서 울 대 학 교
SEOUL NATIONAL UNIVERSITY

『서울대학교』

Windows 취약점진단 보안가이드라인

서울대학교 정보화지원과

개 정 이 력

버전	변경일	변경 사유	변경 내용	작성자	비고
4.0	2019-04-16	내용 개정	신규 취약점 가이드 추가	서울대학교 정보화지원과 (정보보안)	
3.0	2018-10-04	내용 개정	내용 개정	서울대학교 정보화지원과 (정보보안)	
2.0	2017-04-14	내용 개정	내용 개정	서울대학교 정보화지원과 (정보보안)	
1.0	2012-06-23	최초 작성	최초 작성	서울대학교 정보화지원과 (정보보안)	

목 차

Windows 서버 취약점 분석·평가 항목

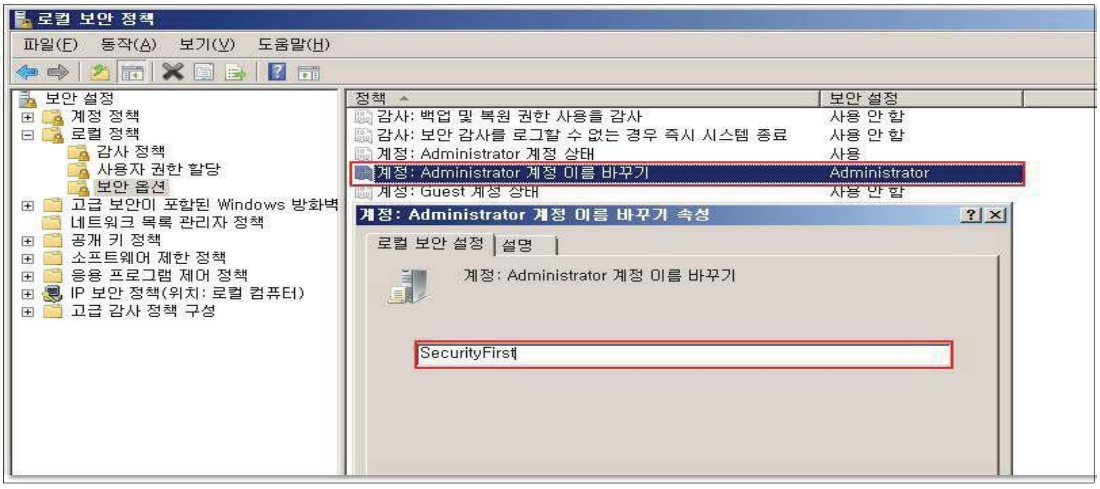
분류	소분류	점검항목	항목 중요도	항목 코드
1. 계정관리	1.1	Administrator 계정 이름 바꾸기	상	W-01
	1.2	Guest 계정 상태	상	W-02
	1.3	불필요한 계정 제거	상	W-03
	1.4	계정 잠금 임계값 설정	상	W-04
	1.5	해독 가능한 암호화를 사용하여 암호 저장 해제	상	W-05
	1.6	관리자 그룹에 최소한의 사용자 포함	상	W-06
	1.7	Everyone 사용권한을 익명 사용자에 적용 해제	중	W-07
	1.8	계정 잠금 기간 설정	중	W-08
	1.9	패스워드 복잡성 설정	중	W-09
	1.10	패스워드 최소 암호 길이	중	W-10
	1.11	패스워드 최대 사용 기간	중	W-11
	1.12	패스워드 최소 사용 기간	중	W-12
	1.13	마지막 사용자 이름 표시 안함	중	W-13
	1.14	로컬 로그온 허용	중	W-14
	1.15	익명 SID/이름 변환 허용 해제	중	W-15
	1.16	최근 암호 기억	중	W-16
	1.17	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	중	W-17
	1.18	원격터미널 접속 가능한 사용자 그룹 제한	중	W-18
2. 파일 및 디렉터리 관리	2..1	공유 권한 및 사용자 그룹 설정	상	W-19
	2.2	하드디스크 기본 공유 제거	상	W-20
	2.3	불필요한 서비스 제거	상	W-21
	2.4	IIS 서비스 구동 점검	상	W-22
	2.5	IIS 디렉토리 리스팅 제거	상	W-23
	2.6	IIS CGI 실행 제한	상	W-24
	2.7	IIS 상위 디렉토리 접근 금지	상	W-25
	2.8	IIS 불필요한 파일 제거	상	W-26
	2.9	IIS 웹프로세스 권한 제한	상	W-27
	2.10	IIS 링크 사용 금지	상	W-28
	2.11	IIS 파일 업로드 및 다운로드 제한	상	W-29

	2.12	IIS DB 연결 취약점 점검	상	W-30
	2.13	IIS 가상 디렉토리 삭제	상	W-31
	2.14	IIS 데이터파일 ACL 적용	상	W-32
	2.15	IIS 미사용 스크립트 매핑 제거	상	W-33
	2.16	IIS Exec 명령어 쉘 호출 진단	상	W-34
	2.17	IIS WebDAV 비활성화	상	W-35
	2.18	NetBIOS 바인딩 서비스 구동 점검	상	W-36
	2.19	FTP 서비스 구동 점검	상	W-37
	2.20	FTP 디렉토리 접근 권한 설정	상	W-38
	2.21	Anonymous FTP 금지	상	W-39
	2.22	FTP 접근 제어 설정	상	W-40
	2.23	DNS Zone Transfer 설정	상	W-41
	2.24	RDS(Remonte Data Services) 제거	상	W-42
	2.25	최신 서비스팩 적용	상	W-43
	2.26	터미널 서비스 암호화 수준 설정	중	W-44
	2.27	IIS 웹 서비스 정보 숨김	중	W-45
	2.28	SNMP 서비스 구동 점검	중	W-46
	2.29	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	W-47
	2.30	SNMP Access control 설정	중	W-48
	2.31	DNS 서비스 구동 점검	중	W-49
	2.32	HTTP/FTP/SMTP 배너 차단	하	W-50
	2.33	Telnet 보안 설정	중	W-51
	2.34	불필요한 ODBC/OLE-DB 데이터소스와 드라이브 제거	중	W-52
	2.35	원격터미널 접속 타임아웃 설정	중	W-53
	2.36	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중	W-54
3. 서비스 관리	3.1	최신 HOT FIX 적용	상	W-55
	3.2	백신 프로그램 업데이트	상	W-56
	3.3	정책에 따른 시스템 로깅설정	중	W-57
4. 로그 관리	4.1	로그의 정기적 검토 및 보고	상	W-58
	4.2	원격으로 액세스 할 수 있는 레지스트리 경로	상	W-59
	4.3	이벤트 로그 관리 설정	하	W-60
	4.4	원격에서 이벤트 로그파일 접근 차단	중	W-61

5. 보안 관리	5.1	백신 프로그램 설치	상	W-62
	5.2	SAM 파일 접근 통제 설정	상	W-63
	5.3	화면보호기 설정	상	W-64
	5.4	로그온 하지 않고 시스템 종료 허용 해제	상	W-65
	5.5	원격 시스템에서 강제로 시스템 종료	상	W-66
	5.6	보안감사를 로그할 수 없는 경우 즉시 시스템 종료 해제	상	W-67
	5.7	SAM 계정과 공유의 익명 열거 허용 안함	상	W-68
	5.8	Autologin 기능 제어	상	W-69
	5.9	이동식 미디어 포맷 및 꺼내기 허용	상	W-70
	5.10	디스크 볼륨 암호화 설정	상	W-71
	5.11	Dos 공격 방어 레지스트리 설정	중	W-72
	5.12	사용자가 프린터 드라이버를 설치할 수 없게 함	중	W-73
	5.13	세션 연결을 중단하기 전에 필요한 유휴시간	중	W-74
	5.14	경고 메시지 설정	하	W-75
	5.15	사용자별 홈 디렉토리 권한 설정	중	W-76
	5.16	LAN Manager 인증 수준	중	W-77
	5.17	보안 채널 데이터 디지털 암호화 또는 서명	중	W-78
	5.18	파일 및 디렉토리 보호	중	W-79
	5.19	컴퓨터 계정 암호 최대 사용 기간	중	W-80
	5.20	시작 프로그램 목록 분석	중	W-81
6. DB 관리	6.1	Windows 인증 모드 사용	중	W-82

1. 계정 관리

1.1. Administrator 계정 이름 바꾸기

W-01 (상)	1. 계정관리 > Administrator 계정 이름 바꾸기
취약점 개요	
점검내용	• 윈도우즈 최상위 관리자 계정인 Administrator의 계정명 변경 여부 점검
점검목적	• 윈도우즈 기본 관리자 계정인 Administrator의 이름을 변경하여, 잘 알려진 계정을 통한 악의적인 패스워드 추측 공격을 차단하고자 함
보안위협	• 일반적으로 관리자 계정으로 잘 알려진 Administrator를 변경하지 않은 경우 악의적인 사용자의 패스워드 추측 공격을 통해 사용 권한 상승의 위험이 있으며, 관리자를 유인하여 침입자의 액세스를 허용하는 악성코드를 실행할 우려가 있음 • 윈도우즈 최상위 관리자 계정인 Administrator는 기본적으로 삭제하거나 잠글 수 없어 악의적인 사용자의 목표가 됨
참고	※ 윈도우즈 서버는 Administrator 계정을 비활성화 할 수 있으나 안전 모드로 컴퓨터를 시작할 경우 본 계정은 자동으로 활성화 됨
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : Administrator Default 계정 이름을 변경한 경우
	취약 : Administrator Default 계정 이름을 변경하지 않은 경우
조치방법	Administrator Default 계정 이름 변경
점검 및 조치 사례	
• Window NT, 2000, 2003, 2008, 2012 Step 1) 시작> 프로그램> 제어판> 관리도구> 로컬 보안 정책> 로컬 정책> 보안옵션 Step 2) "계정: Administrator 계정 이름 바꾸기"를 유지하기 어려운 계정 이름으로 변경  	
조치 시 영향	일반적인 경우 영향 없음

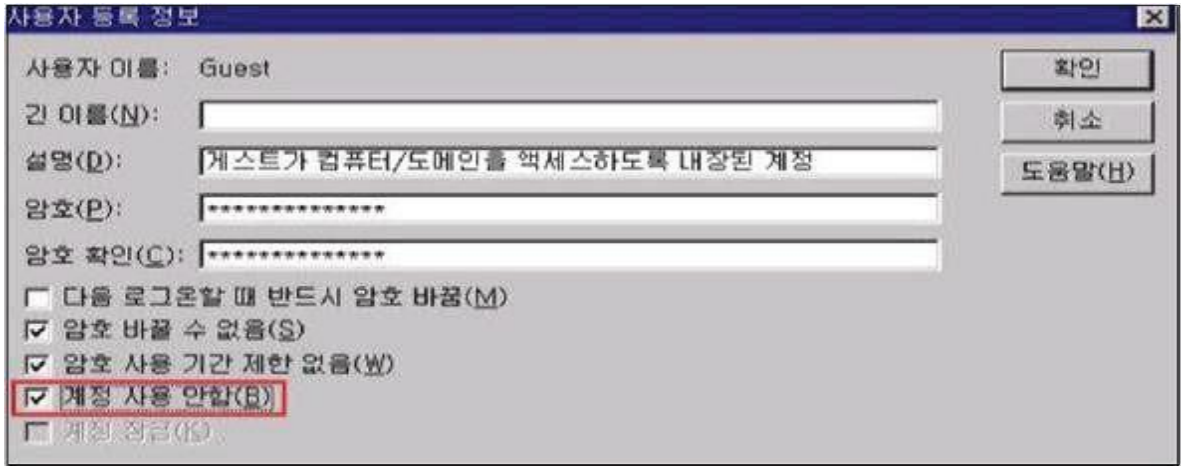
1.2. Guest 계정 상태

W-02 (상)	1. 계정관리 > Guest 계정 상태
취약점 개요	
점검내용	• Guest 계정 비활성화 여부 점검
점검목적	• Guest 계정을 비활성화 하여 불특정 다수의 임시적인 시스템 접근을 차단하기 위함
보안위협	• Guest 계정은 시스템에 임시로 액세스해야 하는 사용자용 계정으로, 이 계정을 사용하여 권한 없는 사용자가 시스템에 익명으로 액세스할 수 있으므로 비인가자 접근, 정보 유출 등 보안 위험이 따를 수 있음
참고	※ 윈도우즈 Guest 계정은 삭제가 불가능한 built-in 계정으로 보안 강화 목적으로 반드시 비활성화 처리 하여야 함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : Guest 계정이 비활성화 되어 있는 경우
	취약 : Guest 계정이 활성화 되어 있는 경우
조치방법	Guest 계정 비활성화
점검 및 조치 사례	

• Window NT

Step 1) 시작> 프로그램> 관리도구> 도메일 사용자 관리> Guest 계정 선택> 등록정보

Step 2) "계정 사용 안함"에 체크

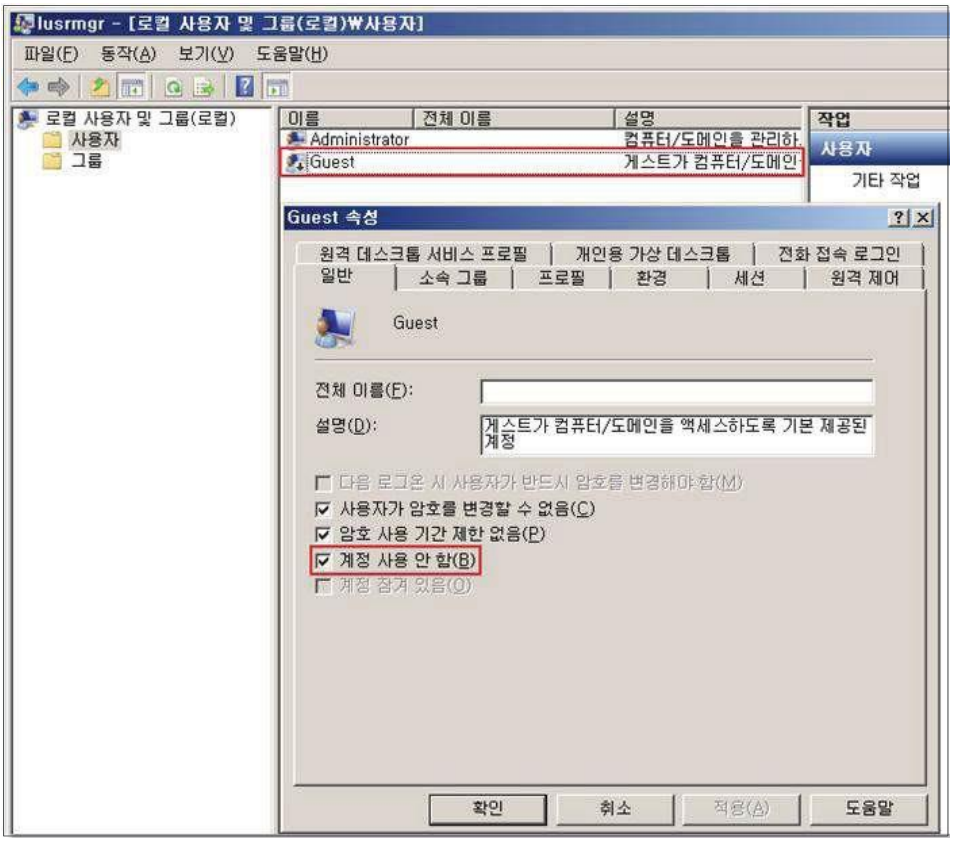


W-02 (상)	1. 계정관리 > Guest 계정 상태

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> LUSRMGR.MSC> 사용자> GUEST> 속성

Step 2) "계정 사용 안 함"에 체크



조치 시 영향	일반적인 경우 영향 없음

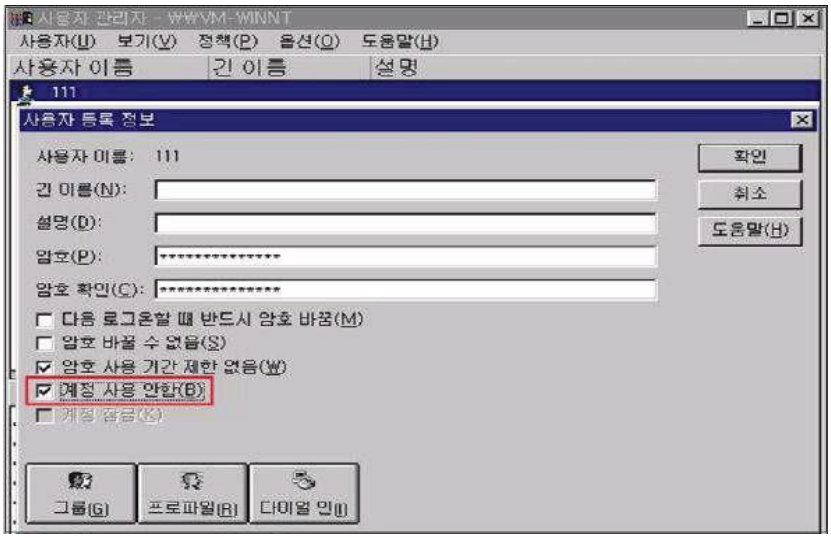
1.3. 불필요한 계정 제거

W-03 (상)	1. 계정관리 > 불필요한 계정 제거
취약점 개요	
점검내용	• 시스템 내 불필요한 계정 및 의심스러운 계정의 존재 여부를 점검
점검목적	• 퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정 및 의심스러운 계정을 삭제하여, 일반적으로 로그인이 필요지 않은 해당 계정들을 통한 로그인을 차단하고, 계정의 패스워드 추측 공격 시도를 차단하고자 함
보안위협	• 관리되지 않은 불필요한 계정은 장기간 패스워드가 변경되지 않아 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격 (Password Guessing Attack)의 가능성이 존재하며, 또한 이런 공격에 의해 계정 정보가 유출되어도 유출 사실을 인지하기 어려움
참고	※ 무작위 대입 공격(Brute Force Attack): 컴퓨터로 암호를 해독하기 위해 조합 가능한 모든 경우의 수를 다 대입해보는 것을 말함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 불필요한 계정이 존재하지 않는 경우
	취약 : 불필요한 계정이 존재하는 경우
조치방법	현재 계정 현황 확인 후 불필요한 계정 삭제
점검 및 조치 사례	

• Window NT

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리> 계정 선택> 등록 정보

Step 2) "계정 사용 안 함"에 체크하거나 계정 삭제

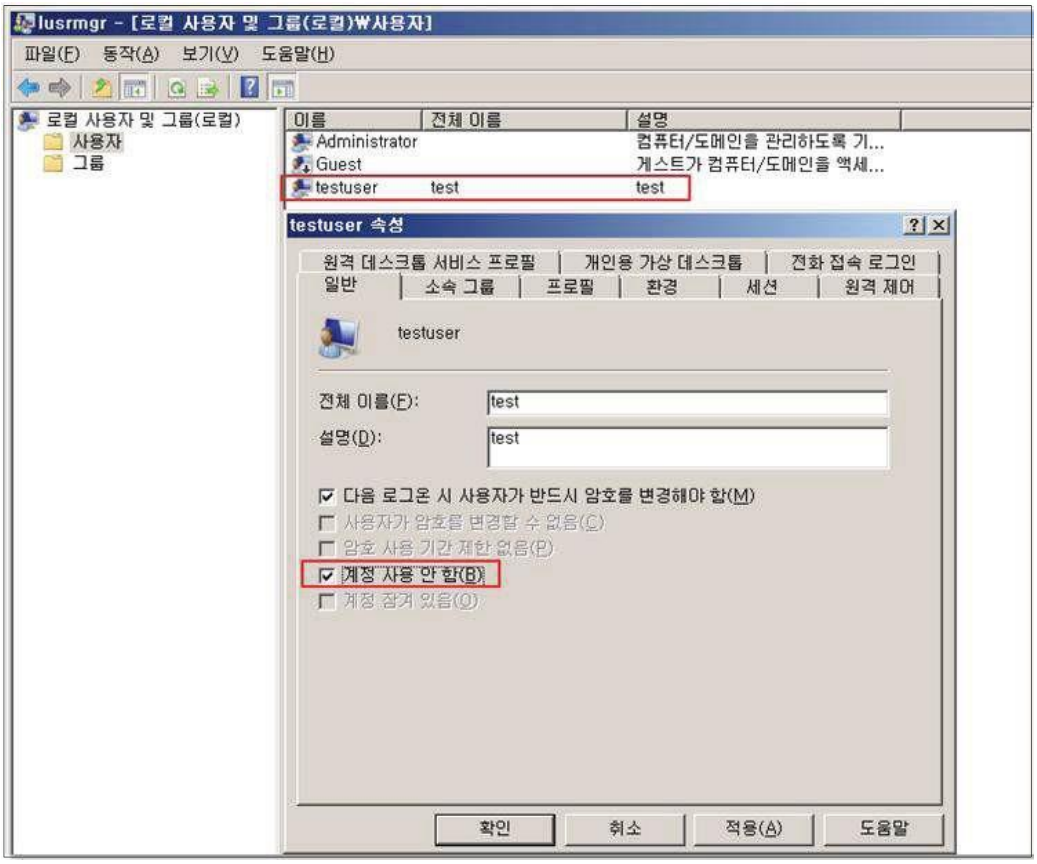


W-03 (상)	1. 계정관리 > 1.3 불필요한 계정 제거

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> LUSRMGR.MSC> 사용자

Step 2) 등록된 계정 중 불필요한 사용자 선택> 속성> "계정 사용 안 함"에 체크하거나 계정 삭제



조치 시 영향	명확하게 파악되지 않은 계정을 삭제하는 경우 해당 계정과 관련한 업무에 장애발생 가능성이 존재함

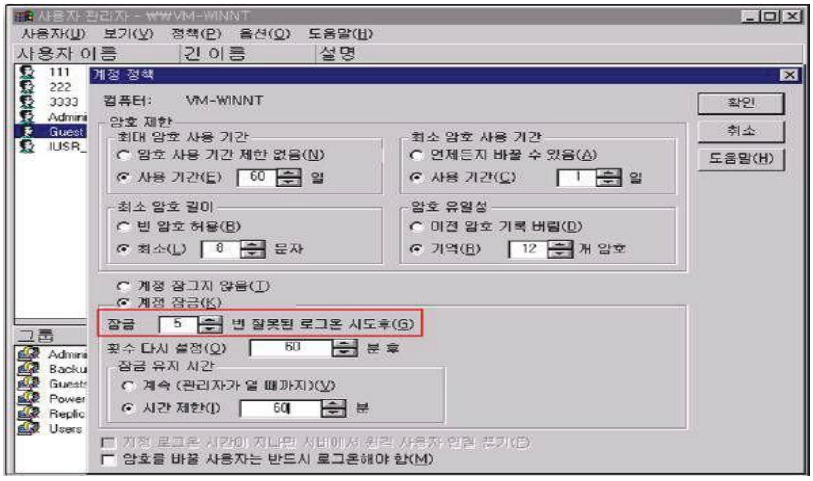
1.4. 계정 잠금 임계값 설정

W-04 (상)	1. 계정관리 > 계정 잠금 임계값 설정
취약점 개요	
점검내용	• 계정 잠금 임계값의 설정 여부 점검
점검목적	• 계정 잠금 임계값을 설정하여 공격자의 자유로운 자동화 암호 유지 공격을 차단하기 위함
보안위협	• 공격자는 시스템의 계정 잠금 임계값이 설정되지 않은 경우 자동화된 방법을 이용하여 모든 사용자 계정에 대해 암호조합 공격을 자유롭게 시도할 수 있으므로 사용자 계정 정보의 노출 위험이 있음
참고	※ 계정 잠금 임계값 설정은 사용자 계정이 잠기는 로그온 실패 횟수를 결정하며 잠긴 계정은 관리자가 재설정하거나 해당 계정의 잠금 유지 시간이 만료되어야 사용할 수 있음 ※ 계정 잠금 정책: 해당 계정이 시스템으로부터 잠기는 환경과 시간을 결정하는 정책으로 '계정 잠금 기간', '계정 잠금 임계값', '다음 시간 후 계정 잠금 수를 원래대로 설정'의 세가지 하위 정책을 가짐 ※ 관련 점검 항목 : W-08(중)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우
	취약 : 계정 잠금 임계값이 6 이상의 값으로 설정되어 있는 경우
조치방법	계정 잠금 임계값을 5번 이하의 값으로 설정
점검 및 조치 사례	

• Window NT

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정 정책

Step 2) "계정 잠금" 선택 후 "잠금"에 "5"이하의 값 설정

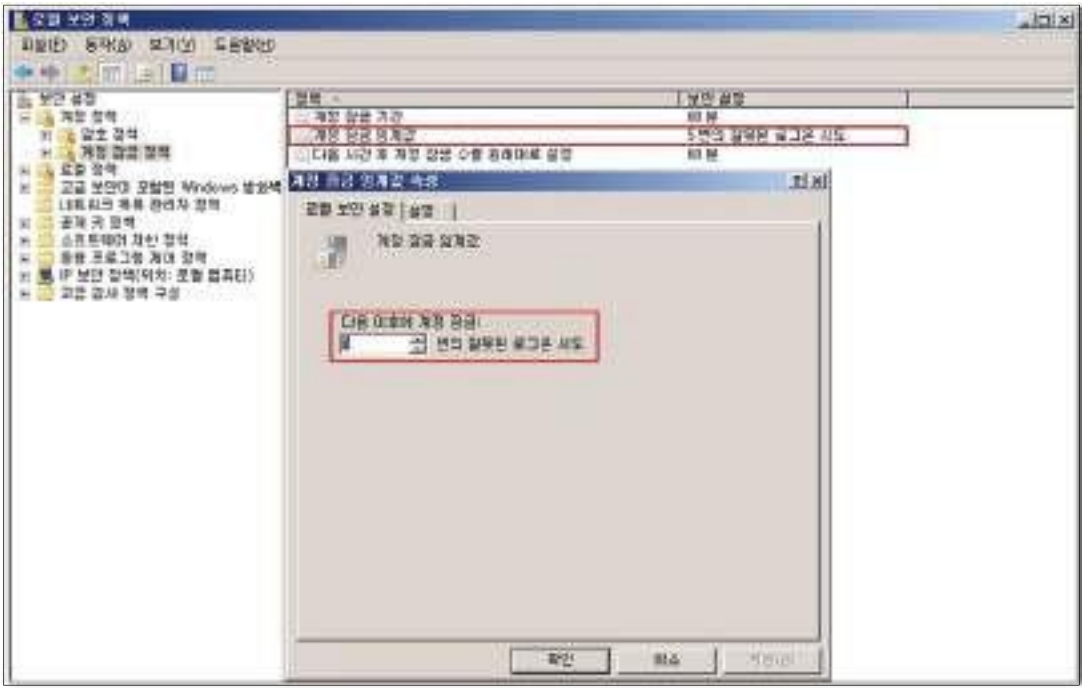


W-04 (상)	1. 계정관리 > 계정 잠금 임계값 설정

- Windows 2000, 2003, 2008, 2012

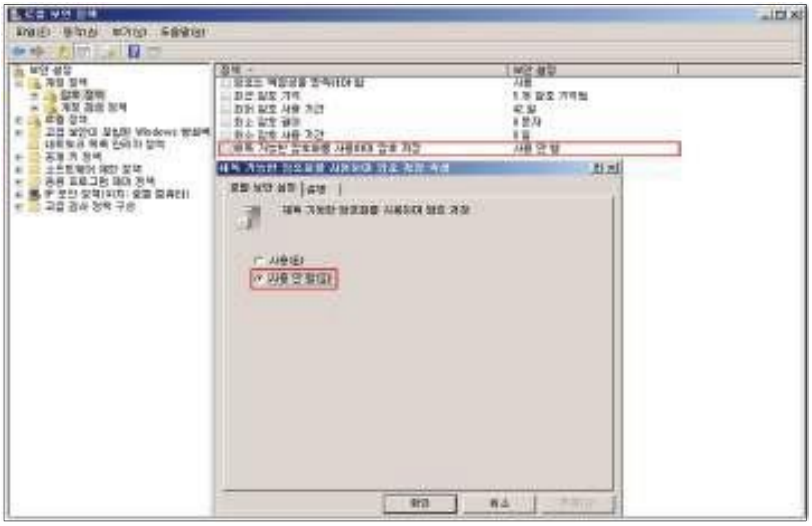
Step 1) 시작> 실행> SECPOL.MSC> 계정 정책> 계정 잠금 정책

Step 2) "계정 잠금 임계값"을 "5"이하의 값으로 설정



조치 시 영향	Administrator 계정은 잠기지 않으며, 일반 계정의 경우 5번 패스워드 입력 실패 시 잠김

1.5. 해독 가능한 암호화를 사용하여 암호 저장 해제

W-05 (상)	1. 계정관리 > 해독 가능한 암호화를 사용하여 암호 저장 해제
취약점 개요	
점검내용	• 해독 가능한 암호화 사용 여부 점검
점검목적	• '해독 가능한 암호화를 사용하여 암호 저장' 정책이 설정되어 사용자 계정 비밀번호가 해독 가능한 텍스트 형태로 저장 되는 것을 차단하기 위함
보안위협	• 위 정책이 설정된 경우 OS에서 사용자 ID, PW를 입력받아 인증을 진행하는 응용프로그램 프로토콜 지원 시 OS 는 사용자의 PW 를 해독 가능한 방식으로 암호를 저장하기 때문에, 노출된 계정에 대해 공격자가 암호 복호화 공격으로 PW를 획득하여 네트워크 리소스에 접근할 수 있음
참고	※ '해독 가능한 암호화를 사용하여 암호 저장' 정책은 암호를 암호화 하지 않은 상태로 저장하여 일반 텍스트 버전의 암호를 저장하는 것과 같으나 시스템에서 기본적으로 동작하지는 않음
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용 안 함" 으로 되어 있는 경우
	취약 : "해독 가능한 암호화를 사용하여 암호 저장" 정책이 "사용" 으로 되어 있는 경우
조치방법	"해독 가능한 암호화를 사용하여 암호 저장"을 "사용 안 함"으로 설정
점검 및 조치 사례	
• Window NT, 2000, 2003, 2008, 2012 Step 1) 시작> 실행> SECPOL.MSC> 계정 정책> 암호 정책 Step 2) "해독 가능한 암호화를 사용하여 암호 저장"을 "사용 안 함"으로 설정 	
조치 시 영향	일반적인 경우 영향 없음

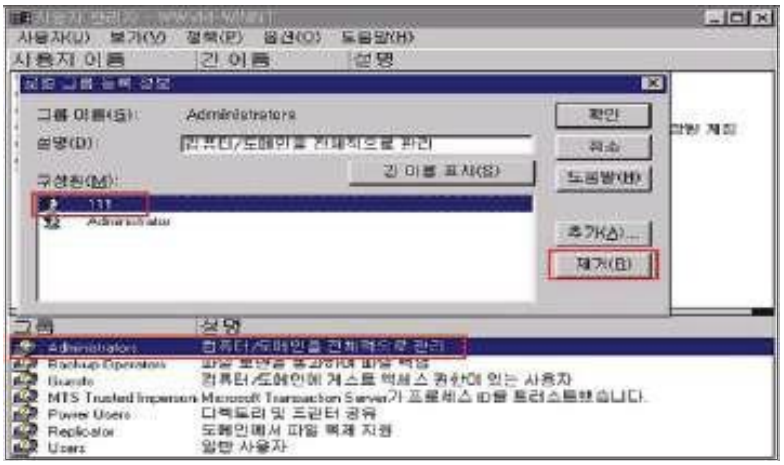
1.6. 관리자 그룹에 최소한의 사용자 포함

W-06 (상)	1. 계정관리 > 관리자 그룹에 최소한의 사용자 포함
취약점 개요	
점검내용	• 관리자 그룹에 불필요한 사용자의 포함 여부 점검
점검목적	• 관리자 그룹 구성원에 불필요한 사용자의 포함 여부를 점검하여, 관리 권한자를 최소화 하고자 함
보안위협	• Administrators와 같은 관리자 그룹에 속한 구성원은 컴퓨터 시스템에 대한 완전하고 제한 없는 액세스 권한을 가지므로, 사용자를 관리자 그룹에 포함시킬 경우 비인가 사용자에 대한 과도한 관리 권한이 부여될 수 있음
참고	※ 관리 권한의 오남용으로 인한 시스템 피해를 줄이기 위해서 관리 업무를 위한 계정과 일반 업무를 위한 계정을 분리하여 사용하는 것이 바람직함 ※ 시스템 관리를 위해서 관리권한 계정과 일반권한 계정을 분리하여 운영하는 것을 권고 ※ 시스템 관리자는 원칙적으로 1명 이하로 유지하고, 부득이하게 2명 이상의 관리 권한자를 유지하여야 하는 경우에는 관리자 그룹에는 최소한의 사용자만 포함하도록 하여야 함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : Administrators 그룹의 구성원을 1명 이하로 유지하거나, 불필요한 관리자 계정이 존재하지 않는 경우
	취약 : Administrators 그룹에 불필요한 관리자 계정이 존재하는 경우
조치방법	Administrators 그룹에 포함된 불필요한 계정 제거
점검 및 조치 사례	

• Window NT

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리> Administrators 그룹> 등록 정보

Step 2) Administrator 그룹에서 불필요한 계정 제거 후 그룹 변경

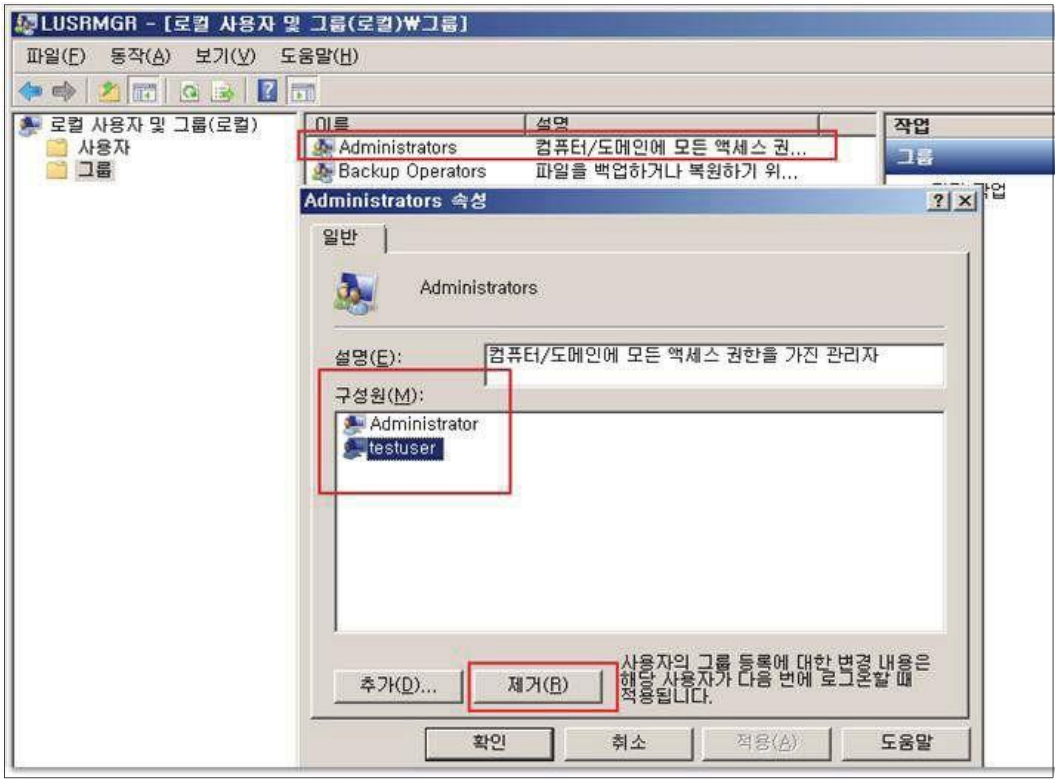


W-06 (상)	1. 계정관리 > 관리자 그룹에 최소한의 사용자 포함

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> LUSRMGR.MSC> 그룹> Administrators> 속성

Step 2) Administrators 그룹에서 불필요한 계정 제거 후 그룹 변경



조치 시 영향	Administrator 그룹에 있는 계정을 잘못 삭제하는 경우 해당 업무에 장애 발생 가능성이 있음

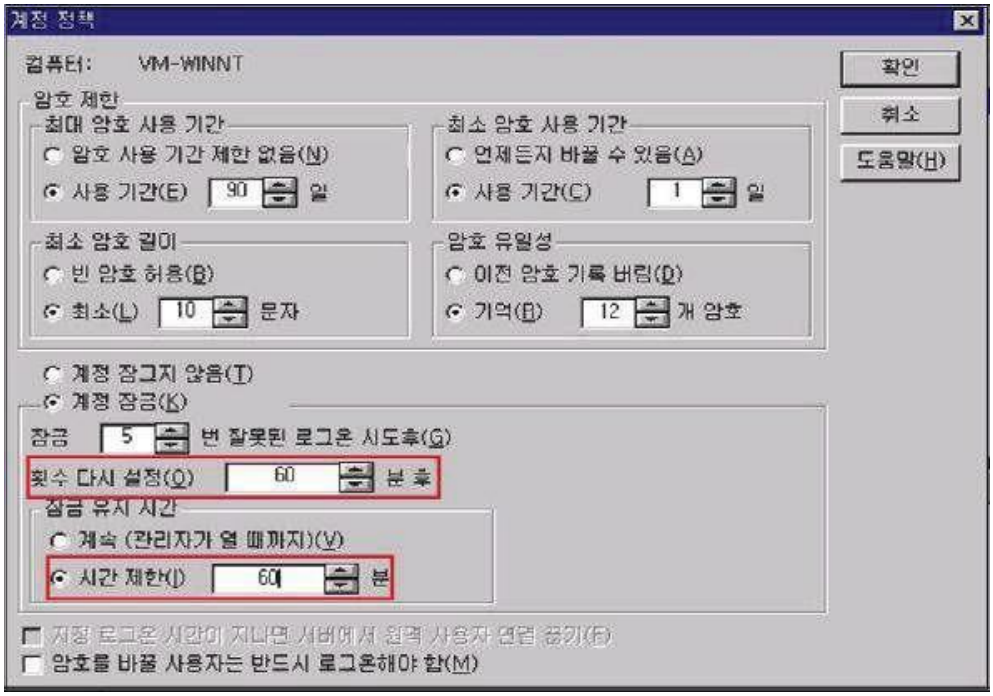
1.7. Everyone 사용 권한을 익명 사용자에게 적용 해제

W-07 (중)	1. 계정관리 > Everyone 사용 권한을 익명 사용자에 적용 해제
취약점 개요	
점검내용	• 'Everyone 사용 권한을 익명 사용자에 적용' 정책의 설정 여부 점검
점검목적	• 익명 사용자가 Everyone 그룹으로 사용 권한을 준 모든 리소스에 접근하는 것을 차단하여 비인가자에 의한 접근 가능성을 제한하기 위함
보안위협	• 해당 정책이 "사용"으로 설정될 경우 권한이 없는 사용자가 익명으로 계정 이름 및 공유 리소스를 나열하고 이 정보를 사용하여 암호를 추측하거나 DoS(Denial of Service) 공격을 실행할 수 있음
참고	※ DoS(Denial of Service): 관리자 권한 없이도 특정서버에 처리할 수 없을 정도로 대량의 접속신호를 한꺼번에 보내 해당 서버가 마비되도록 하는 해킹 기법
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용 안 함" 으로 되어 있는 경우
	취약 : "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용" 으로 되어 있는 경우
조치방법	네트워크 액세스: Everyone 사용 권한을 익명 사용자에게 적용->사용 안 함
점검 및 조치 사례	
• Window 2003, 2008, 2012 Step 1) 시작> 실행> SELPOL.MSC> 로컬 정책> 보안 옵션 Step 2) "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용 안 함"으로 설정 	
조치 시 영향	애플리케이션이나 Backup 용도로 Everyone 공유를 사용하지 않는지 확인 필요

1.8. 계정 잠금 기간 설정

W-08 (중)	1. 계정관리 > 계정 잠금 기간 설정
취약점 개요	
점검내용	• 사용자 계정 잠금 기간 정책 설정 여부 점검
점검목적	• 로그인 실패 임계값 초과 시 일정 시간 동안 계정 잠금을 실시하여 공격자의 자유로운 암호 유지 공격을 차단하기 위함
보안위협	• 로그인 실패 시 일정 시간 동안 계정 잠금을 하지 않은 경우, 공격자의 자동화된 암호 추측 공격이 가능하여, 사용자 계정의 패스워드 정보가 유출될 수 있음
참고	※ 계정 잠금 기간 설정은 계정 잠금 임계값을 초과한 사용자 계정이 잠기는 시간을 결정함. 잠긴 계정은 관리자가 재설정하거나 해당 계정의 잠금 유지 시간이 만료되어야 사용할 수 있음 ※ 계정 잠금 기간 설정을 사용하면 지정한 기간 동안 잠긴 계정은 사용할 수 없으며, 계정 잠금이 해제될 때까지 접근할 수 없음 ※ 계정 잠금 정책: 해당 계정이 시스템으로부터 잠기는 환경과 시간을 결정하는 정책으로 '계정 잠금 기간', '계정 잠금 임계값', '다음 시간 후 계정 잠금 수를 원래대로 설정'의 세가지 하위 정책을 가짐 ※ 관련 점검 항목 : W-4(상)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "계정 잠금 기간" 및 "계정 잠금 기간 원래대로 설정 기간"이 설정되어 있는 경(60분 이상의 값으로 설정하기를 권고함)
	취약 : "계정 잠금 기간" 및 "잠금 기간 원래대로 설정 기간"이 설정되지 않은 경우
조치방법	"계정 잠금 기간" 및 "잠금 기간 원래대로 설정 기간" 60분 설정
점검 및 조치 사례	
• Window NT Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정 정책 Step 2) "횟수 다시 설정"을 "60분 후"로 설정, "잠금 유지 기간"의 "시간 제한"을 "60분" 으로 설정	

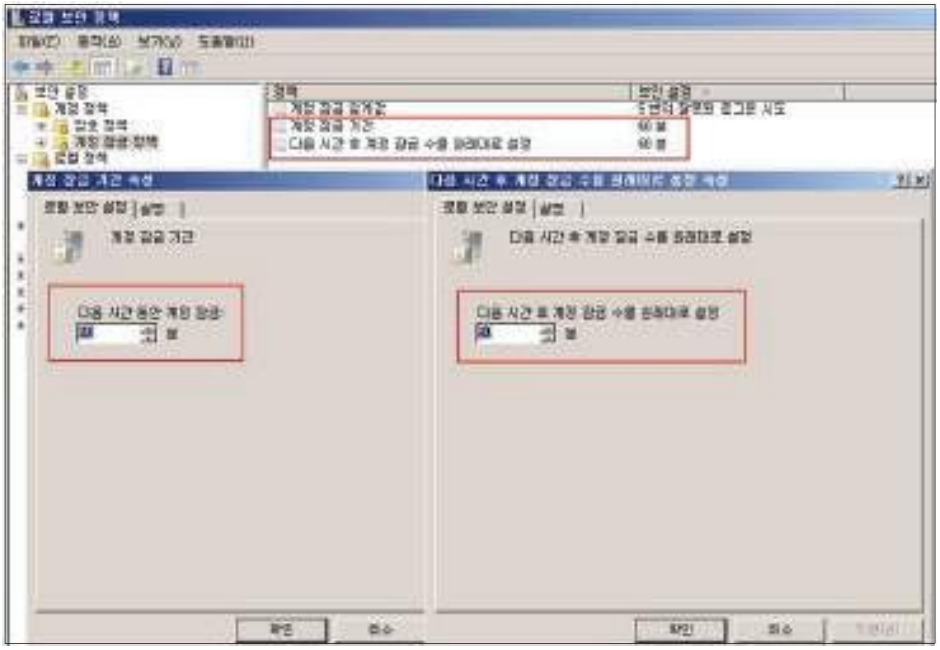
W-08 (중)	1. 계정관리 > 계정 잠금 기간 설정



- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 계정 정책> 계정 잠금 정책

Step 2) "계정 잠금 기간", "다음 시간 후 계정 잠금 수를 원래대로 설정"에 대해 각각 "60분" 설정



조치 시 영향	일반적으로 영향 없음

1.9. 패스워드 복잡성 설정

W-09 (중)	1. 계정관리 > 패스워드 복잡성 설정
취약점 개요	
점검내용	• 계정 패스워드 복잡성 정책 설정 여부 점검
점검목적	• 패스워드 설정 시 문자/숫자/특수문자를 모두 포함한 강화된 패스워드를 사용하여 패스워드 복잡성을 만족하도록 함
보안위협	• 사용자 암호가 패스워드 복잡성을 만족하지 못하는 반복되는 문자, 연속되는 숫자, 계정이름이 포함된 패스워드 등을 사용할 경우 무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격(Password Guessing Attack)에 쉽게 크랙될 수 있음
참고	※ 패스워드 설정 시 영문/숫자/특수문자를 모두 포함하여 강력한 패스워드가 설정될 수 있도록 암호 복잡성을 설정하여야 함 ※ 영·숫자만으로 이루어진 암호는 현재 공개된 패스워드 크랙 유틸리티에 의해 쉽게 유지할 수 있으므로 패스워드 조합 및 길이에 따라 최소 암호 길이 및 암호 복잡성을 적절하게 설정하여 패스워드를 알아낼 수 있는 평균 시간을 증가시킬 수 있도록 설정하여야 함 ※ 관련 점검 항목 : W-10(중), W-11(중), W-12(중)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "암호는 복잡성을 만족해야 함" 정책이 "사용" 으로 되어 있는 경우
	취약 : "암호는 복잡성을 만족해야 함" 정책이 "사용 안 함" 으로 되어 있는 경우
조치방법	암호는 복잡성을 만족해야 함 -+ 사용
점검 및 조치 사례	

• Windows NT, 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 계정 정책> 암호 정책

Step 2) "암호는 복잡성을 만족해야 함"을 "사용"으로 설정

W-09 (중)	1. 계정관리 > 패스워드 복잡성 설정

※ 이 정책 설정은 암호를 변경하거나 새로운 암호 생성 시 아래와 같은 일련의 규정을 만족하는지 결정함. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는, 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

가. 영문 대문자(26개)
나. 영문 소문자(26개)
다. 숫자(10개)
라. 특수문자(32개)

조치 시 영향	일반적으로 영향 없음

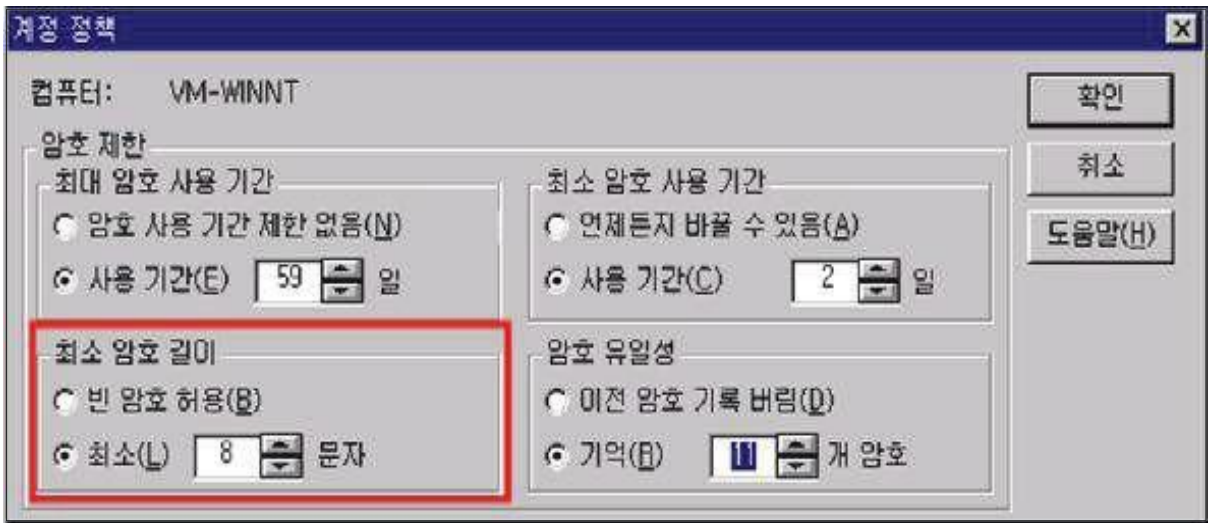
1.10. 패스워드 최소 암호 길이

W-10 (중)	1. 계정관리 > 패스워드 최소 암호 길이
취약점 개요	
점검내용	• 패스워드 최소 암호 길이 정책 설정 여부 점검
점검목적	• 암호에 필요한 최소 문자 수를 지정하여 강화된 패스워드를 사용하기 위함
보안위협	• 짧은 패스워드 및 일반적인 단어와 일반적인 어구를 이용해 암호를 설정한 경우 사전 공격이나 가능한 모든 문자의 조합을 시도하는 무작위 공격을 통해 쉽게 패스워드가 도용될 수 있음
참고	※ 암호정책: 사용자에게 암호를 정기적으로 변경하게 하고, 암호의 최소 길이를 지정하며, 암호가 특정 복잡성을 만족시키도록 하는 등 암호 설정을 사용자 강제하여 컴퓨터를 보호하는 정책 ※ 관련 점검 항목 : W-09(중), W-11(중), W-12(중)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 최소 암호 길이가 8문자 이상으로 설정되어 있는 경우
	취약 : 최소 암호 길이가 설정되지 않았거나 8문자 미만으로 설정되어 있는 경우
조치방법	최소 암호 길이 8문자 이상으로 설정
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정 정책

Step 2) "최소 암호 길이"에 "최소"를 "8문자"로 설정

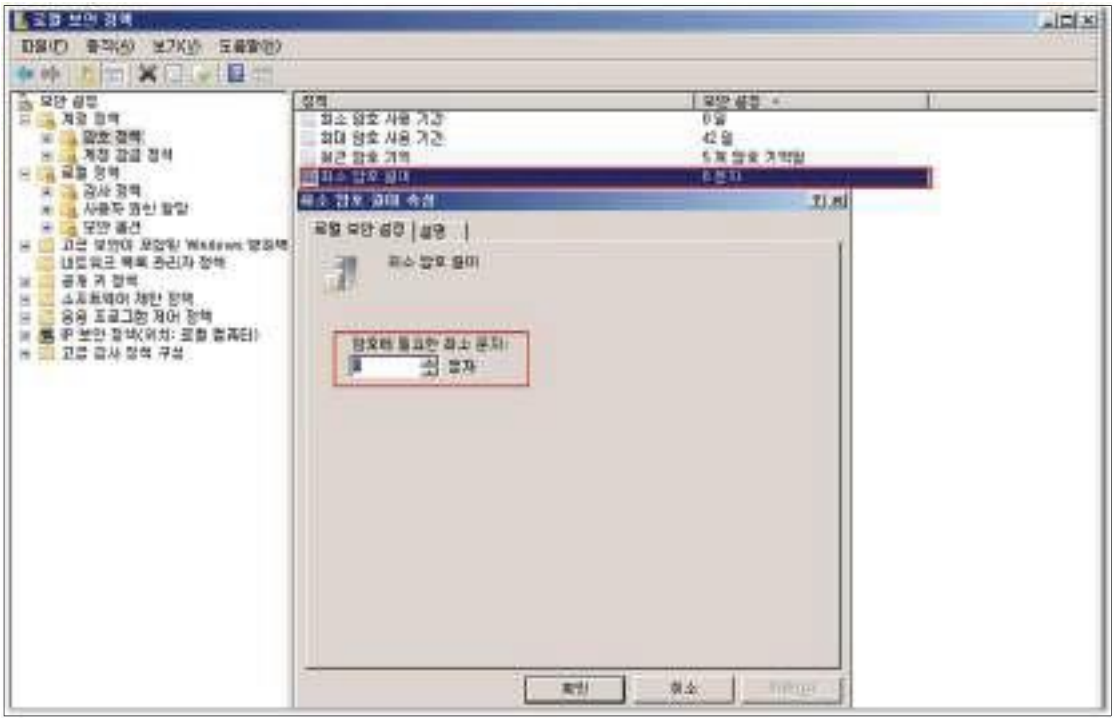


W-10 (중)	1. 계정관리 > 패스워드 최소 암호 길이

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책

Step 2) "최소 암호 길이"를 "8문자"로 설정



조치 시 영향	다음 패스워드 변경 시 8자 이상의 패스워드를 설정하여야 함

1.11. 패스워드 최대 사용 기간

W-11 (중)	1. 계정관리 > 패스워드 최대 사용 기간
취약점 개요	
점검내용	• 패스워드 최대 사용 기간 정책의 설정 여부 점검
점검목적	• 암호가 유효한 최대 날짜를 설정하여 이 날짜가 경과된 사용자는 암호를 변경하도록 하여 암호 크래킹의 가능성을 낮주고, 불법으로 획득한 암호의 무단 사용을 방지하고자 함
보안위협	• 오랫동안 변경하지 않은 패스워드를 지속적으로 사용하는 경우 암호 추측 공격에 의해 유출될 수 있으므로 사용자가 암호를 자주 바꾸도록 하면 유효한 암호가 공격당하는 위험을 줄일 수 있음
참고	※ 암호정책: 사용자에게 암호를 정기적으로 변경하게 하고, 암호의 최소 길이를 지정하며, 암호가 특정 복잡성을 만족시키도록 하는 등 암호 설정을 강제하여 컴퓨터를 보호하는 정책 ※ 관련 점검 항목 : W-09(중), W-11(중), W-12(중)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 최대 암호 사용 기간이 90일 이하로 설정되어 있는 경우
	취약 : 최대 암호 사용 기간이 설정되지 않았거나 90일을 초과하는 값으로 설정된 경우
조치방법	최대 암호 사용 기간 90일 설정
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정

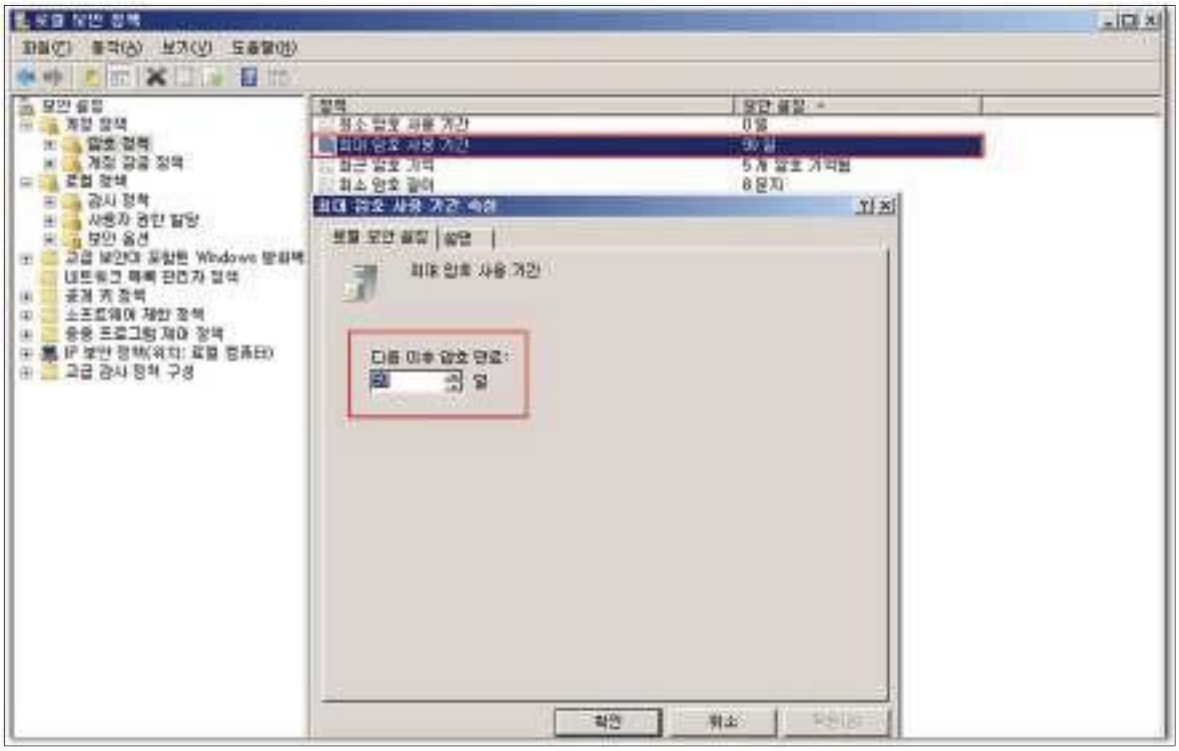
Step 2) "최대 암호 사용 기간"의 "사용 기간"을 "90일"로 설정

W-11 (중)	1. 계정관리 > 패스워드 최대 사용 기간

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책

Step 2) "최대 암호 사용 기간"의 다음 이후 암호 만료 기간을 "90일"로 설정



조치 시 영향	암호 사용기간이 90일로 설정되며 90일 주기로 패스워드를 변경하여야 함 패스워드 사용기간 만료 전 패스워드 변경을 위한 경고 메시지 제공을 권고함

1.12. 패스워드 최소 사용 기간

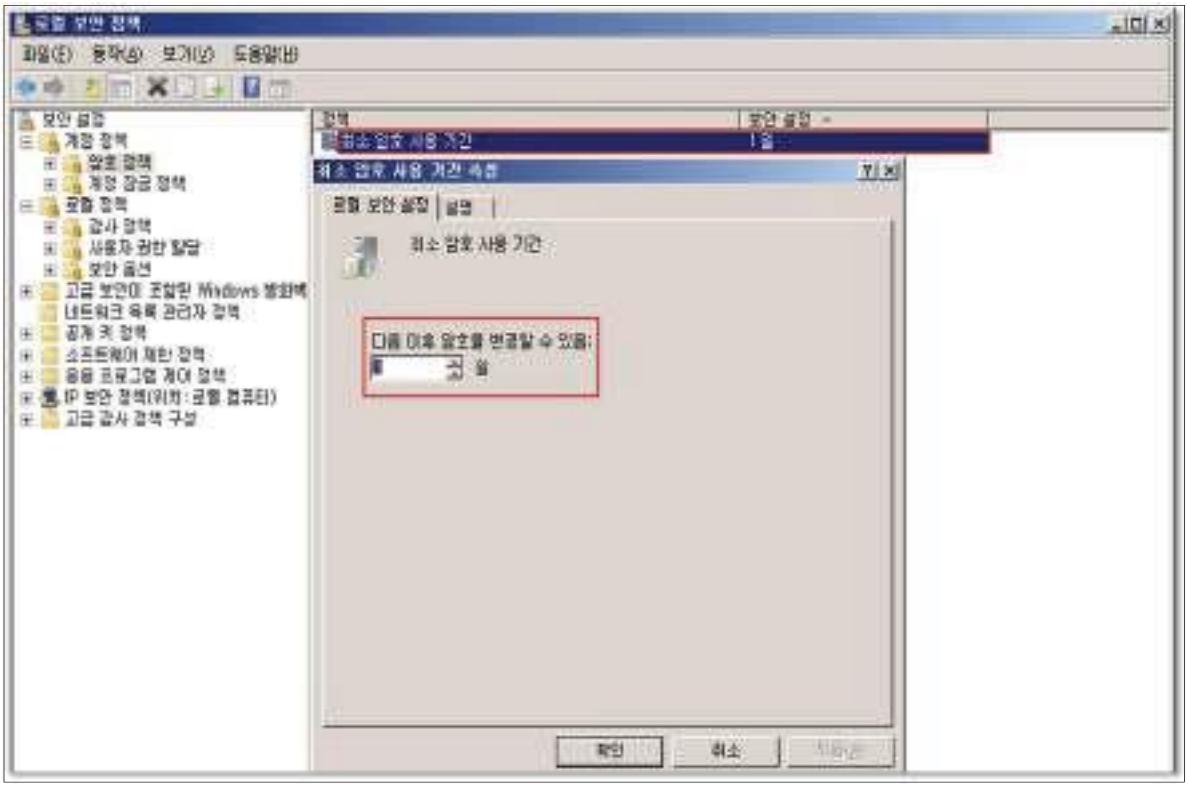
W-12 (중)	1. 계정관리 > 패스워드 최소 사용 기간
취약점 개요	
점검내용	• 패스워드 최소 사용 기간 정책 설정 여부 점검
점검목적	• 암호를 변경할 수 있기 전까지 경과해야 하는 최소 날짜를 설정하여 원래 패스워드로 즉시 변경할 수 없도록 함
보안위협	• 패스워드 변경 후 최소 사용 기간이 설정되지 않은 경우 사용자에게 익숙한 패스워드로 즉시 변동이 가능하여, 이를 재사용함으로써 원래 암호를 같은 날 다시 사용할 수 있음 • 패스워드 변경 정책에 따른 주기적인 패스워드 변경이 무의미해 질 수 있으며, 이로 인해 조직의 계정 보안성을 낮출 수 있음
참고	※ 암호정책: 사용자에게 암호를 정기적으로 변경하게 하고, 암호의 최소 길이를 지정하며, 암호가 특정 복잡성을 만족시키도록 하는 등 암호 설정을 강제하여 컴퓨터를 보호하는 정책 ※ 이 정책은 이전 암호를 그대로 재사용 하는 것을 방지하기 위해 W-16(중) '최근 암호 기억' 정책과 같이 적용될 경우 보안성이 훨씬 강화됨 ※ 관련 점검 항목 : W-09(중), W-10(중), W-11(중), W-16(중)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 최소 암호 사용 기간이 0보다 큰 값으로 설정되어 있는 경우
	취약 : 최소 암호 사용 기간이 0으로 설정되어 있는 경우
조치방법	최소 암호 사용 기간 1일 설정
점검 및 조치 사례	
• Windows NT Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정 Step 2) "최소 암호 사용 기간"에서 "사용 기간"을 "1일"로 설정	

W-12 (중)	1. 계정관리 > 패스워드 최소 사용 기간

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책

Step 2) "최소 암호 사용 기간"을 "1일"로 설정



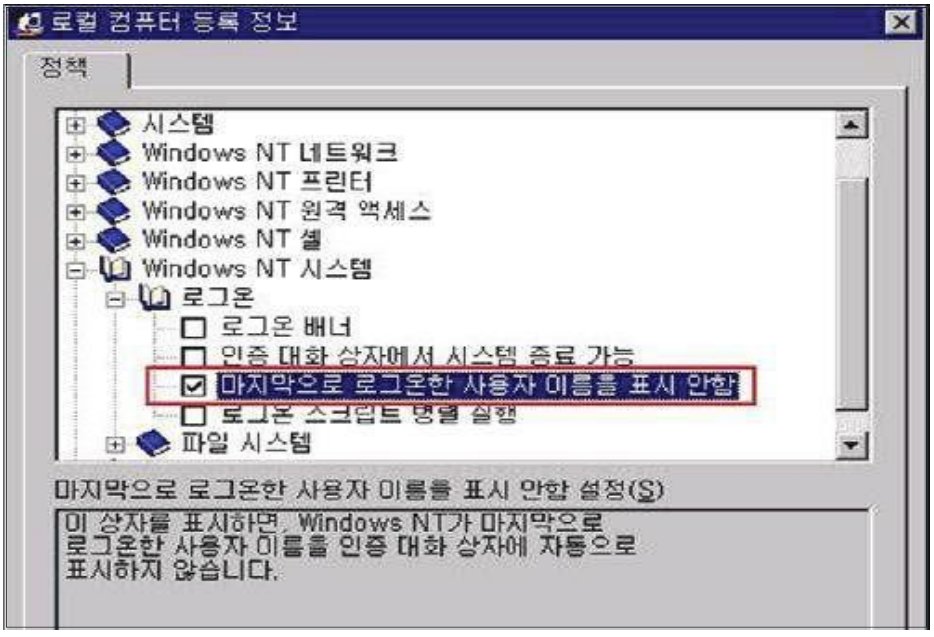
조치 시 영향	패스워드를 변경 후 다시 변경하기 위해서는 1일이 지나야 하며, 일반적으로 영향 없음

1.13. 마지막 사용자 이름 표시 안함

W-13 (중)	1. 계정관리 > 마치막 사용자 이름 표시 안 함
취약점 개요	
점검내용	• 로그인 화면에 마치막 로그온 사용자 이름을 표시하지 않도록 설정되었는지 여부를 점검
점검목적	• Windows 로그인 화면에 마치막 로그온 한 사용자 이름이 표시되지 않도록 하여 악의적인 사용자에게 계정 정보가 노출되는 것을 차단하고자 함
보안위협	• 마치막으로 로그온한 사용자의 이름이 로그온 대화 상자에 표시될 경우 공격자는 이를 획득하여 암호를 추측하거나 무작위 공격을 시도할 수 있음
참고	※ Windows 로그인 화면에 마치막 로그온 한 사용자 이름이 표시될 경우 주로 콘솔 사용자 및 터미널 서비스 이용자에게 시스템에 존재하는 사용자 계정 정보를 노출함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "마치막 사용자 이름 표시 안 함"이 "사용"으로 설정되어 있는 경우
	취약 : "마치막 사용자 이름 표시 안 함"이 "사용 안 함"으로 설정되어 있는 경우
조치방법	• Windows NT : 마치막으로 로그온한 사용자 이름 표시 안 함 -+ 설정 후 저장 • Windows 2000 : 로그온 스크린에 마치막 사용자 이름 표시 안 함 -+ 사용 • Windows 2003, 2008, 2012 : 대화형 로그온: 마치막 사용자 이름 표시 안 함 -+ 사용
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 프로그램> 관리도구> 시스템 정책 편집기> 파일> 레지스트리 열기> 로컬 컴퓨터> 편집> 등록 정보> Windows NT 시스템> 로그온> "마치막으로 로그온한 사용자 이름 표시 안함"을 설정한 후 저장

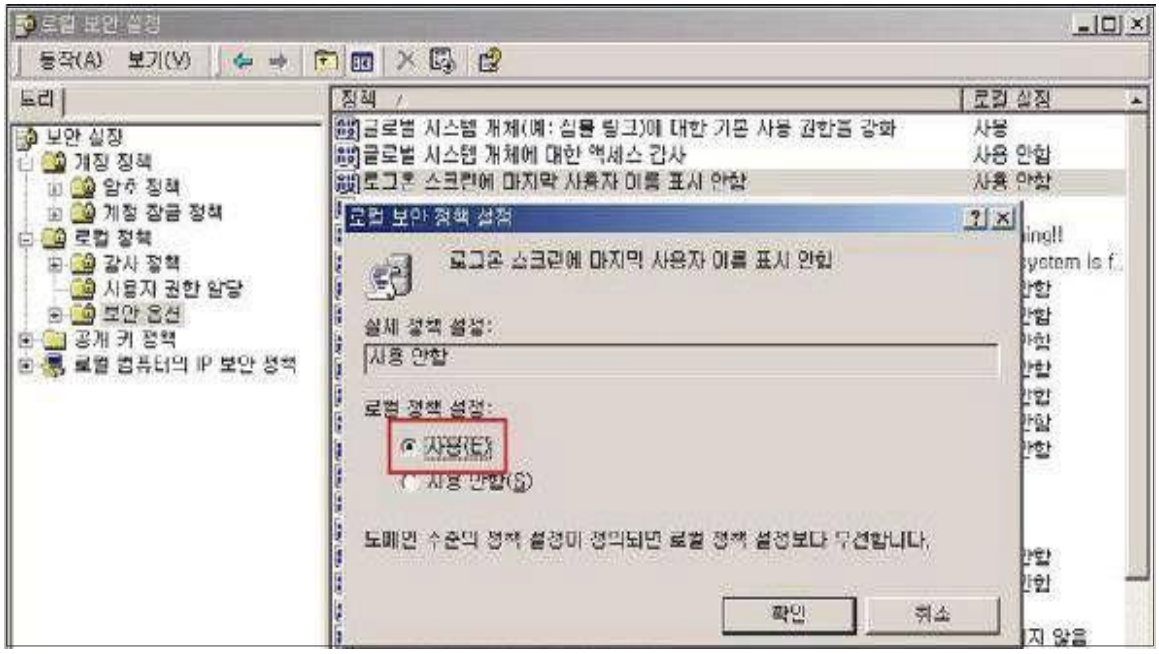


W-13 (중)	1. 계정관리 > 마치막 사용자 이름 표시 안 함

- Windows 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

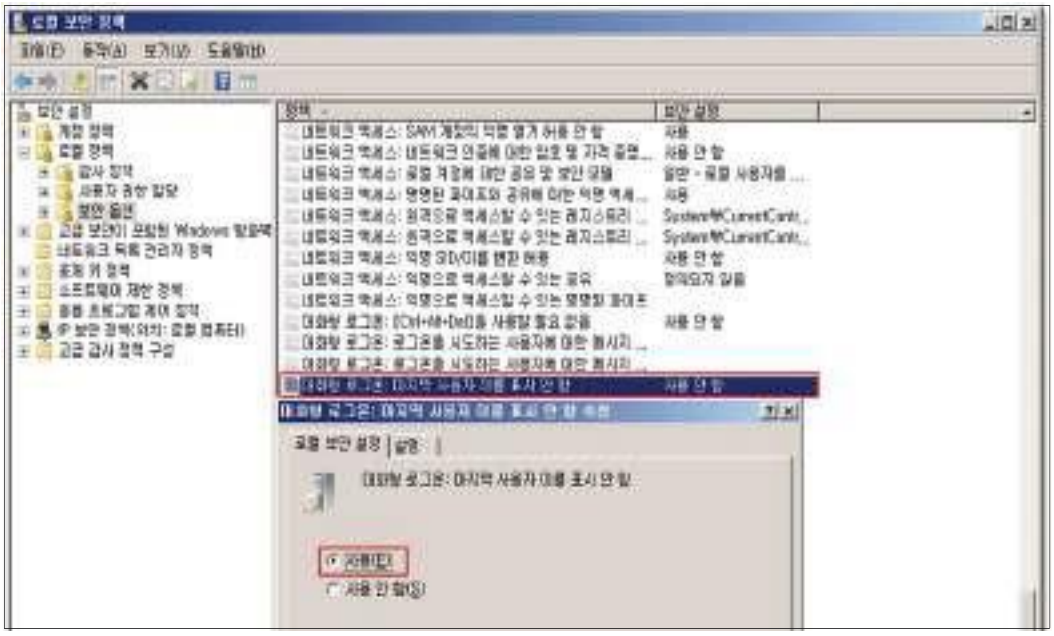
Step 2) "로그온 스크린에 마지막 사용자 이름 표시 안함"을 "사용"으로 설정



- Windows 2003, 2008, 2012

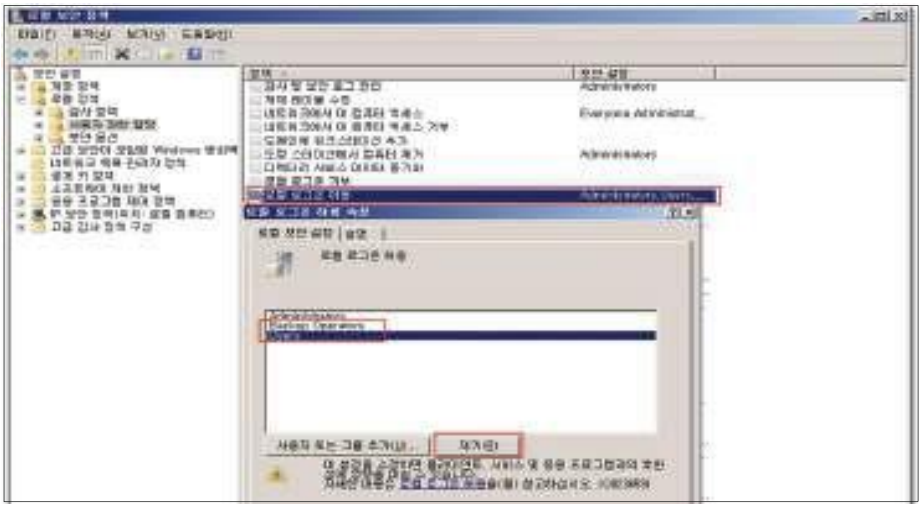
Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "대화형 로그온: 마지막 사용자 이름 표시 안 함"을 "사용"으로 설정



조치 시 영향	일반적인 경우 영향 없음

1.14. 로컬 로그온 허용

W-14 (중)	1. 계정관리 > 로컬 로그온 허용
취약점 개요	
점검내용	• 불필요한 계정의 로컬 로그온을 허용 여부 점검
점검목적	• 불필요한 계정에 로컬 로그온이 허용된 경우를 찾아 비인가자의 불법적인 시스템 로컬 접근을 차단하고자 함
보안위협	• 불필요한 사용자에게 로컬 로그온이 허용된 경우 비인가자를 통한 권한 상승을 위한 악성 코드의 실행 우려가 있음
참고	※ "로컬로 로그온 허용" 권한은 시스템 콘솔에 로그인을 허용하는 권한으로 반드시 콘솔 접근이 필요한 사용자 계정에만 해당 권한을 부여하여야 함 ※ IIS 서비스를 사용할 경우 이 권한에 IUSR_<ComputerName> 계정을 할당함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 로컬 로그온 허용 정책에 Administrators, IUSR_ 만 존재하는 경우
	취약 : 로컬 로그온 허용 정책에 Administrators, IUSR_ 외 다른 계정 및 그룹이 존재하는 경우
조치방법	Administrators, IUSR_ 외 다른 계정 및 그룹의 로컬 로그온 제한
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 사용자 권한 할당 Step 2) "로컬 로그온 허용(또는, 로컬 로그온)" 정책에 "Adminstrators", "IUSR_" 외 다른 계정 및 그룹 제거 	
조치 시 영향	Administrators, IUSR_ 계정 외 로컬에서 접속이 필요한 계정 삭제 시 사용중인 서비스에 장애를 줄 수 있음

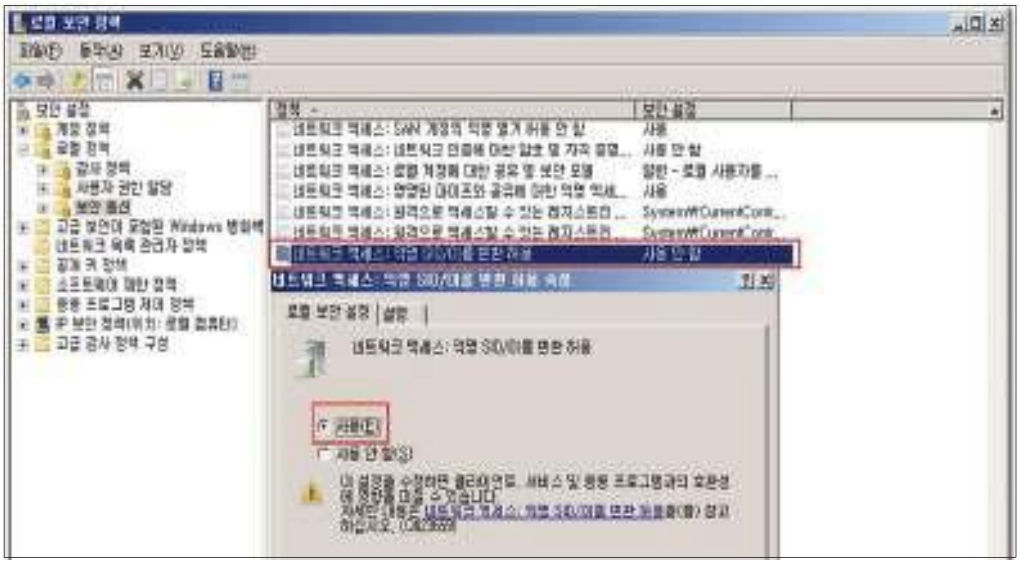
1.15. 익명 SID/이름 변환 허용

W-15 (중)	1. 계정관리 > 익명 SID/이름 변환 허용 해제
취약점 개요	
점검내용	• 익명 SID/이름 변환 정책 적용 여부 점검
점검목적	• 익명 SID/이름 변환 정책을 "사용 안 함"으로 설정하여, SID(보안식별자)를 사용하여 관리자 이름을 찾을 수 없도록 하기 위함
보안위협	• 이 정책이 "사용함"으로 설정된 경우 로컬 접근 권한이 있는 사용자가 잘 알려진 Administrator SID를 사용하여 Administrator 계정의 실제 이름을 알아낼 수 있으며 암호 추측 공격을 실행할 수 있음
참고	※ 이 정책이 설정된 경우 익명 사용자가 다른 사용자의 SID(보안식별자) 특성을 요청할 수 있음 ※ "사용 안 함"으로 정책을 설정할 경우 Windows NT 도메인 환경에서 통신이 불가능하게 될 수 있음
점검대상 및 판단기준	
대상	• Windows 2003, 2008, 2012
판단기준	양호 : "익명 SID/이름 변환 허용" 정책이 "사용 안 함" 으로 되어 있는 경우
	취약 : "익명 SID/이름 변환 허용" 정책이 "사용" 으로 되어 있는 경우
조치방법	네트워크 액세스: 익명 SID/이름 변환 허용 -+ 사용 안 함
점검 및 조치 사례	

• Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "네트워크 액세스: 익명 SID/이름 변환 허용" 정책이 "사용 안 함"으로 설정



※ Windows Server 2000 이하 버전 해당 사항 없음

조치 시 영향	일반적인 경우 영향 없음

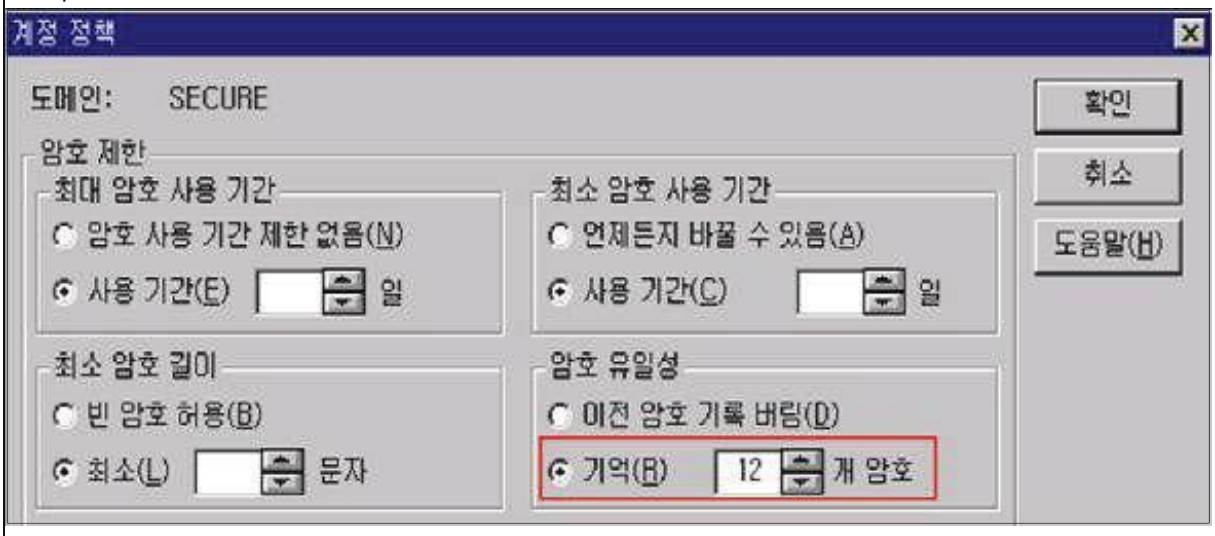
1.16. 최근 암호 기억

W-16 (중)	1. 계정관리 > 최근 암호 기억
취약점 개요	
점검내용	• 최근 암호 기억 정책 설정 여부 점검
점검목적	• 사용자가 현재 암호 또는 최근에 사용했던 암호와 동일한 새 암호를 만드는 것을 방지하기 위함
보안위협	• 최근 암호 기억 정책이 설정되지 않은 경우 특정 계정에 동일한 암호를 오랫동안 사용하는 것이 가능하여 공격자가 무작위 공격을 통해 패스워드 정보 노출 가능성이 커짐
참고	※ 사용자가 현재 암호 또는, 최근에 사용했던 암호와 똑같은 새 암호로 설정할 수 없도록 하여야 함 ※ 이 정책은 암호정책 중 하나로 W-12(중) '패스워드 최소 사용 기간' 정책과 같이 적용될 경우 보안성이 훨씬 강화됨 ※ 관련 점검 항목 : W-09(중), W-10(중), W-11(중), W-12(중)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 최근 암호 기억이 4개 이상으로 설정되어 있는 경우
	취약 : 최근 암호 기억이 4개 미만으로 설정되어 있는 경우
조치방법	최근 암호 기억이 4개 이상으로 설정되어 있는 경우
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 프로그램> 관리도구> 도메인 사용자 관리자> 정책> 계정

Step 2) "암호 유일성"에서 "기억"을 "4개"로 설정

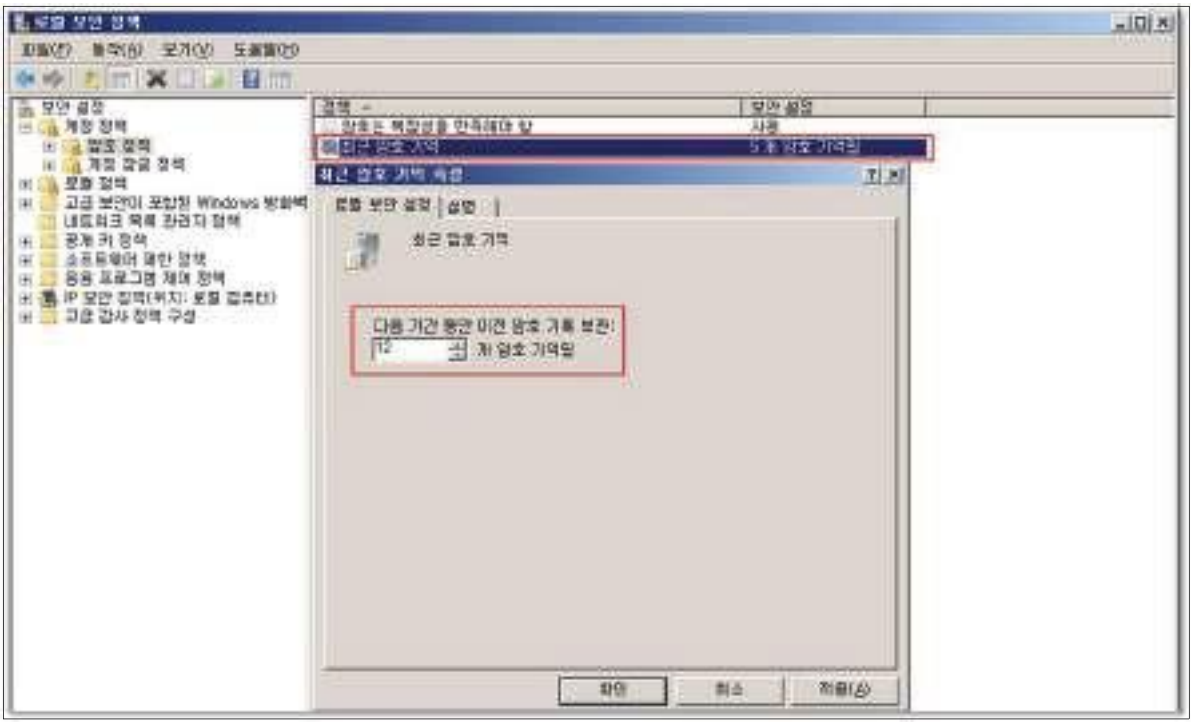


W-16 (중)	1. 계정관리 > 최근 암호 기억

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 계정정책> 암호 정책

Step 2) "최근 암호 기억"을 "4개 암호 기억됨"으로 설정



조치 시 영향	일반적인 경우 영향 없음

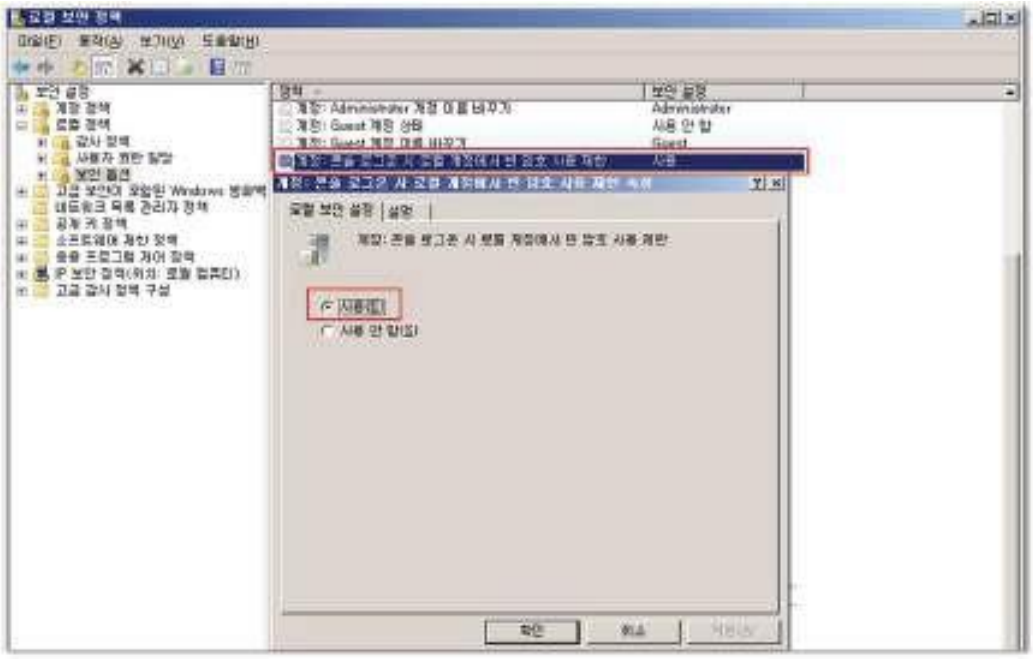
1.17. 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한

W-17 (중)	1. 계정관리 > 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한
취약점 개요	
점검내용	• 콘솔 로그인 시 빈 암호 사용 가능 여부 점검
점검목적	• 빈 암호를 가진 계정의 콘솔 및 네트워크 서비스 접근을 차단하기 위함
보안위협	• 이 정책이 "사용 안 함"으로 설정된 경우 빈 암호를 가진 로컬 계정에 대하여 터미널 서비스(원격 데스크톱 서비스), Telnet 및 FTP와 같은 네트워크 서비스의 원격 대화형 로그온이 가능하여, 시스템 보안에 심각한 위험을 줄 수 있음
참고	※ 윈도우 원격 제어(mstsc)는 보안상 계정에 암호가 걸린 계정만 접속하도록 하고 있으나 이 정책을 활성화하면 계정에 암호가 걸려 있지 않아도 원격 제어가 가능함
점검대상 및 판단기준	
대상	• Windows 2003, 2008, 2012
판단기준	양호 : "콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용"인 경우
	취약 : "콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용 안 함"인 경우
조치방법	계정: 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한 -+ 사용
점검 및 조치 사례	

• Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "계정: 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한" 정책을 "사용"으로 설정



조치 시 영향	일반적인 경우 영향 없음

1.18. 원격터미널 접속 가능한 사용자 그룹 제한

W-18 (중)	1. 계정관리 > 원격터미널 접속 가능한 사용자 그룹 제한
취약점 개요	
점검내용	• 원격터미널 사용자 그룹 내 비인가자 포함 여부 점검
점검목적	• 비인가자의 원격터미널 접속을 제한하기 위함
보안위협	• 원격터미널의 그룹이나 계정을 제한하지 않으면 임의의 사용자가 원격으로 접속하여 해당 서버에 정보를 변경하거나 정보가 유출될 가능성이 있으므로 사용자 그룹과 계정을 설정하여 접속을 제한하여야 함
참고	※ 컴퓨터 관리 > 로컬 사용자 및 그룹 > Remote Desktop Users 그룹에서 추가 가능
점검대상 및 판단기준	
대상	• Windows 2003, 2008, 2012
판단기준	양호 : (관리자 계정을 제외한) 원격접속이 가능한 계정을 생성하여 타 사용자의 원격접속을 제한하고, 원격접속 사용자 그룹에 불필요한 계정이 등록되어 있지 않은 경우
	취약 : (관리자 계정을 제외한) 원격접속이 가능한 별도의 계정이 존재하지 않는 경우
조치방법	관리자 계정과 이외의 계정을 생성, 권한을 제한 -+ 사용
점검 및 조치 사례	

• Windows 2003

Step 1) 제어판> 사용자 계정> 관리자 계정 이외의 계정 생성한 후

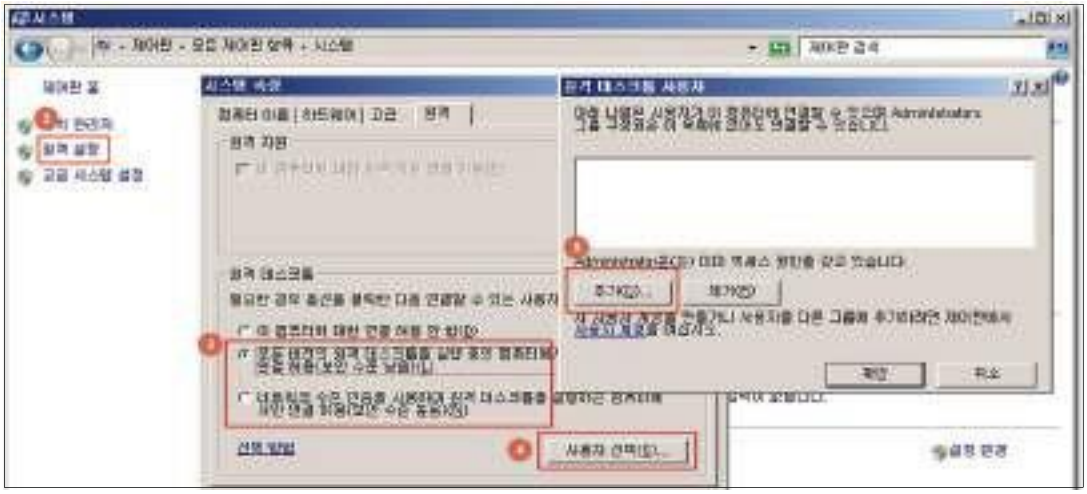
Step 2) 제어판> 시스템> [원격] 탭> [원격] 탭 메뉴에서 "사용자가 이 컴퓨터에 원격으로 연결할 수 있음"에 체크> "원격 사용자 선택"에서 원격 사용자 지정 후 확인

• Windows 2008

Step 1) 제어판> 사용자 계정> 관리자 계정 이외의 계정 생성한 후

Step 2) 제어판> 시스템> 원격 설정> [원격] 탭> [원격 데스크톱] 메뉴> "모든 버전의 원격 데스크톱을 실행 중인 컴퓨터에서 연결 허용(보안 수준 낮음)" 또는 "네트워크 수준 인증을 사용하여 원격 데스크톱을 실행하는 컴퓨터에서만 연결 허용(보안 수준 높음)" 중 하나에 체크> "사용자 선택" 에서 원격 사용자 지정 후 확인

W-18 (중)	1. 계정관리 > 원격터미널 접속 가능한 사용자 그룹 제한



- Windows 2012

Step 1) 제어판> 사용자 계정> 관리자 계정 이외의 계정 생성한 후

Step 2) 제어판> 시스템> 원격 설정> [원격] 탭> [원격 데스크톱] 메뉴> "이 컴퓨터에 대한 원격 연결 허용" 에 체크> "사용자 선택" 에서 원격 사용자 지정 후 확인

조치 시 영향	일반적인 경우 영향 없음

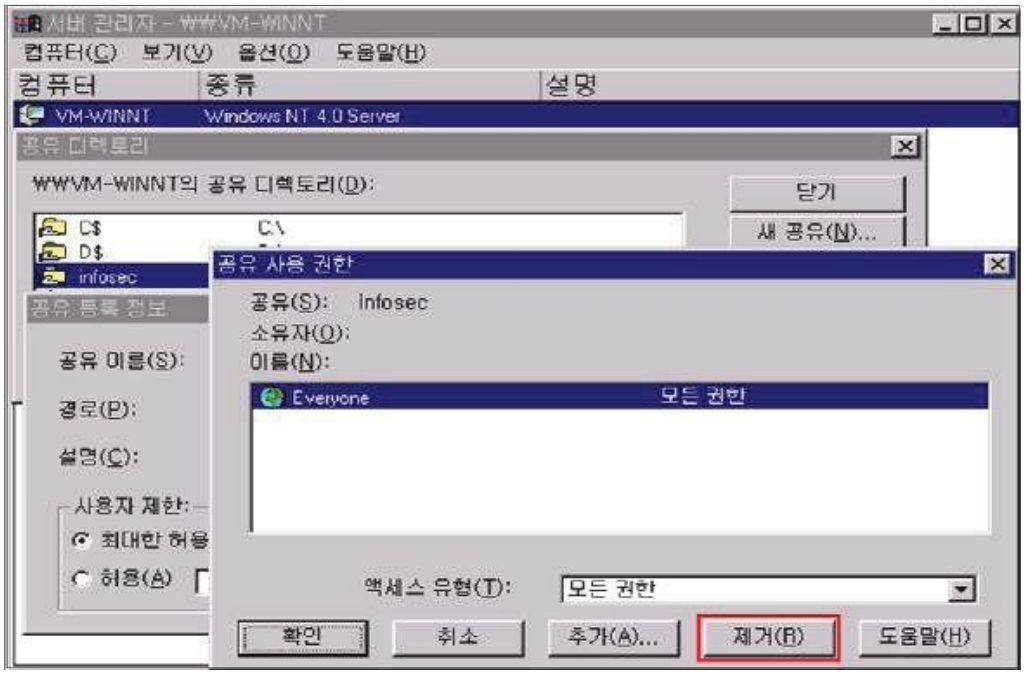
2. 서비스 관리

2.1. 공유 권한 및 사용자 그룹 설정

W-19 (상)	2. 서비스 관리 > 공유 권한 및 사용자 그룹 설정
취약점 개요	
점검내용	• 공유 디렉토리 내 Everyone 권한 존재 여부 점검
점검목적	• 디폴트 공유인 C$, D$, Admin$, IPC$ 등을 제외한 공유 폴더에 Everyone 그룹으로 공유되는 것을 금지하여 익명 사용자의 접근을 차단하기 위함
보안위협	• Everyone이 공유계정에 포함되어 있으면 익명 사용자의 접근이 가능하여 내부 정보 유출 및 악성코드의 감염 우려가 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 일반 공유 디렉토리가 없거나 공유 디렉토리 접근 권한에 Everyone 권한이 없는 경우
	취약 : 일반 공유 디렉토리의 접근 권한에 Everyone 권한이 있는 경우
조치방법	공유 디렉토리 접근 권한에서 Everyone 권한 제거 후 필요한 계정 추가
점검 및 조치 사례	

• Windows NT

Step 1) 프로그램> 관리도구> 서버 관리자> 컴퓨터> 공유 디렉토리> 등록정보> 사용 권한에서 Everyone 으로 된 공유를 제거하고 접근이 필요한 계정의 적절한 권한 추가

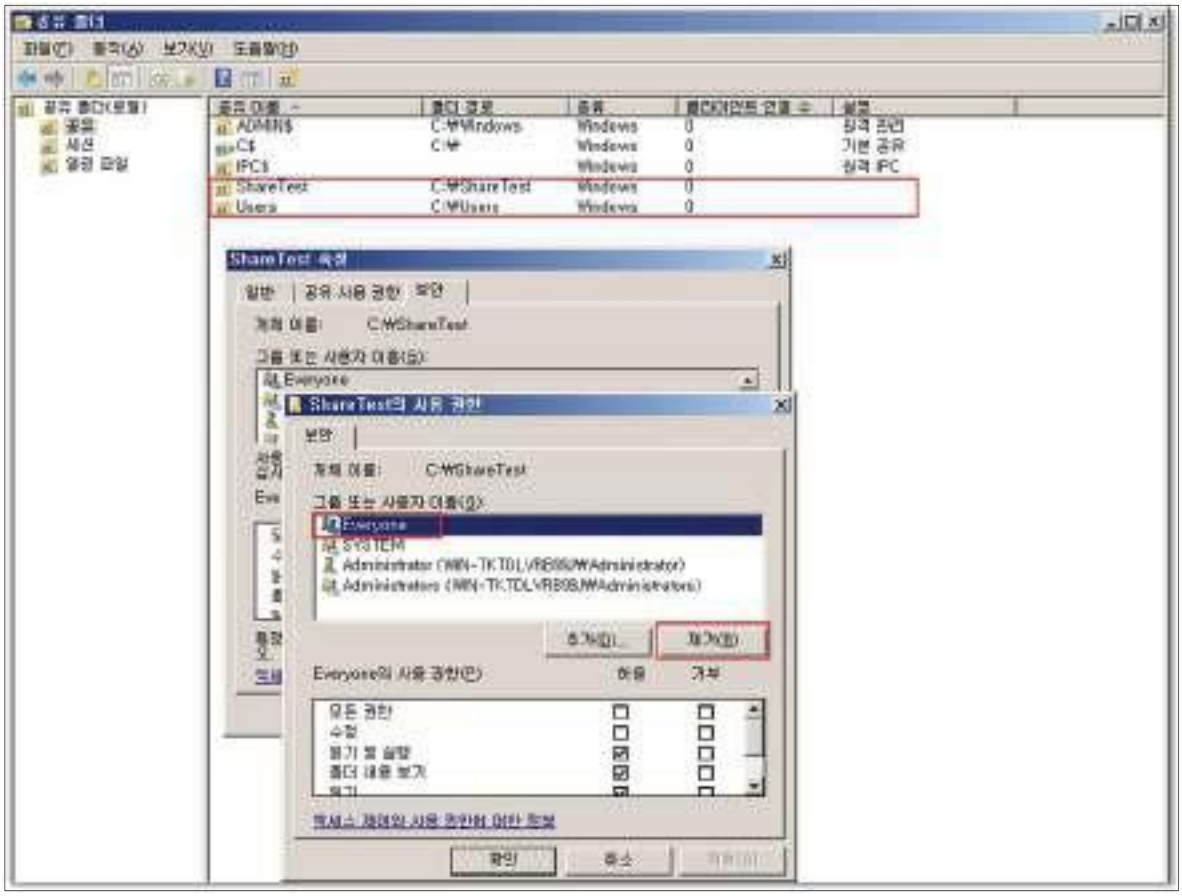


W-19 (상)	2. 서비스 관리 > 공유 권한 및 사용자 그룹 설정

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> FSMGMT.MSC> 공유

Step 2) 사용 권한에서 Everyone 으로 된 공유를 제거하고 접근이 필요한 계정의 적절한 권한 추가



조치 시 영향	애플리케이션이나 Backup 용도로 Everyone 공유를 사용하는 경우 해당 작업에 영향 가능

2.2. 하드디스크 기본 공유 제거

W-20 (상)	2. 서비스 관리 > 하드디스크 기본 공유 제거
취약점 개요	
점검내용	• 하드디스크 기본 공유 제거 여부 점검
점검목적	• 하드디스크 기본 공유를 제거하여 시스템 정보 노출을 차단하고자 함
보안위협	• Windows는 프로그램 및 서비스를 네트워크나 컴퓨터 환경에서 관리하기 위해 시스템 기본 공유 항목을 자동으로 생성함. 이를 제거하지 않으면 비인가자가 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있으며 이러한 공유 기능의 경로를 이용하여 바이러스가 침투될 수 있음
참고	※ 기본 공유: 관리목적으로 자동 생성되는 공유 드라이브(Administrative share). 이러한 드라이브들은 C$, D$, E$ 등과 같이 이름 뒤에 $가 붙어서 숨겨진 공유로 처리되며, Windows 2000, XP에서는 관리자 ID와 Password를 알고 있으면 네트워크를 통해 이러한 공유 드라이브들에 자유롭게 접근할 수 있음. 그러나 이후 버전 Windows에서는 보안상의 이유로 로컬시스템의 관리자가 네트워크를 통해 시스템을 관리하지 못하도록 기본적으로 차단됨
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 레지스트리의 AutoShareServer (WinNT: AutoShareWks)가 0이며 기본 공유가 존재하지 않는 경우
	취약 : 레지스트리의AutoShareServer (WinNT: AutoShareWks)가 1이거나 기본 공유가 존재하는 경우
조치방법	기본 공유 중지 후 레지스트리 값 설정(IPC$, 일반 공유 제외)
점검 및 조치 사례	

• Windows NT

Step 1) 프로그램> 관리도구> 서버 관리자> 컴퓨터> 공유 디렉토리> 공유

W-20 (상)	2. 서비스 관리 > 하드디스크 기본 공유 제거

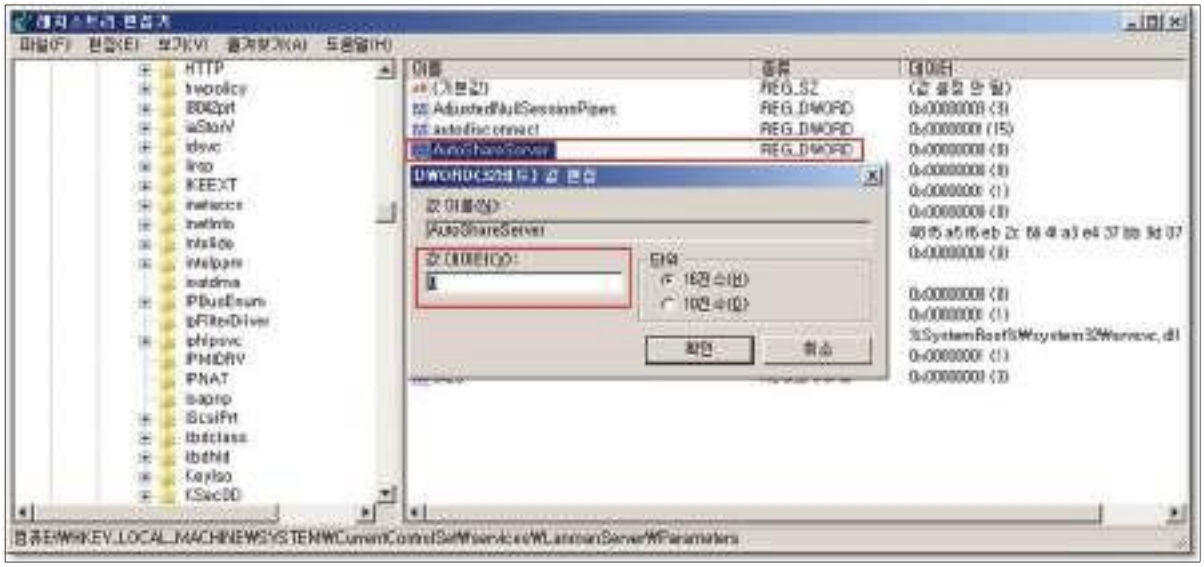
- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> FSMGMT.MSC> 공유> 기본 공유 선택> 마우스 우클릭> 공유 중지

Step 2) 시작> 실행> REGEDIT

아래 레지스트리 값을 0으로 수정함(키 값이 없을 경우 새로 생성함)

"HKLM₩SYSTEM₩CurrentControlSet₩Services₩lanmanserver₩parameters₩AutoShareServer"(Windows NT일 경우: AutoShareWks)



※ 방화벽과 라우터에서 135~139(TCP/UDP)포트를 차단하여 외부로부터의 위험을 제거함으로써 보안성을 높일 수 있음 (Windows 2008 제외)

조치 시 영향	Active Directory, Clustered system에서는 적용 시 영향 있음 ※ Active Directory: 중앙 집중화된 자원 관리를 위한 계층적 디렉토리 서비스 ※ Clustered system: 여러 개의 시스템을 결합하여 사용함

2.3. 불필요한 서비스 제거

W-21 (상)	2. 서비스 관리 > 불필요한 서비스 제거
취약점 개요	
점검내용	• 불필요한 서비스 가동 여부 점검
점검목적	• 사용자 환경에 필요하지 않은 서비스 및 실행 파일을 제거하거나 비활성화 처리하여 이를 통한 악의적인 공격을 차단하기 위함
보안위협	• 시스템에 기본적으로 설치되는 불필요한 취약 서비스들이 제거되지 않은 경우, 해당 서비스의 취약점으로 인한 공격이 가능하며, 네트워크 서비스의 경우 열린 포트를 통한 외부 침임의 가능성이 존재함
참고	※ OS 버전에 따라 '일반적으로 불필요한 서비스' 목록에 나열된 서비스가 제공되지 않을 수 있음
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 일반적으로 불필요한 서비스(아래 목록 참조)가 중지되어 있는 경우
	취약 : 일반적으로 불필요한 서비스(아래 목록 참조)가 구동 중인 경우
조치방법	서비스 중지 후 "사용 안 함" 설정
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 설정> 제어판> 서비스를 선택하여 불필요한 서비스를 중지하고, 시작 옵션에서 "시작 유형"을 "사용 안함"으로 수정

Step 2) 해당 서비스를 선택하고 오른쪽 메뉴에서 "시작 옵션"을 클릭하면 시스템이 시작할 때에 해당 서비스의 시작 유형을 선택할 수 있음. 만약, 시스템 시작 시 자동으로 시작되게 하려면 [자동], 수동으로 서비스를 시작하려면 [수동], 서비스 자체를 사용하지 않으려면 [사용 안함]을 선택한 후 [확인]을 클릭함

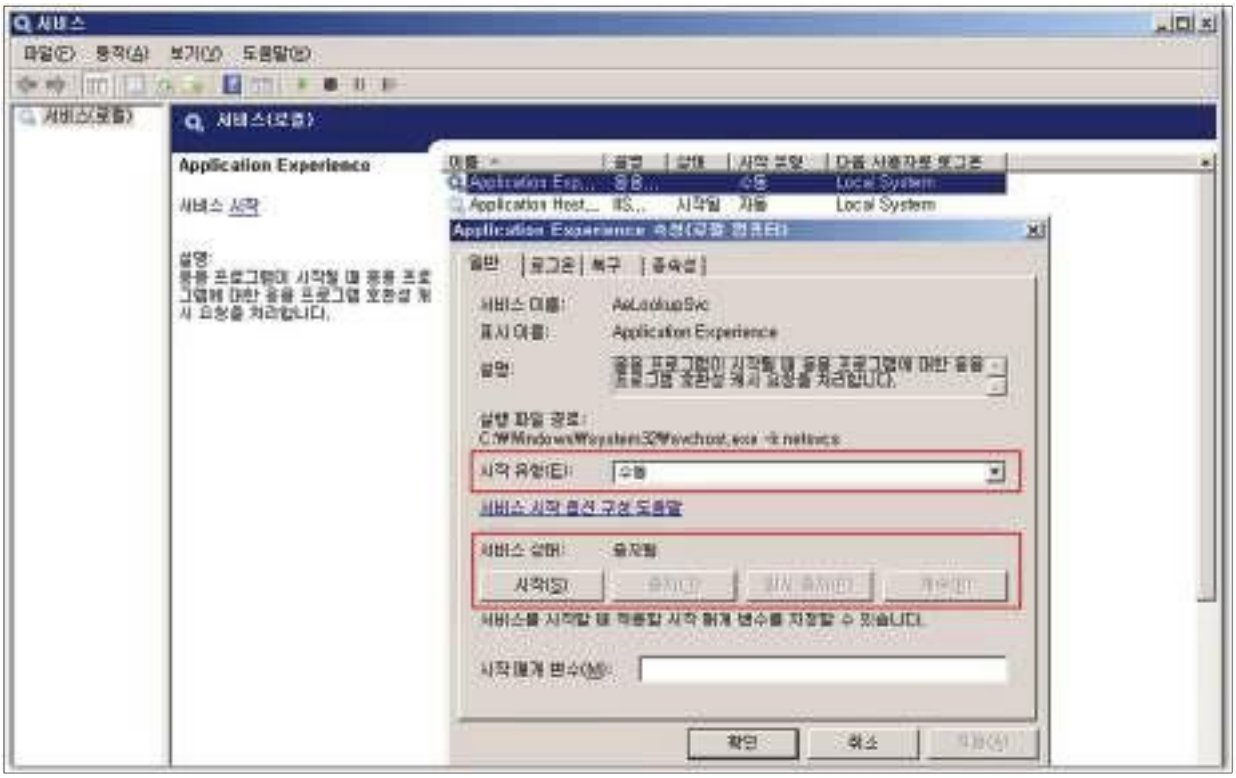
W-21 (상)	2. 서비스 관리 > 불필요한 서비스 제거

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SERVICES.MSC> "해당 서비스" 선택> 속성

Step 2) 시작 유형 -> 사용 안 함

Step 3) 서비스 상태 -> 중지 설정



특별한 목적을 위해 사용하는 서비스가 아니라면 시스템의 업무에 부합되는 서비스가 아닌 기타 디폴트 서비스를 사용하지 않는 것이 좋으며, 시스템 관리자는 대상 시스템의 용도를 정확히 파악해 불필요한 서비스를 제거하여야 함

서비스 시작 유형	설 명
사용 안 함	설치되어 있으나 실행되지 않음
수등	다른 서비스나 응용 프로그램에서 해당 기능을 필요로 할 때만 시작됨
자동	부팅 시에 해당 장치 드라이버가 로드된 후에 운영 체제에 의해 시작됨

W-21 (상)	2. 서비스 관리 > 불필요한 서비스 제거

각 서비스마다 옵션을 설정할 수 있으며 해당 서비스를 선택하고 더블 클릭하게 되면 시작 유형을 선택할 수 있으며 시작 시 로그온 계정을 별도로 설정할 수 있음. 만약, 시스템 시작 시 자동으로 시작되게 하려면 [자동], 수동으로 서비스를 시작하려면 [수동], 서비스 자체를 사용하지 않으려면 [사용 안 함]을 선택한 후 [확인]을 클릭함

※ 일반적으로 불필요한 서비스

서비스명	기능 및 설명
Alerter	네트워크상에서 사용자와 컴퓨터에 관리용 경고메시지를 전송하는 기능
Automatic Updates	중요한 윈도우 업데이트를 다운로드하고 설치할 수 있도록 하는 애플리케이션. 수동패치를 적용하거나, MS패치 관리 서버로 패치를 일괄적으로 관리하는 경우 불필요한 서비스
Clipbook	서버 내 Clipbook을 다른 클라이언트와 공유
Computer Browser	네트워크에 있는 모든 컴퓨터의 목록을 업데이트 하고 관리하는 기능
Cryptographic Services	윈도우 파일의 서명을 확인하는 카탈로그 데이터베이스 서비스를 총괄
DHCP Client	IP 주소와 DNS 이름을 DHCP 서버에 등록하거나 DHCP 서버로부터 동적으로 IP주소를 가져오는 기능을 수행. 단독으로 시스템을 수행하며 고정IP를 사용하는 경우 불필요한 서비스
Distributed Link Tracking Client, Server	네트워크 도메인의 여러 컴퓨터나 일반컴퓨터에서 NTFS 파일간의 연결을 관리하는 도구. Active Directory가 구성되있어지 않은 서버에서는 불필요한 서비스
DNS Client	컴퓨터에 대한 도메인 이름 시스템(DNS)이름을 확인하고 캐시에 보관하는기능. DNS 서버가 아닌 시스템에서는 유명무실하나, IPSEC을 사용하는 경우 필요한 경우 있음
Error reporting Service	프로그램 오류가 시 응용프로그램의 오류를 MS에 보고한다는 내용을 표시하는 기능
Human Interface Device Access	키보드 또는 기타 멀티미디어 장치에 사전 정의된 버튼들을 사용하는 HID장치들을 위한 서비스
IMAPI CD-Burning COM Service	서버에 CD-RW 또는 DVD-RW가 장착되어 보조백업장치 역할을 하기 위해서 자제 레코딩 백업을 할 수 있음
Messenger	클라이언트와 서버 사이에 netsend 및 경고서비스 메시지를 전송하는 기능
NetMeeting Remote Desktop Sharing	윈도우9X 운영체제부터 인증된 사용자가 넷미팅을 사용해서 원격으로 컴퓨터에 접근할 수 있도록 하는 기능
Portable Media Serial Number	컴퓨터에 연결된 이동성 음악연주기(미디기기)의 등록번호를 복원하는 기능
Print Spooler	인쇄 과정에 있는 스풀링을 관리하는 서비스. 프린터가 있는 경우 필수 서비스이나, 프린터가 연결되지 않은 시스템에서는 불필요함
Remote Registry	원격 사용자가 이 컴퓨터에서 레지스트리 설정을 수정할 수 있도록 설정하는 애플리케이션
Simple TCP/IP Services	Echo, Discard, Character Generator, Daytime, Quote of the Day 지원
Wireless Zero Configuration	802.11 어댑터에 대해 자동 구성을 공급하는 기본적인 도구

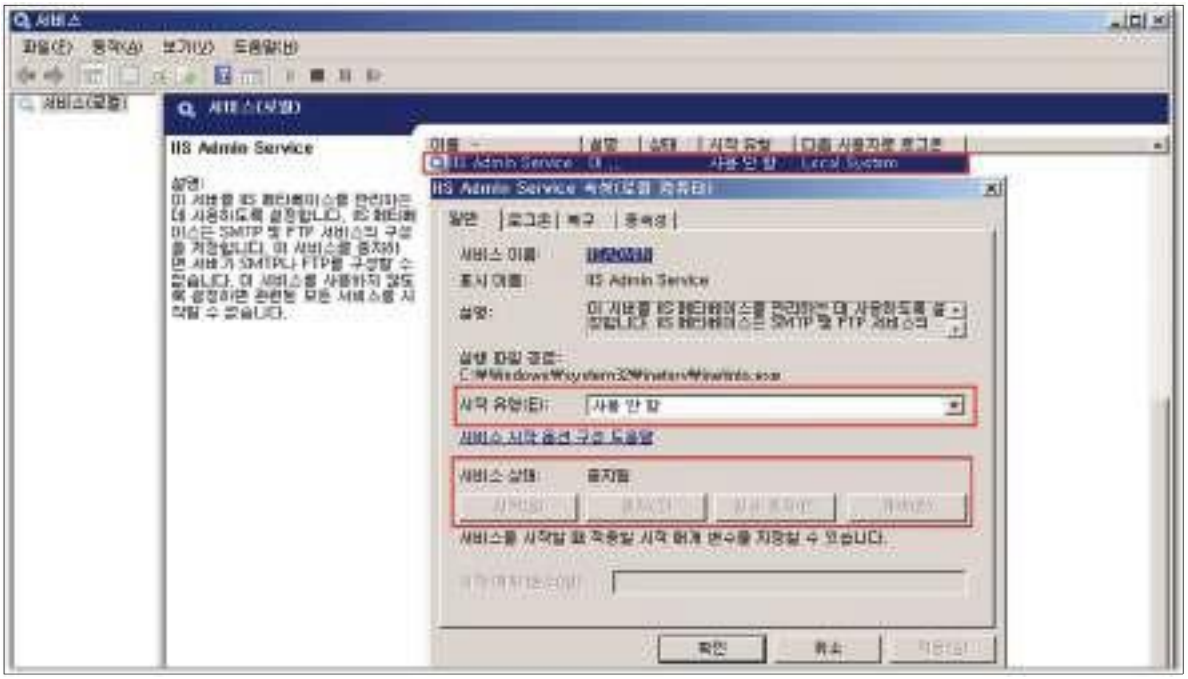
W-21 (상)	2. 서비스 관리 > 불필요한 서비스 제거
운영중인 시스템에서 필수 서비스를 정의하는 것은 매우 복잡한 과정으로 서비스 사용 여부는 시스템의 영향성을 고려하여 신중하게 평가되어야 하므로 Microsoft에서 권고하는 가이드에 따라 전략적으로 적용하여야 함 ※ https://technet.microsoft.com/ko-kr/library/dd547941.aspx (서비스 및 서비스 계정 보안 계획 가이드) 참고 윈도우 시스템 설치 시 기본적으로 설치되는 서비스에 대한 상세 설명은 아래 주소 참조 https://technet.microsoft.com/ko-kr/library/dd547949.aspx	
조치 시 영향	일반적으로 영향 없음

2.4. IIS 서비스 구동 점검

W-22 (상)	2. 서비스 관리 > IIS 서비스 구동 점검
취약점 개요	
점검내용	• 불필요한 IIS 서비스 구동 여부 점검
점검목적	• 불필요한 IIS 서비스가 구동 상태인지를 점검하여 제거하고, 해당 서비스가 취약점이 제거되지 않은 상태로 외부 위협에 노출되지 않도록 하기 위함
보안위협	• IIS 서비스는 WEB, FTP 등의 서비스를 제공해주는 유용한 서비스이나 프로파일링, 서비스 거부, 불법적인 접근, 임의의 코드실행, 정보 공개, 바이러스, 립, 트로이목마 등의 위협에 노출될 수 있어 서비스 불필요 시 삭제하여야 함
참고	※ 일반적으로 불필요한 서비스가 시스템 내 구동되고 있는 경우에는 관리되지 않은 상태로 방지되는 경우가 많아 보안 취약점이 그대로 노출되어 악의적인 공격의 대상이 될 수 있음
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : IIS 서비스가 필요하지 않아 이용하지 않는 경우
	취약 : IIS 서비스를 필요하지 않지만 사용하는 경우
조치방법	IIS 서비스를 사용하지 않는 경우 IIS 서비스 중지
점검 및 조치 사례	

• Windows NT, 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SERVICES.MSC> IISADMIN> 속성> "시작 유형"을 "사용 안 함" 설정 후 중지



※ IIS 가 설치되어 있지 않을 경우 SERVICES.MSC 에서 보이지 않음

조치 시 영향	일반적인 경우 영향 없음

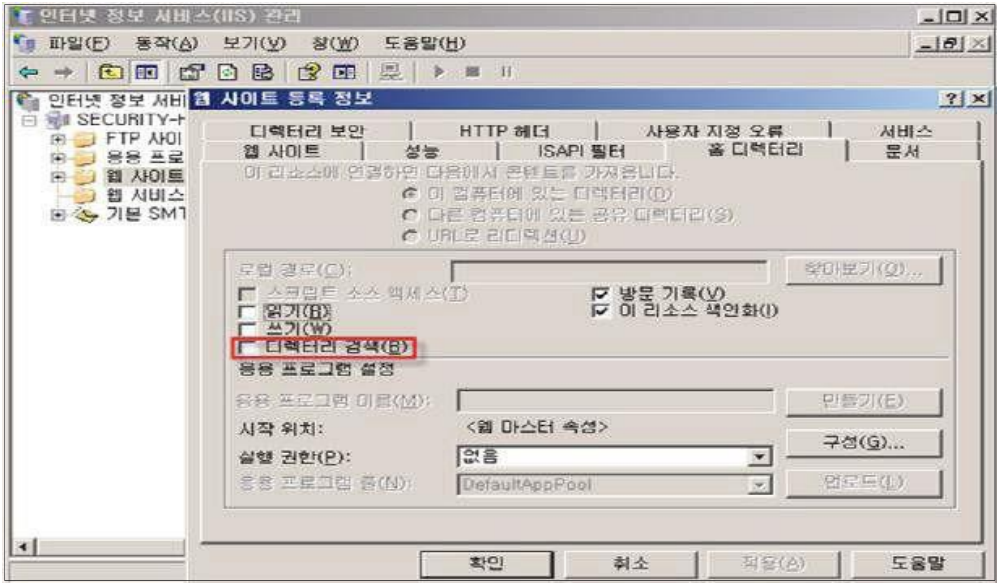
2.5. IIS 디렉토리 리스팅 제거

W-23 (상)	2. 서비스 관리 > IIS 디렉토리 리스팅 제거
취약점 개요	
점검내용	• 웹서버 디렉토리 리스팅 차단 설정 여부 점검
점검목적	• 웹서버 특정 폴더에 대한 디렉토리 리스팅 취약점을 제거하여, 불필요한 파일 정보 노출을 차단하기 위함
보안위협	• 웹서버에 디렉토리 리스팅이 제거되지 않은 경우 외부에서 디렉토리 내에 보유하고 있는 모든 파일 목록 확인 및 파일에 대한 접근이 가능하여 주요 정보의 유출의 가능성이 있음
참고	※ 디렉토리 리스팅 취약점: 디렉토리에 대한 요청 시 기본 페이지가 호출되어 사용자에게 전송하지만, 기본 페이지가 존재하지 않는 경우 디렉토리 내에 존재하는 모든 파일의 목록을 보여주는 취약점
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : "디렉토리 검색" 체크하지 않음
	취약 : "디렉토리 검색" 체크함 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 디렉토리 검색 체크 해제
점검 및 조치 사례	

• Windows 2000(IIS 5.0), 2003(IIS 6.0)

Step 1) 시작> 실행> INETMGR> 웹 사이트> 속성> 홈 디렉토리

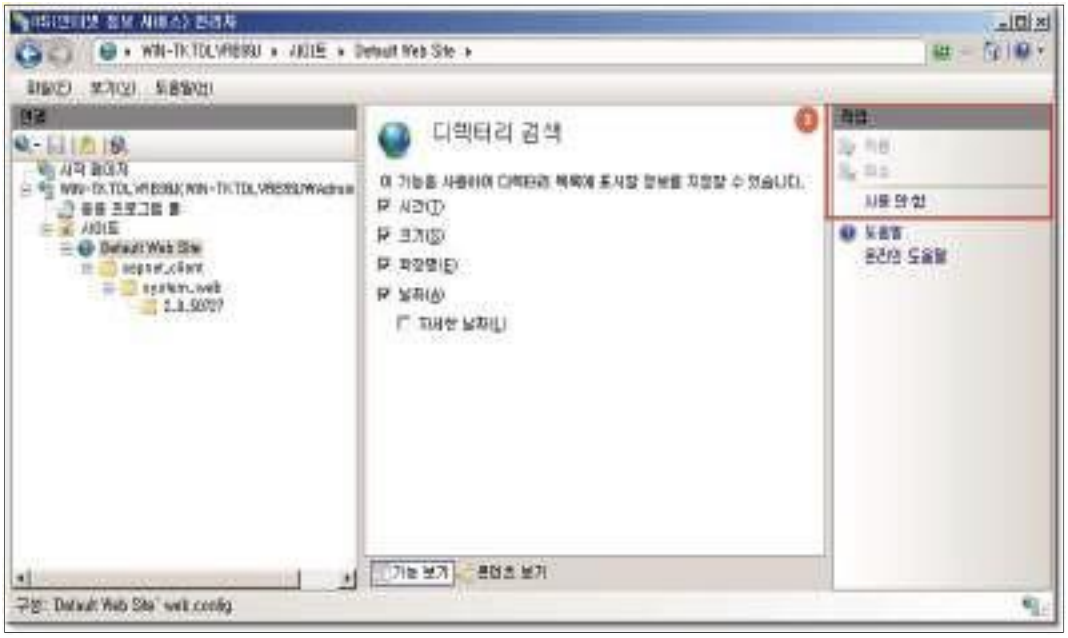
Step 2) "디렉토리 검색" 체크 해제



W-23 (상)	2. 서비스 관리 > 디렉토리 리스팅 제거

- Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹 사이트> IIS> "디렉토리 검색" 선택 후 "사용 안 함" 선택



조치 시 영향	일반적인 경우 영향 없음

2.6. IIS CGI 실행 제한

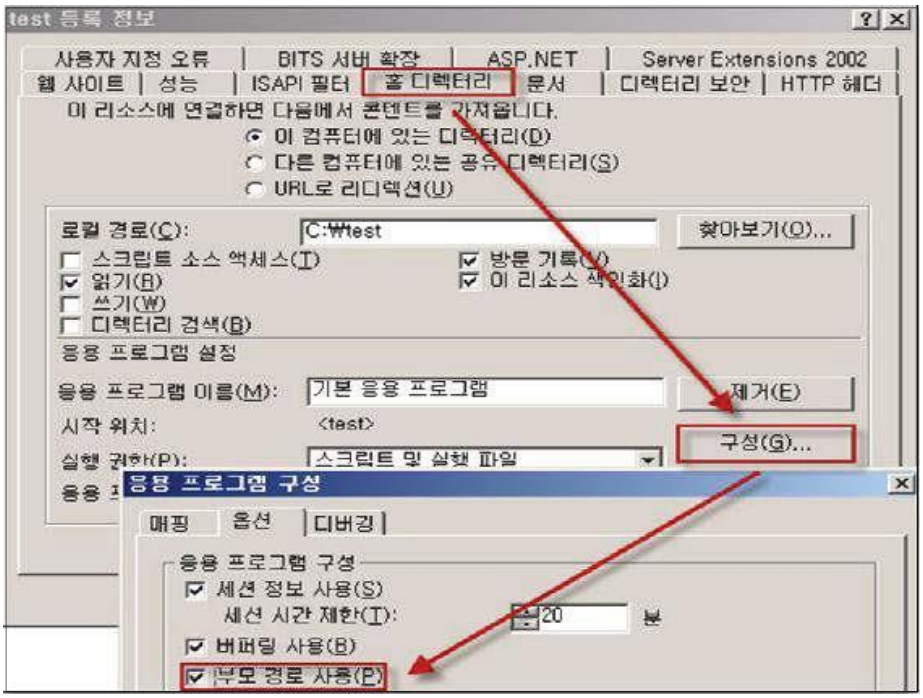
W-24 (상)	2. 서비스 관리 > IIS CGI 실행 제한
취약점 개요	
점검내용	• IIS CGI 실행 제한 설정 여부 점검
점검목적	• CGI 스크립트를 정해진 디렉토리에서만 실행되도록 하여 악의적인 파일의 업로드 및 실행을 방지하기 위함
보안위협	• 게시판이나 자료실과 같이 업로드 되는 파일이 저장되는 디렉토리에 CGI 스크립트가 실행 가능한 경우 악의적인 파일을 업로드하고 이를 실행하여 시스템의 중요 정보가 노출될 수 있으며 침해사고의 경로로 이용될 수 있음.
참고	※ CGI(Common Gateway Interface): 사용자가 서버로 보낸 데이터를 서버에서 작동중인 데이터처리프로그램에 전달하고, 여기에서 처리된 데이터를 다시 서버로 되돌려 보내는 등의 일을 하는 프로그램 ※ 일반적으로 기본 CGI 디렉토리(C:₩inetpubWscripts)는 사용하지 않음
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 해당 디렉토리 Everyone에 모든 권한, 수정 권한, 쓰기 권한이 부여되지 않은 경우
	취약 : 해당 디렉토리 Everyone에 모든 권한, 수정 권한, 쓰기 권한이 부여되어 있는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 Everyone에 모든 권한, 수정 권한, 쓰기 권한 제거 후 Administrators, System 그룹 추가(모든 권한)
점검 및 조치 사례	
• Windows 2000(IIS 5.0), 2003(IIS 6.0), 2008(IIS 7.0), 2012(IIS 8.0) Step 1) 탐색기> 해당 디렉토리> 속성> 보안 (기본 CGI 디렉토리 위치 C:₩inetpubWscripts) Step 2) Everyone 의 모든 권한, 수정 권한, 쓰기 권한 제거  ※ IIS 초기 구축시에는 scripts 폴더가 생성되지 않을 수 있음	
조치 시 영향	해당 디렉토리 확인 후 추가적인 파일이 없다면 영향 없음

2.7. IIS 상위 디렉토리 접근 금지

W-25 (상)	2. 서비스 관리 > IIS 상위 디렉토리 접근 금지
취약점 개요	
점검내용	• IIS 상위 디렉토리 접근 금지 설정 적용 여부 점검
점검목적	• ".." 와 같은 웹서버 상에서 상위 경로를 사용하지 못하도록 설정하여 Unicode 버그 및 서비스 거부 공격에 이용당하지 않도록 하기 위함
보안위협	• 이용자가 상위경로로 이동하는 것이 가능할 경우 하위경로에서 상위로 접근하며 정보 탐색이 가능하여 중요 정보가 노출될 가능성이 존재함
참고	※ ".."는 unicode 버그, 서비스 거부와 같은 공격에 쉽게 이용되므로 허용하지 않는 것을 권장함
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 상위 패스 기능을 제거한 경우
	취약 : 상위 패스 기능을 제거하지 않은 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 Everyone에 모든 권한, 수정 권한, 쓰기 권한 제거 후 Administrators, System 그룹 추가(모든 권한)
점검 및 조치 사례	

• Windows 2000(IIS 5.0), 2003(IIS 6.0)

Step 1) 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 속성> 홈디렉토리> 구성> [옵션] 탭에서 "부모 경로 사용" 의 체크박스 해제 확인



W-25 (상)	2. 서비스 관리 > IIS 상위 디렉토리 접근 금지

- Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리자> 해당 웹사이트> IIS> ASP 선택, "부모 경로 사용" 항목 "False" 설정 확인

조치 시 영향	"../" 와 같이 상대경로를 사용하도록 하드 코딩되어 있는 애플리케이션의 경우 영향 있음

2.8. IIS 불필요한 파일 제거

W-26 (상)	2. 서비스 관리 > IIS 불필요한 파일 제거
취약점 개요	
점검내용	• IIS 설치 시 기본적으로 제공되는 불필요한 파일 제거 여부 점검
점검목적	• IIS 서비스 설치 시 기본으로 설치되는 예제 스크립트, 설명서, 샘플 애플리케이션, 디렉토리 등 서비스에 불필요한 IIS 모듈을 제거하여 불필요한 공격 대상으로 이용되는 것을 방지하기 위함
보안위협	• IIS 서비스 설치 시 기본적으로 제공 되는 파일 및 디렉토리를 제거하지 않을 경우, 해당 파일들로 인해 공격 대상으로 이용되거나 백도어가 심어질 위험이 존재함
참고	-
점검대상 및 판단기준	
대상	• Windows 2000, 2003
판단기준	양호 : 해당 웹 사이트에 IISSamples, IISHelp 가상 디렉토리가 존재하지 않는 경우
	취약 : 해당 웹 사이트에 IISSamples, IISHelp 가상 디렉토리가 존재하는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 가상 디렉토리 삭제
점검 및 조치 사례	
• Windows 2000(IIS 5.0), 2003(IIS 6.0) Step 1) Sample 디렉토리 확인 후 삭제함 c:₩inetpub₩iissamples c:₩winnt₩help₩iishelp (IIS 설명서) c:₩program files₩common files₩system₩msadc₩sample (데이터 액세스) %SystemRoot%₩System32₩Inetsrv₩IISADMPWD ※ IIS 7.0(Windows 2008) 이상 버전 해당 사항 없음	
조치 시 영향	일반적인 경우 영향 없음

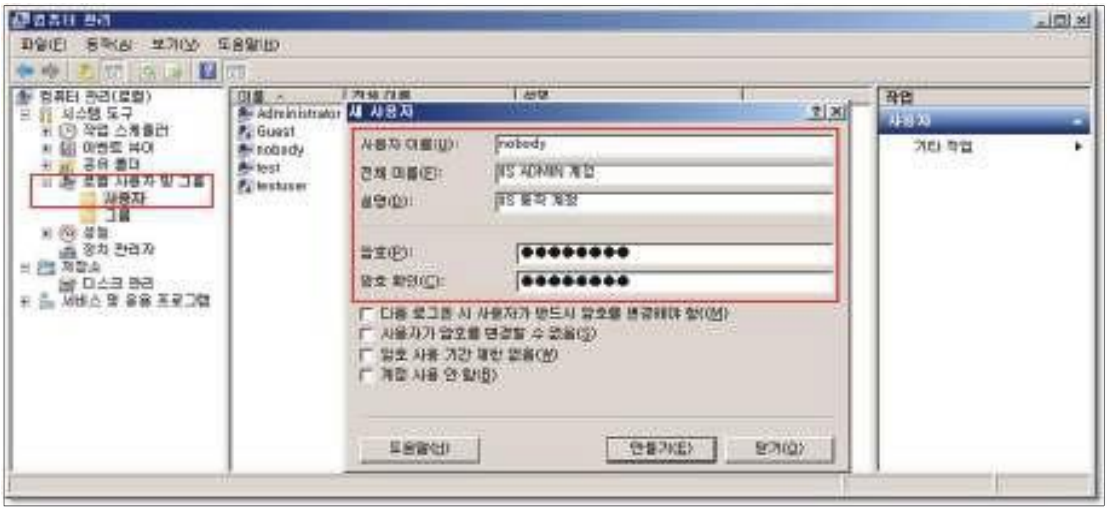
2.9. IIS 웹 프로세스 권한 제한

W-27 (상)	2. 서비스 관리 > 웹 프로세스 권한 제한
취약점 개요	
점검내용	• 웹 프로세스 권한 제한 설정 여부 점검
점검목적	• 웹 프로세스가 웹 서비스 운영에 필요한 최소한의 권한만을 갖도록 제한하여 웹사이트 방문자가 웹 서비스의 취약점을 이용해 시스템에 대한 어떤 권한도 획득할 수 없도록 하기 위함
보안위협	• 웹 프로세스 권한을 제한하지 않은 경우 웹 사이트 방문자가 웹 서비스의 취약점을 이용하여 시스템 권한을 획득할 수 있으며, 웹 취약점을 통해 접속 권한을 획득한 경우에는 관리자 권한을 획득하여 서버에 접속 후 정보의 변경, 훼손 및 유출 할 우려가 있음
참고	※ 참고로 최소 권한의 계정으로 IIS를 구동 시키는 것 이외에 '웹 사이트 등록정보' > '홈 디렉토리' > 응용프로그램 보호(IIS 프로세스 권한 설정)에서도 프로세스 권한을 설정할 수 있음 (점검 및 조치 사례 하단 참조)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 웹 프로세스가 웹 서비스 운영에 필요한 최소한 권한으로 설정되어 있는 경우
	취약 : 웹 프로세스가 관리자 권한이 부여된 계정으로 구동되고 있는 경우
조치방법	시작> 제어판> 관리 도구> 로컬 보안 정책에서 nobody 계정 설정
점검 및 조치 사례	

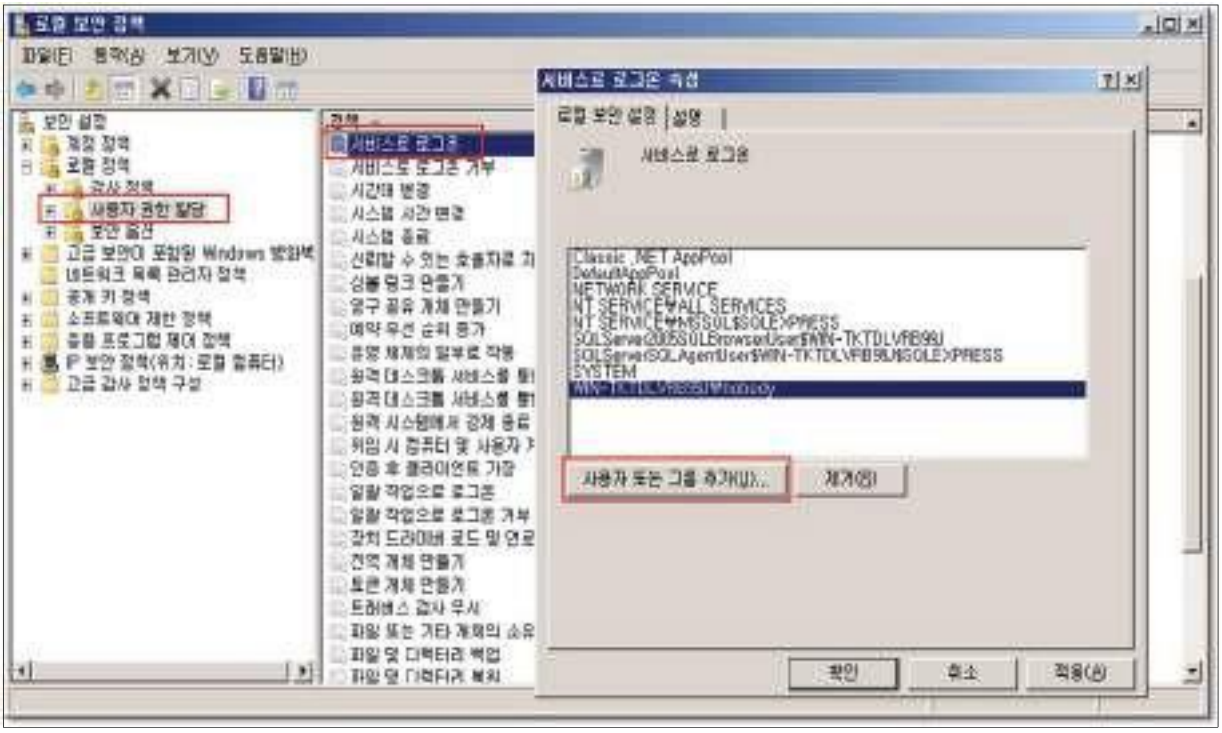
• Windows NT, 2000, 2003, 2008, 2012

Step 1) 시작> 제어판> 관리도구> 컴퓨터 관리> 로컬 사용자 및 그룹> 사용자 선택

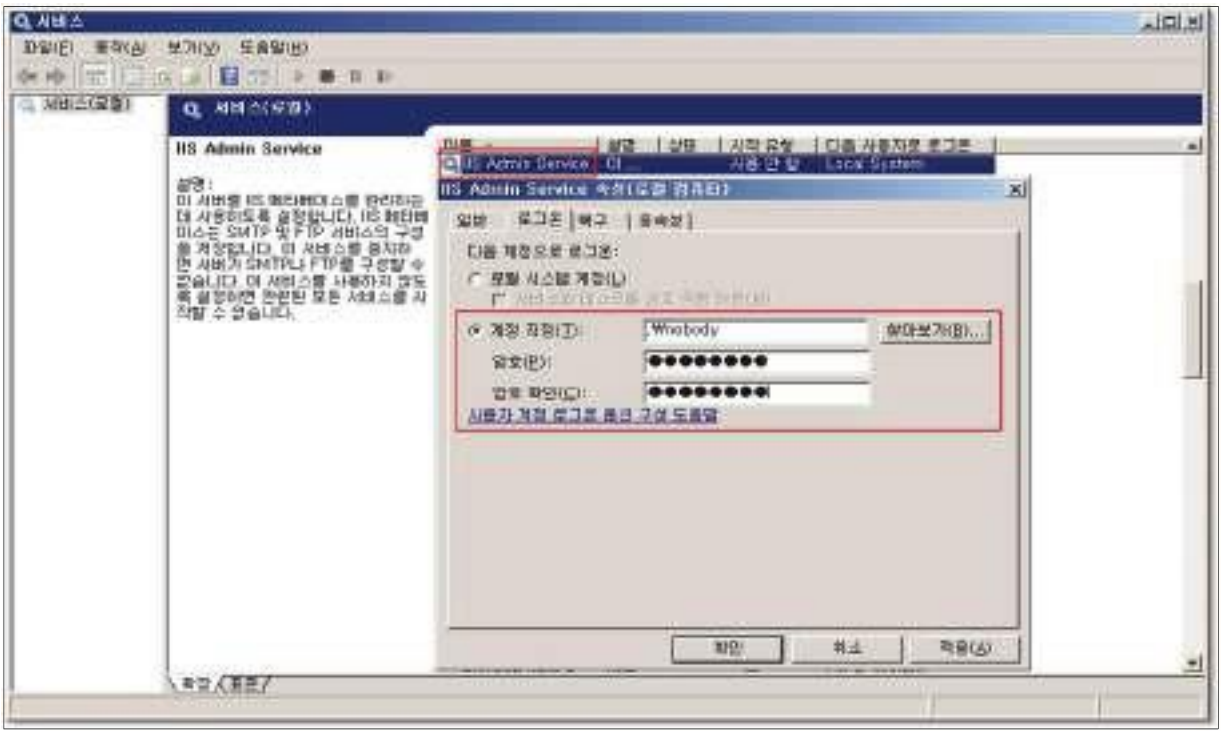
Step 2) nobody 계정 추가(nobody 계정의 소속 그룹에 정해진 User가 있으면 제거)



Step 3) 시작> 제어판> 관리도구> 로컬 보안 정책> 로컬 정책> 사용자 권한 할당 선택, "서비스 로그온"에 "nobody" 계정 추가



Step 4) 시작> 실행> SERVICES.MSC> IIS Admin Service> 속성> [로그온] 탭의 계정 지정에 nobody 계정 및 패스워드 입력



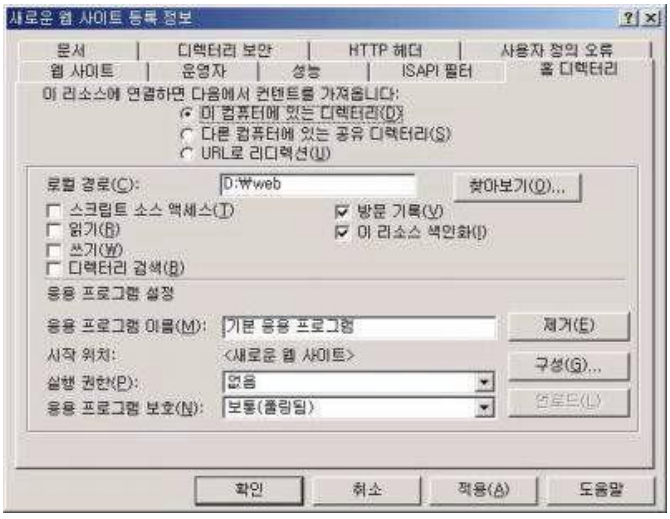
W-27 (상)	2. 서비스 관리 > 웹 프로세스 권한 제한

Step 5) 시작> 프로그램> 윈도우 탐색기> IIS 가 설치된 폴더 속성> [보안] 탭에서 nobody 계정을 추가하고 모든 권한 체크

※ '웹 사이트 등록정보' > '홈 디렉토리 > 응용프로그램 보호(IIS 프로세스 권한 설정)

- 낮음(IIS 프로세스): IIS 프로세스는 시스템 권한을 가짐
- 보통(폴링됨): IIS 프로세스를 실행과 동시에 일반 권한의 계정으로 권한 강화(falling)
- 높음(격리됨): IIS 프로세스를 Guest 권한에 준하는 권한으로 실행시킴

세 가지 권한 중 '낮음'으로 되어 있는 경우, IIS 프로세스는 시스템 권한을 가지게 되므로 해커가 IIS 프로세스의 권한을 획득하면 관리자에 준하는 권한을 가질 수 있으므로 주의 해야 함



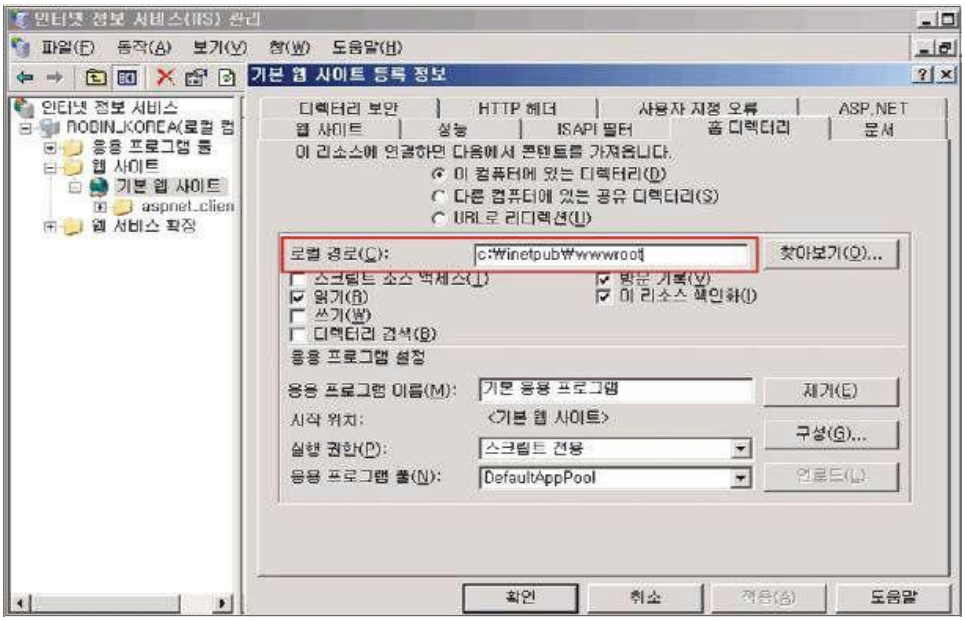
조치 시 영향	일반적인 경우 영향 없음

2.10. IIS 링크 사용금지

W-28 (상)	2. 서비스 관리 > IIS 링크 사용금지
취약점 개요	
점검내용	• IIS 링크 사용금지 설정 여부 점검
점검목적	• 웹 컨텐즈 디렉토리에서 다른 디렉토리나 파일들에 접근할 수 있는 심볼릭 링크, 별칭(aliases), 바로가기 등을 제거하여 허용하지 않은 경로의 접근을 차단하기 위함
보안위협	• 접근을 허용한 웹 콘텐츠 디렉토리 내에 서버의 다른 디렉토리나 파일들에 접근할 수 있는 심볼릭 링크, aliases, 바로가기 등이 존재하는 경우 해당 링크를 통해 허용하지 않은 다른 디렉토리에 액세스 할 수 있는 위험성 존재
참고	-
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 심볼릭 링크, aliases, 바로가기 등의 사용을 허용하지 않는 경우
	취약 : 심볼릭 링크, aliases, 바로가기 등의 사용을 허용하는 경우
조치방법	등록된 웹 사이트의 홈 디렉토리에 있는 심볼릭 링크, aliases, 바로가기 파일 삭제
점검 및 조치 사례	

• Windows 2000(IIS 5.0), 2003(IIS 6.0)

Step 1) 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 속성> [홈 디렉토리] 탭 선택> "로컬 경로" 에서 홈 디렉토리 위치 확인



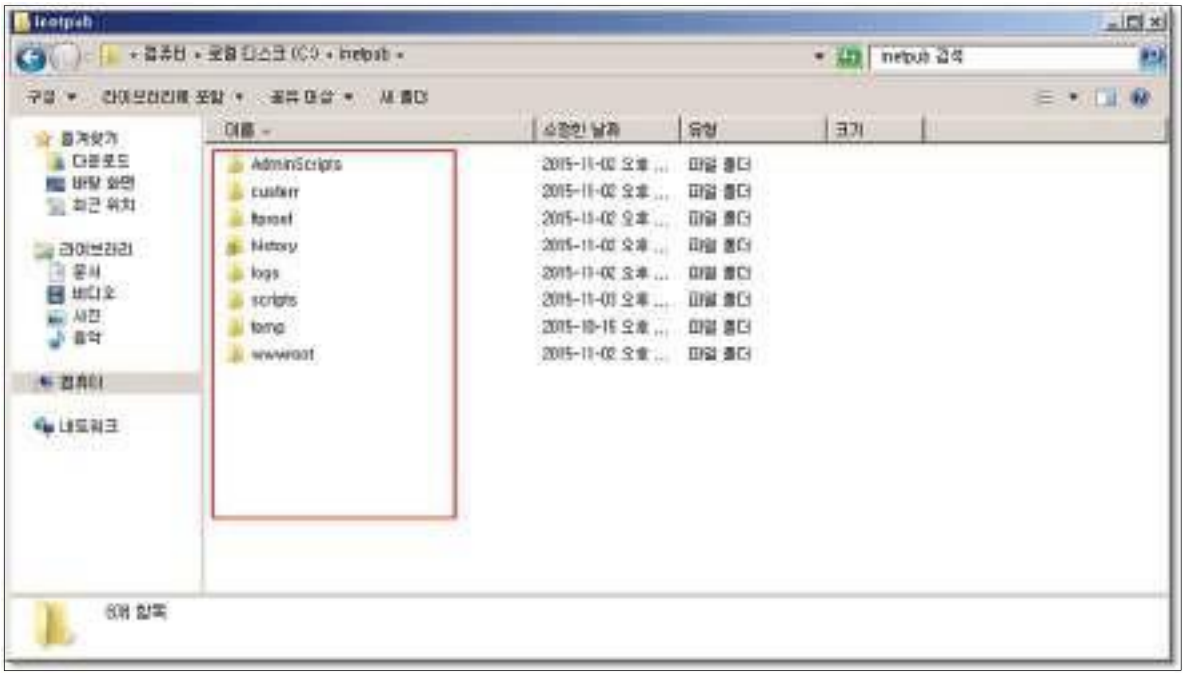
W-28 (상)	2. 서비스 관리 > IIS 링크 사용금지

Step 2) 로컬 경로에 입력된 홈 디렉토리로 이동하여 바로가기 파일 삭제

- Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리자> 해당 웹사이트> 기본 설정> "실제 경로"에서 홈 디렉토리 위치 확인

Step 2) 실제 경로에 입력된 홈 디렉토리로 이동하여 바로가기 파일 삭제



조치 시 영향	일반적인 경우 영향 없음

2.11. IIS 파일 업로드 및 다운로드 제한

W-29 (상)	2. 서비스 관리 > IIS 파일 업로드 및 다운로드 제한
취약점 개요	
점검내용	• IIS 파일 업로드 및 다운로드 제한 설정 여부 점검
점검목적	• 기반시설 시스템은 파일의 업로드 및 다운로드를 원칙적으로 금지하나, 부득이 파일의 업로드 및 다운로드 기능을 활용해야 하는 경우, 파일의 용량 제한을 설정하여 보안성 유지 및 안정적인 웹서버 자원관리를 할 수 있도록 하기 위함
보안위협	• 대용량 파일 업로드 및 다운로드가 가능한 경우 서버 리소스에 영향을 주어 서비스 장애가 발생할 수 있음
참고	※ IIS에서는 파일의 업로드 및 다운로드 기능을 직접적으로 차단하는 기능이 없어, 웹사이트 내 파일의 업로드 및 다운로드 기능의 구현 여부의 병행 점검이 필요
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 웹 프로세스의 서버 자원 관리를 위해 업로드 및 다운로드 용량을 제한하는 경우
	취약 : 웹 프로세스의 서버 자원을 관리하지 않는 경우 (업로드 및 다운로드 용량 미 제한)
조치방법	파일 업로드 및 다운로드 용량을 허용할 수 있는 최소 범위로 설정
점검 및 조치 사례	

• Windows NT, 2000, 2003

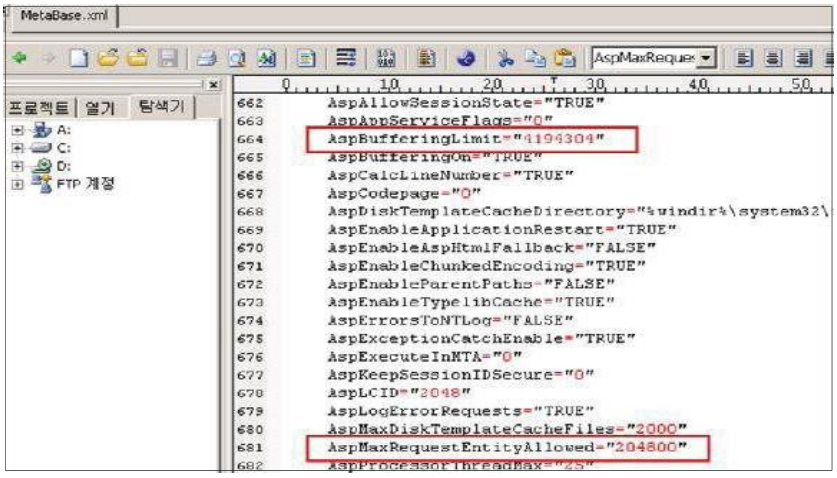
Step 1) 시작> 실행> SERVICES.MSC> IISADMIN> 속성> [일반] 탭에서 서비스 중지

Step 2) %systemroot%Wsystem32WinetsrvWMetaBase.xml 파일을 찾아 편집기로 OPEN

Step 3) AspMaxRequestEntityAllowed 값을 찾아 파일 업로드 용량을 최소 범위로 제한

Step 4) AspBufferingLimit 값을 찾아 파일 다운로드 용량을 최소 범위로 제한

Step 5) 시작> 실행> SERVICES.MSC> IISADMIN> 속성> [일반] 탭에서 서비스 시작

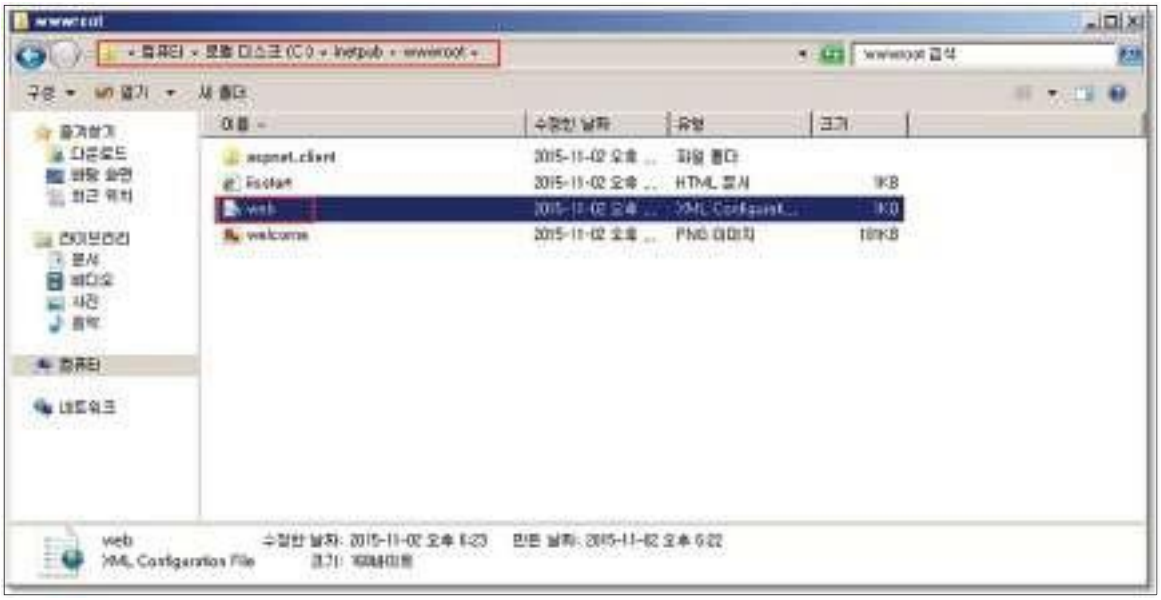


W-29 (상)	2. 서비스 관리 > IIS 파일 업로드 및 다운로드 제한

- Windows 2008, 2012

Step 1) 등록된 웹 사이트의 루트 디렉터리 디렉토리에 있는 web.config 파일 내 아래 항목 추가 (web.config 파일이 없으면 사이트 홈 디렉토리에 새로 생성)

```
<configuration>
  <system.webServer>
    <security>
      <requestFiltering>
          <requestLimits maxAllowedContentLength="콘텐츠용량" />
      </requestFiltering>
    </security>
  </system.webServer>
</configuration>
```

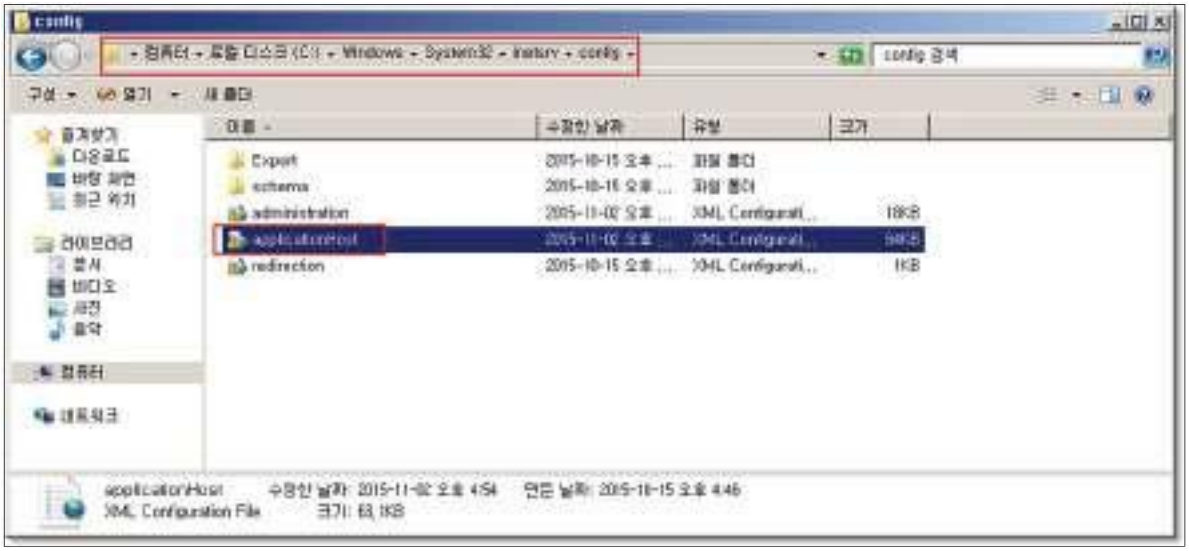


[upload 및 download 용량 제한 - web.config 파일 편집]

Step 2) %systemroot%₩system32₩inetsrv₩config₩applicationHost.config 파일 내 아래 항목 추가

```
<system.webServer>
  <asp>
    <limits bufferingLimit="파일다운로드용량" maxRequestEntityAllowed="파일업로드용량"/>
  </asp>
</system.webServer>
```

W-17 (상)	2. 서비스 관리 > 2.11 IIS 파일 업로드 및 다운로드 제한



[upload 및 download 용량 제한 - applicationHost.config 파일 편집]

※ Default 설정 값

(1) maxAllowedContentLength (콘텐츠 용량) => Default: 30MB

(2) MaxRequestEntityAllowed (파일 업로드 용량) => Default: 200000 byte

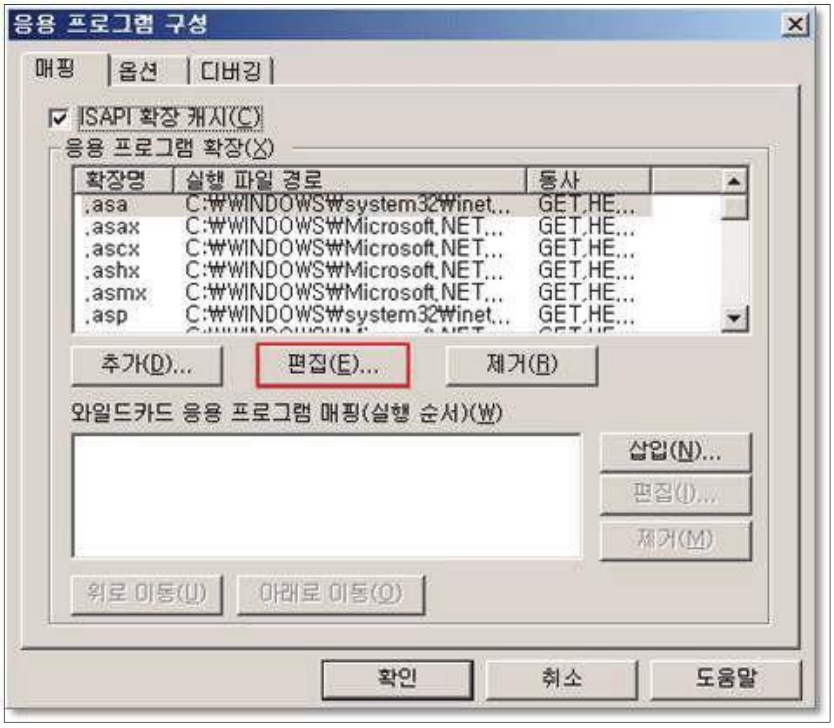
(3) bufferingLimit (파일 다운로드 용량)=> Default: 4MB(4194304 byte)

조치 시 영향	일반적인 경우 영향 없음

2.12. IIS DB 연결 취약점 점검

W-30 (상)	2. 서비스 관리 > IIS DB 연결 취약점 점검
취약점 개요	
점검내용	• Global.asa 또는 별도의 DB 컨넥션을 하는 파일에 대한 취약점 점검
점검목적	• DB 컨넥션 파일(global.asa)에 대한 접근을 제한하여 SQL 서버의 사용자명과 패스워드와 같은 중요 정보의 노출을 차단하기 위함
보안위협	• global.asa 파일에는 데이터베이스 관련 정보(IP 주소, DB명, 패스워드), 내부 IP 주소, 웹 애플리케이션 환경설정 정보 및 기타 정보 등 보안상 민감한 내용이 포함되어 있으므로 해당 파일이 악의적인 사용자에게 노출될 경우 침해사고로 이어질 수 있음
참고	※ global.asa 파일: 각각의 ASP(Active Server Pages) 프로그램을 위해 IIS 서버상에서 관리되는 파일. IIS 서버는 IIS 프로그램이 시작하고 정지할 때, 혹은 웹 클라이언트가 ASP 프로그램의 웹 페이지들을 액세스하는 브라우저 세션들을 시작하고 정지할 때 자동적으로 global.asa 파일을 처리함
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : .asa 매핑 시 특정 동작만 가능하도록 제한하여 설정한 경우 또는 매핑이 없을 경우
	취약 : .asa 매핑 시 모든 동작이 가능하도록 설정한 경우
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 .asa 매핑을 아래 그림과 같이 특정 동작만 가능하도록 추가(IIS 6.0) / asa 설정을 false 함(7.0, 8.0)
점검 및 조치 사례	
• Windows 2000(IIS 5.0), 2003(IIS 6.0) Step 1) asa 매핑 등록 확인 인터넷 정보 서비스(IIS) 관리자> 웹 사이트> 해당 웹 사이트> 속성> [홈 디렉토리] 탭에서 구성> [매핑] 탭 선택 후 .asa 매핑이 등록되어 있는지 확인	

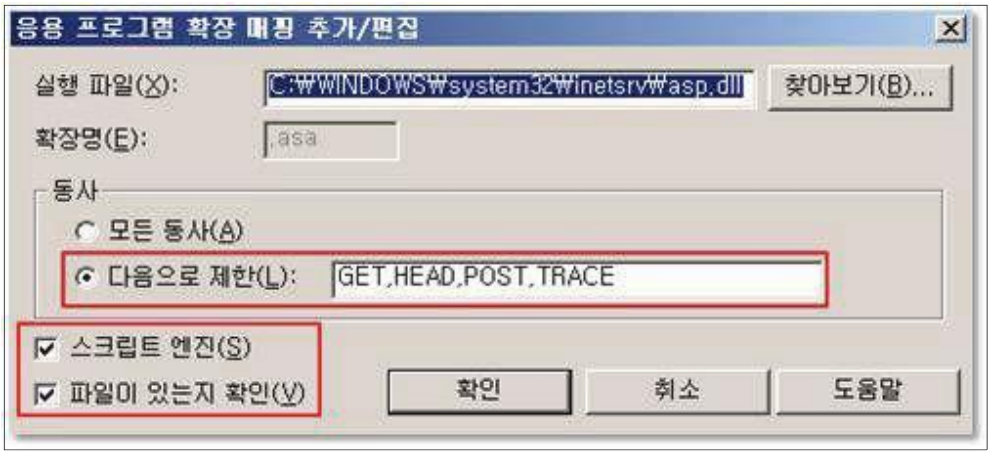
W-30 (상)	2. 서비스 관리 > IIS DB 연결 취약점 점검



Step 2) asa 매핑 등록되어 있다면 특정 동작만 가능하도록 설정되어 있는지 확인

[매핑] 탭에서 [편집] 내용이 다음과 동일하게 설정되어 있는지 확인

- 동사> 다음으로 제한> GET, HEAD, POST, TRACE 입력
- 스크립트 엔진 체크
- 파일이 있는지 확인 체크



- Windows 2008(IIS 7.0), 2012(IIS 8.0)

총 2가지 항목에서 확인 필요

2가지 항목이 모두 아래의 방법과 같이 설정되어 있을 경우 취약하다고 볼 수 있으며, 한 가지 경우라도 설정이 되어 있지 않거나 해당 설정이 없을 시 양호하다고 판단함

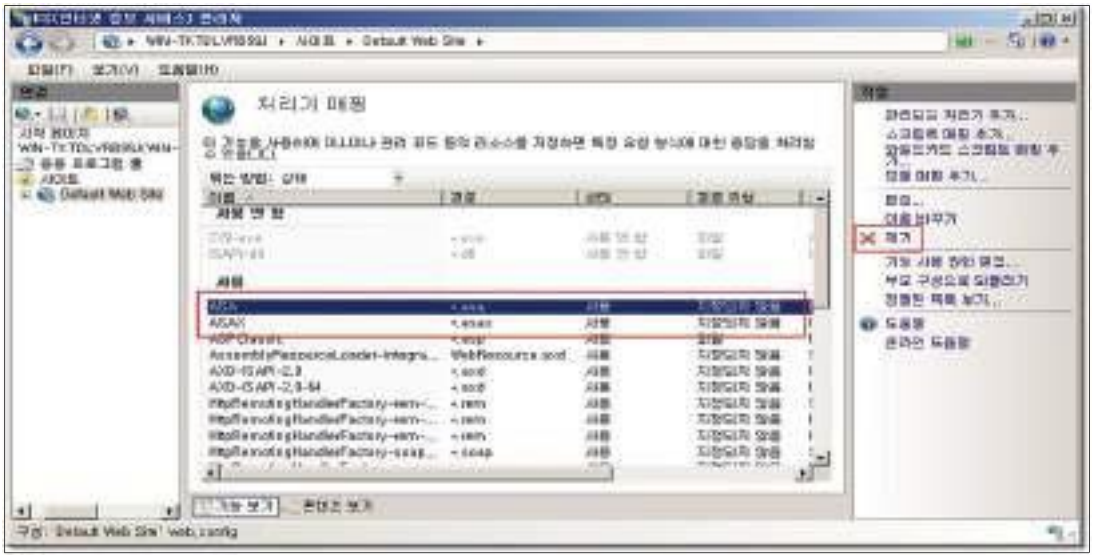
W-30 (상)	2. 서비스 관리 > IIS DB 연결 취약점 점검

1. asa / asax 스크립트 매핑 확인

Step 1) 매핑이 없을 경우 양호

인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> "처리기 매핑" 선택, 사용 항목에 *.asa / *.asax 등록되지 않을 경우 양호

※ 아래 이미지처럼 등록되어 있을 경우 삭제 시 양호

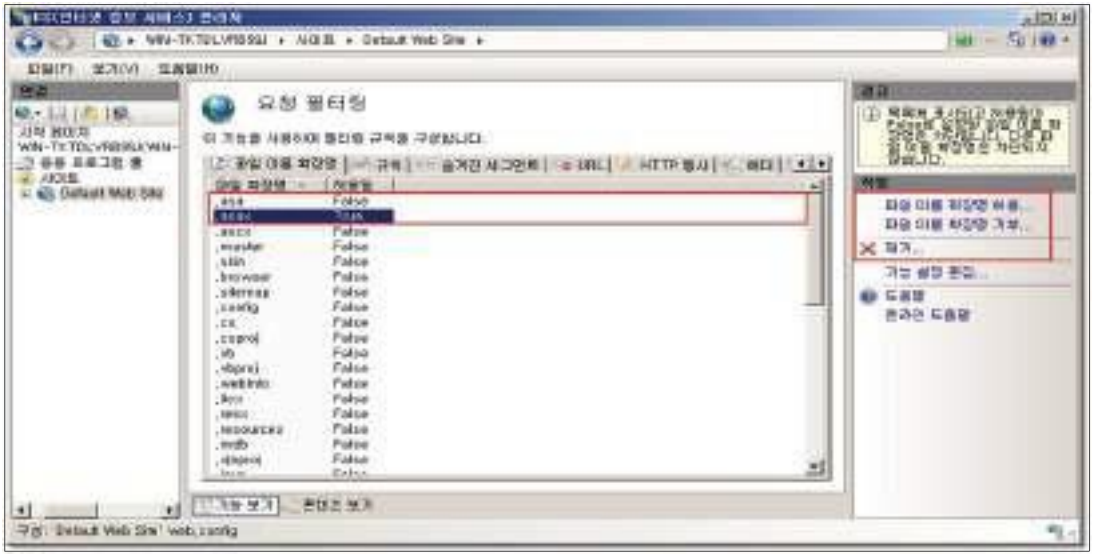


2. asa / asax 파일 필터링 확인

Step 1) false 일 경우 양호

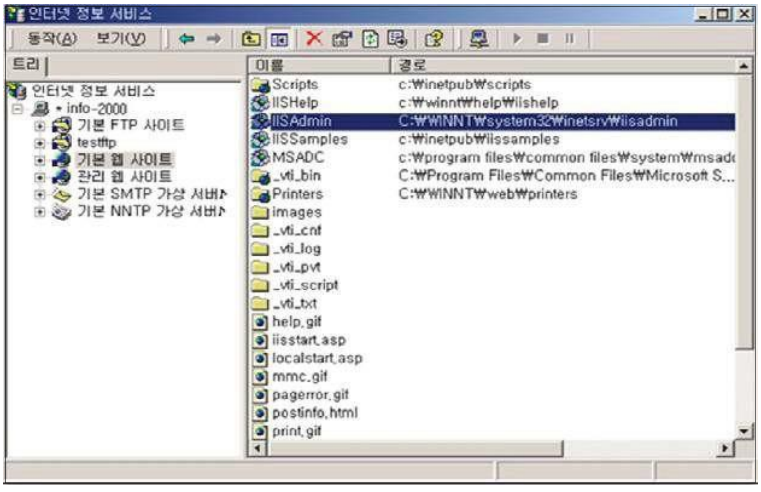
인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> IIS> "요청 필터링" 선택, .asa / .asax 확장자가 false로 설정되어 있는지 확인

※ true 일 경우 제거하고 "파일 이름 확장명 거부" 에 등록



조치 시 영향	일반적인 경우 영향 없음

2.13. IIS 가상 디렉토리 삭제

W-31 (상)	2. 서비스 관리 > IIS 가상 디렉토리 삭제
취약점 개요	
점검내용	• 불필요한 IIS 가상 디렉토리 삭제 여부 점검
점검목적	• IIS 를 설치 시 가상 디렉토리 내에 제공되는 취약한 샘플 어플리케이션을 제거하여 잠재적인 위험을 제거하기 위함
보안위협	• 기본 가상 디렉토리가 삭제되지 않은 경우 ADSI 스크립트를 이용한 기본 웹 사이트 설정을 변경 및 MSADC 가상 디렉토리를 통한 서버 자원 접근이 가능하여 악의적인 공격의 대상이 될 수 있음
참고	※ /issadmpwd 파일을 제거하고 이 외 존재하는 가상 디렉토리 취약점을 줄이기 위해서 IIS Admin에 관계되는 모든 파일 및 디렉토리를 삭제하여야 함 ※ IIS 4.0, 5.0 설치 시 기본적으로 /issadmpwd라는 가상 디렉토리를 생성하는데, 이 디렉토리에는 웹 서버를 통하여 패스워드를 변경시켜주는 기능 등을 하는 .HTR 파일이 존재함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 해당 웹 사이트에 IIS Admin, IIS Adminpwd 가상 디렉토리가 존재하지 않는 경우
	취약 : 해당 웹 사이트에 IIS Admin, IIS Adminpwd 가상 디렉토리가 존재하는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 IIS Admin, IIS Adminpwd 삭제
점검 및 조치 사례	
• Windows 2000(IIS 5.0) Step 1) 시작> 실행> INETMGR> 웹 사이트> IISAdmin, IISAdminpwd 선택> 삭제  ※ Windows 2003(6.0) 이상 버전 해당 사항 없음	
조치 시 영향	일반적으로 IIS 관리용 페이지를 사용하지 않으므로 영향 없음

2.14. IIS 데이터 파일 ACL 적용

W-32 (상)	2. 서비스 관리 > IIS 데이터 파일 ACL 적용
취약점 개요	
점검내용	• IIS 데이터 파일 ACL 적용 여부 점검
점검목적	• 웹 데이터 파일에 ACL을 부여함으로써 권한 없는 사용자로부터의 실행 및 읽기를 방지하고자 함
보안위협	• 웹 데이터 파일에 ACL을 부여되지 않은 경우 권한 없는 사용자로부터의 읽기 및 실행이 가능
참고	※ 향후 필요에 의해 IIS를 설치하여 운용한다면 웹 데이터 파일에 대한 ACL을 부여하는 것이 바람직하며 ACL을 설정할 때에는 다음과 같은 사항을 참고하여 설정하여야 함 1. 가능한 파일의 종류끼리 분류하여 폴더에 저장 2. 홈 디렉토리(기본: c:₩inetpub₩wwwroot)내에 적절한 ACL 권한 부여. ※ ACL(Access Control List): 접근이 허가된 주제들과 허가받은 접근 종류들이 기록된 목록
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 홈 디렉토리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하지 않는 경우(정적 콘텐츠 파일은 Read 권한만)
	취약 : 홈 디렉토리 내에 있는 하위 파일들에 대해 Everyone 권한이 존재하는 경우 (정적 콘텐츠 파일은 Read 권한 제외) ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	IIS 서비스를 사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 홈 디렉토리에 Administrators, System 권한만 설정 후, 하위 디렉토리에 존재하는 모든 Everyone 권한 제거(정적 콘텐츠 파일에 경우 Read 권한 허용)
점검 및 조치 사례	

• Windows 2000(IIS 5.0), 2003(IIS 6.0)

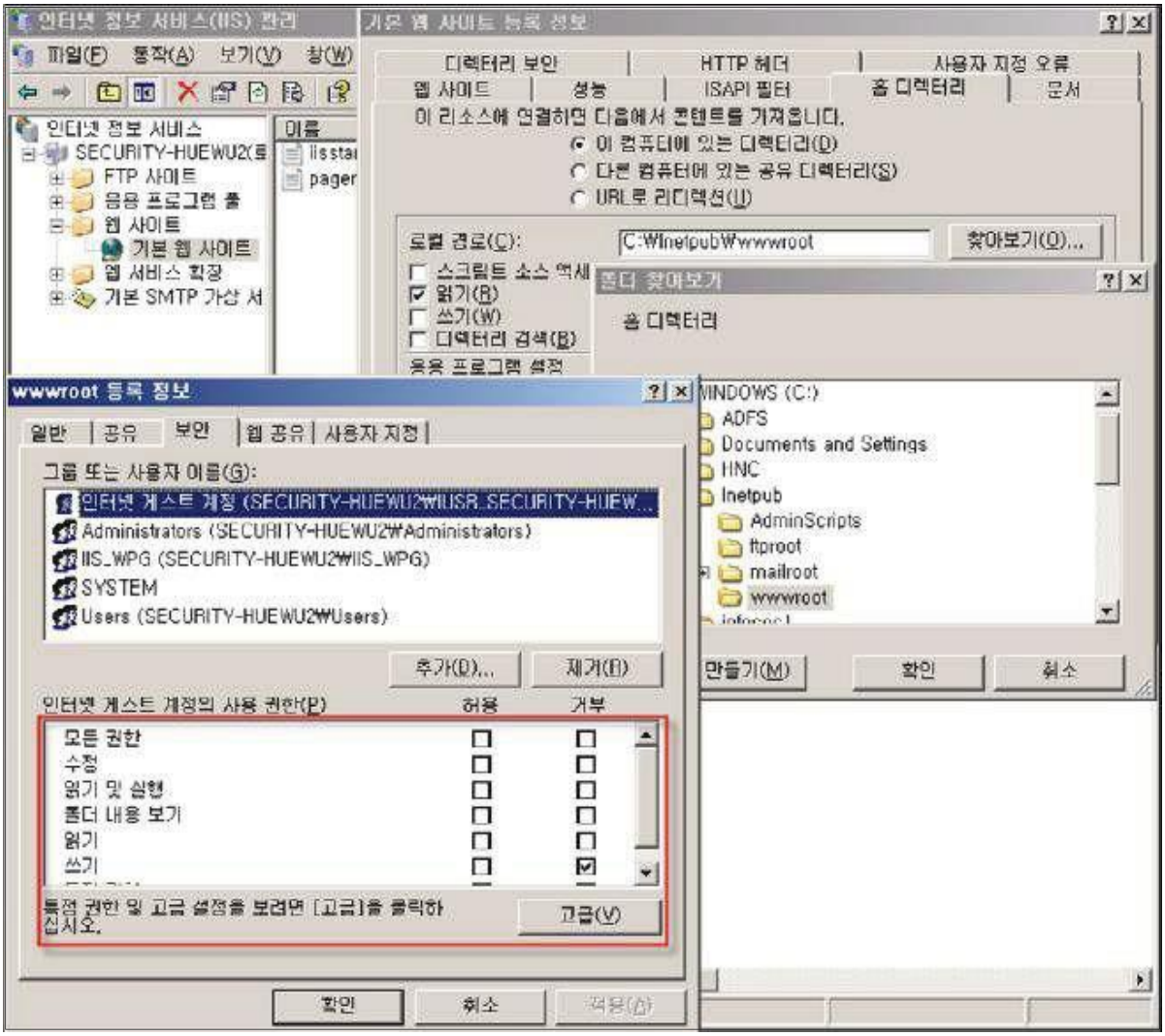
Step 1) 시작> 실행> INETMGR> 웹 사이트> 해당 웹사이트> 속성> 홈 디렉토리 경로 확인

Step 2) 탐색기를 이용하여 홈 디렉토리의 등록정보> [보안] 탭에서 Everyone 권한 확인

Step 3) 아래와 같은 파일들에 대한 불필요한 Everyone 권한 제거

파일 형식	액세스 제어 목록
CGI (.exe, .dll, .cmd, .pl)	모든 사람(X), 관리자/시스템(전제 제어)
스크립트 파일(.asp)	모든 사람(X), 관리자/시스템(전제 제어)
포함 파일(.inc, .shtm, .shtml)	모든 사람(X), 관리자/시스템(전제 제어)
정적 콘텐츠(.txt, .gif, .Jpg, .html)	모든 사람(R), 관리자/시스템(전제 제어)

W-32 (상)	2. 서비스 관리 > IIS 데이터 파일 ACL 적용



- Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 시작> 실행> INETMGR> 사이트> 해당 웹사이트> 기본 설정> 홈 디렉토리 실제 경로 확인

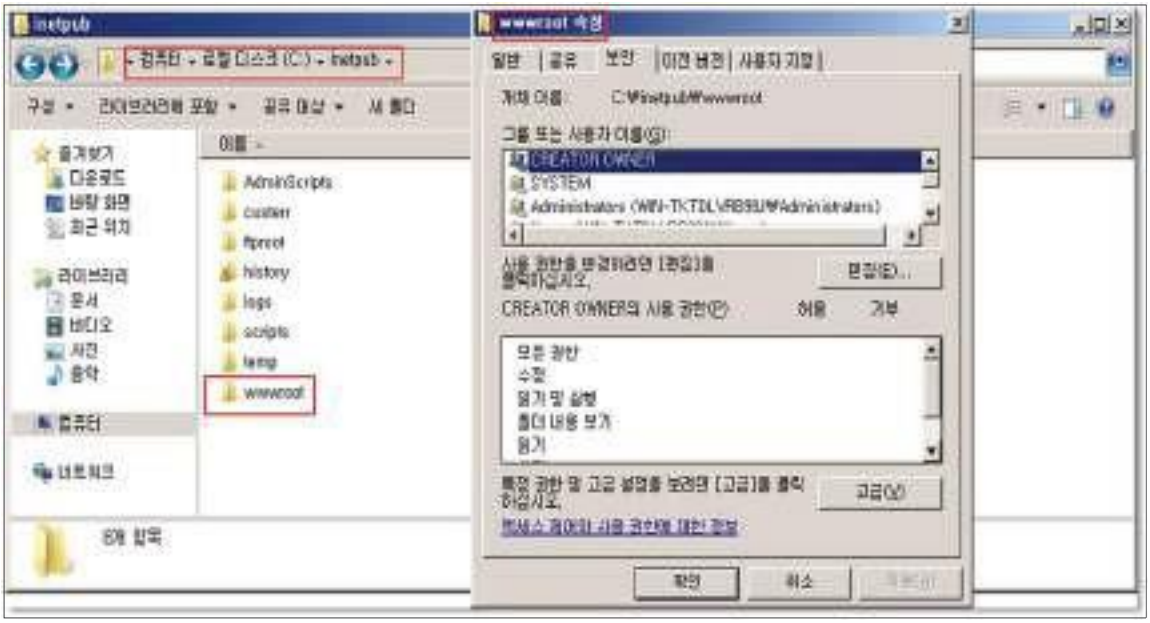
Step 2) 탐색기를 이용하여 홈 디렉토리의 등록 정보> [보안] 탭에서 Everyone권한 확인

Step 3) 아래와 같은 파일들에 대한 불필요한 Everyone 권한 제거

파일 형식	액세스 제어 목록
CGI (.exe, .dll, .cmd, .pl)	모든 사람(X), 관리자/시스템(전제 제어)
스크립트 파일(.asp)	모든 사람(X), 관리자/시스템(전제 제어)

W-32 (상)	2. 서비스 관리 > IIS 데이터 파일 ACL 적용

[웹사이트 실제 경로 확인]



[웹사이트 홈디렉토리 내 everyone 권한 확인]

조치 시 영향	IIS에서 홈 디렉토리 내에 있는 데이터 파일 권한 조치에 따른 검증 필요

2.15. IIS 미사용 스크립트 매핑 제거

W-33 (상)	2. 서비스 관리 > IIS 미사용 스크립트 매핑 제거
취약점 개요	
점검내용	• IIS 미사용 스크립트 매핑 제거 여부 점검
점검목적	• 사용하지 않은 확장자 매핑을 제거하여 추가 공격의 위험을 제거하기 위함
보안위협	• 미사용 확장자 매핑을 제거하지 않은 .htr .idc .stm .shtm .shtml .printer .htw .ida .idq 확장자는 버퍼 오버플로우(Buffer Overflow) 공격 위험이 존재함
참고	※ 사용하지 않는 스크립트 매핑은 보안에 위협이 될 수 있으므로 개발자와 협의하여 불필요한 매핑인지 확인한 후 제거해야 함 ※ .asp나 .shtm 과 같은 확장자들은 특정 DLL 파일과 매핑 되어 있어, 이러한 파일들에 대한 요청이 들어오면 해당 DLL에 의해 처리됨 ※ 스크립트 매핑: IIS는 클라이언트가 요청한 자원의 파일 확장자에 따라서 이를 처리할 ISAPI 확장 핸들러를 지정하게 되어 있는데 이를 스크립트 매핑이라고 함 ※ 버퍼 오버플로우(Buffer Overflow): 메모리에 할당된 버퍼의 양을 초과하는 데이터를 입력하여 프로그램의 복주귀소를 조작, 궁극적으로 해커가 원하는 코드를 실행하는 것
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하지 않는 경우
	취약 : 취약한 매핑(.htr .idc .stm .shtm .shtml .printer .htw .ida .idq)이 존재하는 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 취약한 매핑 제거 (아래 표 참고)
점검 및 조치 사례	

• Windows 2000(IIS 5.0), 2003(IIS 6.0)

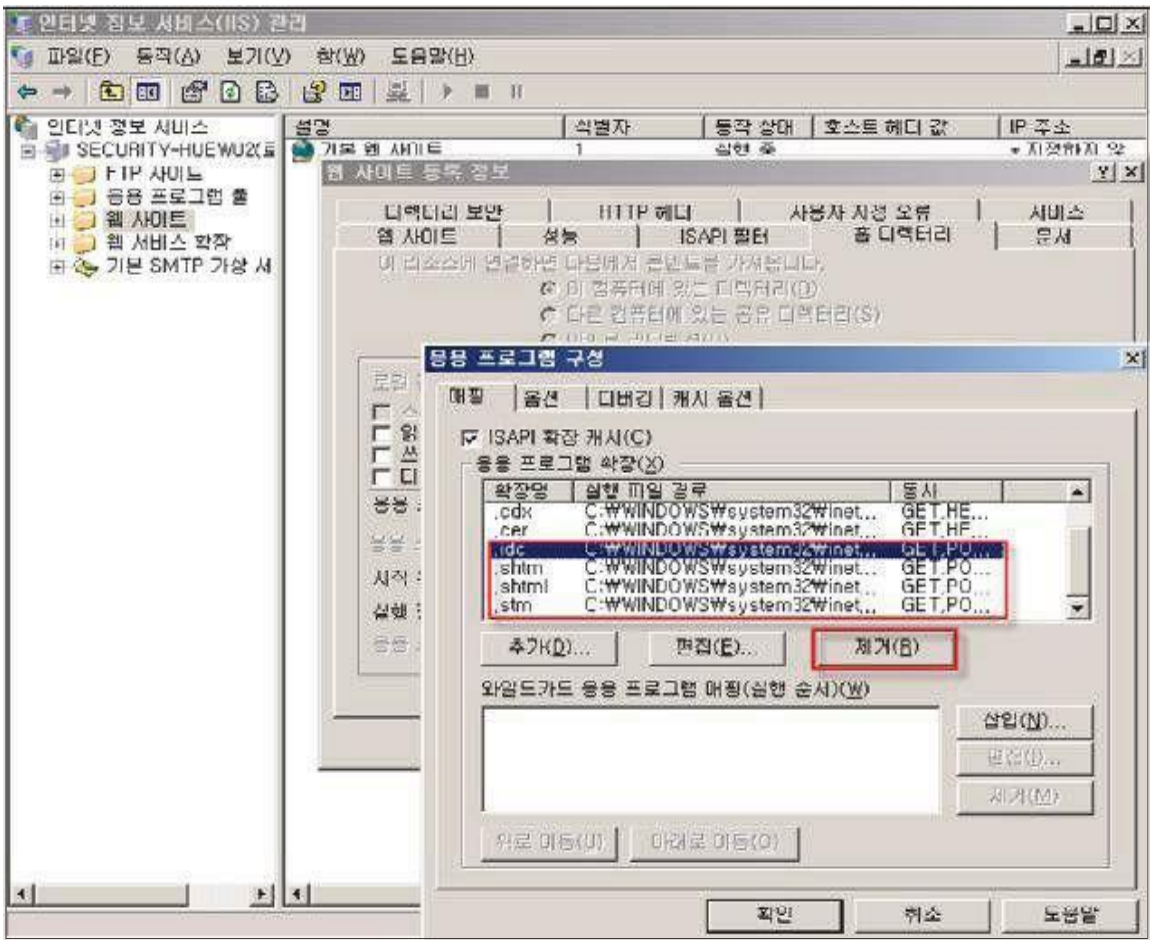
Step 1) 시작> 실행> INETMGR> 웹 사이트> 해당 웹 사이트> 속성> [홈 디렉토리] 탭에서 [구성] 버튼 선택

Step 2) [매핑] 탭에서 아래와 같은 취약한 매핑 제거

확장자명	기능	취약점
asp	Active Server Pages 기능 지원	Buffer Overflow MS02-018 • Win 2000 SP3 이상 양호
htr	Web-based password reset: Outlook Web Access 등에서 웹 기반 응용 프로그램으로 자신의 사용자 계정 암호 변경	+.htr 소스 공개 취약점 MS01-004 • Win 2000 SP3, NT SP 7.0 이상 양호

W-33 (상)	2. 서비스 관리 > IIS 미사용 스크립트 매핑 제거

idc	Internet Database Connector: SQL 서버에 연결하기 위한 정보 등을 관리함. asp를 통해 같은 작업을 수행 가능	Web 디렉토리 패스 공개 Q193689 • NT4.0, NT SP6a이상 양호
stm, stml, shtml	Server-Side Includes	Buffer Overflow MS01-044 • Win 2000 SP3 이상 양호
printer	Internet Printing : URL을 사용하여 페이지를 프린터로 인쇄할 수 있도록 함 IIS가 인터넷이나 인트라넷을 통해 인쇄 서버 기능 수행	Buffer Overflow MS01-023 • Win 2000 SP2 이상 양호
ida, idq	Index Server : idq.dll에 매핑되며 인덱스 서버를 쿼리할 때 사용	Buffer Overflow MS01-033 • Win 2000 SP3 이상 양호
htw	Index Server : webhits.dll에 매핑되며, 인덱스 서버를 쿼리할 때 사용	Webhit 소스 공개 취약점 MS00-006 • Win 2000 SP1 이상 양호

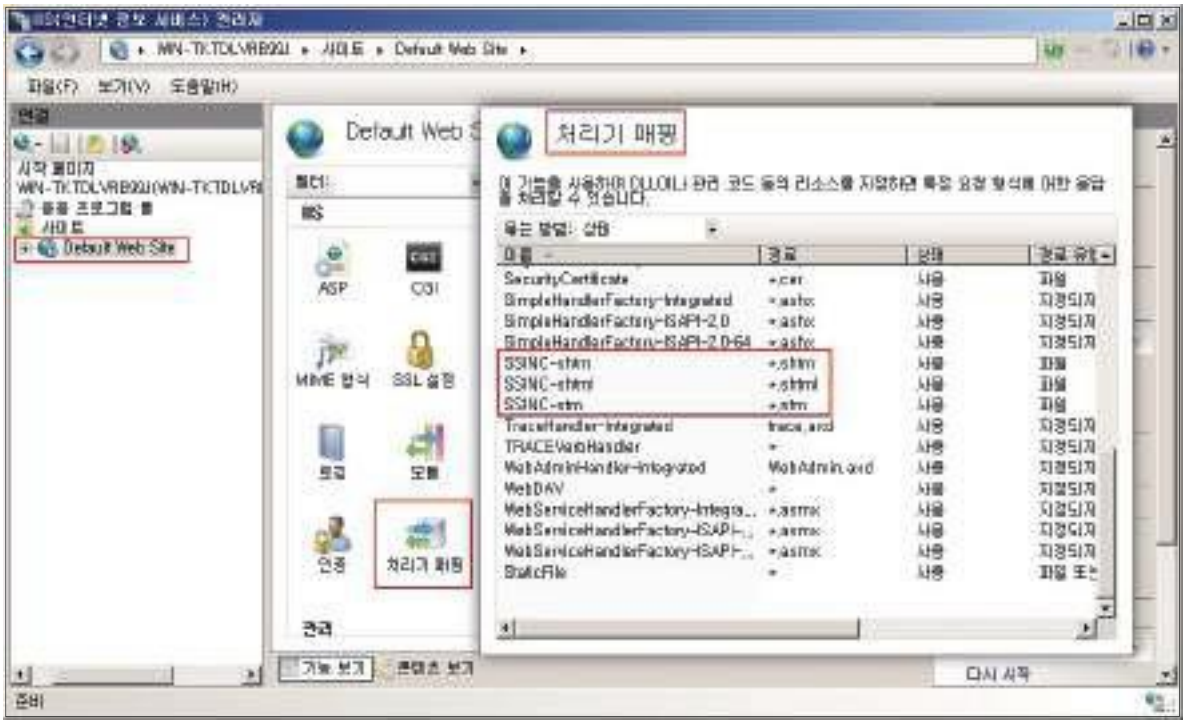


W-33 (상)	2. 서비스 관리 > IIS 미사용 스크립트 매핑 제거

- Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 시작> 실행> INETMGR> 웹 사이트> 해당 웹 사이트> 처리기 매핑 선택

Step 2) 취약한 매핑 제거(.htr, .idc, .stm, .shtm, .shtml, .printer, .htw, .ida, .idq)



조치 시 영향	일반적인 경우 영향 없음

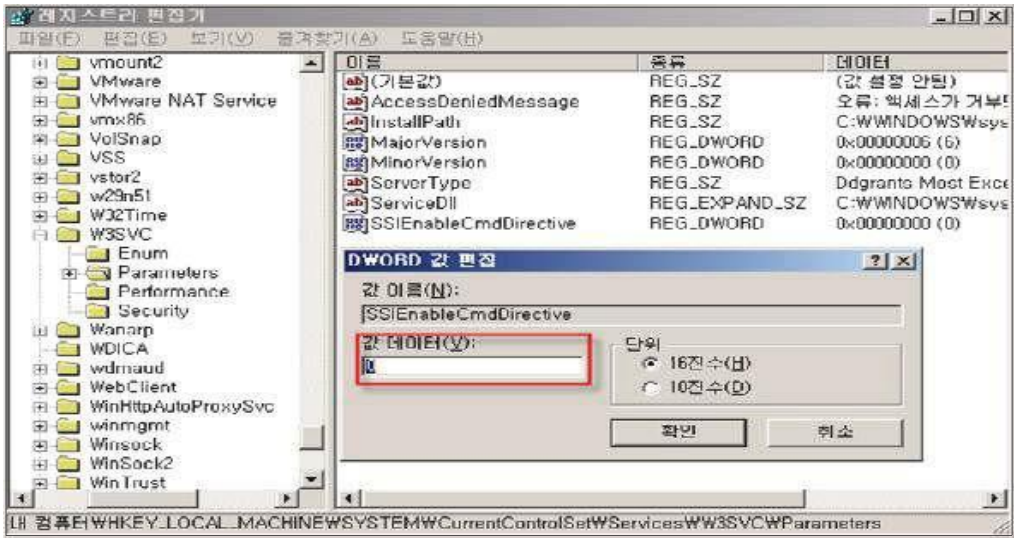
2.16. IIS Exec 명령어 쉘 호출 진단

W-34 (상)	2. 서비스 관리 > IIS Exec 명령어 쉘 호출 진단
취약점 개요	
점검내용	• IIS Exec 명령어 쉘 호출 여부 진단
점검목적	• 웹 서버에서 임의 명령어 호출을 제한하여 허가되지 않은 명령어 실행을 차단하기 위함
보안위협	• 웹 서버에서 # exec 명령어를 통한 명령어 실행이 차단되지 않은 경우, 웹 서버에서 임의의 시스템 명령이 호출 가능하여 허가되지 않은 파일의 실행 위험 존재
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000
판단기준	양호 : IIS 5.0 버전에서 해당 레지스트리 값이 0이거나, IIS 6.0 버전 이상인 경우
	취약 : IIS 5.0 버전에서 해당 레지스트리 값이 1인 경우
조치방법	위의 양호 기준에 맞춰 레지스트리 값 설정
점검 및 조치 사례	

• Windows NT(IIS 4.0), 2000(IIS 5.0)

Step 1) 시작> 실행> REGEDIT> HKLM₩SYSTEM₩CurrentControlSet₩Services₩W3SVC ₩Parameters 검색

Step 2) DWORD> SSIEnableCmdDirective 값을 찾아 값을 "0"으로 입력



※ IIS 6.0 이상 버전(windows 2003 이상) 해당 사항 없음

조치 시 영향	일반적인 경우 영향 없음

2.17. IIS WebDAV 비활성화

W-35 (상)	2. 서비스 관리 > IIS WebDAV 비활성화
취약점 개요	
점검내용	• IIS WebDAV 비활성화 여부 점검
점검목적	• WebDAV 서비스를 비활성화 하여, IIS WebDAV에서 발견되는 다수의 인증 우회 취약점을 제거하고자 함
보안위협	• WebDAV가 활성화 되어 있는 경우 IIS에 악의적으로 작성된 HTTP 요청을 이용하여 인증을 우회함으로써 패스워드로 보호된 WebDAV의 자원에 접근(디렉토리 열람, 파일 다운로드 등)이 가능 • WebDAV에 의해 호출된 일부 구성 요소에 매개 변수를 정확하게 점검하지 않는 결함이 존재하여, 이로 인해 버퍼 오버런이 발생 가능
참고	※ WebDAV(Web Distributed Authoring and Versioning): 사용자가 원격 World Wide Web 서버를 이용하여 파일을 수정하거나 처리할 수 있도록 하는 HTTP의 확장 서비스. 웹상의 공동개발을 지원하기 위한 IETF 표준안(RFC 2518)으로써, 원격지 사용자들 간에 인터넷상에서 파일을 공동 편집하고 관리할 수 있도록 함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 다음 중 한 가지라도 해당하는 경우 1. IIS 서비스를 사용하지 않는 경우 2. DisableWebDAV 값이 1로 설정되어 있는 경우 3. Windows NT, 2000은 서비스팩 4 이상이 설치되어 있는 경우 4. Windows 2003, Windows 2008은 WebDAV가 금지 되어 있는 경우
	취약 : 양호 기준에 한 가지라도 해당하지 않는 경우(2003, 2008은 1,4번만)
조치방법	IIS 서비스를 사용하지 않는 경우 IIS 서비스 중지, 사용할 경우 해당 레지스트리 값을 1로 설정함 (Windows NT, 2000 서비스팩 4 이상 양호, Windows 2003, 2008 WebDAV금지 시 양호)
점검 및 조치 사례	
• Windows NT, 2000 Step 1) 시작> 실행> SERVICES.MSC> World Wide Web Publishing Service> 속성 Step 2) 시작 유형 -> 사용 안 함 / 서비스 상태 -> 중지 < IIS를 사용하지만 WebDAV를 사용하지 않는 경우 > 1. 시작> 실행> REGEDIT 실행 2. HKLM₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters 3. 마우스 우클릭> 새로 만들기 DWORD 값을 선택 4. DisableWebDAV 입력 (Default 값인 "0"을 "1"로 변경)	

W-35 (상)	2. 서비스 관리 > IIS WebDAV 비활성화

<IIS를 사용하고, WebDAV도 필요한 경우 >

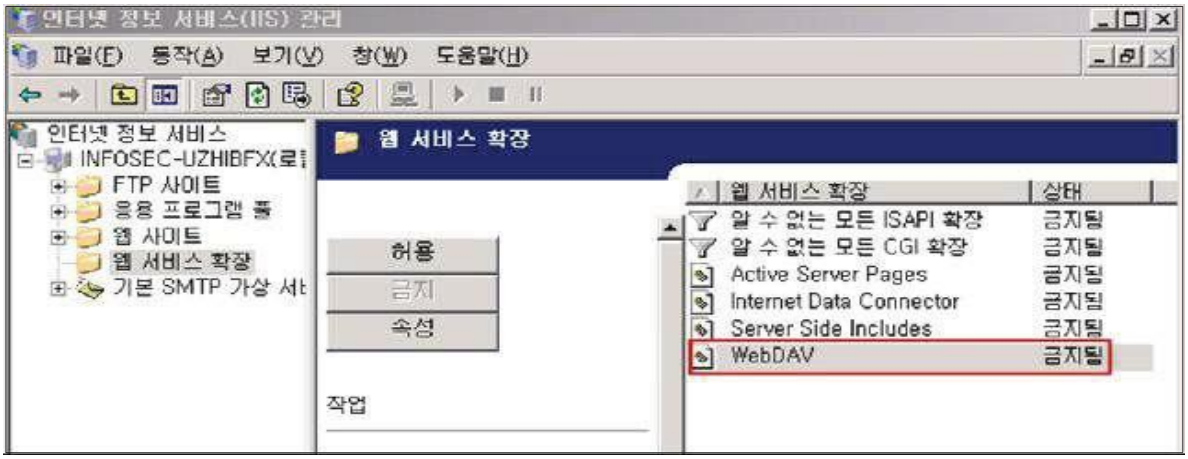
1. Windows NT 인 경우 windows update 실행
2. Windows 2000 서비스팩 버전이 2, 3인 경우 windows update 실행
3. Windows 2000 서비스팩 버전이 4인 경우 - 취약점 없음

※ 시스템 재시작 후 적용됨

- Windows 2003

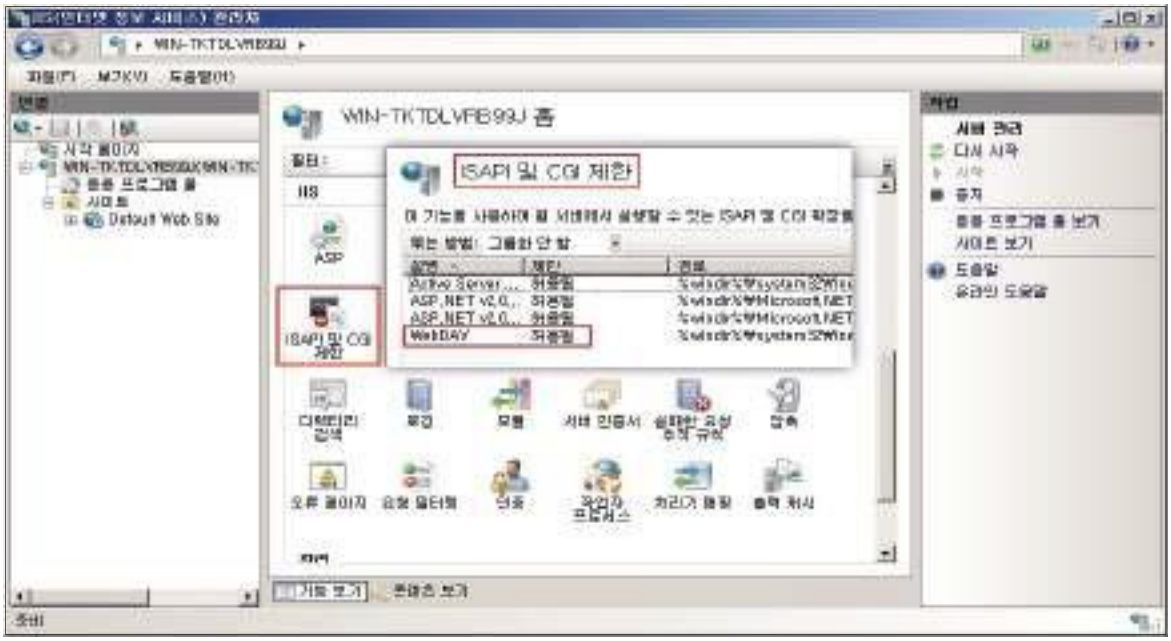
Step 1) 시작> 실행> INETMGR> 웹 사이트> 웹 서비스 확장

Step 2) WebDAV 금지



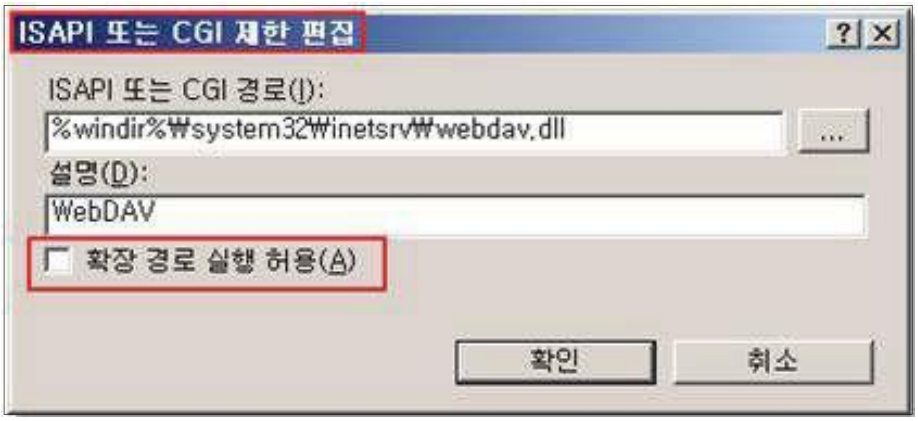
- Windows 2008, 2012

Step 1) 인터넷 정보 서비스(IIS) 관리자> 서버 선택> IIS> "ISAPI 및 CGI 제한" 선택, WebDAV 사용여부 확인 (허용됨일 경우 취약)



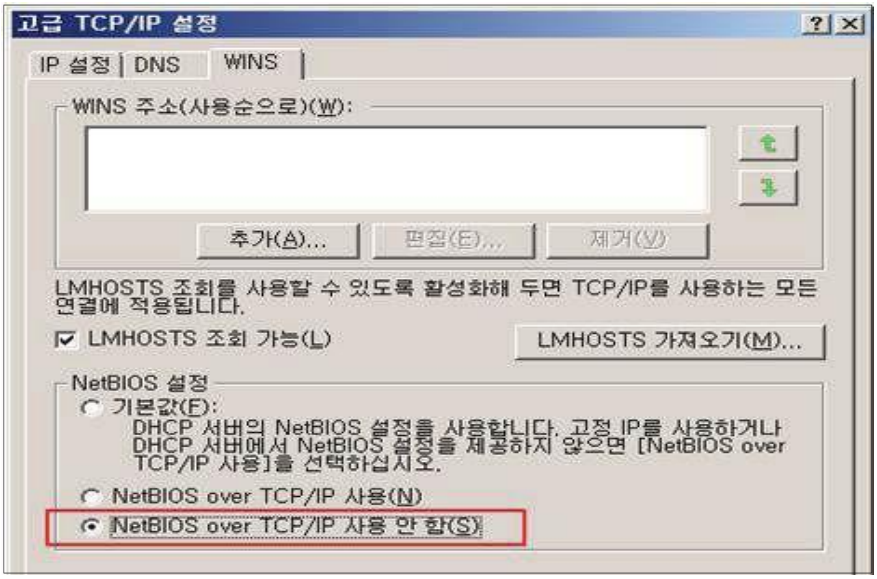
W-35 (상)	2. 서비스 관리 > IIS WebDAV 비활성화

Step 2) 인터넷 정보 서비스(IIS) 관리자> 서버 선택> IIS> "ISAPI 및 CGI 제한" 선택 WebDAV 항목 선택> [작업]에서 제거하거나, 편집> "확장 경로 실행 허용(A)" 체크 해제

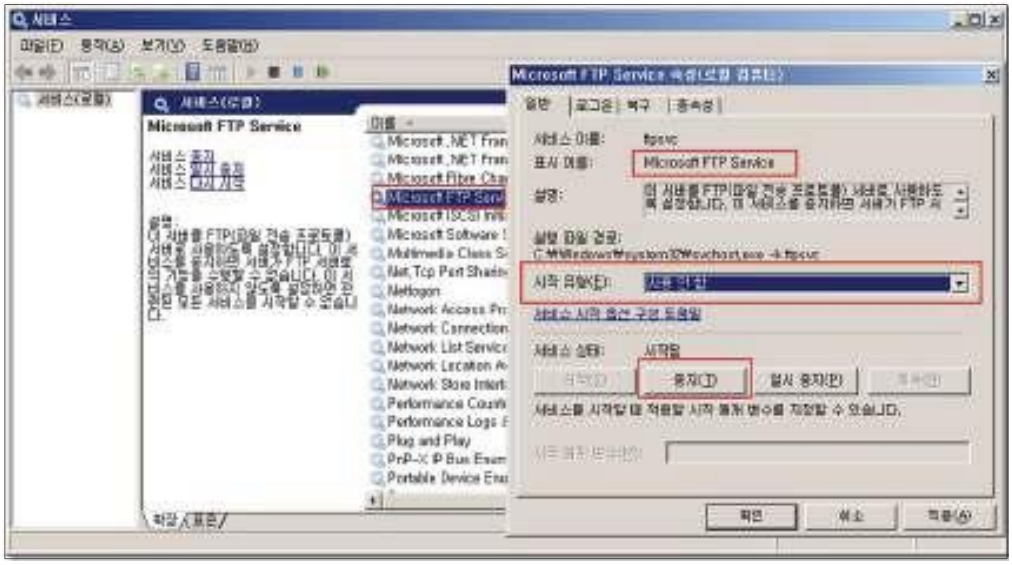


조치 시 영향	일반적인 경우 영향 없음

2.18. NetBIOS 바인딩 서비스 구동 점검

W-36 (상)	2. 서비스 관리 > NetBIOS 바인딩 서비스 구동 점검
취약점 개요	
점검내용	• NetBIOS 바인딩 서비스 구동 여부 점검
점검목적	• NetBIOS와 TCP/IP 바인딩을 제거하여 TCP/IP를 거치게 되는 파일 공유서비스를제공하지 못하도록 하고, 인터넷에서의 공유자원에 대한 접근 시도를 방지하고자 함
보안위협	• 인터넷에 직접 연결되어 있는 윈도우 시스템에서 NetBIOS TCP/IP 바인딩이 활성화 되어 있을 경우 공격자가 네트워크 공유자원을 사용할 우려 존재
참고	※ NetBIOS(Network Basic Input/Output System)는 별개의 컴퓨터상에 있는 애플리케이션들이 근거리통신망 내에서 서로 통신 할 수 있게 해주는 프로그램. IBM pc를 위한 네트워크 인터페이스 체계로 네임, 세션, 데이터그램의 세가지 서비스를 제공하며 NetBIOS를 통해 파일 공유와 프린터 공유 등을 서비스로 이용
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : TCP/IP와 NetBIOS 간의 바인딩이 제거 되어 있는 경우
	취약 : TCP/IP와 NetBIOS 간의 바인딩이 제거 되어있지 않은 경우
조치방법	네트워크 제어판을 이용하여 TCP/IP와 NetBIOS 간의 바인딩(binding) 제거
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 Step 1) 시작> 실행> ncpa.cpl> 로컬 영역 연결> 속성> TCP/IP> [일반] 탭에서 [고급] 클릭> [WINS] 탭에서 TCP/IP에서 "NetBIOS 사용 안 함" 또는, "NetBIOS over TCP/IP 사용 안 함" 선택  	
조치 시 영향	TCP/IP을 거치게 되는 파일 공유 서비스가 제공되지 않음 인터넷에서의 공유 자원에 대한 접근시도가 불가능함 (라우터를 거치지 않은 내부 네트워크에서는 가능함)

2.19. FTP 서비스 구동 점검

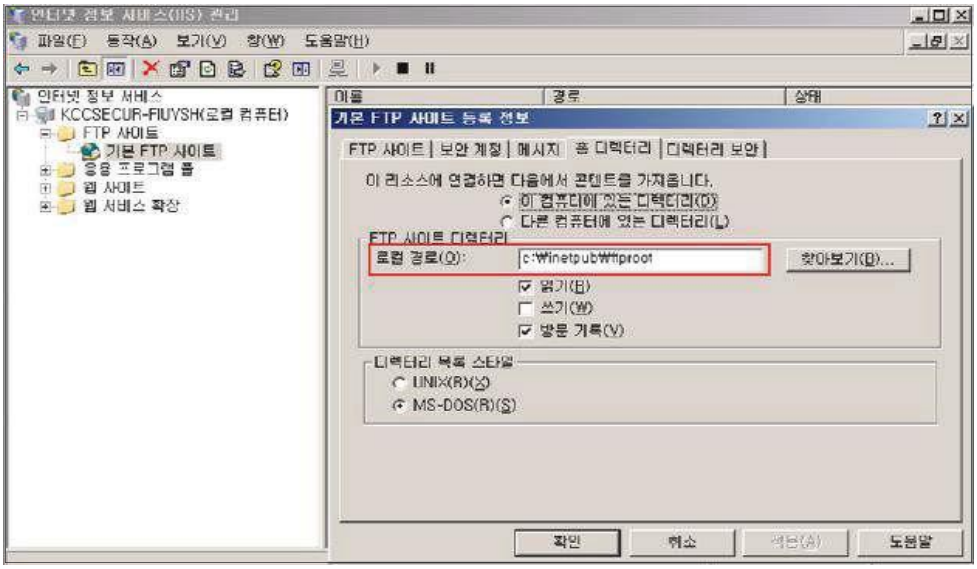
W-37 (상)	2. 서비스 관리 > FTP 서비스 구동 점검
취약점 개요	
점검내용	• 시스템 내 FTP 서비스 구동 여부 점검
점검목적	• 인증 정보가 기본적으로 평문전송 되는 취약한 프로토콜인 FTP의 사용을 제한하여 네트워크 보안성을 높이고자 함
보안위협	• OS에서 제공하는 기본적인 FTP 서비스를 사용할 경우 계정과 패스워드가 암호화 되지 않은 재로 전송 되어 Sniffer에 의한 계정 정보의 노출 위험 존재
참고	※ Sniffer: 네트워크 트래픽을 감시하고 분석하는 프로그램
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : FTP 서비스를 사용하지 않는 경우 또는 secure FTP 서비스를 사용하는 경우
	취약 : FTP 서비스를 사용하는 경우
조치방법	FTP 서비스가 필요하지 않다면 서비스 중지 또는 secure FTP 응용프로그램 사용
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 Step 1) 시작> 실행> SERVICES.MSC> FTP Publishing Service> 속성> [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, FTP 서비스 중지 	
조치 시 영향	일반적인 경우 영향 없음

2.20. FTP 디렉토리 접근권한 설정

W-38 (상)	2. 서비스 관리 > FTP 디렉토리 접근권한 설정
취약점 개요	
점검내용	• FTP 홈디렉토리의 접근 권한 적절성 점검
점검목적	• FTP 서비스 디렉토리의 접근 권한을 적절하게 설정하여 의도지 않은 정보유출 등의 보안 사고를 방지하고자 함
보안위협	• FTP 홈디렉토리에 과도한 권한(예. Everyone Full Control)이 부여된 경우 임의의 사용자가 쓰기, 수정이 가능하여 정보유출, 파일 위·변조 등의 위험 존재
참고	※ 기반시설 시스템은 FTP 서비스를 사용하지 않는 것이 원칙이나, 조직 내에서 해당 서비스를 부득이 사용해야 하는 경우 관련 보호 대책을 수립 및 적용하여 활용하여야 함 ※ 관련 점검 항목 : W-27(상), W-28(상)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : FTP 홈 디렉토리에 Everyone 권한이 없는 경우
	취약 : FTP 홈 디렉토리에 Everyone 권한이 있는 경우
조치방법	FTP 홈 디렉토리에서 Everyone 권한 삭제, 각 사용자에게 적절한 권한 부여
점검 및 조치 사례	

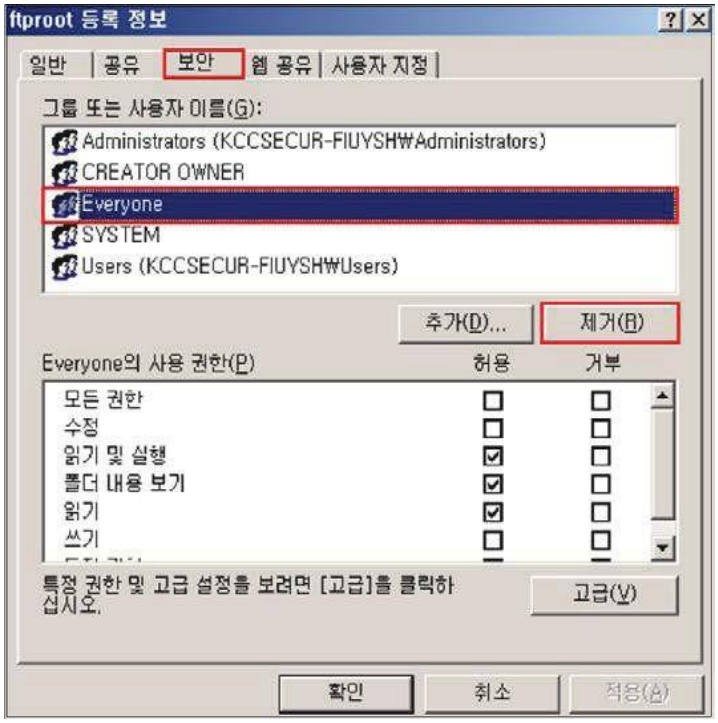
• Windows NT(IIS 4.0), 2000(IIS 5.0), 2003(IIS 6.0)

Step 1) 인터넷 정보 서비스(IIS) 관리> FTP 사이트> 해당 FTP 사이트> 속성> [홈 디렉토리] 탭에서 FTP 홈 디렉토리 확인



Step 2) 탐색기> 홈 디렉토리> 속성> [보안]탭에서 Everyone 권한 제거

W-38 (상)	2. 서비스 관리 > FTP 디렉토리 접근권한 설정



- Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 마우스 우클릭> FTP 게시 추가
Step 2) 이후 진행 과정에서 권한 부여 화면의 액세스 허용 대상 선정 시 [지정한 사용자] 만 선택

※ IIS 7 이상 버전에서는 FTP 사이트를 별도로 생성하지 않고 기존 웹 사이트에 FTP 사이트를 바인딩 하여 사용함. (관리 도구> 인터넷 정보 서비스(IIS) 6.0 관리자에서 FTP 설정 가능)

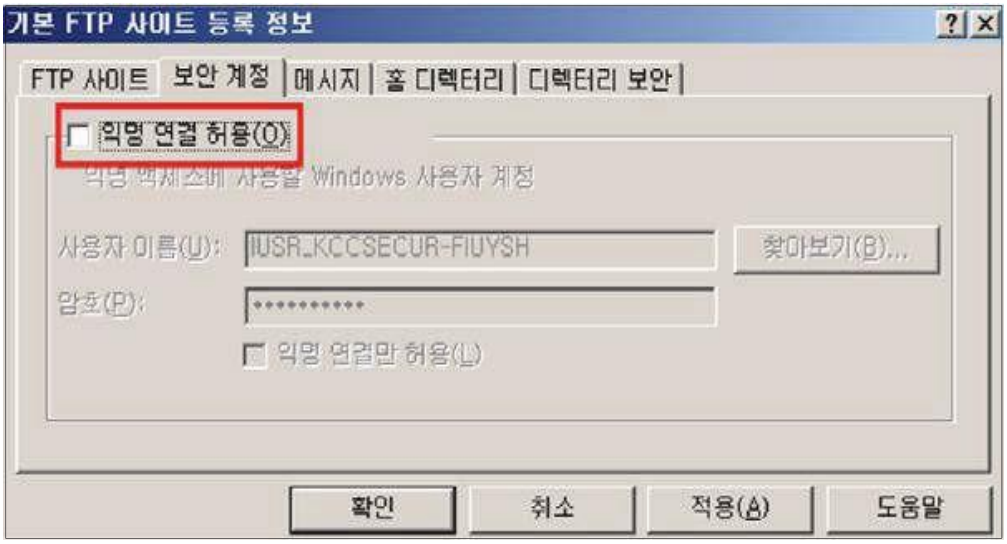
조치 시 영향	일반적인 경우 영향 없음

2.21. Anonymouse FTP 금지

W-39 (상)	2. 서비스 관리 > Anonymous FTP 금지
취약점 개요	
점검내용	• FTP 서비스의 Anonymous(익명) 접속 허용 여부 점검
점검목적	• FTP 익명 접속을 제한하여, 중요 정보의 불법 유출을 차단 하고자 함
보안위협	• FTP 익명 접속이 허용된 경우 핵심 기밀 자료나 내부 정보의 불법 유출 가능성이 존재함
참고	※ 만약 익명 접속이 허용된 FTP 서버에 익명 사용자에 대해 쓰기 권한이 부여된 경우, 정상적으로 업로드한 파일들의 변조가 가능하므로 공개한 디렉토리 내 중요 데이터가 보관되어 있는지 여부를 추가적으로 확인하여야 함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : FTP 서비스를 사용하지 않거나, "익명 연결 허용"이 체크되지 않은 경우
	취약 : FTP 서비스를 사용하거나, "익명 연결 허용"이 체크되어 있는 경우
조치방법	FTP 서비스를 사용하지 않는 경우 서비스 중지, 사용할 경우 "익명 연결 허용" 체크 해제 또는 "익명" 체크 해제
점검 및 조치 사례	

• Windows NT(IIS 4.0), 2000(IIS 5.0), 2003(IIS 6.0)

Step 1) 인터넷 정보 서비스(IIS) 관리> FTP 사이트> 속성> [보안 계정] 탭에서 "익명 연결 허용" 체크박스 해제 (만약 개별 FTP 사이트에 적용할 경우 해당 사이트에만 설정이 적용되고, 기본 설정은 적용 받지 않음)

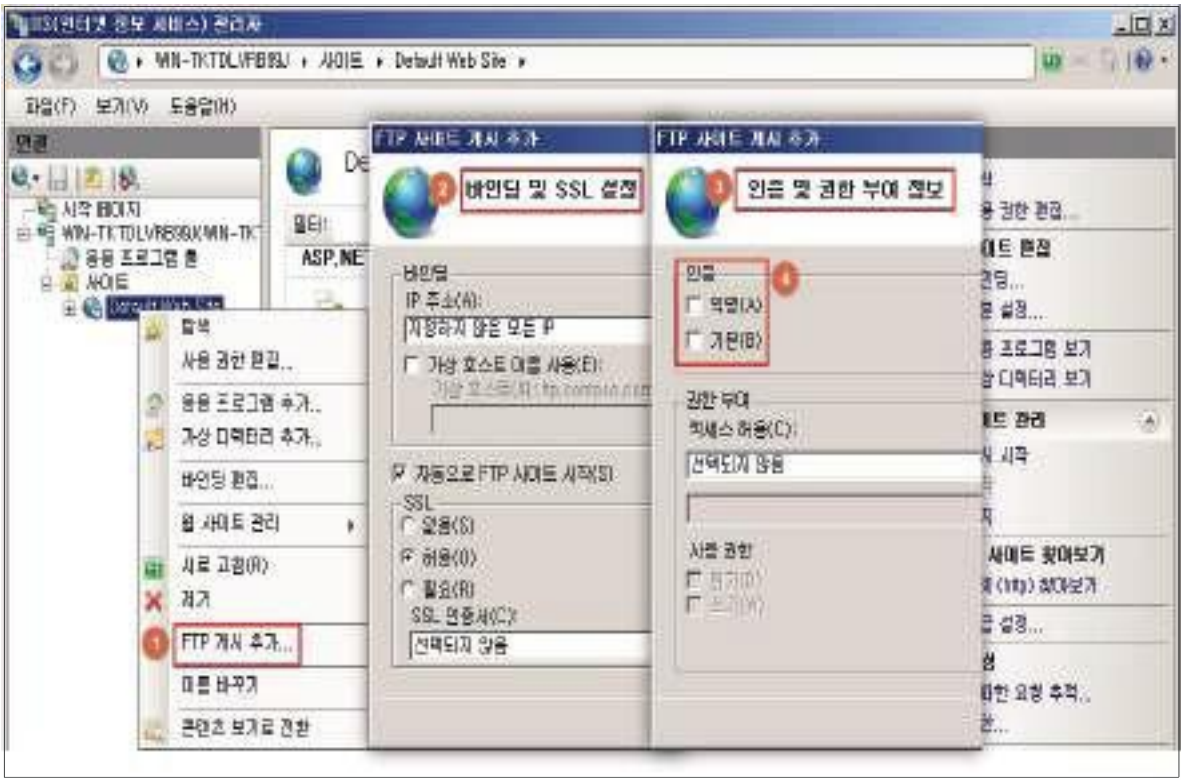


W-39 (상)	2. 서비스 관리 > Anonymous FTP 금지

- Windows 2008(IIS 7.0), 2012(IIS 8.0)

Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> 마우스 우클릭> FTP 게시 추가

Step 2) 이후 진행 과정에서 인증 화면의 익명 체크 박스 해제



※ IIS 7 이상 버전에서는 FTP 사이트를 별도로 생성하지 않고 기존 웹 사이트에 FTP 사이트를 바인딩 하여 사용함. (관리 도구> 인터넷 정보 서비스(IIS) 6.0 관리자에서 FTP 설정 가능)

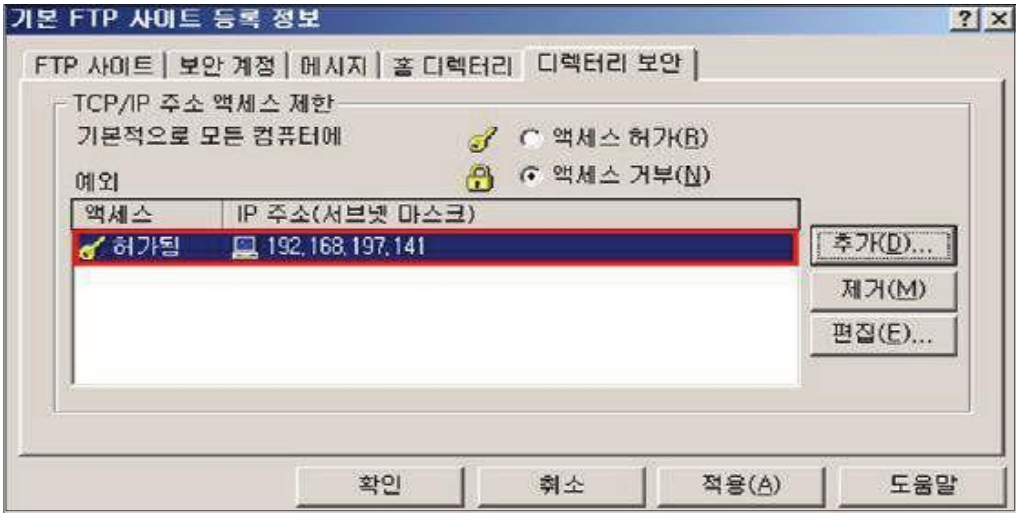
조치 시 영향	애플리케이션에서 익명 연결을 사용할 경우를 제외하고, 일반적으로 영향 없음

2.22. FTP 접근 제어 설정

W-40 (상)	2. 서비스 관리 > FTP 접근 제어 설정
취약점 개요	
점검내용	• FTP 접속 가능한 IP 주소 지정 여부 점검
점검목적	• FTP 접근 시 특정 IP 주소에 대해 콘텐츠 액세스를 허용하여 서비스 보안성을 강화하고자 함
보안위협	• FTP 프로토콜은 로그온에 지정된 자격 증명이나 데이터 자체가 암호화 되지 않고 모든 자격 증명을 일반 텍스트로 네트워크를 통해 전송되는 특성상 서버 클라이언트간 트래픽 스니핑을 통해 인증정보가 쉽게 노출되므로 접속 허용된 사용자 IP를 지정하여 접속자를 제한할 것을 권고
참고	※ 기반시설 시스템은 FTP 서비스를 사용하지 않는 것이 원칙이나, 조직 내에서 해당 서비스를 부득이 사용해야 하는 경우 관련 보호 대책을 수립 및 적용하여 활용하여야 함 ※ 관련 점검 항목 : W-38(상), W-39(상)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 특정 IP 주소에서만 FTP 서버에 접속하도록 접근제어 설정을 적용한 경우
	취약 : 특정 IP 주소에서만 FTP 서버에 접속하도록 접근제어 설정을 적용하지 않은 경우 ※ 조치 시 마스터 속성과 모든 사이트에 적용함
조치방법	특정 IP 주소에서만 FTP 서버에 접속하도록 접근제어 설정
점검 및 조치 사례	

• Windows NT(IIS 4.0), 2000(IIS 5.0), 2003(IIS 6.0)

Step 1) 인터넷 정보 서비스(IIS) 관리> FTP 사이트> 속성> [디렉토리 보안] 탭에서 "액세스 거부" 선택 후 접근 가능 IP 주소 추가 (만약 개별 FTP 사이트에 적용할 경우 해당 사이트에만 설정이 적용되고, 기본 설정은 적용 받지 않음)



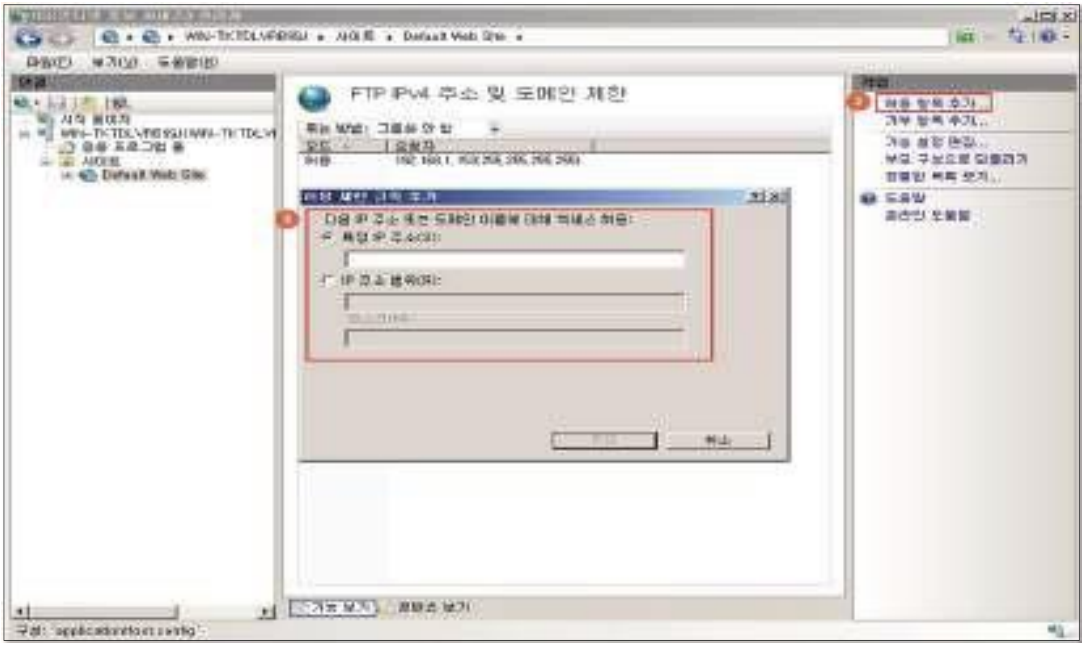
W-40 (상)	2. 서비스 관리 > FTP 접근 제어 설정

[참고] 액세스 허가: 모든 액세스를 허용 후 액세스를 거부할 컴퓨터, 그룹, 도메인 추가
액세스 거부: 모든 액세스를 거부 후 액세스를 허용할 컴퓨터, 그룹, 도메인 추가

- Windows 2008(IIS 7.0), 2012(IIS 8.0)

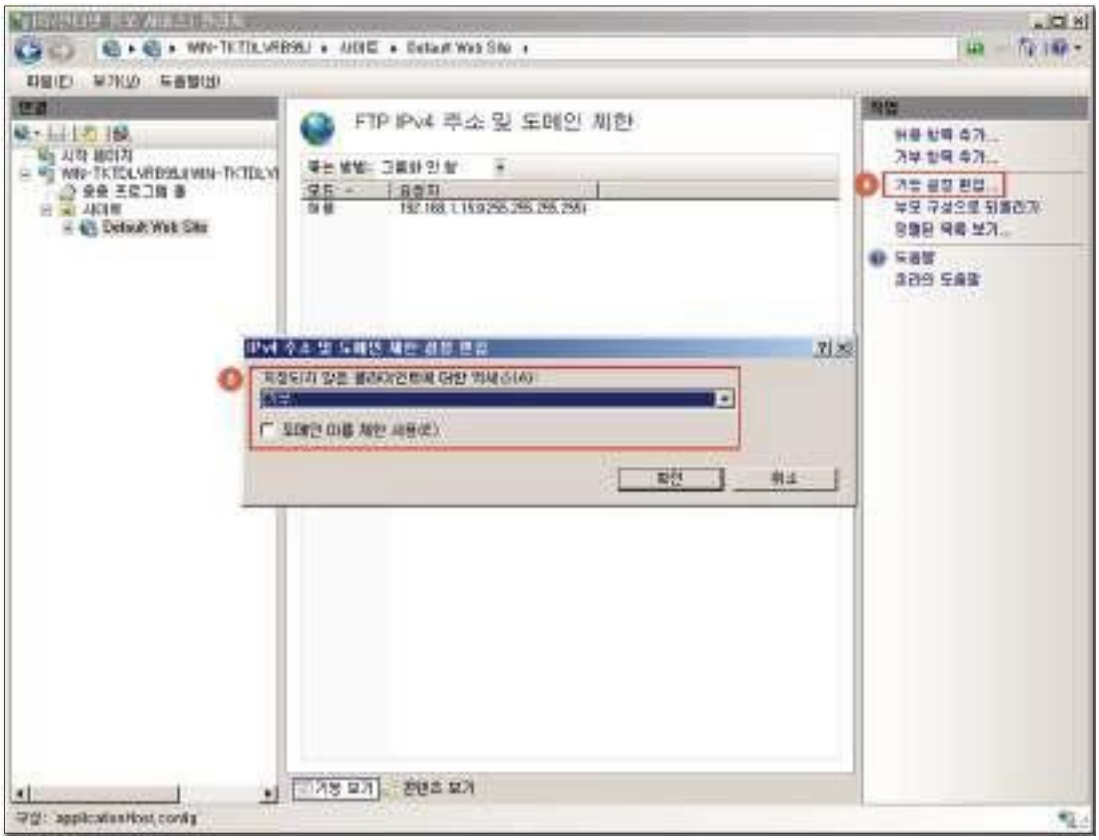
Step 1) 제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리> 해당 웹사이트> FTP IPv4 주소 및 도메인 제한

Step 2) [작업]의 허용 항목 추가에서 FTP 접속을 허용할 IP 입력



W-40 (상)	2. 서비스 관리 > FTP 접근 제어 설정

Step 3) [작업] 의 기능 설정 편집에서 지정되지 않은 클라이언트에 대한 액세스를 거부 선택



※ IIS 7 이상 버전에서는 FTP 사이트를 별도로 생성하지 않고 기존 웹 사이트에 FTP 사이트를 바인딩 하여 사용함. (관리 도구> 인터넷 정보 서비스(IIS) 6.0 관리자에서 FTP 설정 가능)

조치 시 영향	일반적인 경우 영향 없음

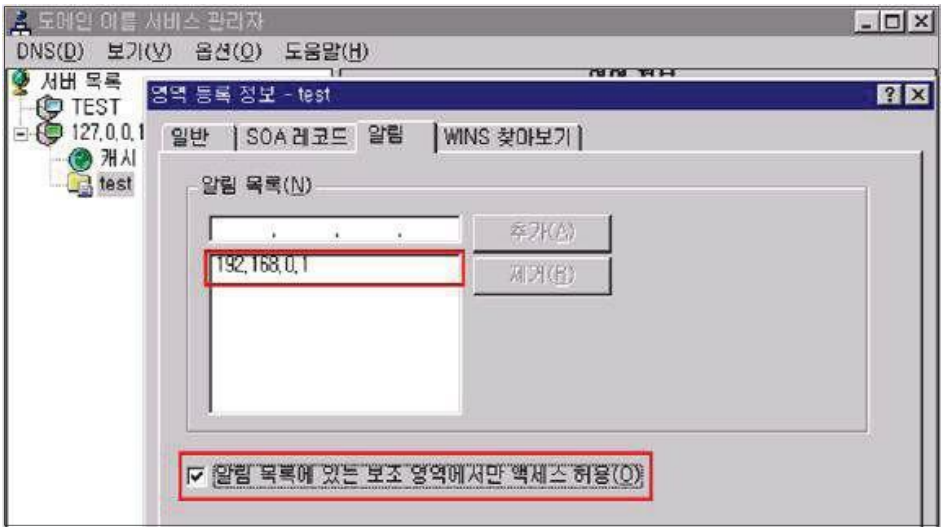
2.23. DNS Zone Transfer 설정

W-41 (상)	2. 서비스 관리 > DNS Zone Transfer 설정
취약점 개요	
점검내용	• DNS Zone Transfer 차단 설정 여부 점검
점검목적	• DNS Zone Transfer 차단 설정을 적용하여 도메인 정보의 불법 외부 유출을 막고자 함
보안위협	• DNS Zone Transfer 차단 설정이 적용되지 않은 경우 DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS 서버가 아닌 외부로 유출 위험 존재
참고	※ zone-transfer: zone(영역) 전송이라고 하며 master와 slave간에 또는 primary와 secondary DNS간에 zone 파일을 동기화하기 위한 용도로 사용되는 기술
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 아래 기준에 해당될 경우 1. DNS 서비스를 사용 않는 경우 2. 영역 전송 허용을 하지 않는 경우 3. 특정 서버로만 설정이 되어 있는 경우
	취약 : 위 3개 기준 중 하나라도 해당 되지 않는 경우
조치방법	불필요 시 서비스 중지/사용 안 함, 사용하는 경우 영역 전송을 특정 서버로 제한하거나 "영역 전송 허용"에 체크 해제
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 프로그램> 관리 도구> DNS 관리자> 각 조회 영역> 해당 영역> 등록 정보> 알림

Step 2) "알림 목록에 있는 보조 영역에서만 액세스 허용" 선택 후 서버 IP 추가

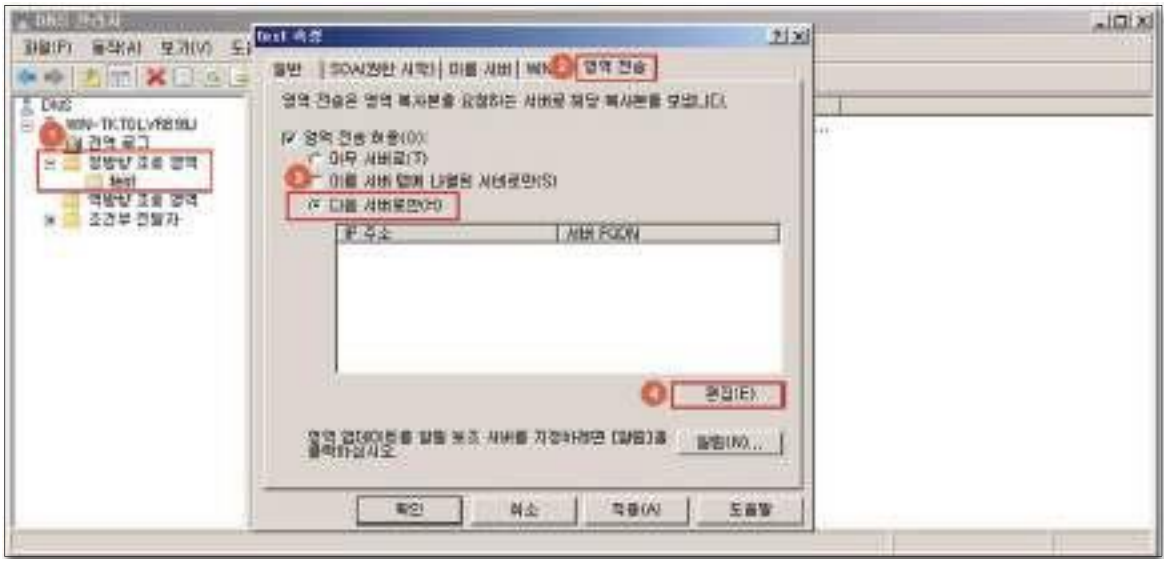


W-41 (상)	2. 서비스 관리 > DNS Zone Transfer 설정

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> DNSMGMT.MSC> 각 조회 영역> 해당 영역> 속성> 영역 전송

Step 2) "다음 서버로만" 선택 후 전송할 서버 IP 추가



Step 3) 불필요 시 해당 서비스 제거

시작> 실행> SERVICES.MSC> DNS 서버> 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, DNS 서비스 중지

조치 시 영향	영역 전송할 경우 서버를 지정해 주면 영향 없음

2.24. RDS(RemoteDataServices)제거

W-42 (상)	2. 서비스 관리 > RDS(Remote Data Services)제거
취약점 개요	
점검내용	• RDS(Remonte Data Services) 비활성화 여부 점검
점검목적	• 취약한 RDS 서비스를 제거하여 불법적인 원격 공격을 차단하기 위함
보안위협	• 취약한 플랫폼의 RDS가 사용되는 경우 서비스 거부 공격이나 원격에서 관리자 권한으로 임의의 명령을 실행할 수 있는 위험이 존재함
참고	※ MDAC 2.7 미만의 버전에서 웹 서버와 웹 클라이언트는 모두 이 취약점으로 인해 위험해질 수 있으므로 RDS가 불필요할 경우 제거하는 것이 안전함 ※ RDS(Remote Data Services): MDAC(Microsoft Data Access Components)의 한 컴포넌트로 클라이언트에 있는 데이터를 다룰 수 있도록 하는 서비스
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 다음 중 한 가지라도 해당되는 경우(2008 이상 양호) 1. IIS를 사용하지 않는 경우 2. Windows 2000 서비스팩 4, Windows 2003 서비스팩 2 이상 설치되어 있는 경우 3. 디폴트 웹 사이트에 MSADC 가상 디렉토리가 존재하지 않는 경우 4. 해당 레지스트리 값이 존재하지 않는 경우
	취약 : 양호 기준에 한 가지도 해당되지 않는 경우
조치방법	사용하지 않는 경우 IIS 서비스 중지/사용 안 함, 사용할 경우 레지스트리 키 값 제거 또는 관련 패치 적용
점검 및 조치 사례	
• Windows NT, 2000, 2003 < RDS 제거 방법 > Step 1) 웹 사이트로부터 "/msadc" 가상 디렉토리 제거 시작> 실행> INETMGR> 웹 사이트 선택 후 오른쪽 디렉토리에서 msadc 제거 Step 2) 다음의 레지스트리 키/디렉토리 제거 HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters₩ADCLaunch₩RDSServer.DataFactory HKEY_LOCAL_MACHMINE₩SYSTEM ₩CurrentControlSet₩Services₩W3SVC₩Parameters₩ADCLaunch₩AdvancedDataFactory HKEY_LOCAL_MACHINE₩SYSTEM₩CurrentControlSet₩Services₩W3SVC₩Parameters₩ADCLaunch₩VbBusObJ.VbBusObJCls	
조치 시 영향	WAS와 연동될 경우 일부 RDS를 사용하는 경우가 있으며 사용할 경우 레지스트리 키 값 제거

2.25. 최신 서비스팩 적용

W-43 (상)	2. 서비스 관리 > 최신 서비스팩 적용
취약점 개요	
점검내용	• 최신 서비스팩 적용 여부 점검
점검목적	• 시스템을 최신 버전으로 유지하여 새로운 위협 및 진행 중인 위협으로부터 중요 정보와 시스템을 보호하기 위함
보안위협	• 보안 업데이트를 적용하지 않은 경우 시스템 및 응용프로그램의 취약성으로 인해 권한 상승, 원격 코드 실행, 보안 기능 우회 등의 문제를 일으킬 수 있음
참고	※ 서비스팩: Windows의 안정성을 높이기 위해 응용프로그램, 서비스, 실행 파일 등 여러 수정 파일들을 모아 놓은 업데이트 프로그램
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 최신 서비스팩이 설치되어 있으며 적용 절차 및 방법이 수립된 경우
	취약 : 최신 서비스팩이 설치되지 않거나, 적용 절차 및 방법이 수립되지 않은 경우
조치방법	설치에 따른 영향도 확인 후 최신 서비스팩 설치(설치 후 시스템 재시작 필요)
점검 및 조치 사례	

• Windows NT, 2000, 2003, 2008, 2012

Step 1) 시작> 실행> Winver

Step 2) 서비스팩 버전 확인 후 최신 버전이 아닌 경우 아래 사이트에서 최신 서비스팩 다운로드 후 설치 또는 자동업데이트 활용

※ 인터넷 립(Worm)이 Windows의 취약점을 이용하여 공격하기 때문에 서비스팩 설치 시에는 네트워크와 분리된 상태에서 설치 할 것을 권장

[최신 서비스팩 정보(2015년 12월 기준)]

운영체제 종류	최신 서비스팩	서비스 제공 여부
Windows NT	Service pack 6a	중단
Windows Server 2000	Service pack 4	중단
Windows Server 2003	Service pack 2	중단
Windows Server 2008	2008: Service pack 2 R2: Service pack 1	제공
Windows Server 2012	2012: 없음 R2: 없음	제공

※ Windows Server 2003이하 버전의 경우 현재(2015년 12월 기준) 공식적인 서비스 제공이 중단되어 조직에서 2003 이하 버전의 시스템을 사용하는 것은 적절하지 않음

[보안 패치 사이트(2015년 12월 기준)]

Microsoft Windows Server 제품별 지원

https://technet.microsoft.com/ko-kr/library/bb625087.aspx

조치 시 영향	설치 후 시스템 재시작이 필요하며 설치에 따른 영향 정도를 확인하여야 함

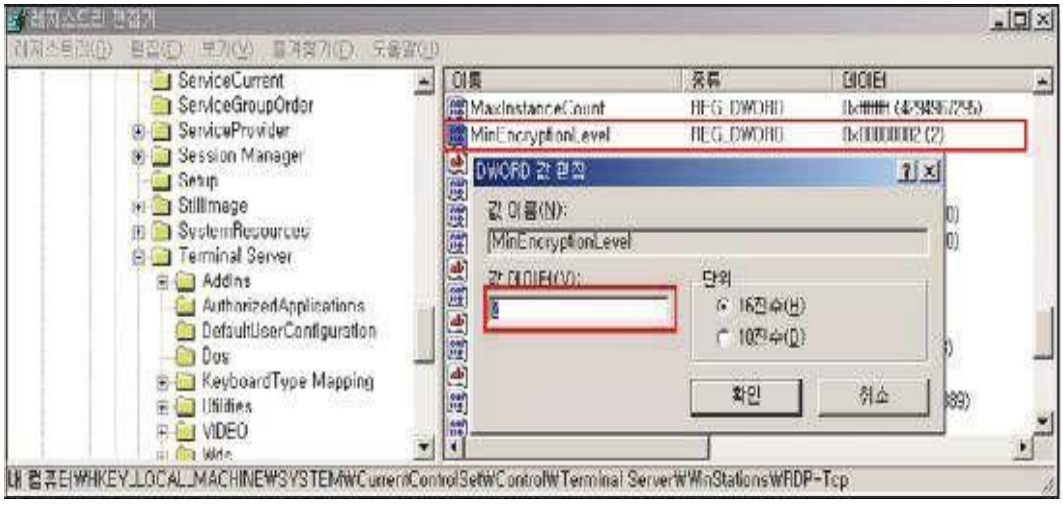
2.26. 터미널 서비스 암호화 수준 변경

W-44 (중)	2. 서비스 관리 > 터미널 서비스 암호화 수준 설정
취약점 개요	
점검내용	• 터미널 서비스 암호화 수준 적절성 점검
점검목적	• 터미널 서비스 암호화 설정으로 데이터를 암호화하여 클라이언트와 서버간의 통신에서 전송되는 데이터를 보호하기 위함
보안위협	• 서버 접속 시에 낮은 암호화 수준을 적용할 경우 악의적인 사용자에 의해 서버와 클라이언트간 주고받는 정보가 노출될 우려가 있음
참고	※ 기반시설 시스템은 터미널 서비스의 사용을 원칙적으로 금지하나, 부득이 해당 서비스를 사용해야 하는 경우 클라이언트 서버간의 데이터 전송 시 암호화하여 보호해야 함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 터미널 서비스를 사용하지 않거나 사용 시 암호화 수준을 "클라이언트와 호환 가능(중간)" 이상으로 설정한 경우
	취약 : 터미널 서비스를 사용하고 암호화 수준이 "낮음" 으로 설정한 경우
조치방법	터미널 서비스의 가동을 '중지' 및 '사용 안 함' 설정을 하거나, 부득이 사용할 경우 암호화 수준 설정 적용
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 실행> regedit

Step 2) HKLM₩SYSTEM₩CurrentControlSet₩Control₩Terminal Server₩WinStations₩RDP-Tcp ₩MinEncryptionLevel 값을 2(중간) 이상으로 설정



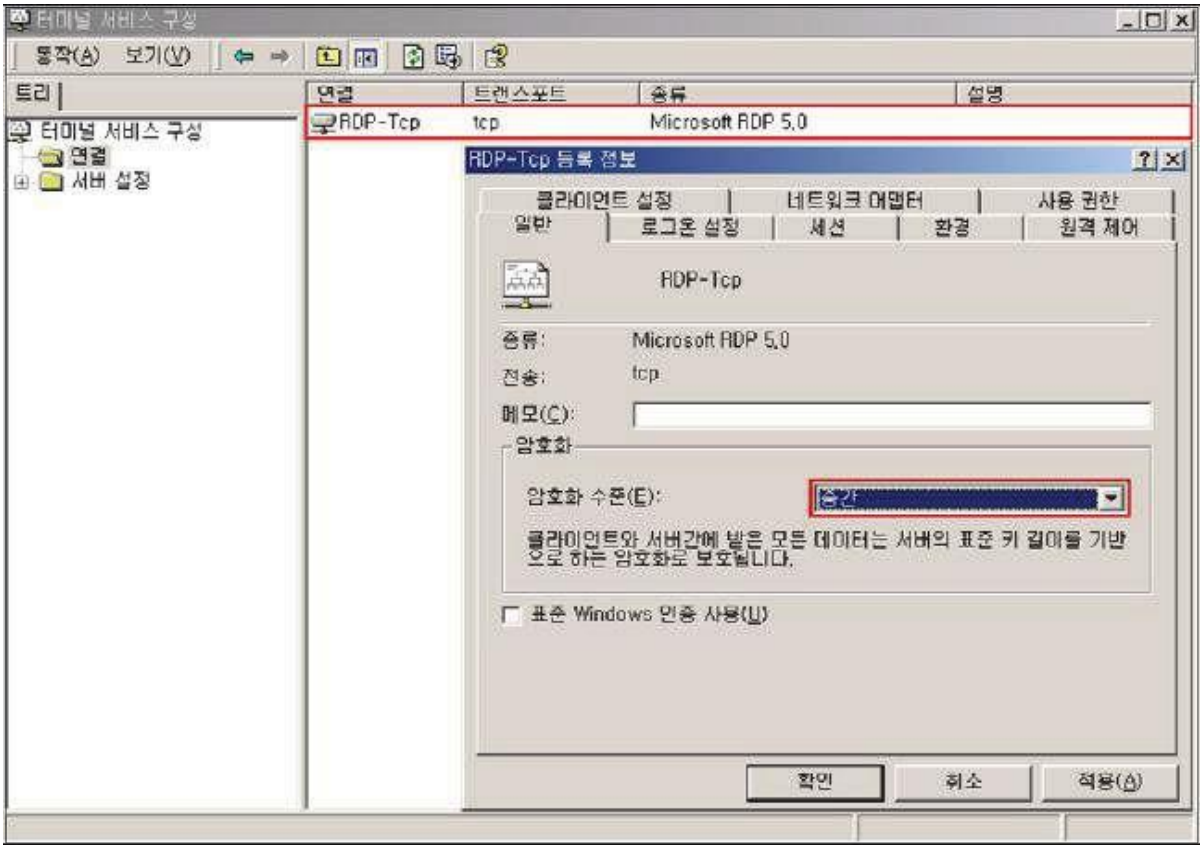
W-44 (중)	2. 서비스 관리 > 터미널 서비스 암호화 수준 설정

- Windows 2000

Step 1) 시작> 실행> TSCC.MSC> "해당 서비스" 선택> 속성

Step 2) 암호화 수준 -+ 중간(Windows 2000) 이상으로 설정

암호화 수준	설 명
낮음	클라이언트에서 서버로 보낸 데이터만 서버의 표준 키 길이를 기반으로 하는 암호화로 보호. 서버가 클라이언트로 보낸 데이터는 보호되지 않음
증간	클라이언트와 서버 간에 받은 모든 데이터는 서버의 표준 키 길이를 기반으로 암호화로 보호
높음	클라이언트와 서버 간에 받은 모든 데이터는 서버의 최대 키 길이를 기반으로 암호화로 보호



- Windows 2003, 2008, 2012

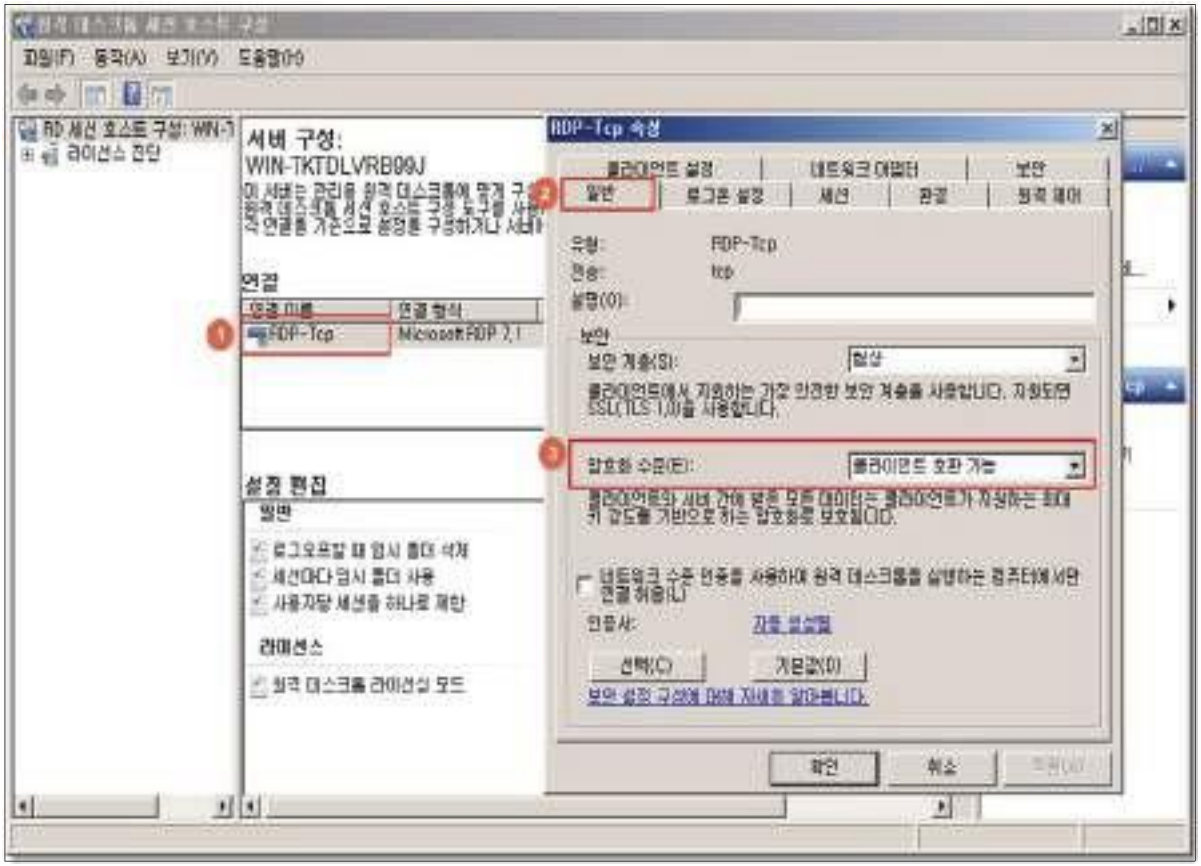
Step 1) Windows 2003: 시작> 실행> TSCC.MSC> "해당 서비스" 선택> 속성

Windows 2008, 2012: 시작> 관리 도구> 원격 데스크톱 서비스> 원격 데스크톱 세션 호스트 구성> RDP-Tcp 속성

Step 2) [일반] 탭에서 암호화 수준 설정 -+ 클라이언트 호환 가능(Windows 2003, 2008, 2012)

W-44 (중)	2. 서비스 관리 > 터미널 서비스 암호화 수준 설정

암호화 수준	설 명
낮음	클라이언트에서 서버로 보내는 모든 데이터는 클라이언트가 지원하는 최대 키 강도를 기반으로 하는 암호화로 보호
클라이언트 호환 가능	클라이언트와 서버 간에 받은 모든 데이터는 클라이언트가 지원하는 최대 키 강도를 기반으로 하는 암호화로 보호
높음	클라이언트와 서버 간에 받은 모든 데이터는 서버의 최대 키 강도를 기반으로 하는 암호화로 보호하며 이 암호화 수준을 지원 하지 않는 클라이언트는 연결할 수 없음
FIS 규격	클라이언트에서 서버로 보내는 모든 데이터를 Federal Information Processing Standard 140-1 유효 암호화 방법을 사용하여 보호



※ 터미널 서비스가 필요한 경우 추가 보완 대책

1. 관리자 이외의 일반 사용자의 터미널 서비스 접속을 허용하지 않음
2. 방화벽에서 터미널 서비스 포트(3389)의 사용을 관리자 컴퓨터의 IP로 제한

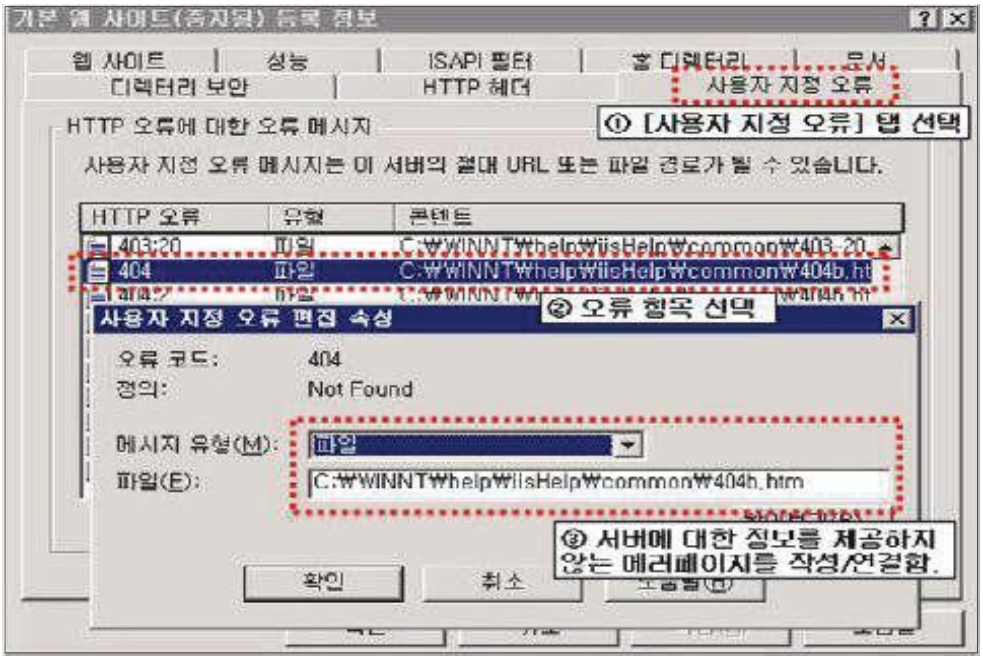
조치 시 영향	암호화 수준 변경 시 일반적으로 영향 없음

2.27. IIS 웹 서비스 정보 숨김

W-45 (중)	2. 서비스 관리 > IIS 웹서비스 정보 숨김
취약점 개요	
점검내용	• IIS 웹서비스 정보 숨김 설정 여부 점검
점검목적	• IIS 웹서비스 운용 시 에러 페이지, 웹 서버 종류, 사용 OS, 사용자 계정이름 등 웹 서버와 관련된 불필요한 정보가 노출되지 않도록 하기 위함
보안위협	• IIS 웹서비스 정보 숨김 설정이 적용되지 않은 경우 악의적인 사용자에게 불필요한 정보가 노출되어 외부 공격을 위한 기초 자료로 이용될 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 웹 서비스 에러 페이지가 별도로 지정되어 있는 경우
	취약 : 웹 서비스 에러 페이지가 별도로 지정되지 않아 에러 발생 시 중요 정보가 노출되는 경우
조치방법	발생 가능한 각 에러에 대한 별도의 웹 서비스 에러 페이지를 지정함
점검 및 조치 사례	

• Windows NT, 2000, 2003

Step 1) 인터넷 정보 서비스(IIS) 관리> 속성> [사용자 지정 오류] 탭에서 400, 401, 403, 404, 500 등 웹 서비스 에러에 대해 별도의 페이지를 지정

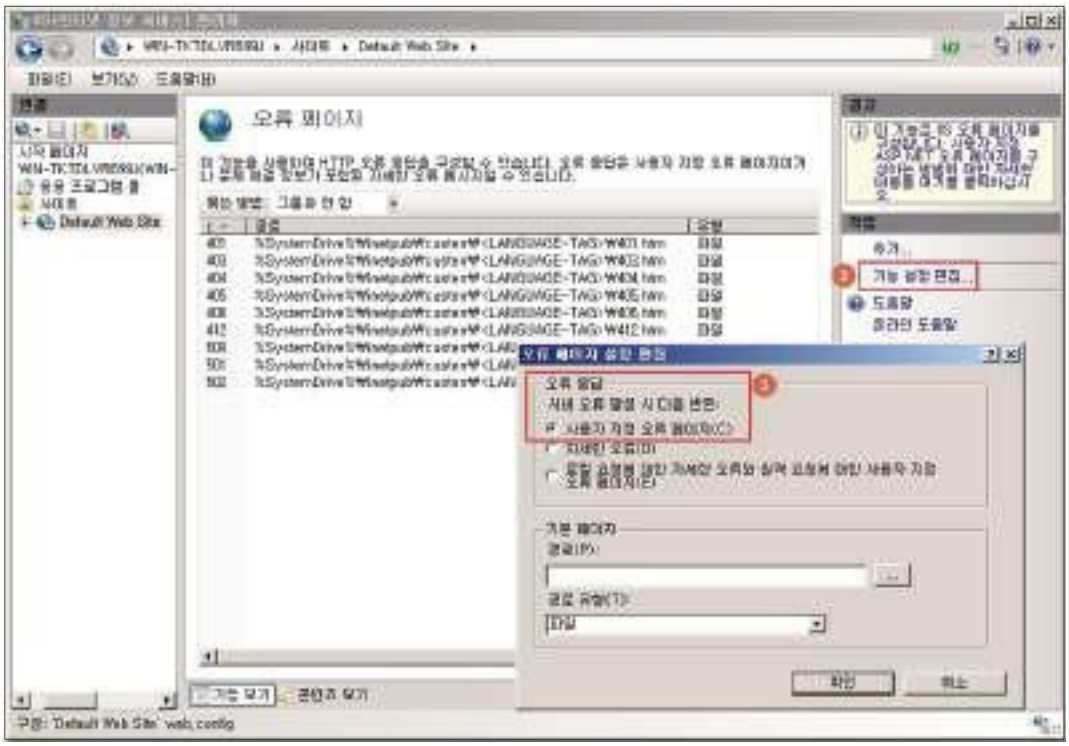


W-45 (중)	2. 서비스 관리 > IIS 웹서비스 정보 숨김

- Windows 2008, 2012

Step 1) 오류 페이지 설정 편집

제어판> 관리도구> 인터넷 정보 서비스(IIS) 관리자> 해당 웹 사이트> [오류 페이지] > [작업] 탭에서 [기능 설정 편집]> "서버오류 발생 시 다음 반환" 항목을 "사용자 지정 오류 페이지"로 설정



조치 시 영향	일반적인 경우 영향 없음

2.28. SNMP 서비스 구동 점검

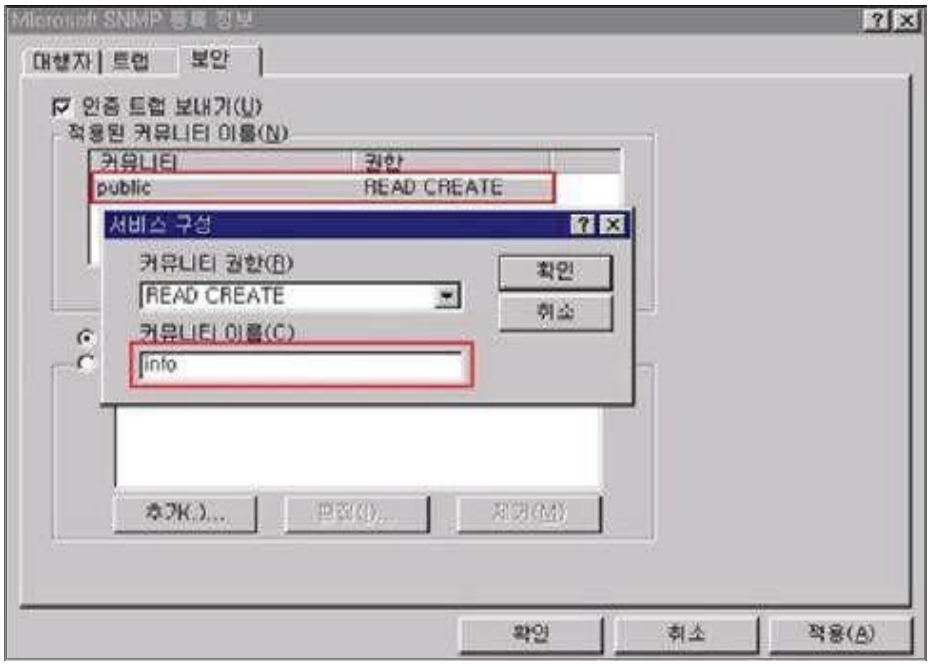
W-46 (중)	2. 서비스 관리 > SNMP 서비스 구동 점검
취약점 개요	
점검내용	• SNMP 서비스 구동 여부 점검
점검목적	• 취약한 SNMP 서비스를 비활성화 하여 시스템의 주요정보 유출 및 불법수정을 방지하기 위함
보안위협	• 취약한 SNMP 서비스를 사용하는 경우 서비스거부공격(DoS, DDoS), 버퍼 오버플로우, 비인가 접속 등의 공격의 위험이 있음
참고	※ SNMP: SNMP(Simple Network Management Protocol)는 MIB(Management Information Base)에 기반한 네트워크 망을 관리하기 위한 목적으로 만들어진 프로토콜로, 간단한 명령으로 원격 시스템의 CPU정보에서부터, 인터페이스 트래픽량 등 여러 가지 정보를 확인 가능
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : SNMP 서비스를 사용하지 않는 경우
	취약 : SNMP 서비스를 사용하는 경우
조치방법	불필요 시 서비스 중지/사용 안 함
점검 및 조치 사례	
• Windows 2000, 2003, 2008, 2012 Step 1) 불필요 시 해당 서비스 제거 시작> 실행> SERVICES.MSC> SNMP Service> 속성에서 "시작 유형"을 "사용 안함"으로 설정한 후, SNMP 서비스를 중지함 	
조치 시 영향	NMS 또는, 별도의 툴에서 SNMP 서비스를 이용하여 서버를 모니터링 하는 경우, 통신하고자 하는 Server/Client에 모두 같은 Community String을 사용하여야 함(서비스> SNMP> 등록 정보> 종속성 참고) ※ NMS(Network Management System): 네트워크 관리 시스템

2.29. SNMP 서비스 커뮤니티스트링의 복잡성 설정

W-47 (중)	2. 서비스 관리 > SNMP 서비스 커뮤니티스트링의 복잡성 설정
취약점 개요	
점검내용	• SNMP 서비스 커뮤니티 스트링(Community String) 적절성 점검
점검목적	• SNMP에서 일종의 패스워드로 사용하는 Community String을 유지할 수 없는 복잡한 값으로 변경하여 불필요한 시스템 정보 노출을 차단하기 위함
보안위협	• Community String 설정을 변경하지 않고 public, private 등 Default 설정 값으로 사용하는 경우, 기본 String 값을 통한 시스템의 주요 정보 및 설정 상태의 비인가자 노출 위험이 존재
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : SNMP 서비스를 사용하지 않거나 Community String이 public, private이 아닌 경우
	취약 : SNMP 서비스를 사용하며, Community String이 public, private인 경우
조치방법	불필요 시 서비스 중지/사용 안 함, 사용 시 Default Community String 변경
점검 및 조치 사례	

• Windows NT

Step 1) 바탕화면> 네트워크 환경> 등록 정보> 서비스/SNMP Service> 등록 정보> 보안

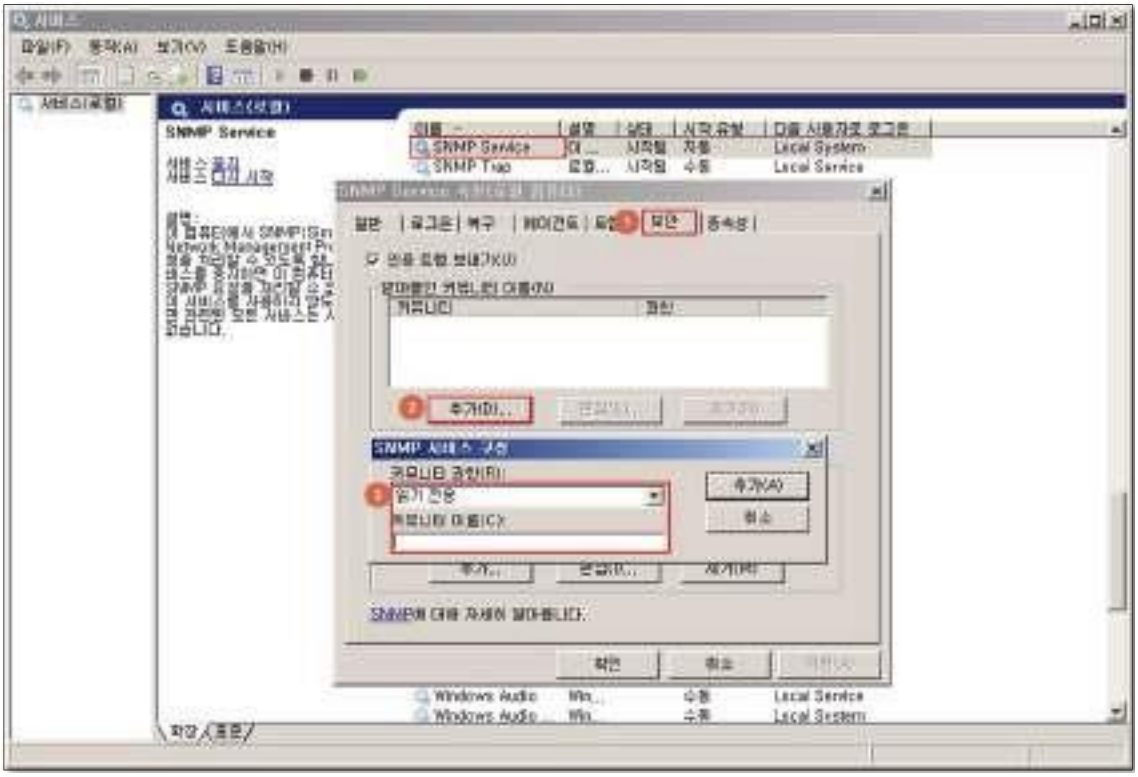


W-47 (중)	2. 서비스 관리 > SNMP 서비스 커뮤니티스트링의 복잡성 설정

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> SERVICES.MSC> SNMP Service> 속성> 보안> [인증 트랩 보내기] 아래 [추가] 버튼>

Step 2) [SNMP 서비스 구성]> 쓰기 권한이 필요하지 않다면 커뮤니티 이름을 읽기 전용 으로 Public/Private이 아닌 이름을 추가(NT의 경우 시작> 제어판> 서비스에서 설정)



Step 3) 불필요 시 해당 서비스 제거

시작> 실행> SERVICES.MSC> SNMP Service> 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, SNMP 서비스 중지

조치 시 영향	NMS 또는, 별도의 툴에서 SNMP 서비스를 이용하여 서버를 모니터링 하는 경우, 통신하고자 하는 Server/Client에 모두 같은 Community String을 사용하여야 함.(서비스> SNMP> 등록 정보> 종속성 참고)

2.30. SNMP Access control 설정

W-48 (중)	2. 서비스 관리 > SNMP Access control 설정
취약점 개요	
점검내용	• SNMP 패킷 접근 제어 설정 여부 점검
점검목적	• SNMP 트래픽에 대한 접근 제어 설정을 하여 내부 네트워크로부터의 악의적인 공격을 차단하기 위함
보안위협	• SNMP Access control 설정을 적용하지 않아 인증되지 않은 내부 서버로부터의 SNMP 트래픽을 차단하지 않을 경우, 장치 구성 변경, 라우팅 테이블 조작, 악의적인 TFTP 서버 구동 등의 SNMP 공격에 노출될 수 있음
참고	※ SNMP(v1, v2c)에서 클라이언트와 데몬간의 get_request(요청)와 get_response(응답) 과정은 암호화가 아닌 평문으로 전송되므로 스니핑(sniffing)이 가능함 ※ SNMP v3의 경우 인증을 위해 암호화가 제공
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 특정 호스트로부터 SNMP 패킷 받아들이기로 설정되어 있는 경우
	취약 : 모든 호스트로부터 SNMP 패킷 받아들이기로 설정되어 있는 경우
조치방법	불필요 시 서비스 중지/사용 안 함, 사용 시 SNMP 패킷 수령 호스트 지정
점검 및 조치 사례	
• Windows 2000, 2003, 2008, 2012 Step 1) 시작> 실행> SERVICES.MSC> SNMP Service> 속성> 보안 Step 2) "인증 트랩 보내기" 및 "다음 호스트로부터 SNMP 패킷 받아들이기" 선택 Step 3) SNMP 호스트 등록 	
조치 시 영향	일반적인 경우 영향 없음

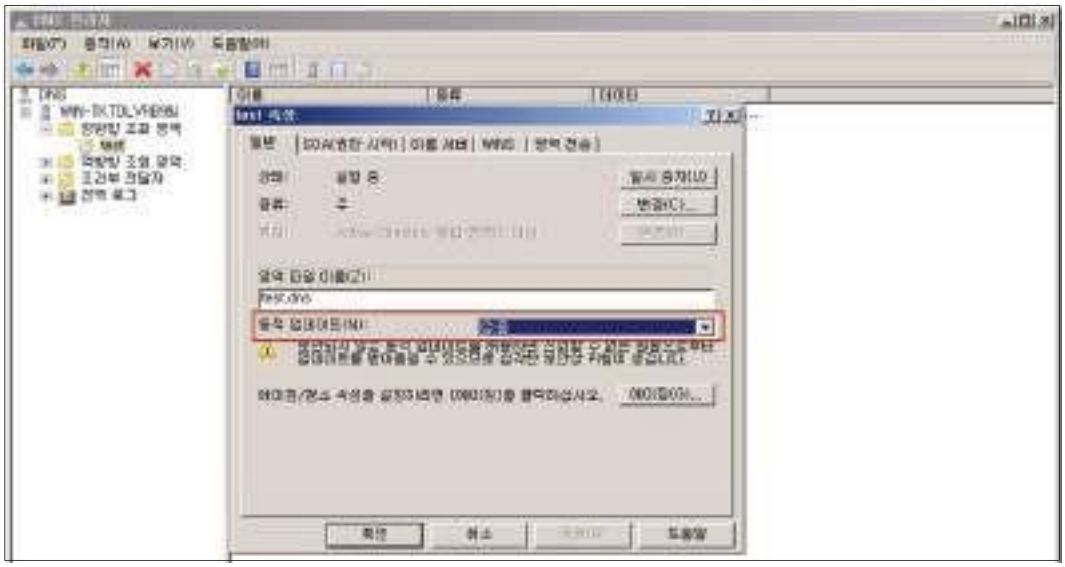
2.31. DNS 서비스 구동 점검

W-49 (중)	2. 서비스 관리 > DNS 서비스 구동 점검
취약점 개요	
점검내용	• DNS 서비스의 동적 업데이트 설정 여부 점검
점검목적	• DNS 동적 업데이트를 비활성화 함으로 신뢰할 수 없는 원본으로부터 업데이트를 받아들이는 위험을 차단하기 위함
보안위협	• DNS 서버에서 동적 업데이트를 사용할 경우 악의적인 사용자에 의해 신뢰할 수 없는 데이터가 받아들여질 위험이 존재함
참고	※ 등적 업데이트: DNS 정보에 변경 사항이 있을 때마다 DNS 클라이언트 컴퓨터가 자신의 리소스 레코드(zone 파일)를 DNS 서버에 자동으로 업데이트하는 기능으로 영역 레코드 수동 관리 작업을 줄일 수 있음
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : DNS 서비스를 사용하지 않거나 동적 업데이트 "없음(아니오)"으로 설정되어 있는 경우
	취약 : 서비스를 사용하며 동적 업데이트가 설정되어 있는 경우
조치방법	일반적으로 동적 업데이트 기능이 필요 없으나 확인 필요
점검 및 조치 사례	

• Windows 2000, 2003, 2008, 2012

Step 1) 시작> 실행> DNSMGMT.MSC> 각 조회 영역> 해당 영역> 속성> 일반

Step 2) 동적 업데이트 -+ 없음(또는, 아니오) 선택



Step 3) 불필요 시 해당 서비스 제거

시작> 실행> SERVICES.MSC> DNS 서버> 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후, DNS 서비스 중지

조치 시 영향	일반적인 경우 영향 없음

2.32. HTTP/FTP/SMTP 배너 차단

W-50 (하)	2. 서비스 관리 > HTTP/FTP/SNMP 배너 차단
취약점 개요	
점검내용	• HTTP/FTP/SNMP 서비스 배너 차단 적용 여부 점검
점검목적	• HTTP/FTP/SNMP 서비스 접속 배너를 통한 불필요한 정보 노출을 방지하기 위함
보안위협	• 서비스 접속 배너가 차단되지 않은 경우 임의의 사용자가 HTTP, FTP, SMTP 접속 시도 시 노출되는 접속 배너 정보를 수집하여 악의적인 공격에 이용할 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : HTTP, FTP, SMTP 접속 시 배너 정보가 보이지 않는 경우
	취약 : HTTP, FTP, SMTP 접속 시 배너 정보가 보여지는 경우
조치방법	사용하지 않는 경우 IIS 서비스 중지/사용 안 함, 사용 시 속성 값 수정
점검 및 조치 사례	

• HTTP

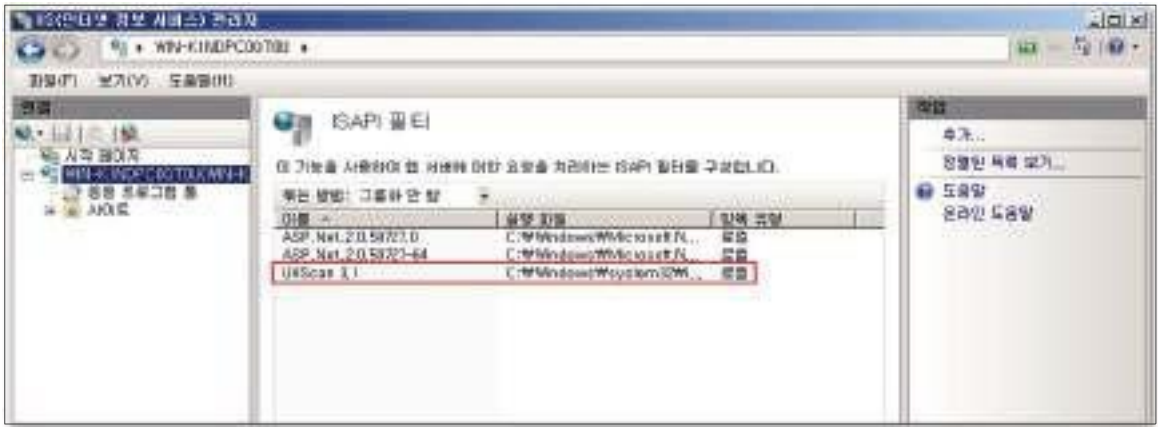
Step 1) Microsoft 다운로드 센터에서 UrlScan을 설치

http://www.iis.net/learn/extensions/working-with-urlscan/urlscan-setup

Step 2) IIS관리자> IIS> ISAPI 필터

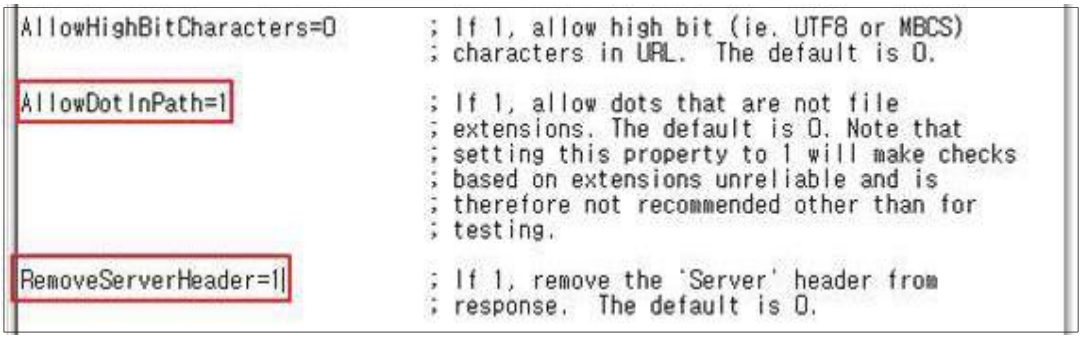
W-50 (하) | 2. 서비스 관리 > HTTP/FTP/SNMP 배너 차단

Step 3) 필터 추가 - UrlScan 3.1 - "C₩Windows₩System32₩inetsrv₩urlscan₩urlscan.dll"



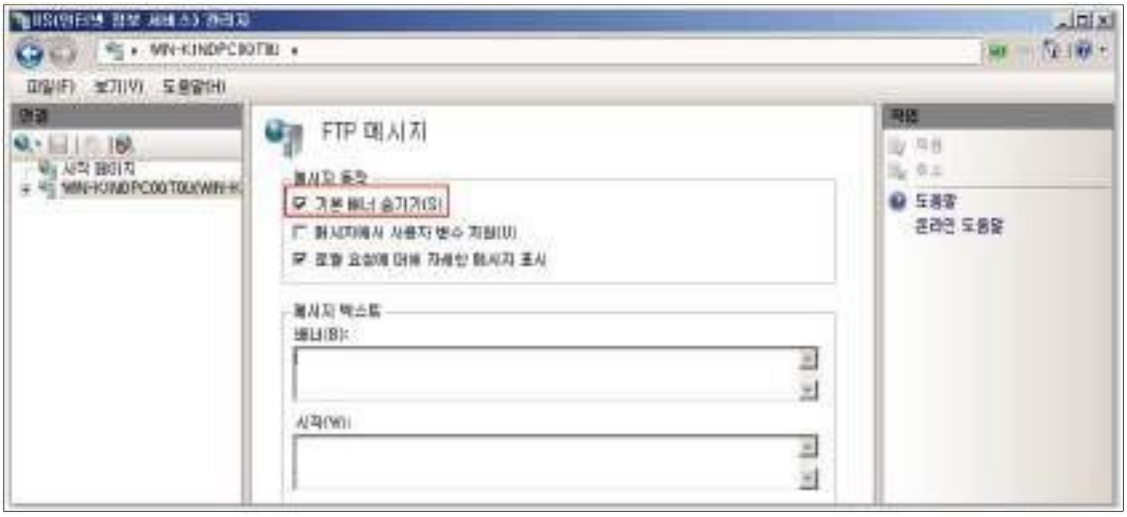
Step 4) UrlScal.ini 파일 내 해당 값 변경 "C₩Windows₩System32₩inetsrv₩urlscan₩urlscan.ini"

- RemoteserverHeader=1
- AllowDotInPath=1



- FTP

Step 1) IIS 관리자 > FTP 메시지> 기본 배너 숨기기 설정



W-50 (하)	2. 서비스 관리 > HTTP/FTP/SNMP 배너 차단

- SMTP

Step 1) IIS 관리자 > 서버 개체 우클릭 > 메타베이스 직접 편집 허용 설정

※ Exchange System Manager에서 사용할 수 없는 매개변수를 변경하려는 경우 메타베이스 설정을 직접 편집 가능함

(예) 다음과 같이 SMTP 통신에서 Exchange 관련 버전 정보를 공개하지 못하도록 기본 SMTP 가상 서버 구성 개체(<IIsSmtpServerLocation="/LM/SmtpSvc/1">)에 ConnectResponse 속성 값을 추가하여 SMTP 서버의 SMTP 배너를 변경할 수 있음

```
<IIsSmtpServer Location ="/LM/SmtpSvc/1">
AdminACL="4963... ... ...a472"
ClusterEnabled="FALSE"
ConnectionTimeout="600"
```

조치 시 영향	일반적인 경우 영향 없음

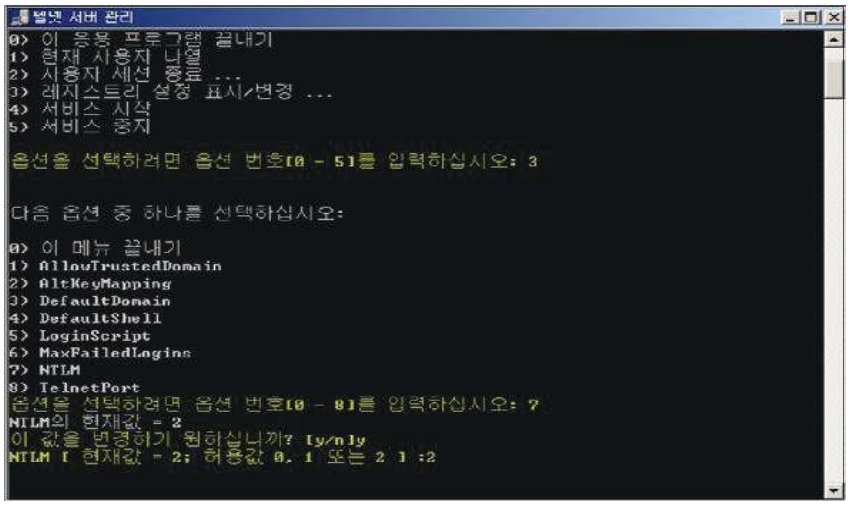
2.33. Telnet 보안 설정

W-51 (중)	2. 서비스 관리 > Telnet 보안 설정
취약점 개요	
점검내용	• Telnet 서비스 구동 비활성화 및 취약한 인증 사용 여부 점검
점검목적	• 취약 프로토콜인 Telnet 서비스의 사용을 원칙적으로 금지하고, 부득이 이용할 경우 네트워크상으로 패스워드를 전송하지 않는 NTLM 인증을 사용하도록 하여 인증 정보의 노출을 차단하기 위함
보안위협	• Telnet 서비스는 평문으로 데이터를 송수신하기 때문에 Password 방식으로 인증을 수행할 경우 ID 및 Password가 외부로 노출될 위험성이 있음
참고	※ Windows 서버의 Telnet 서비스의 두 가지 인증 방법 • NTLM 인증: 암호를 전송하지 않고 negotiate/challenge/response 절차로 인증 수행 • Password 인증: 관리자 및 Telnet Clients 그룹에 포함된 ID/PW로 인증 수행 ※ 기반시설 시스템에서 Telnet 서비스의 이용은 원칙적으로 금지하나, 조직에서 부득이 유사 기능을 활용해야 하는 경우 SSH를 사용하는 것을 권고함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : Telnet 서비스가 구동 되어 있지 않거나 인증 방법이 NTLM인 경우
	취약 : Telnet 서비스가 구동 되어 있으며 인증 방법이 NTLM이 아닌 경우
조치방법	불필요 시 서비스 중지/사용 안 함 설정, 사용 시 인증 방법으로 NTLM만 사용
점검 및 조치 사례	

• Windows NT, 2000

Step 1) 시작> 설정> 제어판> 관리 도구> 텔넷 서버 설정

Step 2) NTLM 인증 방식만 사용



W-51 (중)	2. 서비스 관리 > Telnet 보안 설정

- Windows 2003, 2008, 2012

Step 1) 시작> 실행> cmd> `tlntadmn config`

Step 2) `tlntadmn config sec = +NTLM -passwd` (passwd 인증 방식을 제외하고 NTLM 인증 방식만 사용)

Step 3) 불필요 시 해당 서비스 제거

시작> 실행> SERVICES.MSC> Telnet> 속성 [일반] 탭에서 "시작 유형"을 "사용 안 함"으로 설정한 후 Telnet 서비스 중지

조치 시 영향	일반적인 경우 영향 없음

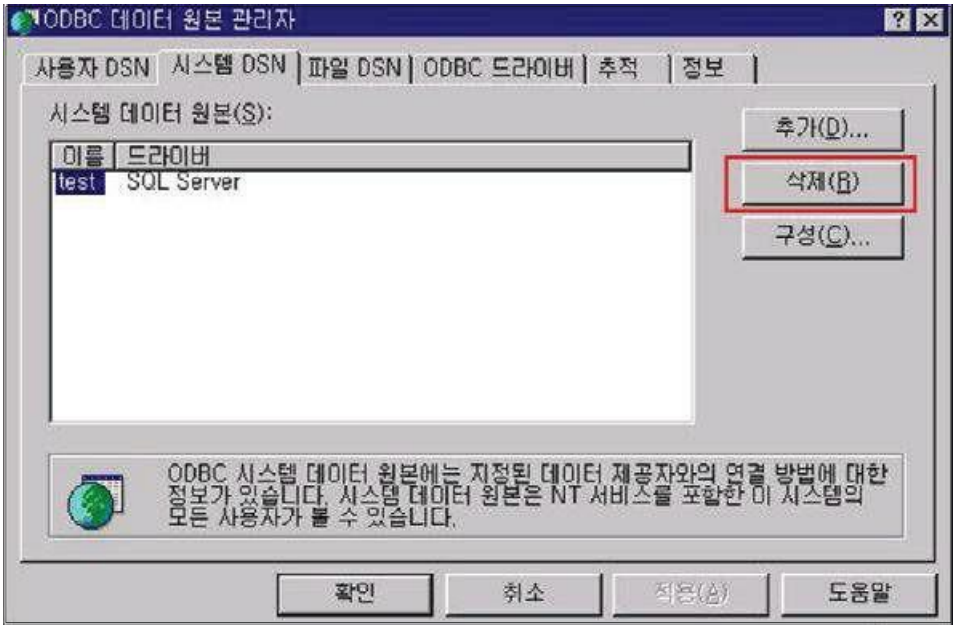
2.34. 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거

W-52 (중)	2. 서비스 관리 > 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거
취약점 개요	
점검내용	• 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거 여부 점검
점검목적	• 불필요한 데이터 소스 및 드라이버를 ODBC 데이터 소스 관리자 도구를 이용해 제거하여 비인가자에 의한 데이터베이스 접속 및 자료 유출을 차단하기 위함
보안위협	• 불필요한 ODBC/OLE-DB 데이터 소스를 통한 비인가자에 의한 데이터베이스 접속 및 자료 유출 위험 존재
참고	※ 특정 샘플 애플리케이션은 샘플 데이터베이스를 위해 ODBC 데이터 소스를 설치하거나 불필요한 ODBC/OLE-DB 데이터베이스 드라이버를 설치하므로 불필요한 데이터 소스나 드라이버는 ODBC 데이터 소스 관리자 도구를 이용해서 제거하는 것이 바람직함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 시스템 DSN 부분의 Data Source를 현재 사용하고 있는 경우
	취약 : 시스템 DSN 부분의 Data Source를 현재 사용하고 있지 않은 경우
조치방법	사용하지 않는 불필요한 ODBC 데이터 소스 제거
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 설정> 제어판> 데이터 원본(ODBC)> 시스템 DSN> 해당 드라이브 클릭

Step 2) 사용하지 않은 데이터 소스 제거

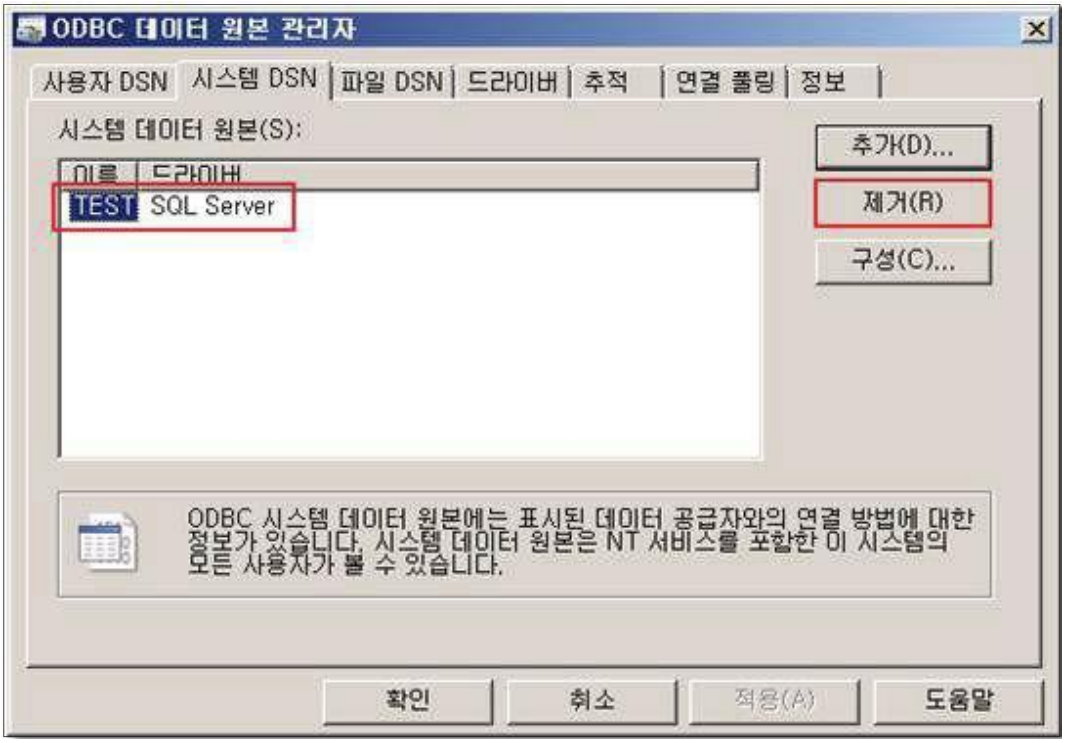


W-52 (중)	2. 서비스 관리 > 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거

- Windows 2000, 2003, 2008, 2012

Step 1) 시작> 설정> 제어판> 관리 도구> 데이터 원본(ODBC)> 시스템 DSN> 해당 드라이브 클릭

Step 2) 사용하지 않는 데이터 소스 제거



조치 시 영향	애플리케이션에서 사용할 경우 양호

2.35. 원격터미널 접속 타임아웃 설정

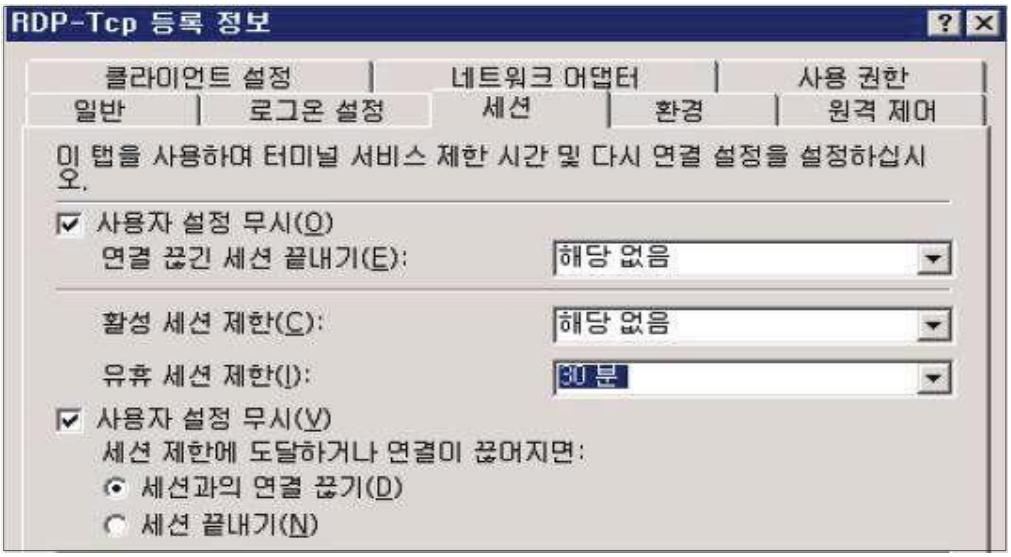
W-53 (중)	2. 서비스 관리 > 원격터미널 접속 타임아웃 설정
취약점 개요	
점검내용	• 원격터미널 접속 타임아웃 설정 여부 점검
점검목적	• 조직에서 부득이 원격터미널 접속을 허용해야 할 경우, 원격터미널 접속 후 일정 시간 동안 이벤트가 발생하지 않은 호스트의 접속을 차단하여 비인가자의 불필요한 접근을 차단하고 정보의 노출을 방지하기 위함
보안위협	• 접속 타임아웃 값이 설정되지 않은 경우 유휴 시간 내 비인가자의 시스템 접근으로 인해 불필요한 내부 정보의 노출 위험이 존재함
참고	※ 기반시설 시스템에서 원격 터미널 서비스의 이용은 원칙적으로 금지하나, 부득이 해당 기능을 활용해야 하는 경우 접속 타임아웃 설정 등의 보안 조치를 반드시 적용하여야 함
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 원격제어 시 Timeout 제어 설정을 적용한 경우
	취약 : 원격제어 시 Timeout 제어 설정을 적용하지 않은 경우
조치방법	Timeout 제어 설정 적용
점검 및 조치 사례	

• Windows 2000, 2003, 2008

Step 1) 시작> 실행> 열기> TSCC.MSC 실행(Windows 2008은 TSCONFIG.MC)

Step 2) RDP-Tcp connection에서 우클릭> 속성 실행

Step 3) [세션] 탭에서 아래 Override user settings(사용자 설정 무시)을 체크하고 Idle session time 세션이 끊어지도록(유휴 세션 제한) 원하는 시간을 설정함

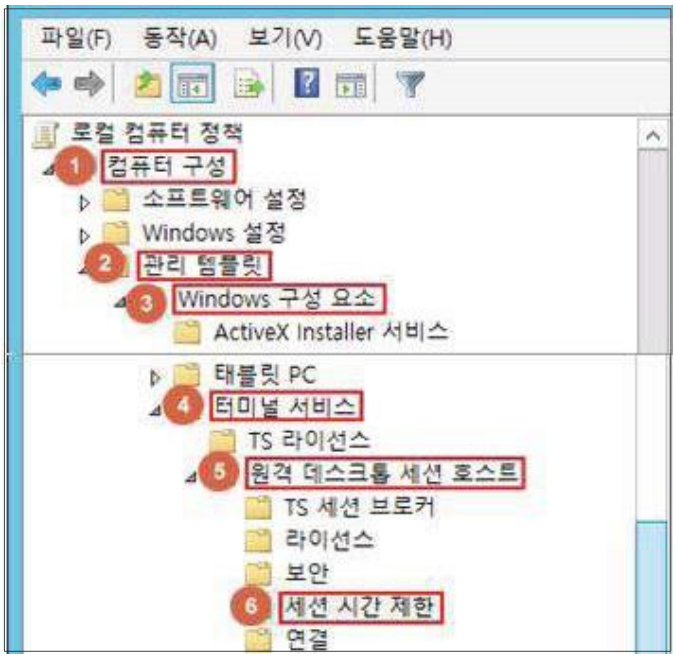


W-53 (중)	2. 서비스 관리 > 원격터미널 접속 타임아웃 설정

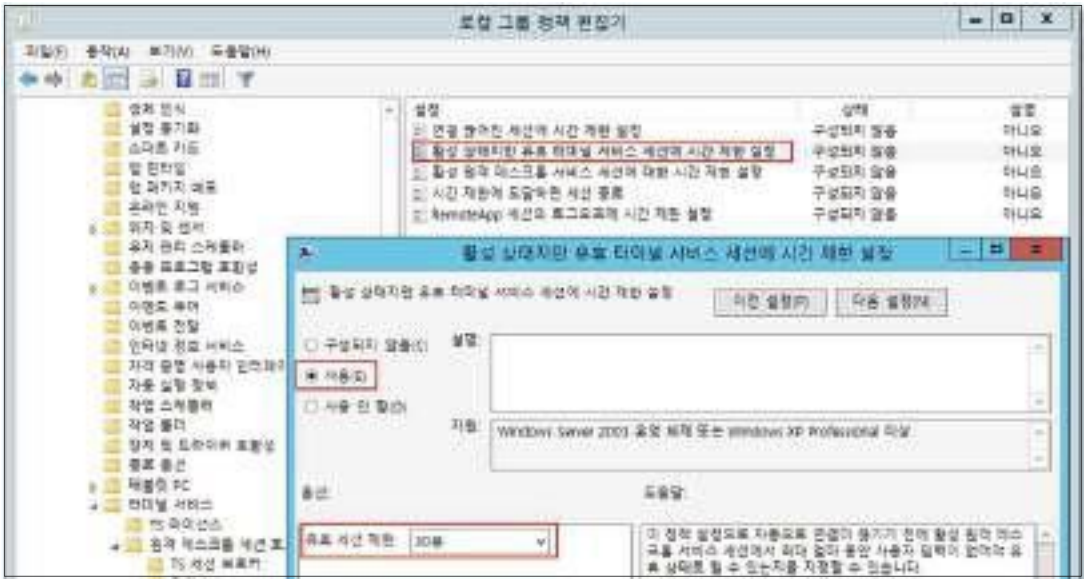
- Windows 2012

Step 1) 시작> 실행> GPEDIT.MSC(로컬 그룹 정책 편집기)

Step 2) 컴퓨터 구성> 관리 템플릿> Windows 구성 요소> 터미널 서비스> 원격 데스크톱 세션 호스트> 세션 시간 제한>



Step 3) [활성 상태지만 유휴 터미널 서비스 세션에 시간 제한 설정]> [유휴 세션 제한]을 30분으로 설정



조치 시 영향	일반적인 경우 영향 없음

2.36. 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검

W-54 (중)	2. 서비스 관리 > 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검
취약점 개요	
점검내용	• 예약된 작업에 의심스러운 명령의 등록 여부 점검
점검목적	• 외부 무단 침입시 설정될 수 있는 불필요한 예약 작업의 등록 여부를 확인하기 위함
보안위협	• 일정 시간마다 미리 설정해둔 프로그램을 실행할 수 있는 예약된 작업은 시작프로그램과 더불어서 해킹과 트로이 목마, 백도어를 설치하여 공격하기 좋은 루트로 사용될 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 불필요한 명령어나 파일 등 주기적인 예약 작업의 존재 여부를 주기적으로 점검하고 제거한 경우
	취약 : 불필요한 명령어나 파일 등 주기적인 예약 작업의 존재 여부를 주기적으로 점검하지 않거나, 해당 작업을 제거하지 않은 경우
조치방법	예약 작업에 대한 주기적인 확인
점검 및 조치 사례	

• Windows 2000, 2003, 2008, 2012

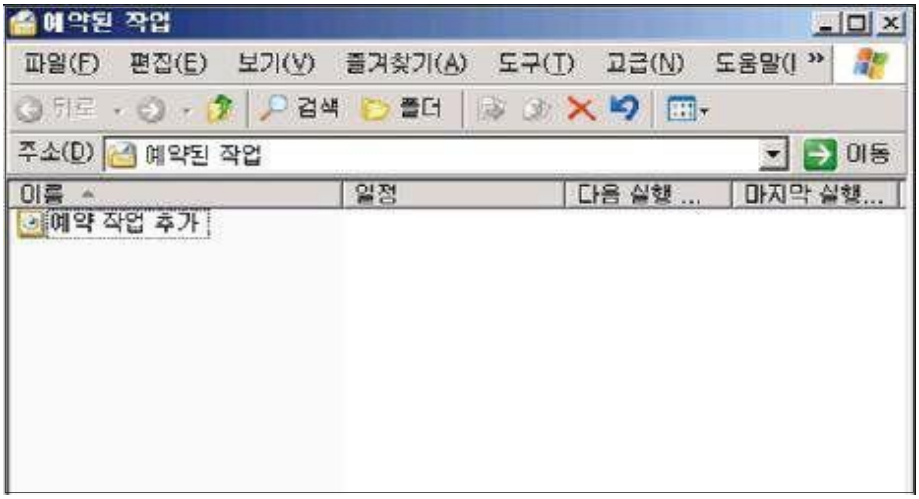
< GUI 확인 방법 >

Step 1) 시작> 설정> 제어판> 예약된 작업 확인

※ 2008, 2012 는 제어판> 관리도구> 작업 스케줄러 에서 확인

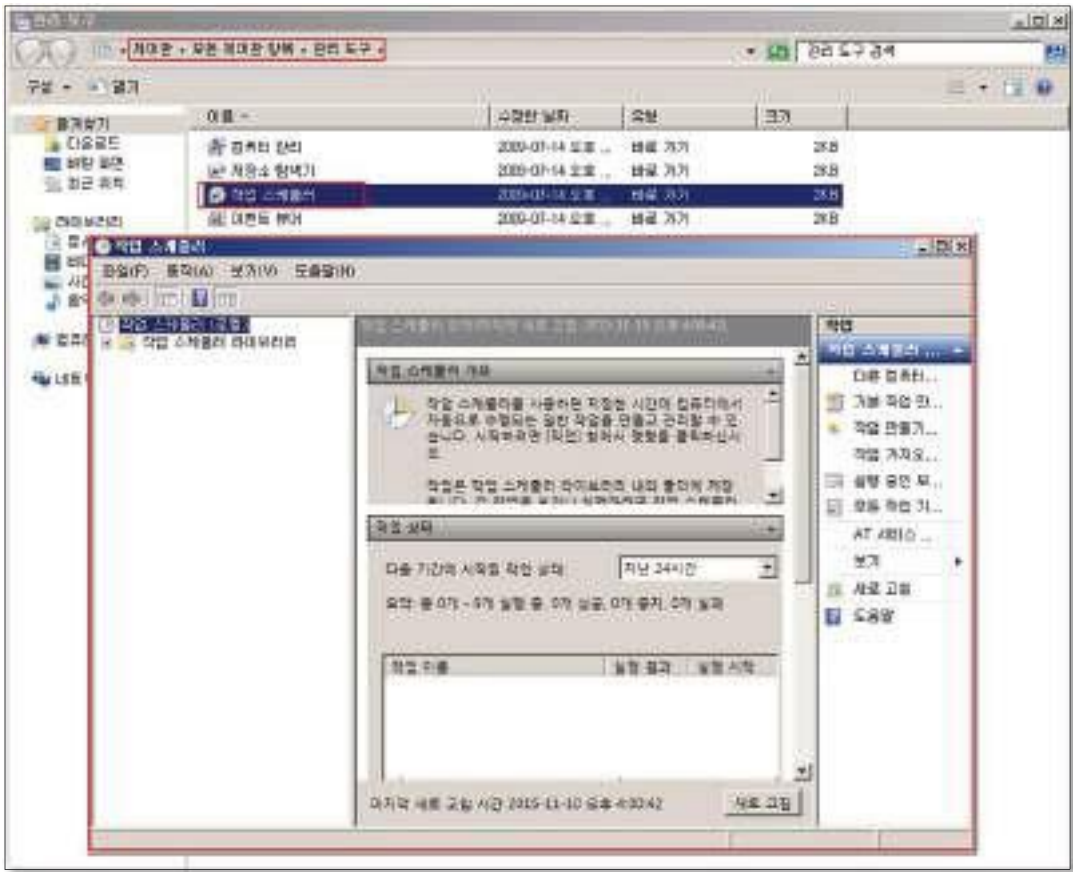
Step 2) 등록된 예약 작업을 선택하여 상세내역 확인

Step 3) 불필요한 파일 존재 시 삭제



[Windows 2000, 2003]

W-54 (중)	2. 서비스 관리 > 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검



[Windows 2008, 2012]

< CLI 확인 방법 >
Step 1) 시작> 실행> cmd 입력
Step 2) cmd 창에서 C:₩>at 명령어를 실행하여 확인 (2012는 schtasks 명령어로 확인)

조치 시 영향	예약작업을 잘못 삭제하는 경우 관련된 작업이 실행되지 않을 수 있음

3. 패치 관리

3.1. 최신 HOT FIX 적용

W-55 (상)	3. 패치 관리 > 최신 HOT FIX 적용
취약점 개요	
점검내용	• 최신 Hot Fix 적용 여부 점검
점검목적	• 최신 Hot Fix를 설치하여 시스템 및 응용프로그램의 취약성을 제거하기 위함
보안위협	• 최신 Hot Fix가 즉시 적용되지 않은 경우 알려진 취약성으로 인한 시스템 공격 가능성 존재
참고	※ Hot Fix보다 취약성을 이용한 공격도구가 먼저 출현할 수 있으므로 Hot Fix는 발표 후 가능한 한 빨리 설치할 것을 권장함 ※ Hot Fix: 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련된)을 패치하기 위해 배포되는 프로그램. 서비스팩이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표됨
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 최신 Hotfix가 있는지 주기적으로 모니터링하고 반영하거나, PMS (Patch Management System) Agent가 설치되어 자동패치배포가 적용된 경우
	취약 : 최신 Hotfix가 있는지 주기적으로 모니터 절차가 없거나, 최신 Hotfix를 반영하지 않은 경우, 또한 PMS(Patch Management System) Agent가 설치되어 있지 않거나, 설치되어 있으나 자동패치배포가 적용되지 않은 경우
조치방법	최신 Hotfix 설치
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 < 수등 HOT FIX 적용 > Step 1) 아래의 패치 리스트를 조회하여, 서버에 필요한 패치를 선별하여 수동으로 설치함 https://technet.microsoft.com/ko-kr/security/ < 자동 HOT FIX 적용 > Step 1) Windows 자동 업데이트 기능을 이용한 설치 제어판> windows update < PMS(Patch Management System) > Step 1) Agent를 설치하여 자동으로 업데이트 되도록 설정함 ※ 주의: 보안 패치 및 Hot Fix 경우 적용 후 시스템 재시작을 요하는 경우가 대부분이므로 관리자는 서비스에 지장이 없는 시간대에 적용할 것을 권장함. 일부 Hot Fix는 수행되고 있는 OS 프로그램이나 개발용 Application 프로그램에 영향을 줄 수 있으므로 패치 적용 전 Application 프로그램을 구분하고, 필요하다면 OS 벤더 또는, Application 엔지니어에게 확인 작업을 거친 후 패치를 수행하여야 함.	
조치 시 영향	설치 후 시스템 재시작이 필요한 경우가 존재하며 설치에 따른 영향도 필요함

3.2. 백신 프로그램 업데이트

W-56 (상)	3. 패치 관리 > 백신 프로그램 업데이트
취약점 개요	
점검내용	• 사용 백신의 최신 업데이트 여부 점검
점검목적	• 백신의 최신 업데이트 상태를 유지하기 위함
보안위협	• 백신이 지속적, 주기적으로 업데이트 되지 않은 경우 계속되는 신종 바이러스의 출현으로 인한 시스템 공격의 우려가 존재
참고	※ 네트워크망이 격리된 기반보호 시설의 경우, 시스템에 설치된 백신의 최신 업데이트 상태 유지를 위해 적절한 업데이트 절차 및 적용 방법 수립이 필요함 ※ 관련 점검 항목 : A-26(상)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있거나, 망 격리 환경의 경우 백신 업데이트를 위한 절차 및 적용 방법이 수립된 경우
	취약 : 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않거나, 망 격리 환경의 경우 백신 업데이트를 위한 절차 및 적용 방법이 수립되지 않은 경우
조치방법	백신 환경설정 메뉴를 통해 DB 및 엔진의 최신 업데이트를 하도록 설정
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 1. 긴급한 경우 수시로 업데이트 진행 (백신 종류마다 다소 차이는 있으나 매주 업데이트가 진행됨) 2. 정기적인 업데이트를 통해 검색엔진을 최신 버전으로 유지하고, 백신 사에서 발표하는 경보 주시 3. 백신 프로그램의 자동 업데이트 기능을 이용하면 온라인을 통해 변동 사항을 자동으로 업데이트 하여 알 수 있음 ※ 4개 백신 업체 모두 긴급 시 수시 업데이트 및 실시간 업데이트 기능 제공 ※ 기타 기관에서 사용중인 백신의 환경설정에서 업데이트 기능 활성화 여부 확인	
조치 시 영향	일반적인 경우 영향 없음

3.3. 정책에 따른 시스템 로깅 설정

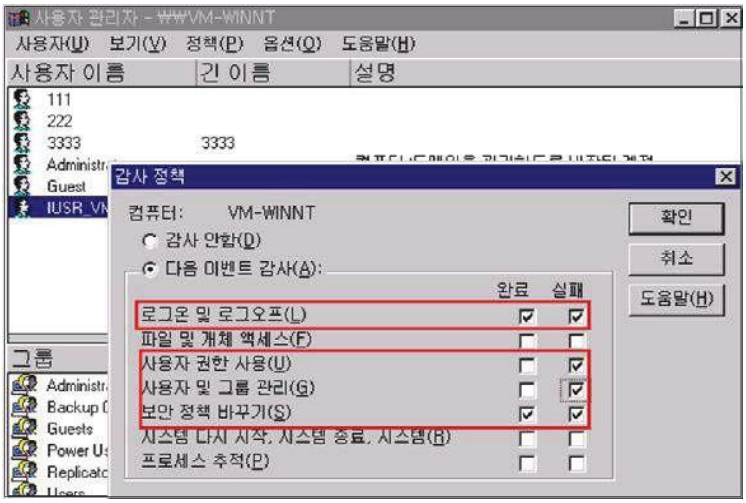
W-57 (중)	3. 패치 관리 > 정책에 따른 시스템 로깅 설정
취약점 개요	
점검내용	• 시스템 로깅 설정 여부 및 적절성 점검
점검목적	• 적절한 로깅 설정으로 유사 시 책임 추적을 위한 로그가 확보될 수 있게 하기 위함
보안위협	• 감사 설정이 구성되어 있지 않거나 감사 설정 수준이 너무 낮은 경우 보안 관련 문제 발생 시 원인을 파악하기 어려우며 법적 대응을 위한 충분한 증거 확보가 어려움
참고	※ 감사 정책을 너무 강화게 설정할 경우, 보안 로그에 불필요한 항목이 많이 기록되므로 중요한 감사 항목 식별이 어려울 수 있으며, 시스템 성능에도 심각한 영향을 줄 수 있기 때문에 법적 요구 사항과 조직의 정책에 따라 꼭 필요한 로그를 남기도록 설정하여야 함 ※ 윈도우 시스템은 보안 로그가 가득 차게 되는 경우 가장 오래된 감사 항목이 덮어 씌워짐 ※ 관련 점검 항목 : A-20(상), A-85(하)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 감사 정책 권고 기준에 따라 감사 설정이 되어 있는 경우
	취약 : 감사 정책 권고 기준에 따라 감사 설정이 되어 있지 않는 경우
조치방법	위와 같은 이벤트에 대한 추가적인 감사 설정
점검 및 조치 사례	

• Windows NT

Step 1) 시작> 프로그램> 관리 도구> 도메인 사용자 관리자> 정책> 감사

< 설정 예시 >

- 로그온 및 로그오프, 보안 정책 바꾸기: 성공/실패 감사
- 사용자 권한 사용, 사용자 및 그룹 관리: 실패 감사
-



W-57 (중)	3. 패치 관리 > 정책에 따른 시스템 로깅 설정

- Windows 2000, 2003, 2008, 2012

< 설정 예시 >

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 감사 정책

- 로그온 이벤트, 계정 로그온 이벤트, 정책 변경 : 성공/실패 감사
- 계정 관리, 디렉토리 서비스 액세스, 권한 사용 : 실패 감사

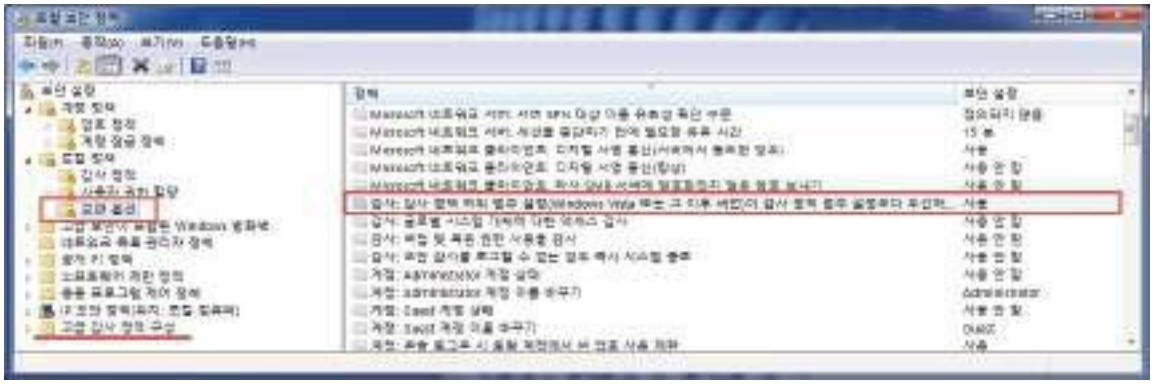
< 감사 정책 권고 기준 >

감사 정책	설정	고급 감사 정책	설정
개체 액세스 감사	감사 안 함	-	감사 안 함
계정 관리 감사	성공	사용자 계정 관리 컴퓨터 계정 관리 보안 그룹 관리	성공 성공 성공
계정 로그온 이벤트 감사	성공	자격 증명 유효성 검사 Kerberos 서비스 티켓 작업 Kerberos 인증서비스	성공 성공 성공
권한 사용 감사	감사 안 함	-	감사 안 함
디렉토리 서비스 액세스 감사	성공	디렉토리 서비스 액세스	성공
로그온 이벤트 감사	성공, 실패	로그온 로그오프 계정 잠금 특수 로그온 네트워크 정책 서버	성공, 실패 성공 성공 성공 성공, 실패
시스템 이벤트 감사	성공, 실패	보안 상태 변경 시스템 무결성 기타 시스템 이벤트	성공 성공, 실패 성공, 실패
정책 변경 감사	성공	감사 정책 변경 인증 정책 변경	성공 성공
프로세스 추적 감사	감사 안 함	-	감사 안 함

W-57 (중)	3. 패치 관리 > 정책에 따른 시스템 로깅 설정

※ 위에서 권고하는 감사 정책은 운영체제 제조사에서 서버 시스템의 보안 수준 유지를 위해 일반적으로 권장하는 설정값임. 감사 이벤트 생성하도록 허가된 작업이 너무 많거나, 많은 수의 개체에 대해 감사 정책을 구성할 경우 과도한 불필요한 이벤트 로그 생성으로 인해 전제 시스템의 성능에 영향을 줄 수 있으므로 책임 추적성을 확보하는 범위 내에서 적절한 감사 정책 수립이 필요함

※ 고급 감사 정책을 지원하는 시스템에서 고급 감사 정책을 활용 할 경우, 로컬 보안 정책 > 로컬 정책 > 보안 옵션 > "감사: 감사 정책 하위 범주 설정(Windows Vista 또는 그 이후 버전)이 감사 정책 범주 설정 보다 우선하도록 강제로 설정합니다" 정책을 먼저 사용하도록 설정하여야 함



< 감사정책 설명 >

정 책	설 명
로그온 이벤트	사용자가 컴퓨터에 로그온하거나 로그오프 할 때마다 로그온이 시도된 컴퓨터의 보안 로그에 이벤트 생성
계정 로그온 이벤트	사용자가 도메인에 로그온하면 도메인 컨트롤러에 로그온 시도 기록
계정 관리	사용자나 그룹이 작성, 변경 또는, 삭제된 시간을 판단하는데 사용
개체 액세스	시스템 액세스 컨트롤 목록(SACL)이 있는 Windows 2000 기반 네트워크의 모든 개체에 대한 감사 활성화 보안 로그에 이벤트를 표시하려면 먼저 개체 액세스 감사를 활성화한 후 감사할 각 개체에 대해 SACL 정의
디렉토리 서비스 액세스	Active Directory 개체의 SACL에 나열된 사용자가 해당 개체에 액세스를 시도할 때 감사 항목 생성
권한 사용	권한 사용의 성공 및 실패를 감사할 경우 사용자 권한을 이용하려고 할 때마다 이벤트 생성
프로세스 추적	실행되는 프로세스에 대한 자세한 추적 정보를 감사하는 경우 이벤트 로그에 프로세스를 작성하고 종료하려고 한 시도 확인
시스템 이벤트	사용자나 프로세스가 컴퓨터 환경을 변경하면 시스템 이벤트가 생성되고, 시스템 이벤트를 감사할 경우 보안 로그 삭제 시간 감사
정책 변경	감사 정책 변경의 성공 및 실패를 감사함

조치 시 영향	일반적인 경우 영향 없음

4. 로그 관리

4.1. 로그의 정기적 검토 및 보고

W-58 (상)	4. 로그 관리 > 로그의 정기적 검토 및 보고
취약점 개요	
점검내용	• 로그의 정기적 검토 및 보고 여부 점검
점검목적	• 정기적인 로그 점검을 통해 안정적인 시스템 상태 유지 및 외부 공격 여부를 파악하기 위함
보안위협	• 로그의 검토 및 보고 절차가 없는 경우 외부 침입시도에 대한 식별이 누락될 수 있고, 침입시도가 의심되는 사례 발견 시 관련 자료를 분석하여 해당 장비에 대한 접근을 차단하는 등의 추가 조치가 어려움
참고	※ 시스템 접속 기록, 계정 관리 로그 등 W-18(중) 점검 항목에서 설정한 보안 로그를 포함하여 응용 프로그램, 시스템 로그 기록에 대하여 주기적인 검토 및 보고가 필요함 ※ 관련 점검 항목 : A-85(하), W-18(중)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 접속기록 등의 보안 로그, 응용 프로그램 및 시스템 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어지는 경우
	취약 : 위 로그 기록에 대해 정기적으로 검토, 분석, 리포트 작성 및 보고 등의 조치가 이루어 지지 않는 경우
조치방법	로그 기록 검토 및 분석을 시행하여 리포트를 작성하고 정기적으로 보고함
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 Step 1) 로그 기록에 대한 정기적 검토 및 분석 실시 (1) 시작> 제어판> 관리 도구> 이벤트 뷰어 (2) 응용 프로그램 로그, 보안 로그, 시스템 로그 분석 ※ OS 구성에 따라 디렉토리 서비스 로그, 파일 복제 서비스 로그, DNS 서버 로그 등 분석  Step 2) 로그 분석 결과에 대한 일일·월간 보고서 작성 및 보고	
조치 시 영향	일반적인 경우 영향 없음

4.2. 원격으로 액세스할 수 있는 레지스트리 경로

W-59 (상)	4. 로그 관리 > 원격으로 액세스 할 수 있는 레지스트리 경로
취약점 개요	
점검내용	• 원격 레지스트리 서비스 사용 여부 점검
점검목적	• 원격 레지스트리 서비스를 비활성화 하여 레지스트리에 대한 원격 접근을 차단하기 위함
보안위협	• 원격 레지스트리 서비스는 액세스에 대한 인증이 취약하여 관리자 계정 외 다른 계정들에게도 원격 레지스트리 액세스를 허용할 우려가 있으며, 레지스트리에 대한 권한설정이 잘못되어 있는 경우 원격에서 레지스트리를 통해 임의의 파일을 실행 할 우려가 있음 • 레지스트리 서비스의 장애는 전제 시스템에 영향을 줄 수 있어 서비스거부공격(DoS) 공격에 이용될 수 있음
참고	※ 레지스트리: 윈도우를 실행하는데 필요한 모든 환경설정 데이터를 모아 두는 중앙 저장소 ※ 원격 레지스트리 서비스: 원격지에 있는 컴퓨터를 한 곳에서 집중관리하기 위한 목적으로 원격 컴퓨터의 레지스트리에 접근할 수 있도록 하는 서비스
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : Remote Registry Service가 중지되어 있는 경우
	취약 : Remote Registry Service가 사용 중인 경우
조치방법	불필요 시 서비스 중지 및 사용 안 함으로 설정
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 Step 1) 시작> 실행> SERVICES.MSC> Remote Registry> 속성 Step 2) 시작 유형 --+ 사용 안 함 Step 3) 서비스 상태 --+ 중지 	
조치 시 영향	Remote Registry Service를 사용하는지 확인 필요 (서비스> Remote Registry Service> 등록 정보> 종속성 참고)

4.3. 이벤트 로그 관리 설정

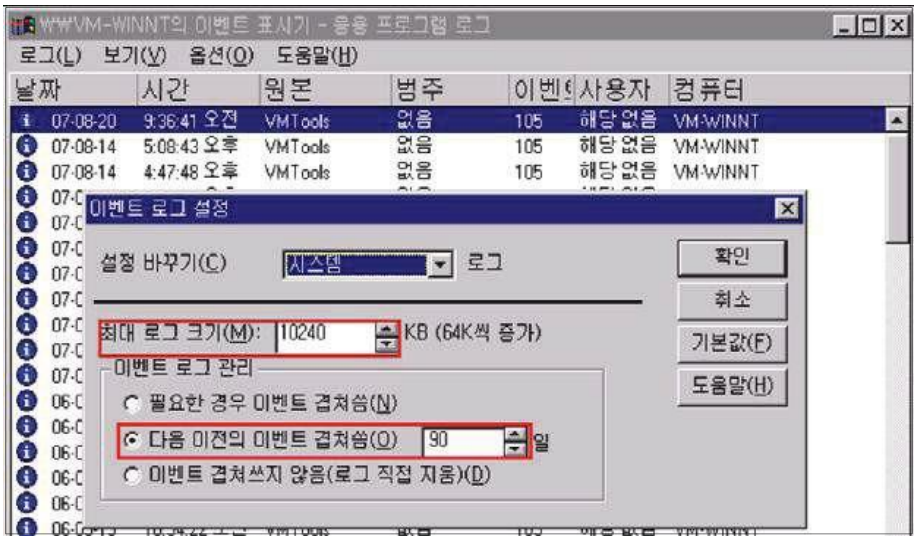
W-60 (하)	4. 로그 관리 > 이벤트 로그 관리 설정
취약점 개요	
점검내용	• 이벤트 로그 파일 용량 및 보관 기간 설정 점검
점검목적	• 유사 시 책임추적을 위해 주요 이벤트가 누락되지 않도록 이벤트 로그 파일의 크기 및 보관 기간을 적절하게 유지하기 위함
보안위협	• 이벤트 로그 파일의 크기가 충분하지 않을 경우 중요 로그가 저장되지 않을 위험이 있으며, 최대 보존 크기를 초과하는 경우 자동으로 덮어 씀으로써 중요 로그의 손실의 우려가 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 최대 로그 크기 "10,240KB 이상"으로 설정, "90일 이후 이벤트 덮어씀" 을 설정한 경우
	취약 : 최대 로그 크기 "10,240KB 미만"으로 설정, 이벤트 덮어씀 기간이 "90일 이하"로 설정된 경우
조치방법	최대 로그 크기 "10,204KB", "90일 이후 이벤트 덮어씀" 설정
점검 및 조치 사례	

• Windows NT

Step 1) 프로그램> 관리 도구> 이벤트 표시기> 로그> 로그 설정

Step 2) 최대 로그 크기 -+ 10240

다음 이전의 이벤트 겹쳐 씀 -+ 90일



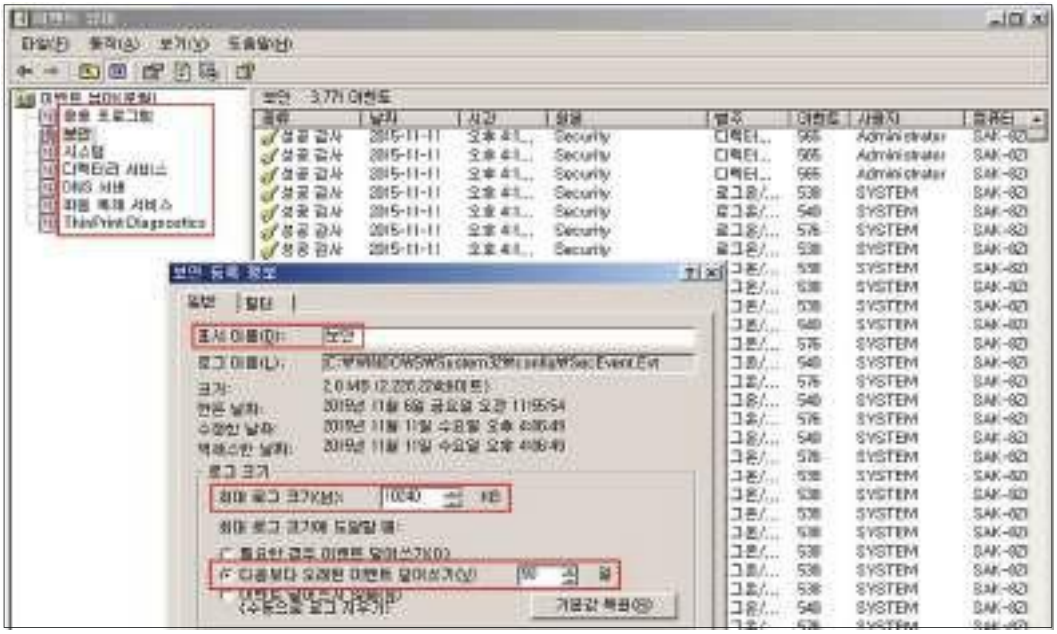
W-60 (하)	4. 로그 관리 > 이벤트 로그 관리 설정

- Windows 2000, 2003, 2008, 2012

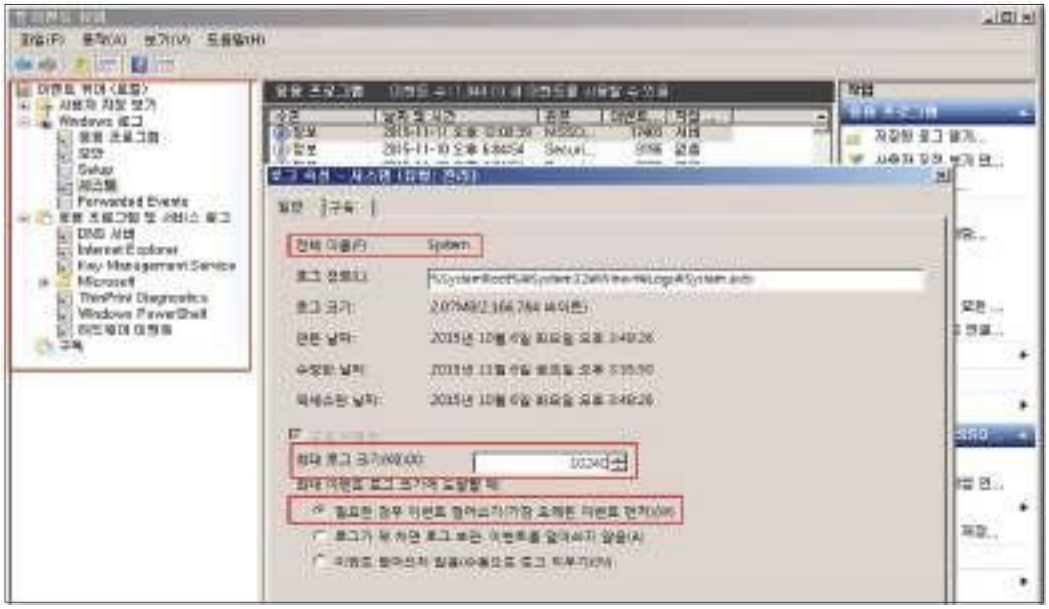
Step 1) 시작> 실행> EVENTVWR.MSC> 해당 로그> 속성> 일반

Step 2) 최대 로그 크기 -+ 10240

최대 로그 크기에 도달할 때: 다음보다 오래된 이벤트 덮어쓰기 -+ 90일



[Windows 2000, 2003]



[Windows 2008, 2012]

※ Windows 2008, 2012 서버의 경우 덮어쓰기 날짜 지정 불가능

조치 시 영향	일반적인 경우 영향 없음

4.4. 원격에서 이벤트 로그 파일 접근 차단

W-61 (중)	4. 로그 관리 > 원격에서 이벤트 로그 파일 접근 차단
취약점 개요	
점검내용	• 원격에서 로그 파일의 접근을 차단하기 위한 권한 적절성 점검
점검목적	• 원격에서 로그 파일을 접근하는 것을 차단하여 로그 파일의 훼손 및 변조를 자단하기 위함
보안위협	• 원격 익명 사용자의 시스템 로그 파일에 접근이 가능한 경우 '중요 시스템 로그' 파일 및 '애플리케이션 로그' 등 중요 보안 감사 정보의 변조·삭제·유출의 위험이 존재
참고	※ 로그 디렉토리 위치 • 시스템 로그 디렉토리: %systemroot%₩system32₩config • IIS 로그 디렉토리: %systemroot%₩system32₩LogFiles
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 로그 디렉토리의 접근권한에 Everyone 권한이 없는 경우
	취약 : 로그 디렉토리의 접근권한에 Everyone 권한이 있는 경우
조치방법	로그 디렉토리의 접근권한에 Everyone 제거
점검 및 조치 사례	

• Windows NT, 2000, 2003, 2008, 2012
Step 1) 탐색기> 로그 디렉토리> 속성> 보안
Step 2) Everyone 제거

※ 일반적으로 시스템 로그는C:₩winnt₩system32₩config 파일에 저장되지만. 애플리케이션 로그 파일은 각각의 애플리케이션마다 로그 저장 위치가 다름. 웹 서버에 많이 사용하는 IIS 경우, C:₩winnt₩system32₩LogFiles에 저장됨.

조치 시 영향	일반적인 경우 영향 없음

5. 보안 관리

5.1. 백신 프로그램 설치

W-62 (상)	5. 보안 관리 > 백신 프로그램 설치
취약점 개요	
점검내용	• 시스템 내 백신 프로그램 설치 여부 점검
점검목적	• 적절한 백신 프로그램을 설치하여 바이러스 감염 여부 진단, 지료 및 파일 보호를 통한 예방 조치를 위함
보안위협	• 백신 프로그램이 설치되지 않은 경우 립, 트로이목마 등의 악성 바이러스로 인한 시스템 피해 위험이 있음
참고	※ 웜: 악의적인 목적을 가지고 자기 자신을 복제해 전파시키며 주로 네트워크 공유 폴더나 메일로 전파됨 ※ 트로이목마: 고의적으로 악의적 목적이 있는 파일, 주로 다른 악성코드나 위장된 프로그램으로 전파되거나 인터넷을 통해 다운로드 됨 ※ 관련 점검 항목 : A-26(상)
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 바이러스 백신 프로그램이 설치되어 있는 경우
	취약 : 바이러스 백신 프로그램이 설치되어 있지 않은 경우
조치방법	담당자를 통해 바이러스 반드시 설치하여야 하도록 함
점검 및 조치 사례	
• 안절수 연구소: http://www.ahnlab.com • 하우리: http://www.hauri.co.kr • 시만텍코리아: http://www.symantec.co.kr • 한국트렌드마이크로: http://www.trendmicro.co.kr • 알약: https://en.estsecurity.com ※ 위 목록에 나열되지 않은 백신에 대해서도 인지도, 효과성 등을 검토하여 설치할 수 있음	
조치 시 영향	일반적인 경우 영향 없음

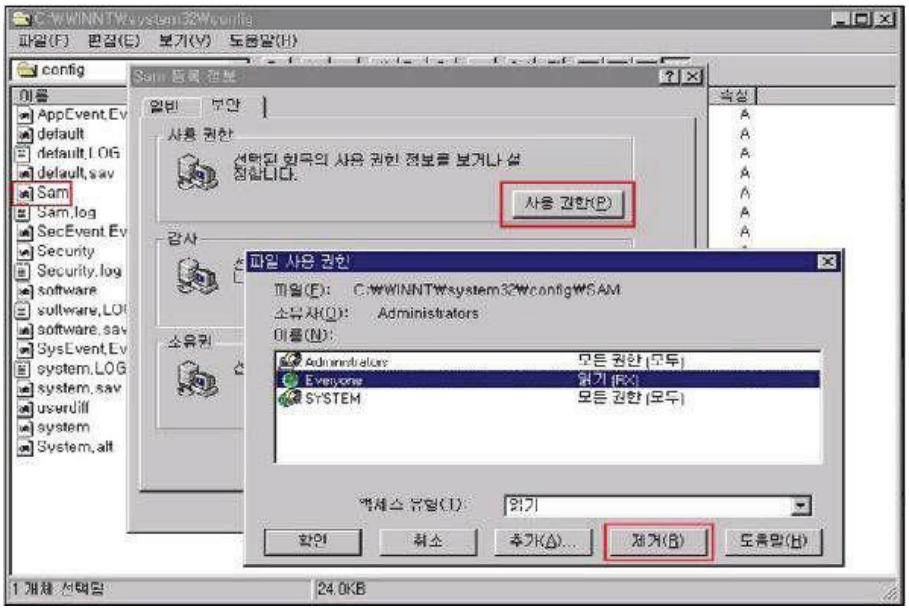
5.2. SAM 파일 접근 통제 설정

W-63 (상)	5. 보안 관리 > SAM 파일 접근 통제 설정
취약점 개요	
점검내용	• SAM 파일 접근 통제 설정 여부 점검
점검목적	• Administrator 및 System 그룹만 SAM 파일에 접근할 수 있도록 제한하여 악의적인 계정 정보 유출을 차단하고자 함
보안위협	• SAM 파일이 노출될 경우 패스워드 공격 시도로 인해 계정 및 패스워드 데이터베이스 정보가 탈취될 우려 존재
참고	※ SAM(Security Account Manager): 사용자와 그룹 계정의 패스워드를 관리하고, LSA(Local Security Authority)를 통한 인증을 제공함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : SAM 파일 접근권한에 Administrator, System 그룹만 모든 권한으로 설정되어 있는 경우
	취약 : SAM 파일 접근권한에 Administrator, System 그룹 외 다른 그룹에 권한이 설정되어 있는 경우
조치방법	SAM 파일 권한 확인 후 Administrator, System 그룹 외 다른 그룹에 설정된 권한 제거
점검 및 조치 사례	

• Windows NT

Step 1) %systemroot%₩system32₩config₩SAM> 속성> 보안

Step 2) Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거

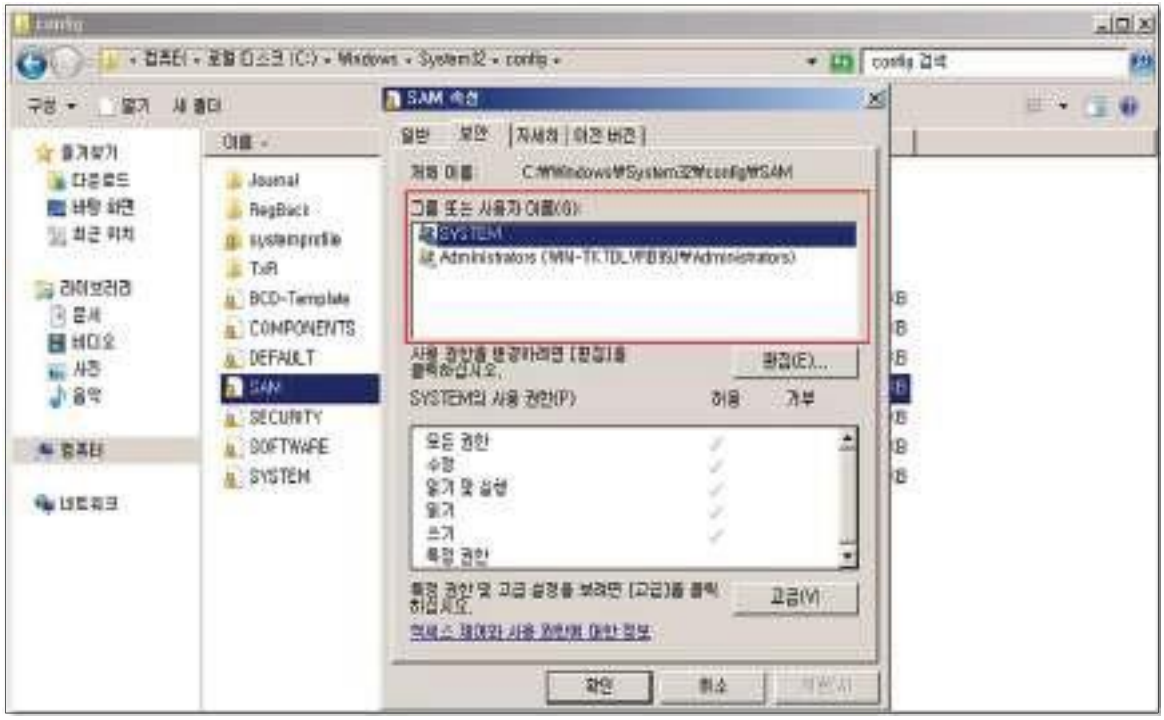


W-63 (상)	5. 보안 관리 > SAM 파일 접근 통제 설정

- Windows 2000, 2003, 2008, 2012

Step 1) %systemroot%₩system32₩config₩SAM> 속성> 보안

Step 2) Administrator, System 그룹 외 다른 사용자 및 그룹 권한 제거



조치 시 영향	일반적인 경우 영향 없음

5.3. 화면보호기설정

W-64 (상)	5. 보안 관리 > 화면보호기 설정
취약점 개요	
점검내용	• 시스템 화면보호기 설정 여부 점검
점검목적	• 사용자가 일정 시간 동안 아무런 작업을 수행하지 않을 경우 자동으로 로그오프 되거나 워크스테이션이 잠기도록 설정하여, 유휴 시간 내 불법적인 시스템 접근을 차단하기 위함
보안위협	• 화면보호기 설정을 하지 않은 경우 사용자가 자리를 비운 사이에 임의의 사용자가 해당 시스템에 접근하여 중요 정보를 유출 하거나, 악의적인 행위를 통해 시스템 운영에 악영향을 미칠 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 화면 보호기를 설정하고 대기 시간이 10분 이하의 값으로 설정되어 있으며, 화면 보호기 해제를 위한 암호를 사용하는 경우
	취약 : 화면 보호기가 설정되지 않았거나 암호를 사용하지 않은 경우 또는, 화면 보호기 대기 시간이 10분을 초과한 값으로 설정되어 있는 경우
조치방법	화면 보호기 사용, 대기 시간 10분, 암호 사용
점검 및 조치 사례	

• Windows NT, 2000

Step 1) 바탕화면> 등록 정보> 화면 보호기> "암호 사용" 체크, 대기 시간 "10분" 설정

W-64 (상)	5. 보안 관리 > 화면보호기 설정

- Windows 2003, 2008, 2012

< Windows 2003 >

Step 1) 바탕화면> 마우스 우클릭> 속성> 디스플레이 등록 정보> [화면 보호기]> "다시 시작할 때 암호로 보호" 체크 "대기 시간" 10분 설정

< Windows 2008, 2012 >

Step 1) 제어판> 디스플레이> 화면보호기 변경> "다시 시작할 때 로그온 화면 표시" 체크, "대기 시간" 10분 설정

조치 시 영향	일반적인 경우 영향 없음

5.4. 로그온하지 않고 시스템 종료 허용 해제

W-65 (상)	5. 보안 관리 > 로그온 하지 않고 시스템 종료 허용 해제
취약점 개요	
점검내용	• 비로그온 사용자의 시스템 종료 허용 여부 점검
점검목적	• 시스템 로그온 창의 종료 버튼을 비활성화 시킴으로써 허가되지 않은 사용자를 통한 불법적인 시스템 종료를 방지하고자 함
보안위협	• 로그온 창에 "시스템 종료" 버튼이 활성화되어 있으면 로그인을 하지 않고도 불법적인 시스템 종료가 가능하여 정상적인 서비스 운영에 영향을 줌
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "로그온 하지 않고 시스템 종료 허용"이 "사용 안 함"으로 설정되어 있는 경우
	취약 : "로그온 하지 않고 시스템 종료 허용"이 "사용"으로 설정되어 있는 경우
조치방법	시스템 종료: 로그온 하지 않고 시스템 종료 허용 --+ 사용 안 함
점검 및 조치 사례	

• Windows NT

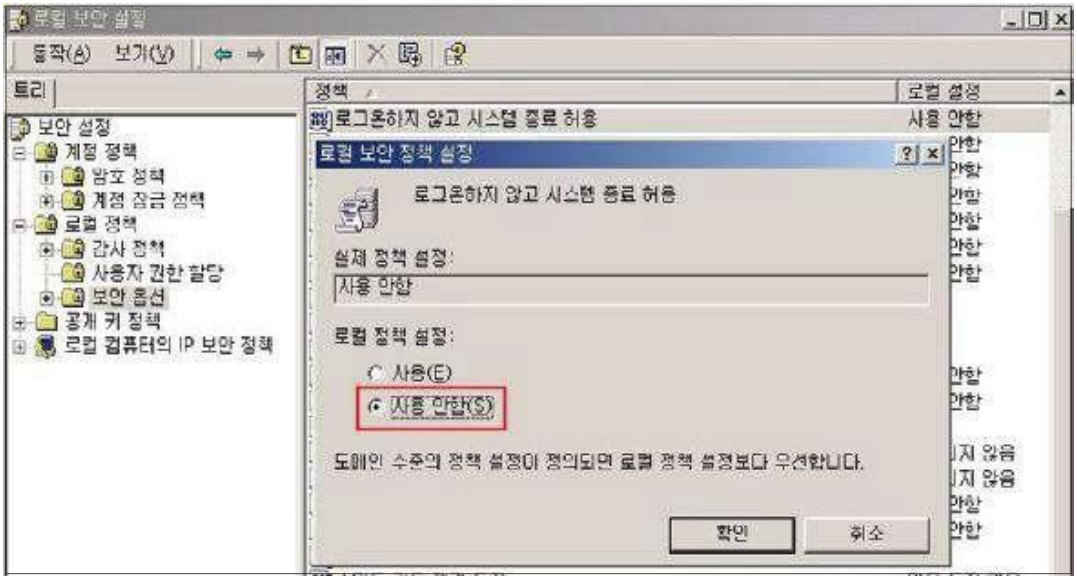
Step 1) HKEY_LOCAL_MACHINEWSOFTWAREWMicrosoftWWindows NTWCurrentVersion
WWinlogonWShutdownWithoutLogon = 0

W-65 (상)	5. 보안 관리 > 로그온 하지 않고 시스템 종료 허용 해제

- Windows 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "로그온 하지 않고 시스템 종료 허용"을 "사용 안함"으로 설정



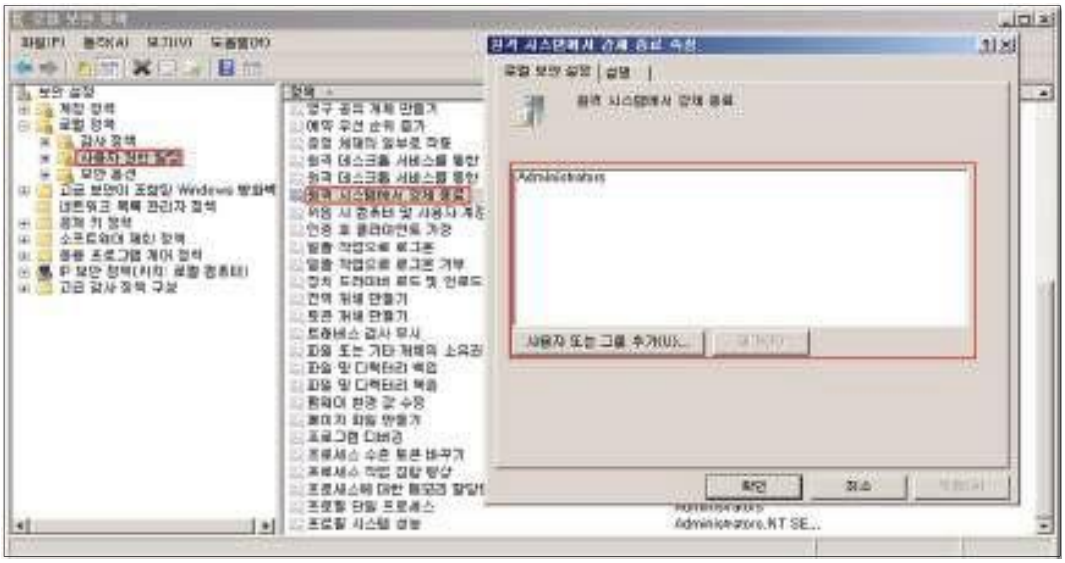
- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "시스템 종료: 로그온 하지 않고 시스템 종료 허용"을 "사용 안함"으로 설정

조치 시 영향	일반적인 경우 영향 없음

5.5. 원격 시스템에서 강제로 시스템 종료

W-66 (상)	5. 보안 관리 > 원격 시스템에서 강제로 시스템 종료
취약점 개요	
점검내용	• 원격 시스템 종료 정책 적절성 점검
점검목적	• 원격에서 네트워크를 통하여 운영 체제를 종료할 수 있는 사용자나 그룹을 설정하여 특정 사용자만 시스템 종료를 허용하기 위함
보안위협	• 원격 시스템 강제 종료 설정이 부적절한 경우 서비스 거부 공격 등에 악용될 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators"만 존재하는 경우
	취약 : "원격 시스템에서 강제로 시스템 종료" 정책에 "Administrators" 외 다른 계정 및 그룹이 존재하는 경우
조치방법	원격 시스템에서 강제로 시스템 종료 -+ Administrators
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 사용자 권한 할당 Step 2) "원격 시스템에서 강제로 시스템 종료" 정책에 Administrators 외 다른 계정 및 그룹 제거 	
조치 시 영향	일반적인 경우 영향 없음

5.6. 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제

W-67 (상)	5. 보안 관리 > 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제
취약점 개요	
점검내용	• '보안 감사를 로그할 수 없는 경우 즉시 시스템 종료' 정책 설정 여부 점검
점검목적	• 해당 정책을 비활성화 함으로써 로그 용량 초과 등의 이유로 이벤트를 기록할 수 없는 경우, 해당 정책으로 인해 시스템이 비정상적으로 종료되는 것을 방지하 기 위함
보안위협	• 해당 정책이 활성화 되어 있는 경우 악의적인 목적으로 시스템 종료를 유발하여 서비스 거부 공격에 악용될 수 있으며, 비정상적인 시스템 종료로 인하여 시스템 및 데이터에 손상을 임힐 수 있음
참고	※ 일반적으로 보안 감사 로그가 꽉 찼을 때 보안 로그에 대한 보존 방법이 [이벤트를 덮어쓰지 않음] 또는 [매일 이벤트 덮어쓰기]인 경우 이벤트가 로그되지 않음. 보안 로그가 꽉 자고 기존 항목을 덮어쓸 수 없을 때 해당 정책을 사용하는 경우 다음과 같은 중지 오류가 나타남 증지: C0000244 {감사 실패} 보안 감사를 만들려고 했으나 만들지 못했습니다. 복구하려면 관리자가 로그온하여 로그를 보관한 다음 로그를 지우고 이 옵션을 원하는 대로 다시 설정해야 합니다. 이 보안 설정을 다시 설정할 때까지는 보안 로그가 꽉 자지 않았더라도 Administrators 그룹의 구성원이 아니면 어떤 사용자도 시스템에 로그온할 수 없습니다.
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책이 "사용 안 함"으로 되어 있는 경우
	취약 : "보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책이 "사용"으로 되어 있는 경우
조치방법	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 -> 사용 안 함

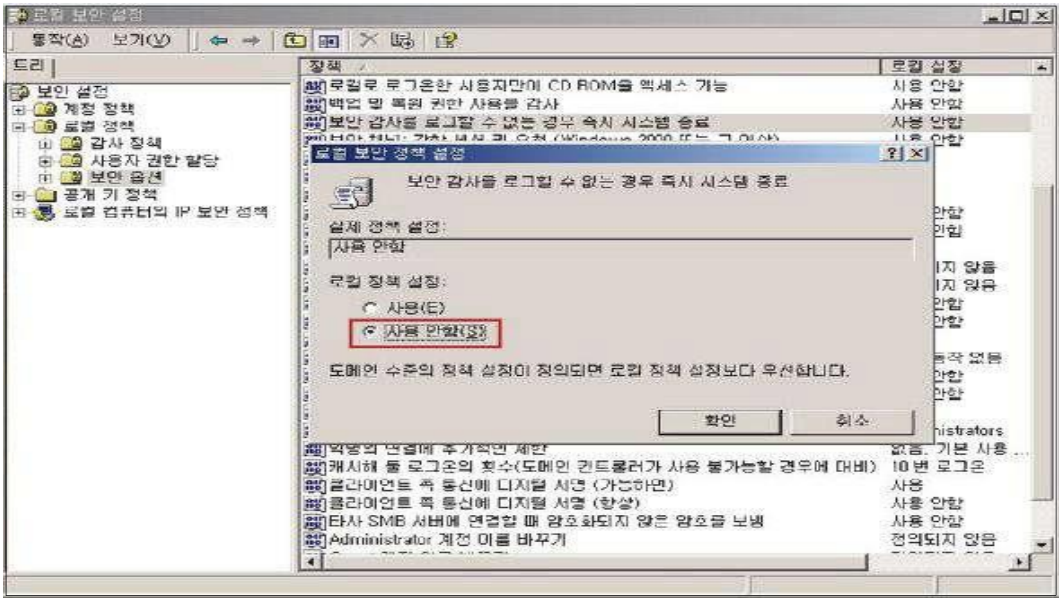
W-67 (상)	5. 보안 관리 > 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제

점검 및 조치 사례

- Windows NT, 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

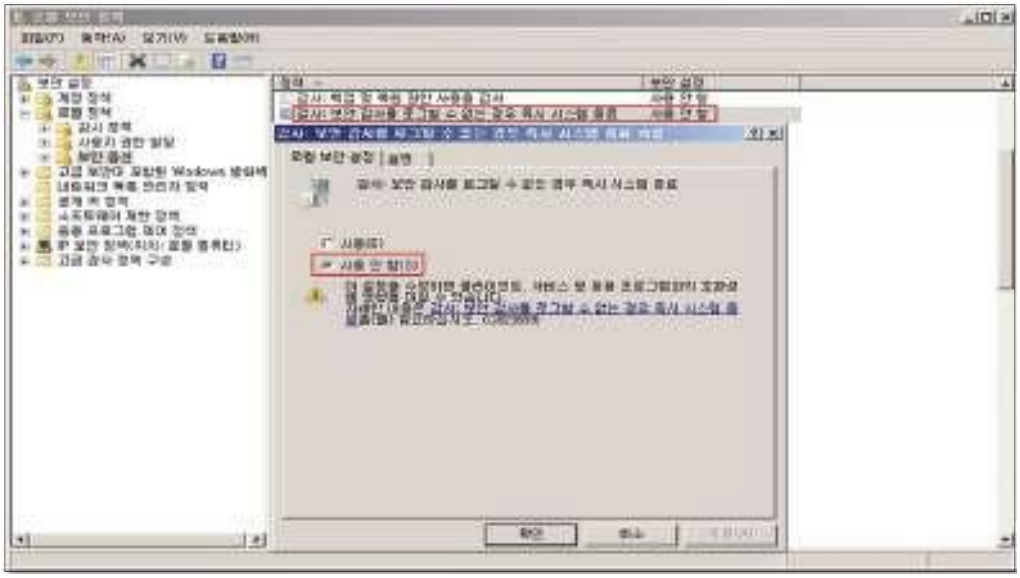
Step 2) "보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책을 "사용 안 함" 으로 설정



- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료" 정책을 "사용 안 함" 으로 설정



조치 시 영향	일반적인 경우 영향 없음

5.7. SAM 계정과 공유의 익명 열거 허용 안 함

W-68 (상)	5. 보안 관리 > SAM 계정과 공유의 익명 열거 허용 안 함
취약점 개요	
점검내용	• 'SAM 계정과 공유의 익명 열거 허용 안 함' 정책 설정 여부 점검
점검목적	• 익명 사용자에 의한 악의적인 계정 정보 탈취를 방지하기 위함
보안위협	• Windows에서는 익명의 사용자가 도메인 계정(사용자, 컴퓨터 및 그룹)과 네트워크 공유 이름의 열거 작업을 수행할 수 있으므로 SAM(보안계정관리자) 계정과 공유의 익명 열거가 허용될 경우 악의적인 사용자가 계정 이름 목록을 확인하고 이 정보를 사용하여 암호를 추측하거나 사회 공학적 공격기법을 수행할 수 있음
참고	※ 방화벽과 라우터에서 135◆139(TCP, UDP)포트 차단을 통해 외부로부터의 위협을 차단함 ※ 네트워크 및 전화 접속 연결> 로컬 영역> 등록 정보> 고급> 고급 설정 > Microsoft 네트워크 파일 및 프린트 공유를 해제하여야 함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 해당 보안 옵션 값이 설정 되어 있는 경우
	취약 : 해당 보안 옵션 값이 설정 되어 있지 않는 경우
조치방법	레지스트리 값 또는, 로컬 보안 정책 설정
점검 및 조치 사례	

• Windows NT

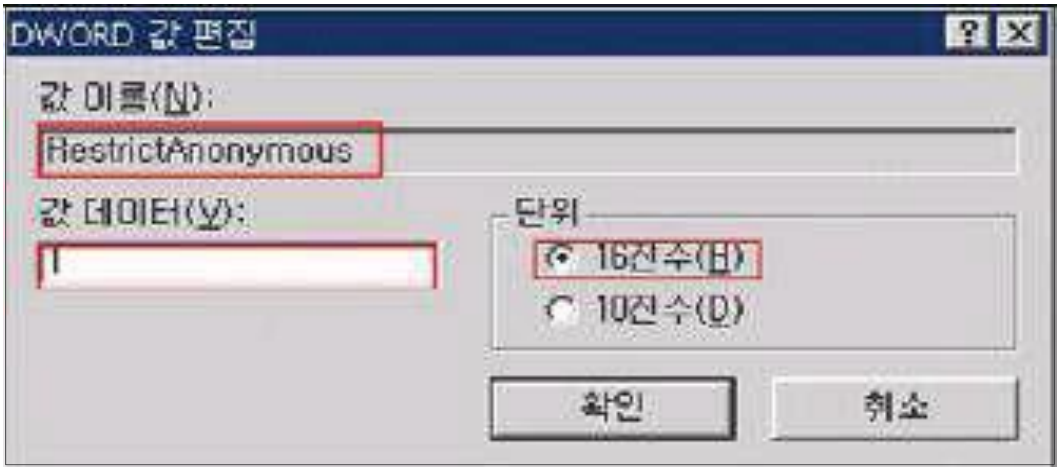
Step 1) 시작> 실행> regedit

Step 2) HKLMWSYSTEMWCurrentControlSetWControlWLSA 레지스트리 검색

Step 3) 우클릭 후 새로 만들기> DWORD 값 선택

W-68 (상)	5. 보안 관리 > SAM 계정과 공유의 익명 열거 허용 안 함

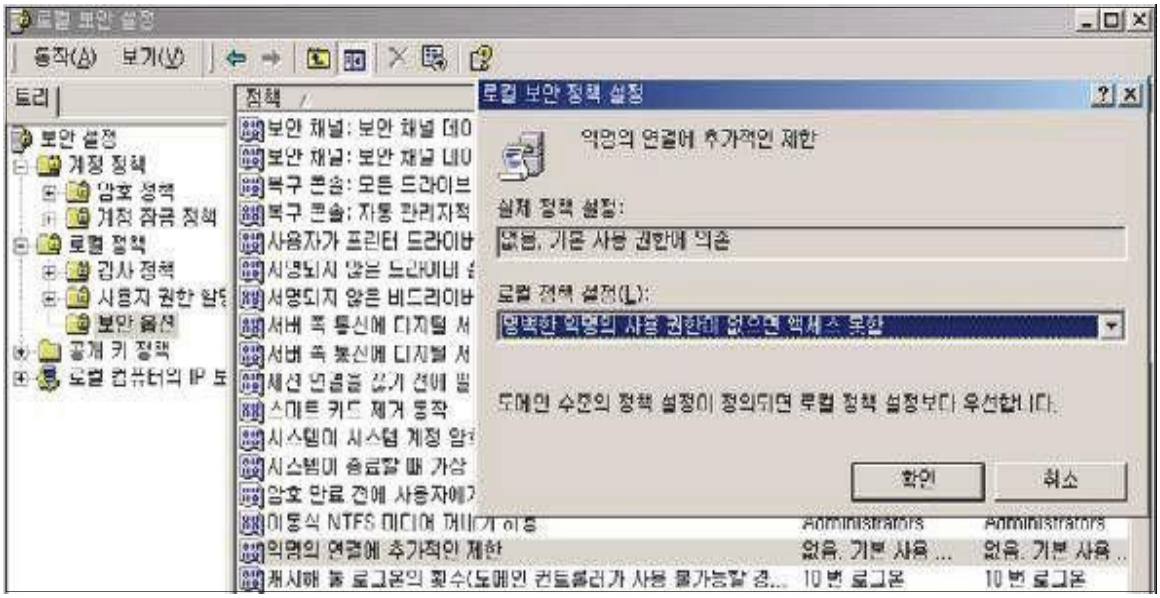
Step 4) RestrictAnonymous를 입력 후 데이터 Default 값인 "0"을 "1"로 변경



- Windows 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "익명의 연결에 추가적인 제한" 에 "명백한 익명의 사용 권한이 없으면 액세스 제한" 선택

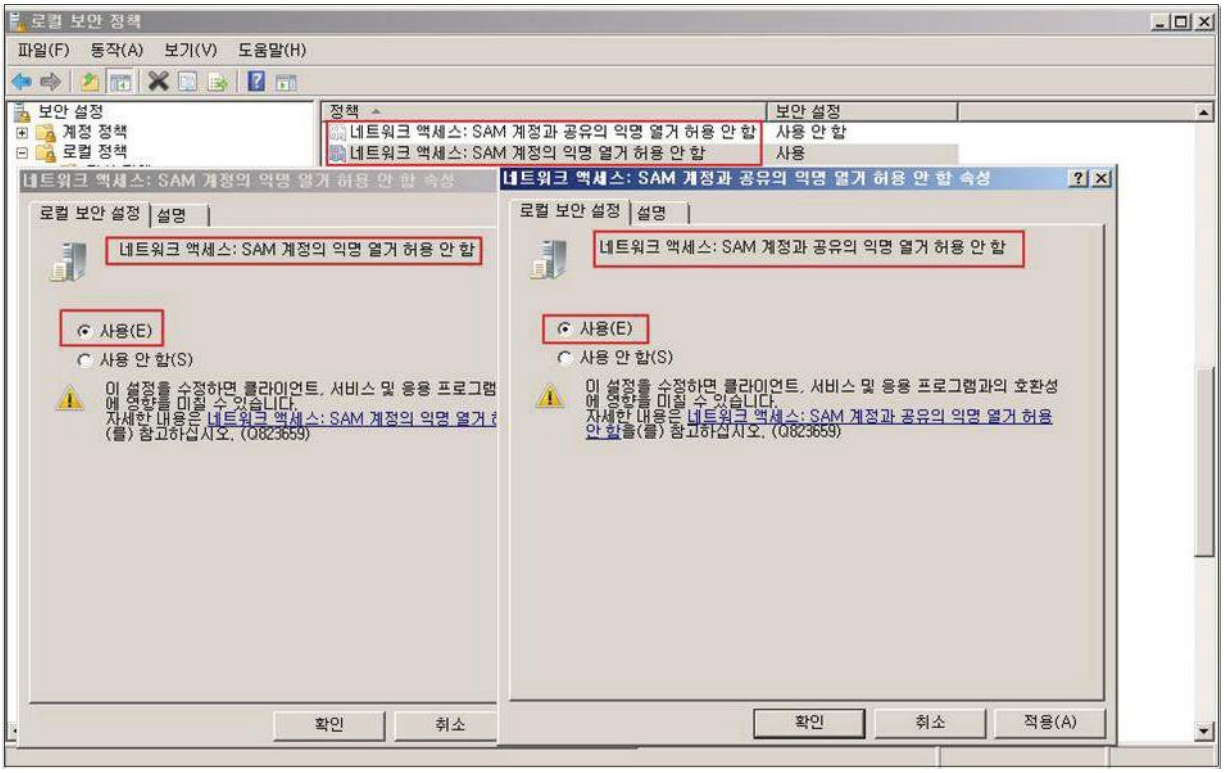


- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

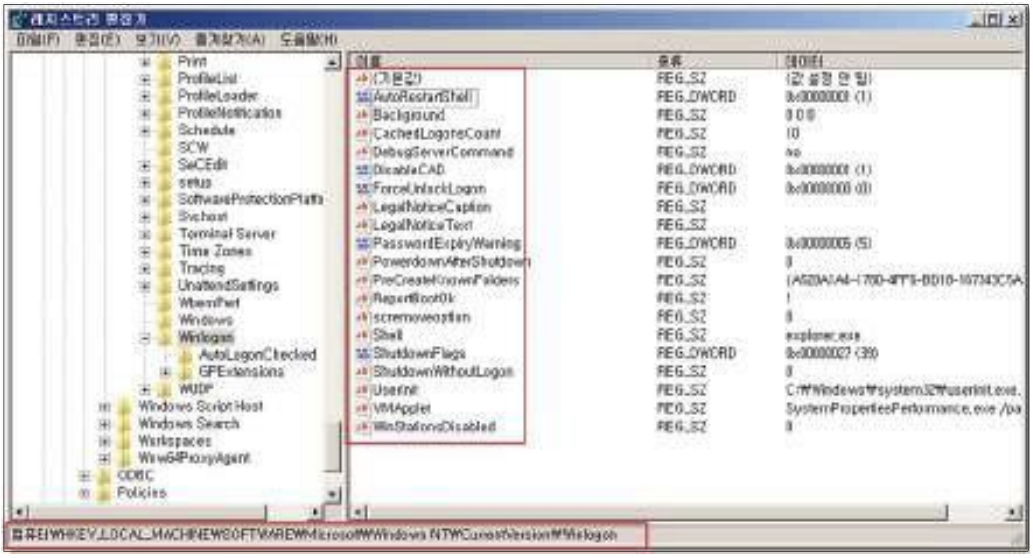
Step 2) "네트워크 액세스 : SAM 계정과 공유의 익명 열거 허용 안 함"과 "네트워크 액세스 : SAM 계정의 익명 열거 허용 안 함"에 "사용" 선택

W-68 (상)	5. 보안 관리 > SAM 계정과 공유의 익명 열거 허용 안 함



조치 시 영향	Active Directory, Clustered system 에서는 적용 시 영향 있음

5.8. Autologon 기능 제어

W-69 (상)	5. 보안 관리 > Autologin 기능 제어
취약점 개요	
점검내용	• Autologin 기능 제어 설정 여부 점검
점검목적	• Autologon 기능을 사용하지 않도록 설정하여 시스템 계정 정보 노출을 차단하기 위함
보안위협	• Autologon 기능을 사용하면 침입자가 해킹 도구를 이용하여 레지스트리에 저장된 로그인 계정 및 패스워드 정보 유출 가능
참고	※ Autologon: 레지스트리에 암호화 되어 저장된 대체 증명을 사용하여 자동으로 로그인하는 기능
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : AutoAdminLogon 값이 없거나 0으로 설정되어 있는 경우
	취약 : AutoAdminLogon 값이 1로 설정되어 있는 경우
조치방법	해당 레지스트리 값이 존재하는 경우 0으로 설정
점검 및 조치 사례	
• Windows NT, 2000, 2003, 2008, 2012 Step 1) 시작> 실행> REGEDIT> HKLMWSOFTWAREWMicrosoftWWindowsNTWCurrentVersionWWinlogon Step 2) "AutoAdminLogon 값"을 "0"으로 설정 Step 3) DefaultPassword 엔트리가 존재한다면 삭제 	
조치 시 영향	반드시 자동 로그인을 사용하여야 할 경우를 제외하고는 일반적으로 영향 없음

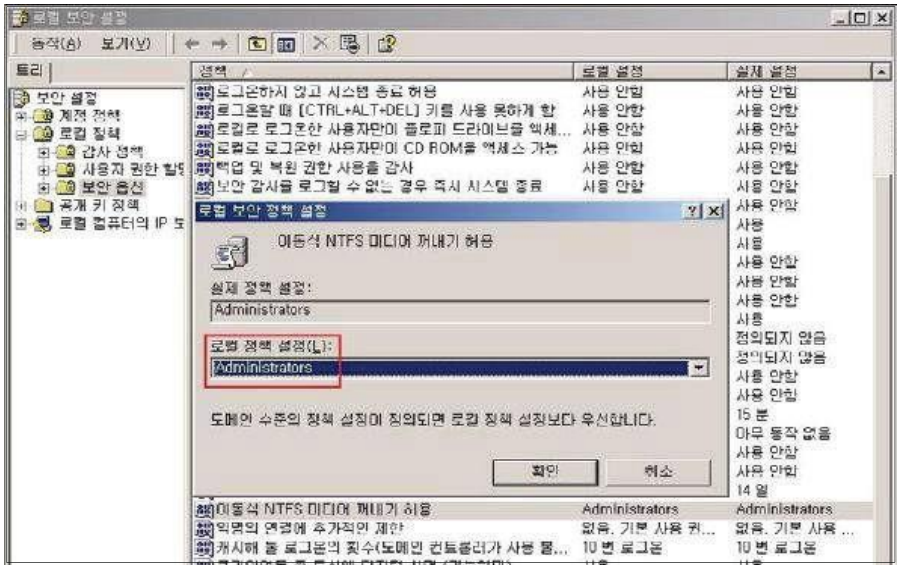
5.9. 이동식 미디어 포맷 및 꺼내기 허용

W-70 (상)	5. 보안 관리 > 이등식 미디어 포맷 및 꺼내기 허용
취약점 개요	
점검내용	• 관리자 이외 NTFS 미디어 포맷 및 꺼내기 허용 여부 점검
점검목적	• 이동식 미디어의 NTFS 포맷 및 꺼내기가 허용되는 사용자를 관리 권한자로 제한함으로써 관리 권한이 없는 사용자 및 비인가자에 의한 불법적인 이동식 미디어의 포맷 및 이동을 차단하기 위함
보안위협	• 관리자 이외 사용자에게 해당 정책이 설정된 경우 비인가자에 의한 불법적인 매제 처리를 허용할 수 있음
참고	※ 해당 보안 설정은 이동식 NTFS 미디어를 포맷하거나 꺼낼 수 있는 사용자를 결정하는 옵션으로 Administrators, Administrators 및 Power Users, Administrators 및 Interactive Users 그룹에 이 기능을 허용할 수 있음
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrator"로 되어 있는 경우
	취약 : "이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrator"로 되어 있지 않은 경우
조치방법	이동식 미디어 포맷 및 꺼내기 허용 -+ Administrator
점검 및 조치 사례	

• Windows NT, 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "이동식 NTFS 미디어 꺼내기 허용" 정책을 "Administrators" 로 설정

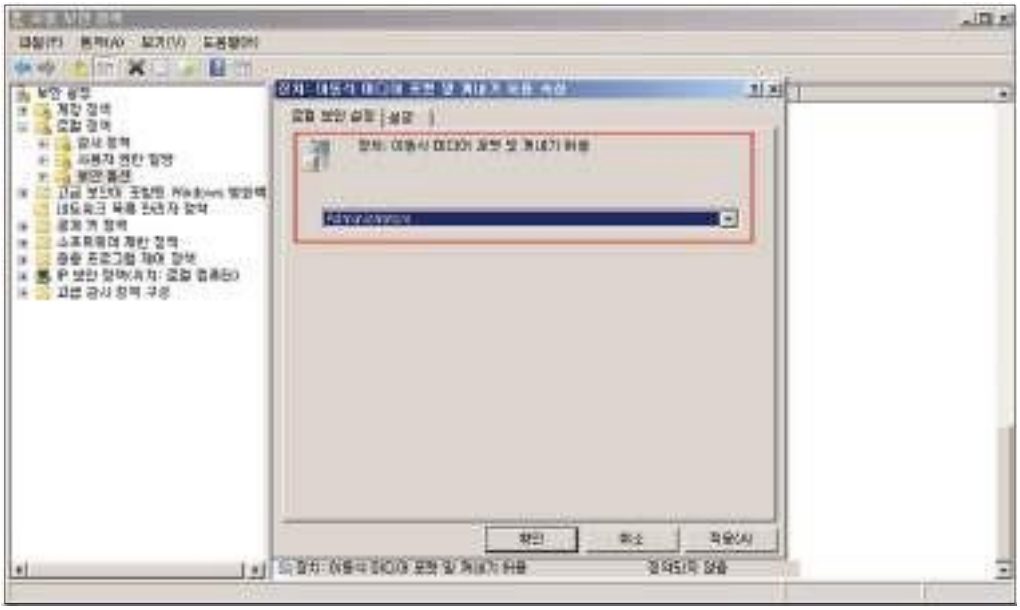


W-70 (상)	5. 보안 관리 > 이등식 미디어 포맷 및 꺼내기 허용

- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "장치 : 이동식 미디어 포맷 및 꺼내기 허용" 정책을 "Administrators" 로 설정



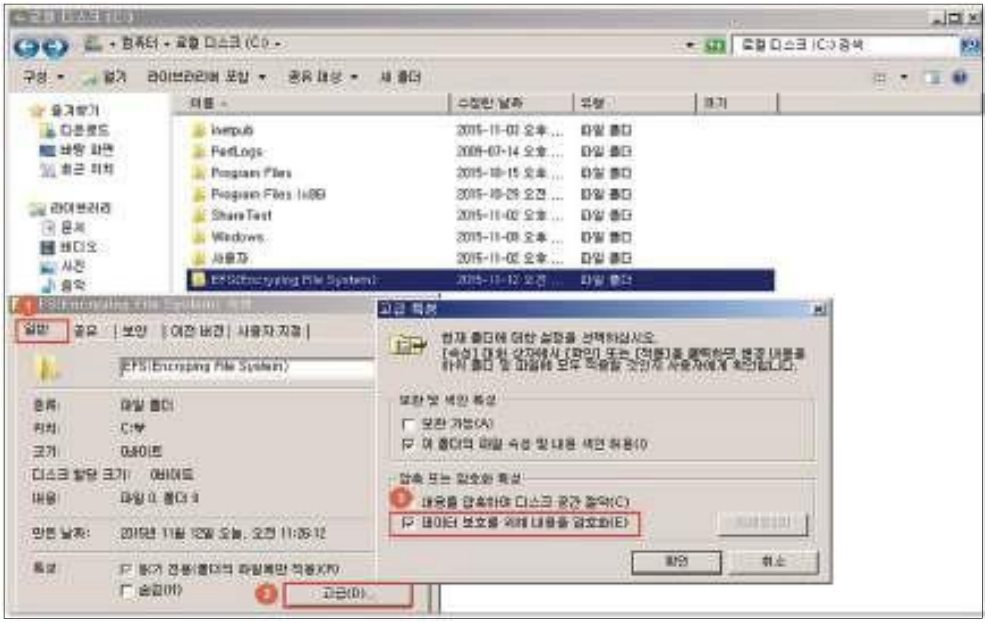
조치 시 영향	일반적으로 영향 없음

5.10. 디스크볼륨 암호화 설정

W-71 (상)	5. 보안 관리 > 디스크볼륨 암호화 설정
취약점 개요	
점검내용	• 디스크볼륨 암호화 설정 여부 점검
점검목적	• 디스크볼륨 암호화 설정을 적용하여 비인가 액세스로부터 중요 데이터를 보호하기 위함
보안위협	• 디스크 볼륨이 암호화 되어 있지 않은 경우 비인가자가 데이터를 열람할 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "데이터 보호를 위해 내용을 암호화" 정책이 선택된 경우
	취약 : "데이터 보호를 위해 내용을 암호화" 정책이 선택되어 있지 않은 경우
조치방법	EFS(Encrypting File System) 활성화
점검 및 조치 사례	

• Windows 2000, 2003, 2008, 2012

Step 1) 폴더 선택> 속성> [일반] 탭> 고급> 고급 특성> "데이터 보호를 위해 내용을 암호화" 선택



※ 폴더 속성> [보안] 탭에서 허가된 사용자 외에는 폴더 내 파일 접근 불가함

조치 시 영향	복호키 분실 시 데이터복구 어려움

5.11. Dos 공격 방어 레지스트리 설정

W-72 (상)	5. 보안 관리 DoS 공격 방어 레지스트리 설정
취약점 개요	
점검내용	• DoS 공격 방어 레지스트리 설정 여부 점검
점검목적	• TCP/IP 스택(Stack)을 강화하는 레지스트리 값 변경을 통하여 DoS 공격을 방어하기 위함
보안위협	• DoS 방어 레지스트리를 설정하지 않은 경우, DoS 공격에 의한 시스템 다운으로 서비스 제공이 중단될 수 있음
참고	※ DoS(서비스 거부 공격): 네트워크 사용자가 컴퓨터나 컴퓨터의 특정 서비스를 사용할 수 없도록 만들기 위한 네트워크 공격
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : DoS 방어 레지스트리 값이 아래와 같이 설정되어 있는 경우
	취약 : DoS 방어 레지스트리 값이 아래와 같이 설정되어 있지 않은 경우 • SynAttackProtect = REG_DWORD 0(False) -> 1 이상 • EnableDeadGWDetect = REG_DWORD 1(True) -> 0 • KeepAliveTime = REG_DWORD 7,200,000(2시간) -> 300,000(5분) • NoNameReleaseOnDemand = REG_DWORD 0(False) -> 1
조치방법	위에 명시된 레지스트리 값을 추가 또는, 변경하여 적용함
점검 및 조치 사례	

레지스트리 값 이름	설 명
SynAttackProtect	SYN-ACK 패킷의 기다리는 시간을 줄여 SYN 공격에 대한 방어 기능 기능을 설정할 수 있음 • 0 => SynAttack 프로텍션을 사용하지 않음 • 1 => 재전송 시도를 줄이고, route 캐쉬 엔트리를 지연시킴 • 2 => 1의 기능 외에도 Winsock에 대한 지시(indication)를 지연시킴
EnableDeadGWDetect	EnableDeadGWDetect를 0으로 설정하지 않으면 서버가 강제로 원하지 않는 Gateway로 전환될 수 있음 • 0 => (False) 작동하지 않는 Gateway을 검색할 수 없음 • 1 => (True) 작동하지 않는 Gateway을 검색할 수 있음
KeepAliveTime	idle connection을 확인하기 위하여 얼마나 자주 Keep-alive 패킷을 보낼지를 결정하는 값임 • 기본 값 => 7,200,000(2시간) • 권장 값 => 300,000(5분)
NoNameReleaseOnDemand	컴퓨터가 이름 해제 요청을 받을 때 NetBIOS 이름 해제 여부를 결정하는 설정으로 이 값은 관리자가 악의적인 이름 해제 공격으로부터 컴퓨터를 보호할 수 있음. • 0 => (False) 해당 기능 사용 안 함 • 1 => (True) 해당 기능 사용

W-72 (상)	5. 보안 관리 > DoS 공격 방어 레지스트리 설정

- Windows NT, 2000, 2003, 2008, 2012

Step 1) 시작> 실행> REGEDIT

Step 2) HKLM₩System₩CurrentControlSet₩Services₩Tcpip₩Parameters₩ 검색

Step 3) 다음의 DOS 방어 레지스트리 값 추가 또는, 변경

레지스트리 값 이름	값 종류	유효 범위	권장 설정 값
SynAttackProtect	REG_DWORD	0, 1, 2	1 또는 2
EnableDeadGWDetect	REG_DWORD	0, 1 (False, True)	0 (False)
KeepAliveTime	REG_DWORD	1 - 0xFFFFFFFF	300,000(5분)으로 변경
NoNameReleaseOnDemand	REG_DWORD	0, 1 (False, True)	1 (True)

조치 시 영향	잘못된 값을 설정할 경우 OS 재설치를 요구할 수 있음

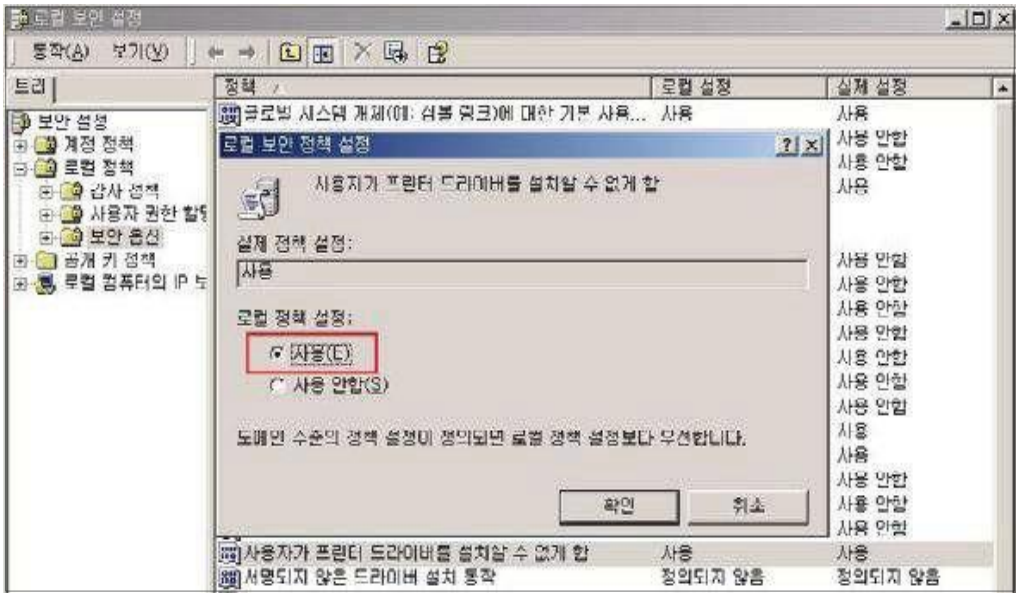
5.12. 사용자가 프린터 드라이버를 설치할 수 없게 함

W-73 (중)	5. 보안 관리 > 사용자가 프린터 드라이버를 설치할 수 없게 함
취약점 개요	
점검내용	• 사용자의 프린터 드라이버 설치 차단 여부 점검
점검목적	• 일반 사용자를 통한 프린터 드라이버 설치를 차단하여 의도하지 않은 시스템 손상을 방지하기 위함
보안위협	• 서버에 프린터 드라이버를 설치하는 경우 악의적인 사용자가 고의적으로 잘못된 프린터 드라이버를 설치하여 컴퓨터를 손상시킬 수 있으며, 프린터 드라이버 로 위장한 악성 코드를 설치할 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책
	취약 : "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책이 "사용 안 함"인 경우
조치방법	사용자가 프린터 드라이버를 설치할 수 없게 함 -+ 사용
점검 및 조치 사례	

• Windows NT, 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "사용자가 프린터 드라이버를 설치할 수 없게 함" 정책을 "사용" 으로 설정

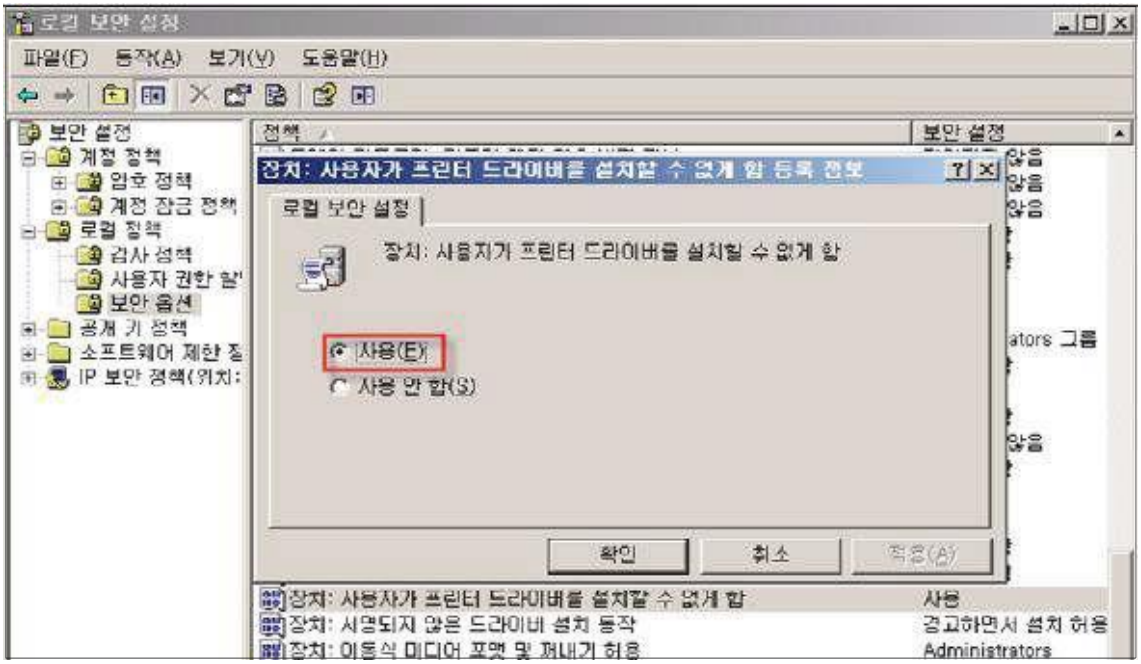


W-73 (중)	5. 보안 관리 > 사용자가 프린터 드라이버를 설치할 수 없게 함

- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "장치: 사용자가 프린터 드라이버를 설치할 수 없게 함" 정책을 "사용" 으로설정

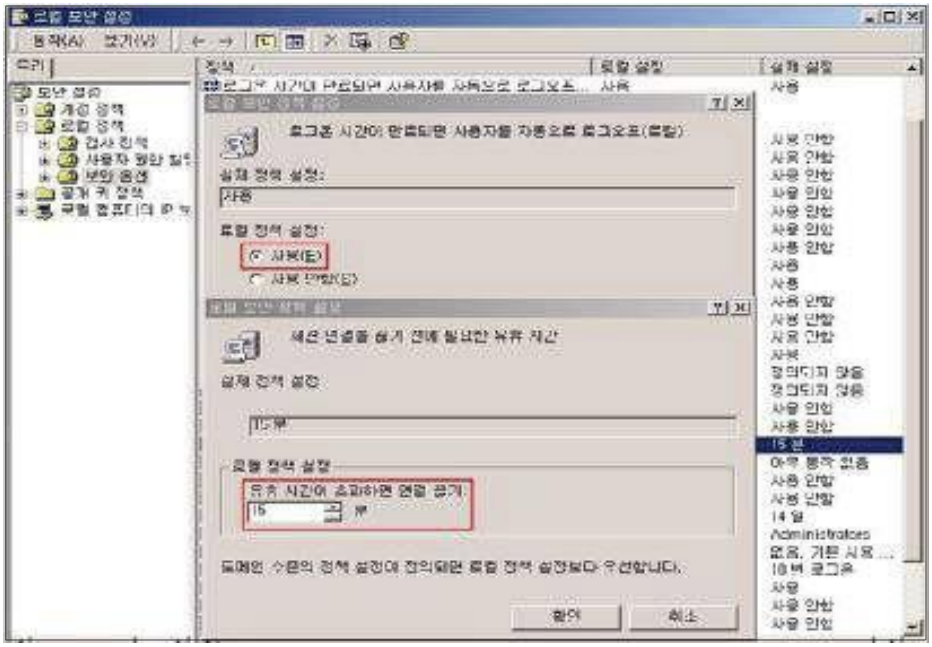


조치 시 영향	일반적인 경우 영향 없음

5.13. 세션 연결을 중단하기 전에 필요한 유휴시간

W-74 (중)	5. 보안 관리 > 세션 연결을 중단하기 전에 필요한 유휴시간
취약점 개요	
점검내용	• 세션 연결 중단 시 유휴시간 설정 여부 점검
점검목적	• 세션이 중단되기 전에 SMB(서버 메시지 블록) 세션에서 보내야 하는 연속 유휴 시간을 결정하여 서비스 거부 공격 등에 악용되지 않도록 하기 위함
보안위협	• SMB 세션에서는 서버 리소스를 사용하며, null(공백) 세션수가 많으면 서버 속도가 느려지거나 서버에 오류를 발생시킬 수 있으므로 공격자는 이를 악용하여 SMB 세션을 반복 설정하여 서버의 SMB 서비스가 느려지거나 응답하지 않게 하여 서비스 거부 공격을 실행 할 수 있음
참고	※ Administrator는 이 정책을 활성화하여 컴퓨터가 비활성 SMB 세션을 중단하는 시점을 제어할 수 있으며, 클라이언트를 다시 시작하면 해당 세션은 자동으로 다시 연결됨. 이 정책의 값을 0으로 설정하면 가능한 한 빨리 유휴 세션 연결은 끊어지며, 최대 값은 99999(208일)로 사실상 정책 설정 해제를 의미함 ※ SMB(서버 메시지 블록): LAN이나 컴퓨터 간의 통신에서 데이터 송수신을 하기 위한 프로토콜
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책을 "사용"으로, "세션 연결을 중단하기 전에 필요한 유휴 시간" 정책을 "15분"으로 설정한 경우
	취약 : "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책이 "사용 안 함"으로, "세션 연결을 중단하기 전에 필요한 유휴 시간" 정책이 "15분"으로 설정되어 있지 않은 경우
조치방법	로그온 시간이 만료되면 클라이언트 연결 끊기 -+ 사용 세션 연결을 중단하기 전에 필요한 유휴 시간 -+ 15분
점검 및 조치 사례	
• Windows NT, 2000 Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션 Step 2) "로그인 시간이 만료되면 클라이언트 연결 끊기" 정책 "사용" 설정 "세션 연결을 중단하기 전에 필요한 유효 시간" 정책 "15분" 설정	

W-74 (중)	5. 보안 관리 > 세션 연결을 중단하기 전에 필요한 유휴시간

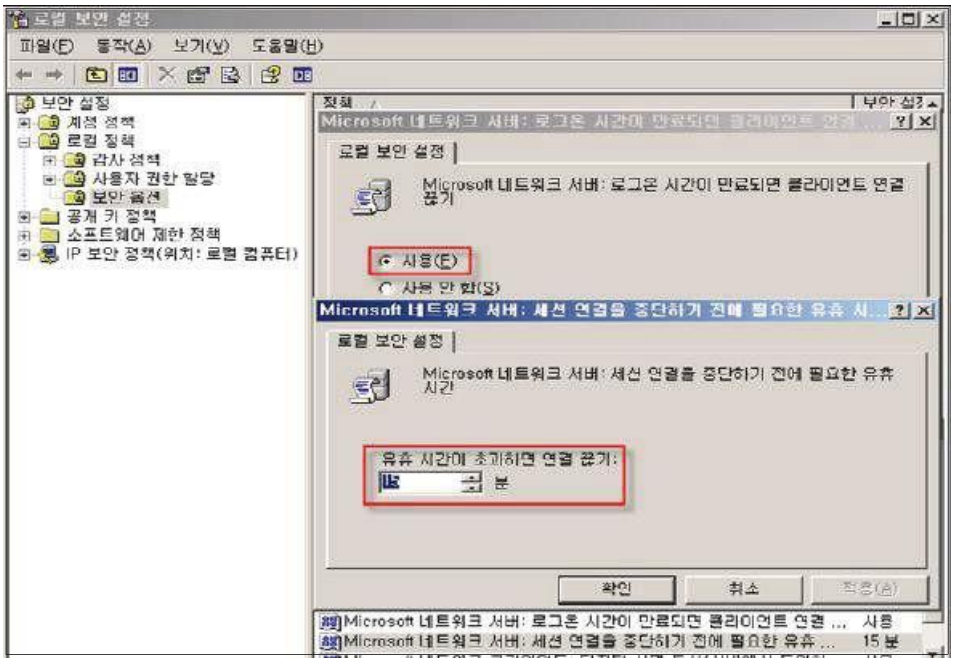


- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책 "사용" 설정

"세션 연결을 중단하기 전에 필요한 유휴 시간" 정책 "15분" 설정



조치 시 영향	일반적인 경우 영향 없음

5.14. 경고 메시지 설정

W-75 (하)	5. 보안 관리 > 경고 메시지 설정
취약점 개요	
점검내용	• 로그온 시 경고 메시지 출력 여부 점검
점검목적	• 로그온 시 경고 메시지를 설정하여 시스템에 로그온을 시도하는 사용자들에게 관리자는 시스템의 불법적인 사용에 대하여 경고 창을 띄움으로써 경각심을 주기 위함
보안위협	• 로그온 경고 메시지가 없는 경우 악의적인 사용자에게 관리자가 적절한 보안수준으로 시스템을 보호하고 있으며, 공격자의 활동을 주시하고 있다는 생각을 상기 시킬 수 없어 간접적인 공격 기회를 제공할 우려 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 로그인 경고 메시지 제목 및 내용이 설정되어 있는 경우
	취약 : 로그인 경고 메시지 제목 및 내용이 설정되어 있지 않은 경우
조치방법	로그인 메시지 제목 및 메시지 내용에 경고 문구 삽입
점검 및 조치 사례	

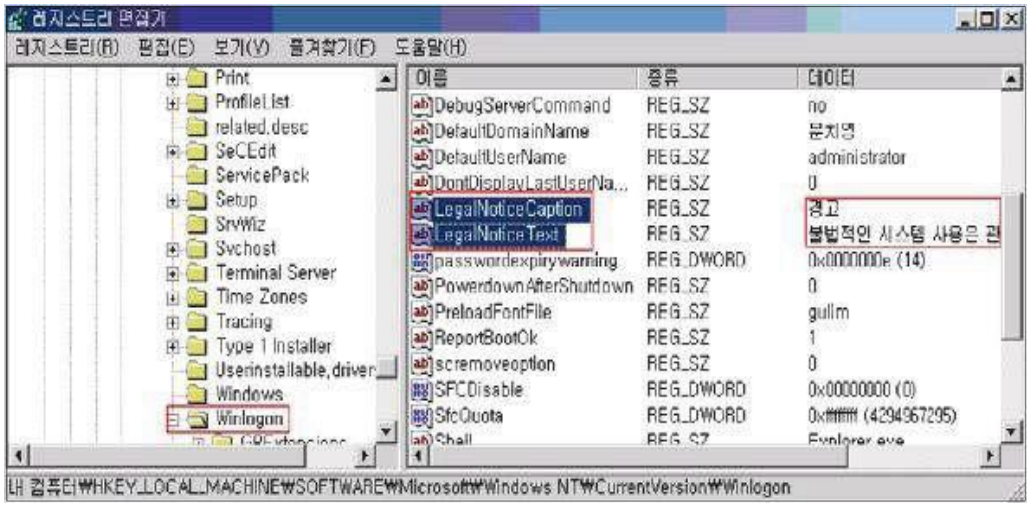
• Windows NT

Step 1) HKEY_LOCAL_MACHINE₩SOFTWARE₩Microsoft₩WindowsNT₩CurrentVersion ₩Winlogon

Step 2) LegalNoticeCaption: 제목

Step 3) LegalNoticeText: 메시지 내용

※ 이저럼 변경된 레지스트리 키의 내용은 시스템을 로그오프 한 후 반영됨



W-75 (하)	5. 보안 관리 > 경고 메시지 설정

- Windows 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) 로그온 시도하는 사용자에 대한 메시지 제목: 배너 제목 입력

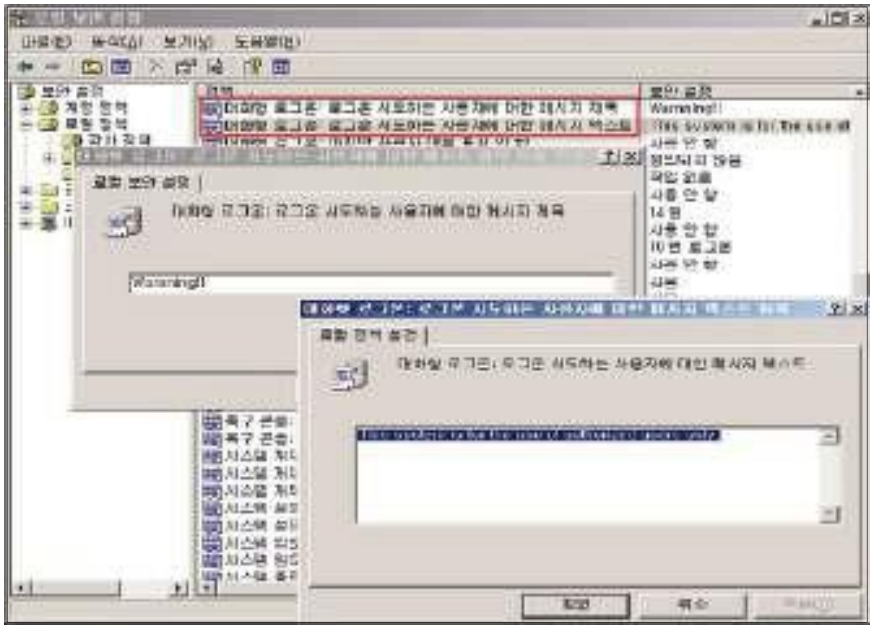
Step 3) 로그온 시도하는 사용자에 대한 메시지 텍스트: 배너 내용 입력

- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) 대화형 로그온: 로그온 시도하는 사용자에 대한 메시지 제목: 배너 제목 입력

Step 3) 대화형 로그온: 로그온 시도하는 사용자에 대한 메시지 텍스트: 배너 내용 입력



조치 시 영향	일반적인 경우 영향 없음

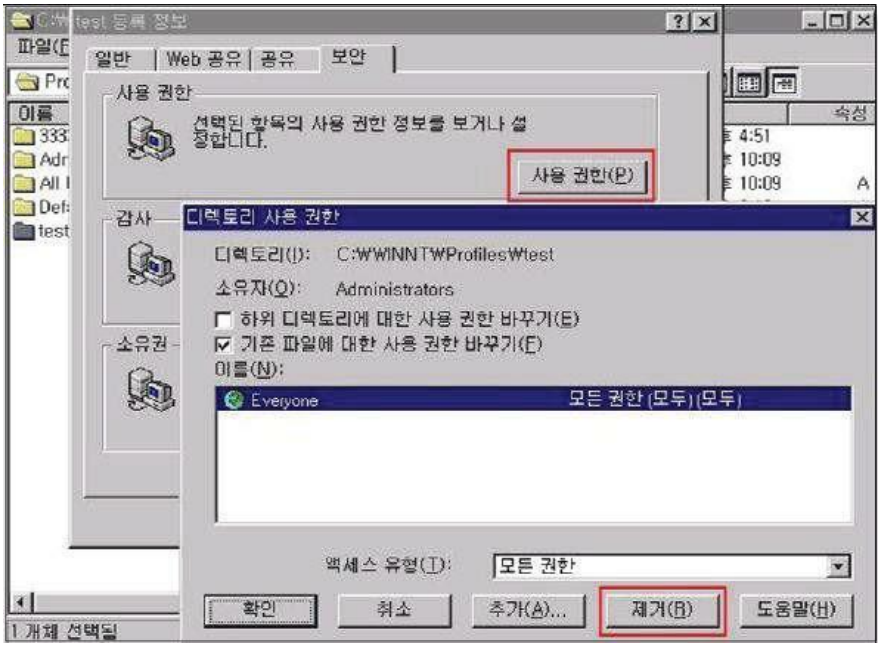
5.15. 사용자별 홈 디렉터리 권한 설정

W-76 (중)	5. 보안 관리 > 사용자별 홀 디렉토리 권한 설정
취약점 개요	
점검내용	• 사용자 홈 디렉토리 권한 적절성 점검
점검목적	• 사용자 홈 디렉토리에 적절한 권한을 부여하여 비인가 사용자에 의한 불필요한 정보 노출을 방지하기 위함
보안위협	• 사용자 계정별 홈 디렉토리의 권한이 제한되어 있지 않은 경우 임의의 사용자나 다른 사용자의 홈 디렉토리에 악의적인 목적으로 접근할 수 있으며, 접근 후 의도 또는, 의도하지 않은 행위로 시스템에 악영향을 미칠 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 홈 디렉토리에 Everyone 권한이 없는 경우 (All Users, Default User 디렉토리 제외)
	취약 : 홈 디렉토리에 Everyone 권한이 있는 경우
조치방법	Everyone 권한 제거
점검 및 조치 사례	

• Windows NT

Step 1) Windows NT: C:₩WinNT₩Profiles₩사용자 홈 디렉토리> 등록 정보> 보안

Step 2) Everyone 권한 제거(All Users, Default User 디렉토리는 제외)

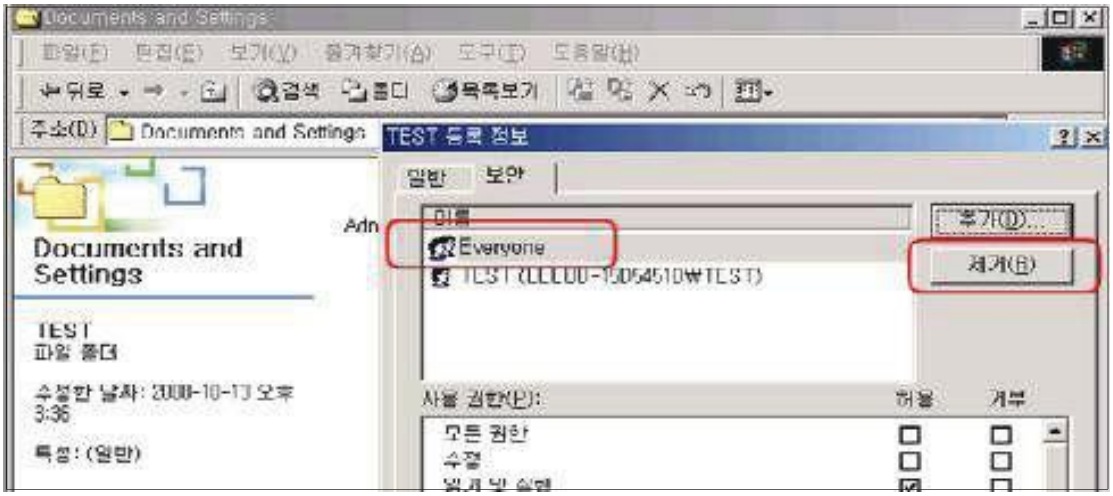


W-76 (중)	5. 보안 관리 > 사용자별 홈 디렉토리 권한 설정

- Windows 2000, 2003

Step 1) C:₩Documents and SettingsW사용자 홈 디렉토리> 속성> 보안

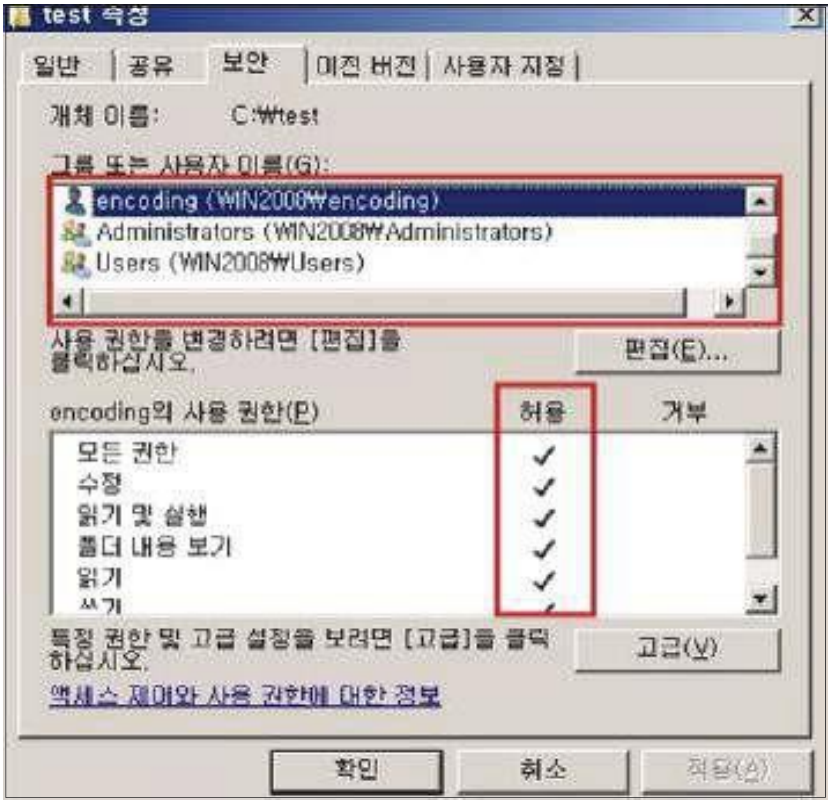
Step 2) Everyone 권한 제거(All Users, Default User 디렉토리는 제외)



- Windows 2008

Step 1) C:₩사용자₩<사용자 계정>

Step 2) 해당 사용자에 대한 권한 외 일반 계정 삭제

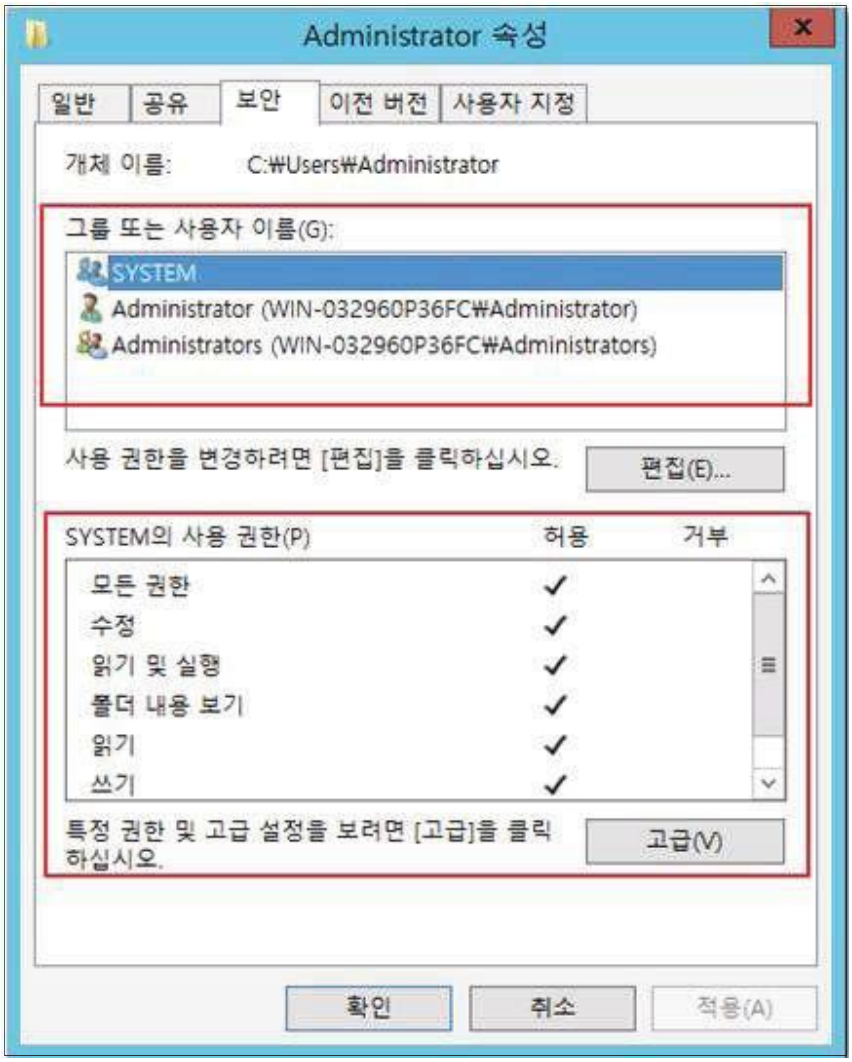


W-76 (중)	5. 보안 관리 > 사용자별 홈 디렉토리 권한 설정

- Windows 2012

Step 1) C:₩사용자₩<사용자 계정>

Step 2) 해당 사용자에 대한 권한 외 일반 계정 삭제



조치 시 영향	일반적인 경우 영향 없음

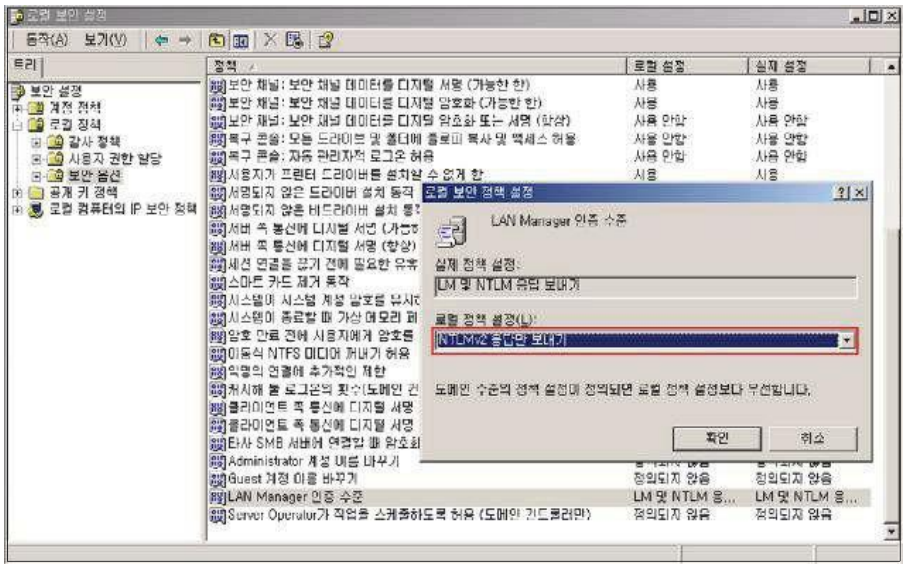
5.16. LAN Manager 인증 수준

W-77 (중)	5. 보안 관리 > LAN Manager 인증 수준
취약점 개요	
점검내용	• LAN Manager 인증 수준 적절성 점검
점검목적	• Lan Manager 인증 수준 설정을 통해 네트워크 로그온에 사용할 Challenge/Response 인증 프로토콜을 결정하며, 안전한 인증 절차를 적용하기 위함
보안위협	• 안전하지 않은 LAN Manager 인증 수준을 사용하는 경우 인증 트래픽을 가로채기를 통해 악의적인 계정 정보 노출을 허용할 수 있음
참고	※ LAN Manager는 네트워크를 통한 파일 및 프린터 공유 등과 같은 작업 시 인증을 담당. NTLMv2는 Windows 2000, 2003, XP 이상에서 지원되며, Windows 98, NT 버전과 통신할 경우 패치를 설치하여야 함
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : "LAN Manager 인증 수준" 정책에 "NTLMv2 응답만 보냄"이 설정되어 있는 경우
	취약 : "LAN Manager 인증 수준" 정책에 "LM" 및 "NTLM"인증이 설정되어 있는 경우
조치방법	Windows 2000: LAN Manager 인증 7수준 -> NTLMv2 응답만 보냄 Windows 2003: 네트워크 보안: LAN Manager 인증 수준 -> NTMLv2 응답만 보냄 Windows 2008: 네트워크 보안: LAN Manager 인증 수준 -> NTMLv2 응답만 보냄 Windows 2012: 네트워크 보안: LAN Manager 인증 수준 -> NTMLv2 응답만 보냄
점검 및 조치 사례	

• Windows NT, 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "LAN Manager 인증 수준" 정책에 "NTLMv2 응답만 보내기" 설정

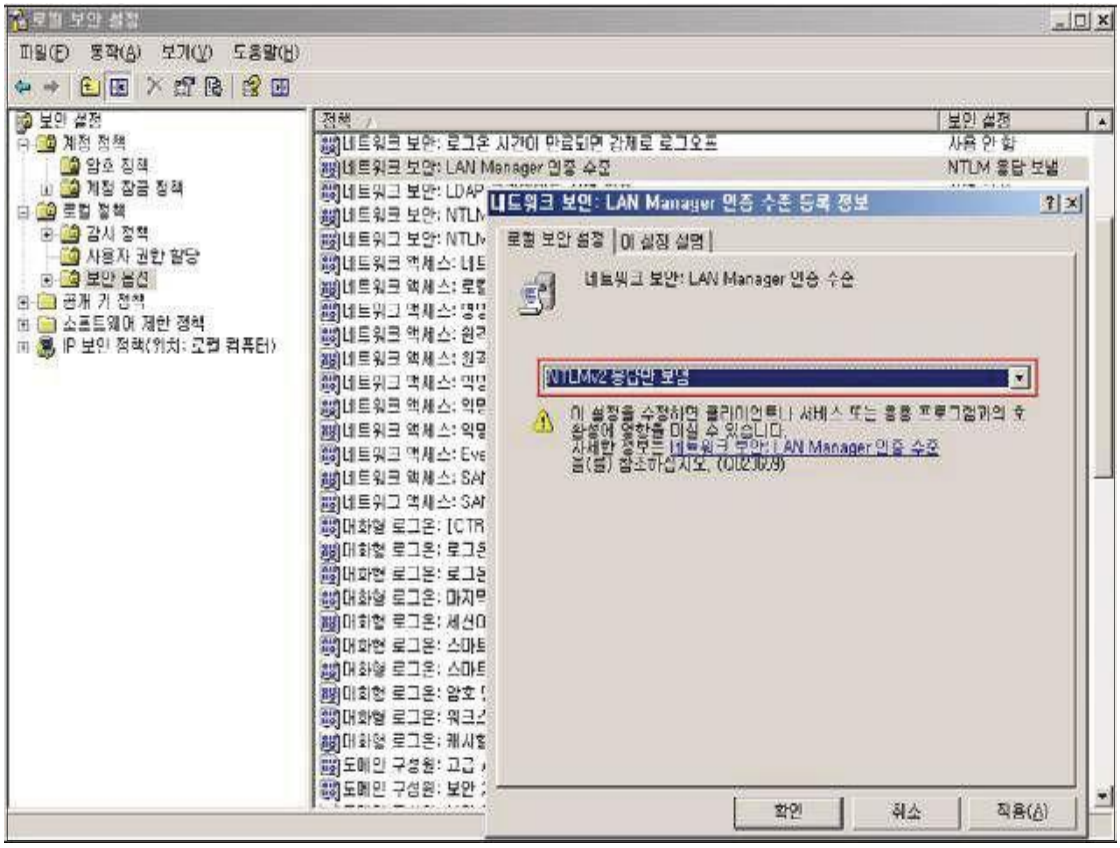


W-77 (중)	5. 보안 관리 > LAN Manager 인증 수준

- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) "네트워크 보안: LAN Manager 인증 수준" 정책에 NTLMv2 응답만 보냄" 설정



조치 시 영향	일반적인 경우 영향 없음

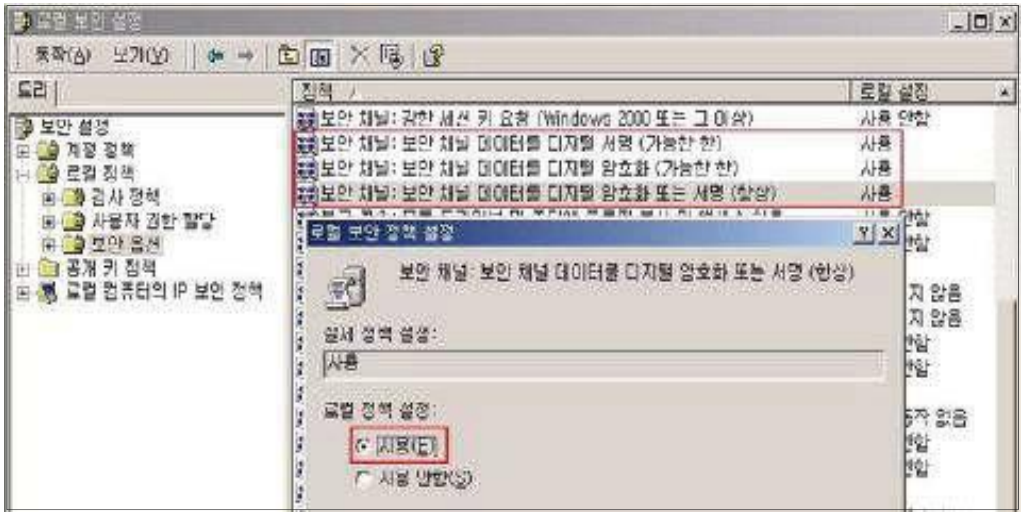
5.17. 보안 채널 데이터 디지털 암호화 또는 서명

W-78 (중)	5. 보안 관리 > 보안 채널 데이터 디지털 암호화 또는 서명
취약점 개요	
점검내용	• 'Windows 채널 데이터 디지털 암호화 또는 서명' 정책 적절성 점검
점검목적	• 해당 정책을 활성화하여 보안 채널의 서명 또는 암호화가 협상되지 않는 한 보안 채널을 확립하지 않기 위함
보안위협	• 보안 채널이 암호화 되지 않은 경우 인증 트래픽 끼어들기 공격, 반복 공격 및 기타 유형의 네트워크 공격 등의 위험 존재
참고	-
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : 아래 3가지 정책이 "사용"으로 되어 있는 경우
	취약 : 아래 3가지 정책이 "사용 안 함" 으로 되어 있는 경우 • 도메인 구성원: 보안 채널 데이터를 디지털 암호화 또는, 서명(항상) • 도메인 구성원: 보안 채널 데이터를 디지털 암호화(가능한 경우) • 도메인 구성원: 보안 채널 데이터를 디지털 서명(가능한 경우)
조치방법	보안 채널 데이터를 디지털 암호화·서명 관련 3개 정책 -+ 사용
점검 및 조치 사례	

• Windows NT, 2000

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

Step 2) 위 3가지 정책을 모두 "사용"으로 설정



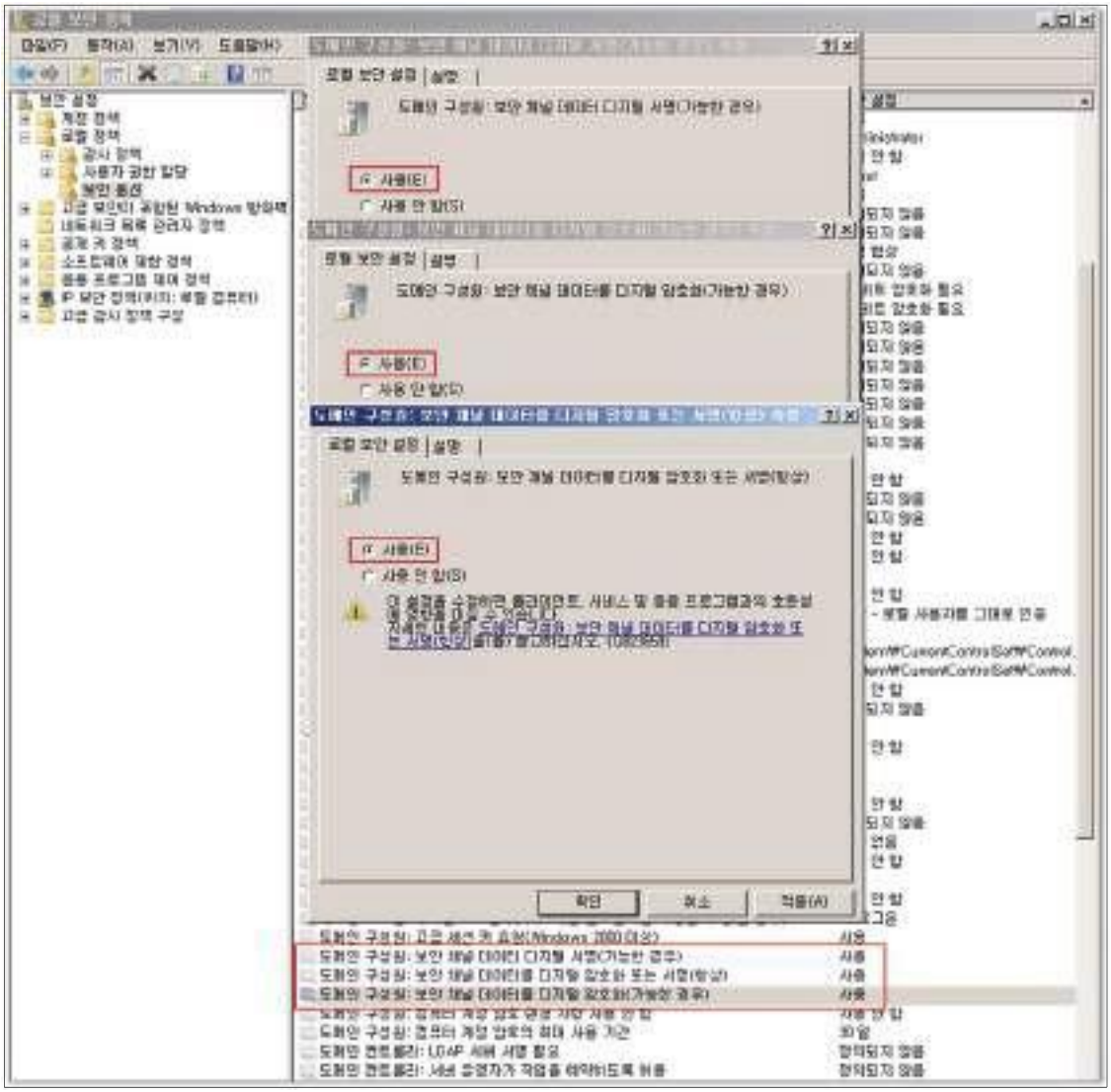
W-78 (중)	5. 보안 관리 > 5.17 보안 채널 데이터 디지털 암호화 또는 서명

- Windows 2003, 2008, 2012

Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션

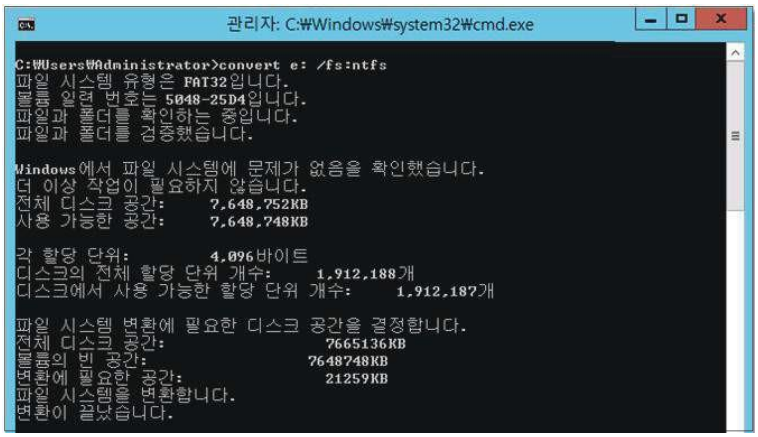
Step 2) 아래 3가지 정책을 모두 "사용" 으로 설정

- 도메인 구성원: 보안 채널 데이터를 디지털 암호화 또는, 서명 (항상)
- 도메인 구성원: 보안 채널: 보안채널 데이터를 디지털 서명 (가능하면)
- 도메인 구성원: 보안 채널: 보안채널 데이터를 디지털 암호화 (가능하면)



조치 시 영향	도메인 구성원만 해당되며, Windows 98/NT와 파일 및 프린터 공유 등의 작업을 하지 않는 경우 일반적으로 영향 없음

5.18. 파일 및 디렉터리 보호

W-79 (중)	5. 보안 관리 > 파일 및 디렉토리 보호
취약점 개요	
점검내용	• NTFS 파일 시스템 사용 여부 점검
점검목적	• FAT 파일 시스템에 비해 보다 강화된 보안 기능을 제공하는 파일 시스템을 사용하기 위함 (파일과 디렉토리에 소유권과 사용 권한 설정이 가능하고 ACL(접근 통제 목록)을 제공)
보안위협	• FAT 파일 시스템 사용 시 사용자별 접근 통제를 적용할 수 없어 중요 정보에 대한 책임 추적성 확보가 어려움
참고	※ 기존에 FAT 파일 시스템을 사용하다가 NTFS로 변환하기 위해서는 `convert.exe` 명령을 사용할 수 있지만 FAT 파일 시스템으로 운영 중 변환해야 하는 경우 Default ACL이 적용되지 않으므로 가능한 초기 설치 시 NTFS 파일 시스템을 선택하는 것을 권장함 ※ 최근 운영체제 버전에서는 FAT32 파일 시스템을 지원하지 않으나 기존 FAT32 에서 NTFS 변환 가능 ※ NTFS, FAT 파일 시스템 비교: FAT32에는 NTFS가 제공하는 보안 기능이 없으므로 컴퓨터에 FAT32 파티션 또는, 볼륨이 있는 경우 컴퓨터에 액세스 가능한 모든 사용자가 파일을 읽을 수 있으며 FAT32에는 크기 제한이 있음.
점검대상 및 판단기준	
대상	• Windows NT, 2000, 2003, 2008, 2012
판단기준	양호 : NTFS 파일 시스템을 사용하는 경우
	취약 : FAT파일 시스템을 사용하는 경우
조치방법	FAT파일 시스템을 사용하고 있다면, 가급적 NTFS 파일 시스템으로 변환
점검 및 조치 사례	
• Windows 2003, 2008, 2012 Step 1) 명령어프롬프트(DOS창)에서 다음과 같이 입력 시작> 실행> CMD> convert 드라이브명: /fs:ntfs (예) convert F: /fs/ntfs라고 입력하면 F 드라이브는 NTFS 형식으로 포맷 됨  	
조치 시 영향	파일시스템을 변환할 경우 기존 파일시스템에 영향을 줄 수 있음

5.19. 컴퓨터 계정 암호 최대 사용 기간

W-80 (중)	5. 보안 관리 > 컴퓨터 계정 암호 최대 사용 기간
취약점 개요	
점검내용	• 컴퓨터 계정 암호 최대 사용 기간 설정 여부 점검
점검목적	• 컴퓨터 계정 암호 최대 사용 기간을 설정하기 위함
보안위협	• 기본적으로 도메인 구성원은 도메인 암호 변경 주기가 적절하지 않은 경우공격자가 무단 공격을 실행하여 하나 이상의 컴퓨터 계정 암호를 추측하기에 충분한 시간을 제공할 수 있음
참고	※ 도메인 구성원이 해당 컴퓨터 계정 암호를 정기적으로 변경할지를 결정할 수 있으며, 기본적으로 도메인 구성원이 사용하는 도메인 암호 변경 기간은 '자동'으로 설정되어 있음
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : "컴퓨터 계정 암호 변경 사용 안 함" 정책을 사용하지 않으며, "컴퓨터 계정 암호 최대 사용 기간" 정책이 "90일"로 설정되어 있는 경우
	취약 : "컴퓨터 계정 암호 변경 사용 안 함" 정책이 "사용"으로 설정되어 있거나 "컴퓨터 계정 암호 최대 사용 기간" 정책이 "90일" 로 설정되어 있지 않은 경우
조치방법	컴퓨터 계정 암호 변경 사용 안 함 -+ 사용 안 함 컴퓨터 계정 암호 최대 사용 기간 -+ 90일
점검 및 조치 사례	
• Windows 2003, 2008, 2012 Step 1) 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션 Step 2) 컴퓨터 계정 암호 변경 사용 안 함 -+ 사용 안 함 컴퓨터 계정 암호 최대 사용 기간 -+ 90일 ※ Windows Server 2000 이하 버전 해당 사항 없음 	
조치 시 영향	도메인 구성원만 해당되며 일반적으로 영향 없음

5.20. 시작프로그램 목록 분석

W-81 (중)	5. 보안 관리 > 시작프로그램 목록 분석
취약점 개요	
점검내용	• 시작프로그램 목록 내 불필요한 항목 존재 여부 점검
점검목적	• 불필요한 시작 프로그램을 삭제하거나 비활성화 하여 악의적인 공격을 차단하기 위함
보안위협	• 윈도우 부팅 시 너무 많은 시작프로그램이 동시에 실행되면 속도가 저하되는 문제가 발생하며, 공격자가 심어놓은 악성 프로그램이나 해킹 툴이 실행되어 시 스템에 피해를 줄 수 있음
참고	-
점검대상 및 판단기준	
대상	• Windows 2000, 2003, 2008, 2012
판단기준	양호 : 시작프로그램 목록을 정기적으로 검사하고 불필요한 서비스 체크 해제를 한 경우
	취약 : 시작프로그램 목록을 정기적으로 검사하지 않고, 부팅 시 불필요한 서비스도 실행되고 있는 경우
조치방법	시작프로그램 목록의 정기적인 검사 실시 및 불필요한 서비스 비활성화
점검 및 조치 사례	
• Windows 2000, 2003, 2008 Step 1) 시작> 검색> msconfig 명령어 입력 Step 2) 시작 프로그램 탭 클릭> 시작 프로그램 목록 중 불필요하거나 의심스러운 항목 체크 표시 해제 • Windows 2012 Step 1) 2012 서버의 경우 시작프로그램 목록 편집이 불가능하며 별도의 편집이나 등록을 위해서는 배치파일이나 레지스트리 값 추가를 이용해서 개인화를 통해 사용할 수 있으나 보안상 권장하지 않음.	
조치 시 영향	일반적인 경우 영향 없음

6. DB 관리

6.1. Windows 인증 모드 사용

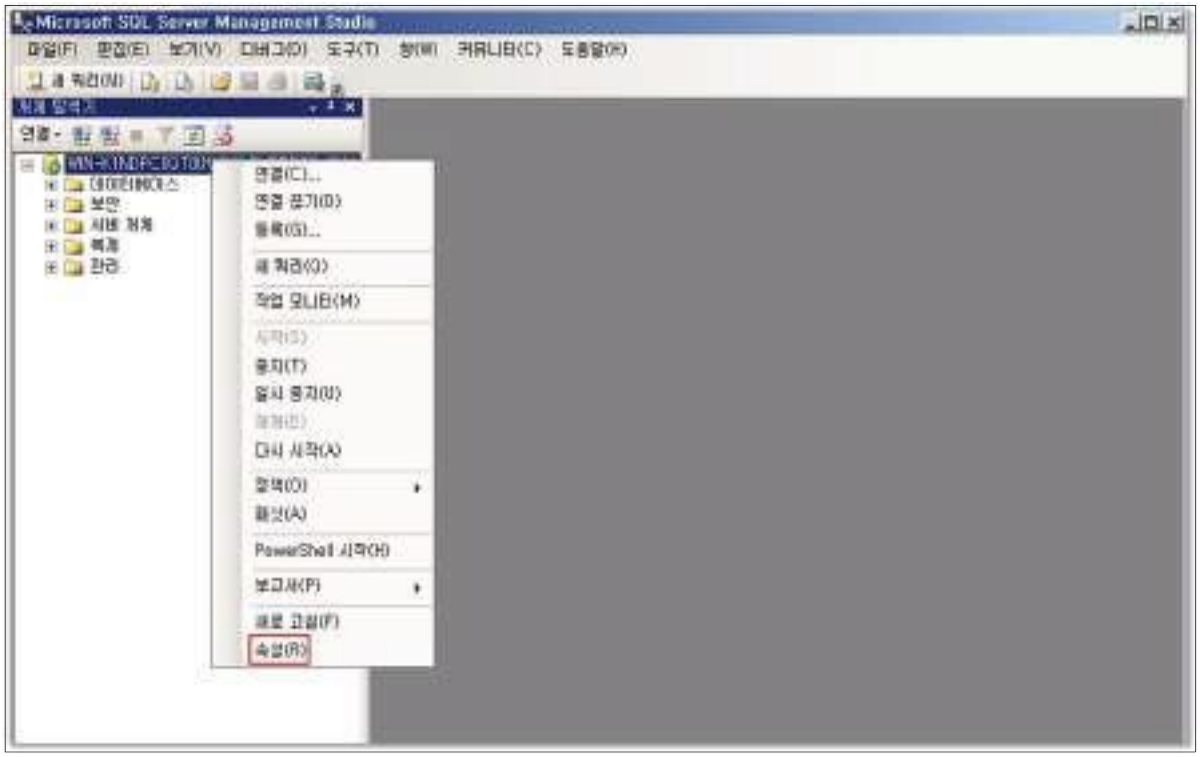
W-82 (중)	6. DB 관리 > Windows 인증 모드 사용
취약점 개요	
점검내용	• DB 로그인 시 Windows 인증 모드 적절성 점검
점검목적	• 적절한 Windows 인증 모드를 적용하여 적합한 복잡성 수준을 유지하기 위함
보안위협	• 혼합 인증모드를 사용하고 sa 계정이 활성화 되어 있는 경우, 잘 알려진 sa 계정에 대한 계정 추측 공격의 우려 존재
참고	※ 데이터베이스 엔진 인증 모드에는 Windows 인증 모드와 SQL Sever가 있는 혼합 모드 두 가지 구성이 있음. Windows 인증 모드 선택 시 SQL Sever 인증을 위해서 설치 프로그램은 sa라는 비활성화 된 계정을 생성하고, 이 계정은 혼합 모드를 사용함으로써 활성화 됨. sa 계정은 일반 사용자들에게 잘 알려진 만큼 쉽게 공격의 대상이 될 수 있으므로 꼭 필요하지 않는 경우 비활성화 하고, 만약 필요하다면 강력한 암호 체계를 사용하여야 함 ※ Windows 인증은 kerberos 보안프로토콜을 사용하며, 강력한 암호정책을 적용하여 적합한 복잡성 수준을 유지함. 또한, 계정 잠금 및 암호만료를 지원하고 SQL 서버가 Windows에서 제공하는 자격증명을 신뢰한 트러스트 연결을 사용하기 때문에 Windows 인증 모드 사용을 권고함 ※ sa 계정: 데이터베이스 서버 설치 시 자동으로 생성되며 DB서버 관리자 계정 ※ kerberos 보안프로토콜: 개방된 컴퓨터 네트워크 내에서 서비스 요구를 인증하기 위한 보안 시스템
점검대상 및 판단기준	
대상	• Windows 2003, 2008, 2012
판단기준	양호 : Windows 인증 모드를 사용하고 sa계정이 비활성화되어 있는 경우 sa계정 사용 시 강력한 암호정책을 설정한 경우
	취약 : 혼합 인증 모드를 사용하고, 활성화 된 sa 계정에 대해 강력한 암호정책 설정을 하지 않은 경우
조치방법	Windows 인증 모드 사용
점검 및 조치 사례	
• Windows 만 인증 활성화 < SQL Server 2005> Step 1) 우클릭> 서버> 등록 정보> 보안 탭> 인증> 인증 모드> Windows만[W]를 클릭하여 활성화시킴  	

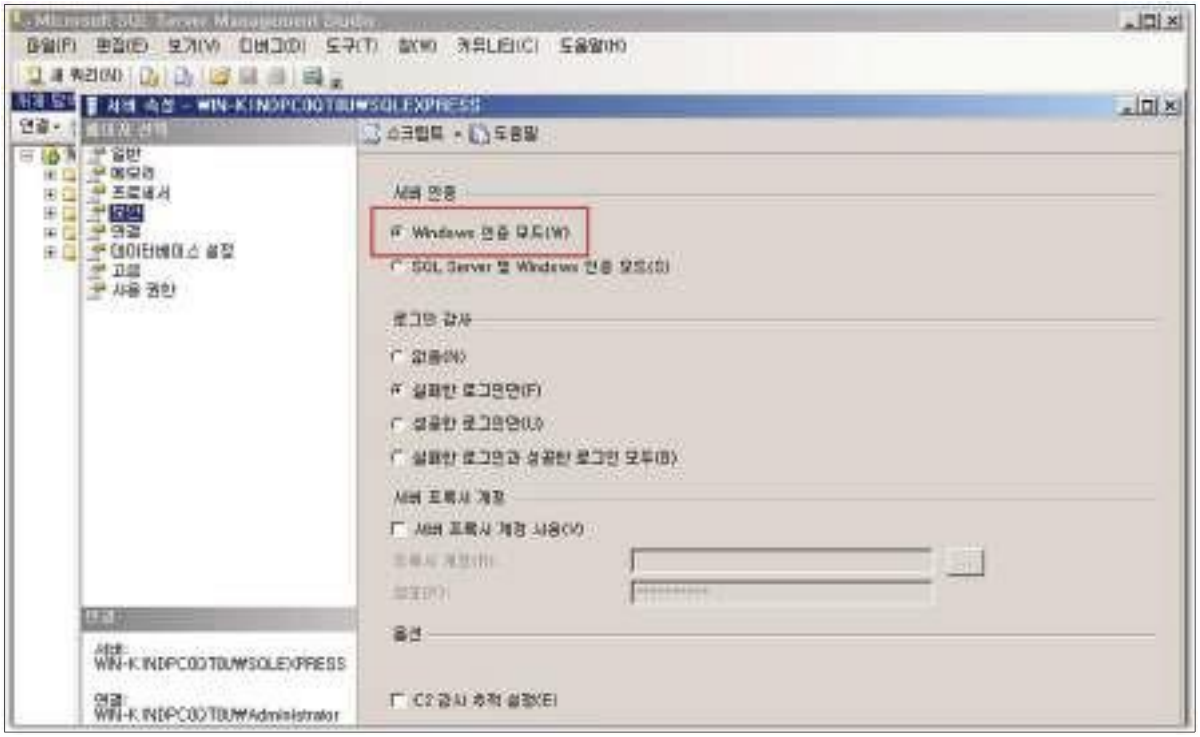
W-82 (중)	6. DB 관리 > Windows 인증 모드 사용

< SQL Server 2008>

Step 1)

SQL Server 매니저 스튜디오> 해당 서버 우클릭> 속성> 보안> Windows 인증 활성화

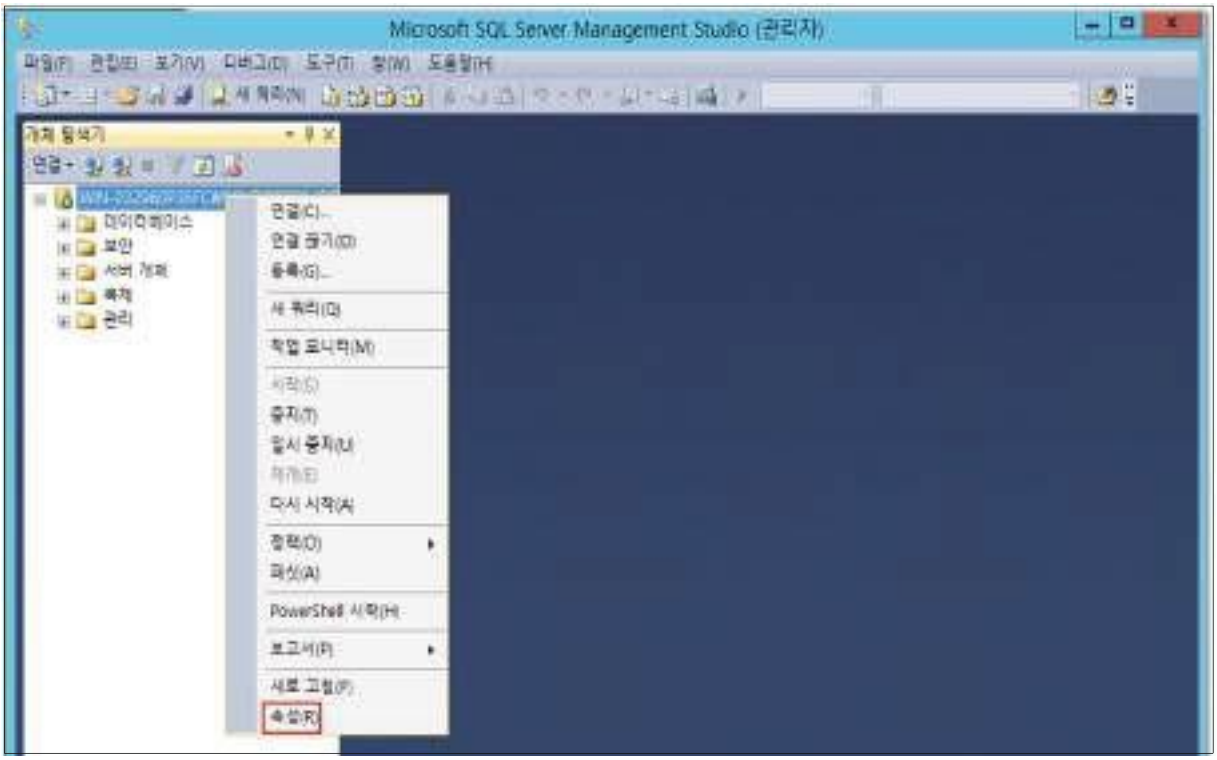


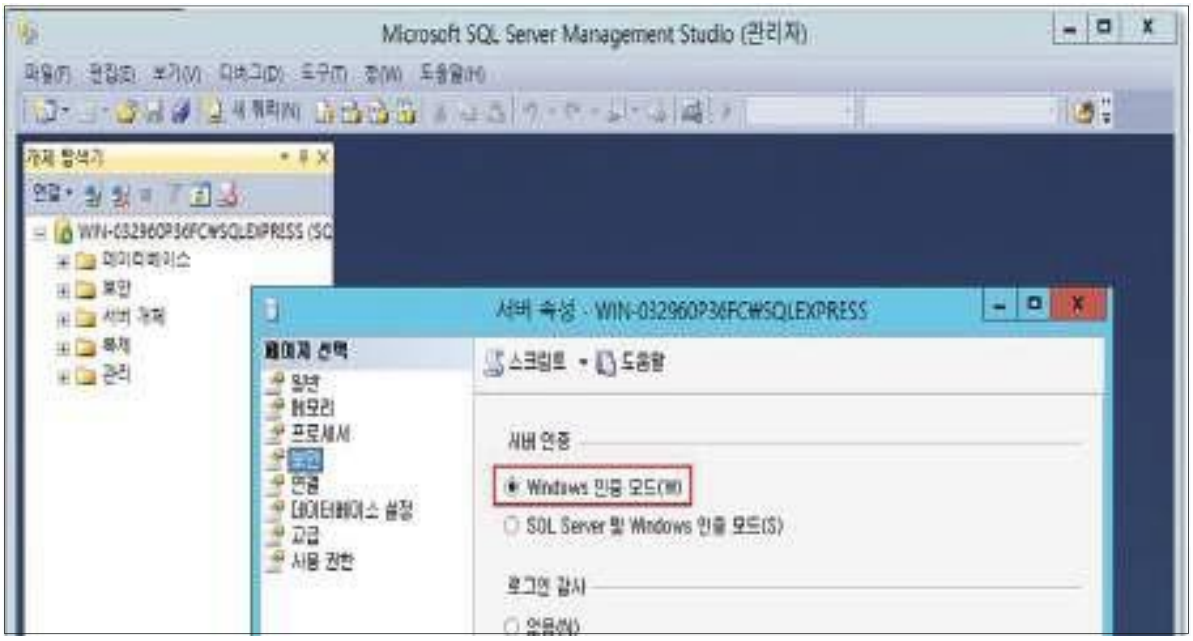


W-82 (중)	6. DB 관리 > Windows 인증 모드 사용

< SQL Server 2012>

Step 1) SQL Server 매니저 스튜디오> 해당서버 우클릭> 속성> 보안 탭> 서버 인증> Windows 인증 모드(W)를 클릭하여 활성화시킴





조치 시 영향	일반적인 경우 영향 없음