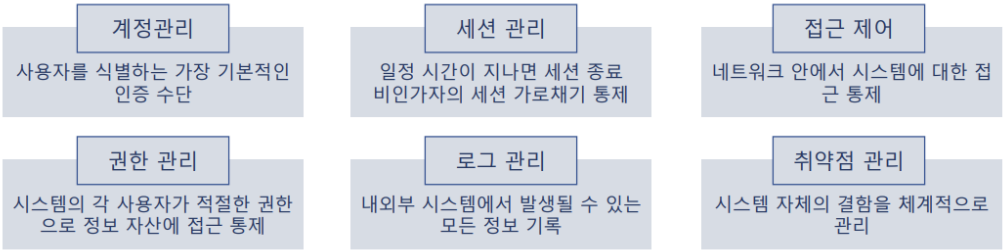
3 / 16 (2)

- 목차
  1. 시스템 보안의 이해
  2. 계정 관리
  3. 세션 관리
  4. 접근 제어
  5. 권한 관리
  6. 로그 관리
  7. 취약점 관리
  8. 모바일 보안

1. 시스템 보안의 이해
   - 시스템
     - 독차적으로 동작할 수 있는 독립적인 개체
     - 전원으로 부터 시작하여 메모리, 디스크, CPU등의 하드웨어 자원과 OS, Driver 등 소프트웨어 자원까지, 시스템을 구성하는 포괄적인 요소들을 포함함
     - 네트워크와 시스템의 융합된 형태의 인프라를 구성
     - 예 : 클라우드, 분산처리 시스템, VDI 등

▪ 시스템 보안 주제



2. 계정 관리

- 식별과 인증
  - 식별 : 어떤 시스템에 로그인 하려면 먼저 자신이 누군지를 알림
  - 인증 : 로그인을 허용하기 위한 확인
- 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, 콜백을 사용해 인증 수행
    - 콜백 : 접속을 요청한 사람의 신원을 확인, 미리 등록된 전화번호로 전화를 되걸어 접속을 요청한 사람이 본인인지 확인
- OS별 계정 관리
- OS별 특성
- 윈도우의 계정 관리
  - net localgroup : 윈도우에서는 기본 그룹을 정의하는데, 시스템에 존재하는 그룹 목록
  - net localgroup administrators : 관리자 그룹의 계정의 존재 형태를 확인
  - net users : 사용자 계정을 모두 확인

▪ 유닉스의 계정 관리

• /etc/passwd : root 계정 및 일반 계정

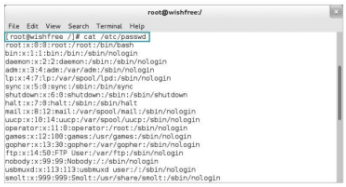


그림 2-5 유닉스의 /etc/passwd 파일 열람

```
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

• /etc/group : root굽을 포함하는 일반 그룹

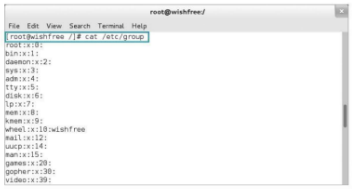


그림 2-6 유닉스의 그룹 확인

```
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

- 데이터베이스의 계정 관리
  - 데이터베이스에도 운영체제처럼 계정이 존재
  - MS-SQL의 관리자 계정은 sa, 오라클의 관리자 계정은 sys, system
  - 둘 다 관리자 계정이지만, sys와 달리 system은 데이터베이스를 생성할 수 없음.
- 응용 프로그램 계정 관리
  - 취약한 응용 프로그램을 통해 공격자가 운영체제에 접근하여 민감한 정보를 습득한 뒤 운영체제를 공격하는 데 이용할 수 잇음.
  - 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 접속시 사용자 모드로 로그인 되며, 사용자 모등서 관리자 모드로 로그인 하려면, 다시 별도의 패스워드 입력
  - 네트워크 장비에서도 계정을 생성하여, 각 계정으로 사용할 수 있는 명령어의 집합을 제한할 수 있음

3. 세션 관리

- 세션 : 사용자와 시스템 사이 또는 두 시스템 사이의 활성화 된 접속

- 지속적인 인증
    - 세션을 유지하기 위한 보안 사항 중 하나
    - 인증에 성공한 후 인증된 사용자가 처음의 사용자인지 지속으로 재인증 작업을 거치는 작업
    - 매번 패스워드를 입력 할 수 없으므로, 시스템은 이를 세션에 대한 타임아웃 설정으로 보완
    - 반면 유닉스 원격에서 접속할 경우 패스워드를 다시 묻지 않고, 세션을 종료한 후 재접속할 것을 요구
    - 시스템이 아닌 웹 서비스를 이용할 때도 '지속적인 인증'이 적용

4. 접근 제어
    - 접근 제어
        - 적절한 권한을 가진 인가자만 특정 시스템이나 정보에 접근하도록 통제하는 것
        - 시스템의 보안 수준을 갖추기 위한 가장 기본적 수단
        - 시스템 및 네트워크에 대한 접근 제어의 가장 기본적인 수단은 IP와 서비스 포트
        - 운영체제에 대한 적절한 접근 제어를 수행하려면 가장 먼저 운영체제에서 어떤 관리적 인터페이스가 운영되고 있는지를 파악해야 함
    - 운영체제의 접근 제어
    - 데이터 베이스 접근 제어
    - 응용 프로그램의 접근 제어
    - 네트워크 장비의 접근 제어
    - 불필요한 인터페이스 제거 : 보안 정책 적용에 관한 고려
    - 운영체제에 대한 접근 목적의 인터페이스를 결정한 다음에는 접근 제어 정책을 적용해야함.
    - 시스템에 대한 접근 제어 정책은 기본적으로 IP를 통해 수행
    - 유닉스의 텔넷이나 SSH, FTP 등은 TCPWrapper를 통해 접근 제어가 가능
    - inetd 데몬은 클라이언트로 부터 inetd가 관리하는 텔넷이나 SSH, FTP 등에 대한 연결 요청을 받고, 실제 서비스를 함으로써 데몬과 클라이언트의 요청을 연결
    - TCPWrapper가 설치되면, inetd 데몬은 TCPWrapper의 tcpd 데몬에 연결을 넘겨준다.

- Tcpd 데몬은 접속을 요구한 클라이언트에 적절한 접근 권한이 있는지 확인한 후 해당 데몬에 연결을 넘겨줌
- 이때 연결에 대한 로그를 실시할 수도 있음

표 2-2 일반적으로 사용되는 관리 인터페이스

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

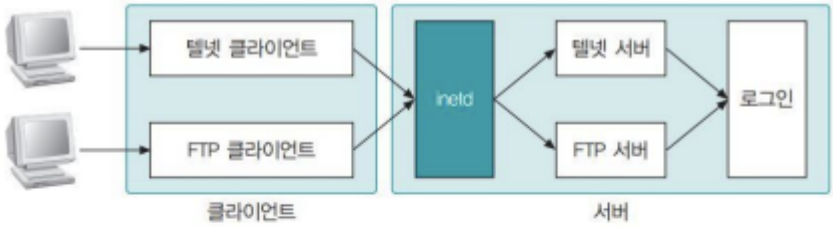


그림 2-9 inetd 데몬을 통한 데몬의 동작

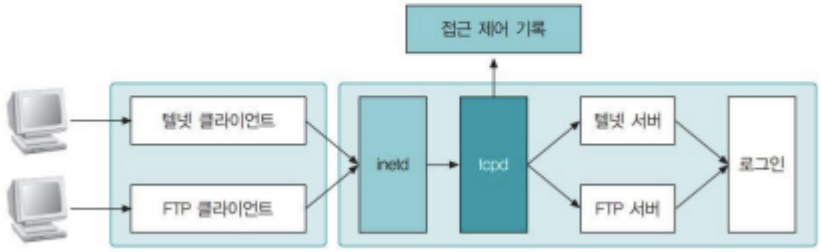


그림 2-10 TCP Wrapper를 통한 데몬의 동작

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

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

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

- MySQL

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

- IIS - Internet Information Services
- Apache
- NGINX

```
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 장비도 IP에 대한 접근 제어가 가능하다.
- 관리 인터페이스에 대한 접근 제어와 ACL을 통한 네트워크 트래픽 접근 제어가 있다.
- 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

▪ 윈도우의 권한 관리

- 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

그림 2-12 임의의 디렉터리에 권한 설정

▪ 유닉스의 권한 관리

- ls 명령(ls –al)

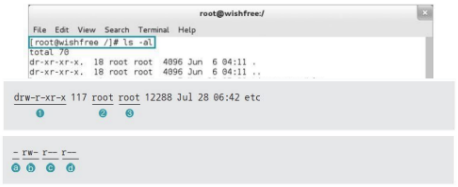


그림 2-13 유닉스의 디렉터리 열람

❶ 파일의 종류와 권한
❷ 파일의 소유자
❸ 파일에 대한 그룹
ⓐ 파일/디렉터리 종류. - 일반 파일을, d 디렉터리를, l 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

▪ Query 권한 관리

- DCL에 의하여 DDL과 DML관리

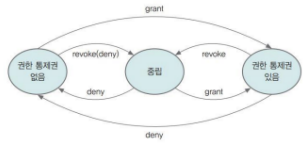


그림 2-14 DCL 명령에 의한 권한 부여 구조

표 2-3 데이터베이스 질의문 종류

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.

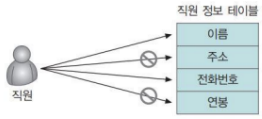


그림 2-15 뷰를 사용하지 않는 경우, 테이블에 대한 접근 제어

▪ 개체에 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

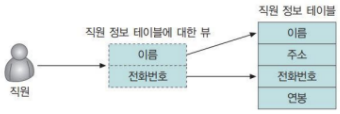
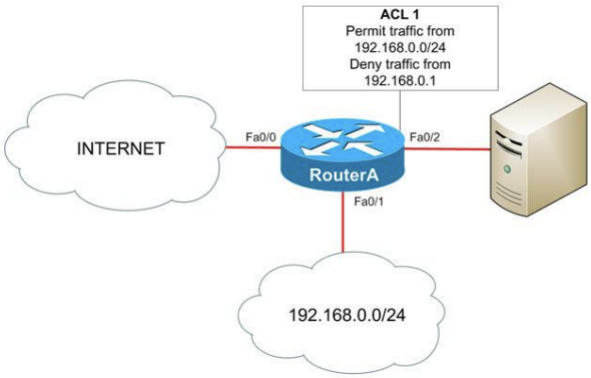


그림 2-16 뷰를 사용하는 경우, 테이블에 대한 접근 제어

- 뷰에 대한 권한만 할당

- 응용 프로그램은 응용 프로그램 내의 권한 관리보다 응용 프로그램 자체의 실행 권하이 더 중요
- 자신을 실행한 계정의 권한을 물려받으므로, 보안상에 문제가 있는 취약한 응용 프로그램의 경우 해당 프로그램을 실행한 계정의 권한이 악용되는 문제가 발생
- 윈도우 IIS에서는 실행 프로세스 권한을 별도로 만들어 사용
- 유닉스에서는 nobody와 같이 제한된 계정이 권한을 사용
- Root
- Admin
- 일반 User
- ACL

- Root
- admin
- 일반 user
- ACL



- 운영체제(서버)의 로그 관리
- 데이터 베이스의 로그 관리
- 응용 프로그램의 로그 관리
- 네트워크 장비의 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
    - 책임 추적성: 추적에 대한 기록의 충실도
    - 감사 추적: 보안과 관련하여 시간대별 이벤트를 기록한 로그
- **Authentication (인증)**
  - 자신의 신원을 시스템에 증명하는 것으로 아이디와 패스워드를 입력하는 과정
  - 해당 시스템이 지문으로 신분을 확인하는 과정
- **Authentication (인증)**
  - 자신의 신원(Identity)을 시스템에 증명하는 것으로 아이디와 패스워드를 입력하는 과정
  - 신원이 확인되어 인증받은 사람이 출입문에 들어가도록 허락하는 과정
- **Accounting**
  - 로그인했을 때 시스템이 이에 대한 기록을 남기는 활동
  - 객체나 파일에 접근한 기록

- 윈도우 로그
  - [제어판]-[관리 도구]-[이벤트 뷰어]를 통해 쌓이는 로깅 정보를 확인

그림 2-17 로컬 정책 중 감사 정책에 대한 설정

표 2-4 이벤트 뷰어에 표시되는 항목

항목	설명
종류	성공 감사와 실패 감사가 있을 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

표 2-5 윈도우의 로그 종류

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 둘이 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 로그한다.
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 관련한 사항을 로그한다.
프로세스 추적 감사	사용자 또는 응용 프로그램이 프로세스를 시작하거나 종료할 때 해당 이벤트가 발생한다.

- 유닉스 로그
  - 유닉스 시스템의 로그 저장 위치
  - /usr/adm (초기 유닉스): 데이터베이스 객체에 권한을 부여
  - /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
  - /var/log/messages 파일에 하드웨어의 구동, 서비스의 동작, 에러 등의 다양한 로그를 남김

표 2-6 유닉스의 로그 종류

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.

- MS-SQL
  - 속성 대화상자의 [보안] 메뉴에서 '일반 로그인 감사'와 'C2 감사 추적'을 설정

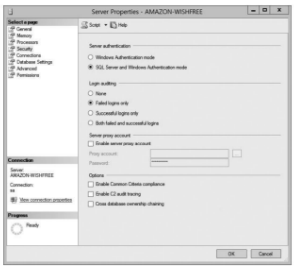


그림 2-25 감사 수준 설정

표 2-7 MySQL 로그의 종류

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) 시점들이 기록되는 바이너리 형태의 파일로, MySQL의 복제를 구성하거나 특정 시점을 복구할 때 사용된다. 일반적으로 Binary 로그는 마스터에서, Rela 로그는 슬레이브에서 생성되며 포맷과 내용은 동일하다.

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

- Oracle
  - 파라미터 파일($ORACLE_HOME/dbs/ init.ora)의 AUDIT_TRAIL 값을 'DB' 또는 'TRUE'로 지정

표 2-9 오라클의 데이터베이스 감사 종류와 예

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 무무와 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.

- IIS Internet Information Services

```
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**: 225밀리세컨드

- Apache (Web Server)
  - 아파치 웹 서버에 대한 기본 접근 로그는 access_log에 남고 형식은 'combined'로 지정
  - httpd.conf 파일에서 combined 형식의 LogFormat을 확인할 수 있음

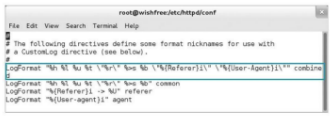


그림 2-31 LogFormat 값의 설정

- 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 수집관리되기도 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+를 사용하기도 함

    - 인증 서버를 통해 네트워크 장비에 대한 인증 시도 및 로그인 정보 등을 확인 할 수 있음.

7. 취약점 관리
    - 패치 관리
        - 응용 프로그램을 만든 제작사가 배포하는 패치 또는 서비스 팩을 적용
        - 윈도우가 사용성이 높아 공격이 많다. 유닉스는 취약점이 있어도 사용률이적어 공격을 덜 받는 편
        - 업데이트를 통해 자동으로 보안 패치를 확인 및 적용
    - 응용 프로그램 위험 관리와 정보 수집 제한
        - 응용 프로그램의 특정 기능이 운영체제 정보를 노출시키기도 함
        - 유닉스에서 이메일을 보낼 때 수신자가 있는 시스템의 sendmail 데몬에 해당 계정이 있는 걸 확인하는 과정으로 일반 계정은 vrfy 명령, 그룹은 expn 명령을 시스템 내부에서 사용
        - 일반 사용자는 텔넷을 이용해 시스템에 존재하는 계정 모곩을 파악할 수 있다.
8. 모바일 보안
    - 모바일의 역사
        - Palm → windows CE → blackberry → IOS → Android
    - IOS 보안 체계
    - IOS 취약점
    - 안드로이드 보안 체계
    - 안드로이드 취약점
    - IOS vs Android

표 2-12 iOS와 안드로이드의 보안 체계 비교

구분	iOS	안드로이드
운영체제	Darwin UNIX에서 파생하여 발전한 OS X의 모바일 버전	리눅스 커널(2.6.25)을 기반으로 만들어진 모바일 운영체제
보안 통제권	애플	개발자 또는 사용자
프로그램 실행 권한	관리자(root)	일반 사용자
응용 프로그램의 서명	애플이 자신의 CA를 통해 각각의 응용 프로그램을 서명하여 배포	개발자가 서명
샌드박스	프로그램 간 데이터 통신을 엄격히 통제	iOS에 비해 상대적으로 자유롭게 애플리케이션 실행이 가능
부팅 절차	암호화 로직으로 서명된 방식에 의해 안전한 부팅 절차 확보	
소프트웨어 관리	단말 기기별 고유한 소프트웨어 설치 키 관리	

- 과제
  - 보안 제품 혹은 시스템을 선정하고, 선정 사유를 기술해 주세요.
  - 해당 시스템이 사용하고 있는 IT기술은 무엇인지 확인하세요.
  - 그 기술의 동작원리에 대해 간략히 설명하세요.