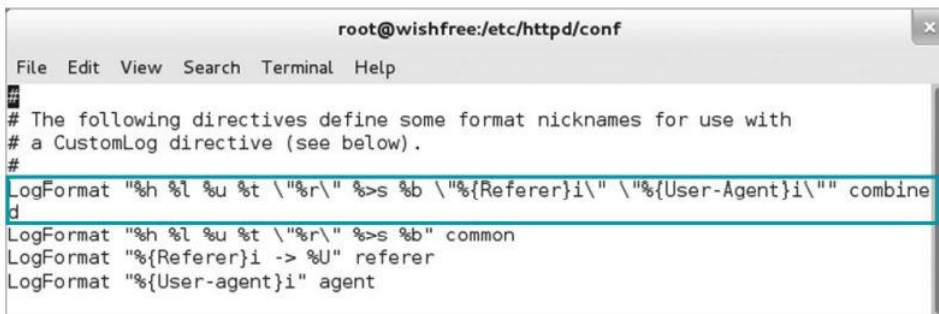
■ 샘플 로그의 실제 구성

- 날짜와 시간: 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 데이터의 크기: 0
- 클라이언트에서 서버로 전송한 데이터의 크기: 0
- 처리 소요 시간: 225ms

응용 프로그램 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



```
root@wishfree:/etc/httpd/conf
File Edit View Search Terminal Help
# The following directives define some format nicknames for use with
# a CustomLog directive (see below).
#
LogFormat "%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"" combined
LogFormat "%h %l %u %t \"%r\" %>s %b" common
LogFormat "%{Referer}i -> %U" referer
LogFormat "%{User-agent}i" agent
```

LogFormat 값 설정

응용 프로그램 로그 관리

□ 아파치 웹 서버의 로그

▣ LogFormat에서 설정된 combined 형식의 각 항목

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
%i	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

combined 형식 로그에 사용되는 항목

□ 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...

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(SIEM)에 의해 수집·관리되기도 함

▣ 네트워크 관리 시스템의 로그

- 트래픽 모니터링 시스템과 네트워크 관리 시스템(NMS)의 로그를 참고할 수 있음

▣ 네트워크 장비 인증 시스템의 로그

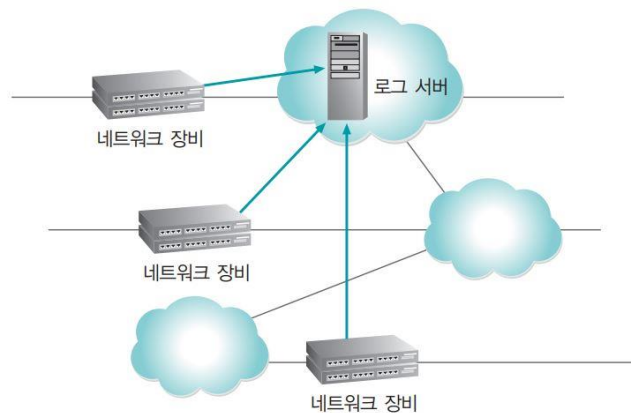
- 대규모 네트워크를 운영하는 곳에서는 라우터나 스위치의 인증을 일원화하기 위해 인증 서버를 따로 구성함
- 인증 서버에서 네트워크 장비에 대한 **인증 시도** 및 **로그인 정보** 등을 확인할 수 있음

네트워크 장비의 로그 관리

□ 네트워크 보안 시스템의 로그

▣ 로그 서버

- 대부분의 네트워크 장비에는 하드디스크와 같이 로그를 저장할 저장 공간이 없어 로그 서버를 별도로 두고 운영
- **로그서버를 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



네트워크 장비의 로그 생성과 보존

CONTENTS

❑ 취약점 관리

❑ 패치 관리

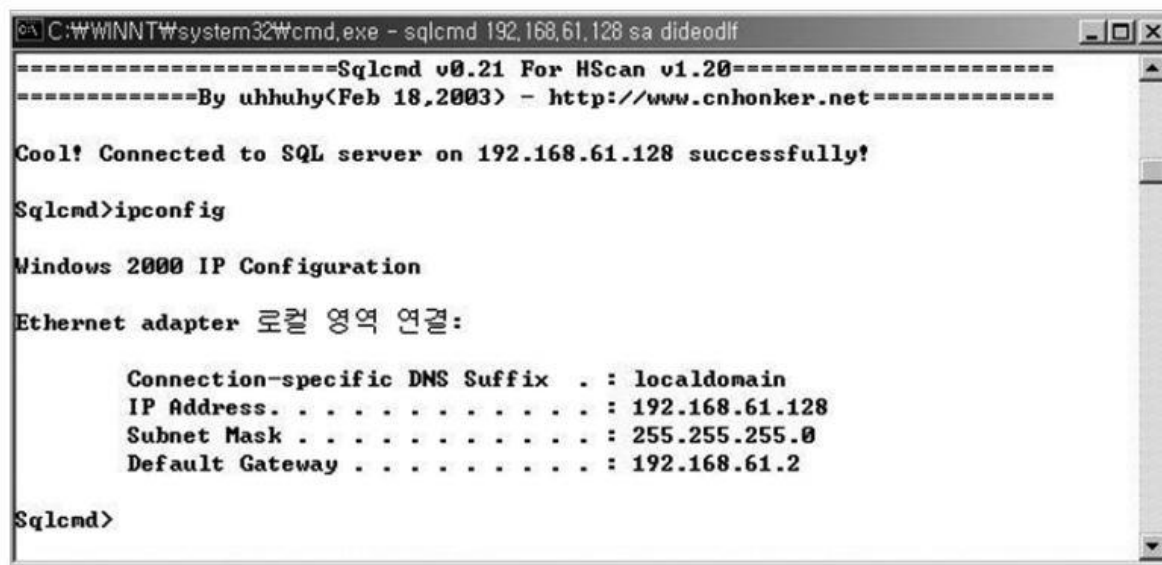
- 응용 프로그램을 만든 제작사가 배포하는 패치 또는 서비스 팩을 적용해 시스템 자체의 취약점을 보완
- 유닉스 시스템에도 내재된 취약점이 있지만 윈도우는 사용률이 훨씬 높고 접근하기도 쉬워 공격을 더 많이 받음
- 윈도우 업데이트를 통해 자동으로 보안 패치를 확인하고 적용할 수 있음



➔ 취약점 관리

□ 응용 프로그램별 고유 위험 관리

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



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

=====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>
```

➔ 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 과정
 - 일반 계정은 **vrify** 명령, 그룹은 **expn** 명령을 시스템 내부에서 사용
- 일반 사용자는 텔넷을 이용해 시스템에 존재하는 계정 목록을 파악할 수 있음(PrivayOption에서 해당 VRFY 명령 사용을 제한)

```
telnet 192.168.61.129 25
vrify root
vrify wishfree
vrify abc
```



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

sendmail 데몬에 접속 및 vrify 명령 실행 결과

- 시스템 보안의 이해
- 계정 관리
- 세션 관리
- 접근 제어
- 권한 관리
- 로그 관리
- 취약점 관리

참고문헌

- ▣ 정보 보안 개론 - 한권으로 배우는 핵심 보안 이론, 양대일, 한빛 아카데미

Q & A

