답안지

과정명	오픈소스 기반 보안 취약점 분석 실무자 양성	담당교사	홍제준	월차	
과목명	시스템 보안구축	훈련생 이름	임서규	평가일자	
평가 방법	문제해결 시나리오				

답안

마이그레이션 보고서

(주)IT에듀케이션

- 목차 -

1. 소개

2. 웹 어플리케이션 서비스 환경
   1) 제원
   2) 원본 웹 서버와 옮겨갈 대상 서버 설명

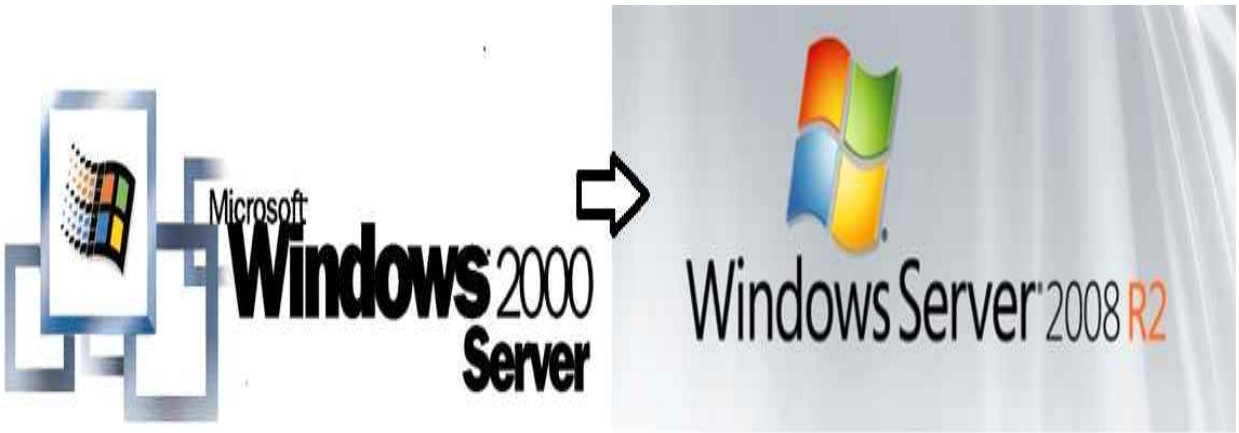
3. 상대 서버(Windows Server 2008 R2) 구축
   1) 서버 OS 설치
   2) IIS기능 설치
   3) MSSQL(SQL Server 2008) 데이터베이스 설치 및 설정

4. 원본 서버 백업파일 형성(Windows Server 2000)
   1) 소스 백업파일 형성
   2) 데이터베이스 백업파일 형성

5. 마이그레이션 할 상대 서버 작업(Windows Server 2008 R2)
   1) 보안 환경
   2) 취약점 분석표
   3) 취약점 설정

1. 소개

안녕하십니까, 현재 IT에듀케이션에서 회사의 서버 보안을 담당하고 있는 시스템 엔지니어 임서규라고 합니다. 현재 실습용 웹 서비스에 사용 중 인 서버의 운영체제가 지원이 종료된 지 오래된 운영체제이며 웹서버인 IIS 또한 오래 된 버전이라 보안상의 위험이 많은 상태입니다. 따라서 저희 서버 보안팀이 보안요구 사항을 만족하는 새로운 시스템을 설계하고 구축한 후에 마이그레이션을 실시하는 내용입니다.



<그림1> Windows2000 Server , Windows Server2008 R2의 제품 로고

먼저 마이그레이션에 대해서 간략하게 설명을 드리겠습니다. 마이그레이션이란 한 운영환경으로부터, 대개의 경우 좀 더 낫다고 여겨지는 다른 운영환경으로 옮겨가는 과정을 말합니다. 현재 저희가 사용하고 있는 Microsoft Windows Server 2000 버전에서 조금 더 안정적인 시스템인 Microsoft Windows Server 2008 R2로 옮길 예정입니다.

2. 웹 어플리케이션 서비스 환경

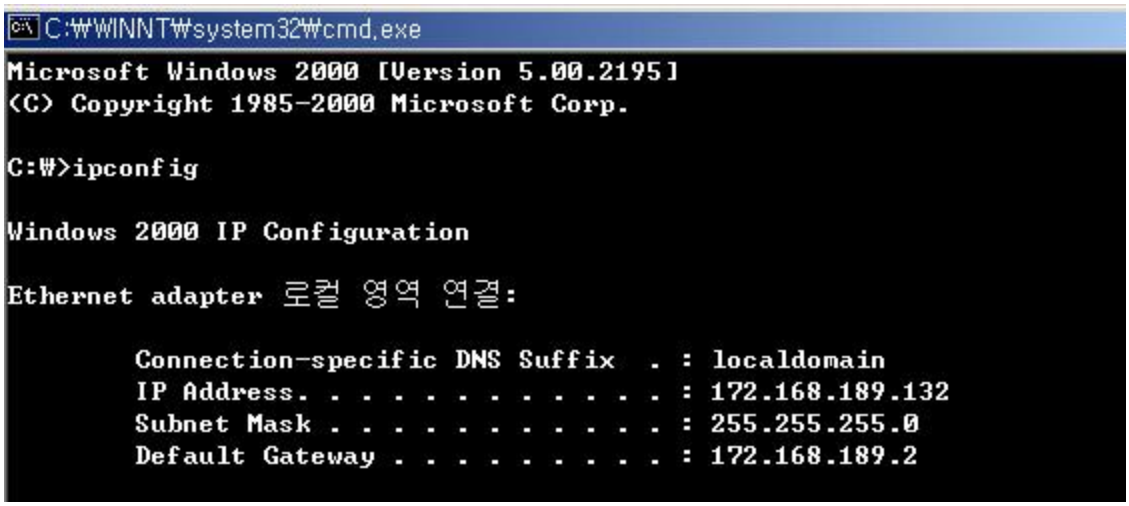
1) 제원

서버	OS	IIS	Script Language	Data Base
현재 서버	Windows 2000 Server	IIS5.0	ASP	MSSQL2000
변경 서버	Windows Server 2008 R2	IIS7.5	ASP	MSSQL2008

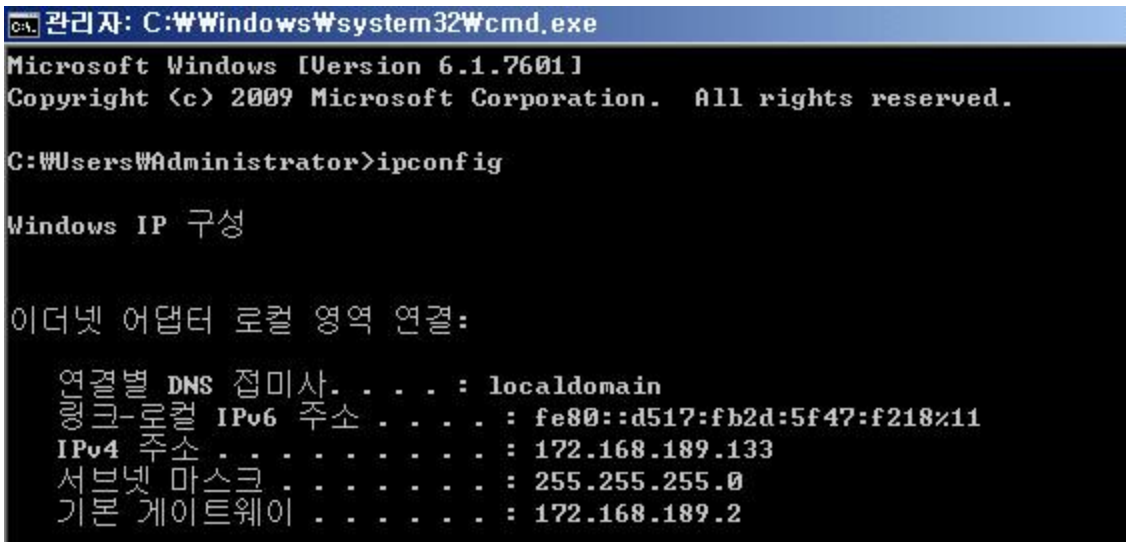
OS는 Operation System의 약자이며 운영체제를 뜻합니다.
IIS란 인터넷 정보 서비스를 뜻하며, 마이크로소프트 윈도우를 사용하는 서버들을 위한 인터넷 기반 서비스들의 모임을 의미합니다. 아파치 웹서버에 이어 세계에서 두 번째로 가장 잘 알려진 웹서버입니다. 지금까지 IIS 8.0버전이 나왔습니다(IIS 8.0은 Windows Server 2012, Windows 8부터 사용가능합니다). 장점이자 단점이라면 마이크로소프트에서 제공하는 윈도우 OS에서만 사용이 가능하다는 것입니다.
ASP는 Active Server Pages의 약자이며 PHP와는 다르게 윈도우의 IIS에서만 쓰이는 스크립트 언어(서버사이드 스크립트)를 의미합니다. 동적으로 서버에서 작동하는 페이지라고 생각하시면 되겠습니다. 반대로 반응에 의한 변화가 없고 고정적인 페이지라면 HTML이 있습니다.
MSSQL은 윈도우 서버에서만 구동이 되고 c#과는 가장 높은 호환성을 자랑하는 DBMS(데이터베이스를 관리해주는 시스템)입니다.

2) 원본 웹 서버와 옮겨갈 대상 서버 설명

각각의 서버는 현재 컴퓨터가 다르며 Windows 2000 서버가 현재 저희 회사의 서버이며 옮겨갈 대상은 Windows 2008 R2 서버입니다. 웹 사이트 이름은 webhack이라고 지정 되어있으며 웹해킹 교육실습용으로 이용하고 있습니다. 현재 이 사이트의 데이터베이스와 소스를 원본 서버(Windows 2000)에서 추출하여 마이그레이션을 할 대상 서버인 Windwos 2008 R2 서버로 옮깁니다. 다음은 각각 서버의 IP정보입니다. 이것은 로컬의 주소, 즉 웹 서버의 IP를 의미합니다.



<그림2> Windows 2000 서버의 IP 정보(ipconfig)



<그림3> Windows 2008 R2 서버의 IP 정보(ipconfig)

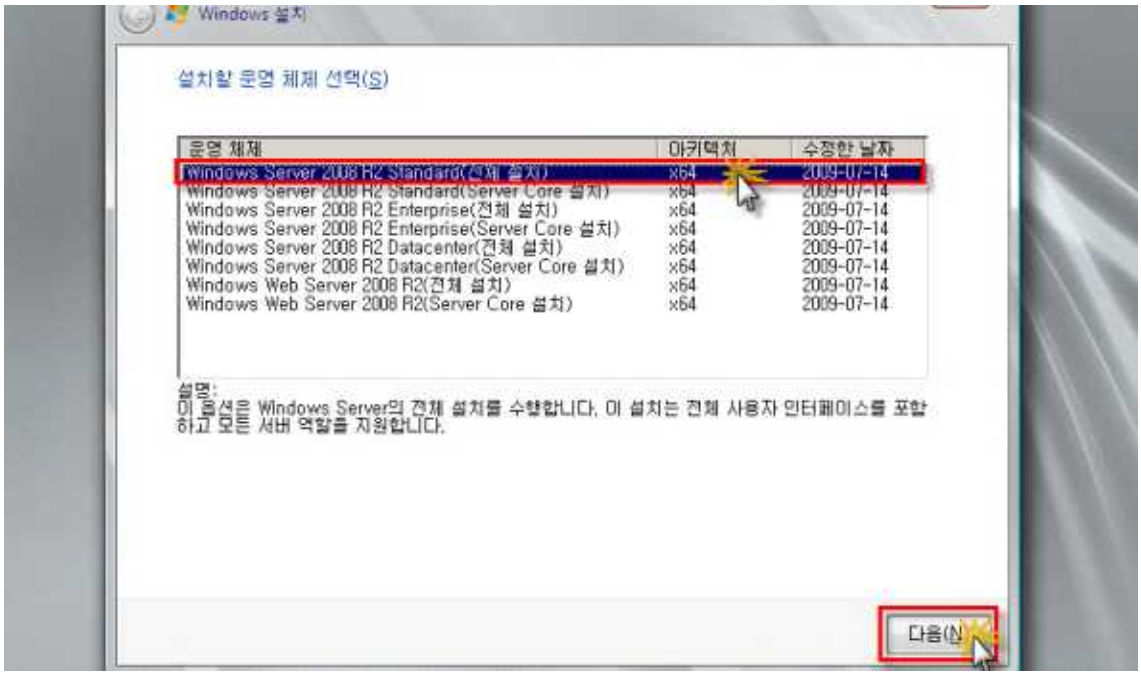
3. 대상 서버(Windows Server 2008 R2) 구축

1) 서버 OS 설치

<그림4>Windows Server 2008 R2 DVD나 CD를 넣고 부팅합니다.

<그림5>다음 화면에서 지금 설치를 클릭합니다.

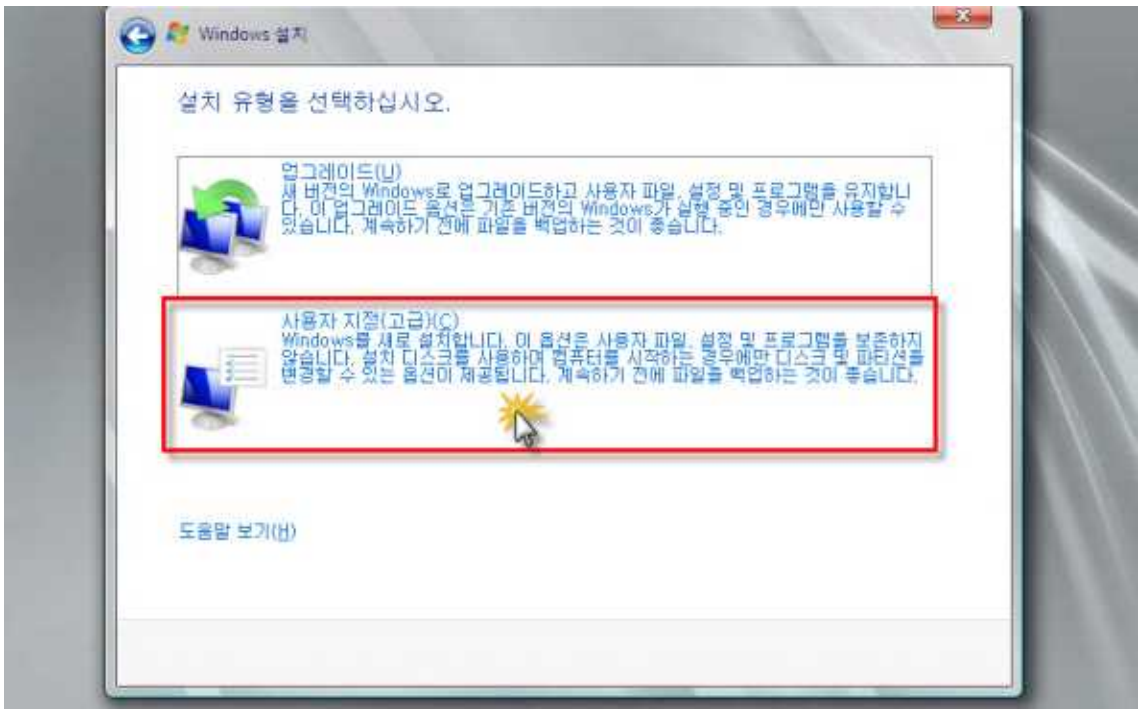
<그림6>설치 프로그램의 시작이 진행됩니다.



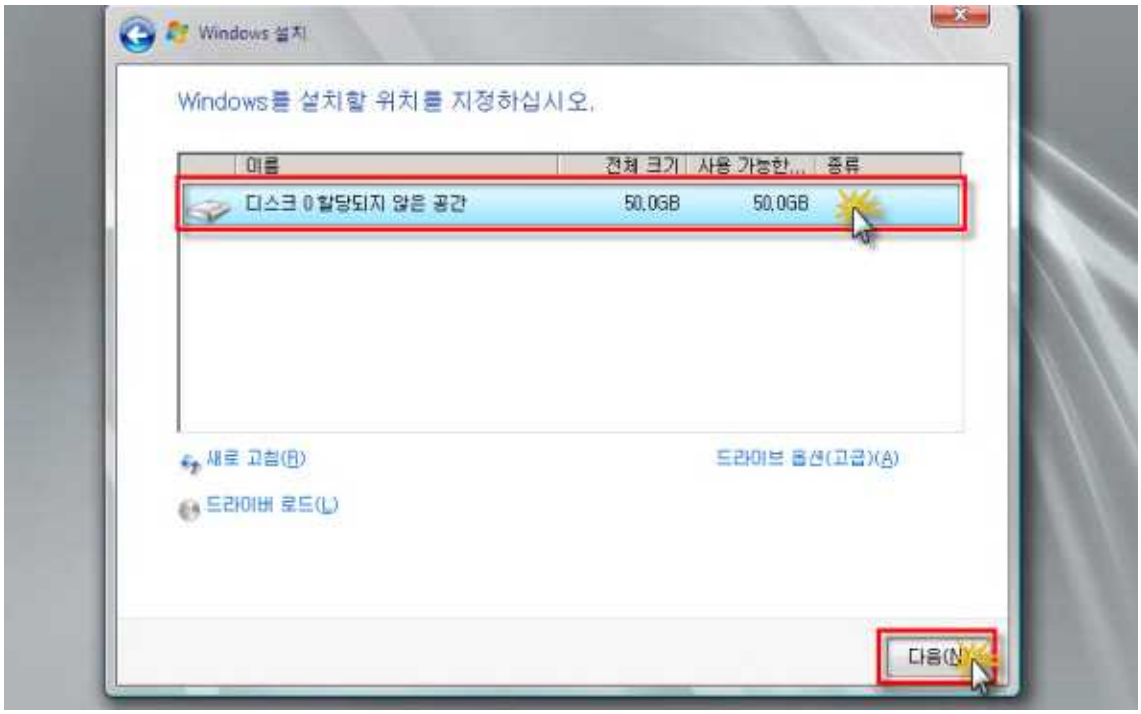
<그림7>설치 가능한 라이센스의 OS버전을 선택한후 다음을 클릭합니다.

저희는 Standard(전체설치)를 채택하였습니다.

<그림8>사용권 계약서를 읽어본 후 동의함에 체크하고 다음을 클릭합니다.



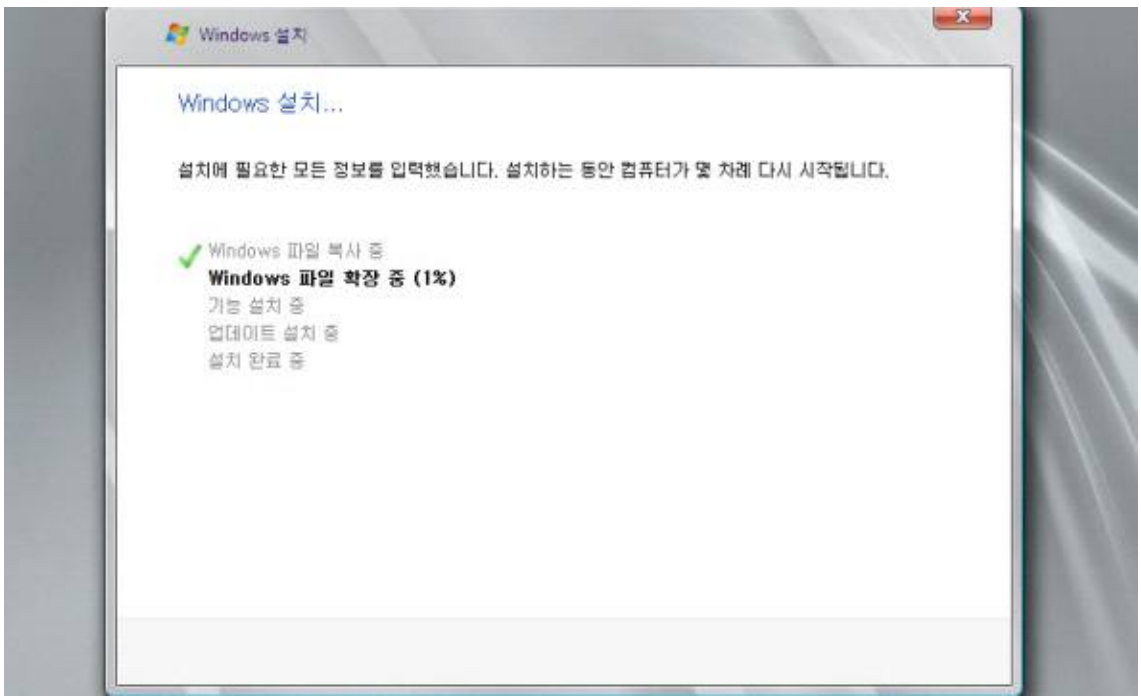
<그림9>처음 설치하는 경우 사용자 지정(고급)을 클릭합니다.



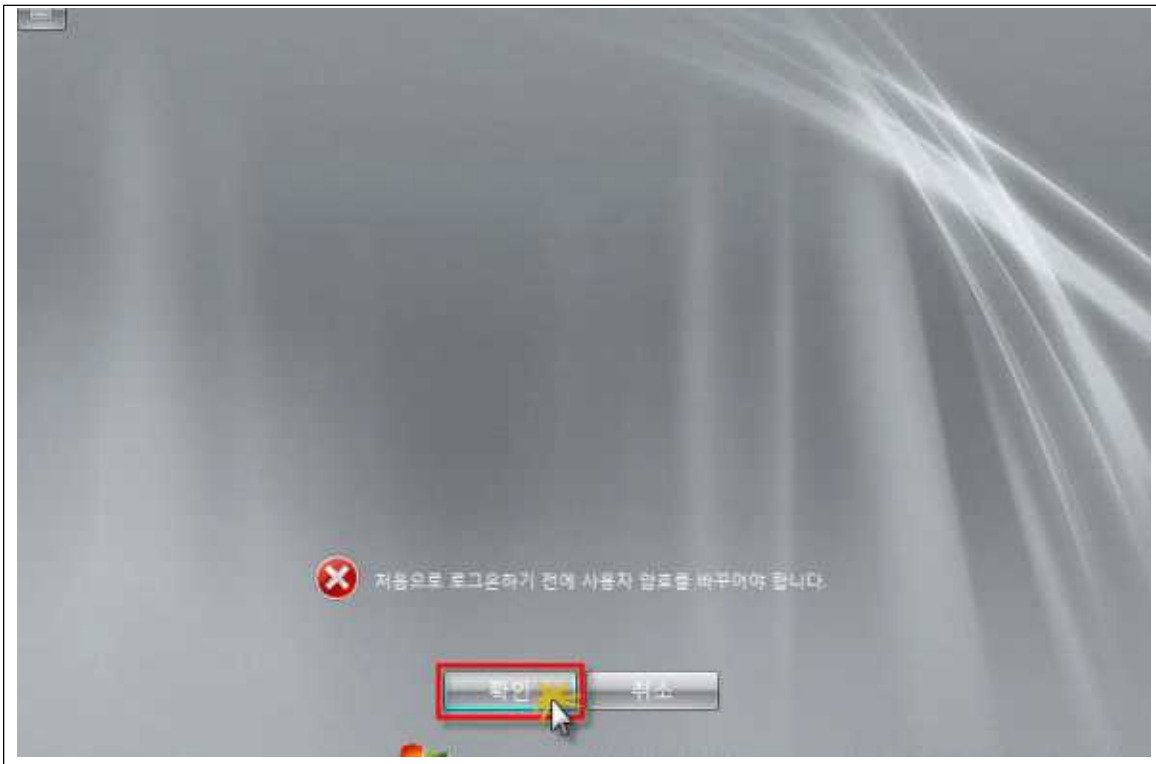
<그림10>설치할 드라이브를 선택한 후 다음을 클릭합니다.

-드라이브 옵션 : 디스크 파티션을 여러 개로 분할 할 수 있는 메뉴가 활성화됩니다.

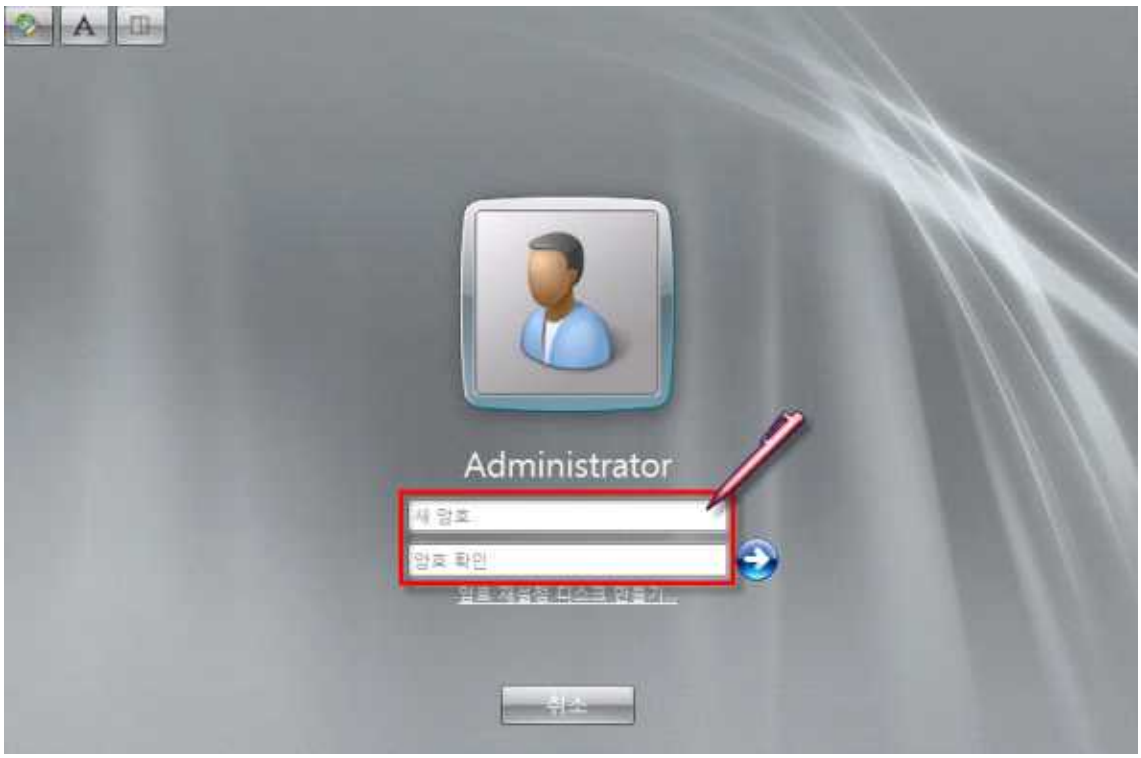
-드라이버 로드 : SAS 및 RAID컨트롤러의 드라이버를 설치 전에 로드 할 수 있습니다.



<그림11>설치를 시작 합니다. 이 과정 후에 재부팅이 강제로 진행됩니다.

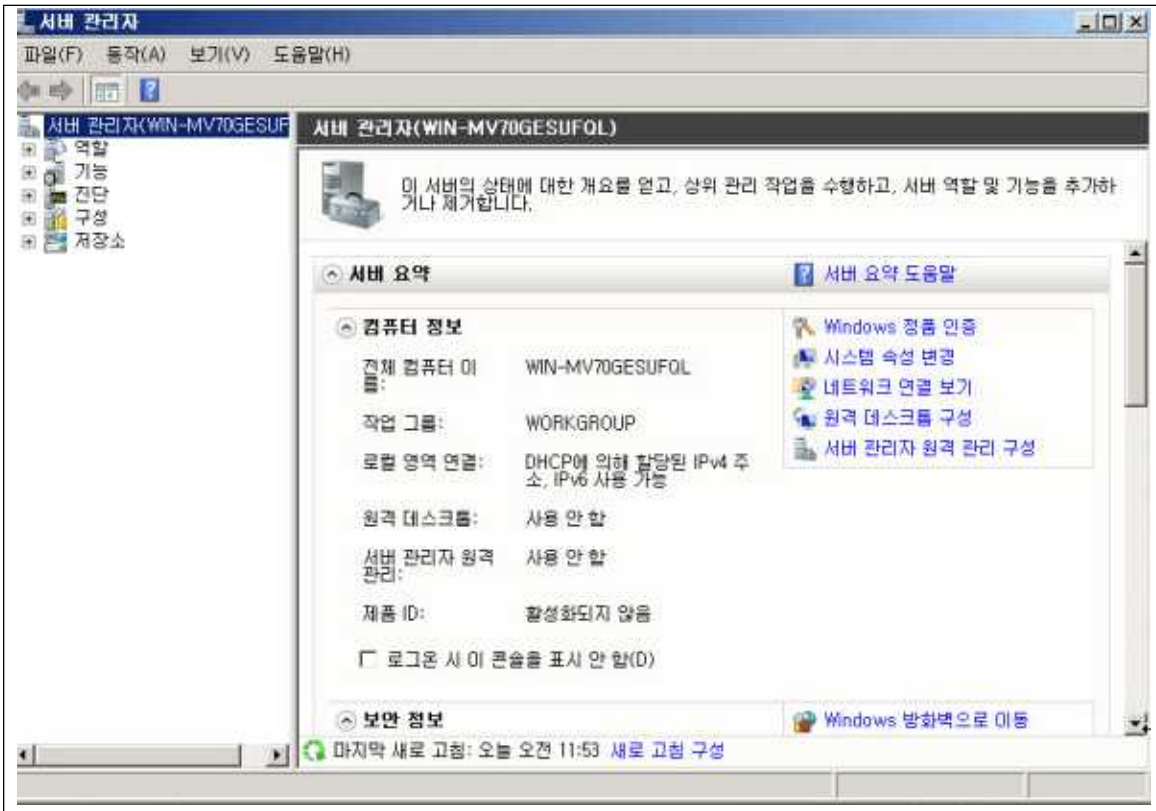


<그림12>재부팅 후 처음 사용을 위한 화면이 나타납니다. 확인을 클릭합니다.



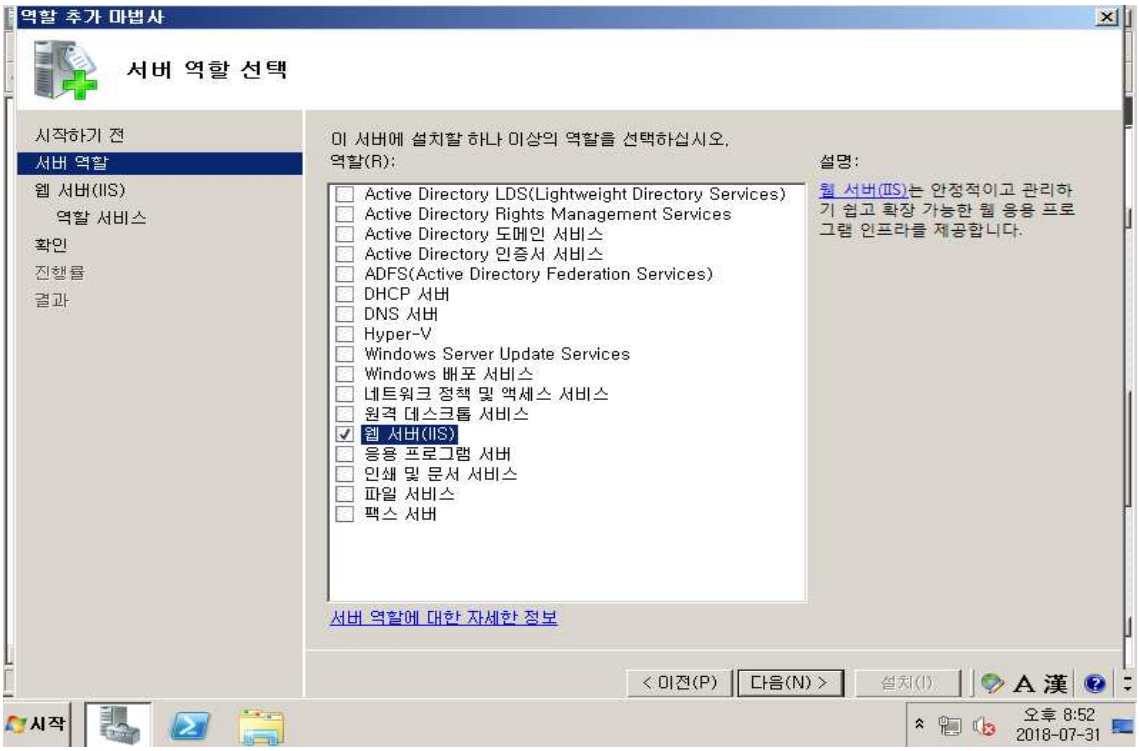
<그림13>Administrator 암호를 설정합니다.

Windows Server 2008의 암호정책은 강력합니다. 따라서 영문,숫자,특수문자를 조합해야합니다.

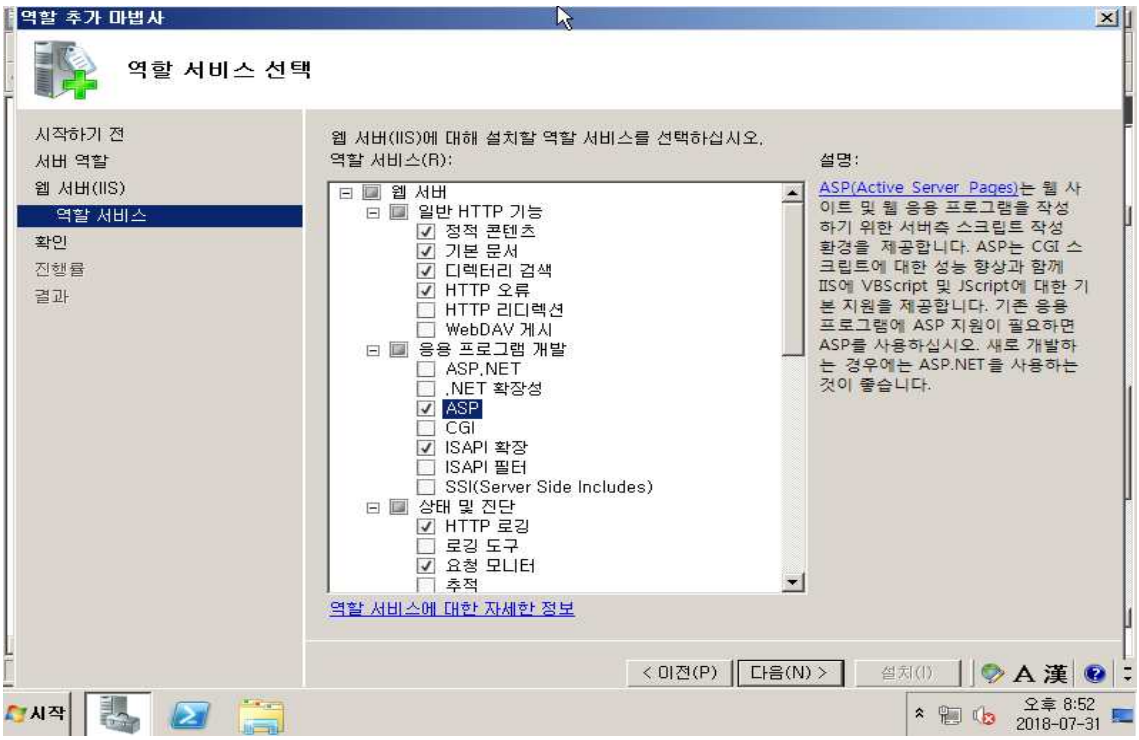


<그림14>서버 관리자의 화면을 확인후에 닫아줍니다. 기본적인 OS 설치가 완료되었습니다.

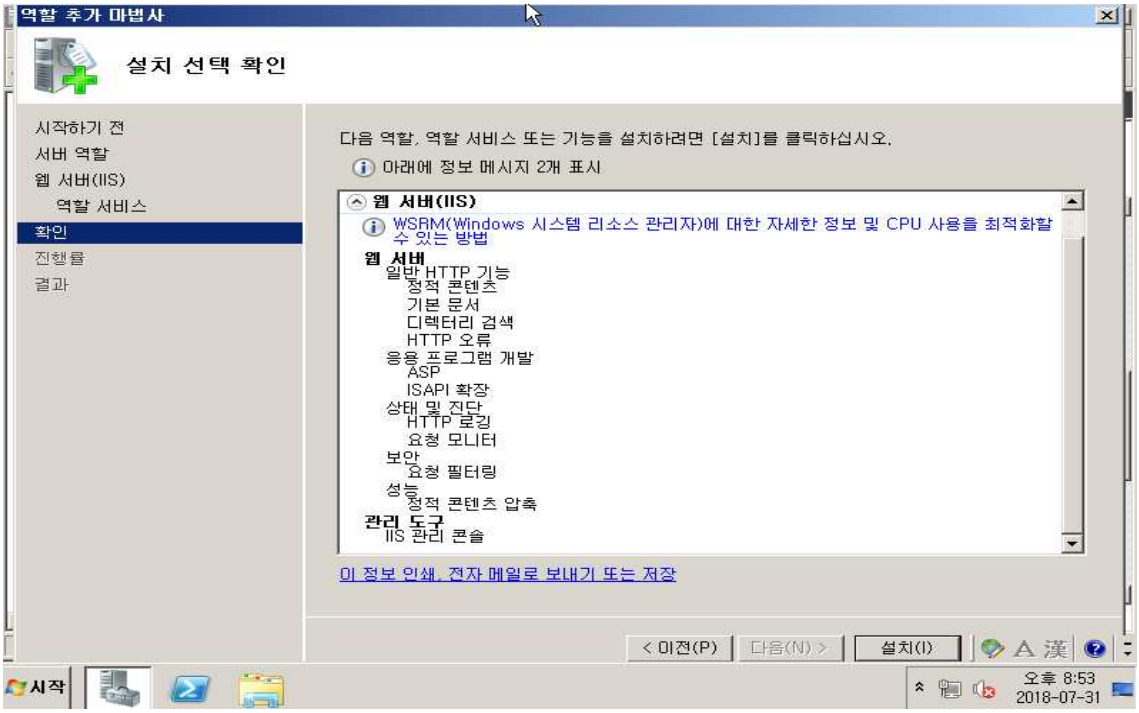
2) IIS 기능 설치



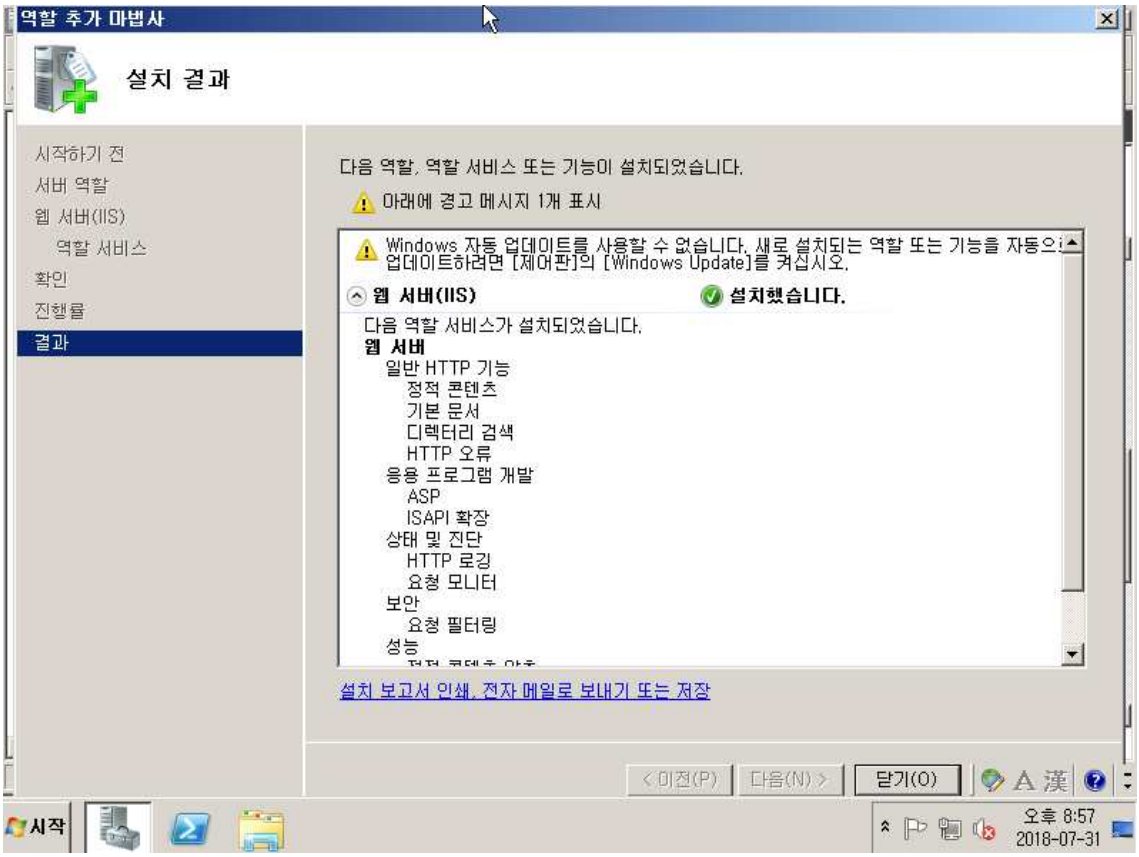
<그림15>서버 관리자에 접속하여 역할 추가를 선택합니다. 웹 서버(IIS)를 클릭합니다.



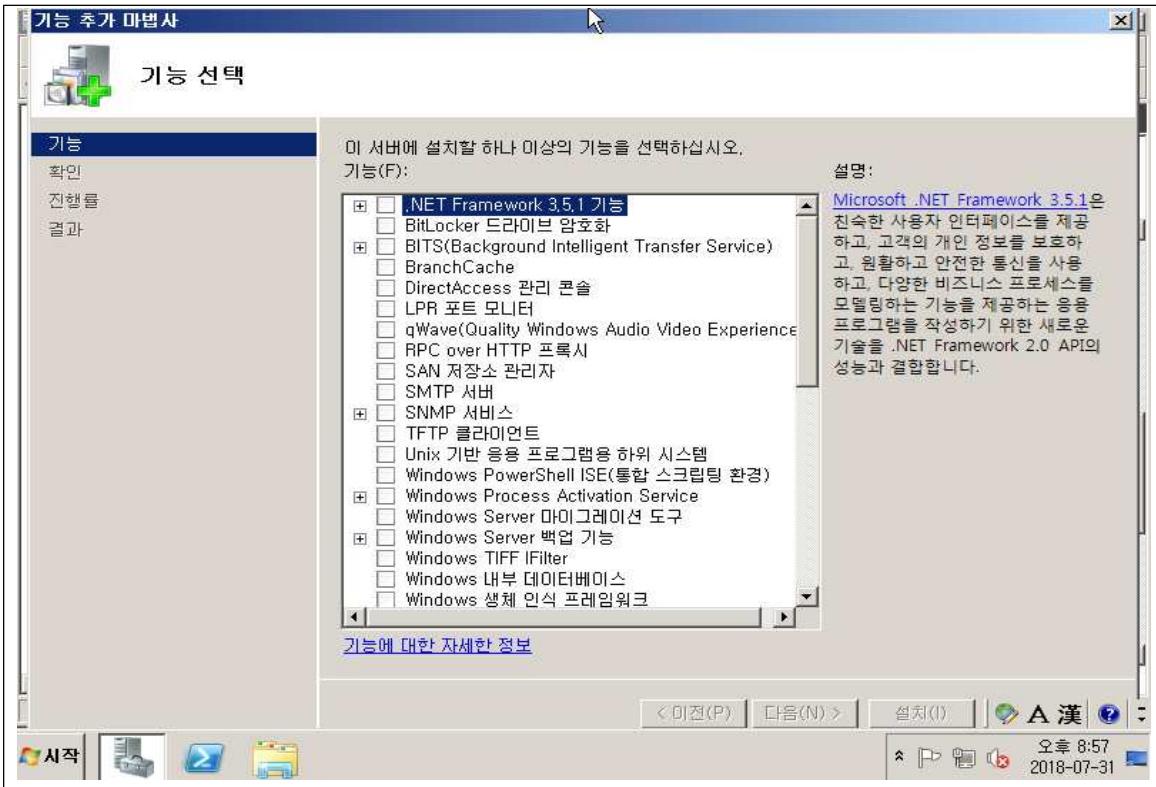
<그림16>웹 서버의 역할 서비스 중 ASP와 ISAPI 확장을 클릭합니다.



<그림17> IIS 설치를 진행할 서비스 항목들을 체크합니다.

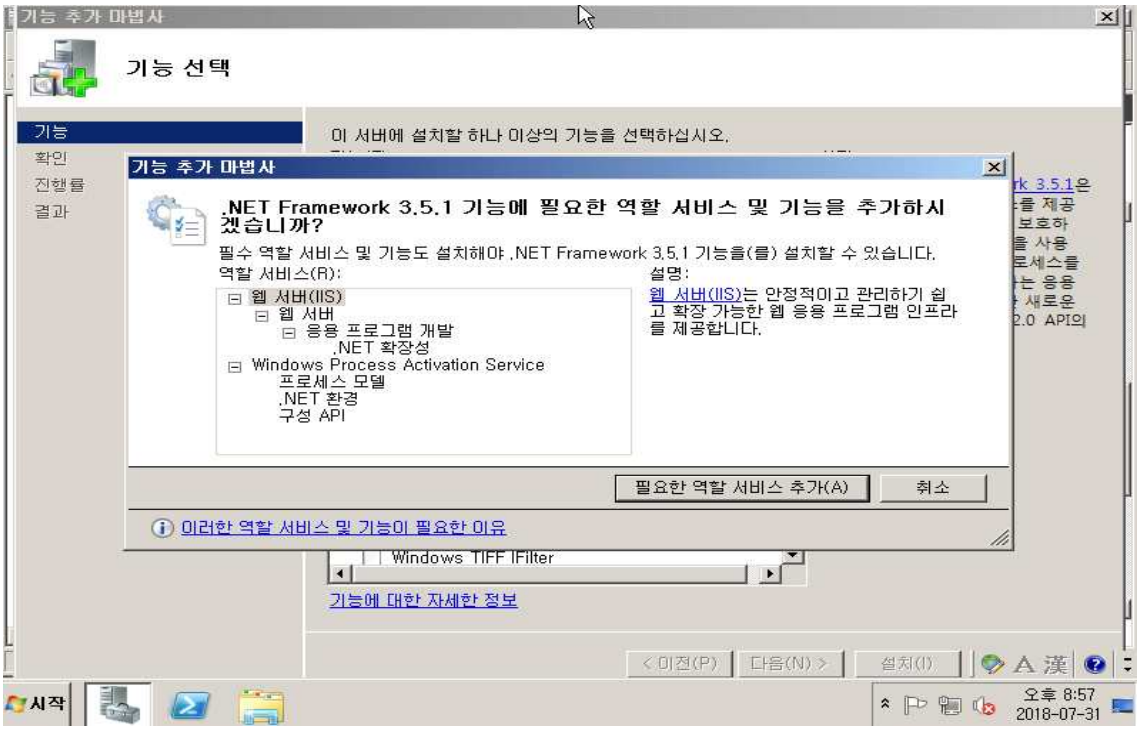


<그림18> IIS 기능 설치가 완료된 결과 모습입니다.

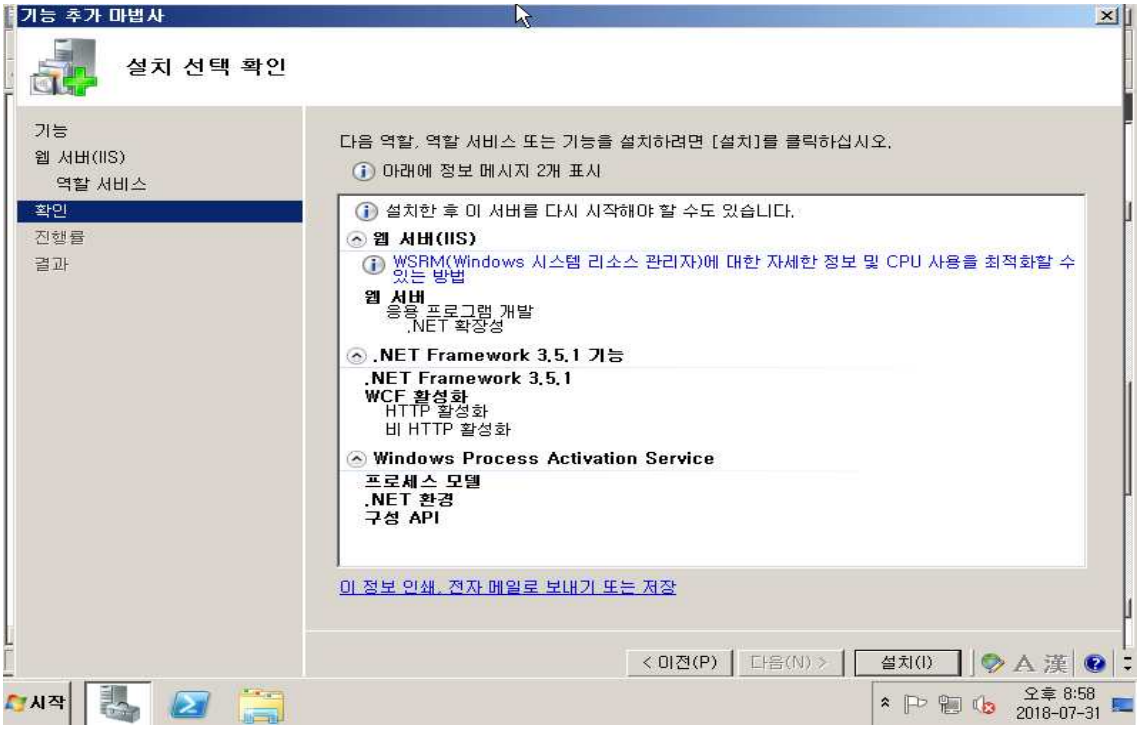


<그림19> 기능 추가를 클릭합니다. .NET Framework 3.5.1 기능을 설치 클릭 합니다.

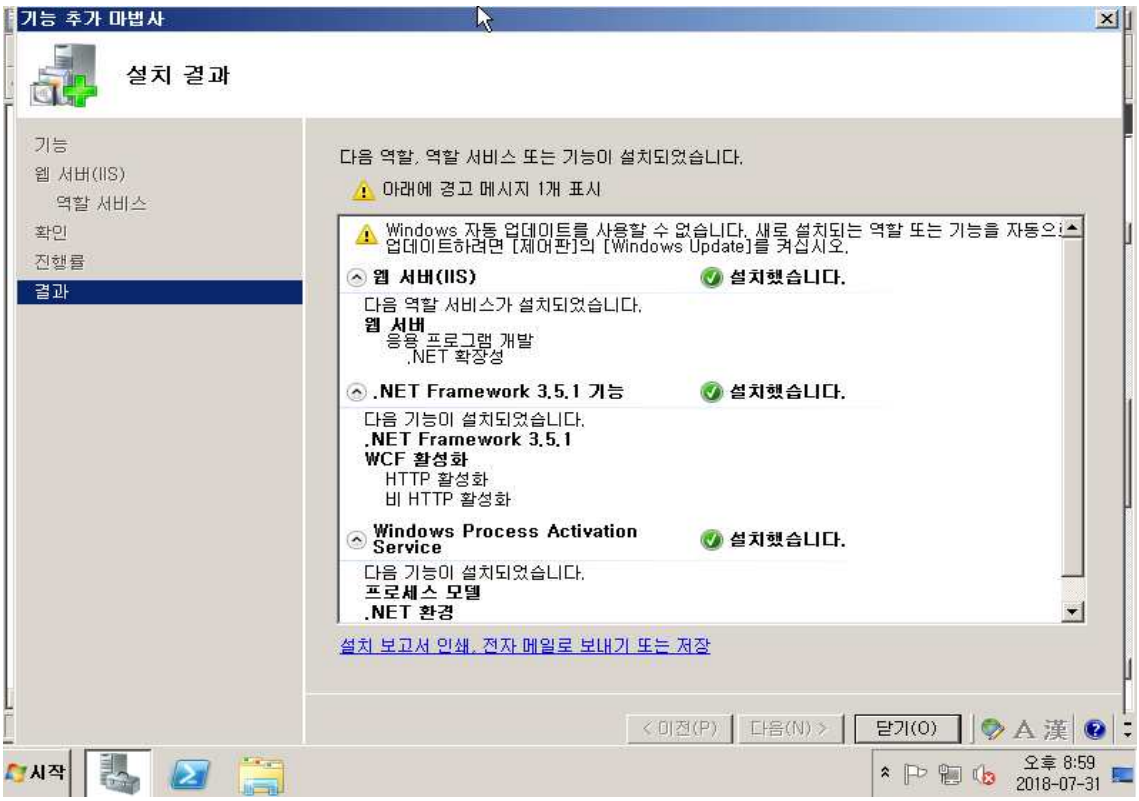
이것은 IIS를 좀 더 안정적으로 사용하기 위한 기능으로서, 애플리케이션의 개발과 실행 시 언어에 종속적이지 않은 플랫폼을 제공하기 위해 개발된 것입니다.



<그림20> 필요한 역할 서비스 추가를 클릭합니다.



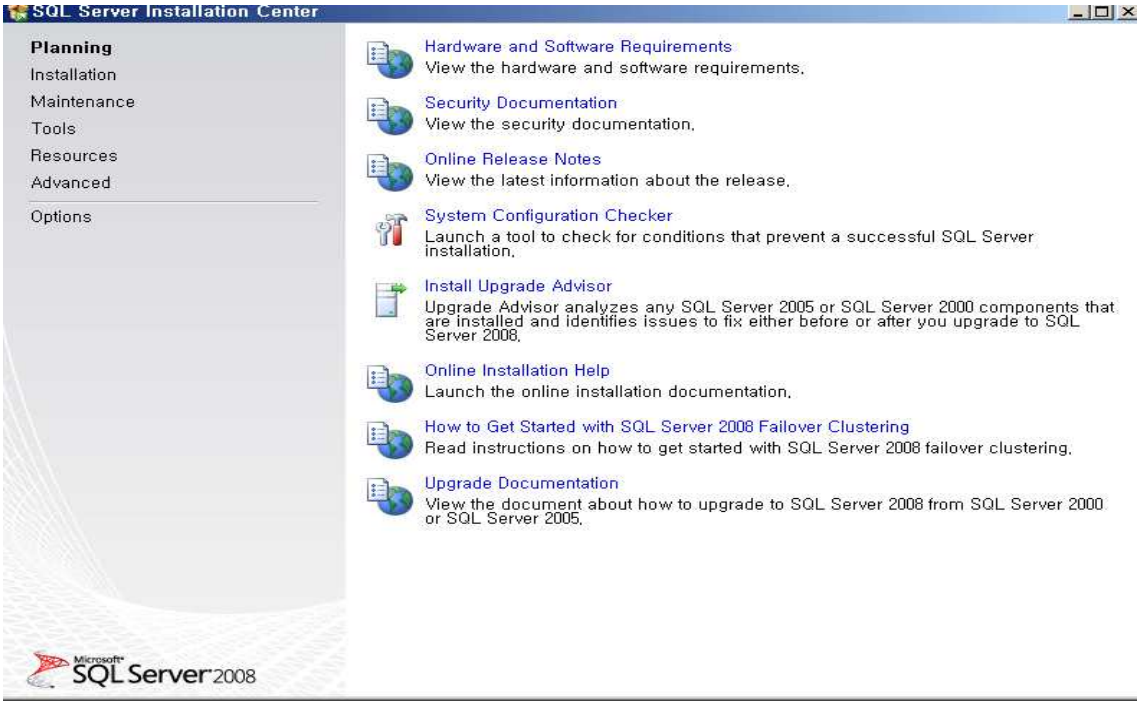
<그림21> 설치할 항목을 체크합니다.



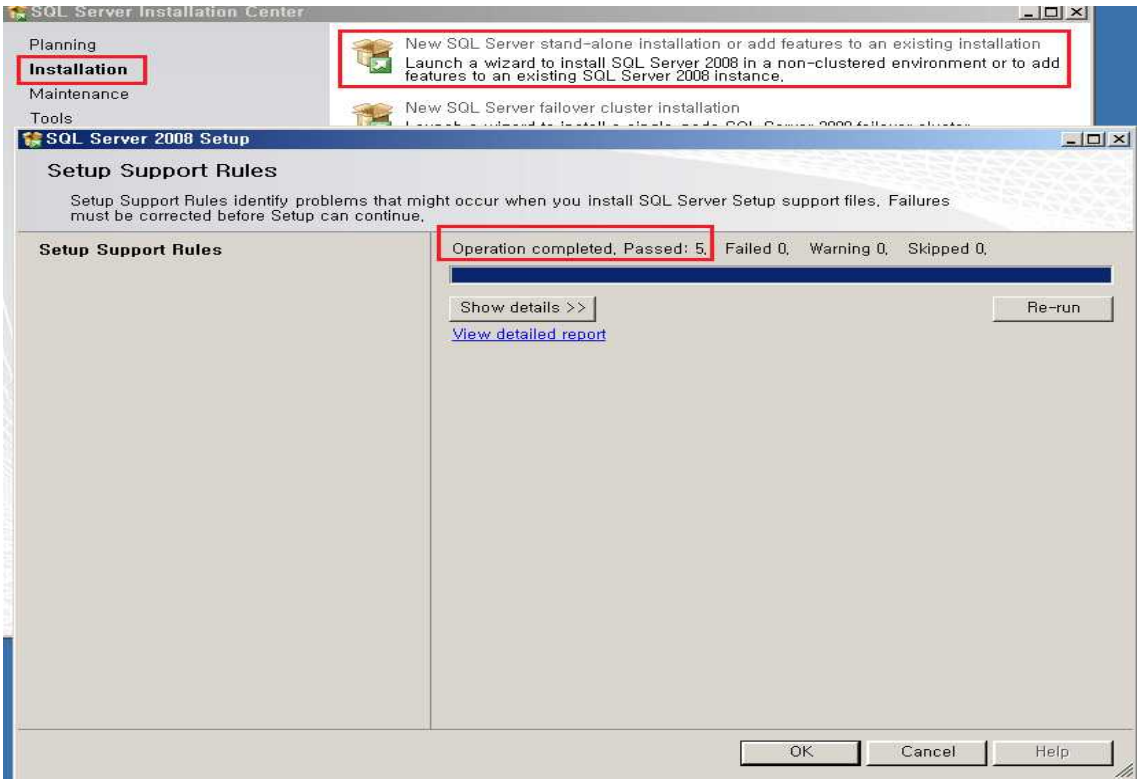
<그림22> 기능 추가를 완료한 모습입니다.

3) MSSQL(SQL Server 2008) 데이터베이스 설치 및 설정

SQLFULL_ENU_x64를 다운 받은 후에 CD를 실행합니다.

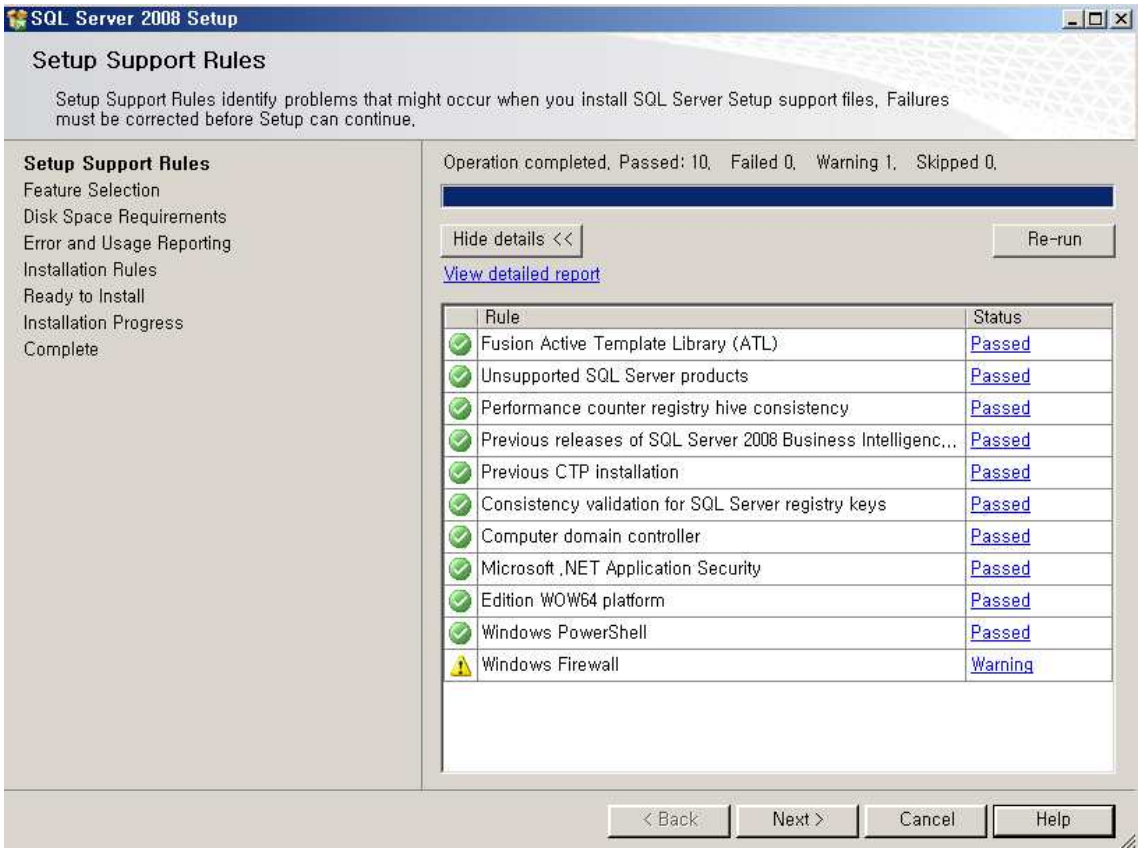


<그림23> CD를 실행후 초기 다운 설정 화면입니다.

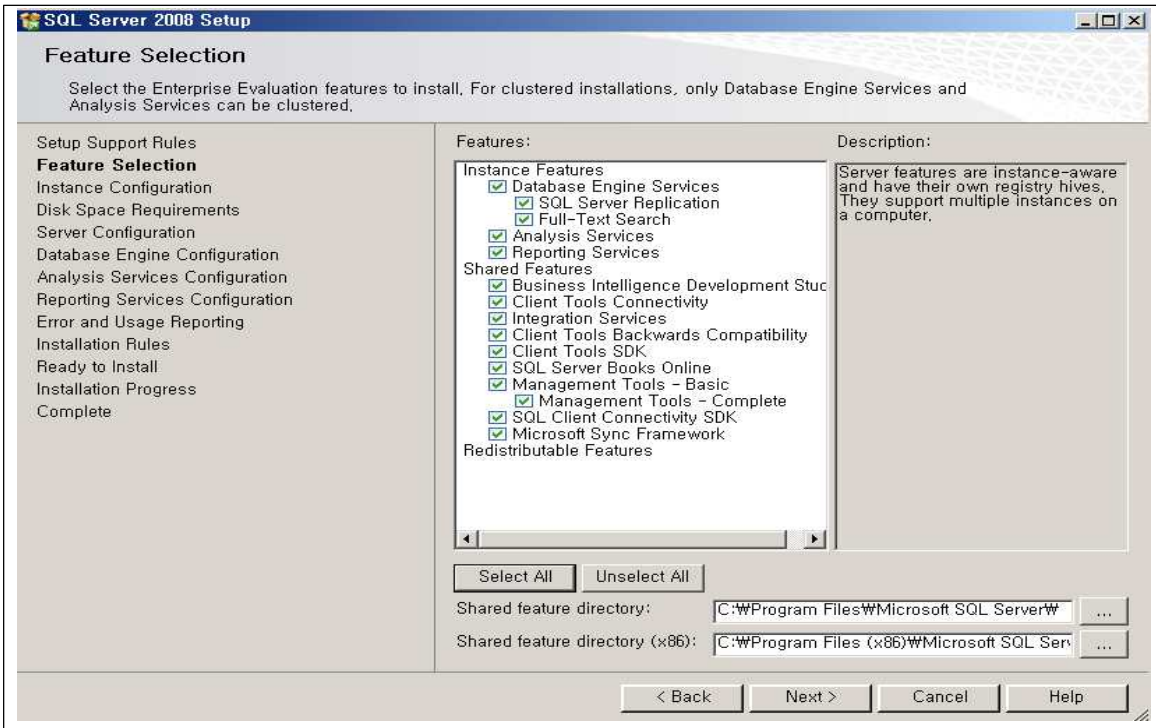


<그림24>Installation > SQL server stand-alone(단독실행형) 설치 완료후 확인합니다.

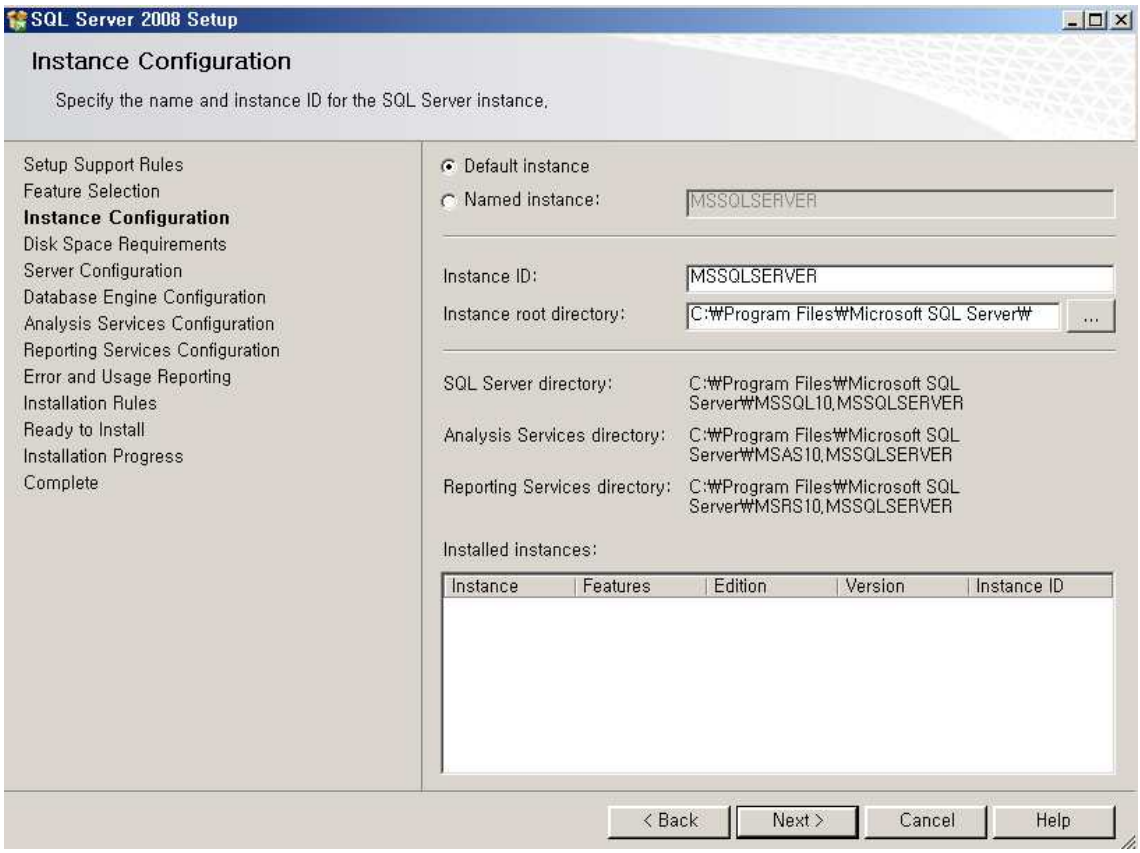
<그림25> CD-key를 입력하신 후에 라이센스를 읽어보신 후 동의합니다.



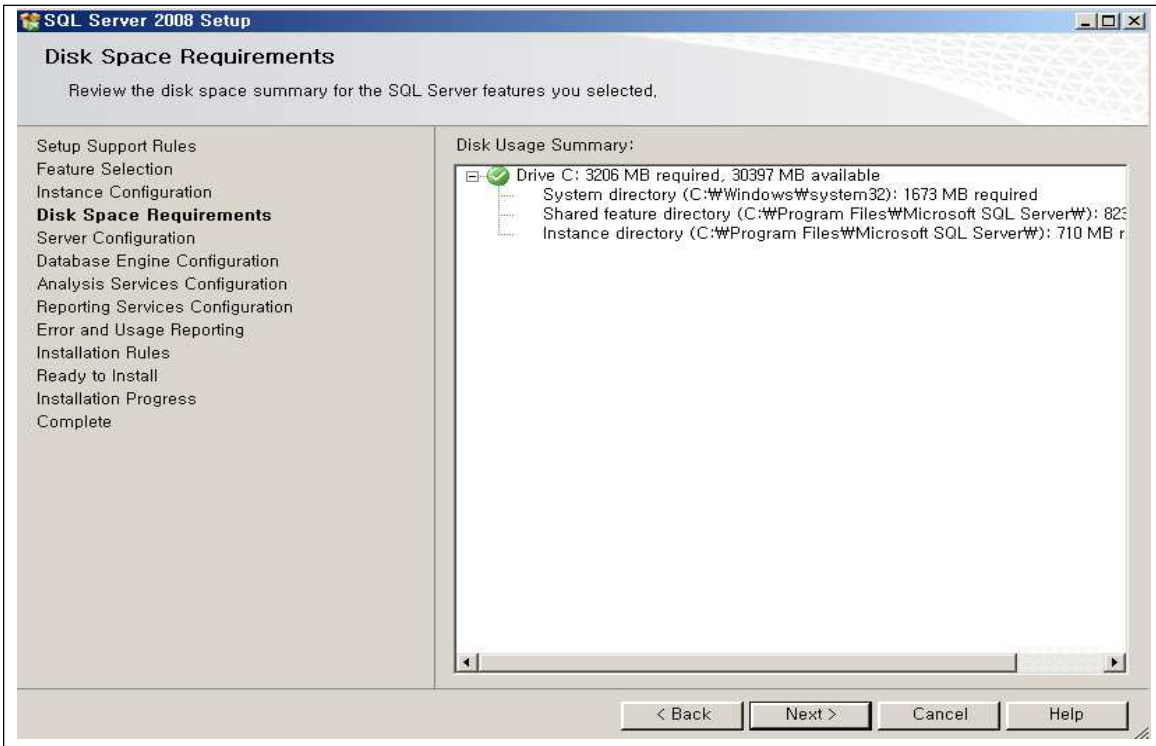
<그림26>Install 실행창이 다운되고 실행된 모습입니다.



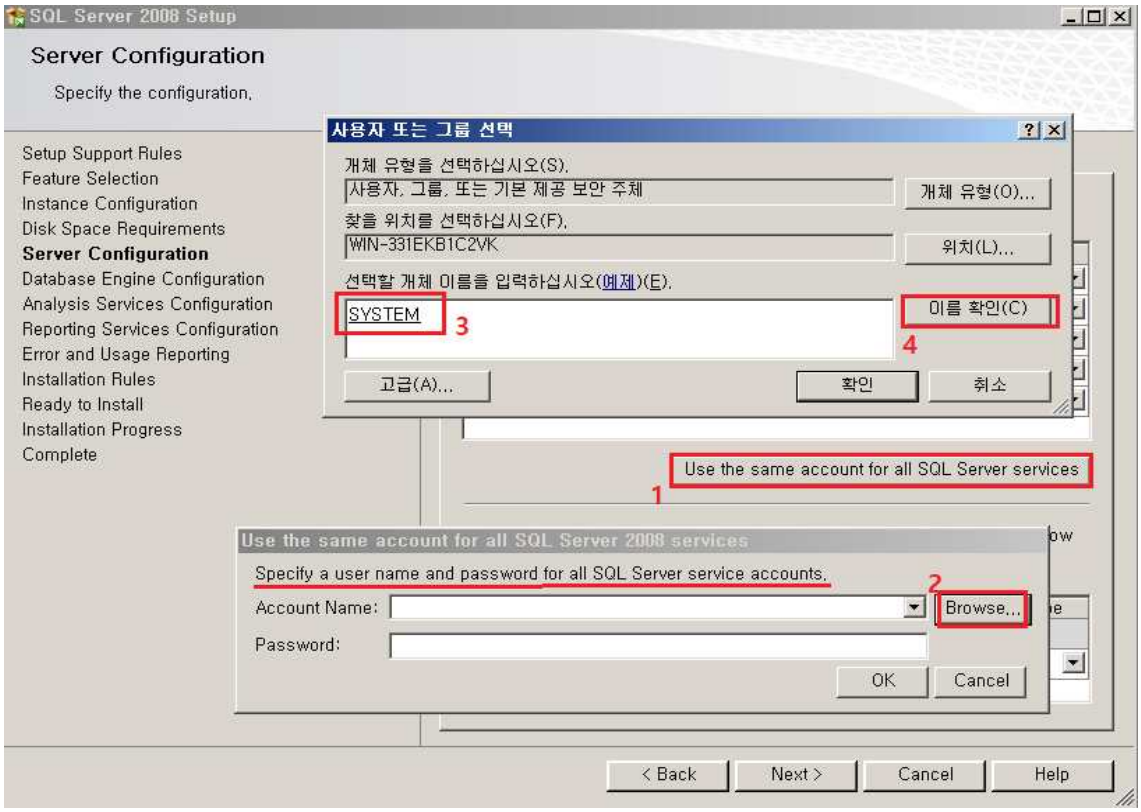
<그림27> 구성요소는 모두 선택합니다.



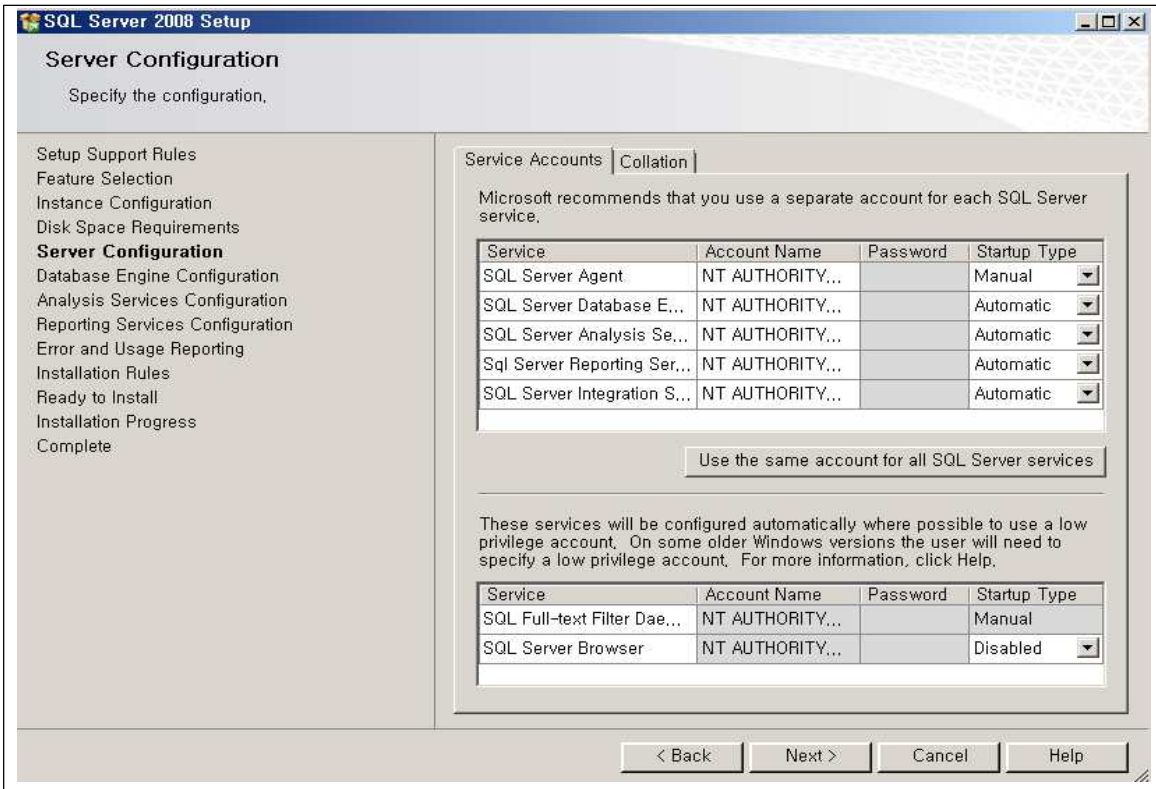
<그림28> Instance값은 모두 디폴트 값으로 설정하고 넘어갑니다.



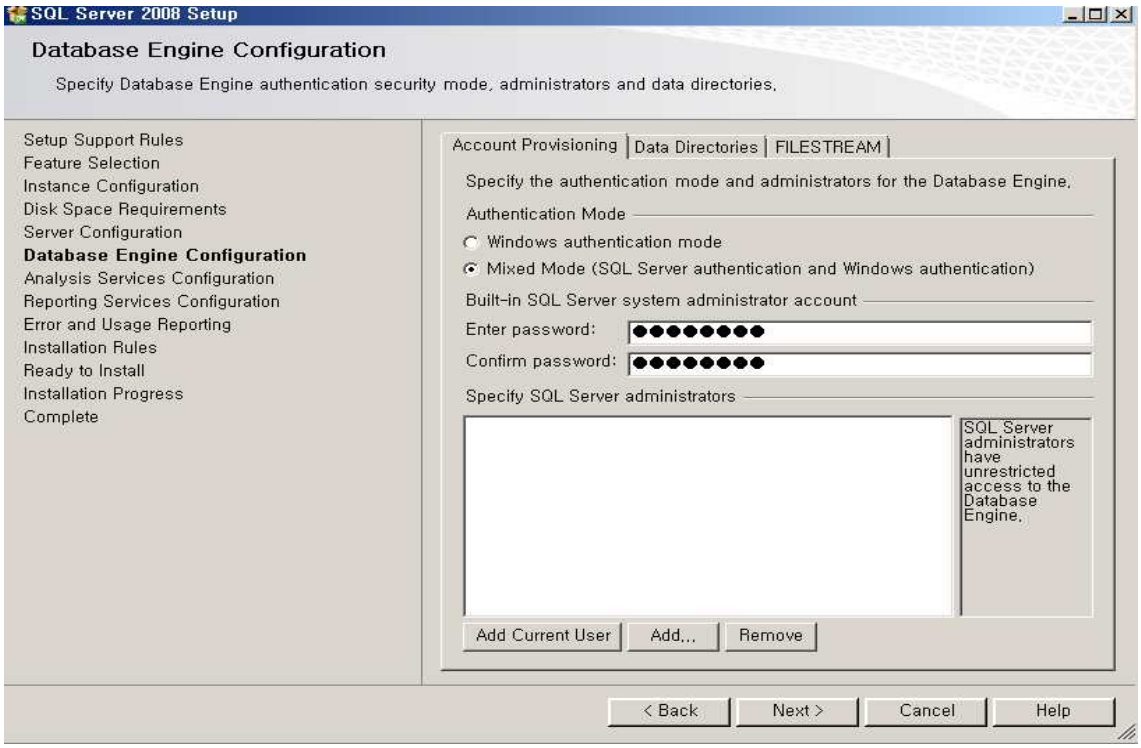
<그림29> 디스크 할당량을 확인합니다.



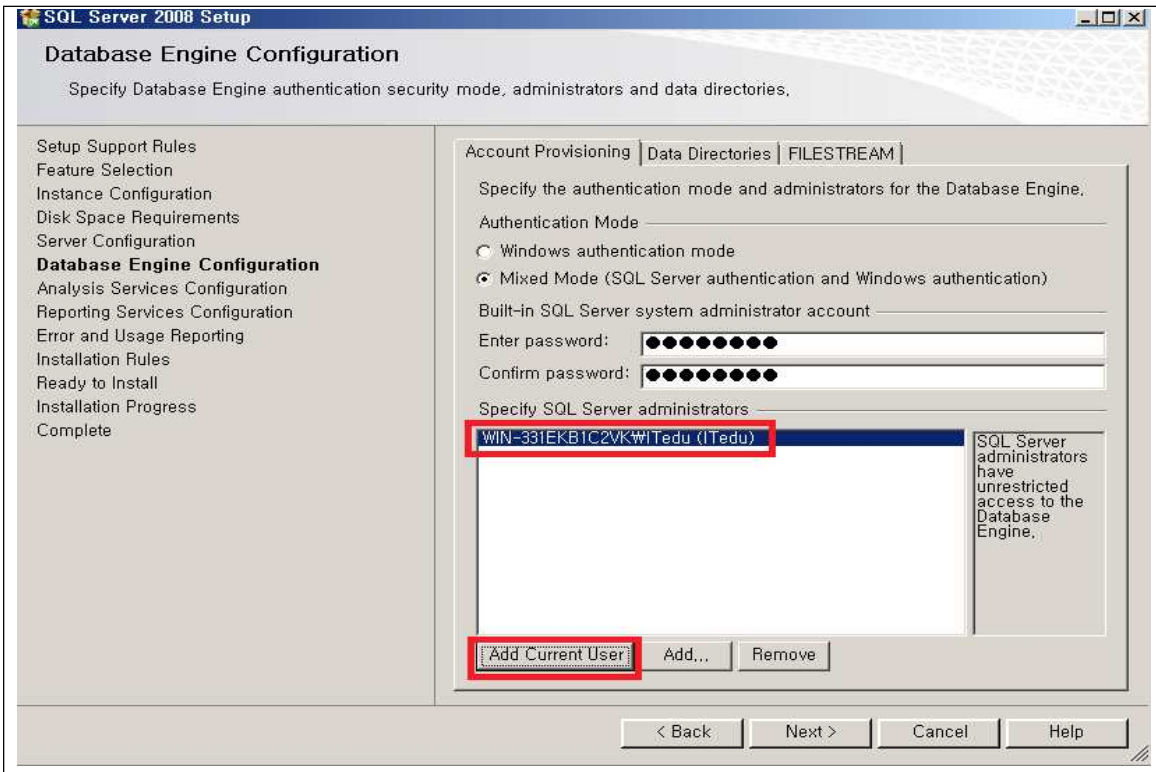
<그림30> SQL server서비스의 계정 사용자를 SYSTEM계정 하나로 묶습니다.



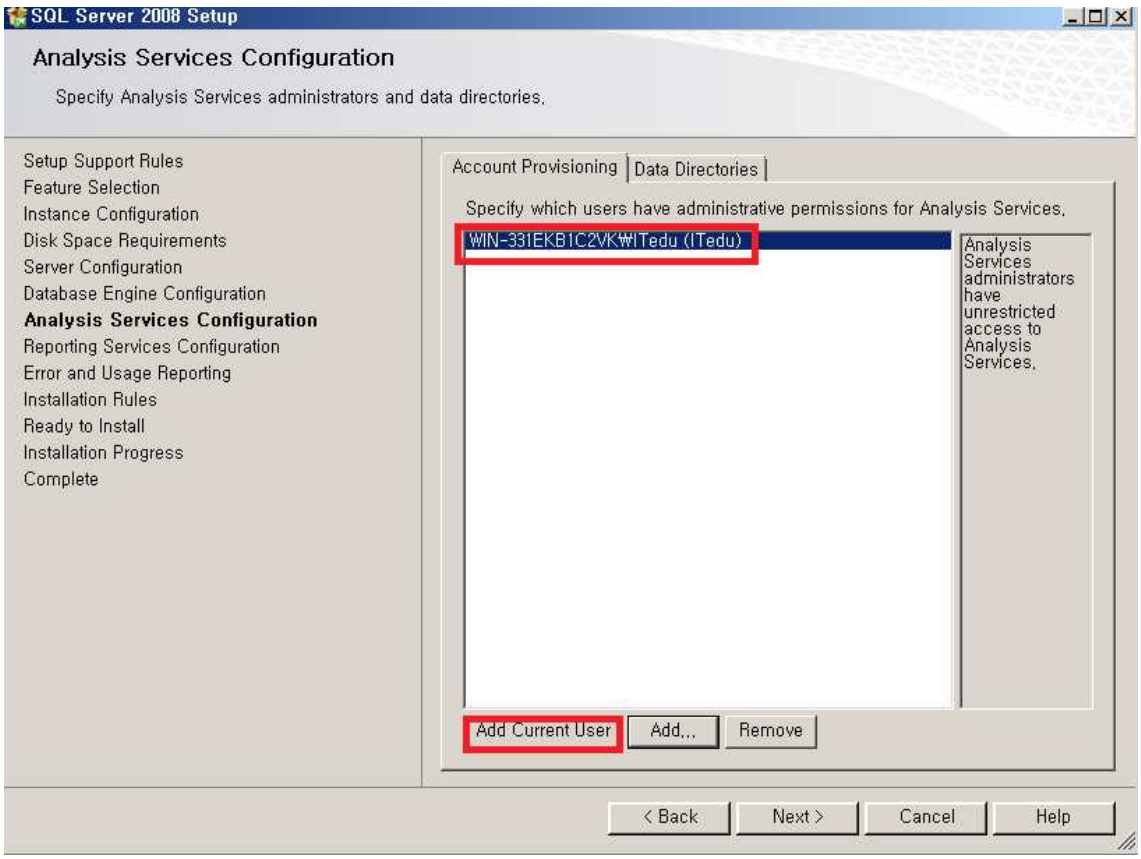
<그림31> 설정 후 비밀번호는 설정하지 않고 다음으로 넘어갑니다.



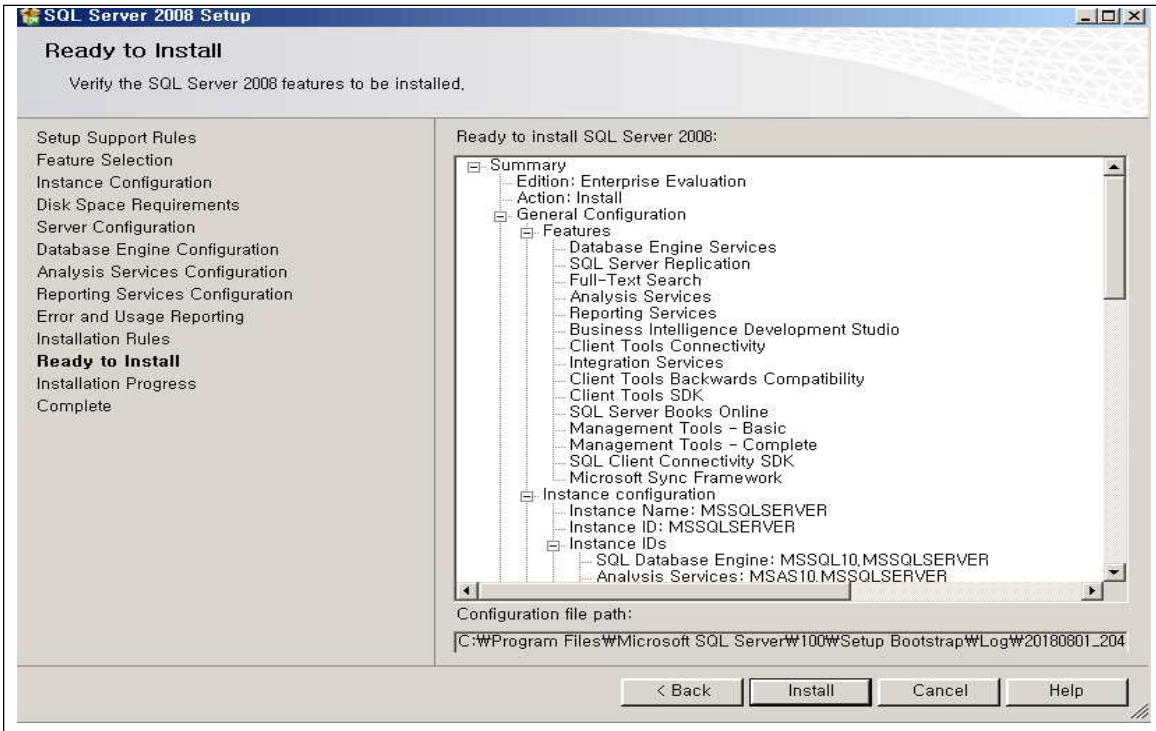
<그림32> Mix모드로 윈도우계정과 SQL계정을 통합합니다. 이때 패스워드는 윈도우 관리자계정의 패스워드인데 암호 복잡성을 따져서 만듭니다.



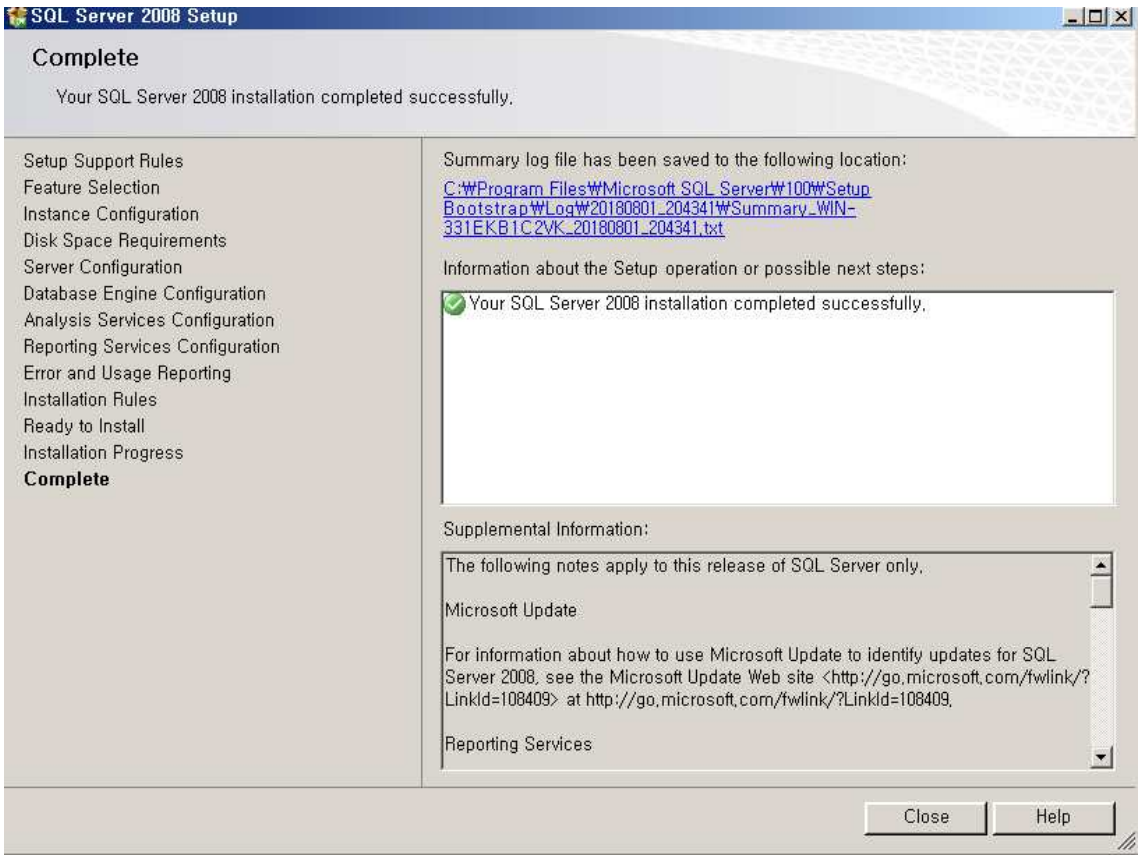
<그림33> Add Current User 클릭 후 현재 사용자계정(관리자)을 추가합니다.



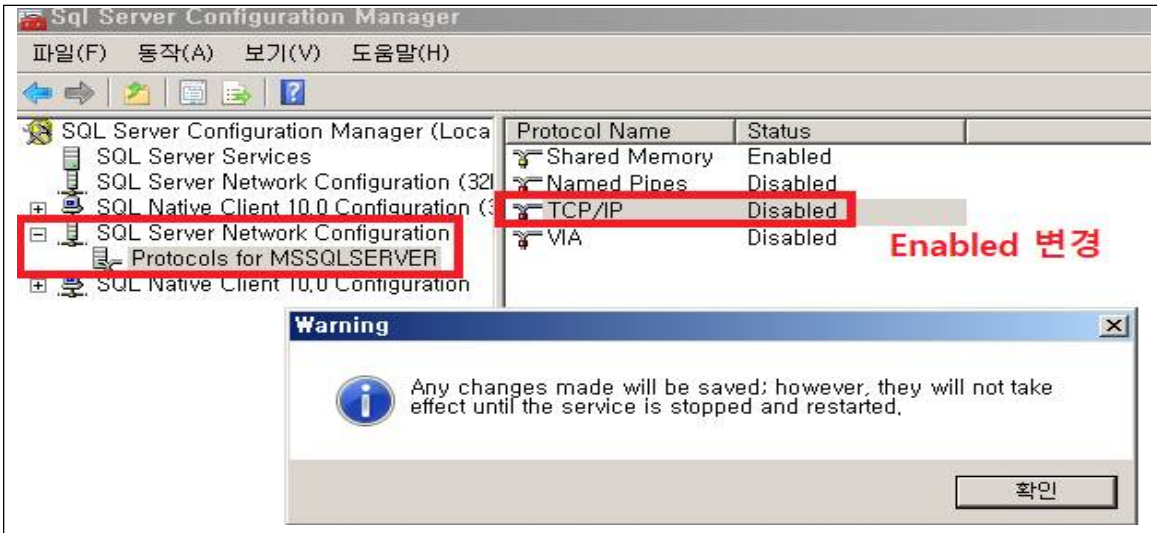
<그림34> 위와같이 Add Current User를 클릭하여 추가합니다.



<그림35> 나머지 매뉴얼은 디폴트값으로 다 넘어가신 후에 Install하게 될 목록들을 체크합니다.

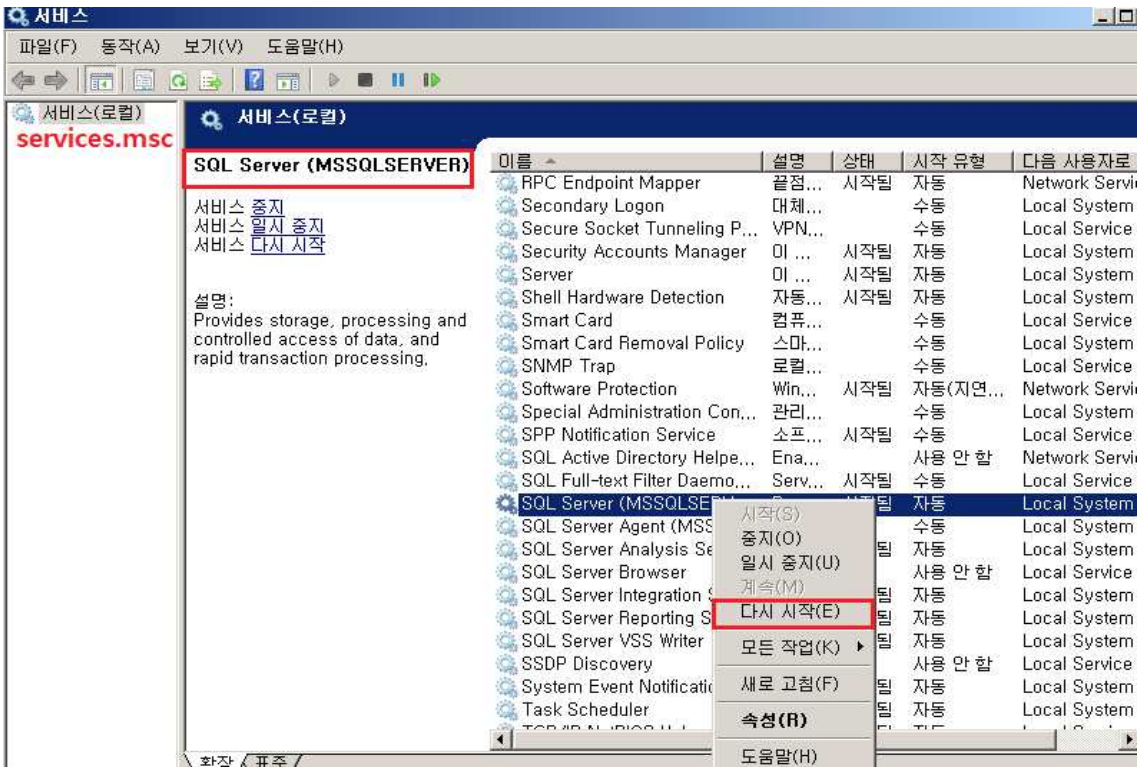


<그림36> 설치가 완료된 후 재부팅 합니다.



<그림37> 설치가 끝났으면 Configuration Manager로 가셔서 SQL Server Network Configuration에 Protocols for MSSQLSERVER로 들어가신 후 TCP/IP를 Enabled로 변경합니다. 서비스를 재시작 하라고 경고 문구가 뜹니다.

(경로 : 시작 > 모든 프로그램 > Microsoft SQL server2008 > Configuration Tools)

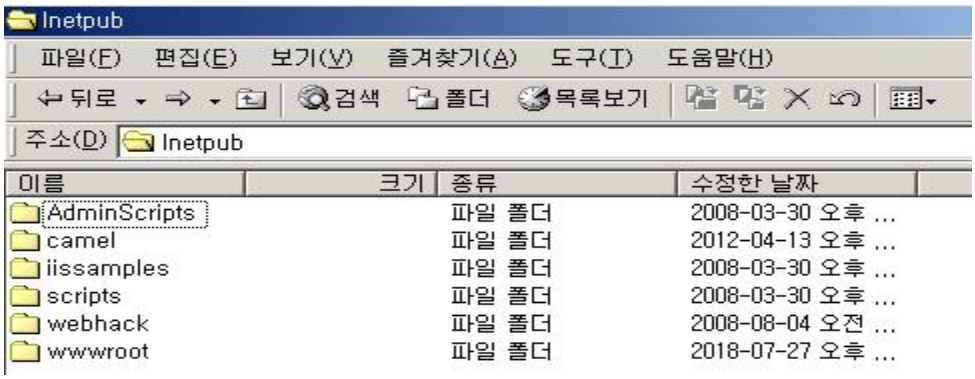


<그림38> 경고 문구에 따라 services.msc로 실행하신 후 SQL Server(MSSSQLSERVER)를 재시작 합니다. 이로 설치와 기본 설정이 완료되었습니다.

4. 원본 서버 백업파일 형성(Windows 2000 Server)

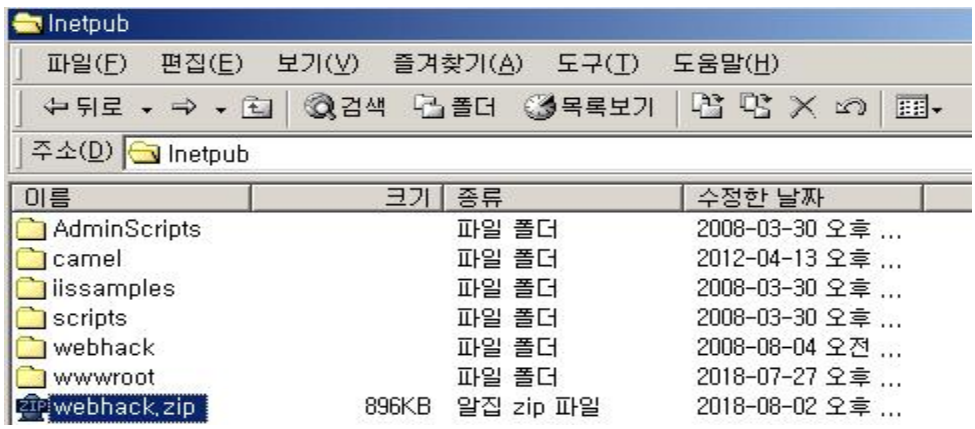
1) 소스 백업파일 형성

이동작업을 하기 이전에 먼저 본 서버에서 webhack서버의 소스자료 부터 백업합니다.



<그림39> C드라이브 > Inetpub 으로 가시면 webhack 파일 폴더가 있습니다. 이것을 백업파일 용도로 압축합니다.

<그림40> webhack 폴더의 내부 소스 자료 모습입니다.

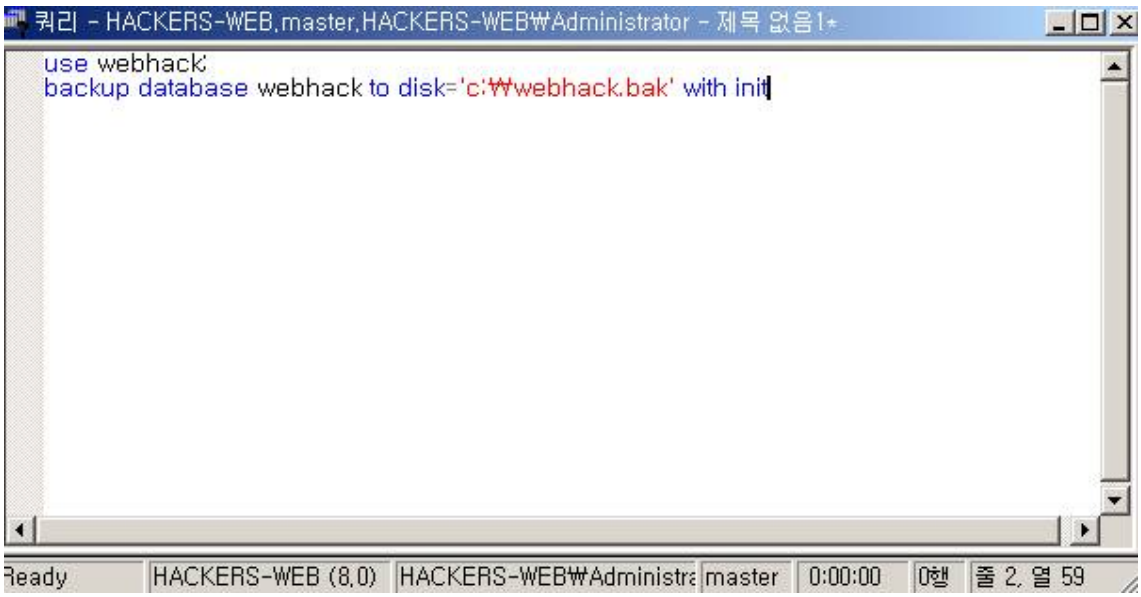


<그림41> 알집으로 압축한 파일을 Window 2008 server로 옮기기 위해 이동식 디스크에 따로 저장합니다. FTP를 이용하셔도 됩니다.

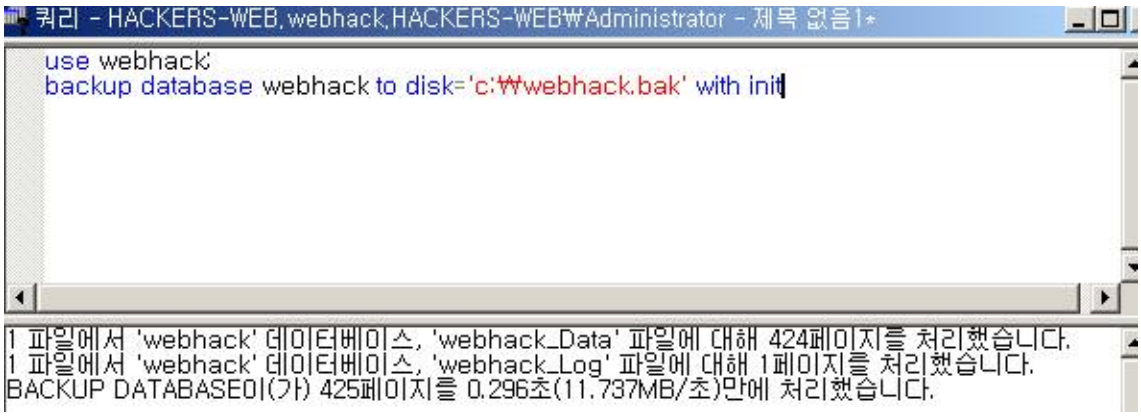
2) 데이터베이스 백업파일 형성

데이터베이스는 SQL Server로 접속하여 .bak 파일의 형태로 백업합니다.

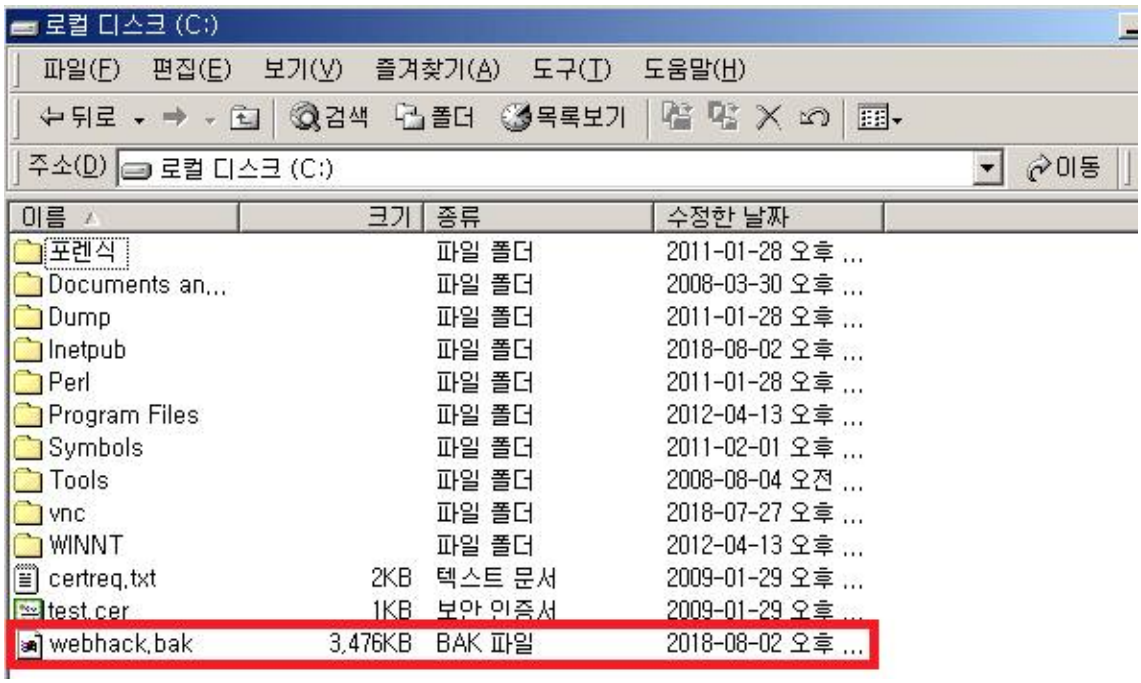
<그림42> 시작 > 프로그램 > Microsoft SQL Server로 가셔서 쿼리분석기를 실행하신 후에 윈도우 인증으로 접속합니다.



<그림43> 백업파일을 형성하기 위한 구문을 쿼리에 작성하신 후 F5을 눌러 실행합니다.



<그림44> 정상적으로 처리 된 것을 확인합니다.



<그림45> C드라이브에 webhack.bak 형태로 저장되었는지 확인합니다.

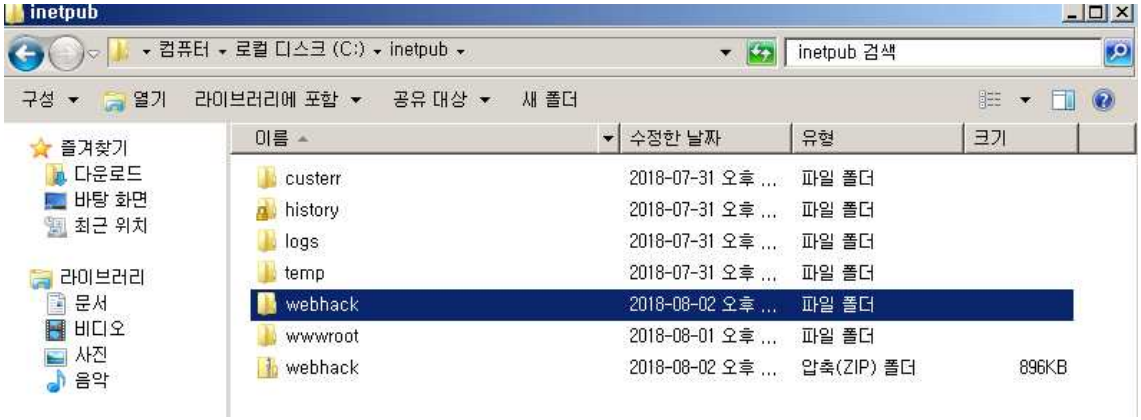
이로써 데이터베이스 백업 파일 형성이 완료 되었습니다.

데이터베이스 백업파일 또한 webhack 소스자료와 같이 다른 저장소에 저장해둡니다.

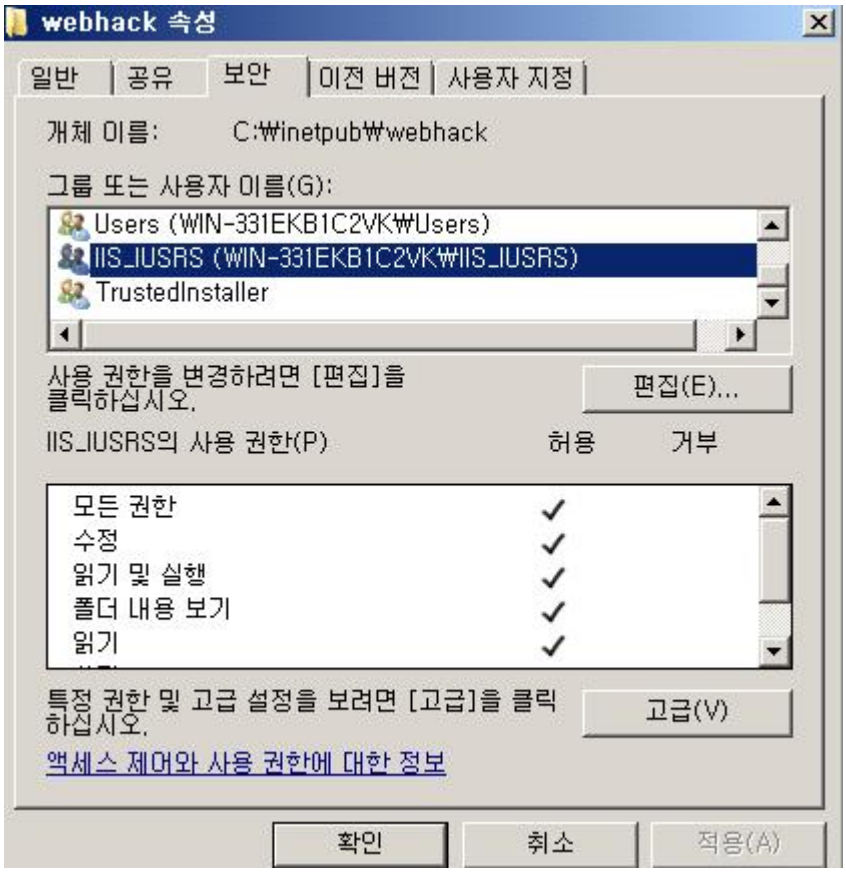
5. 마이그레이션 할 상대 서버 작업(Windows Server 2008 R2)

1) 웹 서버 소스파일 이동 및 저장

앞서 저장해 두었던 webhack 웹서버의 소스를 이동 시킵니다.

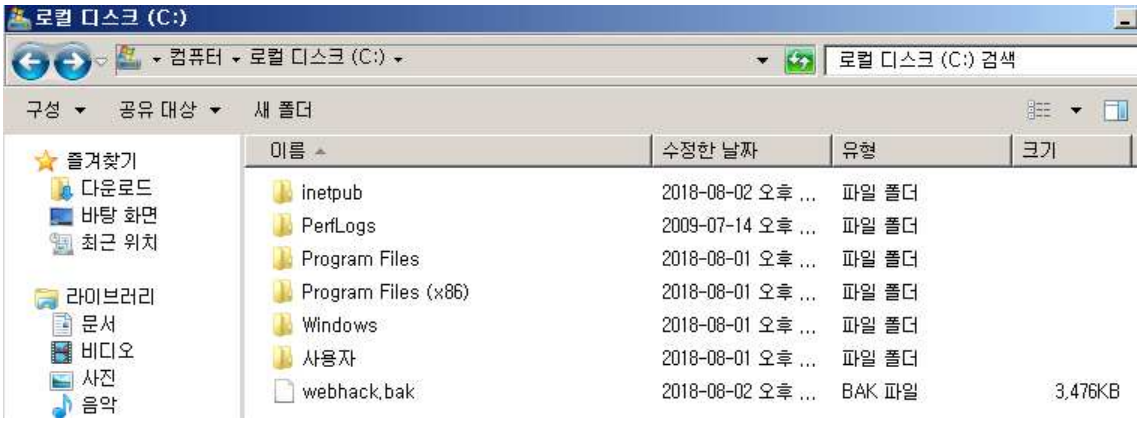


<그림46> C드라이브 > inetpub 에 저장후 압축을 푼 모습입니다.



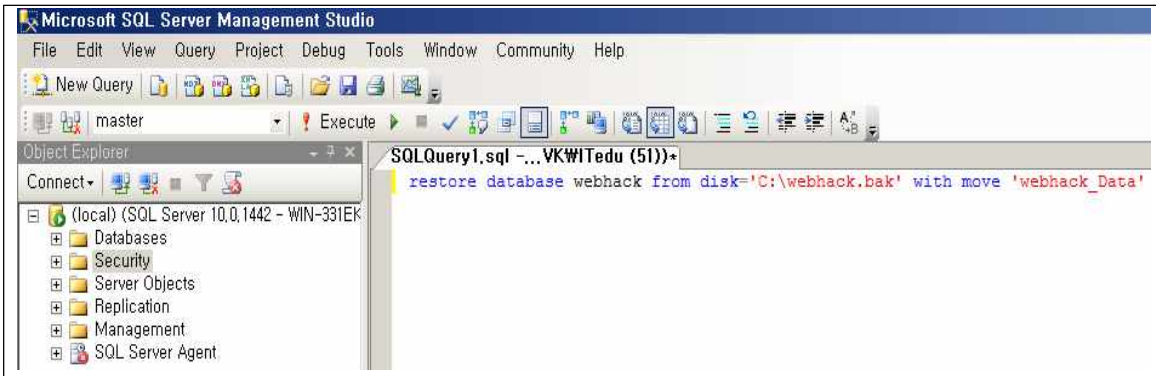
<그림47> webhack 폴더에 IIS_SUSRS를 추가하여 모든 권한으로 파일권한을 수정합니다.
이것은 IIS 사용자 그룹입니다.

2) 웹 서버 데이터베이스 파일 이동 및 저장



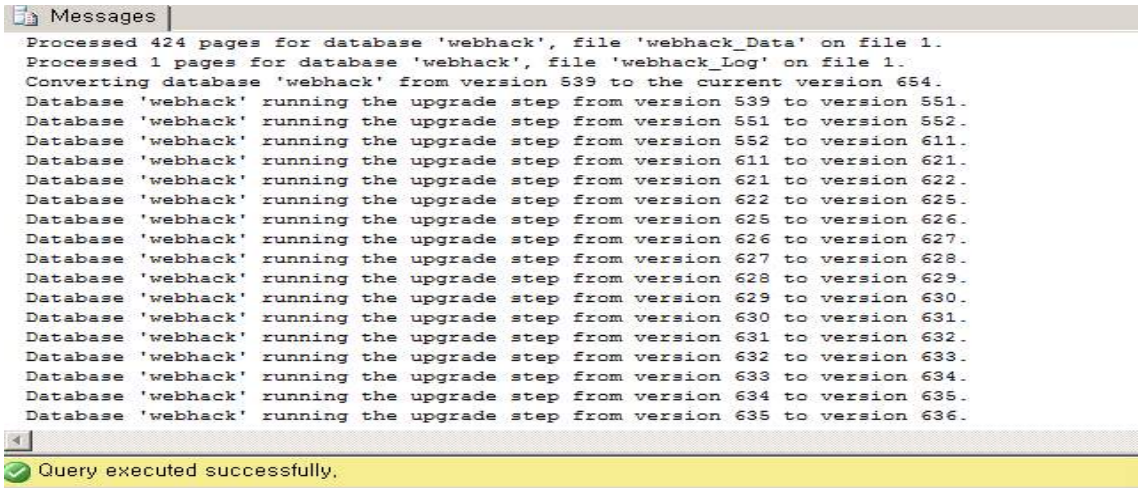
<그림48> 저장해두었던 DB파일(webhack.bak)을 C드라이브 경로에 저장합니다.
저장한 후에 SQL Server Management Studio 로 접속합니다.
(경로 : 시작 > 모든 프로그램 > SQL Server 2008)

<그림49> 로컬 사용자 계정으로 접속합니다.

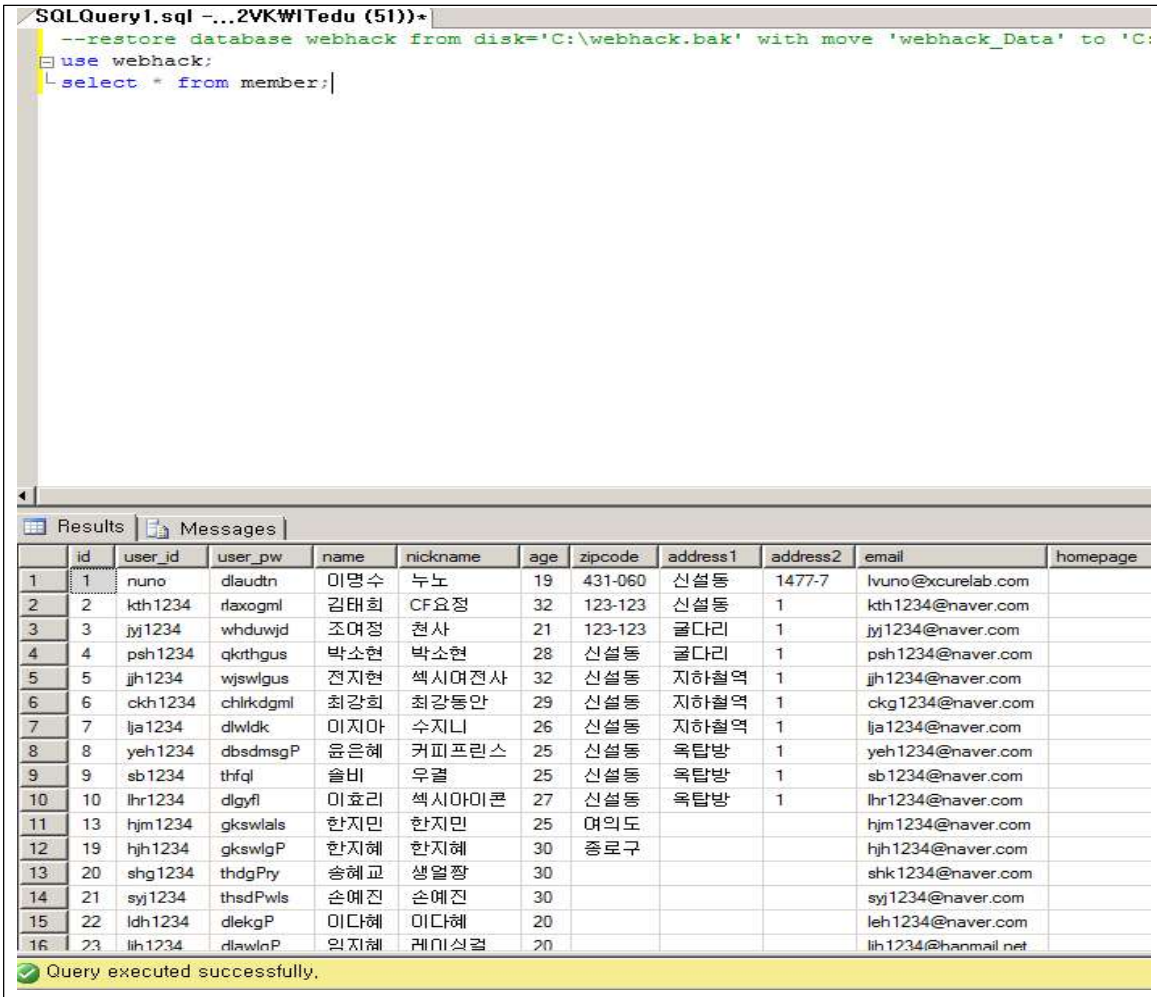


<그림50> 왼쪽 상단에 New Query를 선택하신후 백업한 데이터베이스 연동을 위한 쿼리 작성을 합니다. 띄어쓰기를 하게 되면 구문 적용이 되지 않습니다. 구문내용은 아래와 같습니다.

<그림51> C드라이브에 저장해둔 webhack.bak파일을 경로를 지정하여 Data와 Log파일로 복사하는 구문입니다.



<그림52> 쿼리가 성공적으로 실행되었음 하단 메시지에서 확인합니다.

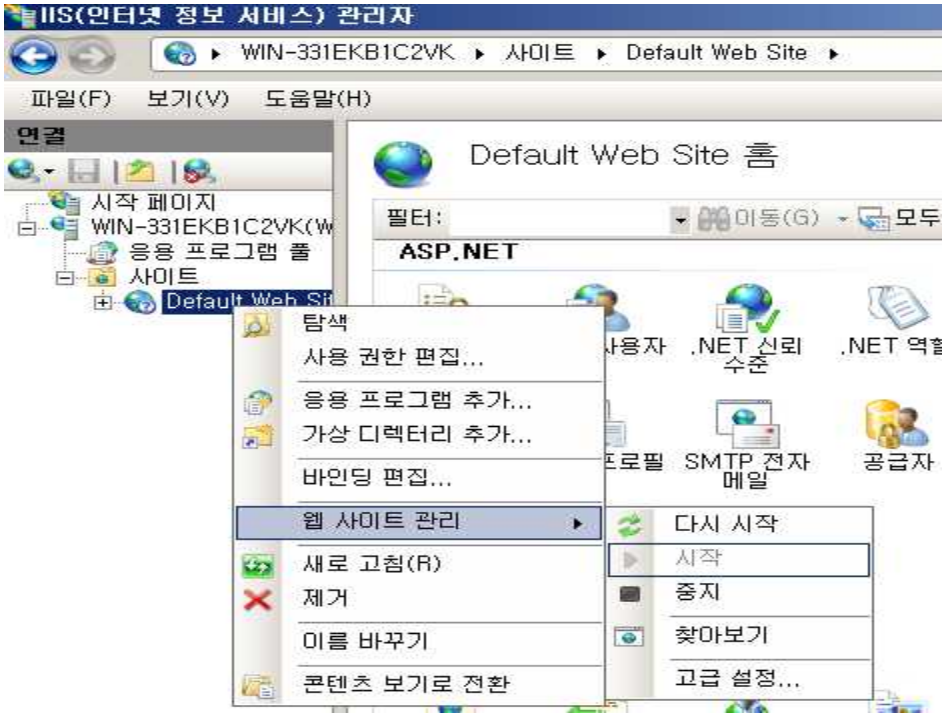


	id	user_id	user_pw	name	nickname	age	zipcode	address1	address2	email	homepage
1	1	nuno	dlaudtn	이명수	누노	19	431-060	신설동	1477-7	lvuno@xcurelab.com	
2	2	kth1234	rlaxogml	김태희	CF요정	32	123-123	신설동	1	kth1234@naver.com	
3	3	jyj1234	whduwjd	조여정	천사	21	123-123	굴다리	1	jyj1234@naver.com	
4	4	psh1234	qkrthgus	박소현	박소현	28	신설동	굴다리	1	psh1234@naver.com	
5	5	jjh1234	wjswlgus	전지현	섹시여전사	32	신설동	지하철역	1	jjh1234@naver.com	
6	6	ckh1234	chlrkdgml	최강희	최강동안	29	신설동	지하철역	1	ckg1234@naver.com	
7	7	lja1234	dlwldk	이지아	수지니	26	신설동	지하철역	1	lja1234@naver.com	
8	8	yeh1234	dbsdmsgP	윤은혜	커피프린스	25	신설동	옥탑방	1	yeh1234@naver.com	
9	9	sb1234	thfql	송비	우결	25	신설동	옥탑방	1	sb1234@naver.com	
10	10	lhr1234	dlgyfl	이효리	섹시아이콘	27	신설동	옥탑방	1	lhr1234@naver.com	
11	13	hjm1234	gkswlals	한지민	한지민	25	여의도			hjm1234@naver.com	
12	19	hjh1234	gkswlgP	한지혜	한지혜	30	종로구			hjh1234@naver.com	
13	20	shg1234	thdgPry	송혜교	생얼짱	30				shk1234@naver.com	
14	21	syj1234	thsdPwls	손예진	손예진	30				syj1234@naver.com	
15	22	ldh1234	dlekgP	이다혜	이다혜	20				leh1234@naver.com	
16	23	lih1234	dlawlgP	임지혜	레이싱걸	20				lih1234@hanmail.net	

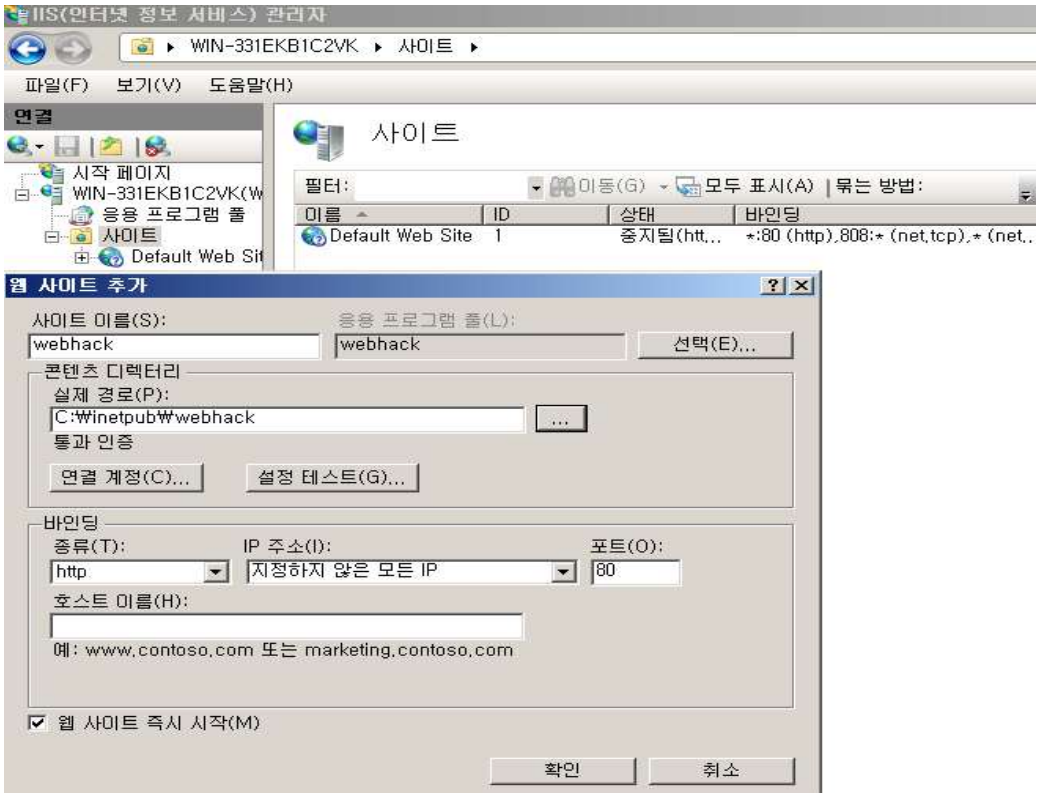
<그림53> 위에 실행했던 구문은 주석 처리 후 데이터베이스가 제대로 연동 되었는지 확인합니다.

이로써 데이터베이스 백업 파일 이동 작업이 완료되었습니다.

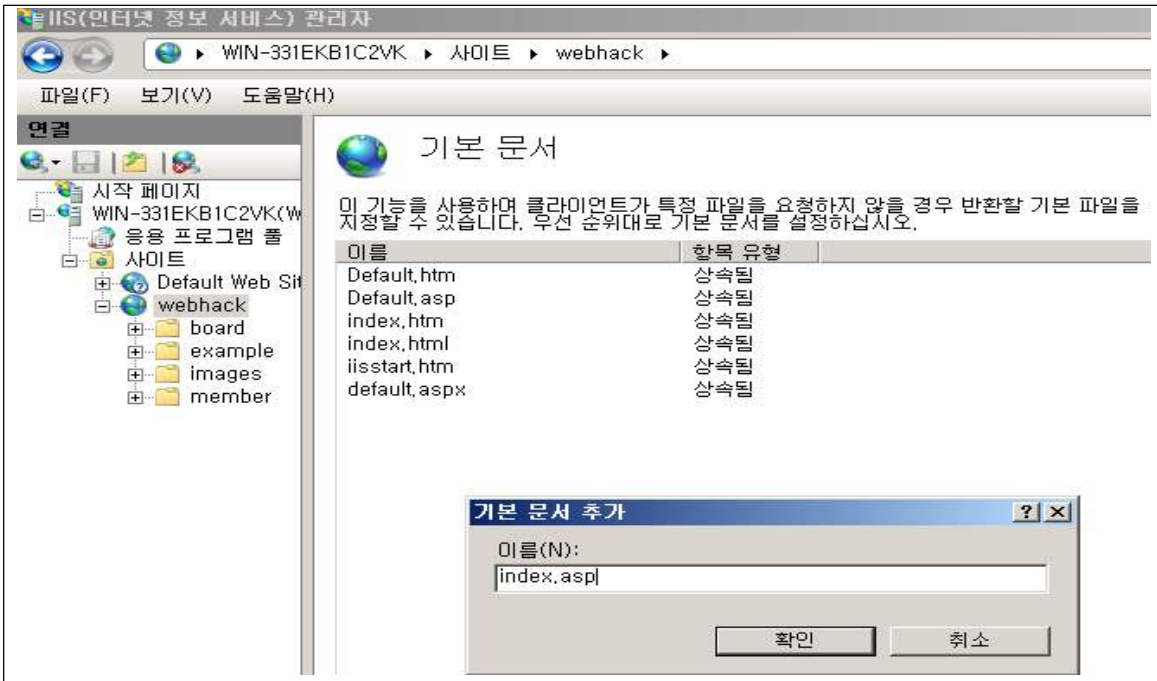
3) 사이트 추가 및 설정



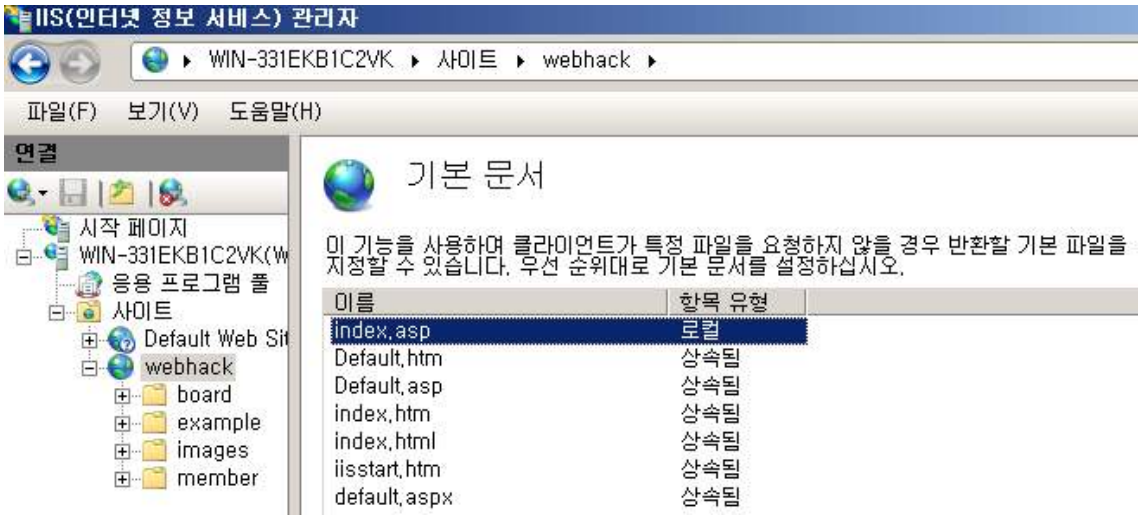
<그림54> IIS관리자로 접속한 후에 Default 사이트를 중지합니다.



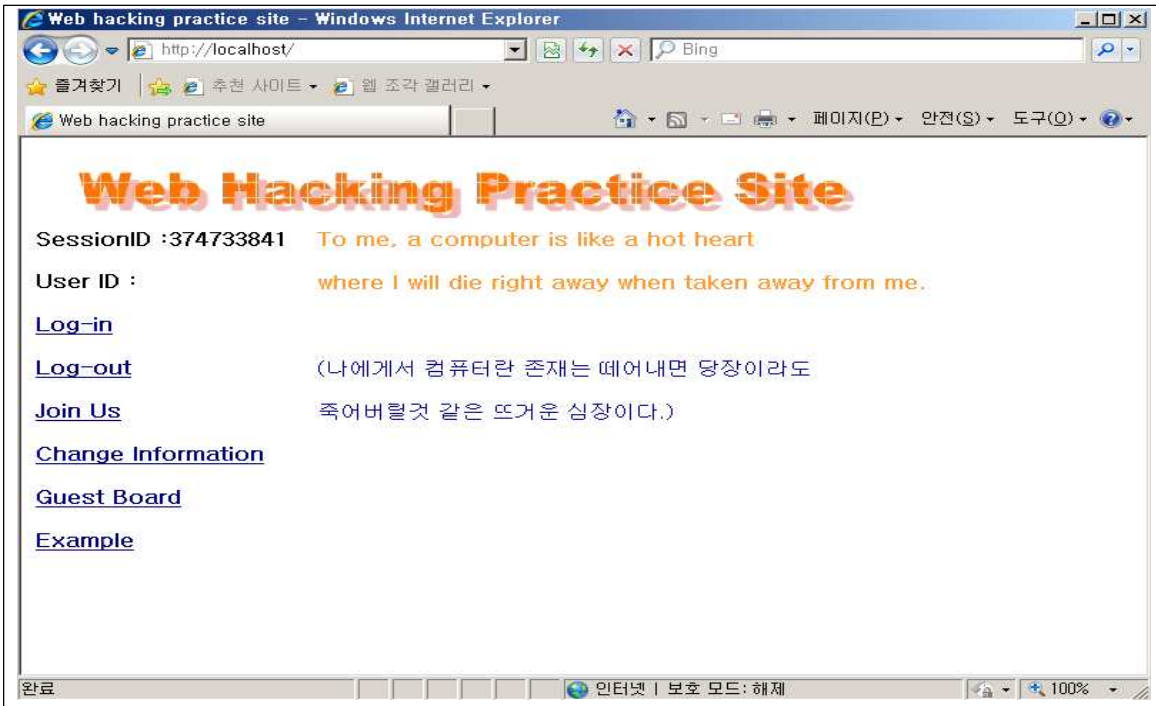
<그림55> webhack 웹 사이트를 새롭게 추가합니다. 실제 경로는 저장된 소스파일 경로 입니다.



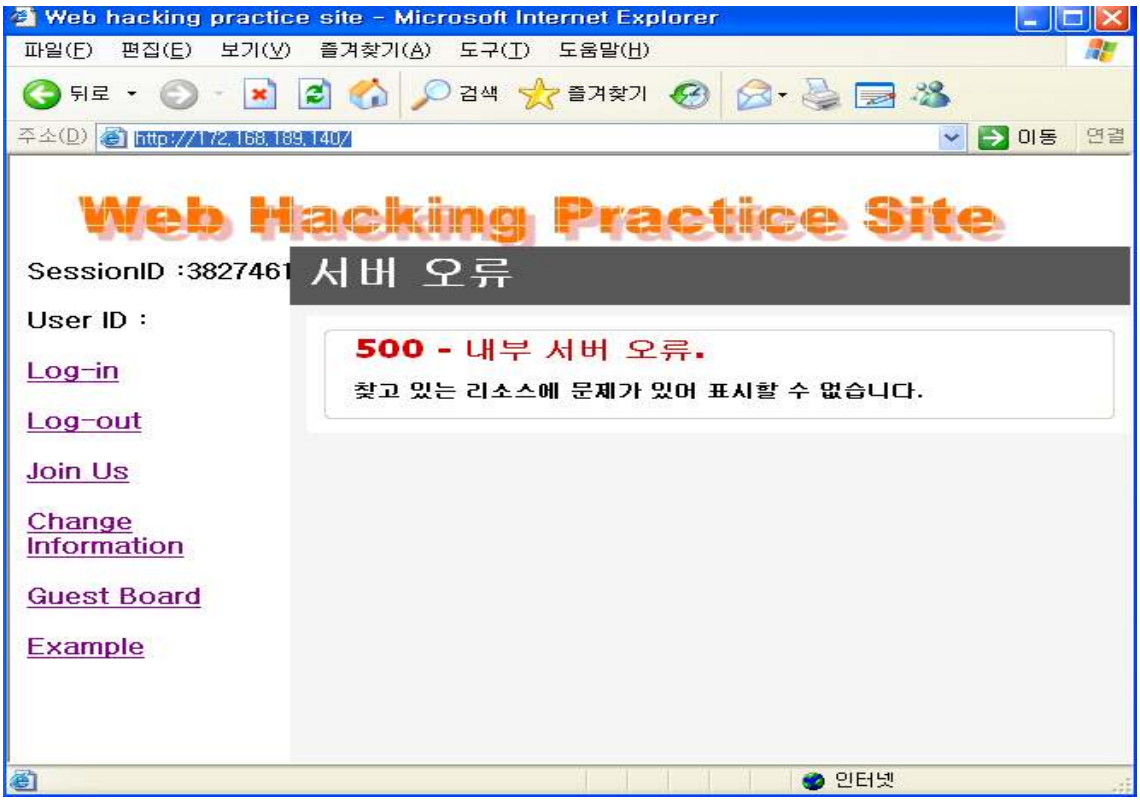
<그림56> index.asp 생성 모습



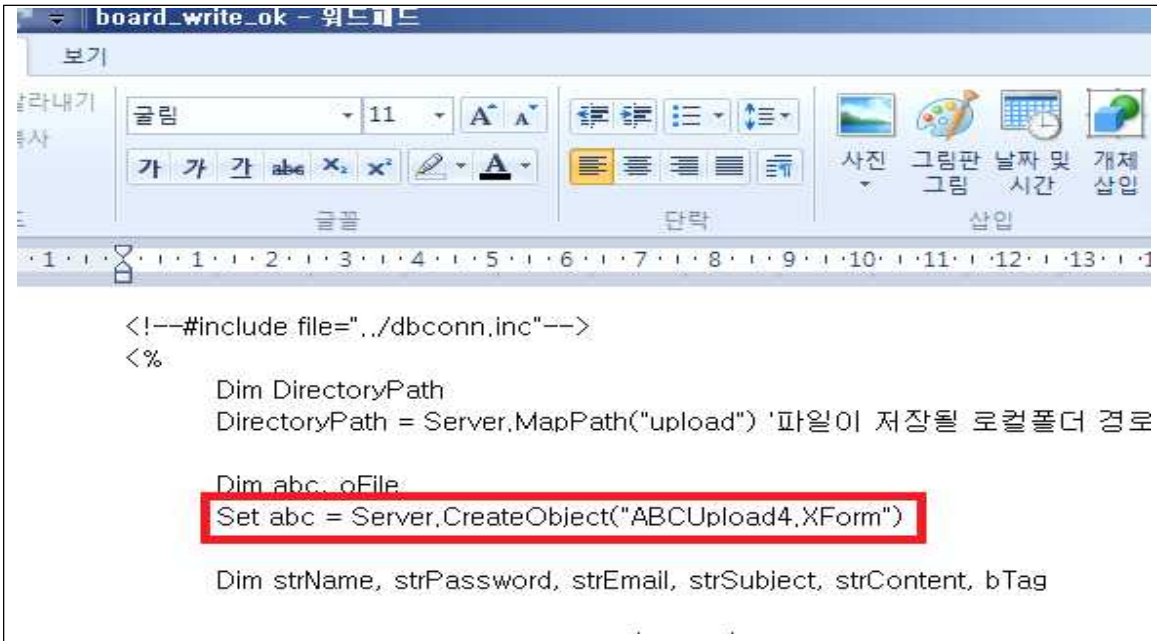
<그림57> webhack사이트의 기본문서로 접속해서 index.asp를 맨 우선순위로 설정 추가합니다.
메인이 떠야하기 때문에 이와 같이 설정합니다.



<그림58> index.asp를 설정 후 정상 작동을 확인합니다. 다른 컴퓨터에서도 테스트 해봅니다.

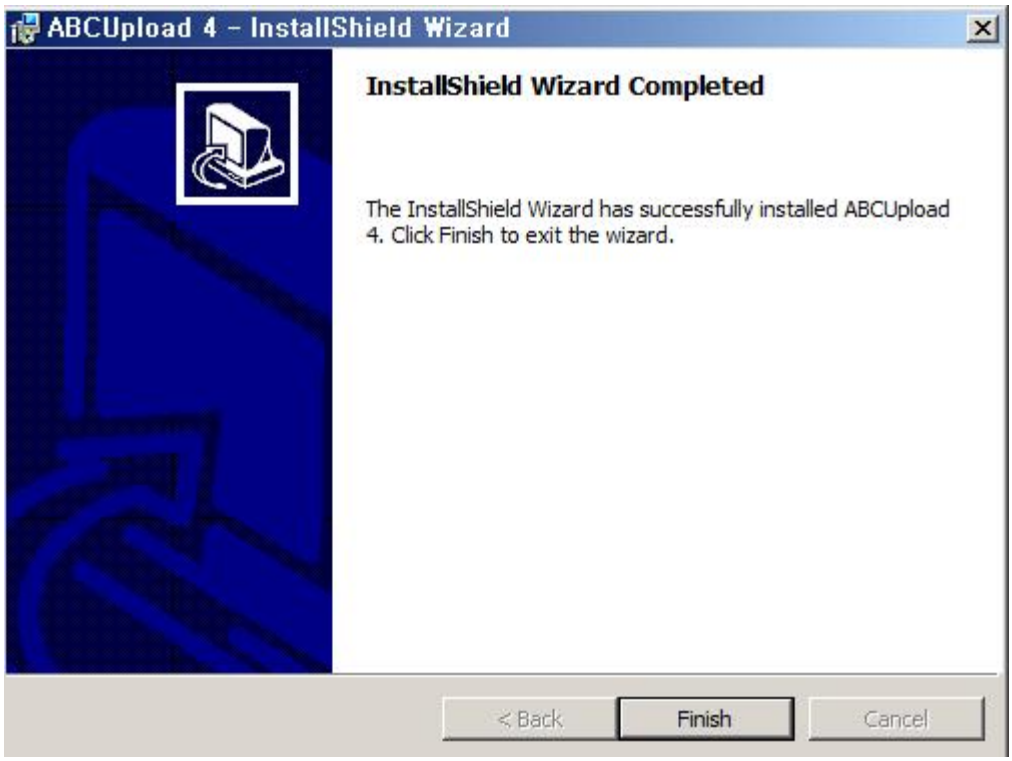


<그림59> XP환경의 다른 컴퓨터에서 사이트를 테스트해본 결과 500번의 서버오류를 발견하였습니다. Change Information과 Guest Board에서 리소스를 불러오지 못하고 있습니다.

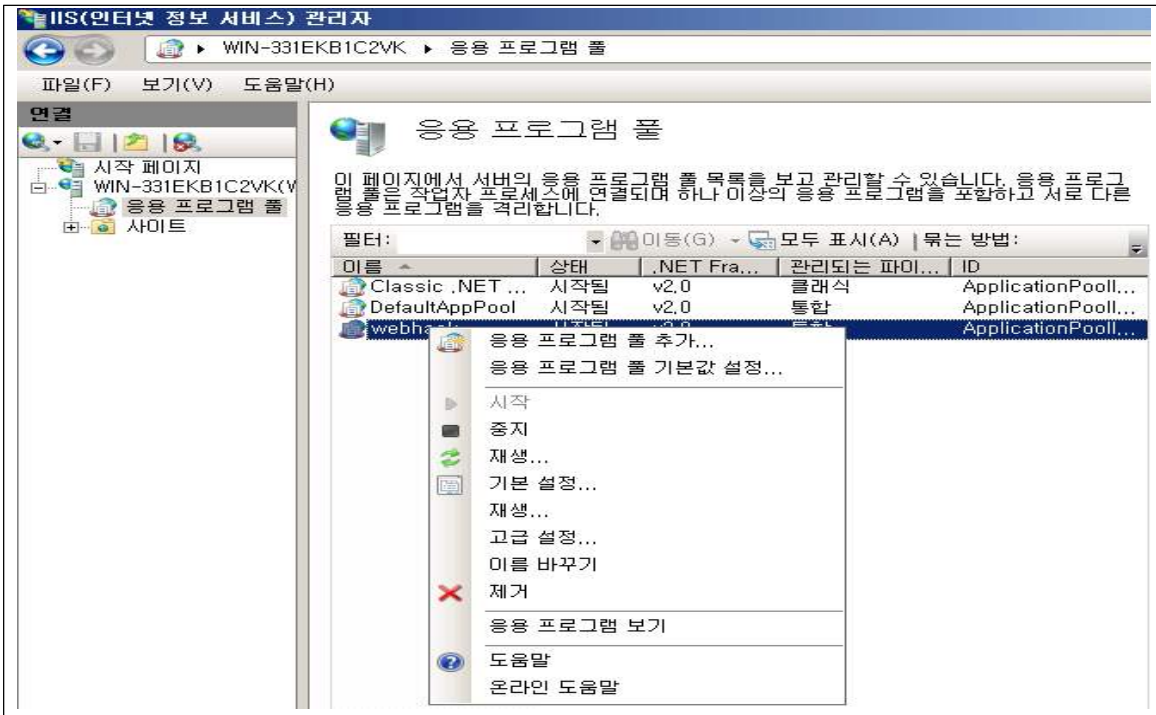


<그림60> board_wirte_ok.asp 의 소스 내용

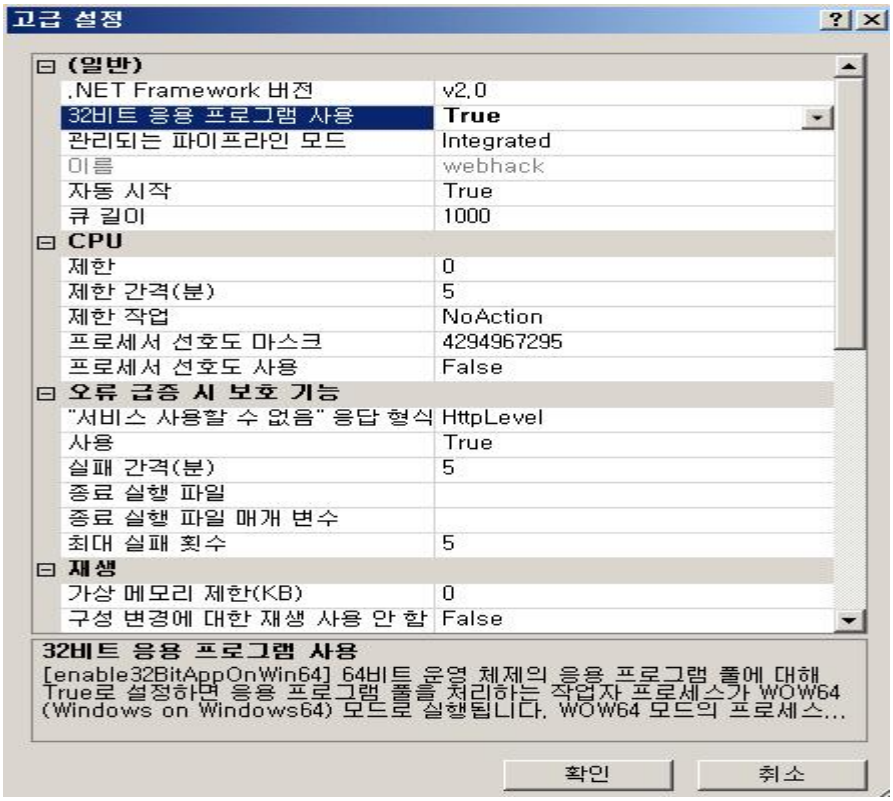
서버파일을 체크 해본결과, inetpub\webhack\board 에 글쓰기에 대한 오류를 발견하였습니다. board_write_ok.asp에서 오브젝트 라이브러리를 불러오지 못하는 오류였습니다. upload 폴더에 IIS_IUSER의 권한 설정과 IIS 응용프로그램 풀에서 32비트 모듈 실행 설정 그리고 라이브러리를 새로 설치해야 합니다.



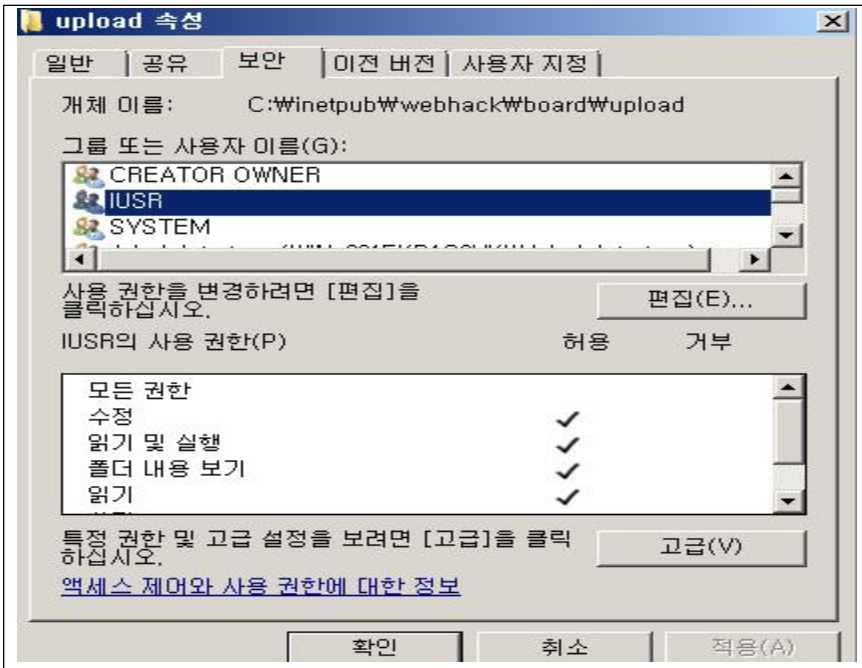
<그림61> 라이브러리 ABCUpload 4를 설치합니다.



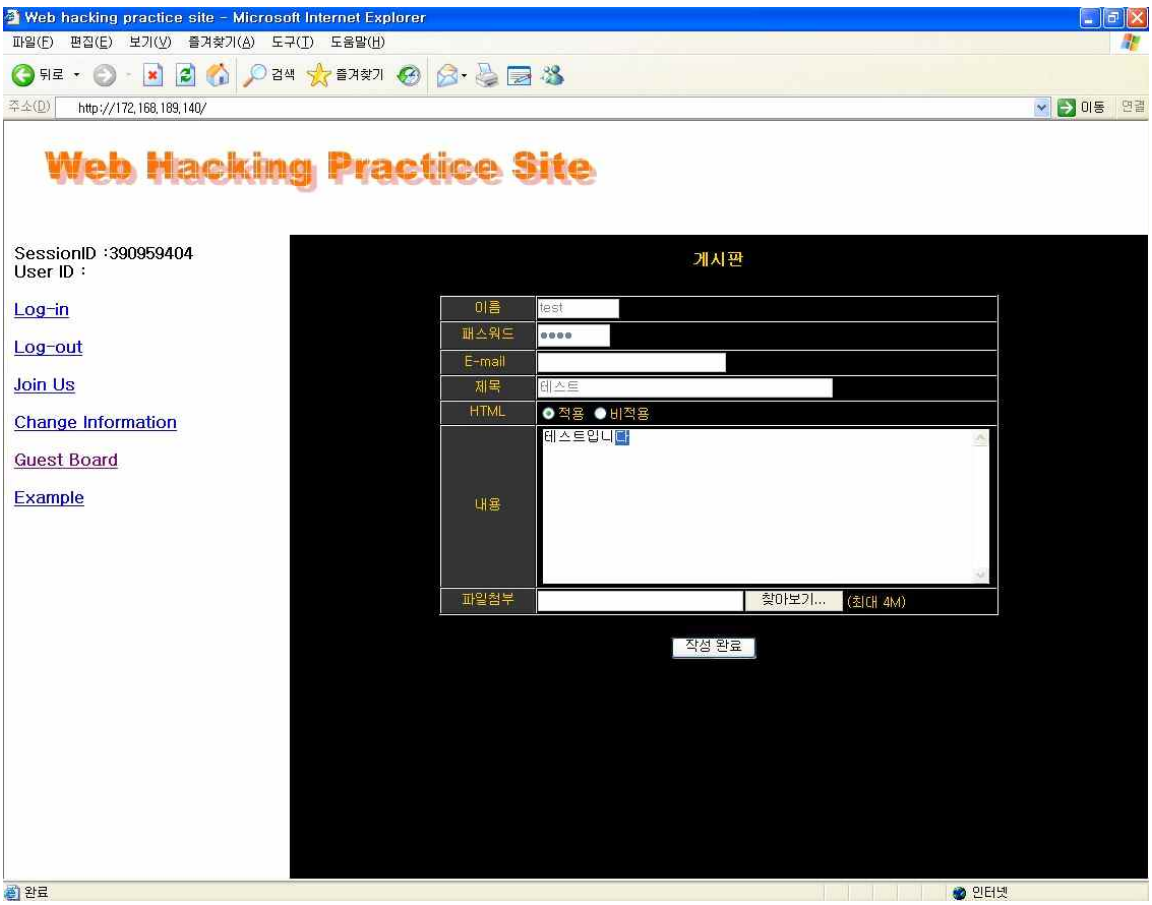
<그림62> 응용프로그램 풀 > webhackpool > 고급설정 이동



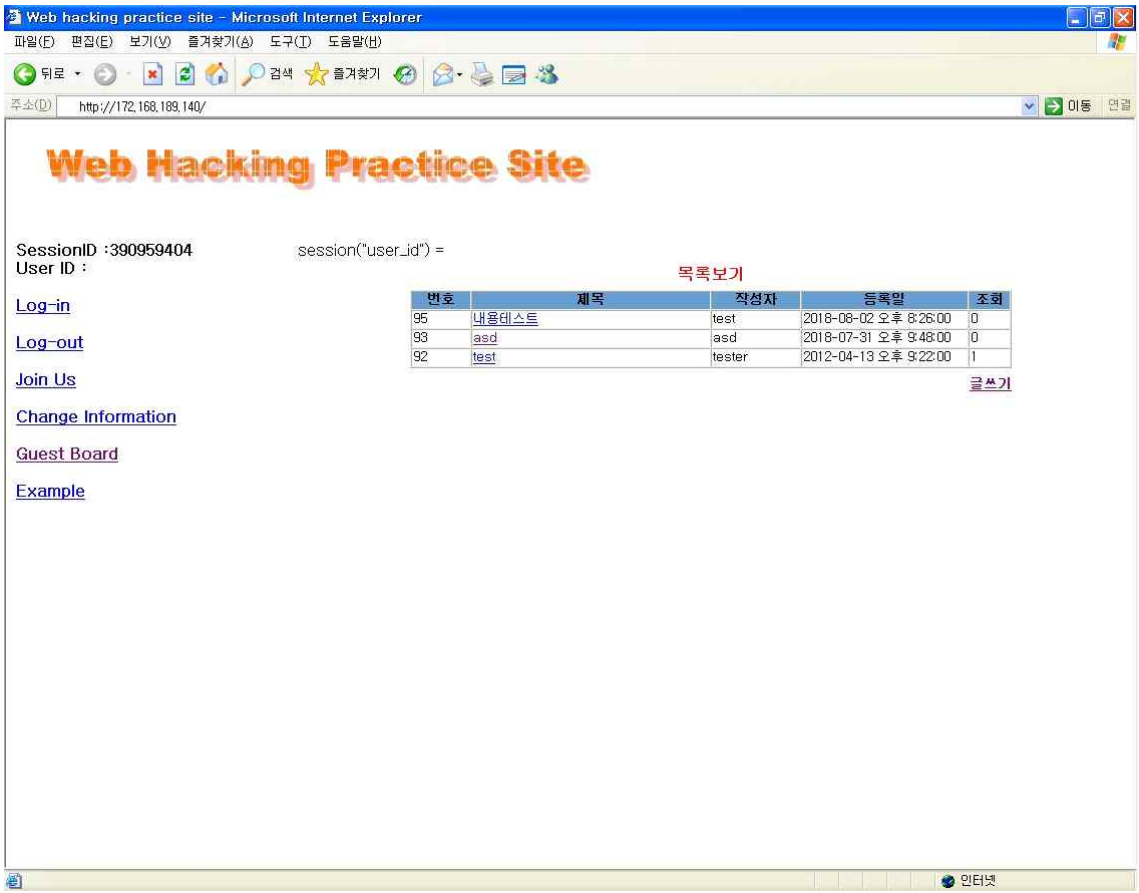
<그림63> 고급설정에서 32비트 True로 변경합니다.



<그림64> upload 폴더에 IUSR의 권한을 부여합니다.(수정권한까지)



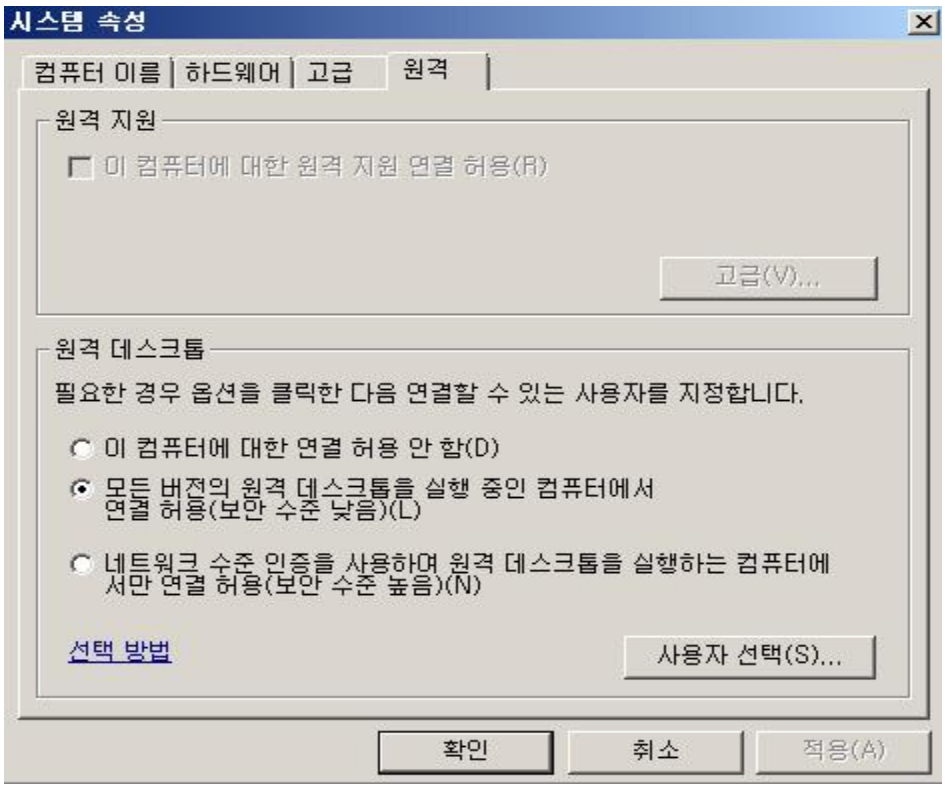
<그림65> 게시판에 접속이 되는 것을 확인. 게시판에 글을 작성해봅니다.



<그림66> 게시판에 글이 제대로 올라오는 것을 확인합니다.

5. 보안 취약점 분석 비교 및 설정

1) 보안 환경



<그림67>

취약점을 분석하기에 앞서 현재 저희 회사 서버의 보안환경은 호환성을 위해 원격 데스크톱 설정에서 “보안 수준 낮음”으로 활성화 되어 있습니다. 이에 따른 환경에 맞춰 보안 취약점을 해결합니다. 저희가 선택한 이 설정은 다른 사용자가 사용 중인 원격 데스크톱 연결 버전을 모르는 경우 사용되며, Windows Server 2003이하 버전들이 이에 속합니다.

2) 취약점 분석표

보안 요구사항	시스템 보안 설정
윈도우 구 버전 취약점	Win2000 -> Win2008R2 업그레이드
IIS 구 버전 취약점	IIS 5.0 -> IIS 7.5 업그레이드
DB 구 버전 취약점	MSSQL2000 -> MSSQL2008 업그레이드
계정 취약점 관리	로컬 계정 사용 설정 (Administrator 계정 이름 변경/Guest 계정 상태 변경)
	계정 잠금 정책 설정
	불필요한 계정 제거
	암호 정책 설정
시스템 보안 취약점	로컬 감사정책 설정
	이벤트 뷰어 설정
	공유 폴더 설정
파일 시스템 취약점	SAM 파일 권한 설정
DoS 공격 대비 취약점	익명 사용자에 대한 권한 설정

윈도우, IIS, DB 구 버전 취약점에 대한 것은 Win2008R2를 설치함으로써 해결하였습니다. 나머지 보안 요구사항은 분석표 순서에 따라 보안설정에 대해 설명 드리겠습니다.

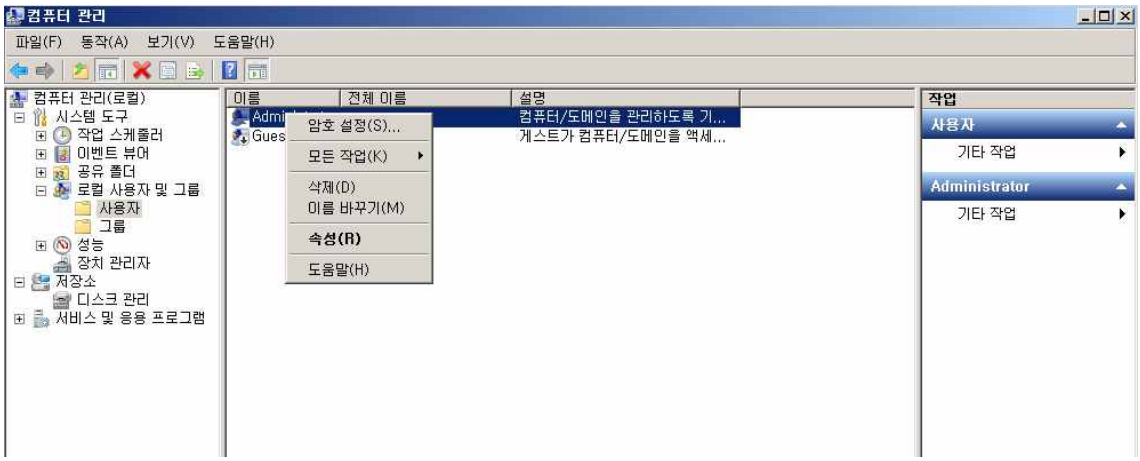
3) 취약점 설정

■ 보안 요구사항 : 계정 취약점 관리

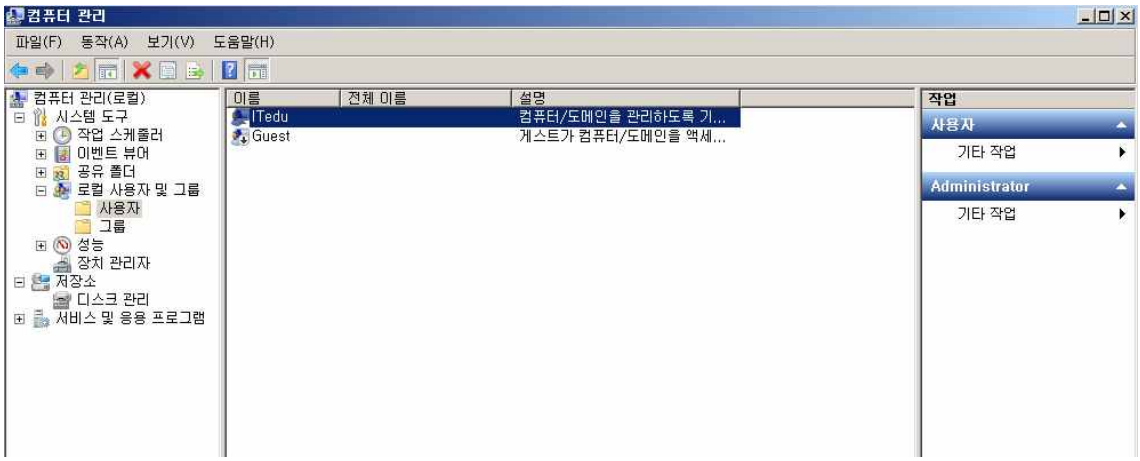
■ 취약점 항목 : 로컬 계정 사용 설정

■ Administrator(관리자) 계정 이름 변경

-Administrator 계정을 관리자 계정이 아닌 일반 계정으로 사용하거나, Administrator가 아닌 다른 이름의 관리자 계정을 생성해 사용해야 합니다. Password는 최소 9자리 이상으로 영문과 숫자, 특수문자를 혼합하여 사용합니다. 최고 관리자 이름을 변경함으로써 외부로의 침입을 한층 더 안정적으로 보안하기 위함입니다.



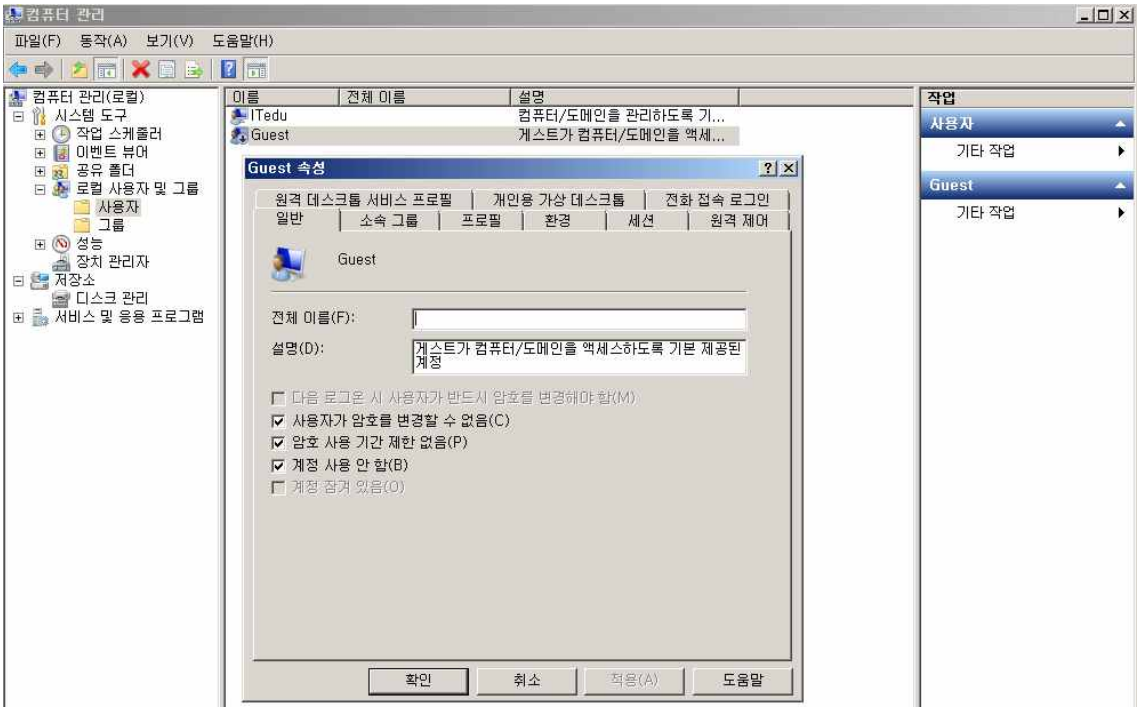
<그림68>시작 -> 관리도구 -> 컴퓨터 관리 -> 로컬 사용자 및 그룹 -> 사용자 -> Administrator 이름 바꾸기 선택 > 관리자 계정 이름 변경



<그림69>Administrtor 계정을 ITedu 라는 이름으로 변경된 것을 확인합니다.

■ Guest 계정 비활성화

- 대부분의 시스템은 Guest 계정의 사용을 필요치 않으며 앞으로도 계속 Guest 계정의 사용을 제한해야 하며, 불특정 다수의 접근이 필요할 경우 Guest 가 아닌 일반 사용자 계정을 생성해 사용하도록 해야 합니다.



<그림70>시작 -> 관리도구 -> 컴퓨터 관리 -> 로컬 사용자 및 그룹 -> 사용자 > Guest 계정에 대한 사용 제한 설정 후에 Guest계정이 비활성화 된 모습입니다.

■ 보안 요구사항 : 계정 취약점 관리

■ 취약점 항목 : 계정 잠금 정책 설정

로그온 실패 횟수와 계정 잠금 기간, 계정 잠금 복귀 시간을 설정하여, 서버에 대한 패스워드 무차별 대입공격 등에 대응하고 보안수준을 향상시킵니다.

◆ 정책명 : 계정잠금 기간

◆ 설정값(권고) : 60분

◆ 내용 : 사용자가 정해진 횟수 이상 로그온에 실패하면 시스템은 해당 계정을 60분 동안 잠금(60분 동안 로그인 불가)

◆ 정책명 : 계정 잠금 임계값

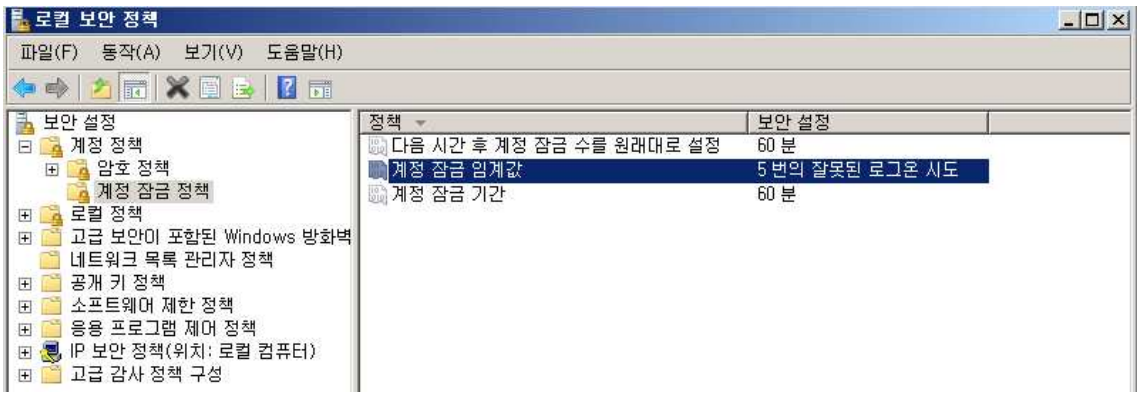
◆ 설정값(권고) : 5번의 잘못된 로그온 시도

◆ 내용 : 로그인 시도 횟수를 5번으로 설정하며, 5번 이상 로그인에 실패하였을 경우 계정 잠금 시간만큼 계정은 잠기게 됩니다.

◆ 정책명 : 다음 시간 후 계정 잠금 수를 원래대로 설정

◆ 설정값(권고) : 60분

◆ 내용 : 잘못된 로그온 시도 후에 60분이 경과해야, 로그온 시도 카운터를 0으로 설정합니다.



<그림71> 시작 -> 관리도구 -> 컴퓨터 관리 > 로컬보안 정책 -> 계정 정책 -> 계정잠금 정책

- "계정 잠금 기간" : 60분

"다음 시간 후 계정 잠금을 원래대로 설정" : 60분

"계정 잠금 임계 값" : 5번

■ 보안 요구사항 : 계정 취약점 관리

■ 취약점 항목 : 불필요한 계정 제거

퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정이 존재하는지 점검합니다.

관리되지 않은 불필요한 계정은 장기간 패스워드가 변경되지 않아, 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing)에 의해 계정 정보가 유출되어도 인지하기 어렵습니다.

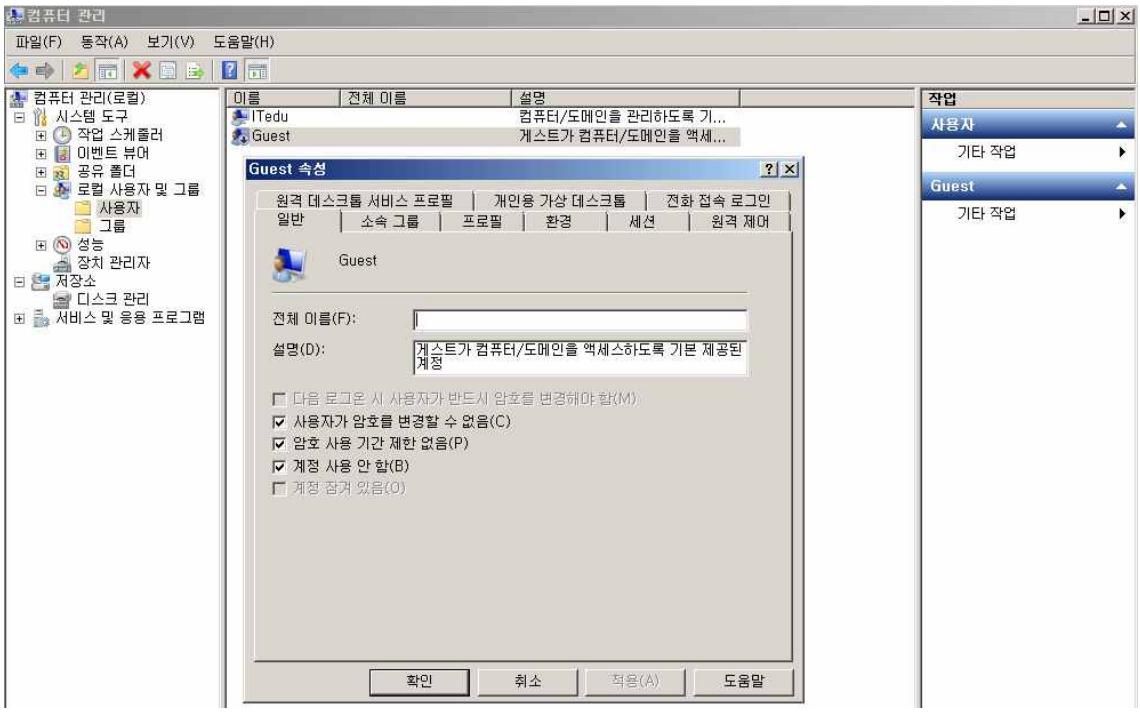
* 무작위 대입 공격(Brute Force Attack) : 컴퓨터로 암호를 해독하기 위해 가능한 모든 키를 하나하나 추론해 보는 시도

■ 보안대책

- 양호 : 불필요한 계정이 존재하지 않는 경우
- 취약 : 불필요한 계정이 존재하는 경우

■ 조치방법

- 현재 계정 현황 확인 후 불필요한 계정 삭제



<그림72>

방법은 위에서 말씀드렸던 <그림25>와 같이 Guest계정을 사용안함으로서 조치를 취하였습니다. 추후에 다른 계정이 생성이 되어 있다면 이와 같은 방법을 시행합니다.

■ 보안 요구사항 : 계정 취약점 관리

■ 취약점 항목 : 암호 정책 설정

패스워드 추측 공격을 방지하기 위한 사용자 패스워드 정책 설정입니다.

패스워드 추측 공격을 피하기 위하여 패스워드 복잡성 및 최소길이를 설정합니다.

다음은 설정할 값에 대한 설명입니다.

정책	설정값(권고)	내용
암호는 복잡성을 만족해야 함	사용	아래의 조건을 만족하는 비밀번호만 사용가능 - 사용자의 계정 이름이나 연속되는 문자 2개를 초과하는 사용자 전체이름의 일부를 포함하지않음. - 길이가 최소한 6자 이상이어야 함. - 다음 네가지 범주 중 세가지의 문자를 포함해야함. ▶ 영문 대.소문자, 숫자, 특수문자
최대 암호 사용 기간	90일	- 비밀번호를 사용할 수 있는 기간을 90일로 지정 - 90일 이후 시스템에서 사용자에게 암호 변경을 요청
최소 암호 길이	9문자	사용자 계정의 비밀번호 길이를 9자 이상으로 제한.

<그림73> 시작 -> 관리도구 -> 로컬보안 정책 -> 계정정책 -> 암호 정책 선택 후 설정

※ 비밀번호를 생성시 아래와 같은 사용은 지양 하셔야 합니다.

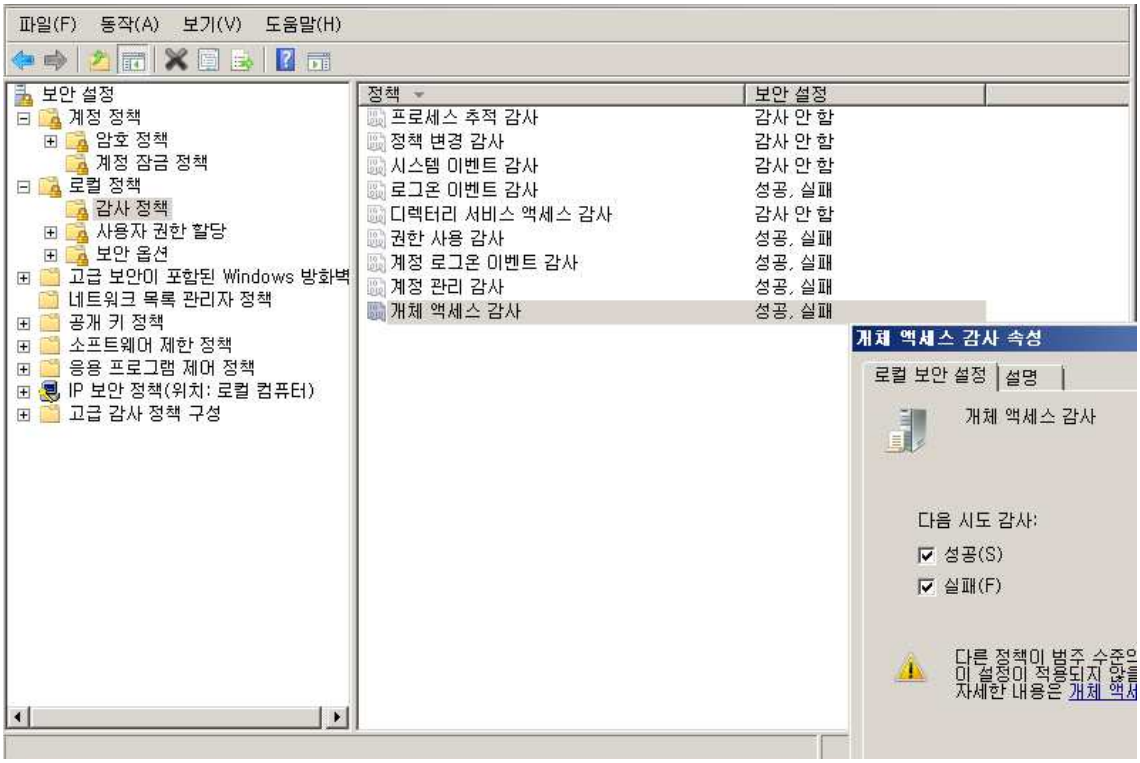
- 계정과 동일하거나 유사한 문자, 부서명, 담당자성명, 생일, 연속성 있는 문자 및 숫자

■ 보안 요구사항 : 시스템 보안 취약점

■ 취약점 항목 : 로컬 감사 정책 설정

감사정책 설정을 통해 보안 로그에서 계정 로그온/로그오프에 대한 감사를 설정합니다. 아래의 표는 각 정책에 대한 설명입니다.

정책	설정값(권고)	설명
개체 엑세스	성공/실패	- 시스템 액세스 컨트롤 목록(SACL)이 있는 Windows 기반 네트워크의 모든 개체에 대해 감사를 활성화 - 보안 로그에 이벤트를 표시하려면 먼저 개체 액세스 감사를 활성화한 후 감사할 각 개체에 대해 SACL을 정의
계정 관리	성공/실패	- 사용자나 그룹이 작성, 변경 또는 삭제된 시간을 판단하는데 사용
계정 로그온 이벤트	성공/실패	- 사용자가 도메인에 로그온하면 도메인 컨트롤러에 로그온 시도가 기록
권한 사용	성공/실패	- 권한 사용의 성공 및 실패를 감사할 경우 사용자 권한을 이용하려고 할 때마다 이벤트가 생성
디렉터리 서비스 엑세스	-	- Active Directory 개체의 SACL에 나열된 사용자가 해당 개체에 액세스를 시도할 때 감사 항목이 생성
로그온 이벤트	성공/실패	- 사용자가 컴퓨터에 로그온하거나 로그오프할 때마다 로그온이 시도된 컴퓨터의 보안 로그에 이벤트가 생성
시스템 이벤트	-	- 사용자나 프로세스가 컴퓨터 환경을 변경하면 시스템 이벤트가 생성 - 시스템 이벤트를 감사할 경우 보안 로그가 삭제된 시간도 감사
정책 변경	-	- 감사 정책 변경의 성공 및 실패를 감사
프로세스 추적	-	- 실행되는 프로세스에 대한 자세한 추적 정보를 감사하는 경우 이벤트 로그에 프로세스를 작성하고 종료하려고 한 시도가 나타남



<그림74> 제어판 -> 관리도구 -> 로컬보안정책 -> 로컬정책 -> 감사설정

- 개체 액세스 감사, 계정 관리 감사, 계정 로그온 이벤트 감사, 권한 사용 감사, 로그온 이벤트 감사에 대해서는 반드시 "성공", "실패" 모두 기록되도록 감사 설정합니다.

<로컬 감사 정책 테스트 결과>

보안 이벤트 수: 15,847 (!) 새 이벤트를 사용할 수 있음

키워드	날짜 및 시간	원본	이벤트 ID	작업 범주
감사 실패	2018-08-02 오후 9:08:20	Microsoft Windows security auditing.	5157	필터링 플랫폼 연결
감사 실패	2018-08-02 오후 9:08:20	Microsoft Windows security auditing.	5152	필터링 플랫폼 패킷 삭제
감사 성공	2018-08-02 오후 9:08:09	Microsoft Windows security auditing.	5156	필터링 플랫폼 연결
감사 성공	2018-08-02 오후 9:08:09	Microsoft Windows security auditing.	5158	필터링 플랫폼 연결
감사 성공	2018-08-02 오후 9:08:00	Microsoft Windows security auditing.	4673	중요한 권한 사용
감사 성공	2018-08-02 오후 9:08:00	Microsoft Windows security auditing.	4673	중요한 권한 사용
감사 실패	2018-08-02 오후 9:08:00	Microsoft Windows security auditing.	4656	파일 시스템
감사 성공	2018-08-02 오후 9:07:41	Microsoft Windows security auditing.	5156	필터링 플랫폼 연결
감사 성공	2018-08-02 오후 9:07:38	Microsoft Windows security auditing.	5156	필터링 플랫폼 연결
감사 성공	2018-08-02 오후 9:07:38	Microsoft Windows security auditing.	5158	필터링 플랫폼 연결
감사 실패	2018-08-02 오후 9:07:25	Microsoft Windows security auditing.	5157	필터링 플랫폼 연결

시스템 이벤트 수: 1,625

수준	날짜 및 시간	원본	이벤트 ID	작업 범주
정보	2018-08-02 오후 8:22:13	Service Control Manager	7036	없음
정보	2018-08-02 오후 8:22:13	Service Control Manager	7036	없음
정보	2018-08-02 오후 8:22:13	Iphlpsvc	4200	없음
정보	2018-08-02 오후 8:22:13	Service Control Manager	7036	없음
정보	2018-08-02 오후 8:22:13	Service Control Manager	7036	없음
정보	2018-08-02 오후 8:22:12	Service Control Manager	7036	없음
정보	2018-08-02 오후 8:22:10	Service Control Manager	7036	없음
경고	2018-08-02 오후 8:22:10	DNS Client Events	1014	없음
정보	2018-08-02 오후 8:22:08	Service Control Manager	7036	없음
정보	2018-08-02 오후 8:22:03	Service Control Manager	7036	없음
정보	2018-08-02 오후 8:22:03	Service Control Manager	7036	없음

응용 프로그램 이벤트 수: 1,438

수준	날짜 및 시간	원본	이벤트 ID	작업 범주
정보	2018-08-02 오후 8:31:24	LoadPerf	1000	없음
정보	2018-08-02 오후 8:31:24	LoadPerf	1001	없음
정보	2018-08-02 오후 8:27:24	Security-SPP	1003	없음
정보	2018-08-02 오후 8:27:24	Security-SPP	8196	없음
정보	2018-08-02 오후 8:25:18	VSS	8224	없음
오류	2018-08-02 오후 8:23:20	WMI	10	없음
정보	2018-08-02 오후 8:22:52	MSSQLSERVER	18456	(4)
정보	2018-08-02 오후 8:22:50	MSSQLSERVER	18456	(4)
정보	2018-08-02 오후 8:22:49	MSSQLSERVER	18456	(4)
정보	2018-08-02 오후 8:22:48	MSSQLSERVER	18456	(4)
정보	2018-08-02 오후 8:22:47	MSSQLSERVER	18456	(4)

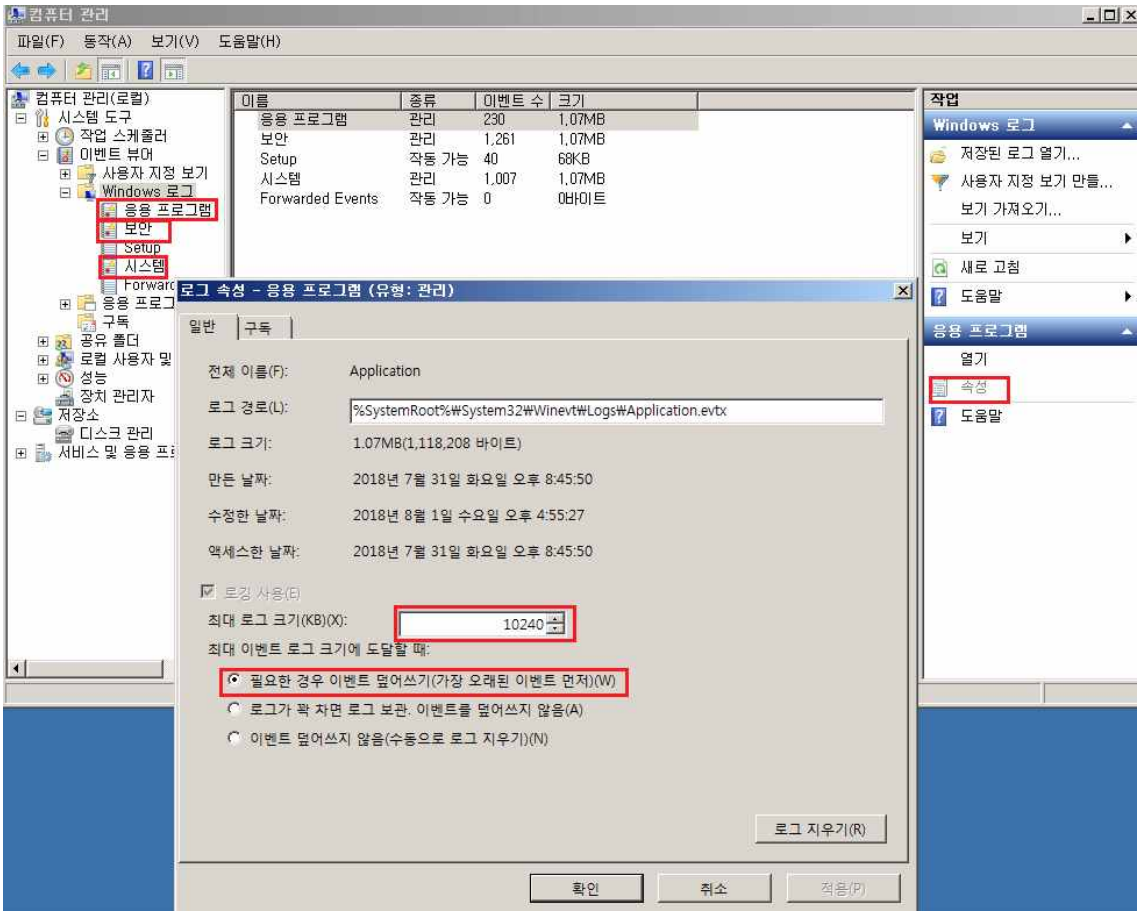
보안/ 시스템 / 응용프로그램 모두 정상적으로 성공과 실패에 대한 로그가 기록되는 것을 확인하였습니다.

■ 취약점 구분 : 시스템 보안 설정

■ 취약점 항목 : 이벤트 뷰어 설정

접근자 추적 및 불법 접근자 확인 자료를 위한 보안 로그의 설정입니다.

정보시스템의 효율적인 통제·관리, 사고 발생 시 추적 등을 위하여 시스템에 최근 6개월 간의 보안 로그가 저장되도록 설정해야 합니다. 따라서 아래와 같이 설정합니다.



<그림75> 제어판 -> 관리도구 -> 컴퓨터 관리 -> 이벤트 뷰어 -> Windows 로그(응용 프로그램, 보안, 시스템)

- 최대 로그 크기를 10Mbyte(10240KB) 또는 그 이상으로 설정
  (-> 6개월 간 로그가 저장 되도록 크기 설정)
- 최대 로그 크기에 도달할 때 "필요한 경우 이벤트 덮어쓰기" 선택

■ **취약점 구분 : 시스템 보안 설정**

■ **취약점 항목 : 공유 폴더 설정**

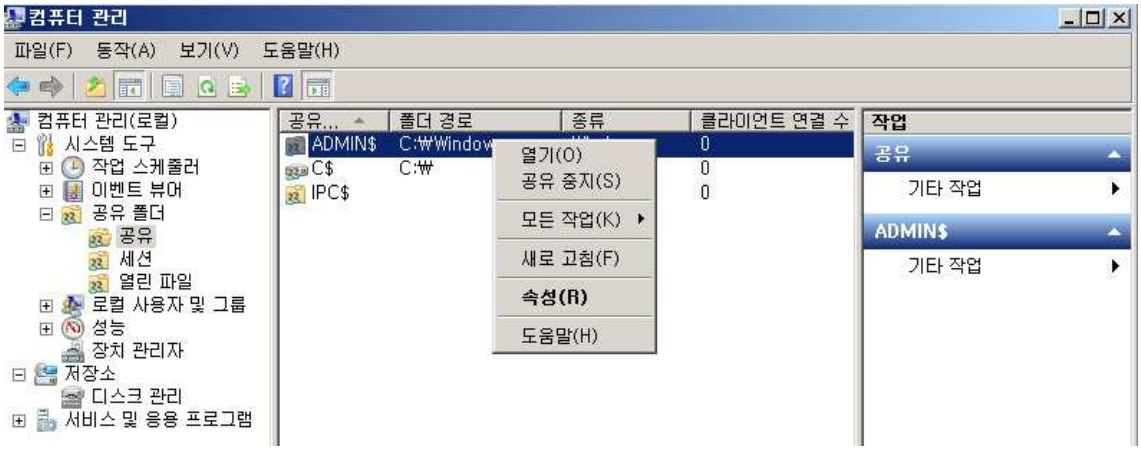
시스템 공유폴더 제거 및 공유 폴더 권한 설정입니다.

시스템에 설정된 공유폴더로 인해 비인가자가 시스템 자원에 접근할 수 있는 취약점이 존재합니다. 따라서 불필요한 디렉토리 공유를 제거하거나, 사용중인 공유폴더 접근 권한에 "Everyone"을 삭제하고 암호 설정합니다.

<시스템 기본 공유 폴더 제거>

- 디렉토리의 공유제거 후, 레지스트리 값을 변경합니다.

① 공유제거



<그림76>컴퓨터 관리 -> 공유폴더 -> 공유 -> 해당공유폴더 확인 -> 마우스 우클릭 -> 공유중지

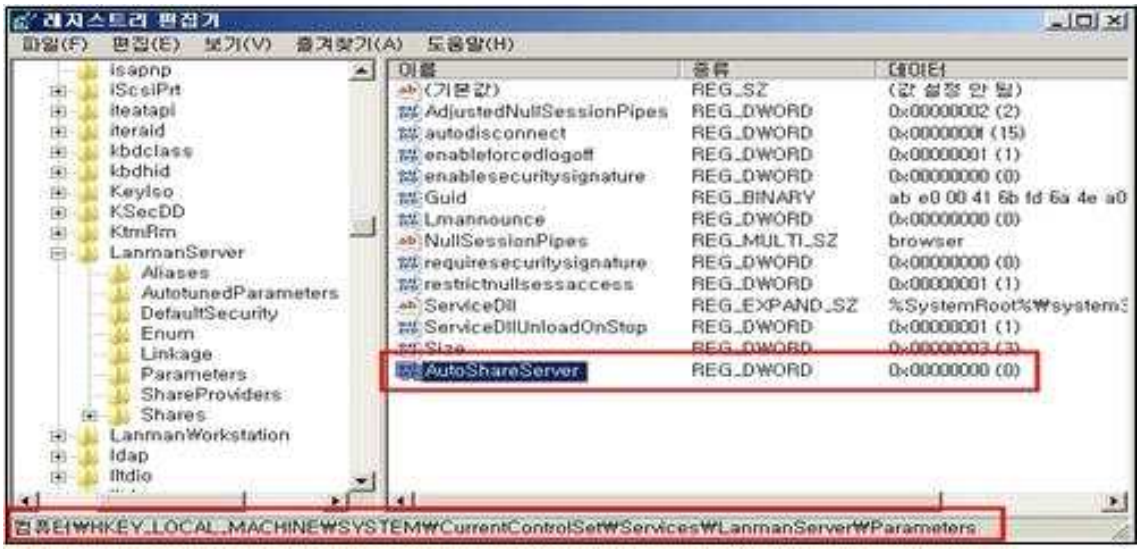
※ IPC$는 서비스에 영향을 미칠 수 있으므로 삭제 전 검토 필요

(원격관리, 기본공유만 제거 권고)

IPC를 제외한 ADMIN과 C를 사용중지 합니다.

② 레지스트리 값 변경

레지스트리 값을 수정해야 시스템 재부팅 후 디폴트 폴더가 자동 공유되는 것을 방지할 수 있습니다.



<그림77>

-> regedit.exe 실행

-> 레지스트리 수정

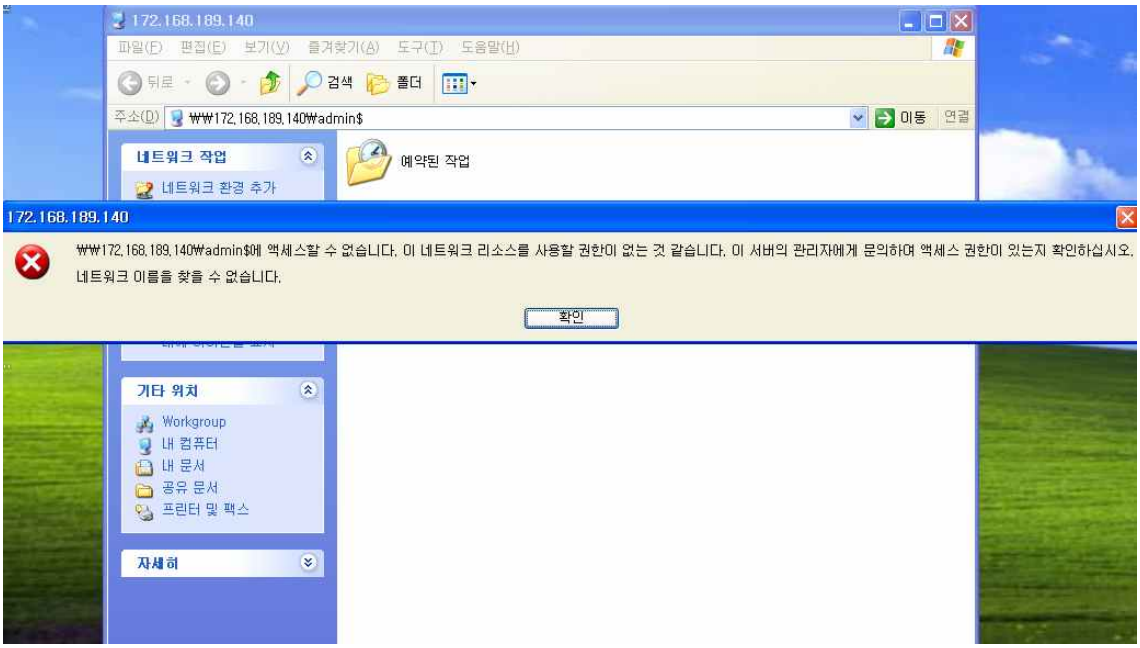
위치 : HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters

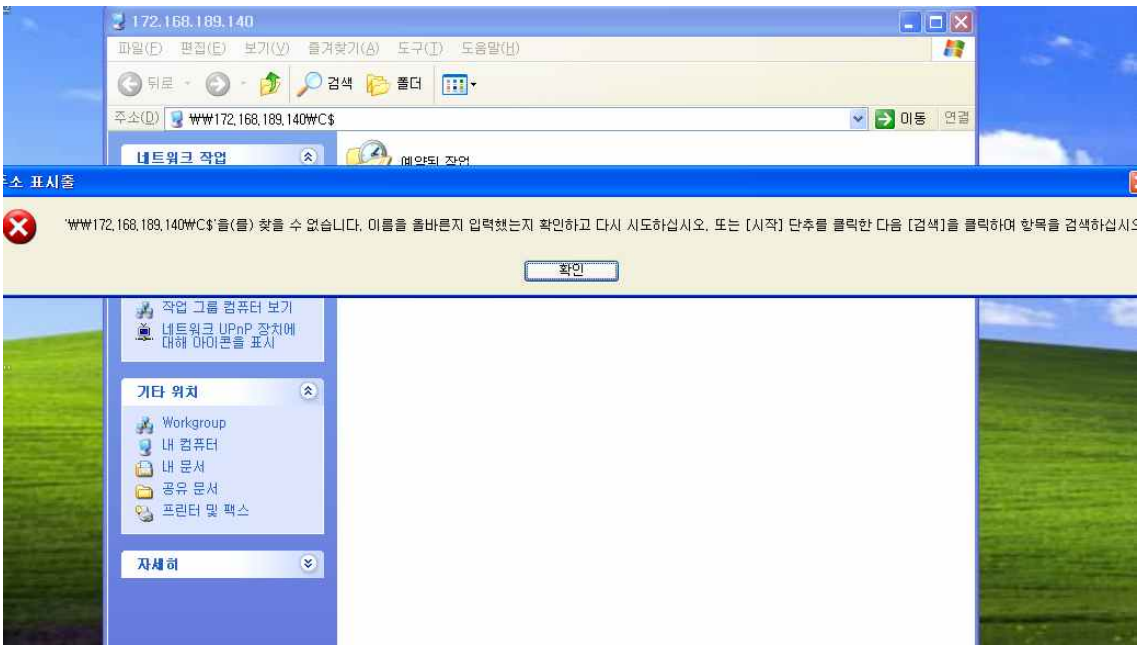
-> 설정 값 입력

- Value name : AutoShareServer
- DataType : DWORD(32bit)
- Value : 0(Zero)

※ 위 그림과 같이 AutoShareServer를 추가하거나 값을 '0'(Zero)로 변경합니다.

< 공유 폴더 제거 설정 후 테스트 결과 >

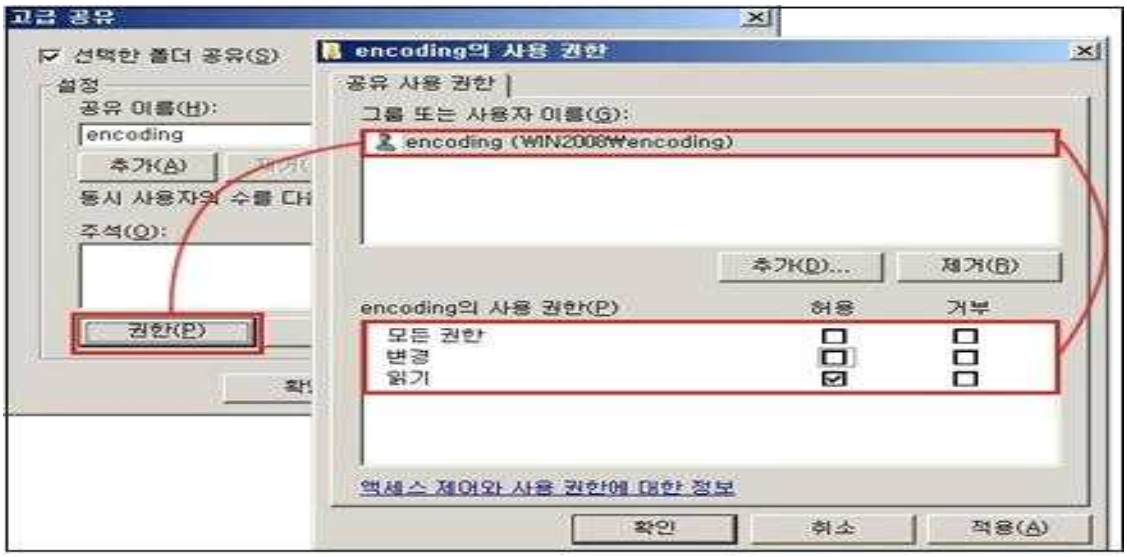




<그림78> XP의 환경의 다른 IP인 컴퓨터로 해당 서버의 공유가 중지된 것을 확인되었습니다. ADMIN$과 C$모두 엑세스 거부되었습니다.

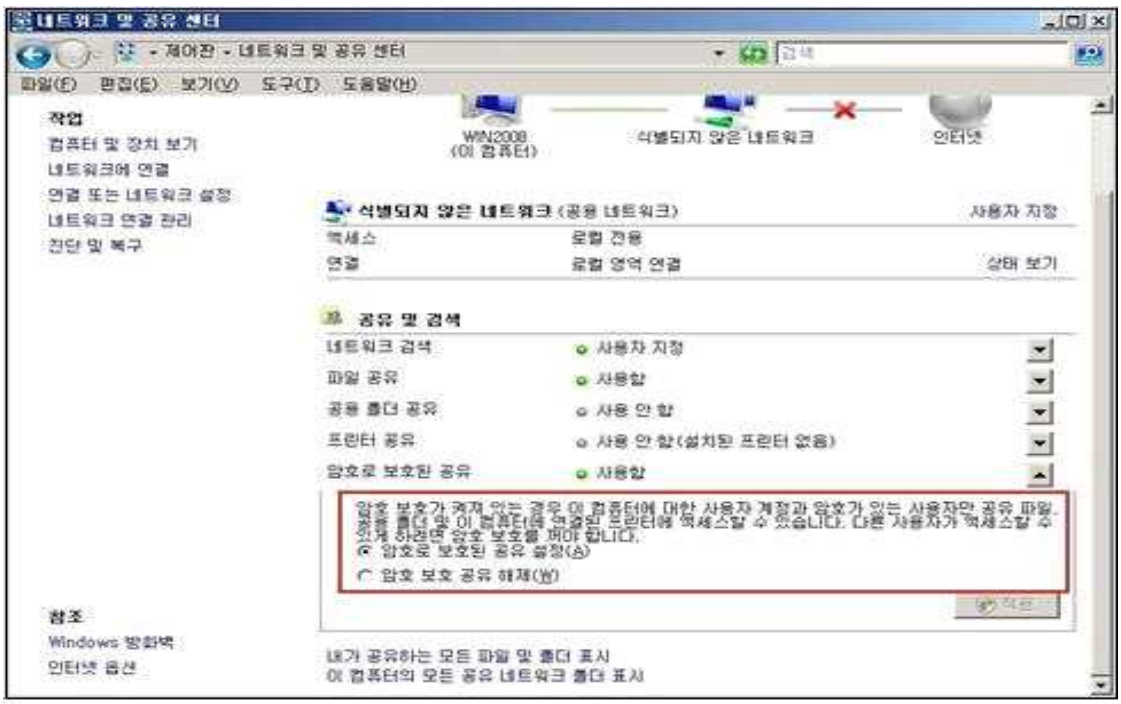
<공유 폴더 사용 시 권한 설정>

① 공유할 사용자 설정(Everyone의 권한 삭제)



<그림79> 공유 디렉토리 -> 속성 -> 공유탭 선택 -> 사용권한 에서 Everyone으로 된 공유를 제거하고, 접근이 필요한 계정에만 권한을 부여

② 공유 디렉토리에 접근 시 암호를 입력하도록 설정

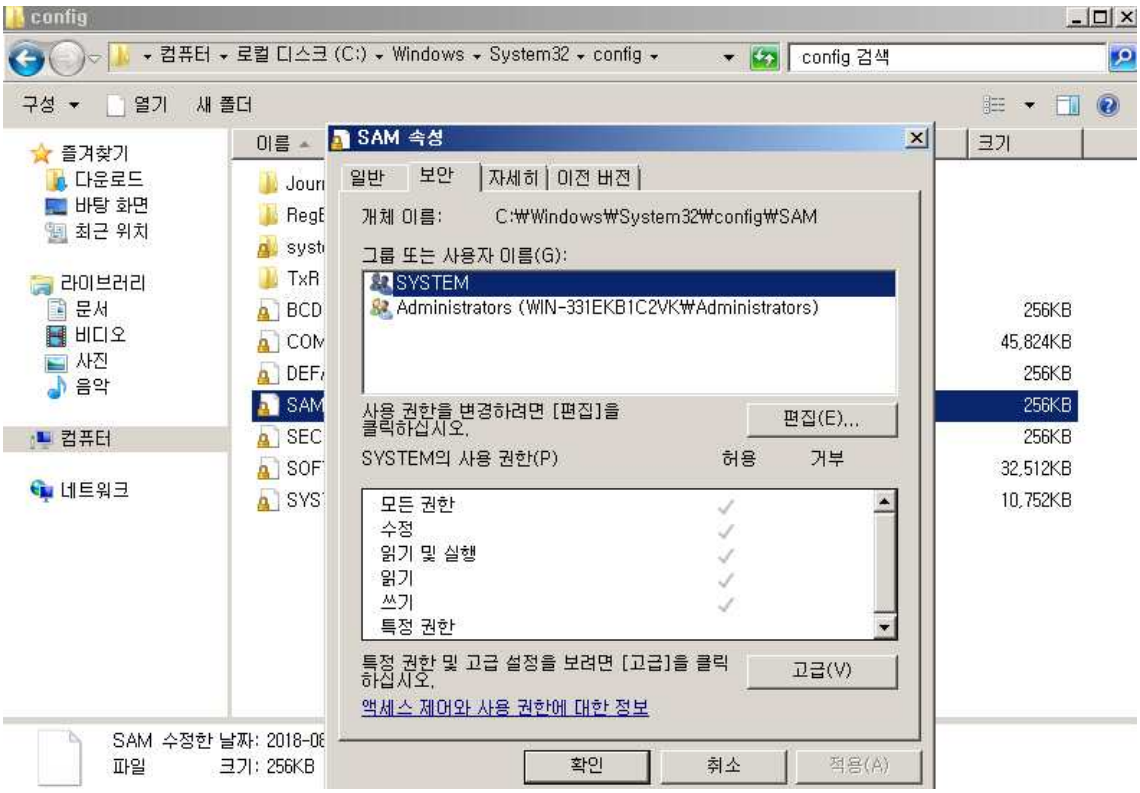


<그림80> 제어판 -> 네트워크 및 인터넷 -> 네트워크 및 공유센터 -> 암호로 보호된 공유에서 공유설정

■ 취약점 구분 : 파일 시스템 취약점

■ 취약점 항목 : SAM 파일 권한 설정

사용자와 그룹계정을 다루고 LSA 인증을 제공하는 SAM 파일 접근을 제한/설정합니다. Security Account Manager(SAM)파일은 시스템 내 사용자 계정과 그룹에 대한 정보를 보유하는 중요한 파일로, 패스워드 공격 시도에 의해 노출될 수 있으므로 Administrator 및 System 그룹 이외에는 SAM파일에 접근할 수 없도록 제한해야합니다.



<그림81>C:\Windows\System32\config\SAM파일 > 속성보안 > 권한설정

Administrator, System 그룹만 모든 권한으로 등록합니다.

■ 취약점 구분 : DoS 공격 대비 취약점

■ 취약점 항목 : 익명 사용자 권한 설정

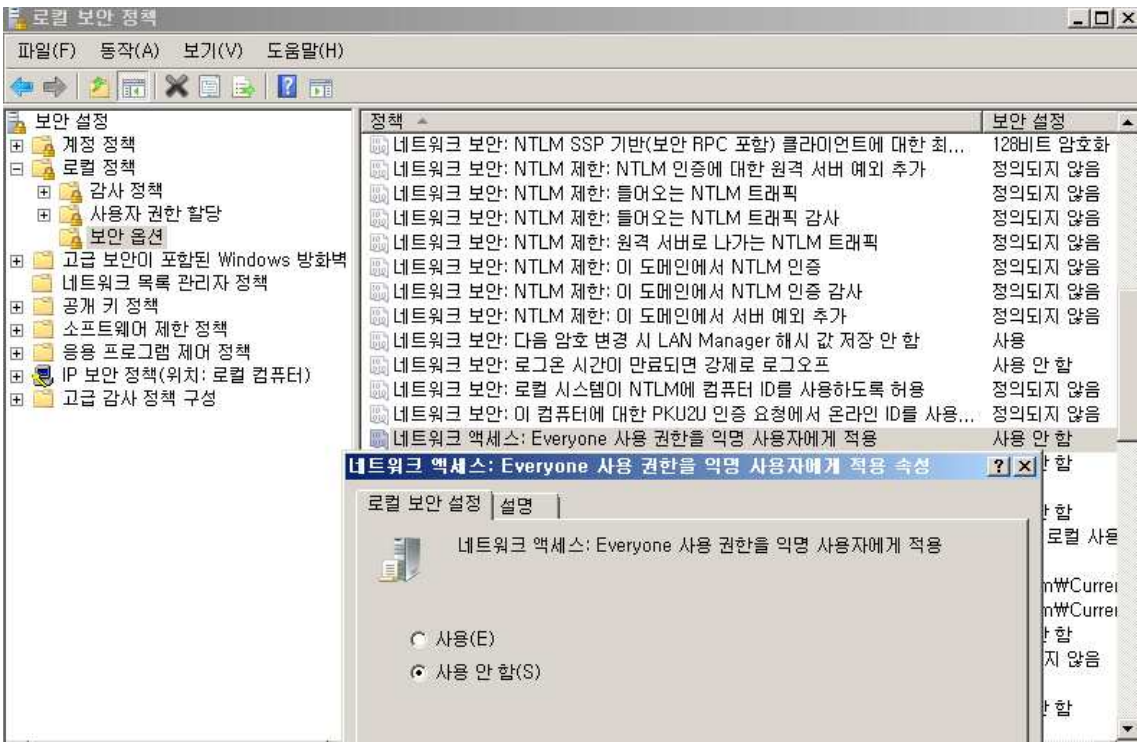
익명 사용자가 Everyone 그룹으로 사용 권한을 준 모든 리소스에 접근할지를 결정합니다. 만약 "사용"으로 설정할 경우 권한이 없는 사용자가 익명으로 계정 이름 및 공유 리소스를 나열하고 이 정보를 사용하여 암호를 추측하거나 DoS(Denial of Service) 공격을 실행 할 수 있습니다.

DoS(Denial of Service) : 관리자 권한 없이도 특정서버에 처리할 수 없을 정도로 대량의 접속 신호를 한꺼번에 보내 해당 서버가 마비되도록 하는 해킹 기법

양호 : "Everyone 사용 권한을 익명 사용자에게 적용 정책이 "사용 안 함" 설정.

취약 : "Everyone 사용 권한을 익명 사용자에게 적용 정책이 "사용" 설정.

네트워크 액세스 : Everyone 사용 권한을 익명 사용자에게 적용을 안 함으로서 보안 대비 설정을 합니다.



<그림82> 시작 -> 실행 -> 로컬 보안 정책 -> 로컬 정책 -> 보안 옵션

"Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용 안 함"으로 설정

이후에 애플리케이션이나 Backup 용도로 Everyone 공유를 사용하지 않는지 확인이 필요합니다.