

취약점 진단 보고서
(Window 2003)

이헌진

목 차

1. Windows 서버 취약점 분석 · 평가 항목

2. 취약점 항목

2.1 계정 관리

2.2 서비스 관리

2.3 패치 관리

2.4 로그 관리

2.5 보안 관리

2.6 DB 관리

1. Windows 서버 취약점 분석 · 평가 항목

윈도우즈 서버 취약점 분석 · 평가 항목				
분류	점검항목	항목 중요도	항목코드	점검
1. 계정관리	Administrator 계정 이름 바꾸기	상	W-01	X
	Guest 계정 상태	상	W-02	O
	불필요한 계정 제거	상	W-03	X
	계정 잠금 임계값 설정	상	W-04	X
	해독 가능한 암호화를 사용하여 암호 저장	상	W-05	O
	관리자 그룹에 최소한의 사용자 포함	상	W-06	X
	Everyone 사용 권한을 익명 사용자에게 적용	중	W-07	O
	계정 잠금 기간 설정	중	W-08	X
	패스워드 복잡성 설정	중	W-09	X
	패스워드 최소 암호 길이	중	W-10	X
	패스워드 최대 사용 기간	중	W-11	O
	패스워드 최소 사용 기간	중	W-12	X
	마지막 사용자 이름 표시 안함	중	W-13	X
	로컬 로그인 허용	중	W-14	X
	익명 SID/이름 변환 허용	중	W-15	O
	최근 암호 기억	중	W-16	X
	콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한	중	W-17	O
	원격 터미널 접속 가능한 사용자 그룹 제한	중	W-18	O
2. 서비스 관리	공유 권한 및 사용자 그룹 설정	상	W-19	O
	하드디스크 기본 공유 제거	상	W-20	X
	불필요한 서비스 제거	상	W-21	O
	IIS 서비스 구동 점검	상	W-22	O
	IIS 디렉토리 리스팅 제거	상	W-23	O
	IIS CGI 실행 제한	상	W-24	O
	IIS 상위 디렉토리 접근 금지	상	W-25	O
	IIS 불필요한 파일 제거	상	W-26	O
	IIS 웹 프로세스 권한 제한	상	W-27	O
	IIS 링크 사용금지	상	W-28	O
	IIS 파일 업로드 및 다운로드 제한	상	W-29	O
	IIS DB 연결 취약점 점검	상	W-30	O
	IIS 가상 디렉토리 삭제	상	W-31	O

	IIS 데이터 파일 ACL 적용	상	W-32	O
	IIS 미사용 스크립트 매핑 제거	상	W-33	O
	IIS Exec 명령어 쉘 호출 진단	상	W-34	O
	IIS WebDAV 비활성화	상	W-35	O
	NetBIOS 바인딩 서비스 구동 점검	상	W-36	O
	FTP 서비스 구동 점검	상	W-37	X
	FTP 디렉토리 접근 권한 설정	상	W-38	O
	Anonymous FTP 접근	상	W-39	X
	FTP 접근 제어 설정	상	W-40	X
	DNS Zone Transfer 설정	상	W-41	X
	RDS(RemoteDataServices)제거	상	W-42	O
	최신 서비스팩 적용	상	W-43	X
	터미널 서비스 암호화 수준 설정	중	W-44	O
	IIS 웹서비스 정보 숨김	중	W-45	O
	SNMP 서비스 구동 점검	중	W-46	O
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	W-47	O
	SNMP Access control 설정	중	W-48	O
	DNS 서비스 구동 점검	중	W-49	O
	HTTP/FTP/SMTP 배너 차단	하	W-50	X
	Telnet 보안 설정	중	W-51	O
	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거	중	W-52	O
	원격 터미널 접속 타임아웃 설정	중	W-53	X
	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중	W-54	O
3. 패치관리	최신 HOT FIX 적용	상	W-55	X
	백신 프로그램 업데이트	상	W-56	X
	정책에 따른 시스템 로깅 설정	중	W-57	O
4. 로그관리	로그의 정기적 검토 및 보고	상	W-58	O
	원격으로 액세스할 수 있는 레지스트리 경로	상	W-59	X
	이벤트 로그 관리 설정	하	W-60	O
	원격에서 이벤트 로그 파일 접근 차단	중	W-61	O
5. 보안관리	백신 프로그램 설치	상	W-62	X

	SAM 파일 접근 통제 설정	상	W-63	O
	화면보호기 설정	상	W-64	O
	로그온하지 않고 시스템 종료 허용	상	W-65	O
	원격 시스템에서 강제로 시스템 종료	상	W-66	O
	보안 감사를 로그할 수 없는 경우 즉시 시스템 종료	상	W-67	X
	SAM 계정과 공유의 익명 열거 허용 안 함	상	W-68	O
	Autologon 기능 제어	상	W-69	O
	이동식 미디어 포맷 및 꺼내기 허용	상	W-70	X
	디스크볼륨 암호화 설정	상	W-71	X
	DoS 공격 방어 레지스트리 설정	중	W-72	O
	사용자가 프린터 드라이버를 설치할 수 없게 함	중	W-73	O
	세션 연결을 중단하기 전에 필요한 유희시간	중	W-74	X
	경고 메시지 설정	하	W-75	O
	사용자별 홈 디렉터리 권한 설정	중	W-76	X
	LAN Manager 인증 수준	중	W-77	X
	보안 채널 데이터 디지털 암호화 또는 서명	중	W-78	O
	파일 및 디렉토리 보호	중	W-79	O
	컴퓨터 계정 암호 최대 사용 기간	중	W-80	O
	시작프로그램 목록 분석	중	W-81	O
6. DB 관리	Windows 인증 모드 사용	중	W-82	O

표 1 Windows 서버 취약점 분석 · 평가 항목

2. 취약 항목

2.1 계정 관리


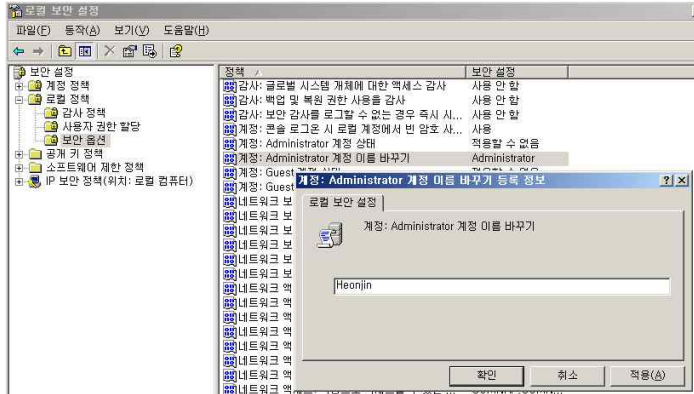
취약점 항목	1.1 Administrator 계정 이름 바꾸기				
대상 OS	Window 2003	위험도	상	Code	W-01
취약점 개요	일반적으로 관리자 계정을 Administrator로 설정한 경우 로그인 시도 실패 횟수의 제한이 없는 점을 이용해 악의적인 사용자가 패스워드 유추 공격을 계속해서 시도할 수 있음. 관리자 계정의 이름을 변경함으로써 공격자가 패스워드뿐만 아니라 계정 이름을 쉽게 유추하지 못하도록 하여야 함.				
보안대책					
판단기준	양호 : Administrator Default 계정 이름을 변경한 경우				
	취약 : Administrator Default 계정 이름을 변경하지 않은 경우				
조치방법	Administrator Default 계정 이름 변경				
보안 설정 방법					
1. Administrator 계정을 변경 안함					
<div></div> <div>그림 1 Administrator</div>					
2. 시작 > 프로그램 > 제어판 > 관리도구 > 로컬 보안 정책 > 로컬 정책 > 보안 옵션 > Administrator 계정 이름 바꾸기					
<div></div> <div>그림 2 Administrator 변경</div>					
조치시 영향	일반적으로 없음				

표 2 Administrator 계정 이름 바꾸기

취약점 항목	1.3 불필요한 계정 제거				
대상 OS	Window 2003	위험도	상	Code	W-03
취약점 개요	퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정이 존재하는지 점검함. 관리되지 않은 불필요한 계정은 장기간 패스워드가 변경되지 않아 *무작위 대입 공격(Brute Force Attack)이나 패스워드 추측 공격>Password Guessing)에 의해 계정 정보가 유출되어도 인지하기 어려움.				
보안대책					
판단기준	양호 : 불필요한 계정이 존재하지 않는 경우				
	취약 : 불필요한 계정이 존재하는 경우				
조치방법	현재 계정 현황 확인 후 불필요한 계정 삭제				

보안 설정 방법

1. 사용자 그룹에 불필요한 infosechack 계정이 있는 것을 확인



그림 3 불필요한 계정

2. 시작 > 프로그램 > 관리 도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > 계정 삭제

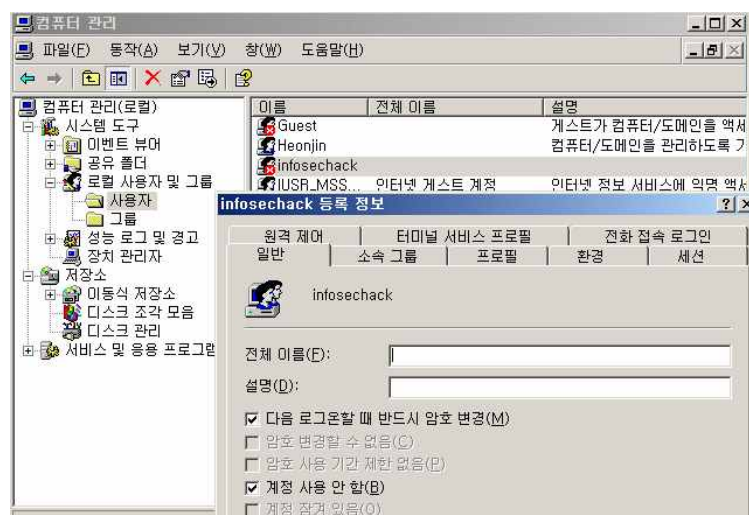


그림 4 계정 삭제

조치시 영향	계정의 사용여부를 파악하여 사용하지 않는 계정일 경우 제거

표 3 불필요한 계정 제거

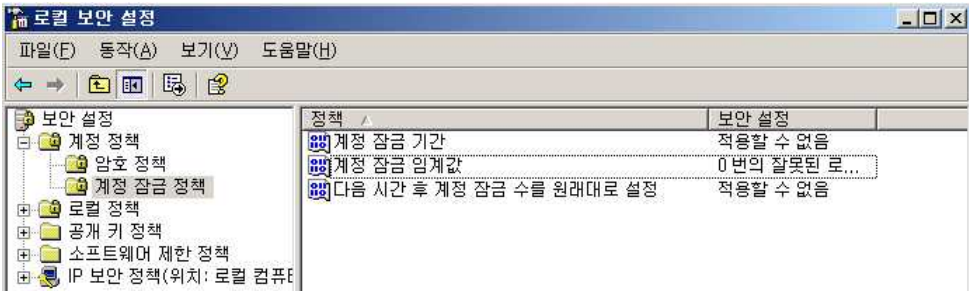
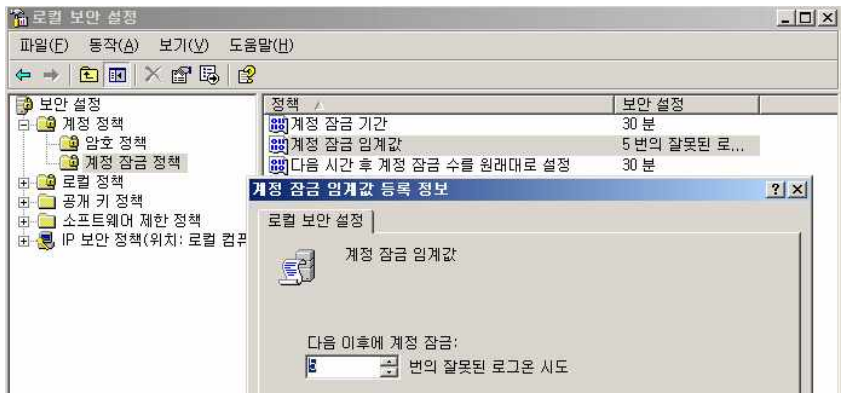
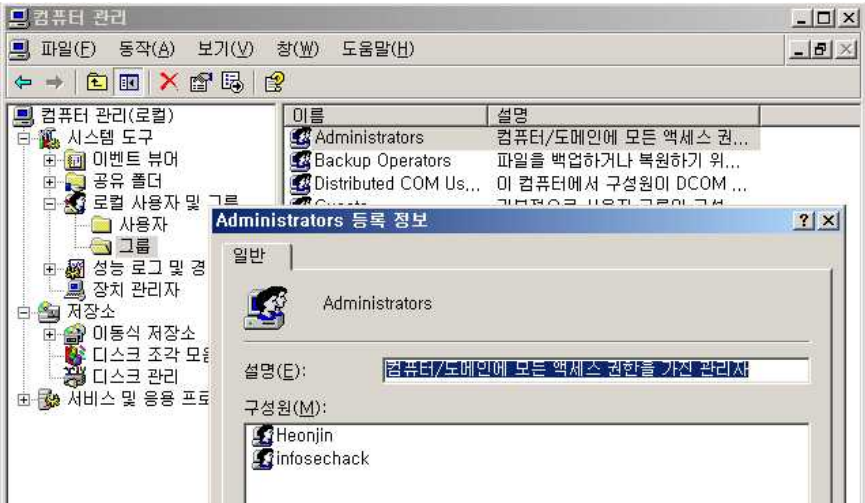
취약점 항목	1.4 계정 잠금 임계값 설정				
대상 OS	Window 2003	위험도	상	Code	W-04
취약점 개요	자동화된 방법을 이용하여 공격자는 모든 사용자 계정에 대해 암호조합 공격을 시도할 수 있으므로 계정 잠금 임계값 설정을 적용하여 로그인 실패 횟수를 제한하여야 함.				
보안대책					
판단기준	양호 : 계정 잠금 임계값이 5 이하의 값으로 설정되어 있는 경우				
	취약 : 계정 잠금 임계값이 5 이하의 값으로 설정되어 있지 않는 경우				
조치방법	계정 잠금 임계값을 5번 이하의 값으로 설정				
보안 설정 방법					
1. 계정 잠금 임계값이 설정이 안되어 있음					
					
그림 5 계정 잠금 임계값					
2. 계정 잠금 임계값을 5이하로 설정 변경					
					
그림 6 계정 잠금 임계값 설정					
조치시 영향	Administrator 계정은 잠기지 않으며, 일반 계정의 경우 5번 패스워드 입력 실패시 잠김				

표 4 계정 잠금 임계값 설정

취약점 항목	1.6 관리자 그룹에 최소한의 사용자 포함				
대상 OS	Window 2003	위험도	상	Code	W-06
취약점 개요	일반 사용자 권한으로부터 받을 수 있는 시스템 피해를 줄이기 위해서 관리 업무를 위한 계정과 일반 업무를 위한 계정을 분리하여 사용하는 것이 바람직함. 시스템 관리를 위해서는 각각 두 개의 계정을 가져야 하며 관리자 그룹에는 가능한 최소한의 사용자만 포함하도록 하여야 함				
보안대책					
판단기준	양호 : Administrator 그룹에 불필요한 관리자 계정이 존재하지 않는 경우				
	취약 : Administrator 그룹에 불필요한 관리자 계정이 존재하는 경우				
조치방법	Administrator 그룹에 포함된 불필요한 계정 제거				
보안 설정 방법					
1. 시작 > 실행 > lusrmgr.msc > 그룹 > Administrator > 속성					
- 불필요한 사용자 infosechack을 확인 가능					
					
그림 7 불필요한 사용자					
2. 사용자 제거					

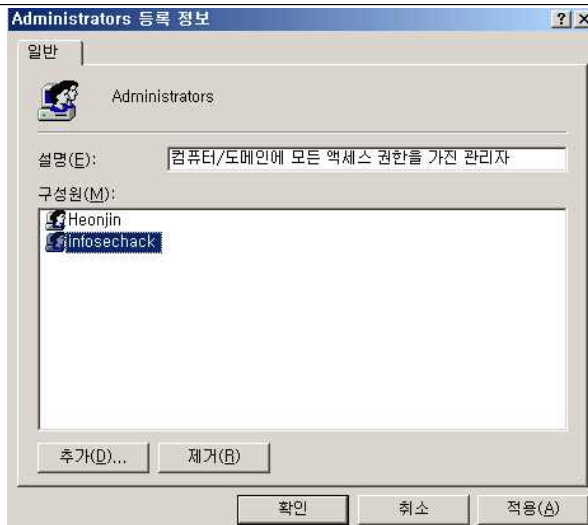


그림 8 사용자 제거

조치시 영향	Administrator 권한이 필요 없을 경우 변경 시 영향 없음
--------	---------------------------------------

표 5 관리자 그룹에 최소한의 사용자 포함

취약점 항목	1.8 계정 잠금 기간 설정				
대상 OS	Window 2003	위험도	중	Code	W-08
취약점 개요	계정 잠금 기간 설정을 사용하면 지정한 기간 동안 잠긴 계정을 사용할 수 없으며, 계정 잠금이 해제될 때까지 접근할 수 없음. 따라서 공격자가 자동으로 암호를 추측하는 것이 어렵게 되어 암호공격 효과를 낮출 수 있음.				
보안대책					
판단기준	양호 : “계정 잠금 기간” 및 “계정 잠금 수를 원래대로 설정 기간”이 설정되어 있는 경우				
	취약 : “계정 잠금 기간” 및 “계정 잠금 수를 원래대로 설정 기간”이 설정되지 않은 경우				
조치방법	“계정 잠금 기간” 및 “잠금 기간 원래대로 설정 기간” 60분 설정				

보안 설정 방법

1. “계정 잠금 기간”, “다음 시간 후 계정 잠금 수를 원래대로 설정”이 적용이 안되어 있음

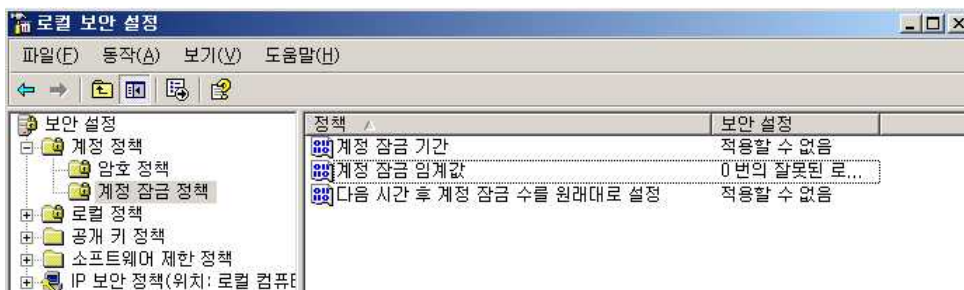


그림 9 계정 잠금 임계값

2. “계정 잠금 기간”, “다음 시간 후 계정 잠금 수를 원래대로 설정”을 60분으로 적용

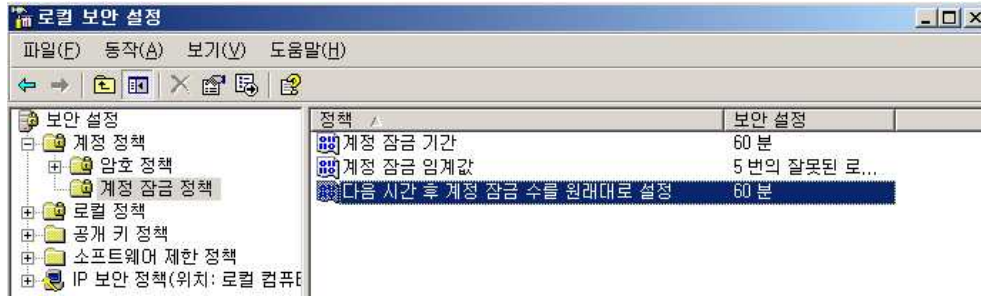


그림 10 잠금 기간 설정

조치시 영향	일반적으로 영향 없음
--------	-------------

표 6 계정 잠금 기간 설정

취약점 항목	1.9 패스워드 복잡성 설정				
대상 OS	Window 2003	위험도	중	Code	W-09
취약점 개요	패스워드 설정 시 문자/숫자/특수문자를 모두 포함하여 강력한 패스워드가 설정될 수 있도록 암호 복잡성을 설정하여야 함. 영·숫자만으로 이루어진 암호는 현재 공개된 패스워드 크랙 유틸리티에 의해 쉽게 유추할 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.				
보안대책					
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				
보안 설정 방법					

1. 시작 > 프로그램 > 관리도구 > 로컬 보안 설정 > 암호 정책 > 암호는 복잡성을 만족해야 함

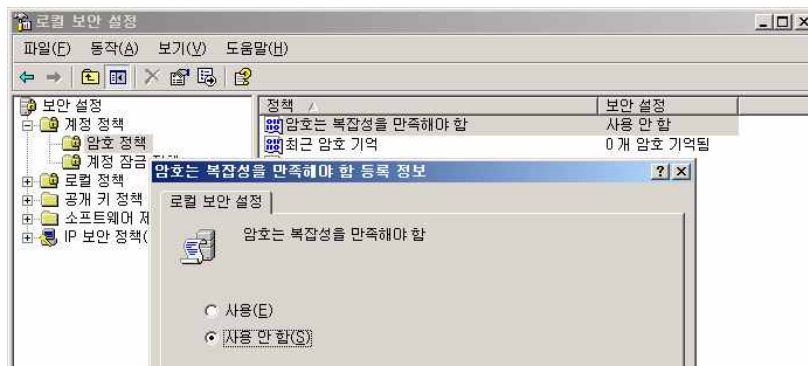


그림 11 암호 복잡성 사용 안 함

2. 사용으로 변경

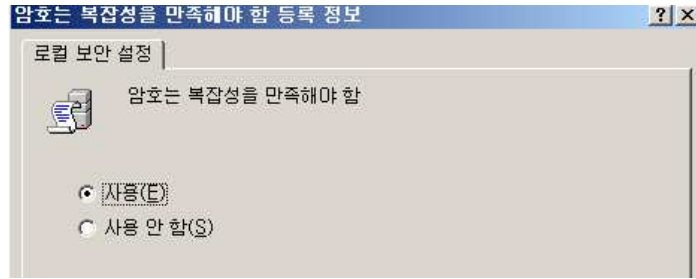


그림 12 암호 복잡성 사용

※ 이 정책 설정은 암호를 변경하거나 새로운 암호 생성 시 아래와 같은 일련의 규정을 만족하는지 결정함
다음 각 목의 문자 종류 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)

조치시 영향	일반적으로 영향 없음
--------	-------------

표 7 패스워드 복잡성 설정

취약점 항목	1.10 패스워드 최소 암호 길이				
대상 OS	Window 2003	위험도	중	Code	W-10
취약점 개요	일반적인 단어와 구를 이용해 취약하게 암호를 설정한 계정은 사전 공격과 가능한 모든 문자의 조합을 시도하는 무작위 대입을 통해 권한을 도용당할 수 있음. 최소 암호길이를 8자리로 설정하면 대부분 환경에서 적절한 보안이 제공될 뿐만 아니라 사용자가 쉽게 기억할 수 있으며 무작위 공격을 방어할 수 있음.				
보안대책					
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”에 “최소”를 “8문자”로 설정				
보안 설정 방법					
1. 시작 > 프로그램 > 관리 도구 > 로컬 보안 정책 > 암호 정책 > 최소 암호 길이					

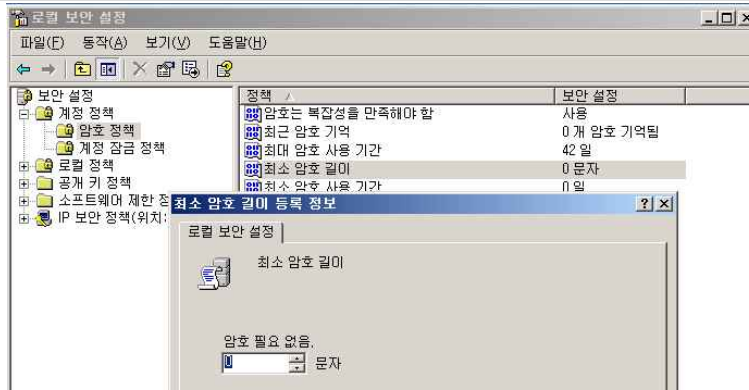


그림 13 최소 암호 길이

2. 최소 암호 길이 설정

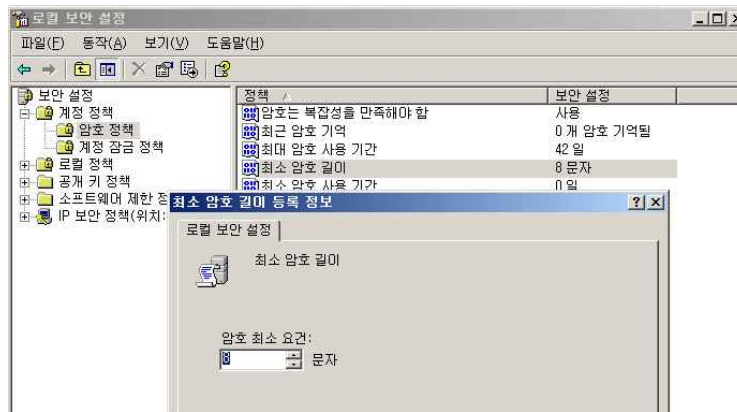


그림 14 최소 암호 길이 8글자

조치시 영향	다음 패스워드 변경 시 8자 이상의 패스워드를 설정하여야 함
--------	-----------------------------------

표 8 패스워드 최소 암호 길이

취약점 항목	1.12 패스워드 최소 사용 기간				
대상 OS	Window 2003	위험도	중	Code	W-12
취약점 개요	패스워드 변경에 시간적 제약이 없다면 이전에 즐겨 사용했던 암호를 다시 사용할 수 있으므로 주기적으로 패스워드를 변경하는 정책의 효과가 없어짐. 최소 암호 사용 기간 정책 설정을 0보다 큰 값으로 구성하면 최근 암호 기억 설정을 유효하게 사용함으로써 이전 암호를 다시 사용하는 것을 막을 수 있음.				
보안대책					
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				

보안 설정 방법

1. 시작 > 프로그램 > 관리 도구 > 로컬 보안 정책 > 암호 정책 > 최소 암호 사용 기간 등록 정보

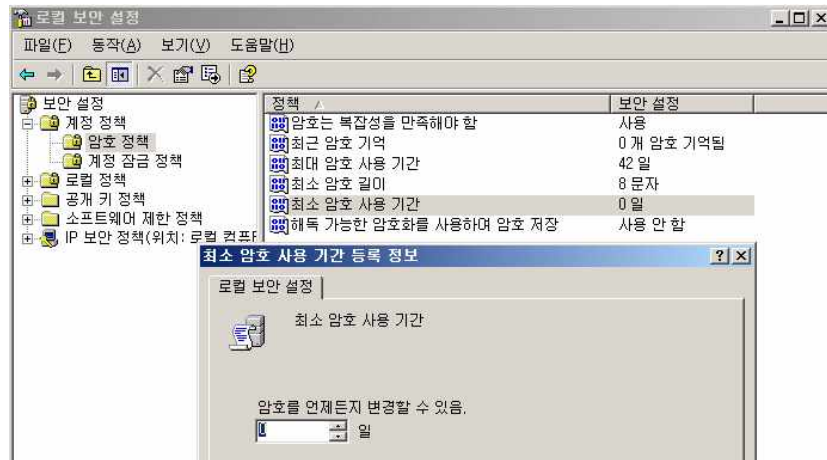


그림 15 최소 암호 사용 기간

2. 최소 암호 사용 기간 등록 정보를 1일로 변경

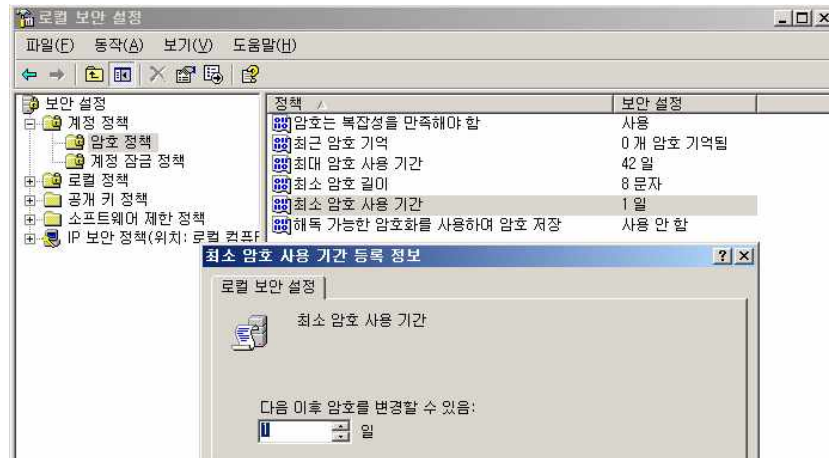


그림 16 최소 암호 사용 기간 변경

조치시 영향	패스워드를 변경 후 다시 변경하기 위해서는 1일이 지나야 하며, 일반적으로 영향 없음
--------	---

표 9 패스워드 최소 사용 기간

취약점 항목	1.13 마지막 사용자 이름 표시 안함				
대상 OS	Window 2003	위험도	중	Code	W-13
취약점 개요	마지막으로 로그인한 사용자의 이름이 로그인 대화 상자에 표시될 경우 공격자는 이를 획득하여 암호를 추측하거나 무작위 공격을 시도할 수 있음. 실제로 콘솔에 접근할 수 있는 사용자 또는, 터미널 서비스를 통해 서버에 연결할 수 있는 사용자들에게 쉽게 노출될 수 있으므로 사용자 이름이 표시되지 않도록 설정하여야 함.				

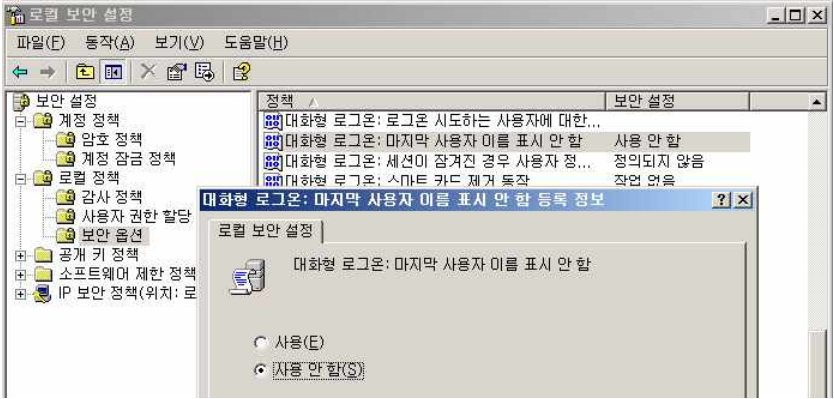
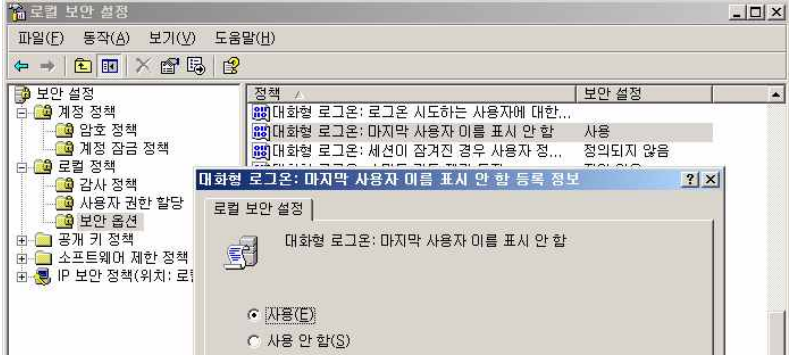
보안대책	
판단기준	양호 : “마지막 사용자 이름 표시 안 함”이 “사용”으로 설정되어 있는 경우
	취약 : “마지막 사용자 이름 표시 안 함”이 “사용”으로 설정되어 있는 경우
조치방법	Windows NT: 마지막으로 로그인한 사용자 이름 표시 안 함 → 설정 후 저장 Windows 2000: 로그인 스크린에 마지막 사용자 이름 표시 안 함 → 사용 Windows 2003, 2008: 대화형 로그인: 마지막 사용자 이름 표시 안 함 → 사용
보안 설정 방법	
1. 시작 > 프로그램 > 관리 도구 > 로컬 보안 설정 > 보안 옵션 > 대화형 로그인 : 마지막 사용자 이름 표시 안함	
 <p>그림 17 마지막 사용자 이름 표시 사용 안함</p>	
2. 사용 안 함 -> 사용	
 <p>그림 18 마지막 사용자 이름 표시 사용</p>	
조치시 영향	패스워드를 변경 후 다시 변경하기 위해서는 1일이 지나야 하며, 일반적으로 영향 없음

표 10 마지막 사용자 이름 표시 안함

취약점 항목	1.14 로컬 로그인 허용				
대상 OS	Window 2003	위험도	중	Code	W-14

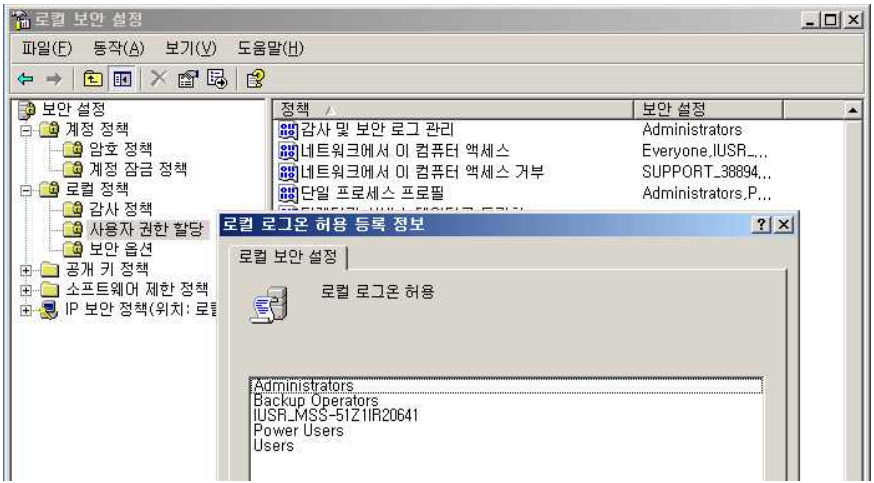
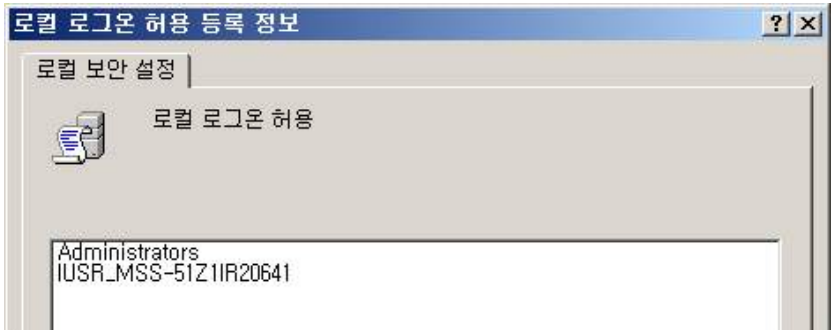
취약점 개요	<p>“로컬로 로그인 허용” 권한은 시스템 콘솔에 로그인을 허용하는 권한으로 반드시 콘솔 접근이 필요한 사용자 계정에만 해당 권한을 부여하여야 함. 만약 해당 권한을 적절하게 제한하지 않은 경우 권한 없는 사용자가 자신의 사용 권한을 상승시키기 위해 악의적인 코드를 실행할 수 있음</p> <p>※ IIS 서비스를 사용할 경우 이 권한에 ISUR_<ComputerName> 계정을 할당함.</p>
보안대책	
판단기준	양호 : 로컬 로그인 정책에 Administrator, IUSR_만 존재하는 경우
	취약 : 로컬 로그인 정책에 Administrator, IUSR_ 외 다른 계정 및 그룹이 존재하는 경우
조치방법	Administrator, IUSR_외 다른 계정 및 그룹의 로컬 로그인 제한
보안 설정 방법	
<p>1. 시작 > 프로그램 > 관리 도구 > 로컬 정책 설정 > 사용자 권한 할당 > 로컬 로그인 허용</p>  <p>그림 19 로컬 로그인 허용 정보</p>	
<p>2. Administrator, IUSR_ 빼고 제거</p>  <p>그림 20 로컬 로그인 허용 제거</p>	
조치시 영향	일반적인 경우 영향 없음

표 11 로컬 로그인 허용

취약점 항목	1.16 최근 암호 기억				
대상 OS	Window 2003	위험도	중	Code	W-16
취약점 개요	사용자가 현재 암호 또는, 최근에 사용했던 암호와 똑같은 새 암호로 설정할 수 없도록 하여야 함. 특정 계정에 같은 암호를 오래 사용할수록 공격자가 무작위 공격을 통해 암호를 확인할 가능성이 커지며, 유출된 계정의 암호를 바꾸지 않는 한 계속 악용될 수 있음. 또한, 암호를 변경해야 할 경우 암호를 다시 사용하는 것을 금지하지 않거나, 적은 수의 암호를 계속해서 다시 사용할 수 있도록 허용하면 좋은 암호 정책의 효과가 크게 반감됨.				
보안대책					
판단기준	양호 : 최근 암호 기억이 12개 이상으로 설정되어 있는 경우				
	취약 : 최근 암호 기억이 12개 미만으로 설정되어 있는 경우				
조치방법	최근 암호 기억을 12개 암호로 설정				

보안 설정 방법

1. 시작 > 프로그램 > 관리 도구 > 로컬 보안 정책 > 암호 정책 > 최근 암호 기억

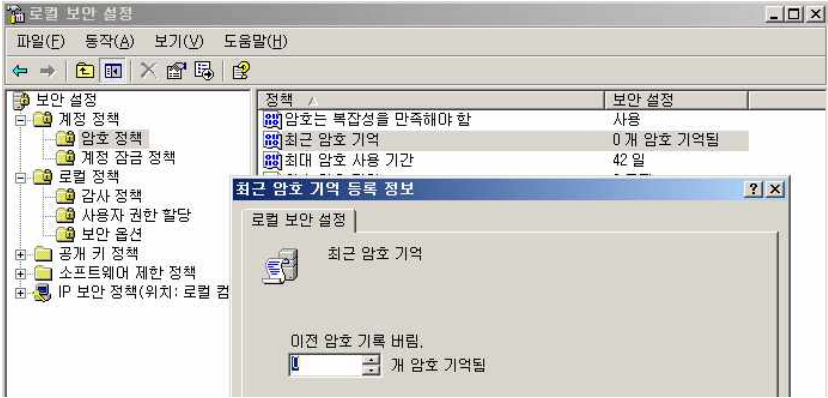


그림 21 최근 암호 기억

2. 최근 암호 기억을 12개 이상으로 변경

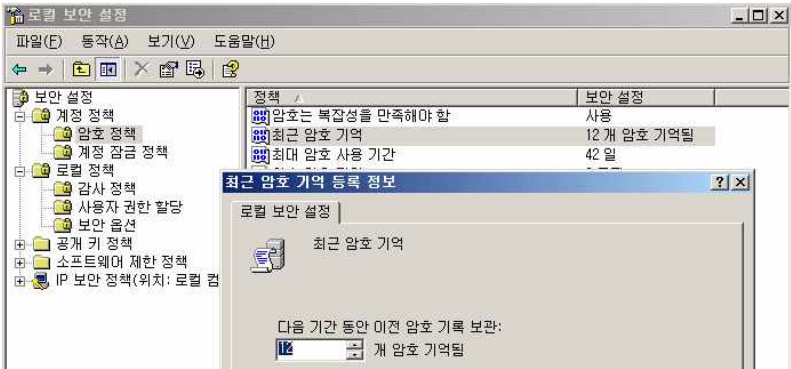


그림 22 최근 암호 기억 변경

조치시 영향	일반적인 경우 영향 없음
--------	---------------

표 12 최근 암호 기억

2.2 서비스 관리

취약점 항목	2.2 하드디스크 기본 공유 제거				
대상 OS	Window 2003	위험도	상	Code	W-20
취약점 개요	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.				
보안대책					
판단기준	양호 : AutoshareServer(WinNT: AutoShareWks)가 0이며 기본 공유가 존재하지 않는 경우				
	취약 : AutoshareServer(WinNT: AutoShareWks)가 1이거나 기본 공유가 존재하는 경우				
조치방법	기본 공유 중지 후 레지스트리 값 설정(IPC\$, 일반 공유 제외)				

보안 설정 방법

1. 시작 > 실행 > fsmgmt.msc > 공유 > 기본 공유 확인



그림 23 기본 공유 확인

2. 기본 공유 존재시 공유 중지

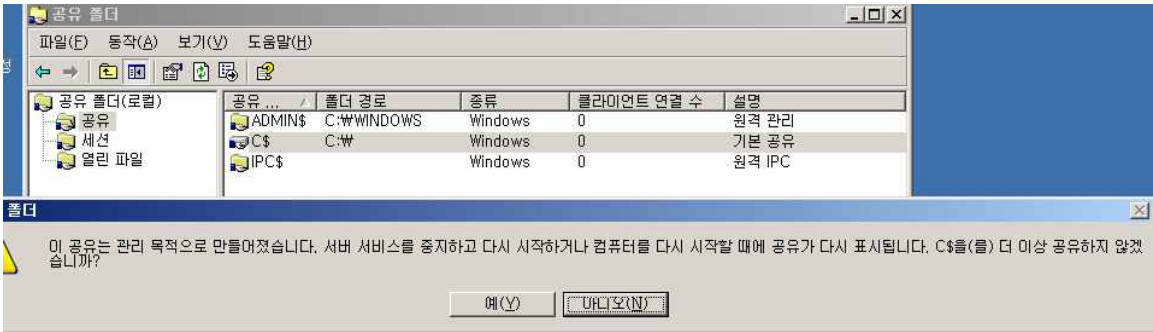


그림 24 기본공유 중지

공유 ...	폴더 경로	종류	클라이언트 연결 수	설명
ADMIN\$	C:\WINDOWS	Windows	0	원격 관리
IPC\$		Windows	0	원격 IPC

그림 25 기본 공유 중지

조치시 영향	일반적인 경우 영향 없음
--------	---------------

표 13 하드디스크 기본 공유 제거

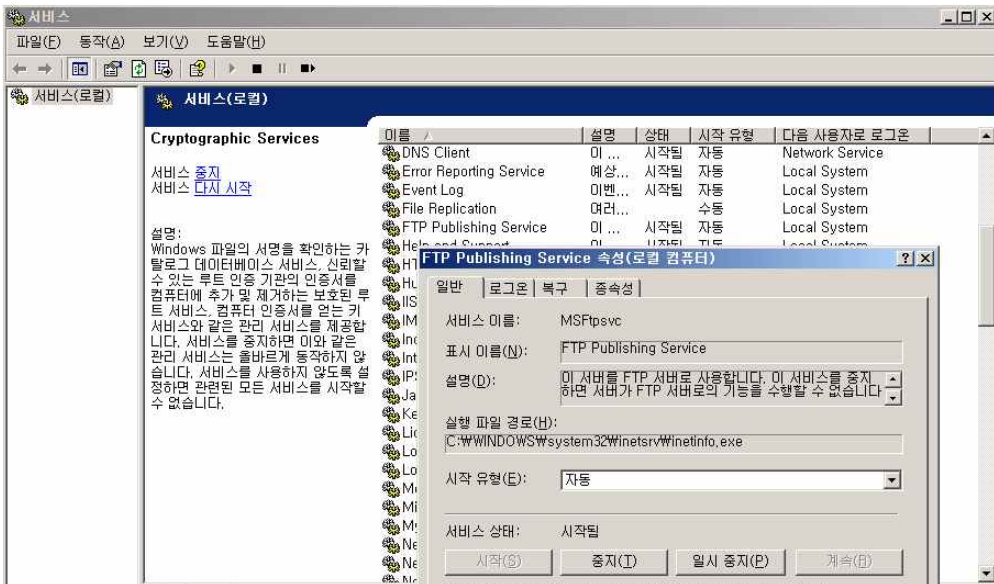
취약점 항목		2.19 FTP 서비스 구동 점검			
대상 OS	Window 2003	위험도	상	Code	W-37
취약점 개요	기본적인 FTP 서비스는 계정과 패스워드가 암호화되지 않은 채로 전송되어 간단한 Sniffer에 의해서도 스니핑이 가능하므로 FTP 서비스를 사용하지 않을 것을 권고함.				
보안대책					
판단기준	양호 : FTP 서비스를 사용하지 않는 경우				
	취약 : FTP 서비스를 사용하는 경우				
조치방법	FTP 서비스가 필요하지 않다면 서비스 중지				
보안 설정 방법					
1. 시작 > 실행 > services.msc > ftp publishing service > 속성 > [일반] 탭에서 “시작 유형”을 “사용 안 함”으로 설정한 후, FTP 서비스 중지					
					
그림 26 FTP 중지					
조치시 영향	일반적인 경우 영향 없음				

표 14 FTP 서비스 구동 점검

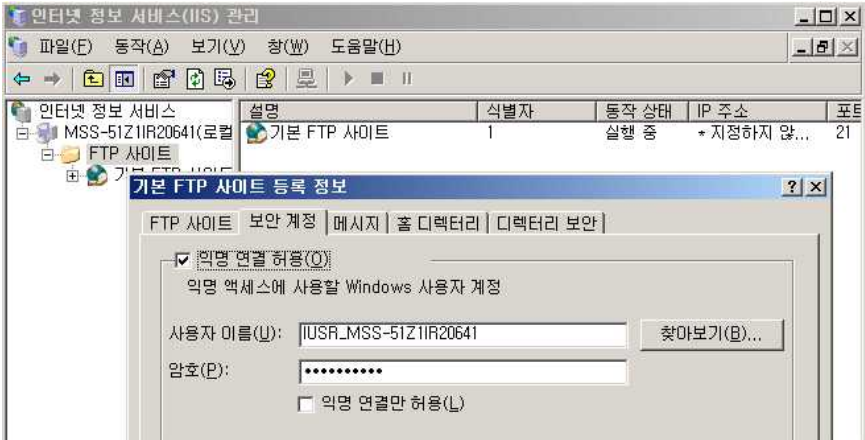
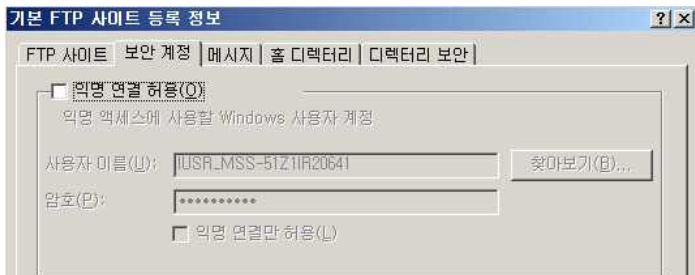
취약점 항목	2.21 Anonymous FTP 금지				
대상 OS	Window 2003	위험도	상	Code	W-39
취약점 개요	기본적인 FTP 서비스는 계정과 패스워드가 암호화되지 않은 채로 전송되어 간단한 Sniffer에 의해서도 스니핑이 가능하므로 FTP 서비스를 사용하지 않을 것을 권고. 만약 불가피하게 FTP 서비스를 이용해야 하는 경우 FTP Default 설정이 익명연결 허용을 차단하고, 특정 IP 주소에서 접속하도록 접근제어 설정을 적용하여야함.				
보안대책					
판단기준	양호 : FTP 서비스를 사용하지 않거나, “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				
보안 설정 방법					
1. 인터넷 정보 서비스(IIS) 관리 > FTP 사이트 > 속성 > [보안 계정] 탭에서 “익명 연결 허용” 체크 박스 해제 (만약 개별 FTP 사이트에 적용할 경우 해당 사이트에만 설정이 적용되고, 기본 설정은 적용 받지 않음)					
<div></div>					
그림 27 FTP 익명 연결					
2. 익명 연결 허용 해제					
<div></div>					
그림 28 익명 연결 해제					
조치시 영향	애플리케이션에서 익명 연결을 사용할 경우를 제외하고, 일반적으로 영향 없음				

표 15 Anonymous FTP 금지

취약점 항목	2.22 FTP 접근 제어 설정				
대상 OS	Window 2003	위험도	상	Code	W-40
취약점 개요	기본적인 FTP 서비스는 계정과 패스워드가 암호화되지 않은 채로 전송되어 간단한 Sniffer에 의해서도 스니핑이 가능하므로 FTP 서비스를 사용하지 않을 것을 권고. 만약 불가피하게 FTP 서비스를 이용해야 하는 경우 특정 IP 주소에 허가된 사용자만이 접속할 수 있도록 접근제어 설정을 적용하여야 함.				
보안대책					
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				

보안 설정 방법

1. 인터넷 정보 서비스(IIS) 관리 > FTP 사이트 > 속성 > [디렉터리 보안] 탭

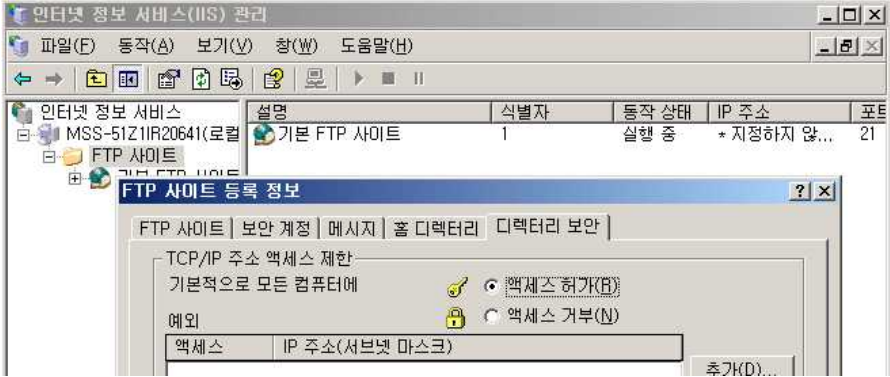


그림 29 IP 제한

2. “액세스 거부” 선택 후 접근 가능 IP 주소 추가(만약 개별 FTP 사이트에 적용할 경우 해당 사이트에만 설정이 적용되고, 기본 설정은 적용 받지 않음)

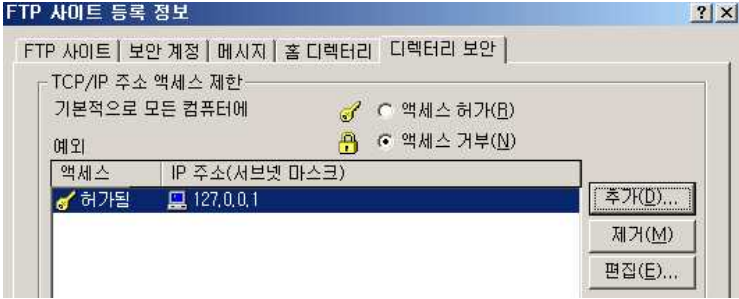


그림 30 FTP IP 제한

[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

※ 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)	
조치시 영향	일반적으로 영향 없음

표 16 FTP 접근 제어 설정

취약점 항목	2.23 DNS Zone Transfer 설정				
대상 OS	Window 2003	위험도	상	Code	W-41
취약점 개요	DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS서버가 아닌 다른 외부로 유출하는 것은 보안상 바람직하지 않으므로 적절한 보안 설정을 통하여 도메인 정보 전송을 제한하여야 함. 만약, DNS 도메인 정보가 외부로 누출될 경우 악의적인 사용자가 해당 정보를 이용하여 홈페이지 및 하위 URL 정보를 입수하여 웹 어플리케이션 구조를 예측할 수 있음.				
보안대책					
판단기준	양호 : 아래 기준에 해당될 경우 1. DNS 서비스를 사용 않는 경우 2. 영역 전송 허용을 하지 않는 경우 3. 특정 서버로만 설정이 되어 있지 않는 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				
보안 설정 방법					
1. 시작 > 실행 > dnsmgmt.msc > 각 조회 영역 > 해당 영역 > 속성 > 영역 전송 2. “다음 서버로만” 선택 후 전송할 서버 IP 추가 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.					

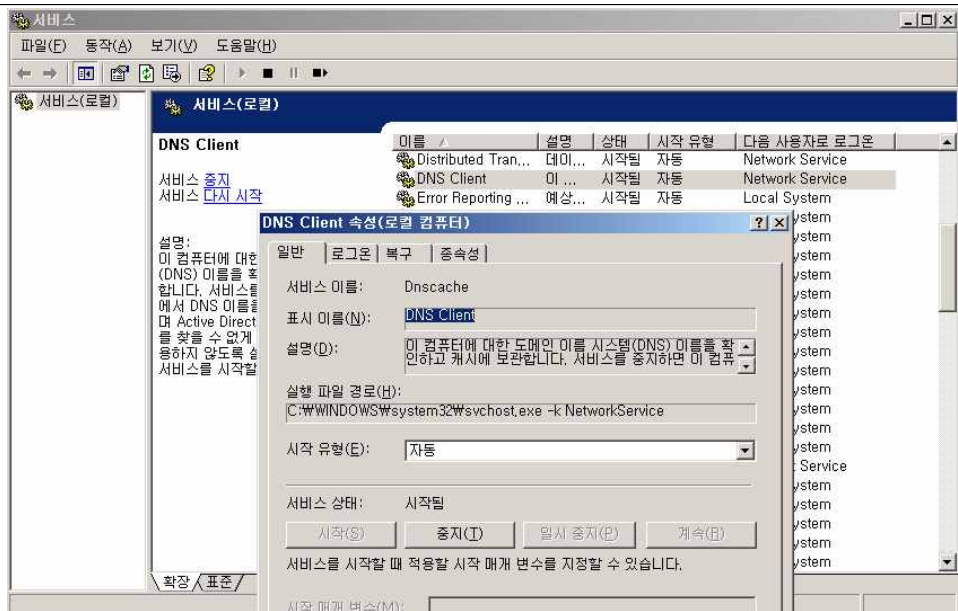


그림 31 DNS Client 중지

조치시 영향	영역 전송할 경우 서버를 지정해 주면 영향 없음
--------	----------------------------

표 17 DNS Zone Transfer 설정

취약점 항목	2.25 최신 서비스팩 적용				
대상 OS	Window 2003	위험도	상	Code	W-43
취약점 개요	서비스팩은 Windows의 안정성을 높이기 위해 응용프로그램, 서비스, 실행 파일 등 여러 가지 파일들을 모아 놓은 업데이트 프로그램이므로 항상 최신 버전으로 유지할 수 있도록 권고함.				
보안대책					
판단기준	양호 : 최신 서비스팩이 설치되어 있는 경우				
	취약 : 최신 서비스팩이 설치되어 있는 경우				
조치방법	설치에 따른 영향도 확인 후 최신 서비스팩 설치 (설치 후 시스템 재시작 필요)				
보안 설정 방법					
1. 시작 > 실행 > winver					



그림 32 서비스팩 확인

2. 서비스팩 버전 확인 후 최신 버전이 아닌 경우 아래 사이트에서 최신 서비스팩 다운로드 후 설치
 ※ 인터넷 뮌(Woram)이 Windows의 취약점을 이용하여 공격하기 때문에 서비스팩 설치 시에는 네트워크와 분리된 상태에서 설치 할 것을 권장

[보안 패치 사이트]

Microsoft Windows Server 제품별 지원

<http://support.microsoft.com/ph/1163>

조치시 영향	설치 후 시스템 재시작이 필요하며 설치에 따른 영향 정도를 확인하여야 함
--------	--

표 18 최신 서비스팩 적용

취약점 항목	2.32 HTTP/FTP/SMTP 배너 차단				
대상 OS	Window 2003	위험도	하	Code	W-50
취약점 개요	임의의 사용자가 HTTP/FTP/SMTP 접속 시도 시 보이는 접속 배너 정보를 수집하여 해킹에 사용할 수 있음.				
보안대책					
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				
보안 설정 방법					
1. FTP ftpsvc2.dll를 Hex 편집기로 불러온 다음 “Microsoft FTP Service” 부분을 찾아 수정 ※ DLL파일이 메모리에 로드되어 있어 편집이 불가능하므로 윈도우를 명령 프롬프트만 나타나도록 부팅한 후 해당 파일을 변경					

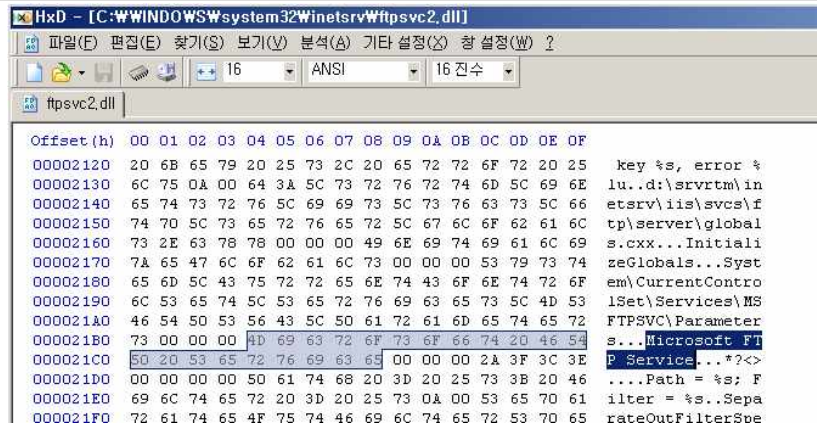


그림 33 HxD로 배너제거

조치시 영향	일반적으로 영향 없음
--------	-------------

표 19 HTTP/FTP/SNMP 배너 차단

취약점 항목	2.35 원격터미널 접속 타임아웃 설정				
대상 OS	Window 2003	위험도	중	Code	W-53
취약점 개요	일반적으로 웹 서비스 이용 시 사용자의 브라우저에서 어떠한 이벤트도 발생하지 않는다면 웹 서버에서 보안상 자동으로 세션을 끊는 경우가 있음. 이와 같은 방식으로 원격제어를 이용하여 터미널에 접속 후 일정 시간 동안 이벤트가 발생시키지 않는다면 세션을 종료시키기 위해 Timeout 설정을 해주어야 함.				
보안대책					
판단기준	양호 : 원격제어 시 Timeout 제어 설정을 적용한 경우				
	취약 : 원격제어 시 Timeout 제어 설정을 적용하지 않은 경우				
조치방법	Timeout 제어 설정 적용				
보안 설정 방법					
1. 시작 > 실행 > tscc.msc 실행 (Windows 2008은 tsconfig.msc)					
2. RDP-TCP-Connection에서 우클릭 > 속성 실행					



그림 34 RDP-Tcp 속성

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

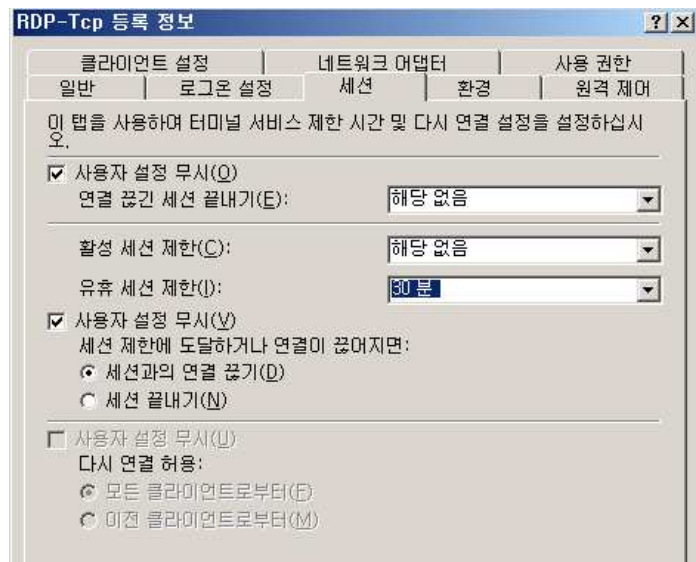


그림 35 RDP-Tcp 세션

조치시 영향	애플리케이션에서 사용할 경우는 양호
--------	---------------------

표 20 원격터미널 접속 타임아웃 설정

2.3 패치 관리

취약점 항목	3.1 최신 HOT FIX 적용
--------	-------------------

대상 OS	Window 2003	위험도	상	Code	W-55
취약점 개요	Hot Fix는 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련된)을 패치하기 위해 배포되는 프로그램으로 각각의 서비스팩이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표됨. 때론, Hot Fix보다 취약성을 이용한 공격도구가 먼저 출현할 수 있으므로 Hot Fix는 발표 후 가능한 한 빨리 설치할 것을 권장함.				
보안대책					
판단기준	양호 : 최신 Hotfix 또는, PMS(Patch Management System) Agent가 설치되어 있는 경우				
	취약 : 최신 Hotfix 또는, PMS(Patch Management System) Agent가 설치되어 있지 않은 경우				
조치방법	최신 Hotfix 설치				
보안 설정 방법					
<p>1. 아래의 패치 리스트를 조회하여, 서버에 필요한 패치를 선별하여 수동으로 설치함</p> <p>http://www.microsoft.com/korea/technet/security/current.asp</p> <p>2. Windows 자동 업데이트 기능을 이용한 설치</p> <p>수동 업데이트의 부담을 덜어주기 위하여 Microsoft에서는 자동으로 시스템에 필요한 Hot Fix 및 소프트웨어 업그레이드를 보여주고 다운로드 및 적용을 쉽게 하기 위한 사이트를 마련해 놓고 있음Internet Explorer 도구 메뉴 중 “Windows Update”를 선택하면 자동으로 Windows Update 사이트로 이동하게 되며, 다음의 URL을 직접 주소 입력 창에 입력 가능함</p> <p>http://windowsupdate.microsoft.com/?IE</p> <p>3. PMS(Patch Management System) Agent를 설치하여 자동으로 업데이트되도록 설정함</p> <p>※ 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</p>					
조치시 영향	설치 후 시스템 재시작이 필요한 경우가 존재하며 설치에 따른 영향도 필요함				

표 21 최신 HOT FIX 적용

취약점 항목	3.2 백신 프로그램 업데이트				
대상 OS	Window 2003	위험도	상	Code	W-56
취약점 개요	계속되는 신종 바이러스의 출현으로 인해 백신 프로그램의 설치만으로는 그 효과를 볼 수 없으므로 바이러스 정보에 대한 주기적인 업데이트를 통해 최신의 바이러스까지 치료할 수 있는 기능이 필요함.				

보안대책	
판단기준	양호 : 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있는 경우
	취약 : 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않은 경우
조치방법	담당자를 통해 바이러스 백신을 설치 후 엔진 업데이트를 설정하도록 권고
보안 설정 방법	
1. 긴급한 경우 수시로 업데이트 진행 (백신 종류마다 다소 차이는 있으나 매주 업데이트가 이뤄짐) 2. 정기적인 업데이트를 통해 검색엔진을 최신 버전으로 유지하고, 백신사에서 발표하는 경보 주시 3. 백신 프로그램의 자동 업데이트 기능을 이용하면 온라인을 통해 변동 사항을 자동으로 업데이트하여 알 수 있음 4. 현재 서버에는 백신이 안 깔려 있으므로 V3 설치 • 안철수 연구소, 하우리: 매주 수요일 정기업데이트 • 시만텍코리아, 트랜드마이크로: 매주 목요일 정기업데이트 (미국 시간으로 수요일) ※ 4개 백신 업체 모두 긴급 시 수시 업데이트 및 실시간 업데이트 기능 제공.	
조치시 영향	일반적으로 영향 없음

표 22 백신 프로그램 업데이트

2.4 로그 관리

취약점 항목	4.2 원격으로 액세스할 수 있는 레지스트리 경로				
대상 OS	Window 2003	위험도	상	Code	W-59
취약점 개요	Windows에 의해 사용되는 모든 초기화 및 환경설정 정보가 레지스트리에 저장되므로 레지스트리에 대한 철저한 보안이 요구됨. 레지스트리 편집기는 원격접속으로도 그 키를 바꿀 수 있지만, 대단히 위험하므로 네트워크를 통한 레지스트리 접속을 차단하여야 함. 원격에서 레지스트리로의 접근을 위해서는 관리자의 권한 또는 원격에서 접근하기 위한 특별한 계정이 필요함. 윈도우에서는 원격에서 레지스트리 접근에 대한 요구를 다루기 위해 원격 레지스트리 서비스를 제공하고 있는데, 이 서비스를 중지시키면 레지스트리에 대한 어떠한 원격 접근도 막을 수 있으므로 불가피한 경우를 제외하고는 사용을 중지할 것을 권고함.				
보안대책					
판단기준	양호 : Remote Registry Service가 중지되어 있는 경우				
	취약 : Remote Registry Service가 사용 중인 경우				

취약점 항목	5.1 백신 프로그램 설치				
대상 OS	Window 2003	위험도	상	Code	W-62
취약점 개요	웜, 트로이목마 등의 악성 바이러스로 인한 피해규모가 커지고 있으므로 이에 대한 피해를 최소화하기 위해 반드시 바이러스 백신 프로그램을 설치 및 운영하여야 함. 바이러스 백신 프로그램은 바이러스 감염 여부 진단 및 치료뿐만 아니라 파일 보호를 통한 예방 조치도 가능함.				
보안대책					
판단기준	양호 : 바이러스 백신 프로그램이 설치되어 있는 경우				
	취약 : 바이러스 백신 프로그램이 설치되어 있지 않은 경우				
조치방법	담당자를 통해 바이러스 백신 반드시 설치하도록 하여야함				
보안 설정 방법					
안철수 연구소, 알약, AVG, Avast, 카스퍼스키, 하우리, 시만텍 코리아, 트렌드 마이크로 등등 백신을 설치					
조치시 영향	일반적으로 영향 없음				

표 24 백신 프로그램 설치

취약점 항목	5.7 SAM 계정과 공유의 익명 열거 허용 안 함				
대상 OS	Window 2003	위험도	상	Code	W-68
취약점 개요	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.				
보안대책					
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				
보안 설정 방법					
1. 시작 > 실행 > secpol.msc > 로컬 정책 > 보안 옵션					

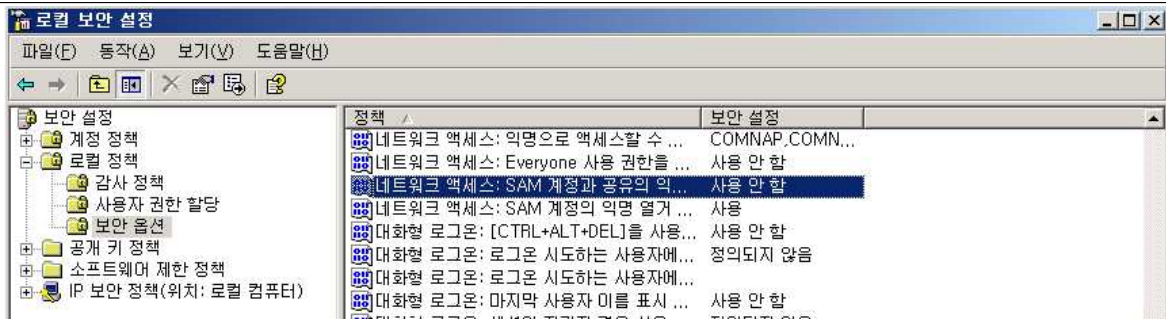


그림 38 SAM 계정과 공유의 이름 열거

2. “SAM 계정과 공유의 이름 열거 허용 안 함”과 “SAM 계정의 이름 열거 허용 안 함”에 “사용” 선택

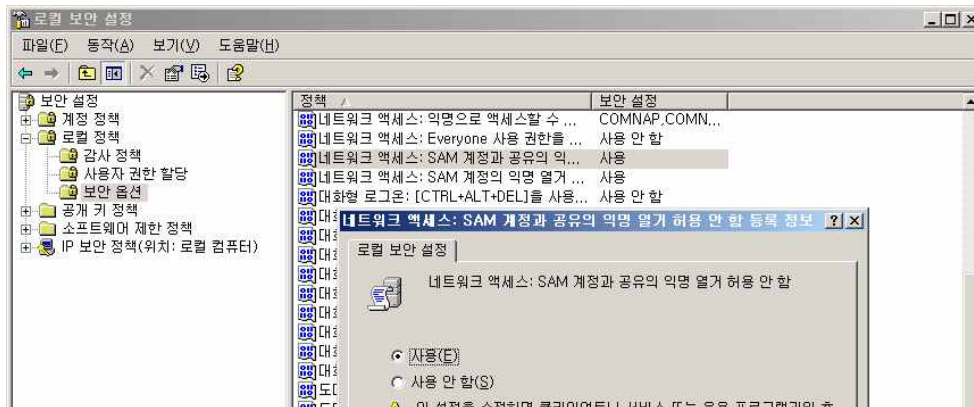


그림 39 SAM 계정과 공유의 이름 열거

- 방화벽과 라우터에서 135~139(TCP, UDP)포트 차단을 통해 외부로부터의 위협을 차단함
- 원천적으로 봉쇄
- 네트워크 및 전화 접속 연결> 로컬 영역> 등록 정보> 고급> 고급 설정> Microsoft 네트워크 파일 및 프린트 공유를 해제하여야 함

조치시 영향	일반적으로 영향 없음
--------	-------------

표 25 SAM 계정과 공유의 이름 열거 허용 안 함

취약점 항목	5.10 디스크볼륨 암호화 설정				
대상 OS	Window 2003	위험도	상	Code	W-71
취약점 개요	디스크 볼륨이 암호화 되어 있지 않은 경우 비인가자가 데이터를 열람할 수 있음.				
	보안대책				
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				
	보안 설정 방법				

1. 폴더 선택 > 속성 > [일반] 탭 > 고급 > 고급 특성

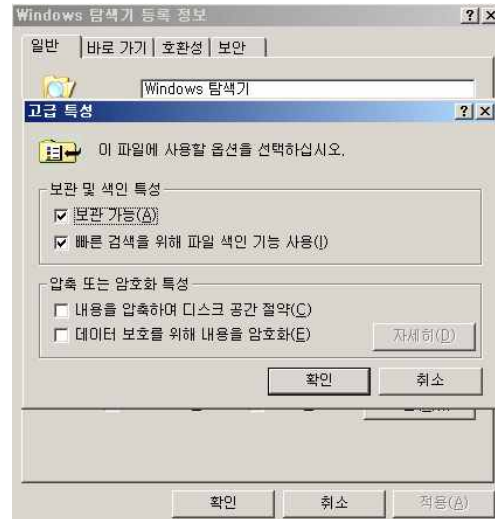


그림 40 디스크볼륨 암호화 설정

2. “데이터 보호를 위해 내용을 암호화” 선택

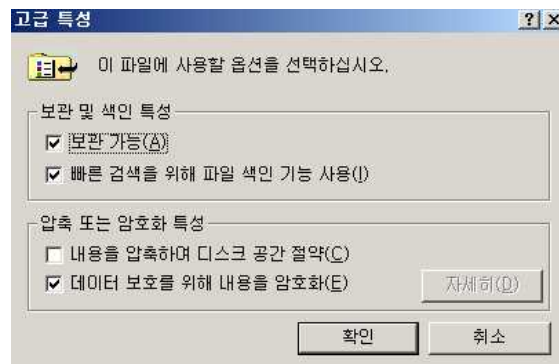


그림 41 디스크볼륨 암호화 설정

조치시 영향	복호키 분실 시 데이터복구 어려움
--------	--------------------

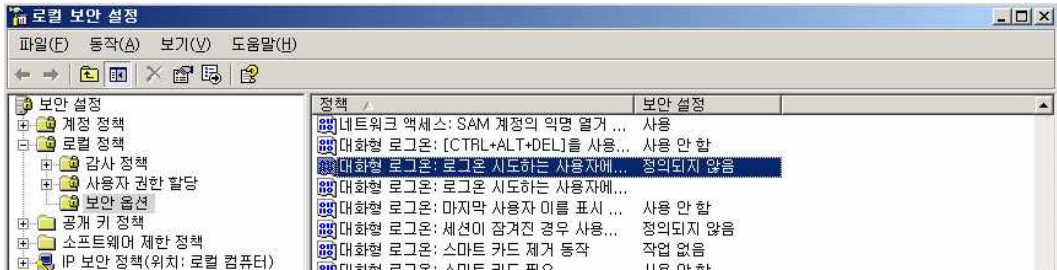
표 26 디스크볼륨 암호화 설정

취약점 항목	5.11 DoS공격 방어 레지스트리 설정				
대상 OS	Window 2003	위험도	중	Code	W-72
취약점 개요	DoS(서비스 거부 공격)은 네트워크 사용자가 컴퓨터나 컴퓨터의 특정 서비스를 사용할 수 없도록 만들기 위한 네트워크 공격으로, TCP/IP 스택(Stack)을 강화하는 레지스트리 값 변경을 통하여 DoS 공격을 방어할 수 있음. 만약 DoS 방어 레지스트리를 설정하지 않은 경우 DoS 공격에 의한 시스템 다운으로 서비스 제공이 중단될 수 있음.				
보안대책					

KeepAliveTime	REG_DWORD	1 - 0xFFFFFFFF	300,000(5분)으로 변경
NoNameReleasedOnDemand	REG_DWORD	0, 1 (False, True)	1 (True)

조치시 영향	잘못된 값을 설정할 경우 OS 재설치를 요구할 수 있음
--------	--------------------------------

표 27 DoS공격 방어 레지스트리 설정

취약점 항목	5.14 경고 메시지 설정				
대상 OS	Window 2003	위험도	하	Code	W-75
취약점 개요	<p>시스템에 로그온을 시도하는 사용자들에게 관리자는 시스템의 불법적인 사용에 대하여 경고 창을 띄움으로써 경각심을 줄 수 있음. 이러한 경고창의 효과는 악의적인 사용자에게 관리자가 적절한 보안수준으로 시스템을 보호하고 있으며, 공격자의 활동을 주시하고 있다는 생각을 상기시킴으로써 간접적으로 공격 피해를 감소시키는 효과를 볼 수 있음.</p>				
보안대책					
판단기준	양호 : 로그인 경고 메시지제목 및 내용이 설정되어 있는 경우				
	취약 : 로그인 경고 메시지제목 및 내용이 설정되어 있지 않은 경우				
조치방법	로그인 메시지 제목 및 메시지 내용에 경고 문구 삽입				
보안 설정 방법					
1. 시작 > 실행 > secpol.msc > 로컬 정책 > 보안 옵션					
					
그림 42 배너					
2. 대화형 로그온: 로그온 시도하는 사용자에게 대한 메시지 제목 : 배너 제목 입력					

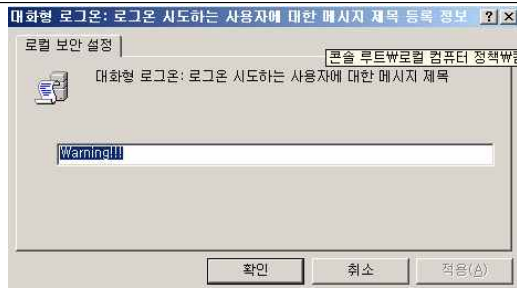


그림 43 배너 제목

3. 대화형 로그인 : 로그인 시도하는 사용자에게 대한 메시지 텍스트 : 배너 내용 입력

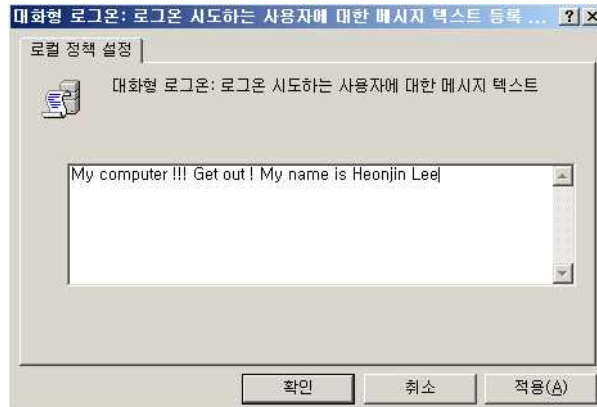


그림 44 배너 내용

조치시 영향	일반적인 경우 영향 없음
--------	---------------

표 30 경고 메시지 설정

취약점 항목	5.16 LAN Manager 인증 수준				
대상 OS	Window 2003	위험도	중	Code	W-77
취약점 개요	LAN Manager 인증 수준 설정을 통해 네트워크 로그인에 사용할 Challenge/Response 인증 프로토콜을 결정하며, 이 설정은 클라이언트가 사용하는 인증 프로토콜 수준, 협상된 세션 보안 수준 및 서버가 사용하는 인증 수준에 영향을 주기 때문에 보다 안전한 인증을 위해 NTLMv2를 사용하는 것을 권장함. ※ NTLMv2는 Windows 2000, 2003, XP 이상에서 지원되며, Windows 98, NT 버전과 통신 할 경우 패치를 설치하여야 함.				
보안대책					
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 수준 -> NTLMv2 응답만 보냄 Windows 2003: 네트워크 보안: LAN Manager 인증 수준 -> NTLMv2 응답만 보냄				

보안 설정 방법

1. 시작 > 실행 > secpol.msc > 로컬 정책 > 보안 옵션

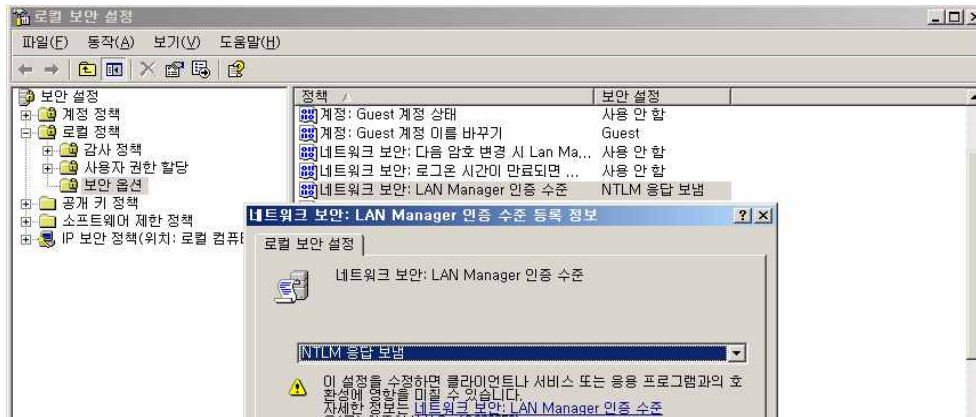


그림 45 LAN Manager 정보

2. “네트워크 보안: LAN Manager 인증 수준 정책에 “NTLMv2 응답만 보냄” 설정

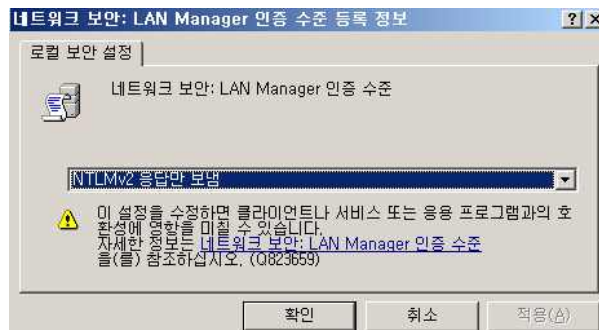


그림 46 NTLMv2 응답만 보냄

조치시 영향

일반적인 경우 영향 없음

표 31 LAN Manager 인증 수준