



서울대학교
SEOUL NATIONAL UNIVERSITY

서버 보안 가이드라인

– Windows 2008 –

2017. 4. 14

정보화본부 정보보안팀

제/개정 이력

버전	제/개정 일자	내용	제/개정자
Ver. 2.0	17. 04. 14.	전면 개정	김재만

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

목 차

1. 계정관리	1
1.1. 로컬 계정 사용 설정	1
1.2. 계정 잠금 정책 설정	5
1.3. 암호 정책 설정	7
1.4. 취약한 패스워드 점검	9
1.5. 사용자 계정 컨트롤(User Account Control) 설정	10
1.6. 익명 SID/이름 변환 허용 정책 점검	12
1.7. 콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한 정책 점검	14
2. 파일 시스템	15
2.1. CMD.EXE 파일 권한 설정	15
2.2. 사용자 홈 디렉터리 접근제한	17
2.3. 공유 폴더 설정	18
2.4. SAM(Security Account Manager) 파일 권한 설정	21
3. 네트워크 서비스	22
3.1. 불필요한 서비스 제거	22
3.2. 터미널 서비스 암호화 수준 설정	25
3.3. NetBIOS 서비스 보안 설정	27
4. 주요 응용 설정	29
4.1. Telnet 서비스 보안 설정	29
4.2. DNS(Domain Name Service) 보안 설정	31
4.3. SNMP(Simple Network Management Protocol) 서비스 보안 설정	33
5. 시스템 보안 설정	35
5.1. 원격 로그파일 접근 진단	35
5.2. 화면 보호기 설정	36
5.3. 이벤트 뷰어 설정	37
5.4. 로그인 시 경고 메시지 표시 설정	38
5.5. 마지막 로그인 사용자 계정 숨김	40
5.6. 로그인 하지 않은 사용자 시스템종료 방지	42
5.7. 로컬 감사정책 설정	44
5.8. 가상 메모리 페이지 파일 삭제 설정	46
5.9. 예약된 작업 의심스런 명령어나 파일 점검	48
5.10. 원격 시스템 종료 권한 설정	50
5.11. 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 방지	51

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

6. 바이러스 진단	52
6.1. 백신 프로그램 설치	52
6.2. 최신 엔진 업데이트	53
7. 레지스트리 보안 설정	54
7.1. SAM(Security Account Manager) 보안 감사 설정	54
7.2. Null Session 설정	56
7.3. Remote Registry Service 설정	58
7.4. AutoLogon 제한 설정	60
8. 보안 패치	61
8.1. 최신 서비스 팩 적용	61
8.2. 최신 HOT FIX 적용	62
9. 이슈 취약점	63
9.1. HeartBleed 취약점	63

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

1. 계정관리

1.1. 로컬 계정 사용 설정

분류	계정관리	보안항목	로컬 계정 사용 설정	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	상
내용 및 적용방법				

로컬계정의 Administrator, GUEST 계정 관리 및 사용하는 계정 점검

■ 기준

- 가. Administrators그룹에 관리자 계정인 Administrator 계정 변경
- 나. GUEST 계정 비활성화
- 다. 사용하는 계정에 대해 “전체이름”또는 “설명” 부분 내용 기입

※가, 나, 다 항목 모두 적용해야 함

양호 - Administrators그룹에 관리자 계정인 Administrator의 이름을 바꾸어 사용하는 경우

Guest 계정 비활성화되어 있는 경우
불필요한 계정이 존재하지 않을 경우

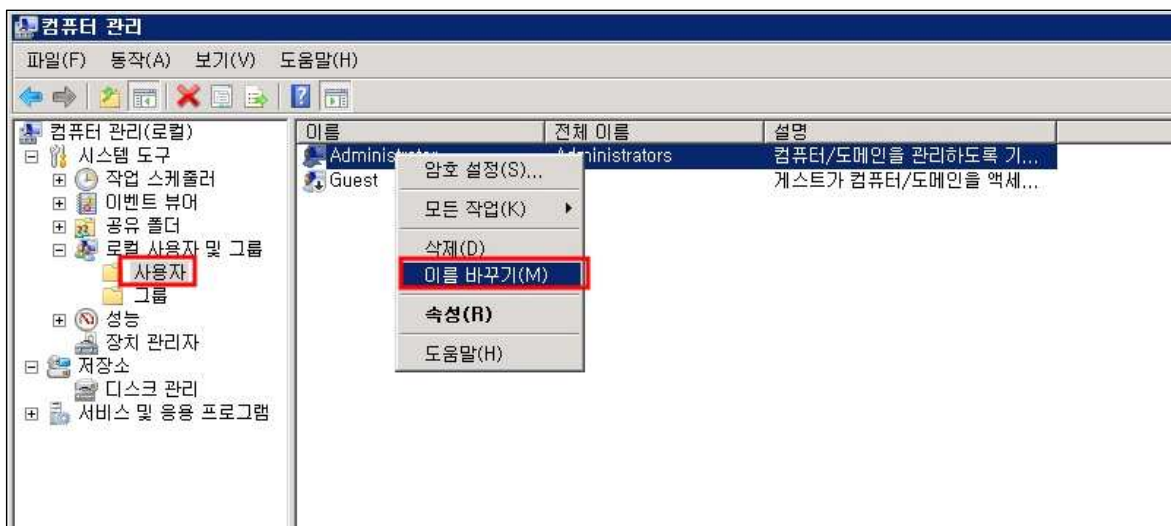
취약 - Administrators그룹에 관리자 계정인 Administrator가 존재하는 경우

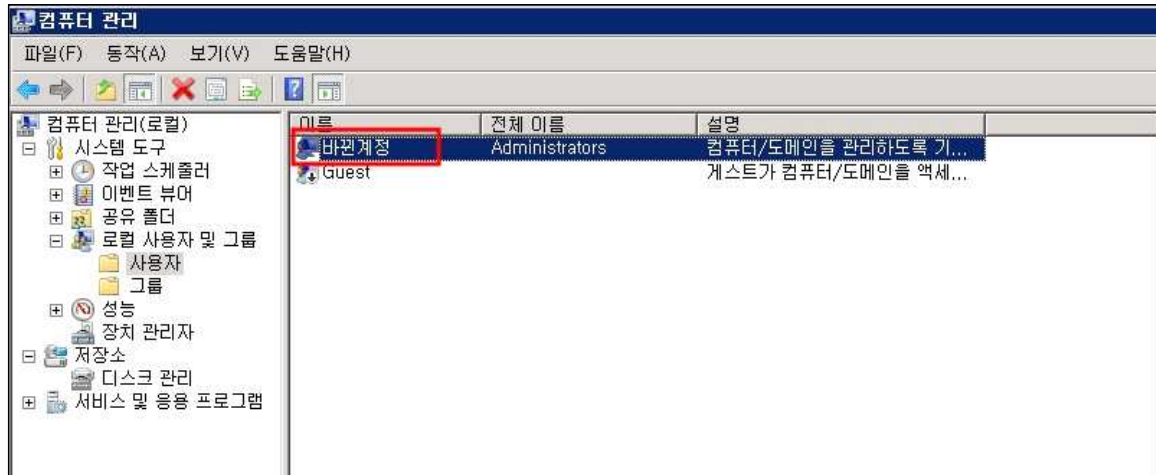
Guest 계정 활성화되어 있는 경우
불필요한 계정이 존재할 경우

■ 조치방법

1. Administrators 그룹에 관리자 계정인 Administrator 계정 변경

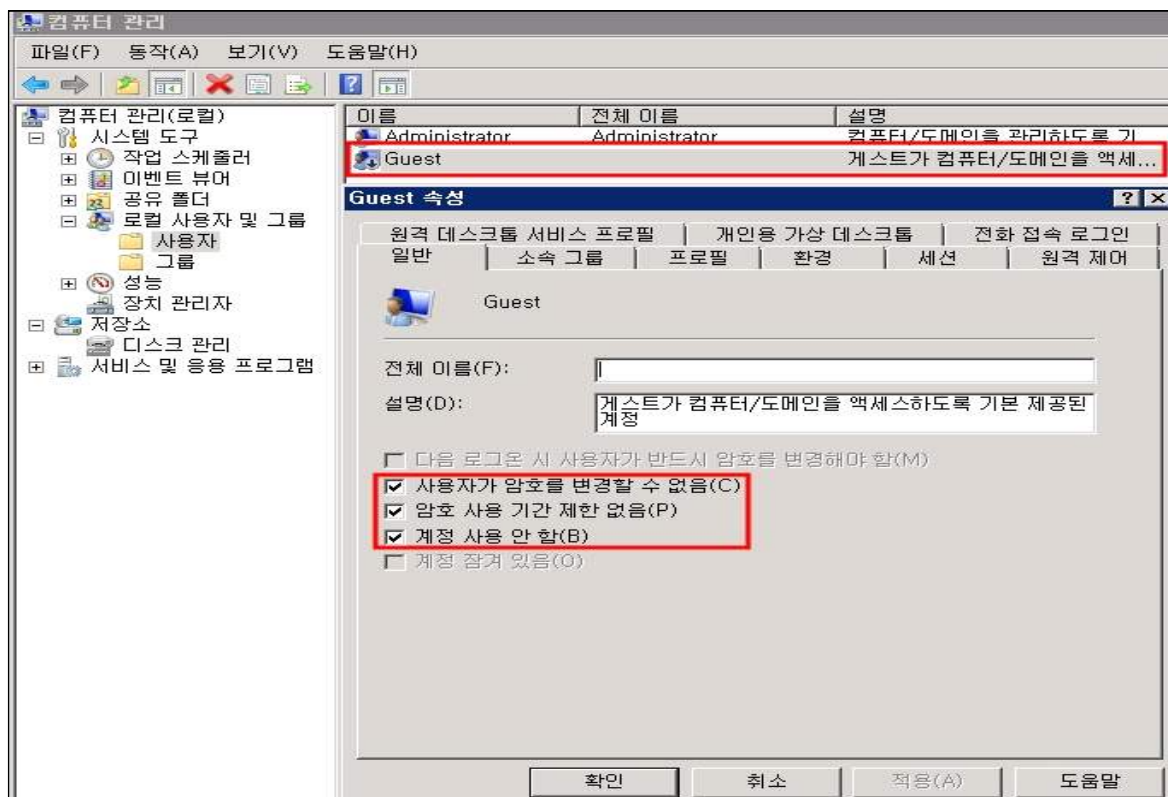
시작 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹> 사용자 > Administrator 이름 바꾸기
선택 관리자 계정 변경





2. GUEST 계정 비 활성화

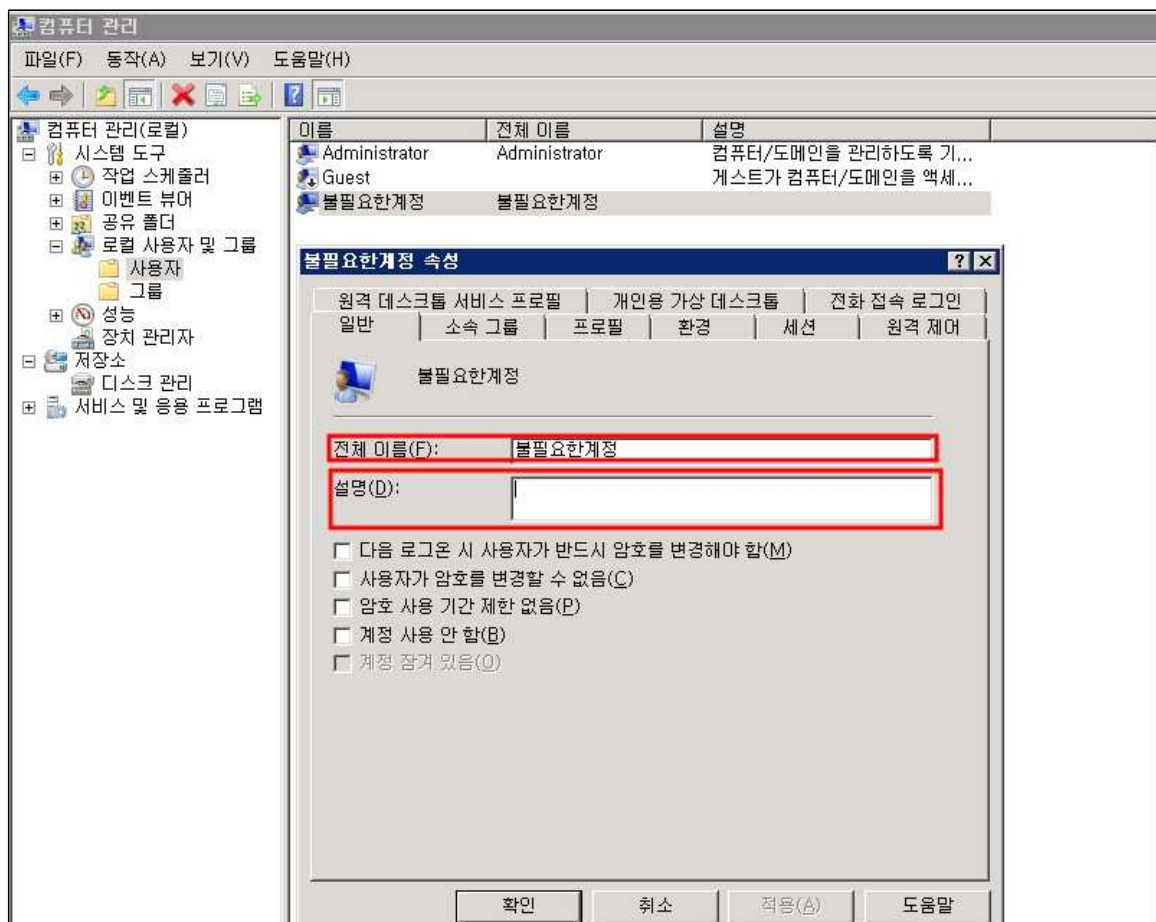
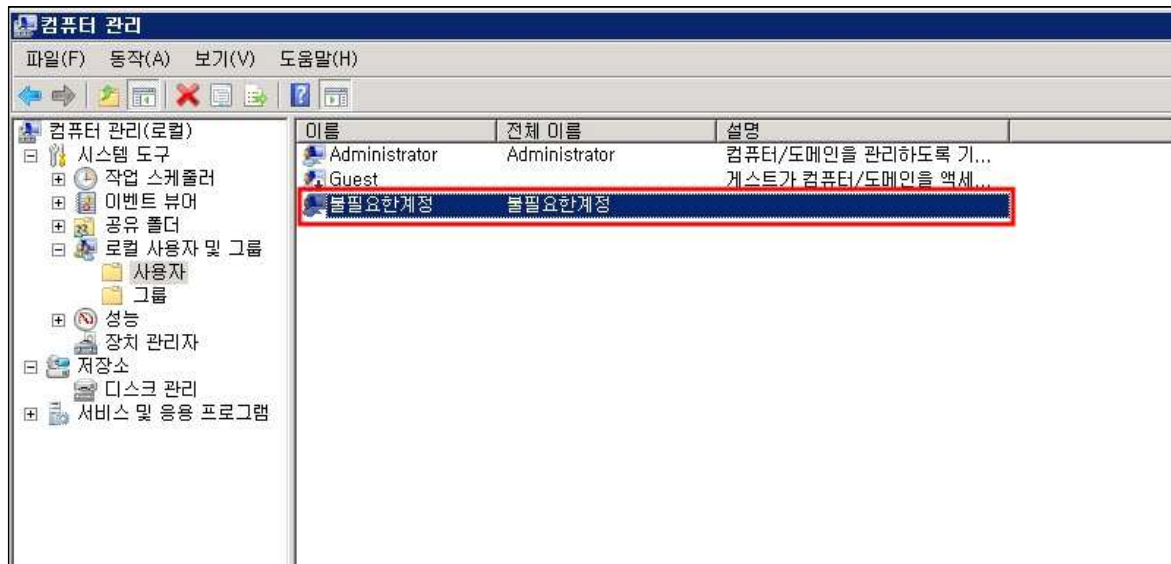
시작 > 관리도구 > 컴퓨터 관리 > 로컬 사용자 및 그룹 > 사용자 > Guest 계정에 대한 사용 제한 설정



3. 무자격 사용자 ID 제거

[무자격 사용자 ID 제거 조치 방법]

시작 > 관리도구 > 컴퓨터관리 > 로컬 사용자 및 그룹 > 사용자를 선택하여 더 이상 사용되지 않는 계정을 제거



■ 상세설명

1. Administrators 그룹에 관리자 계정인 Administrator 계정 변경

일반적으로 관리자를 위한 계정과 일반 사용자들을 위한 계정을 분리하여 사용하는 것이 바람직하며 만일 시스템 관리자라면 두 개의 계정을 가지는 것이 좋음. 하나는 관리업무를 위한

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

것이고, 다른 하나는 일반적인 일을 하기 위한 것임. 예를 들어 일반사용자 권한으로부터 활성화된 바이러스에 비해 관리자 권한을 가진 계정으로부터 활성화된 바이러스라면 시스템에 훨씬 많은 피해를 줄 수 있음.

또한 관리자 계정으로 설정되어 있는 "Administrator" 계정을 다른 이름으로 바꾸고 "Administrator"라는 가짜 계정을 만들어 아무런 권한도 주지 않는 방법을 사용할 수 있는데, 이러한 방법은 "모호함을 통한 보안(Security through obscurity)"의 한 예임. 즉 Bogus 계정을 만드는 것임.

Administrator 계정은 로그인 시 몇 번이고 실패해도 절대 접속을 차단하지 않기 때문에 시스템을 공격하려는 사람들은 이 계정의 패스워드 유추를 계속 시도할 수 있음. 따라서 관리자 계정의 이름을 바꿈으로써 공격자는 패스워드뿐만 아니라 계정이름도 유추 하여야 하는 어려움을 줄 수 있음.

또 하나의 방법은 보안정책 설정에서 로그인 실패 횟수에 따른 계정 잠금을 설정함으로써 brute force 공격이나 사전공격에 대응할 수 있음.

Administrator 계정을 관리자 계정이 아닌 일반 계정으로 사용하거나 Administrator 가 아닌 다른 이름의 관리자 계정을 생성해 사용하도록 해야 하며, Administrator 권한을 가지는 유저는 최소한의 숫자로 제한 되어야 함. 또한, Password는 최소 8자리 이상으로 숫자와 영어, 특수문자를 혼합하여 사용

2. GUEST 계정 비활성화

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

3. 사용하는 계정에 대해 “전체이름” 또는 “설명” 부분 내용 기입

퇴직, 전직, 휴직 등의 이유로 더 이상 사용하지 않는 계정, 불필요한 계정, 의심스러운 계정이 있는지 점검 함.

아래 계정에 대해서는 기본적으로 사용되는 계정으로써 설명이 불충분해도 무방

whoau	컴퓨터/도메인을 관리하도록 기본 제공된 계정
secaudit	보안진단 임시계정
bemsadmin	BizEMS 관리자 계정
bewsadmin	NT 통합 백업계정
ctsa	CONTROL-SA 계정
opsadmin	operator 계정
Ecmadmin	ECM 관리자 계정
Exrunmanager	Exchange 서비스 계정
Mcmsservice	전화연동을 위한 서비스 계정
Tbmsadmin	tbms 관리자 계정

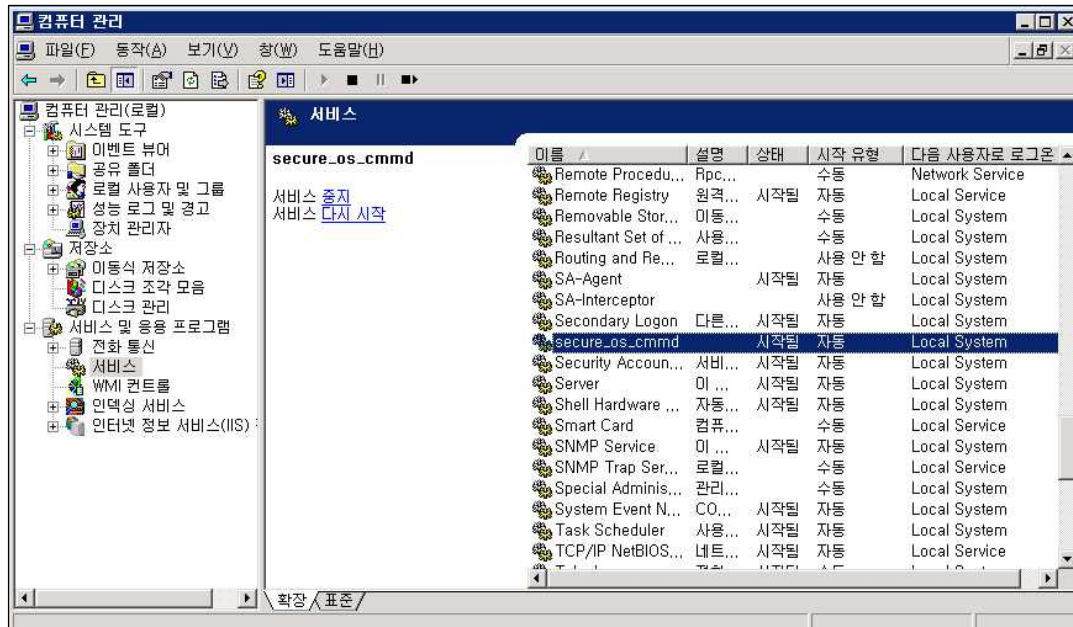
비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

1.2. 계정 잠금 정책 설정

분류	계정관리	보안항목	계정 잠금 정책 설정	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	상
내용 및 적용방법	<p>시스템 보안을 위한 계정 잠금 설정</p> <p>■ 기준</p> <div style="border: 1px solid black; padding: 10px; margin: 10px 0;"> 가. 계정 잠금 기간 60분 이상, 계정 잠금 임계값 5번 이하 계정 잠금 기간 원래대로 설정 60분 이상 ※ AMS(접근제어관리시스템)에 연동되어 있을 경우(레드아울, Control-SA 등) Active Directory 로 로그인한 경우 예외처리 </div> <p>양호 - 계정 잠금 기간 60분, 계정 잠금 기간 원래대로 설정 60분 계정 잠금 임계 값 5번</p> <p>취약 - 계정 잠금 기간 및 잠금 기간 원래대로 설정 기간이 60분 보다 작거나, 계정 잠금 임계 값 5번보다 클 경우</p> <p>■ 조치방법</p> <p>제어판 > 관리도구 > 로컬 보안 정책 > 계정 정책 > 계정 잠금 정책 > “계정 잠금 기간” / ”다음 시간 후 계정 잠금 수를 원래대로 설정” 을 “60분”으로 설정 “계정 잠금 임계 값”을 “5번”으로 설정</p> <div style="border: 1px solid black; height: 150px; margin: 10px 0;"></div> <p>※ AMS 확인방법 예시(레드아울) 컴퓨터 관리>서비스>secure_os_cmmd 서비스 [시작됨]</p>			



■ 상세설명

시스템 보안향상을 위해 보안정책 설정에서 로그인 실패 횟수와 시간에 따른 계정 잠금 기간 및 계정 잠금 복귀 시간을 설정함으로써 brute force 공격이나 패스워드 크랙 공격에 대응할 수 있도록 잠금정책을 점검 함.

계정 잠금 기간 60분으로 설정 : 만일 사용자가 로그인을 시도할 때 정해진 횟수 이상 로그인에 실패하면 시스템은 자동적으로 해당 계정을 60분 동안 잠기게 됨

다음 시간 후 계정 잠금 수를 원래대로 설정 60분으로 설정 : 잠겨진 계정으로 다시 로그인을 시도할 수 있는 시간간격은 60분 임

5번 잘못된 로그인 시도 후 계정 잠금 : 로그인 시도 횟수를 5번으로 설정하며, 5번 이상 로그인에 실패 하였을 경우 계정 잠금 시간만큼 계정은 잠기게 됨

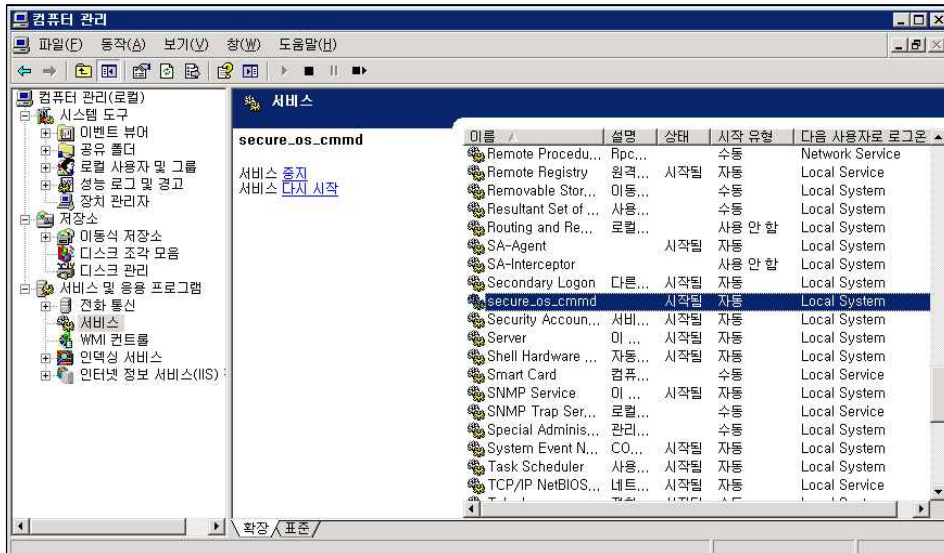
비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

1.3. 암호 정책 설정

분류	계정관리	보안항목	암호 정책 설정	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	상
내용 및 적용방법				
패스워드 추측 공격을 방지하기 위한 사용자 패스워드 정책 설정				
■ 기준				
<div><div>가. 암호정책 설정</div><div>암호는 복잡성을 만족해야 함 → “사용”</div><div>최근 암호 기억 → “12”</div><div>최대 암호 사용 기간 → “60일(이하)”</div><div>최소 암호 길이 → “8문자(이상)”</div><div>최소 암호 사용 시간 → “1일(이상)”</div><div>해독 가능한 암호화를 사용하여 암호 저장 → “사용안함”</div><div>나. 패스워드 설정</div><div>문자/숫자/특수문자 2종류 이상의 조합으로 10자 이상, 3종류 이상의 조합으로 8자 이상</div><div>※ AMS(접근제어관리시스템)에 연동되어 있을 경우(레드아울, Control-SA 등)</div><div>Active Directory 로 로그인한 경우 예외처리</div></div>				
<div>양호 - 위 기준을 모두 만족할 때</div> <div>취약 - 위 기준 중 하나라도 만족하지 않을 때</div>				
■ 조치방법				
1. 암호정책 설정 방법				
시작 > 관리도구 > 로컬 보안 정책>계정정책>암호 정책 선택 후 설정				
<div></div>				
※ AMS 확인방법 예시(레드아울)				
컴퓨터 관리>서비스>secure_os_cmmd 서비스 [시작됨]				



2. 패스워드 설정 기준

1) 패스워드는 아래의 4가지 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성

(1) 영문 대문자 (26개), 영문 소문자 (26개), 숫자 (10개), 특수문자 (32개)

2) 패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계

- (1) Null 패스워드 사용 금지
- (2) 문자 또는 숫자만으로 구성 금지
- (3) 사용자 ID와 동일하거나 유사하지 않은 패스워드 금지
- (4) 연속적인 문자/숫자(예. 1111, 1234, abcd) 사용 금지
- (5) 주기성 패스워드 재사용 금지
- (6) 전화번호, 생일같이 추측하기 쉬운 개인정보 패스워드로 사용 금지

3) SAM 파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호사용을 권장 (8자의 암호사용 권장)

4) 아래와 같은 암호는 설정 지양

Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자성명, 대표업무명

“root”, “rootroot”, “root123”, “123root”, “admin”, “admin123”, “123admin”, “osadmin”, “adminos”

■ 상세설명

패스워드 추측공격을 피하기 위하여 패스워드 최소길이를 설정하고, 패스워드가 임의의 경로를 통해 유출되었을 때, 임의로 접속한 사용자가 언제든지 다시 접속할 수 있는 환경을 방지하기 위해 패스워드 날짜 제한을 점검함

더욱 보안을 강화하기 위하여, 각 사용자의 로그인 시간 및 로그인 가능 워크스테이션 정의, 계정 사용기간 정의, RAS(Remote Access Service) 기능 사용시 Call-back 기능 등 대단히 다양한 보안기능을 설정할 수 있으며 사용자 권한 정책의 변화는 사용자가 다음에 로그인 할 때 적용됨.

비고

장기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

1.4. 취약한 패스워드 점검

분류	계정 관리	보안항목	취약한 패스워드 점검	
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)		중요도	상
내용 및 적용방법				
<p>패스워드가 없거나, 사용자 ID와 동일 또는 유추가 용이한 쉬운 패스워드를 사용하고 있는지 점검함.</p>				
<p>■ 기준</p> <div><p>가. 계정과 유사하지 않은 8자 이상의 영문, 숫자, 특수문자의 조합으로 암호를 설정해야 함</p></div>				
<p>양호 - 계정과 유사하지 않은 8자 이상의 영문/숫자/특수문자의 조합으로 암호가 설정된 경우 취약 - 계정과 유사하지 않은 8자 이상의 영문/숫자/특수문자의 조합으로 암호 설정되지 않은 경우</p>				
<p>■ 조치방안</p> <p><패스워드 설정 기준></p> <p>1. 패스워드는 아래의 4가지 문자 종류 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성</p> <p>1) 영문 대문자 (26개), 영문 소문자 (26개), 숫자 (10개), 특수문자 (32개)</p> <p>2. 패스워드는 비인가자에 의한 추측이 어렵도록 다음의 사항을 반영하여 설계</p> <p>1) Null 패스워드 사용 금지</p> <p>2) 문자 또는 숫자만으로 구성 금지</p> <p>3) 사용자 ID와 동일하거나 유사하지 않은 패스워드 금지</p> <p>4) 연속적인 문자/숫자(예. 1111, 1234, abcd) 사용 금지</p> <p>5) 주기성 패스워드 재사용 금지</p> <p>6) 전화번호, 생일같이 추측하기 쉬운 개인정보 패스워드로 사용 금지</p> <p>3. SAM 파일에 암호를 저장하기 위해 사용되는 LANMan 알고리즘은 8자 단위로 글자를 나누어 암호화하기 때문에 8의 배수가 되는 암호사용을 권장 (8자의 암호사용 권장)</p> <p>4. 아래와 같은 암호는 설정 지양</p> <p>Null, 계정과 동일하거나 유사한 스트링, 지역명, 부서명, 담당자성명, 대표업무명, “root”, “rootroot”, “root123”, “123root”, “admin”, “admin123”, “123admin”, “osadmin”, “adminos”</p>				
비고	장기 적용(적용 시 개발자 및 운영자 협의)			

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

1.5. 사용자 계정 컨트롤(User Account Control) 설정

분류	계정관리	보안항목	사용자 계정 컨트롤 설정	
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)		중요도	하
내용 및 적용방법				

UAC 사용으로 권한 없는 사용자의 프로그램 설치 설정 변경을 제한

■ 기준

- 가. 사용자 계정 컨트롤(UAC) 사용 (Windows 2008)
 사용자 계정 컨트롤(UAC) 사용 (Windows 2008 R2)
 - ‘프로그램에서 사용자 모르게 컴퓨터를 변경하려는 경우에만 알림’ 이상

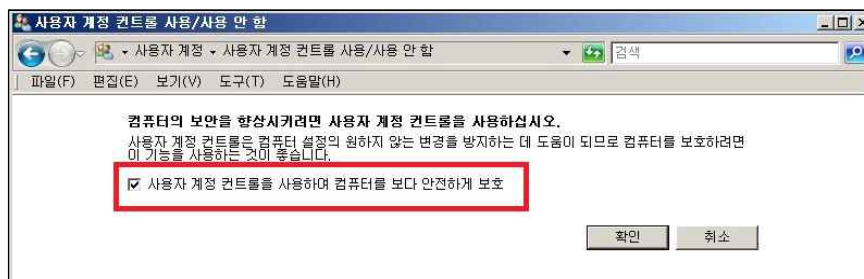
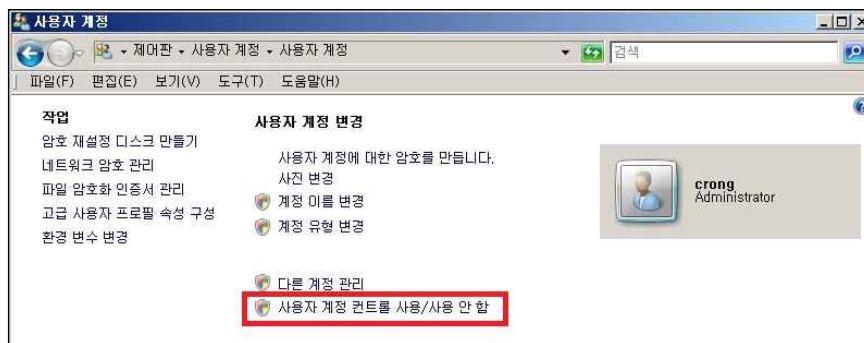
양호 - 사용자 계정 컨트롤(UAC) 사용

취약 - 사용자 계정 컨트롤(UAC) 사용 안함

■ 조치방법

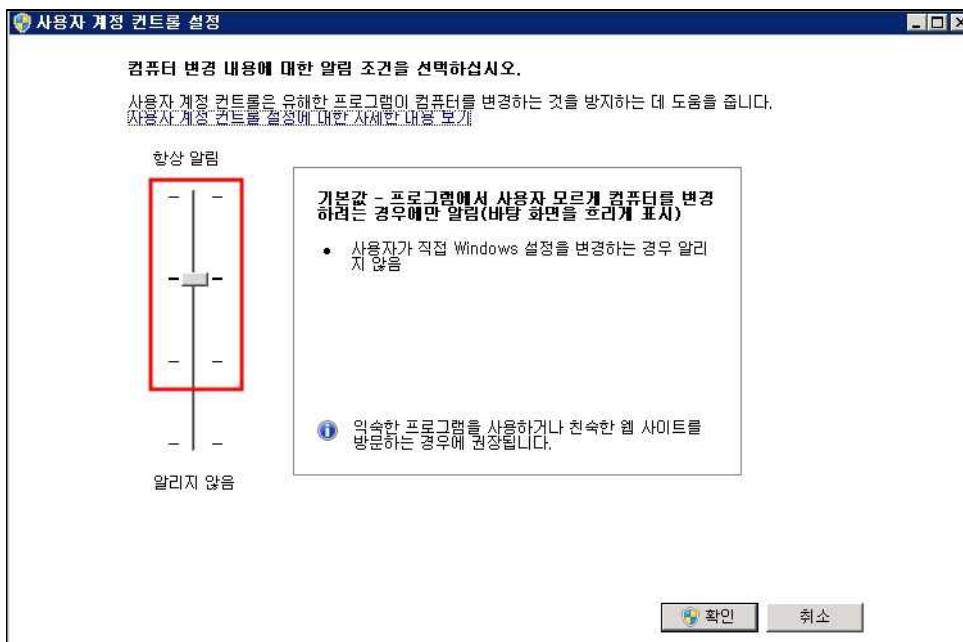
[Windows 2008 인 경우]

시작 > 제어판 > 사용자 계정 > 사용자 계정 > 사용자 계정 컨트롤 사용/사용 안 함 > ‘사용자 계정 컨트롤을 사용하여 컴퓨터를 보다 안전하게 보호’ 체크



[Windows 2008 R2인 경우]

시작 > 제어판 > 사용자 계정 > 사용자 계정 > 사용자 계정 컨트롤 설정 변경 > ‘프로그램에서 사용자 모르게 컴퓨터를 변경하려는 경우에만 알림’ 이상



■ 상세설명

사용자 계정 컨트롤(UAC, User Account Control) 기능은 Windows VISTA버전부터 추가된 보안 기능임. 제한된 전체관리자 권한, 제한된 일반유저 권한, Guest권한으로 분류됨.

일반적으로 사용자가 운영체제 설치 후 갖게 되는 계정은 제한된 일반유저 권한으로 데스크톱(explorer.exe)을 실행한다. 따라서 기본적으로 관리자를 포함한 모든 사용자는 Windows 시스템에 일반유저(관리자계정, 표준사용자계정)로 로그인하게 된다. 단 Guest 계정은 별도의 Guest 권한만을 사용할 수 있음.

사용자 계정 컨트롤(UAC)에서는 컴퓨터의 작동에 영향을 줄 수 있는 작업을 실행하거나 다른 사용자에게 영향을 주는 설정을 변경하려고 할 때, 설정을 변경하기 전에 사용 권한이나 관리자 암호를 요구하는 방식으로 악성소프트웨어(malware) 및 스파이웨어가 사용권한 없이 시스템에 설치 및 실행되는 것을 방지함.

비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

1.6. 익명 SID/이름 변환 허용 정책 점검

분류	계정관리	보안항목	익명 SID/이름 변환 허용 정책		
대상 OS	Windows 2008			중요도	중
내용 및 적용방법					

익명 SID/이름 변환 허용 정책이 “사용 안 함” 으로 설정되어 있는지 점검함.

■ 기준

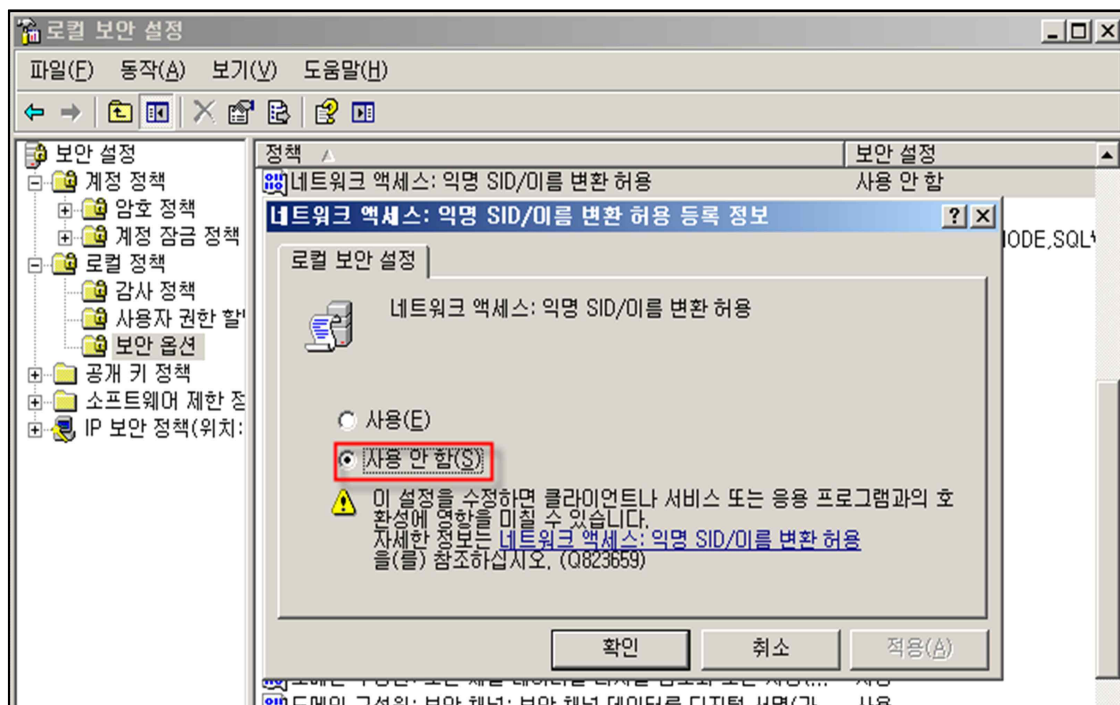
가 “익명 SID/이름 변환 허용” 정책이 “사용 안 함”으로 설정해야 함

양호 - “익명 SID/이름 변환 허용” 정책이 “사용 안 함” 으로 설정 되어 있는 경우

취약 - “익명 SID/이름 변환 허용” 정책이 “사용” 으로 설정 되어 있는 경우

■ 조치방안

1. 시작 > 실행 > SECPOL.MSC > 로컬 정책 > 보안 옵션
2. “네트워크 액세스: 익명 SID/이름 변환 허용” 정책이 “사용 안 함” 으로 설정



■ 상세설명

이 정책은 익명 사용자가 다른 사용자의 SID 특성을 요청할 수 있는지 결정하는 정책으로 사용 함으로 설정시 이를 이용해 로컬 접근 권한이 있는 사용자가 잘 알려진 Administrator SID를 사용하여 Administrator 계정의 실제 이름을 알아낼 수 있으며 암호 추측 공격을 실행할 수 있음.

구성원 컴퓨터의 경우 이 정책 설정의 기본 구성이 “사용 안 함”으로 설정되어 있으나, 도메인 컨트롤러의 경우 기본 구성은 “사용”으로 설정 되어 있음. 도메인 컨트롤러에 대해 이 정책 설정을 “사용 안 함” 으로 설정할 경우 예를들어 다음과 같은 Windows NT 도메인 환경에서 통신이 불가능 할 수 있으므로 확인이 필요

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

■ 서비스 영향

<익명 SID/이름 변환 허용 정책 “사용 안 함” 설정시 도메인과 통신하지 못할 수 있는 서버>

Windows NT 4.0 기반 원격 액세스 서비스 서버

Windows NT 3.x 기반 컴퓨터 또는 Windows NT 4.0 기반 컴퓨터에서 실행되는 Microsoft SQL Servers

Windows NT 3.x 도메인 또는 Windows NT 4.0 도메인에 있는 Windows 2000 기반 컴퓨터에서 실행되는 원격 액세스 서비스 서버 또는 Microsoft SQL Server

비고	장기 적용(적용 시 개발자 및 운영자 협의)
-----------	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

1.7. 콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한 정책 점검

분류	계정관리	보안항목	콘솔 로그인 시 정책 점검
대상 OS	Windows 2008		중요도
내용 및 적용방법			중

콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한 정책이 “사용” 으로 설정되어 있는지 점검함.

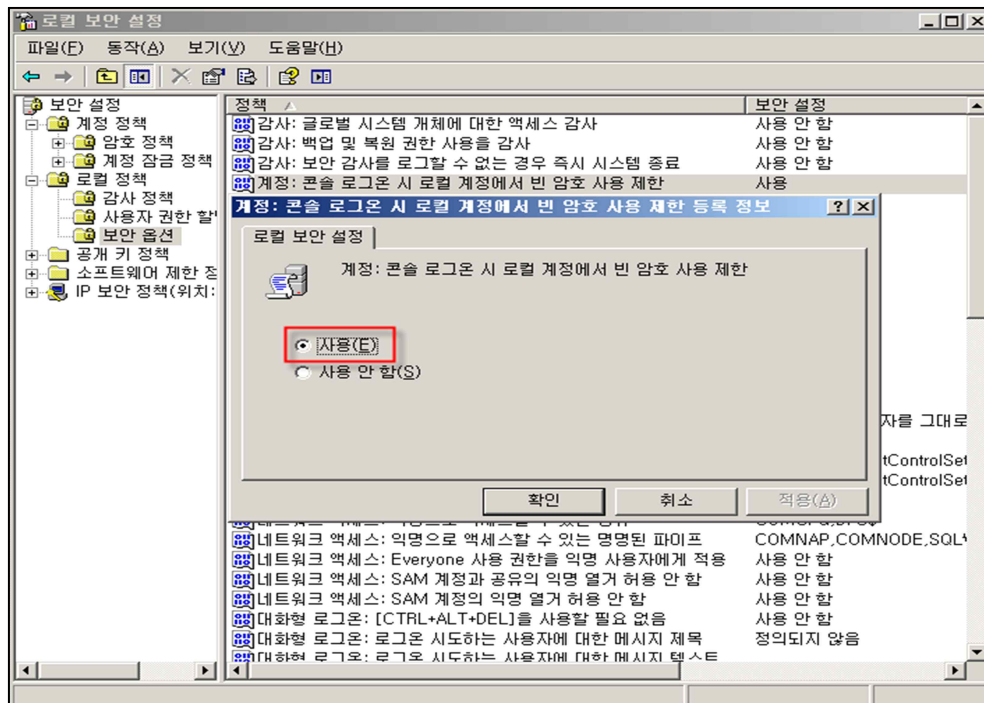
■ 기준

가 “콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한” 정책이 “사용”으로 설정해야 함

양호 - “콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한” 정책이 “사용”으로 설정 되어 있는 경우
취약 - “콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한” 정책이 “사용 안 함”으로 설정 되어 있는 경우

■ 조치방안

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. “콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한” 정책을 “사용” 으로 설정



■ 상세설명

이 정책은 암호로 보호되지 않는 로컬 계정을 사용하여 터미널 서비스, Telnet 및 FTP와 같은 네트워크 서비스의 원격 대화형 로그인이 불가능하게 설정하는 정책으로 “사용안함”으로 설정시 공격자가 물리적으로 안전한 위치에 있지 않는 컴퓨터로 암호가 없는 로컬 계정을 사용하여 로그인 할 수 있으므로 취약함 이 보안 정책은 콘솔에서 수행하는 대화형 로그인이나 도메인 계정을 사용하는 로그인에는 영향을 주지 않음

비고	장기 적용(적용 시 개발자 및 운영자 협의)
----	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

2. 파일 시스템

2.1. CMD.EXE 파일 권한 설정

분류	파일 시스템	보안항목	CMD.EXE 파일 권한 설정
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)	중요도	중
내용 및 적용방법			

IIS 사용시 CMD.EXE 보안 취약점 방지 설정

■ 기준

가. IIS 서비스가 실행 중이 아니거나, administrators, system, TrustedInstaller 만 실행 권한 설정

양호 - IIS 서비스가 실행 중이 아니거나, administrator 와 system, TrustedInstaller 만 실행 권한 설정되어 있을 경우

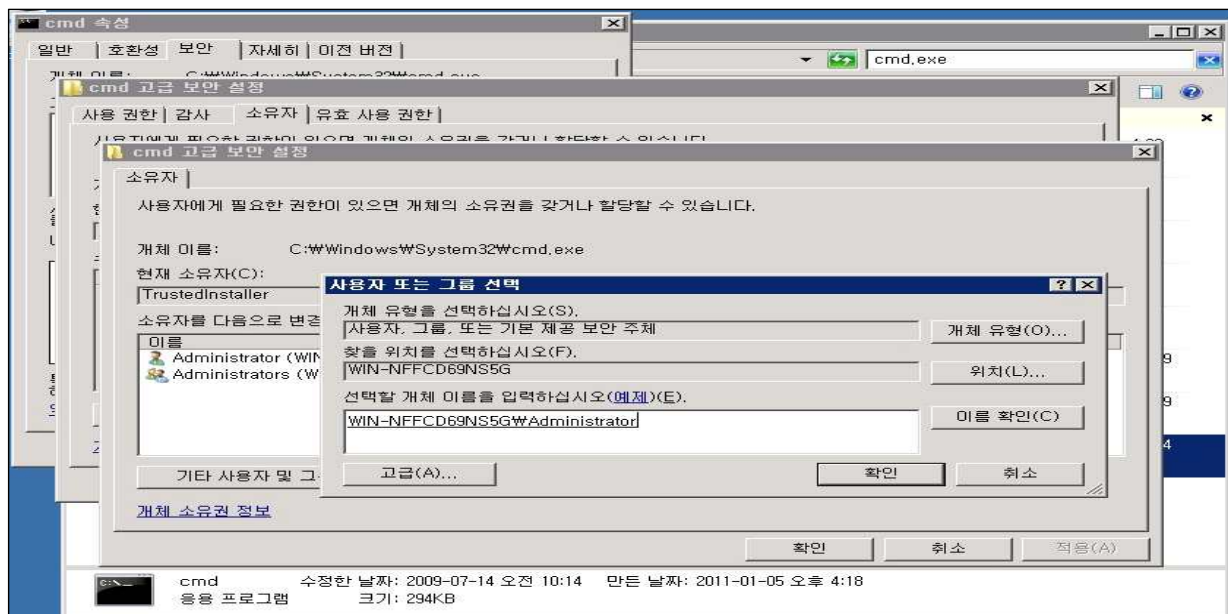
취약 - IIS가 실행 중이면서, administrator 와 system, TrustedInstaller 이 외에도 실행 권한이 설정 되어 있을 경우

■ 조치방법

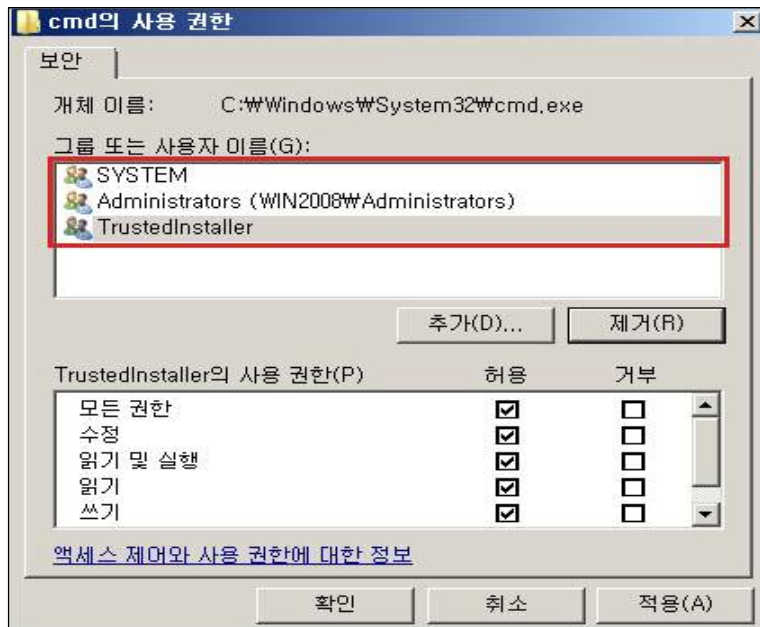
- UAC 보호 설정시 사용권한 설정 및 제거 불가, UAC 해제 후 변경

WRP(Windows Resource Protection) 보안모델이 적용되어 소유자 변경 후 권한 변경

- CMD.EXE 소유자 변경 à C:\WINDOWS\system32\cmd.exe 파일선택 > 속성 > 보안 > 고급 > 소유자 > 편집 > 기타 사용자 및 그룹 > 관리자 계정으로 변경

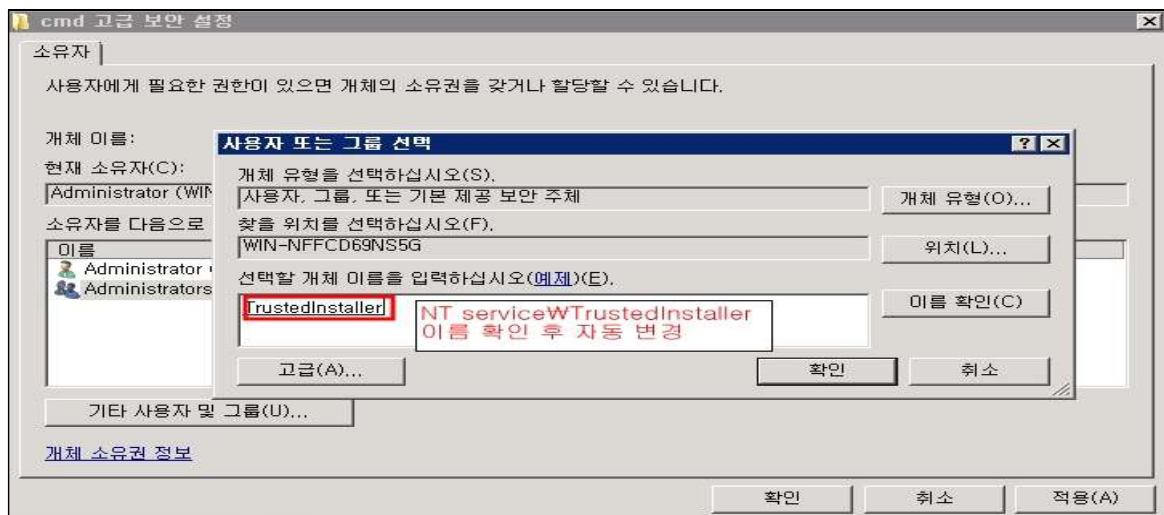


- 탐색기 > C:\WINDOWS\system32\cmd.exe 파일선택 > 속성 > 보안 > administrators, system, TrustedInstaller 외에 권한제거



관리자 계정으로 변경한 파일을 원래대로 소유자 변경

- CMD.EXE 소유자 > C:\WINDOWS\system32\cmd.exe 파일선택 > 속성 > 보안 > 고급 > 소유자 > 편집 > 기타 사용자 및 그룹 > NT service\TrustedInstaller 로 변경



■ 상세설명

IIS는 batch파일을 Interpret하기 위해서 자동적으로 cmd를 실행하는데 여기서 요청된 파일의 다른 부분을 이용해 공격자는 '&' 와 같은 Character를 삽입함으로써 원하는 명령을 실행 가능함

비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

2.2. 사용자 홈 디렉터리 접근제한

분류	파일 시스템	보안항목	사용자 홈 디렉터리 접근제한		
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)			중요도	중
내용 및 적용방법					

임의의 사용자 다른 사용자 계정 별 홈디렉토리 접근제한 설정

■ 기준

가. 홈디렉토리 권한중 Users:F 또는 Everyone:F 설정 금지

양호 - 홈 디렉터리 권한 중 Users:F 또는 Everyone:F 가 없을 경우

취약 - 홈 디렉터리 권한 중 Users:F 또는 Everyone:F 가 있을 경우

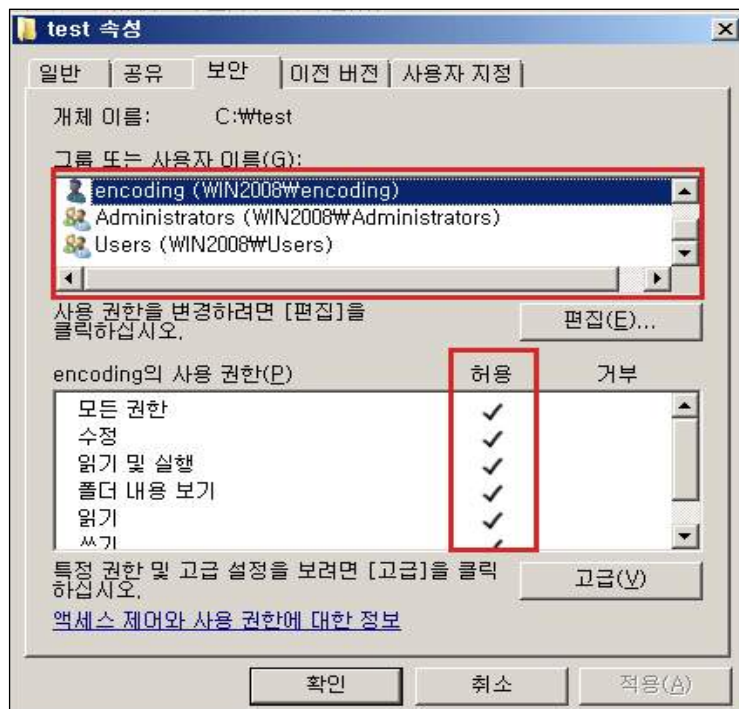
■ 조치방법

- 사용자 홈 디렉터리 권한 설정

1) 디렉터리 위치

Windows 2008 R2: C:\사용자\사용자계정

2) 해당 사용자에게 대한 권한의 일반 계정 삭제



■ 상세설명

사용자 계정 별 홈 디렉터리의 권한이 제한되어 있지 않을 경우 임의의 사용자가 파일 및 디렉터리에 접근이 가능하므로 해당 사용자만의 접근 권한을 설정해야 함.

비고	단기 적용(적용 시 개발자 및 운영자 협의)
----	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

2.3. 공유 폴더 설정

분류	파일 시스템	보안항목	공유 폴더 설정
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)		중요도 상
내용 및 적용방법			

침해사고 예방을 위한 시스템 공유폴더 제거 및 공유 폴더 권한 설정

■ 기준

- 가. C\$, D\$, Admin\$ 등의 기본 공유폴더 제거
- 나. 해당 레지스트리의 AutoShareServer 값 0 으로 설정
- 다. 공유 폴더 사용 시 공유 폴더 접근 권한에 Everyone 제거 및 암호로 보호된 공유 설정

양호 - 기본공유 디렉터리가 없거나 공유 디렉터리 접근 권한에 Everyone 없을 경우

해당 레지스트리의 AutoShareServer 값 = 0, 암호로 보호된 공유 설정이 된 경우

취약 - 기본공유 디렉터리의 접근 권한에 Everyone이 있거나, 암호 보호 공유가 해제된 경우

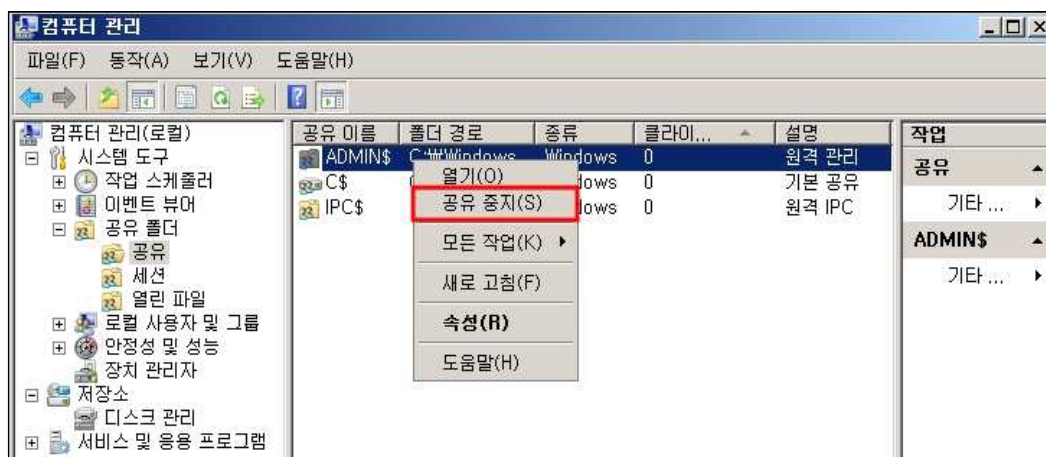
■ 조치방법

<시스템 기본 공유 폴더 제거>

※ 공유제거 방법 1, 또는 2를 통해 공유 제거 후에 레지스트리를 설정

[공유제거 방법 1]

컴퓨터 관리 > 공유폴더 > 공유 > 해당 공유 폴더 마우스 우 클릭 > 공유 중지



[공유제거 방법 2]

CMD창에서 net share 명령어를 이용하여 공유 디렉터리를 확인

net share 공유명 /delete 명령을 통해 공유 제거


```

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.0.6001.1]
(C) Copyright 1985-2005 Microsoft Corp.

C:\Users\Administrator>net share

공유 이름    리소스    설명
-----
C$           C:\       기본 공유
IPC$         C:\       IPC 관리
ADMIN$       C:\Windows
명령을 잘 실행했습니다.

C:\Users\Administrator>net share C$ /delete
C$이<가> 제거되었습니다.

C:\Users\Administrator>net share ADMIN$ /delete
ADMIN$이<가> 제거되었습니다.

C:\Users\Administrator>net share

공유 이름    리소스    설명
-----
IPC$         C:\       원격 IPC
명령을 잘 실행했습니다.

C:\Users\Administrator>
  
```

[레지스트리 값 입력 방법]

1. 시스템 재부팅 후 디폴트 폴더 자동 공유 방지법

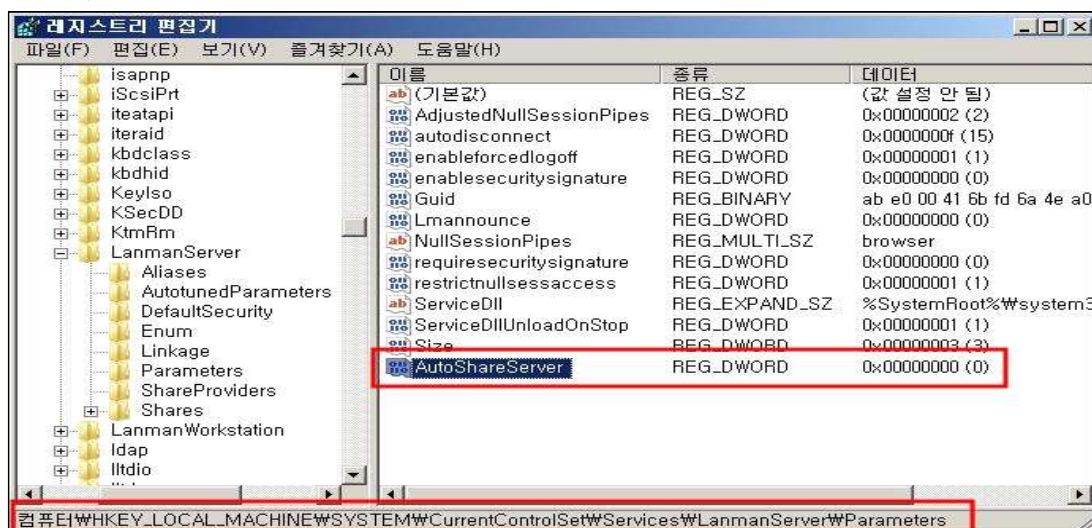
- (1) regedit.exe를 실행
- (2) 레지스트리를 수정

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters

(3) 설정 값 입력

- Value name : AutoShareServer
- Data Type : DWORD(32bit)
- Value : 0(zero)

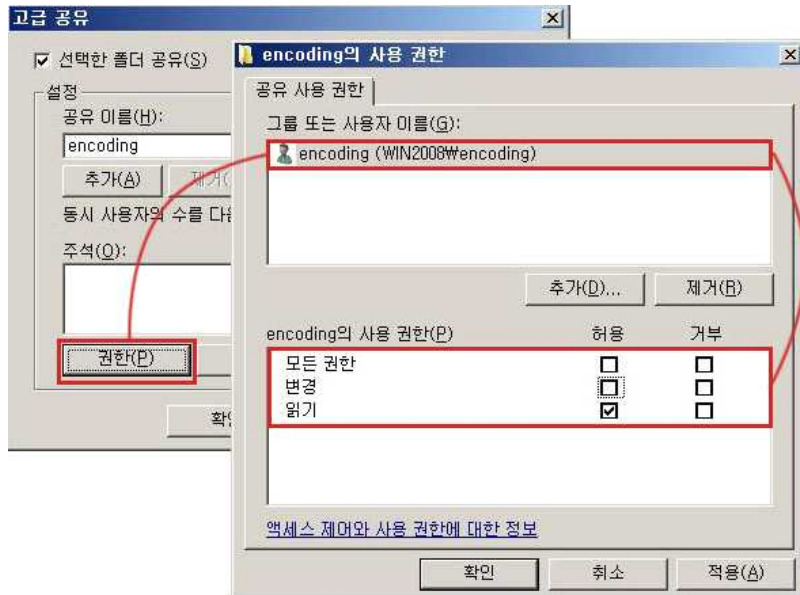
아래 그림과 같이 AutoShareServer를 추가하거나 값을 0으로 변경



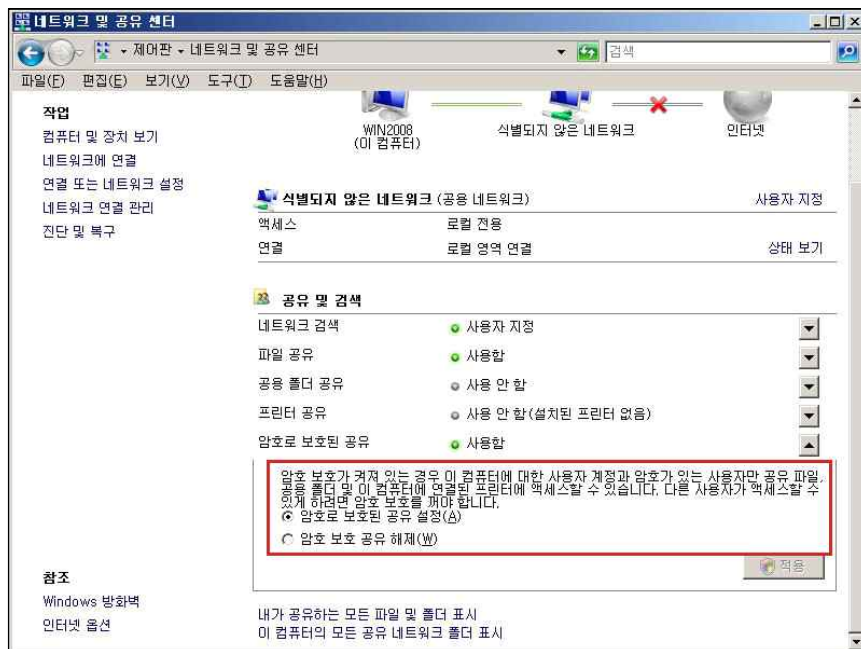
또한, 방화벽과 라우터에서 135,139(TCP/UDP)포트를 차단하여 외부로부터의 위험을 제거함으로써 보안성을 높일 수 있음

<공유 폴더 사용 시 권한 설정>

공유 디렉터리 -> 속성 -> 공유탭 선택 -> 사용권한 에서 Everyone으로 된 공유를 제거하고 접근이 필요한 계정의 적절한 권한을 추가



제어판 > 네트워크 및 인터넷 > 네트워크 및 공유센터 > 암호로 보호된 공유에서 공유설정



■ 상세설명

시스템의 기본공유 항목이 제거되지 않게 되면 모든 시스템 자원에 접근할 수 있는 위험한 상황이 발생할 수 있음. 최근에 발생한 Nimda 바이러스도 여러 가지 방법 중에서 이러한 공유기능을 침투의 한 경로로 이용한 것임.

비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

2.4. SAM(Security Account Manager) 파일 권한 설정

분류	파일 시스템	보안항목	SAM 파일 권한 설정	
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)		중요도	상
내용 및 적용방법				

사용자와 그룹계정을 다루고 LSA 인증을 제공하는 SAM 파일 접근 제한 설정

■ 기준

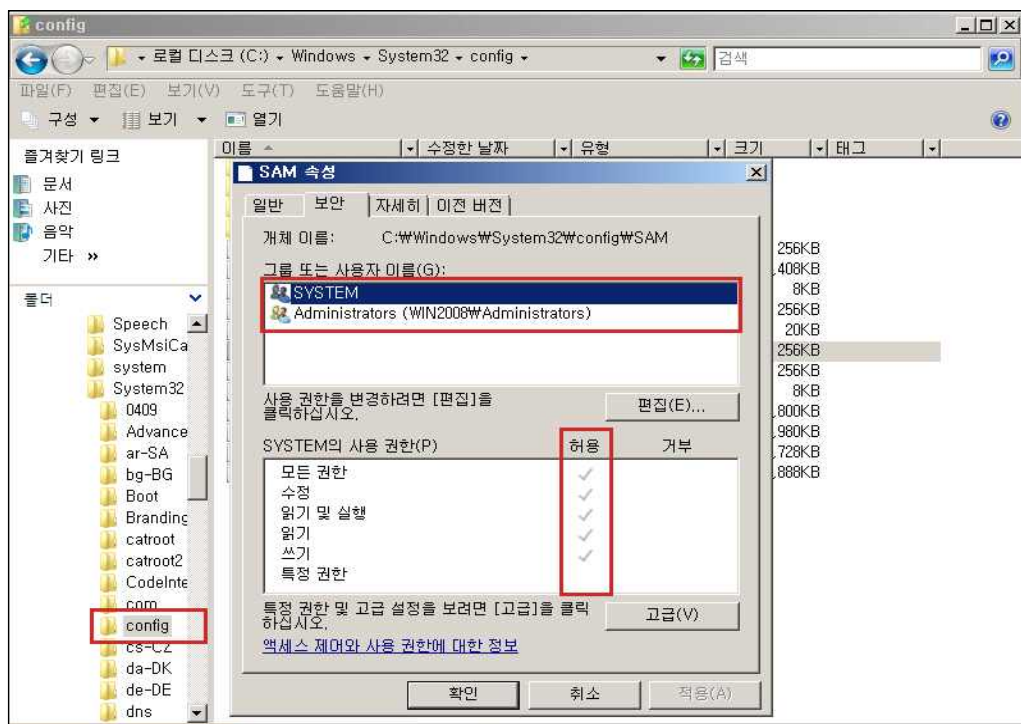
가. SAM 파일 접근권한이 Administrators, System 그룹만 모든 권한 설정

양호 - SAM 파일 접근권한이 Administrator, System 그룹만 모든 권한으로 등록되어 있는 경우

취약 - SAM 파일에 Administrator, System 그룹 외 다른 그룹에 권한이 설정되어 있을 경우

■ 조치방법

[Windows]\WINDOWS\System32\config\SAM파일 > 속성 > 보안 > Administrators, System 그룹만 모든 권한으로 등록되어 있는지 확인



■ 상세설명

Security Account Manager (SAM) 파일은 사용자와 그룹 계정들을 다루고, LSA를 위한 인증을 제공함. 패스워드 공격 시도에 의한 Password Database 노출될 수 있으므로 Administrator 및 System 그룹외에는 SAM 파일에 대한 접근이 제한 되어야 함

비고	단기 적용(적용 시 개발자 및 운영자 협의)
----	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

3. 네트워크 서비스

3.1. 불필요한 서비스 제거

분류	네트워크 서비스	보안항목	불필요한 서비스 제거	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	중
내용 및 적용방법				

보안상 취약한 불필요한 서비스 제거

■ 기준

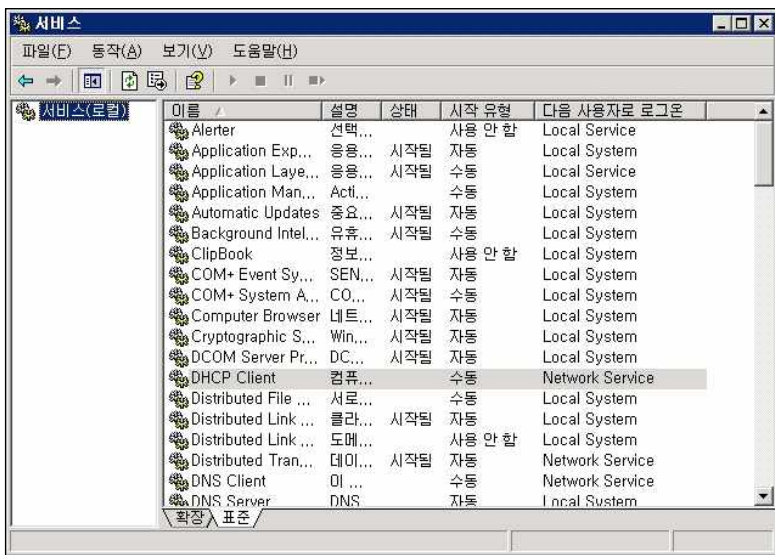
가. 불필요한 서비스 중지

양호 - 불필요한 서비스가 구동 중이지 않을 경우(하단 표 참고)

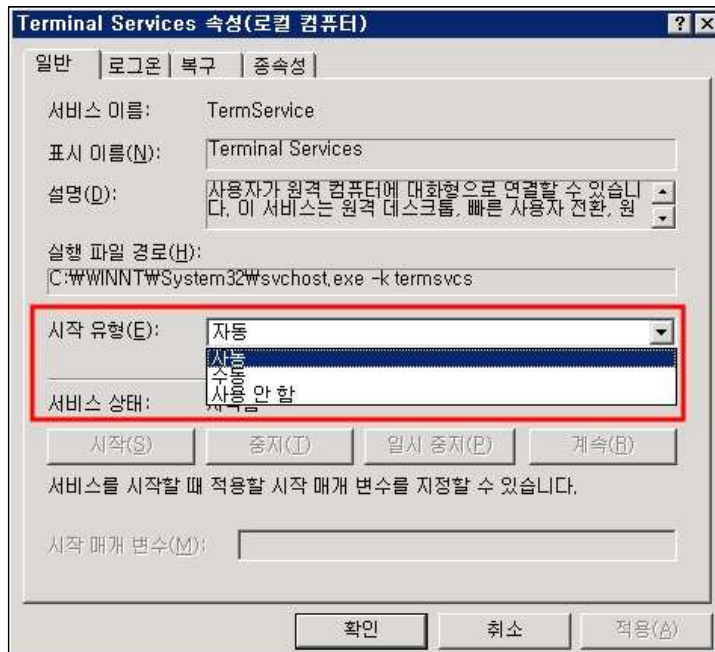
취약 - 불필요한 서비스가 구동 중일 경우

■ 조치방안

시작 > 설정 > 제어판 > 관리도구 > 서비스를 선택하여 속성에서 불필요한 서비스를 중지하고, "시작유형"을 "사용 안 함"으로 수정



각 서비스 마다 옵션을 설정할 수 있으며 해당 서비스를 선택하고 더블 클릭하게 되면 시작 유형을 선택할 수 있으며 시작 시 로그인 계정을 별도로 설정할 수 있음. 만약, 시스템 시작 시 자동으로 시작되게 하려면 [자동], 수동으로 서비스를 시작하려면 [수동], 서비스 자체를 사용하지 않으려면 [사용안함]을 선택한 후 [확인]을 클릭



■ 상세설명

일반적으로 시스템에는 필요하지 않은 서비스들이 디폴트로 설치되어 실행되고 있음. 이러한 서비스들은 해커가 침입할 수 있는 취약점을 드러내게 되는 원인이 될 수 있으며 또한 시스템 자원을 낭비하게 되므로 필요하지 않은 서비스를 중지시켜야 함.

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 서비스 제거

서비스 시작 유형	설 명
사용 안함	설치되어 있으나 실행되지 않음
수동	다른 서비스나 응용 프로그램에서 해당 기능을 필요로 할 때만 시작됨
자동	부팅 시에 해당 장치 드라이버가 로드 된 후에 운영 체제에 의해 시작됨

– 다음은 불필요한 서비스의 리스트임. 반드시 필요하지 않다면 사용중지 할 것.

- Alerter
- ClipBook Server
- ComputerBrowser
- DHCPClient
- Messenger
- NetBIOSInterface
- NetLogon
- NetworkDDE
- Network DDE DSDM
- Scheduler
- SimpleTCP/IP
- Spooler

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

<div> <ul style="list-style-type: none"> - TCP/IPNetBIOSHelper - WINSClient(TCP/IP) </div>	
비고	단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

3.2. 터미널 서비스 암호화 수준 설정

분류	네트워크 서비스	보안항목	터미널 서비스 암호화 수준 설정	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	중
내용 및 적용방법				

시스템 보안 향상을 위한 터미널 서비스 중지 및 설정

■ 기준

- 가. 터미널 서비스를 사용 중지,
- 나. 터미널 서비스 사용 시 암호화 수준을 “클라이언트 호환 가능” 이상으로 설정

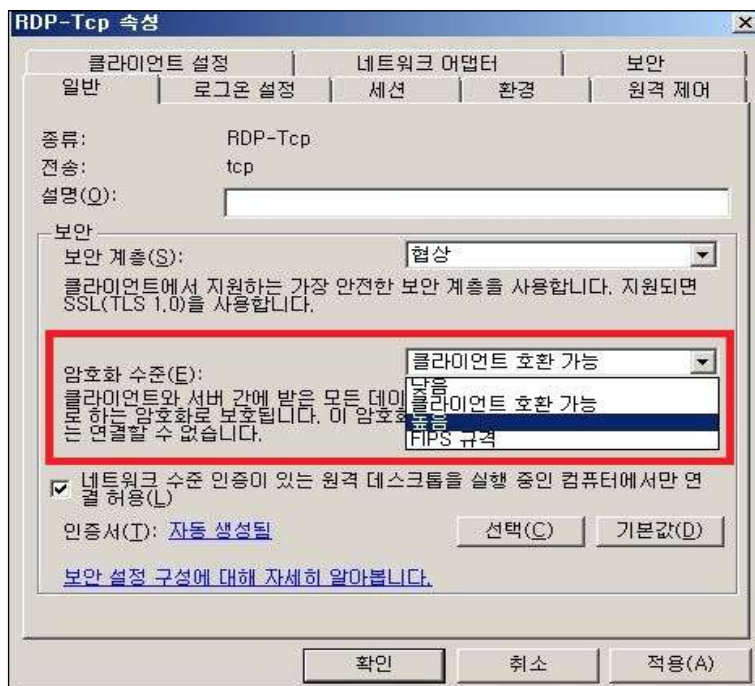
양호 - 터미널 서비스가 사용하지 않거나 사용 할 시 “클라이언트 호환 가능” 이상으로 설정한 경우

취약 - 터미널 서비스를 사용하고 암호화 수준이 “낮음” 으로 설정한 경우

■ 조치방법

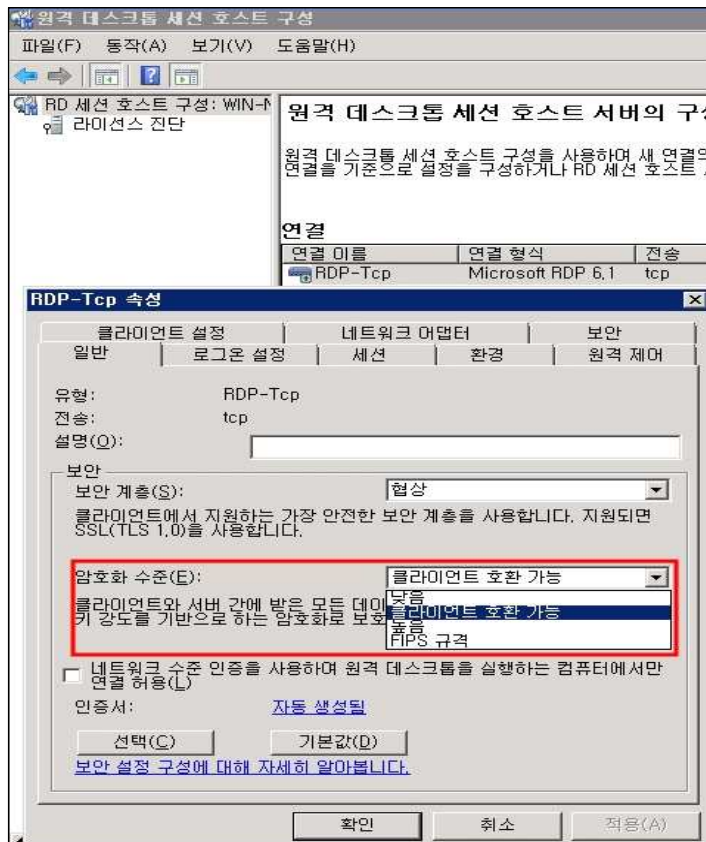
[2008인 경우]

시작 > 제어판 > 관리 도구 > 터미널 서비스 > 터미널 서비스 구성 > RDP-Tcp 속성



[2008 R2 인 경우]

시작 > 관리 도구 > 원격 데스크톱 서비스 > 원격 데스크톱 세션 호스트 구성 > RDP-Tcp 속성



■ 상세설명

터미널 서비스는 원격지에 있는 서버를 관리하기 위한 유용한 도구이나 취약한 패스워드를 사용하거나 접근제어가 적절치 못할 경우 해킹의 도구로 악용될 수 있으므로 불필요하게 터미널 서비스가 사용되고 있는지 점검함.

터미널 서비스가 필요한 경우에는 관리자 이외의 일반 사용자의 터미널 서비스 접속을 허용하지 않으며, 방화벽에서 터미널 서비스 포트(3389)의 사용을 관리자 컴퓨터의 IP로 제한

암호화 수준

- ✓ 낮음 - 클라이언트에서 서버로 보내는 모든 데이터는 클라이언트가 지원하는 최대 키 강도를 기반으로 하는 암호화로 보호됨
- ✓ 클라이언트 호환 가능 - 클라이언트와 서버 간에 받은 모든 데이터는 클라이언트가 지원하는 최대 키 강도를 기반으로 하는 암호화로 보호됨
- ✓ 높음 - 클라이언트와 서버 간에 받은 모든 데이터는 서버의 최대 키 강도를 기반으로 하는 암호화로 보호됩니다. 이 암호화 수준을 지원하지 않는 클라이언트는 연결할 수 없음
- ✓ FIPS 규격 - 클라이언트에서 서버로 보내는 모든 데이터를 Federal Information Processing Standard 140-1 유효 암호화 방법을 사용하여 보호됨

비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

3.3. NetBIOS 서비스 보안 설정

분류	네트워크 서비스	보안항목	NetBIOS 서비스 보안 설정		
대상 OS	Windows 2008			중요도	상
내용 및 적용방법					

시스템 보안 향상을 위한 NetBIOS 서비스 중지 및 설정

■ 기준

- 가. NetBIOS 서비스를 사용 중지,
- 나. NetBIOS 서비스 사용 시 “NetBios over TCP/IP 사용 안 함” 설정

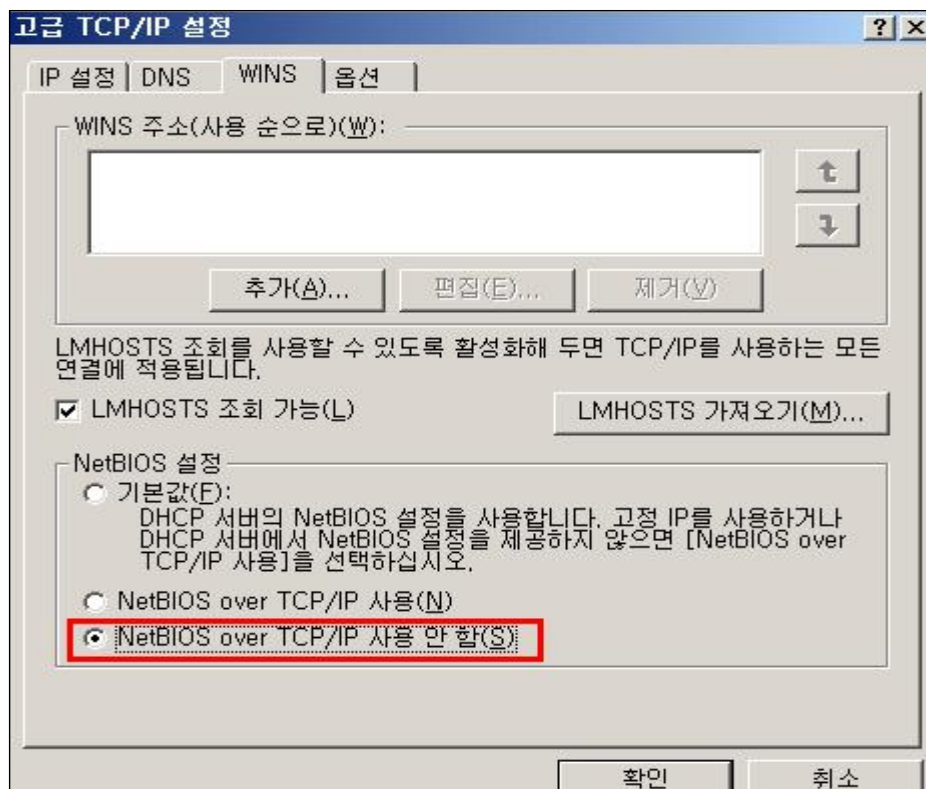
양호 - NetBIOS서비스를 사용하지 않거나 사용 할 시 “TCP/IP에서 NetBios 사용 안함” 설정한 경우

취약 - NetBIOS서비스를 사용하고 “TCP/IP에서 NetBios 사용 안함” 설정하지 않은 경우

■ 조치방법

NetBIOS 서비스가 필요한 경우

- 시작 > 실행 > ncpa.cpl > 로컬 영역 연결 > 속성 > TCP/IP > [일반] 탭에서 [고급] 클릭 > [WINS] 탭에서 TCP/IP에서 “NetBios over TCP/IP 사용 안 함”선택



■ 상세설명

TCP/IP NetBIOS Helper 서비스는 NetBIOS Over TCP/IP(NetBT) 서비스 및 NetBIO 이름 확인 지원을 네트워크의 클라이언트에 제공하여 사용자가 파일을 공유 하거나, 인쇄하거나, 네트워크에 로그인 할 수 있는 유용한 서비스지만 윈도우 NT 시스템이 인터넷에 직접 연결되어 있으면 공격자가 쉽게 파일시스템을 사용할 수 있으므로 서비스 불필요시 서비스를 중지하거나 NetBIOS에

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

대한 접근 통제가 적용되어야 함.

■ 서비스 영향

<TCP/IP에서 NetBios 사용안함 설정시>

TCP/IP을 거치게 되는 파일 공유 서비스가 제공되지 않음
 인터넷에서의 공유 자원에 대한 접근시도가 불가능함
 (라우터를 거치지 않은 내부 네트워크에서는 가능함)

비고	단기 적용(적용 시 개발자 및 운영자 협의)
-----------	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

4. 주요 응용 설정

4.1. Telnet 서비스 보안 설정

분류	주요 응용 설정	보안항목	Telnet 서비스 보안 설정	
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)	중요도	중	
내용 및 적용방법				

Telnet 서비스 사용시 보안을 위한 인증방법 점검

■ 기준

가. Telnet 서비스가 중지되거나 인증방법을 NTLM 설정

양호 - Telnet 서비스가 구동 되어 있지 않거나 인증방법이 NTLM 일 경우

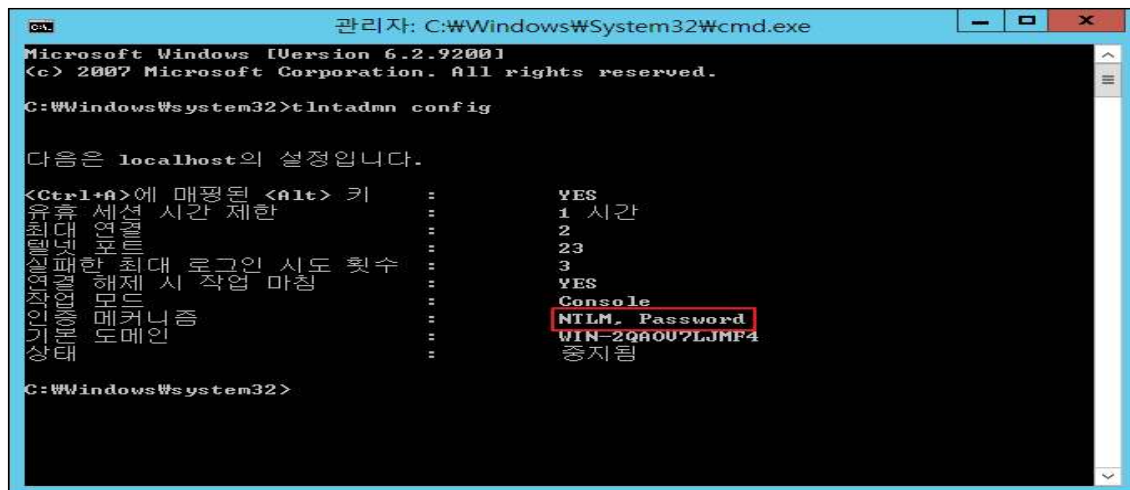
취약 - Telnet 서비스가 구동 되어 있으며 인증방법이 NTLM 이 아닐 경우

■ 조치방법

SSH, IPsec 등을 이용한 암호화 통신을 권장

Telnet 서비스에 대한 설정 확인 시작 > 실행 > cmd.exe > tlntadmn config

Telnet 서비스에 대한 설정은 시작 > 실행 > cmd.exe > tlntadmn config sec = +ntlm -passwd



■ 상세설명

Windows 2008에서는 기본적으로 Telnet 서비스에 대하여 NTLM 인증을 사용. 이는 별도의 계정, 비밀번호의 입력 없이 클라이언트 컴퓨터의 로그인 계정 및 패스워드를 이용하여 Telnet 서버와 인증을 하는 것으로서 Windows 계열의 클라이언트만 사용할 수 있는 인증임. NTLM 을 사용하지 않고 ID/PASSWORD를 직접 입력하여 인증(NTLM값이 0일 경우)할 수도 있는데 이는 클라이언트가 유닉스 계열 또는 NTLM 인증을 사용할 수 없을 때에 이러한 인증 방법을 사용할 수 있음

Telnet 서비스의 필요성에 의하여 사용하게 된다면 접속 환경에 따라 인증방법을 정해주어야 함. 다만 NTLM 인증이 클라이언트 O/S 에 제약이 있고 별도의 키보드 입력이 없으므로 다소 보안적인 서버 운용을 할 수 있다는 점이 있으나 로컬 컴퓨터를 외부 공격자가 장악하게 된다면 이는 텔넷 서버로의 접속에 아무런 제약을 받지 않고 로그인 할 수 있으므로 주의

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

또한, 엄격한 계정정책을 사용하지 않으면 외부의 비인가자에 의한 침해의 통로가 될 수 있으며 Telnet을 이용한 통신은 암호화 되지 않은 평문으로 전송되므로 간단한 Sniffer 에 의해서도 정보가 유출될 수 있음

비고	장기 적용(적용 시 개발자 및 운영자 협의)
-----------	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

4.2. DNS(Domain Name Service) 보안 설정

분류	주요 응용 설정	보안항목	DNS 보안 설정	
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)		중요도	중
내용 및 적용방법				

DNS 서비스 사용 시 특정 서버로만 전송을 하도록 되어 있는지 점검

■ 기준

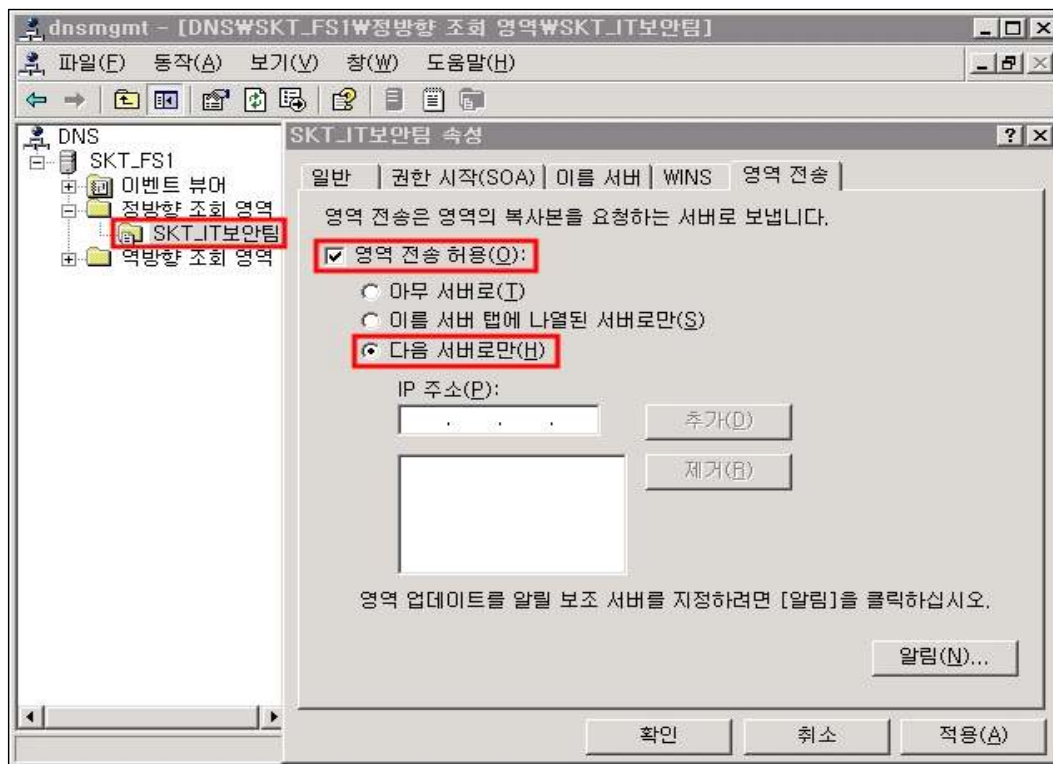
가. DNS서비스를 사용 않거나, 영역 전송을 “특정 서버로만” 설정

양호 - DNS 서비스를 사용 않거나, 영역 전송이 “특정 서버로만” 설정되어 있을 경우

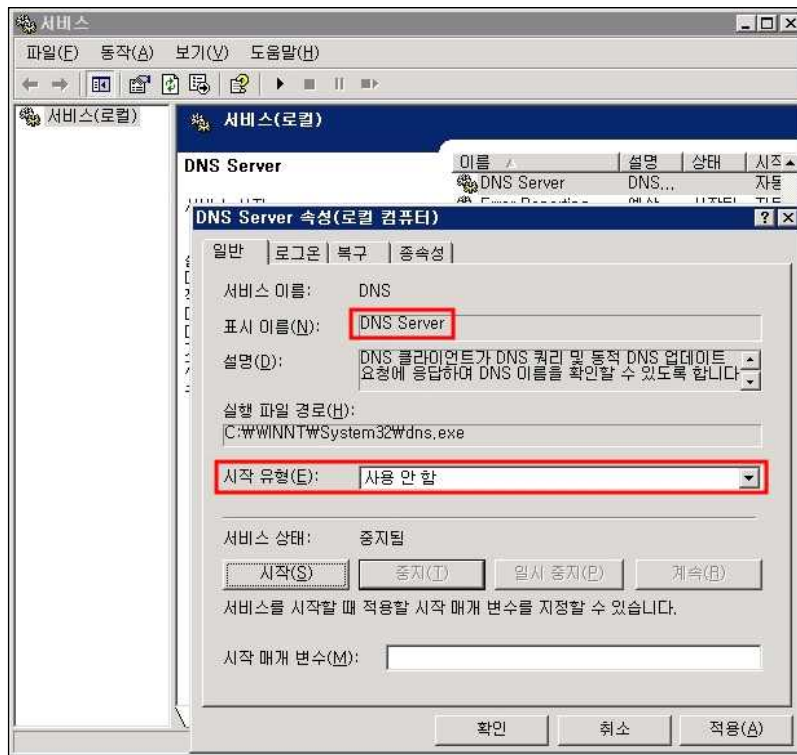
취약 - DNS서비스를 사용하며, 영역 전송이 “특정 서버로만” 설정되지 않은 경우

■ 조치방법

승인된 DNS서버로만 전송이 되도록 제한을 해야 하며 제어판 > 관리도구 > DNS > 영역전송 탭에서 각각 도메인의 속성을 선택하여 설정 및 확인 가능. 영역전송을 아무 서버에게나 허용 금지



DNS 서버를 사용하지 않을 경우 아래 그림과 같이 제어판 > 관리도구 > 서비스 > DNS Server항목의 속성에서 ‘시작 유형’란은 수동으로 변경하고, ‘서비스 상태’란은 중지 버튼을 눌러 DNS 서버 중지



■ 상세설명

DNS 서버에 저장되어 있는 도메인 정보를 승인된 DNS서버가 아닌 다른 외부로 유출하는 것은 보안상 바람직하지 않으며 적절한 설정을 통하여 이러한 정보의 전송을 제한할 수 있음. DNS 서버를 사용하지 않을 경우 중지시킴.

비고

장기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

4.3. SNMP(Simple Network Management Protocol) 서비스 보안 설정

분류	주요 응용 설정	보안항목	SNMP 서비스 보안 설정	
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)		중요도	상
내용 및 적용방법				

SNMP 서비스 사용 시 Community String 으로 사용하는 문자 점검

■ 기준

가. SNMP서비스를 사용하지 않거나 Community String을 public, private 설정안함
(SNMP Brute Force Attack 또는 SNMP Dictionary Attack이 가능하므로 반드시 8자리 이상의 자릿수와 숫자, 기호를 혼합하여 강력한 패스워드 형식으로 설정)

나. SNMP 서비스가 시작되고 있으나, SNMP Community string 설정 없음

양호 - SNMP 서비스를 사용하지 않거나 Community 스트링이 public, private 이 아닐 경우
(SNMP Brute Force Attack 또는 SNMP Dictionary Attack이 가능하므로 반드시 8자리 이상의 자릿수와 숫자, 기호를 혼합하여 강력한 패스워드 형식으로 설정)

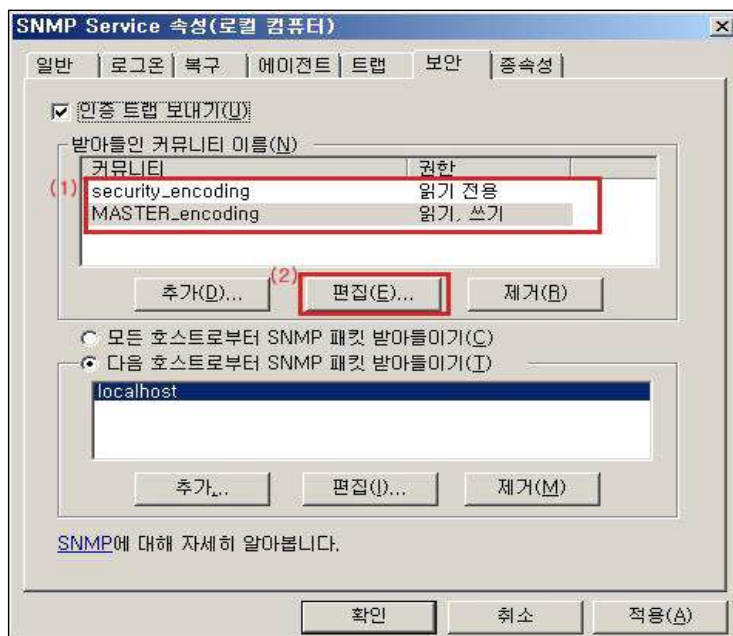
SNMP 서비스가 시작되고 있으나, SNMP community string이 없는 경우

취약 - SNMP 서비스를 사용하며 Community 스트링이 public, private 인 경우

■ 조치방법

Default Community String (public, private) 변경.

관리도구 > 서비스 > SNMP Service > 속성 > 보안 탭에서 커뮤니티 이름을 편집



- 불필요시 해당 서비스 제거

시작>제어판>관리도구>서비스>SNMP Service 에서 [시작 유형]을 [사용 안 함]으로 만든 후, SNMP 서비스를 중지

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

■ 상세설명

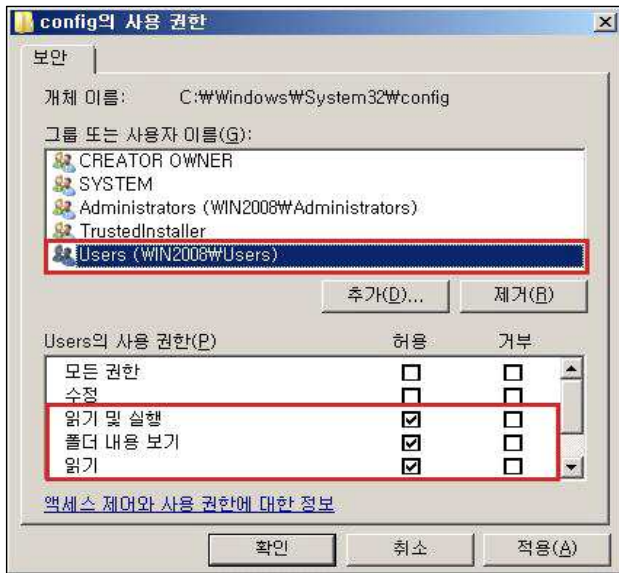
SNMP 서비스는 시스템 상태를 실시간으로 파악하거나 설정하기 위하여 사용하는 서비스임. 그러나 이 정보를 받기 위한 일종의 패스워드인 Community String이 Default로 public, private로 설정되어 있는 경우가 많으며, 이를 변경하지 않으면 이 String을 악용하여 비인가 사용자가 시스템의 주요 정보 및 설정 상황을 파악 할 수 있는 취약성이 존재함.

비고	장기 적용(적용 시 개발자 및 운영자 협의)
-----------	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5. 시스템 보안 설정

5.1. 원격 로그파일 접근 진단

분류	시스템 보안 설정	보안항목	원격 로그파일 접근 진단
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도
			하
내용 및 적용방법			
<p>원격 익명 사용자의 시스템 로그파일 디렉토리 접근 제한</p> <p>■ 기준</p> <p>가. 시스템 로그파일 디렉토리의 접근권한에 Users/Everyone 모든 권한, 수정, 쓰기 권한 제한</p> <p>양호 - 해당 디렉토리의 접근권한이 Users/Everyone 에 모든권한, 수정 및 쓰기 권한이 없는 경우 취약 - 해당 디렉토리의 접근권한이 Users/Everyone 에 모든권한, 수정 및 쓰기 권한이 있는 경우</p> <p>■ 조치방법</p> <p>다음의 경로에 Users/Everyone의 수정 및 쓰기 권한을 제거</p> <ul style="list-style-type: none"> - 시스템 로그파일 경로 : C:\WINDOWS\system32\config - 기타 App 로그파일 경로 : C:\WINDOWS\system32\LogFiles  <p>■ 상세설명</p> <p>익명으로 중요 '시스템로그' 파일 및 '어플리케이션 로그' 파일에 접근 가능하여 중요 보안 감사 정보의 변조/삭제/유출의 위험이 존재 하므로 원격 익명사용자의 시스템 로그 접근을 방지해야 됨. 일반적으로 시스템 로그파일은 C:\WINDOWS\system32\config에 저장되나 어플리케이션 로그파일은 각각의 어플리케이션마다 로그저장 위치가 다름. 웹 서버에 많이 사용하는 IIS 의 경우에는 C:\WINDOWS\system32\LogFiles에 IIS 로그 저장이 이루어짐.</p>			
비고	단기 적용(적용 시 개발자 및 운영자 협의)		

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.2. 화면 보호기 설정

분류	시스템 보안 설정	보안항목	화면 보호기 설정		
대상 OS	Windows Server 2012			중요도	하
내용 및 적용방법					

인가된 사용자의 자리 이탈시 정보 유출의 가능성을 최소화하기 위한 화면 보호기 설정

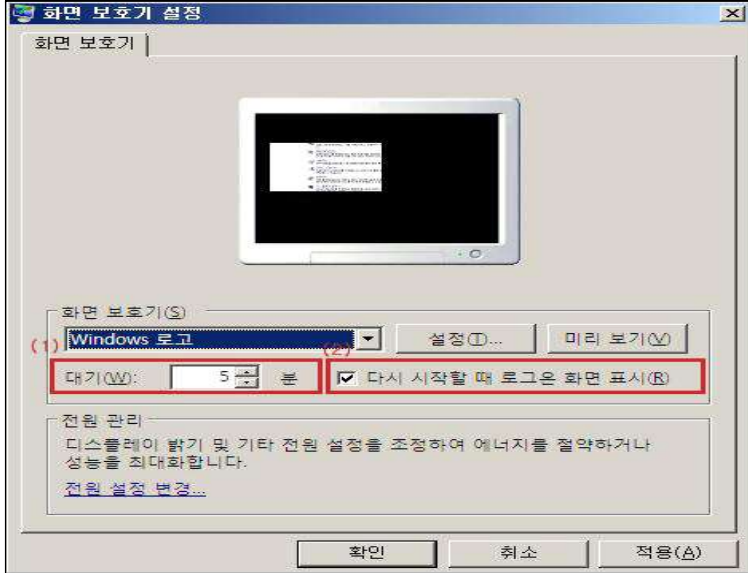
■ 기준

가. 화면보호기를 설정
화면보호기 설정 = 사용
암호 사용 = 사용
대기 시간 = 5분
※ 실제 사용되고 있는 모든 관리자 계정의 화면보호기 설정 확인

양호 - 화면보호기를 설정하고, 암호를 사용하며, 대기 시간이 5분일 경우
취약 - 화면보호기가 설정되어 있지 않거나, 암호를 사용하지 않거나, 대기시간이 5분 초과 일 경우

■ 조치방법

화면 보호기 적용 혹은 잠금 상태 유지가 되는지 확인
제어판 > 디스플레이 > 화면 보호기 변경 > 화면 보호기 “선택”, “다시 시작할 때 로그인 화면 표시” 활성화 설정, “대기 시간” 5분 권장



■ 상세설명

로그오프하거나 워크스테이션 잠금 설정이 되어있는지 여부를 확인함. 자리 이탈시의 정보 유출 가능성을 최소화 함.

비고	단기 적용(적용 시 개발자 및 운영자 협의)
----	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.3. 이벤트 뷰어 설정

분류	시스템 보안 설정	보안항목	이벤트 뷰어 설정	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	상
내용 및 적용방법				

접근자 추적 및 불법 접근자 확인 자료를 위한 보안 로그의 설정

■ 기준

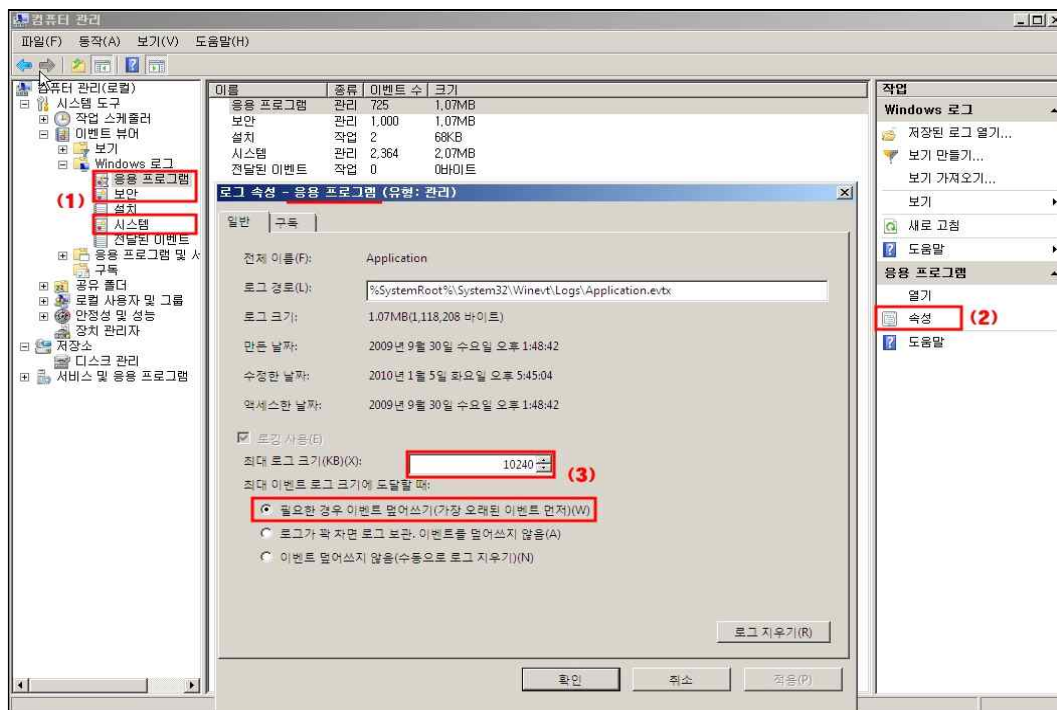
- 가. 이벤트 뷰어(로컬) 응용 프로그램, 보안, 시스템의 로그 설정
- 최대 로그 크기 10240KB 이상이고
 - “필요한 경우 이벤트 덮어쓰기” 로 설정

양호 - 최대 로그 크기 10240KB 이상이고 “필요한 경우 이벤트 덮어쓰기” 설정되어 있는 경우

취약 - 최대 로그 크기 10240KB 미만이거나 필요한 경우 이벤트 덮어쓰기” 설정되지 않은 경우

■ 조치방법

제어판 > 관리도구 > 컴퓨터관리 > 이벤트 뷰어 > Windows로그 (응용 프로그램 | 보안 | 시스템)



- 최대 로그 크기를 10Mbyte(10240KB)
- 최대 로그 크기에 도달할 때 “필요한 경우 이벤트 덮어쓰기” 선택

■ 상세설명

최대 로그 크기는 10MBytes 이상, 이벤트 로그 관리는 ‘필요한 경우 이벤트 덮어쓰기’으로 설정하여 보안 로그의 크기를 유지하고 접근자 추적 및 불법 접근자 확인 자료로 이용.

비고	단기 적용(적용 시 개발자 및 운영자 협의)
----	--------------------------

5.4. 로그인 시 경고 메시지 표시 설정

분류	시스템 보안 설정	보안항목	로그인 시 경고 표시 설정
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)		중요도 중

내용 및 적용방법

비인가자의 시스템 로그인 시 불법적인 사용을 경고

■ 기준

가. 로그인시 경고 메시지 표시

양호 - 로그인시 경고 메시지가 뜰 경우

취약 - 로그인시 경고 메시지가 뜨지 않을 경우

■ 조치방법

* 조치 방법 1, 2, 3 중 한가지 방법으로 선택 적용하더라도 시스템 재시작 없이 설정 값이 연동되어 변경되므로 세가지 조치 방법 중 택일하여 적용

[조치 방법1]

경고 메시지를 삽입하는 것이 필요하므로 아래의 레지스트리 항목을 수정하여 관리자가 삽입하고자 하는 메시지내용을 추가할 것을 권고

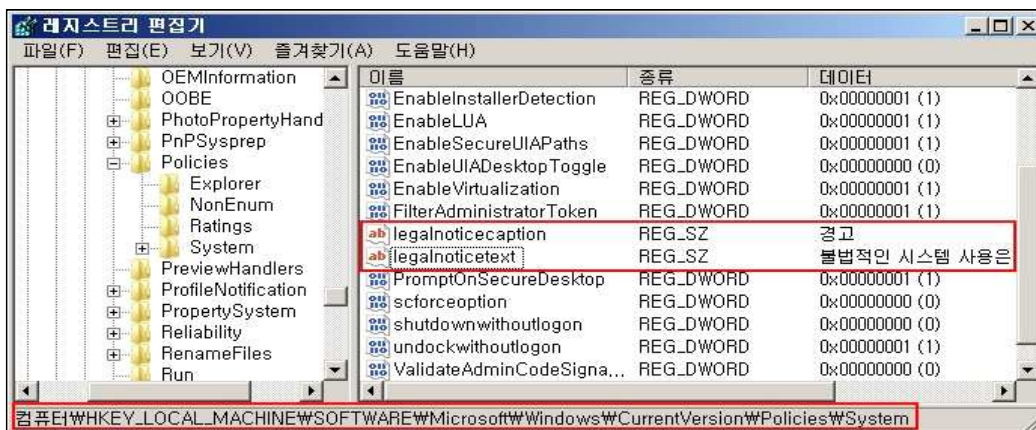
[레지스트리 위치]

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

[레지스트리 키]

LegalNoticeCaption : 제목

LegalNoticeText : 메시지 내용



[조치 방법2]

아래의 레지스트리 항목을 수정하여 관리자가 삽입하고자 하는 메시지내용을 추가할 것을 권고

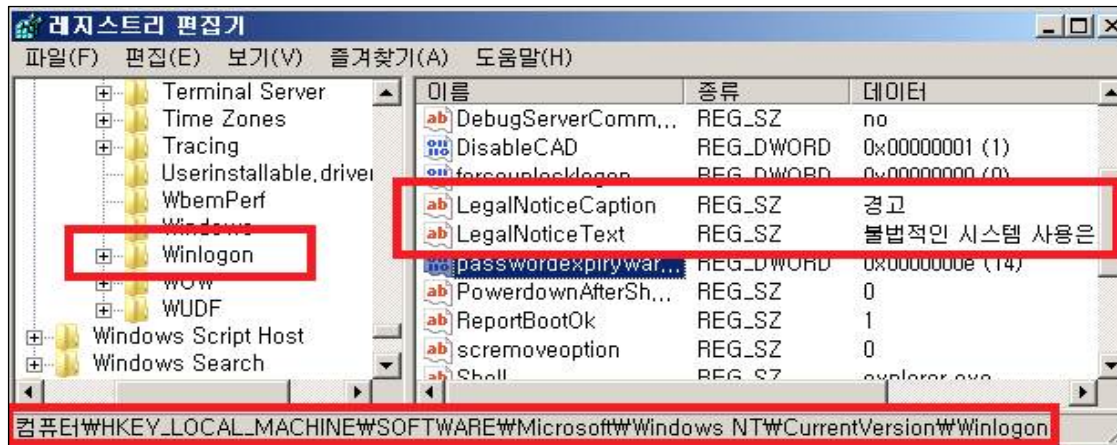
[레지스트리 위치]

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

[레지스트리 키]

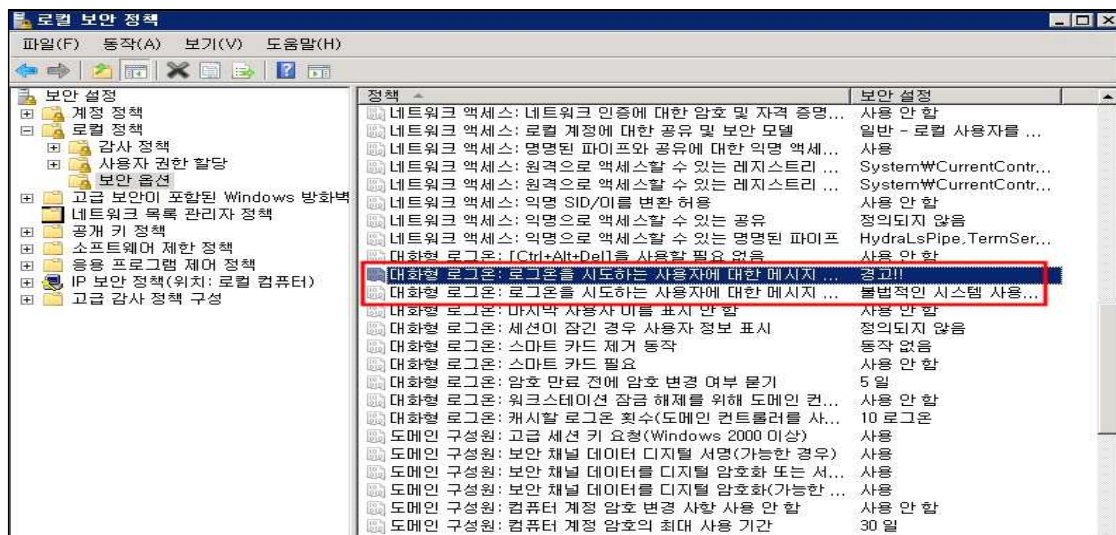
LegalNoticeCaption : 제목 (예: 경고)

LegalNoticeText : 메시지 내용 (예 : 불법적인 시스템 사용은 관련법에 의해 처벌을 받습니다.)



[조치 방법3]

- 관리도구 à 로컬 보안 정책 à 로컬 정책 à 보안 옵션
- “대화형 로그온 : 로그온 시도하는 사용자에게 대한 메시지 제목” 정책란에 제목을 삽입
- “대화형 로그온 :로그온 시도하는 사용자에게 대한 메시지 텍스트” 정책란에 내용을 삽입



■ 상세설명

시스템에 로그인 하려는 사용자에게 관리자는 시스템의 불법적인 사용에 대하여 경고 창을 띄울 수 있음. 로그인 하기 이전에 사용자는 이러한 경고 메시지를 주지한 후 “확인” 버튼을 누름으로써 패스워드를 입력할 수 있는 로그인 창이 나타남.

이러한 경고창의 효과는 악의의 사용자로부터 시스템을 직접적으로 보호하지는 못하지만 관리자가 적절한 보안수준으로 시스템을 보호하고 있으며 공격자의 활동을 주시하고 있다는 생각을 들게 하여 간접적으로 공격 피해를 감소시키는 효과를 볼 수 있음.

비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.5. 마지막 로그인 사용자 계정 숨김

분류	시스템 보안 설정	보안항목	마지막 로그인 사용자 계정 숨김
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도
내용 및 적용방법			중

비인가자가 시스템에 접근 시 마지막 사용자 숨김 설정으로 ID,PW 강제공격의 위험성을 낮춤

■ 기준

가. "DontDisplayLastUserName"이 "1"로 설정

양호 - "DontDisplayLastUserName"이 "1"로 설정되어 있는 경우

취약 - "DontDisplayLastUserName"이 "1"로 설정되어 있지 않을 경우

■ 조치방법

* 조치 방법 1, 2 중 한가지 방법으로 선택 적용하더라도 시스템 재시작 없이 설정 값이 연동되어 변경되므로 두가지 조치 방법 중 택일하여 적용

[조치 방법1]

[레지스트리의 값 변경]

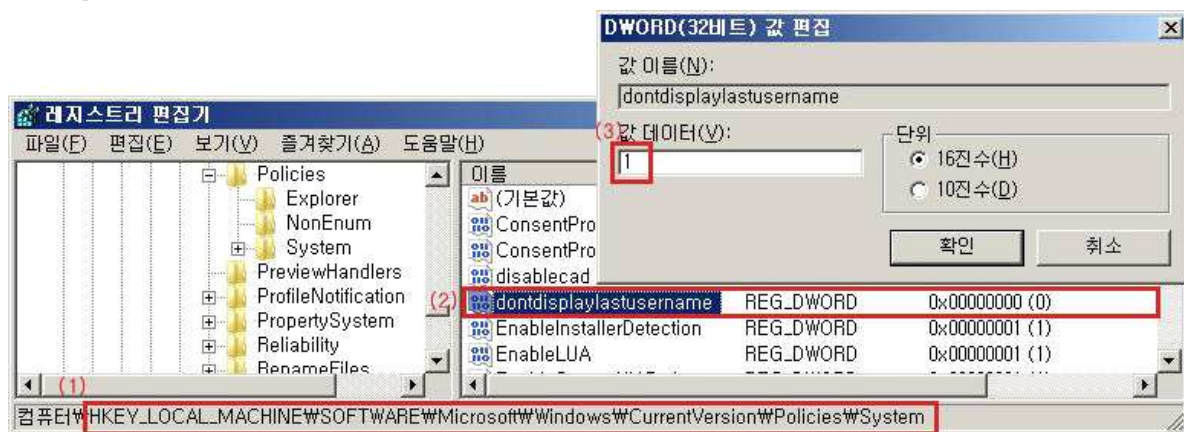
시작 -> 실행(regedit.exe)

[레지스트리 위치]

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

[레지스트리 값]

DontDisplayLastUserName = 1

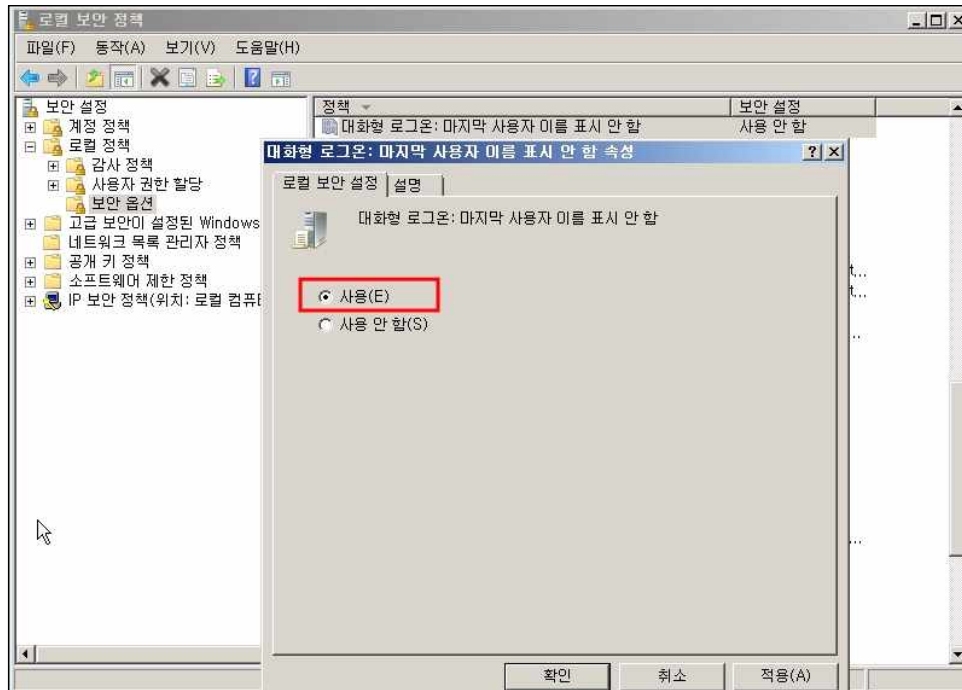


[조치 방법2]

[마지막 로그인 사용자 계정 숨김 설정]

☞ 시작>관리도구>로컬 보안 정책>로컬 정책>보안 옵션

☞ '로그온 스크린에 마지막 사용자 이름 표시 안함'을 더블 클릭 -> 사용



■ 상세설명

마지막 로그인 사용자 보이기를 ON시켜 놓으면 공격자가 사용자의 컴퓨터를 켜보기만 하여도 계정을 알 수 있으므로 강제공격등에 이용할 수 있음. Login ID를 공격자가 알수 있으므로, 유추 및 강제공격 가능

비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.6. 로그인 하지 않은 사용자 시스템종료 방지

분류	시스템 보안 설정	보안항목	로그온 하지 않은 사용자 시스템종료 방지	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	중
내용 및 적용방법				

비 인가자의 시스템 종료를 방지하기 위한 설정

■ 기준

가. 해당 레지스트리의 “ShutdownWithoutLogon” 값 “0”으로 설정

양호 - “ShutdownWithoutLogon”이 “0”으로 설정되어 있을 경우

취약 - “ShutdownWithoutLogon”이 “1”으로 설정되어 있을 경우

■ 조치방법

* 조치 방법 1, 2 중 한가지 방법으로 선택 적용하더라도 시스템 재시작 없이 설정 값이 연동되어 변경되므로 두가지 조치 방법중 택일하여 적용

[조치 방법1]

[레지스트리의 값 변경]

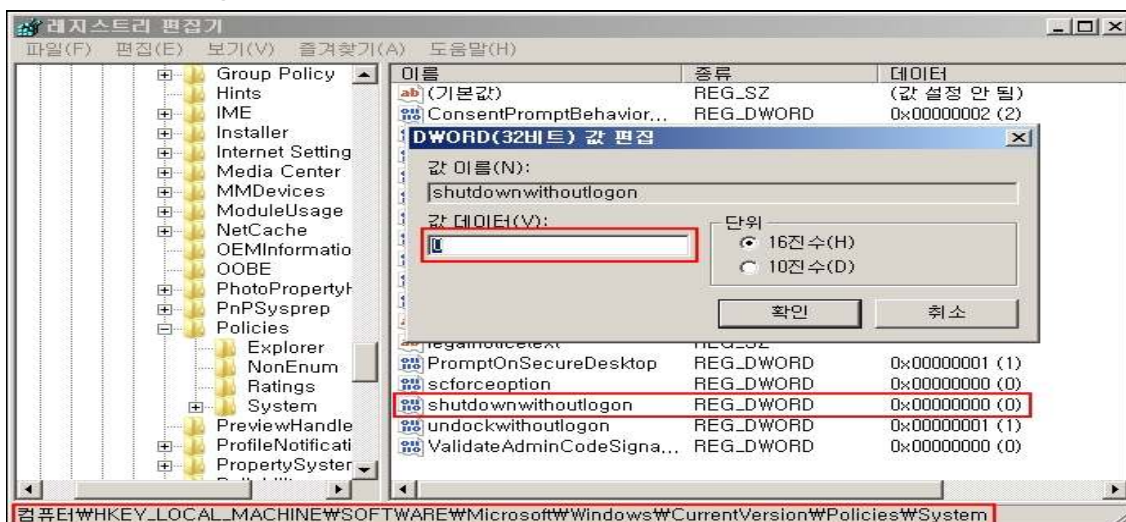
시작 -> 실행(regedit.exe)

[레지스트리 위치]

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

[레지스트리 값]

ShutdownWithoutLogon = 0

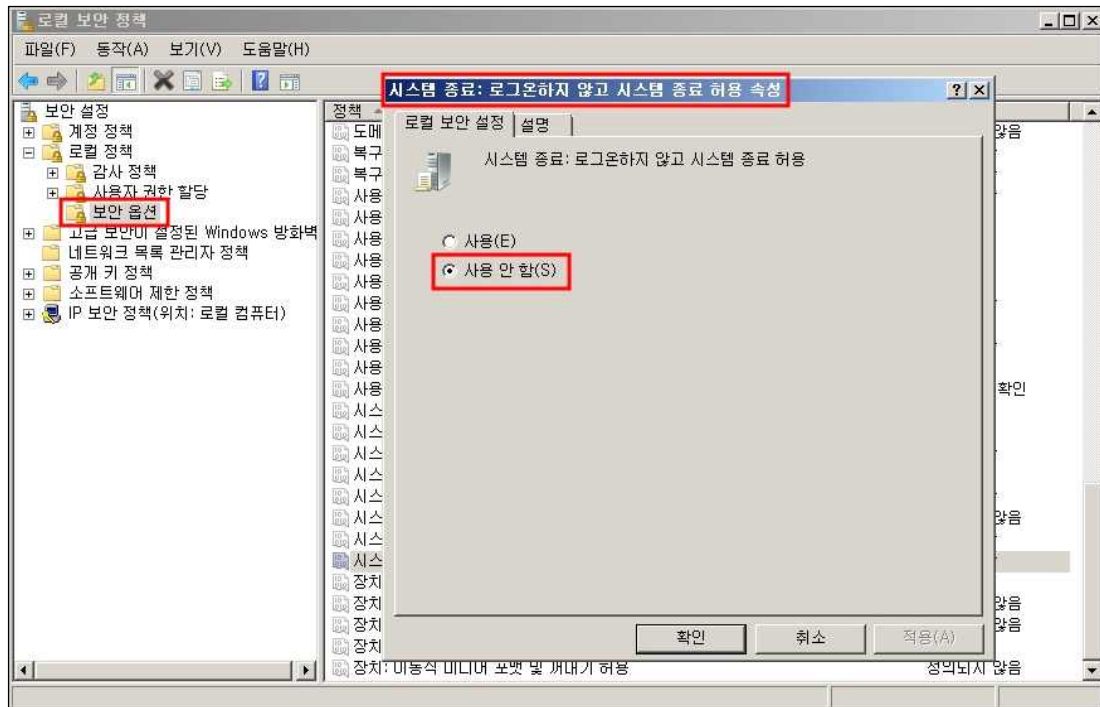


[조치 방법2]

[마지막 로그인 사용자 계정 숨김 설정]

☞ 시작>관리도구>로컬 보안 정책>로컬 정책>보안 옵션

☞ '시스템 종료 : 로그인 하지 않고 시스템 종료 허용'을 더블 클릭 -> 사용안함



■ 상세설명

로그온 창에 “시스템 종료”버튼이 활성화되면, 비인가된 사용자가 또는 인가된 사용자의 비의도적인 실수 등으로 로그인을 하지 않고도 시스템의 불법적인 시스템 다운을 가능하게 하여, 정상적인 서비스에 장애를 발생시킬 수 있음.

시스템 종료 버튼을 비활성화 시킴으로 비인가된 사용자로부터의 불법적인 시스템다운, 비의도적인 실수 등을 미연에 방지할 수 있음.

비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.7. 로컬 감사정책 설정

분류	시스템 보안 설정	보안항목	로컬 감사정책 설정	
대상 OS	Windows 2008 Standard / Enterprise Edition(R2 포함)		중요도	상
내용 및 적용방법				

감사정책 설정을 통해 보안 로그에서 계정 로그인/로그오프에 대한 감사 설정

■ 기준

가. 아래 이벤트 감사 항목에 대해서는 반드시 “성공|실패” 감사 설정

- 개체 액세스 감사
- 계정 관리 감사
- 계정 로그인 이벤트 감사
- 권한 사용 감사
- 로그인 이벤트 감사

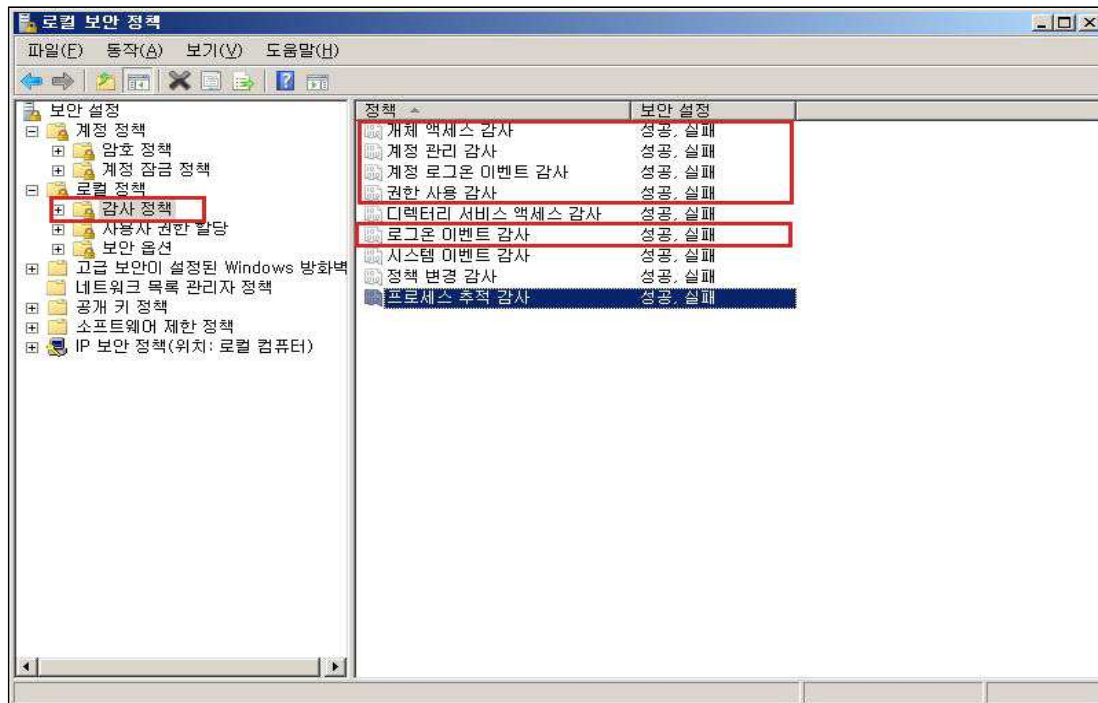
양호 - 상기 이벤트 감사 항목에 대해서는 반드시 “성공|실패” 감사 설정.

취약 - 상기 이벤트 감사 항목에 “성공|실패” 설정이 되어 있지 않은 경우

■ 조치방법

시작>관리도구>로컬보안정책>로컬정책>감사설정

개체 액세스 감사, 계정 관리 감사, 계정 로그인 이벤트 감사, 권한 사용 감사, 로그인 이벤트 감사에 대해서는 반드시 “성공|실패” 감사 설정



■ 상세설명

아래의 감사 정책 설정 예를 참고하여 적절한 감사 정책을 적용

감사정책에 의해 생성된 로그는 관리도구>이벤트 표시기를 통해서 확인

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

정 책	설 명
개체 액세스	시스템 액세스 컨트롤 목록(SACL)이 있는 Windows 기반 네트워크의 모든 개체에 대해 감사를 활성화 보안 로그에 이벤트를 표시하려면 먼저 개체 액세스 감사를 활성화한 후 감사할 각 개체에 대해 SACL을 정의
계정 관리	사용자나 그룹이 생성, 변경 또는 삭제된 시간을 판단하는데 사용
계정 로그인 이벤트	사용자가 도메인에 로그인하면 도메인 컨트롤러에 로그인 시도가 기록
권한 사용	권한 사용의 성공 및 실패를 감사할 경우 사용자 권한을 이용하려고 할 때마다 이벤트가 생성
디렉토리 서비스 액세스	Active Directory 개체의 SACL에 나열된 사용자가 해당 개체에 액세스를 시도할 때 감사 항목이 생성
로그온 이벤트	사용자가 컴퓨터에 로그인하거나 로그오프할 때마다 로그온이 시도된 컴퓨터의 보안 로그에 이벤트가 생성
시스템 이벤트	사용자나 프로세스가 컴퓨터 환경을 변경하면 시스템 이벤트가 생성 시스템 이벤트를 감사할 경우 보안 로그가 삭제된 시간도 감사
정책 변경	감사 정책 변경의 성공 및 실패를 감사
프로세스 추적	실행되는 프로세스에 대한 자세한 추적 정보를 감사하는 경우 이벤트 로그에 프로세스를 작성하고 종료하려고 한 시도가 나타남
비고	단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.8. 가상 메모리 페이지 파일 삭제 설정

분류	시스템 보안 설정	보안항목	가상메모리 페이지 파일 삭제 설정	
대상 OS	Windows Server 2012		중요도	하

내용 및 적용방법

민감한 정보들이 담긴 페이지 파일의 노출을 제한하기 위한 설정

■ 기준

가. “ClearPageFileAtShutdown”이 “1”로 설정

양호 - “ClearPageFileAtShutdown”이 “1”로 설정

취약 - “ClearPageFileAtShutdown”이 “1”로 설정 되어 있지 않은 경우

■ 조치방법

* 조치 방법 1, 2 중 한가지 방법으로 선택 적용하더라도 시스템 재시작 없이 설정 값이 연동되어 변경되므로 두가지 조치 방법 중 택일하여 적용

[조치 방법1]

레지스트리의 값 변경

시작 -> 실행(regedit.exe)

[레지스트리 위치]

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\MemoryManagement

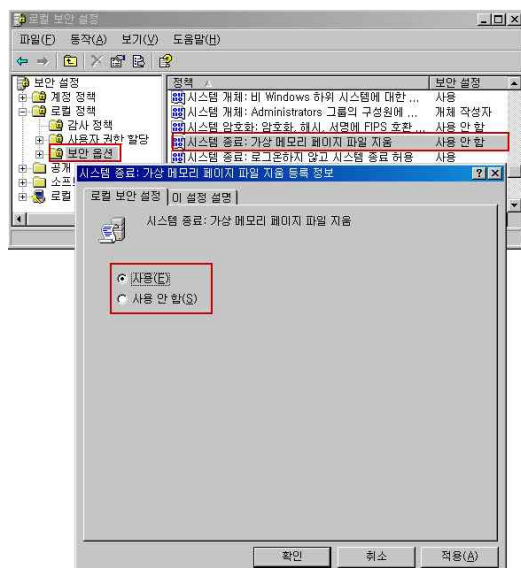
[레지스트리 키]

ClearPageFileAtShutdown = 1

[조치 방법 2]

시작>제어판>관리도구>로컬보안설정>로컬정책>보안 옵션에서

‘시스템이 종료할 때 가상 메모리 페이지 파일 지움’ 항목을 사용으로 설정함



 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

■ 상세설명

일부 프로그램은 암호화되지 않은 패스워드나 기타 민감한 정보를 임시로 메모리에 저장할 수 있기 때문에, Windows 가상 메모리 아키텍처로 인하여 이러한 민감한 정보들이 담긴 페이지 파일(Pagefile)이 노출될 경우 위험을 초래할 수 있음.

비고	단기 적용(적용 시 개발자 및 운영자 협의)
-----------	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.9. 예약된 작업 의심스런 명령어나 파일 점검

분류	시스템 보안 설정	보안항목	예약된 작업 점검	
대상 OS	Windows 2008		중요도	중
내용 및 적용방법				

예약된 작업에 불필요한 파일이나 명령어가 있는지 점검

■ 기준

가. 예약된 작업에 접속하여 불필요한 명령어나 파일이 있는지 점검

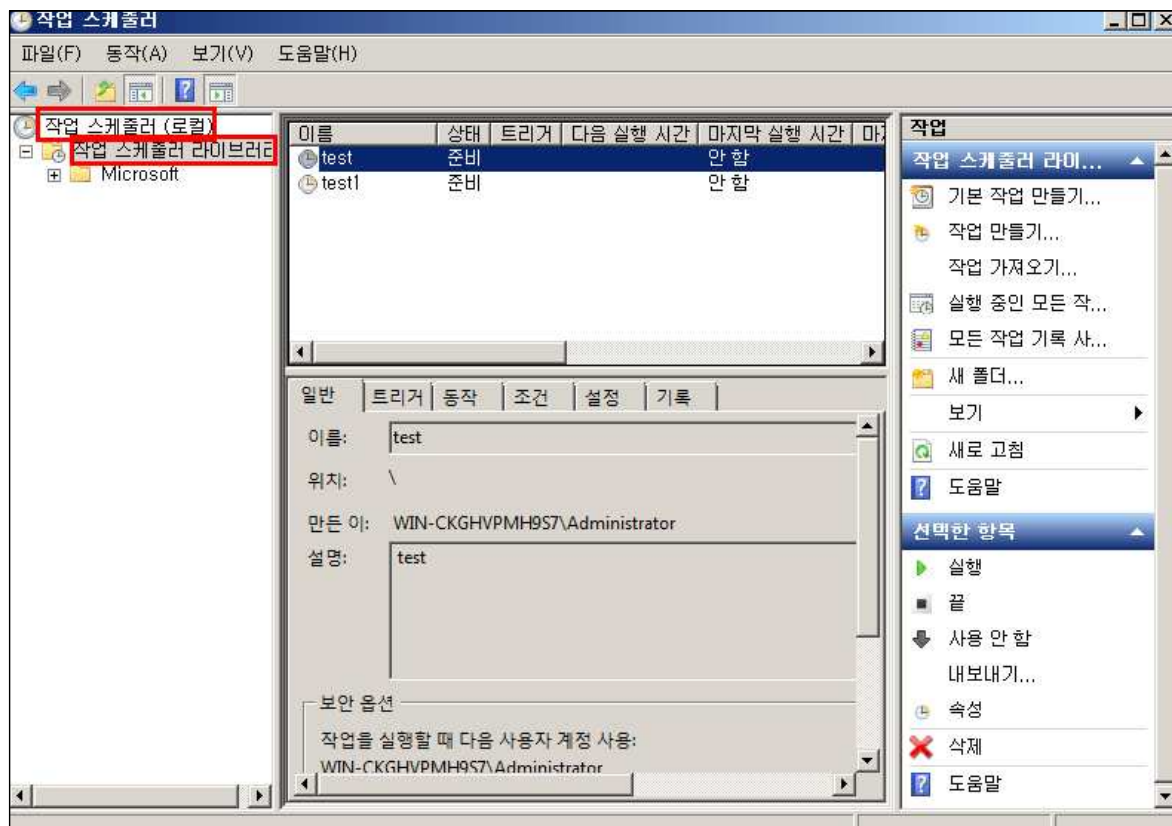
양호 - 예약된 작업에 접속하여 불필요한 명령어나 파일이 있는지 확인한 경우

취약 - 예약된 작업에 접속을 하지 않아 확인을 하지 않거나, 방치하고 있는 경우

■ 조치방법

< GUI 확인 방법 >

1. 시작> 제어판> 시스템 및 보안> 예약작업> 작업 스케줄러(로컬)> 작업 스케줄러 라이브러리
2. 등록된 예약 작업을 선택하여 상세내역 확인
3. 불필요한 파일 존재 시 삭제



< CLI 확인 방법 >

1. 시작> 실행> cmd 입력
2. cmd 창에서 C:\>schtasks.exe 명령어를 실행하여 확인
3. 불필요한 파일 존재 시 삭제


```

관리자: 명령 프롬프트
C:\>schtasks.exe

폴더: \
작업 이름      다음 실행 시간      상태
=====
test           N/A                준비
test1          N/A                준비
test2          2015-02-05 오후 3:29:00 준비

폴더: \Microsoft
작업 이름      다음 실행 시간      상태
=====
정보:사용자의 액세스 수준에서 현재 사용할 수 있는 작업이 없습니다.

폴더: \Microsoft\Windows
작업 이름      다음 실행 시간      상태
=====
정보:사용자의 액세스 수준에서 현재 사용할 수 있는 작업이 없습니다.

폴더: \Microsoft\Windows\Active Directory Rights Management Services Client
작업 이름      다음 실행 시간      상태
=====
AD RMS Rights Policy Template Management 사용 안 함
AD RMS Rights Policy Template Management N/A                준비
    
```

■ 상세설명

일정 시간마다 미리 설정해둔 프로그램을 실행할 수 있는 예약된 작업은 시작프로그램과 더불어서 해킹과 트로이 목마, 백도어를 설치하여 공격하기 좋은 루트로 사용될 수 있으므로 예약된 작업에 주기적으로 접속하여 불필요한 파일이나 명령어가 있는지 점검이 필요함.

비고

장기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.10. 원격 시스템 종료 권한 설정

분류	시스템 보안 설정	보안항목	원격 시스템 종료 권한 설정
대상 OS	Windows 2008		중요도
내용 및 적용방법			상

원격 네트워크를 통하여 운영 체제 시스템 종료 권한이 허용되는 사용자 설정

■ 기준

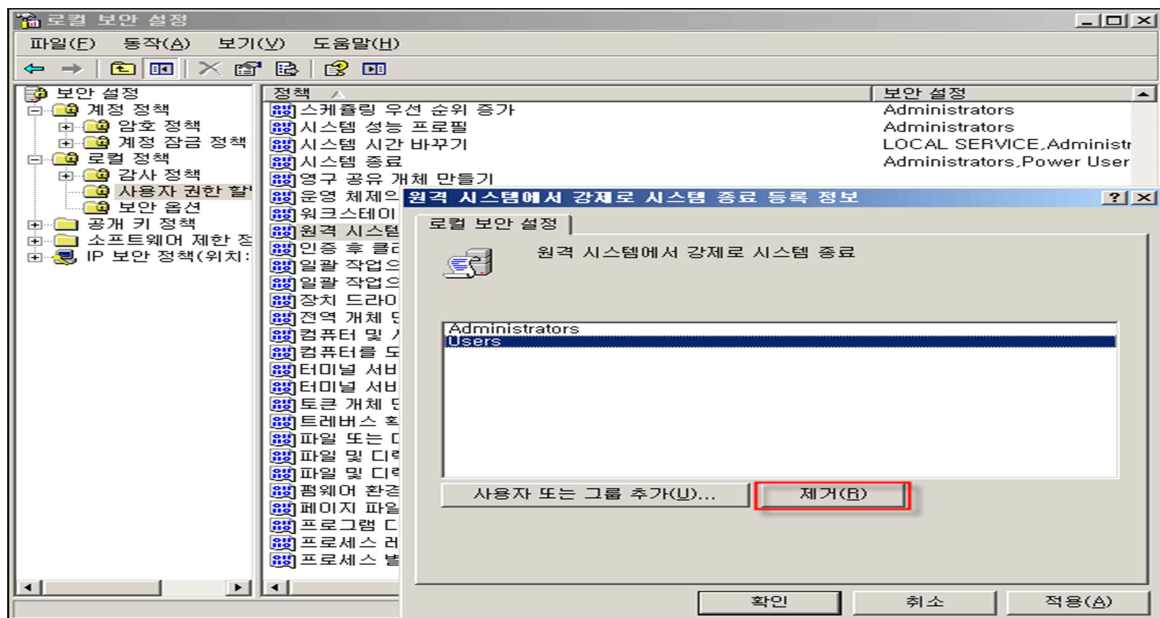
가. “원격 시스템에서 강제로 시스템 종료” 권한을 “Administrators”로 설정

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

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 사용자 권한 할당
2. “원격 시스템에서 강제로 시스템 종료” 정책에 Administrators 외 다른 계정 및 그룹 제거



■ 상세설명

이 정책 설정은 원격에서 네트워크를 통하여 운영 체제를 종료할 수 있는 사용자나 그룹을 결정하여 특정 사용자만 원격에서 시스템 종료를 제어할 수 있도록 설정함. 만약 해당 권한 부여가 부적절할 경우 서비스 거부 공격에 악용될 수 있음

비고	단기 적용(적용 시 개발자 및 운영자 협의)
-----------	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

5.11. 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 방지

분류	시스템 보안 설정	보안항목	보안감사 정책 설정	
대상 OS	Windows 2008			중요도 상
내용 및 적용방법				

보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 여부 설정

■ 기준

가. “보안 감사를 로그할 수 없는 경우 즉시 시스템 종료” 정책이 “사용 안 함”으로 설정

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

1. 시작> 실행> SECPOL.MSC> 로컬 정책> 보안 옵션
2. “보안 감사를 로그할 수 없는 경우 즉시 시스템 종료” 정책을 “사용 안 함” 으로 설정

■ 상세설명

이 정책 설정은 보안 이벤트를 기록할 수 없는 경우 컴퓨터를 즉시 종료할 것인지 결정함. “보안감사를 로그 할 수 없는 경우 즉시 시스템 종료” 정책을 사용 시 서비스 거부 공격에 악용될 수 있으며, 비정상적인 시스템 종료로 인하여 시스템 및 데이터에 손상을 입힐 수 있음.

비고	단기 적용(적용 시 개발자 및 운영자 협의)
----	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

6. 바이러스 진단

6.1. 백신 프로그램 설치

분류	바이러스 진단	보안항목	백신 프로그램 설치	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	상
내용 및 적용방법	<p>악성 파일 및 바이러스로부터 시스템을 보호하기위한 백신 프로그램 설치</p> <p>■ 기준</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">가. 바이러스 백신 프로그램 설치</div> <p>양호 - 바이러스 백신 프로그램이 설치되어 있는 경우 취약 - 바이러스 백신 프로그램이 설치되어 있지 않은 경우</p> <p>■ 조치방법</p> <p>담당자를 통해 바이러스 백신 프로그램을 반드시 설치해야 함.</p> <p>안철수 연구소 : http://www.ahnlab.com 하우리 : http://www.hauri.co.kr 시만텍코리아 : http://www.symantec.co.kr 한국트렌드마이크로: http://www.trendmicro.co.kr/</p> <p>■ 상세설명</p> <p>웜, 트로이목마 등의 악성 바이러스로 인한 피해규모가 커지고 있으며 이에 대한 피해를 최소화하기 위해 반드시 바이러스 백신 프로그램을 설치해야 함.</p> <p>바이러스 백신 프로그램은 바이러스 감염 여부 진단 및 치료, 파일의 보호를 할 수 있으며 예방도 가능함.</p>			
비고	장기 적용(적용 시 개발자 및 운영자 협의)			

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

6.2. 최신 엔진 업데이트

분류	바이러스 진단	보안항목	최신 엔진 업데이트	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	상
내용 및 적용방법	<p>악성 파일 및 바이러스로부터 시스템을 보호하기 위한 백신 프로그램 업데이트 점검</p> <p>■ 기준</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">가. 최신 엔진 업데이트 설치</div> <p>양호 - 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있을 경우 취약 - 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않은 경우</p> <p>■ 조치방법</p> <p>백신 사들 마다 다소 차이는 있으나 매주 업데이트가 이뤄지고, 긴급한 경우 수시로 업데이트를 하고있음. 정기적인 업데이트를 통해 검색엔진을 최신 버전으로 유지하고, 백신 에서 발표하는 경보를 주시</p> <p>또한, 백신 프로그램의 자동 업데이트 기능을 이용하면 인터넷에 연결되어 있을 때 변동 사항을 자동으로 업데이트 가능</p> <p>안철수연구소, 하우리 : 매주 수요일 정기업데이트 시만텍코리아, 트랜드마이크로 : 매주 목요일 정기업데이트 (미국시간으로 수요일)</p> <p>※ 4개 백신업체 모두 긴급시 수시업데이트 및 실시간 업데이트 기능 제공</p> <p>■ 상세설명</p> <p>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.</p>			
비고	장기 적용(적용 시 개발자 및 운영자 협의)			

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

7. 레지스트리 보안 설정

7.1. SAM(Security Account Manager) 보안 감사 설정

분류	레지스트리 보안 설정	보안항목	SAM 보안 감사 설정	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	하
내용 및 적용방법				

계정의 대한 보안운영을 위한 SAM 파일의 대한 감사 설정

■ 기준

가. SAM 파일의 대한 레지스트리 값에 Everyone 에 대한 감사 설정

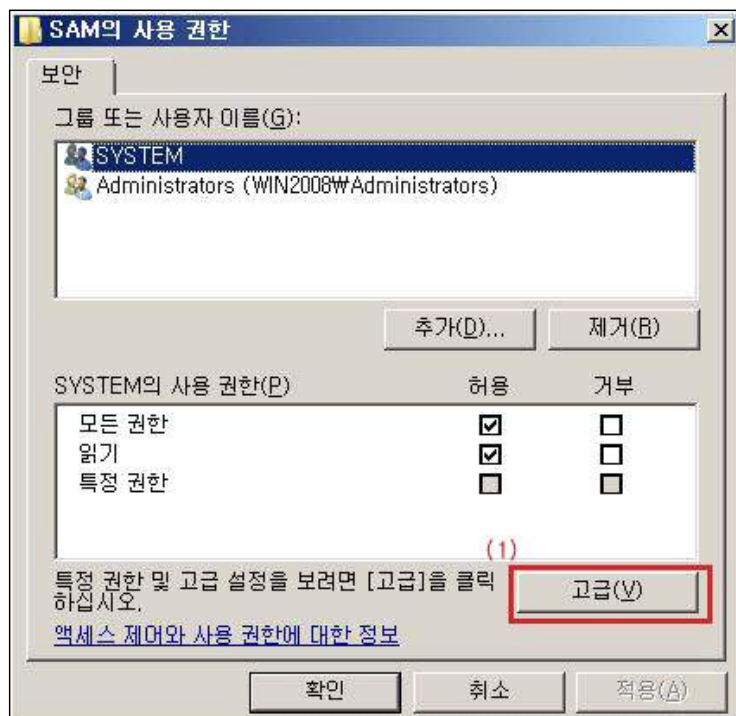
양호 - 해당 레지스트리 값에 Everyone 에 대한 감사설정이 되어 있을 경우

취약 - 해당 레지스트리 값에 Everyone 에 대한 감사설정이 되어 있지 않을 경우

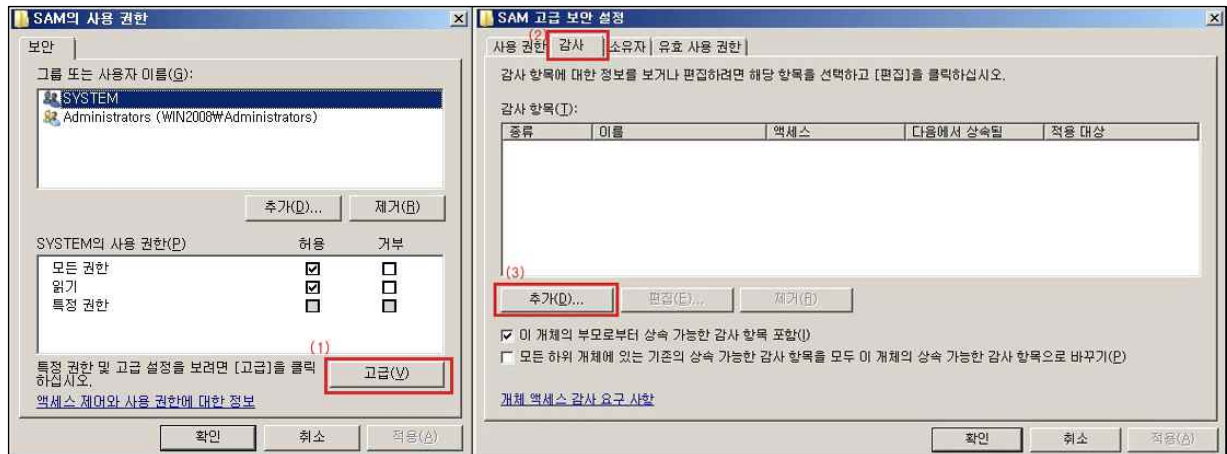
■ 조치방법

시작>실행>regedit 실행

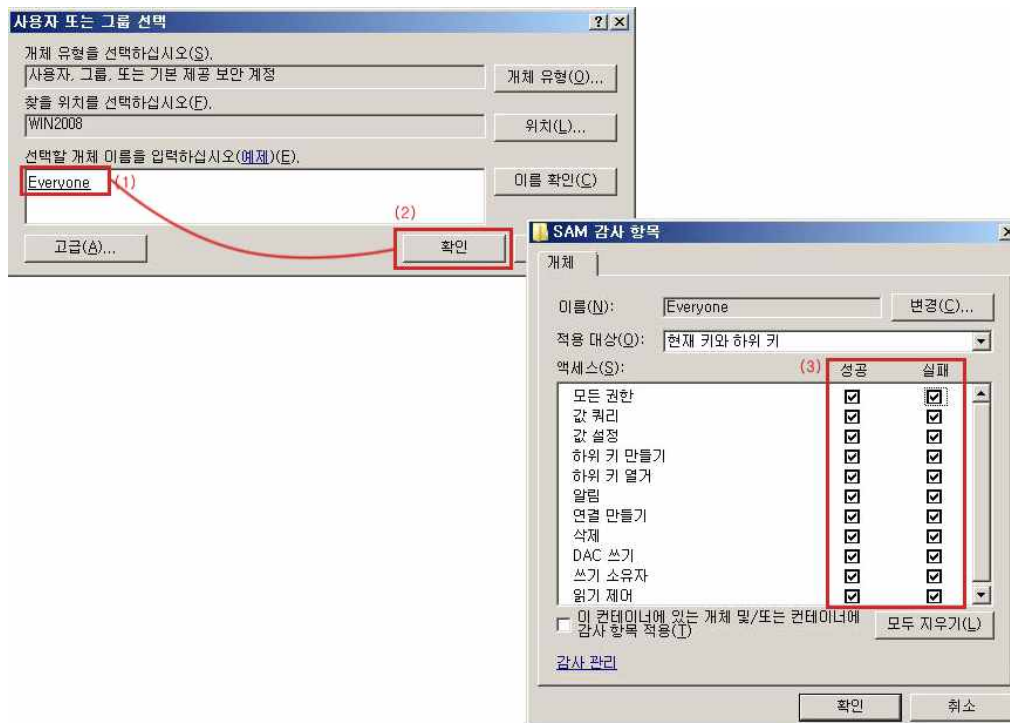
HKLM 에서 SAM 키를 선택한 후 편집 메뉴에서 [사용권한] 선택



“고급” 옵션을 선택 후 SAM 고급 보안 설정 창에서 “감사”탭 > “추가” 선택



감사할 사용자 및 그룹을 추가함 (Everyone 권고)



객체 액세스 모든 옵션에 대해 성공/실패 감사 체크

■ 상세설명

SAM 에 대한 감사를 설정하여 감시하는 기능. SAM 은 Security Account Manager 의 약어로써 Windows 시스템에서의 계정에 대한 인증을 관리함. 계정의 인증 성공 및 실패에 대한 감사를 함으로써 서버에 대한 좀 더 보안적인 운영을 할 수 있음.

비고

단기 적용(적용 시 개발자 및 운영자 협의)

7.2. Null Session 설정

분류	레지스트리 보안 설정	보안항목	Null Session 설정		
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)			중요도	상
내용 및 적용방법					

비 인가자가 Null Session 을 통한 접근을 제한 하는 설정

■ 기준

가. 해당 레지스트리의 "RestrictAnonymous" 값이 "2"로 설정

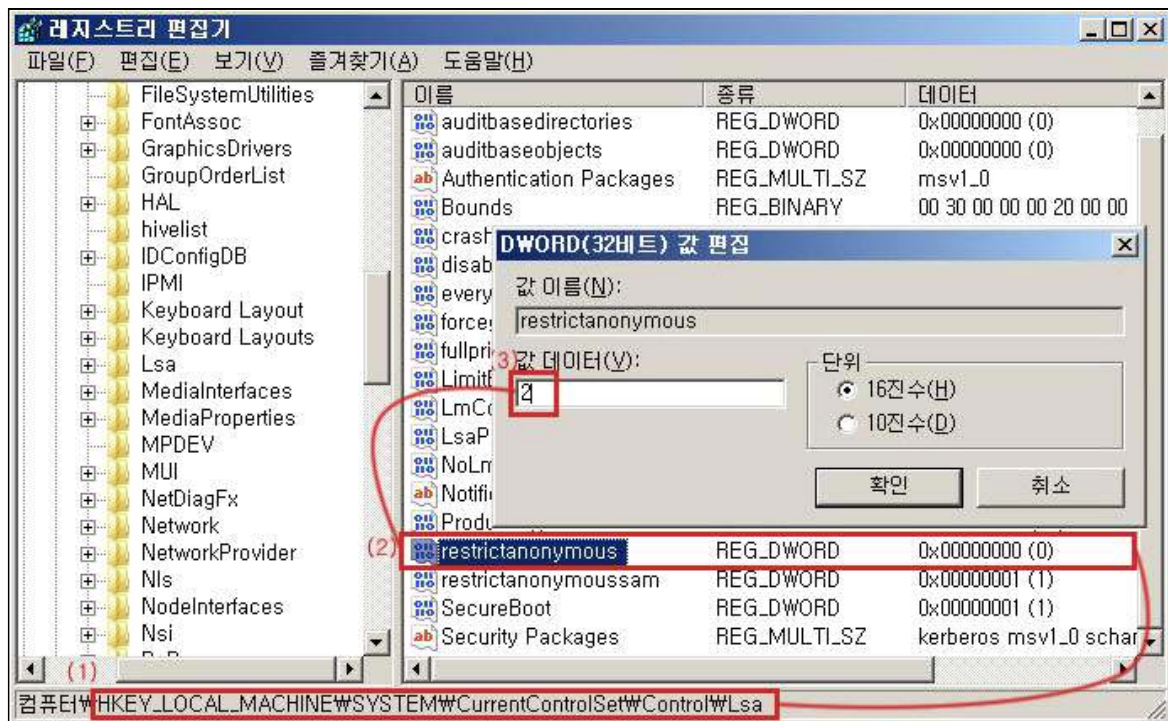
양호 - 해당 레지스트리의 RestrictAnonymous 값이 "2"로 설정된 경우

취약 - 해당 레지스트리의 RestrictAnonymous 값이 "2"가 아니거나 설정되지 않은 경우

■ 조치방법

- 인증된 사용자만 접속허용

1. 시작>실행>regedit 를 실행
2. HKLM\SYSTEM\CurrentControlSet\Control\Lsa 레지스트리를 검색
3. 오른쪽 버튼을 눌러 새로만들기|DWORD값 을 선택
4. RestrictAnonymous 를 입력. 이때 값을 "2"로 변경



■ 상세설명

Windows는 비인가된 사용자가 Null Session을 통해 사용자 인증을 거치지 않고 서버에 접근, 시스템 내부로의 접근이 가능한 취약성이 존재함.

- 인증된 사용자만 접속허용

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

참조) 로컬 보안 설정의 “SAM 계정과 공유의 익명 열거 허용 안 함” 에서 “사용” 설정시 레지스트리 값에는 “1” 값이 적용 되므로 “레지스트리 편집기(regedit.exe)”를 통해 값을 직접 “2”로 설정할 것을 권고. 해당 레지스트리 값이 “1”로 설정시, SMB를 통해 null session을 맺은 후 목록화를 이용하여 시스템의 중요 정보 획득이 가능

비고	단기 적용(적용 시 개발자 및 운영자 협의)
-----------	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

7.3. Remote Registry Service 설정

분류	레지스트리 보안 설정	보안항목	Remote Registry Service 설정
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)	중요도	하
내용 및 적용방법			

원격으로 레지스트리 접근 제한을 위한 Remote Registry Service 제거

■ 기준

가. Remote Registry Service 제거

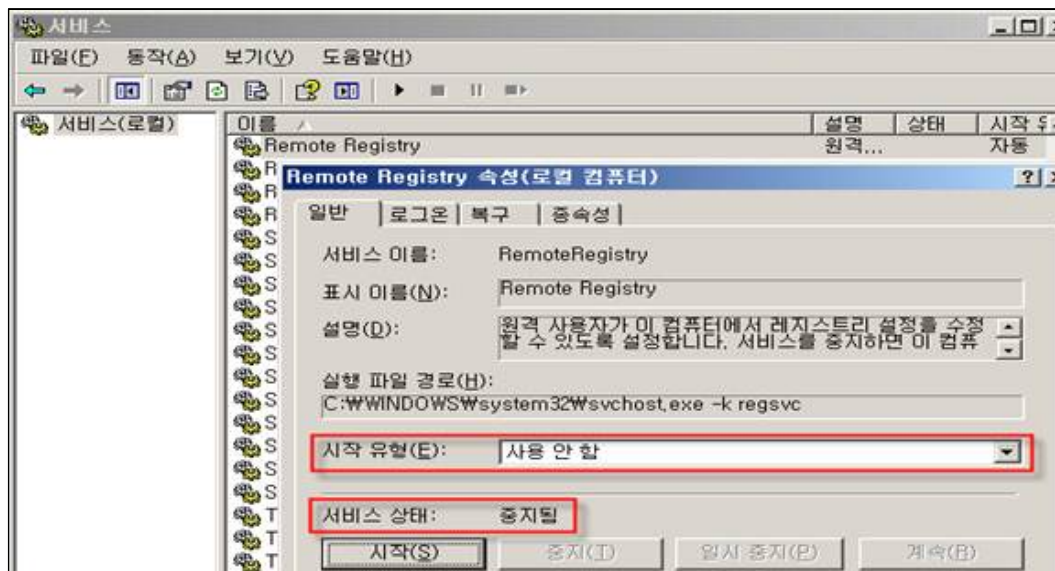
양호 - Remote Registry Service 가 중지되어 있을 경우

취약 - Remote Registry Service 가 사용 중일 경우

■ 조치방법

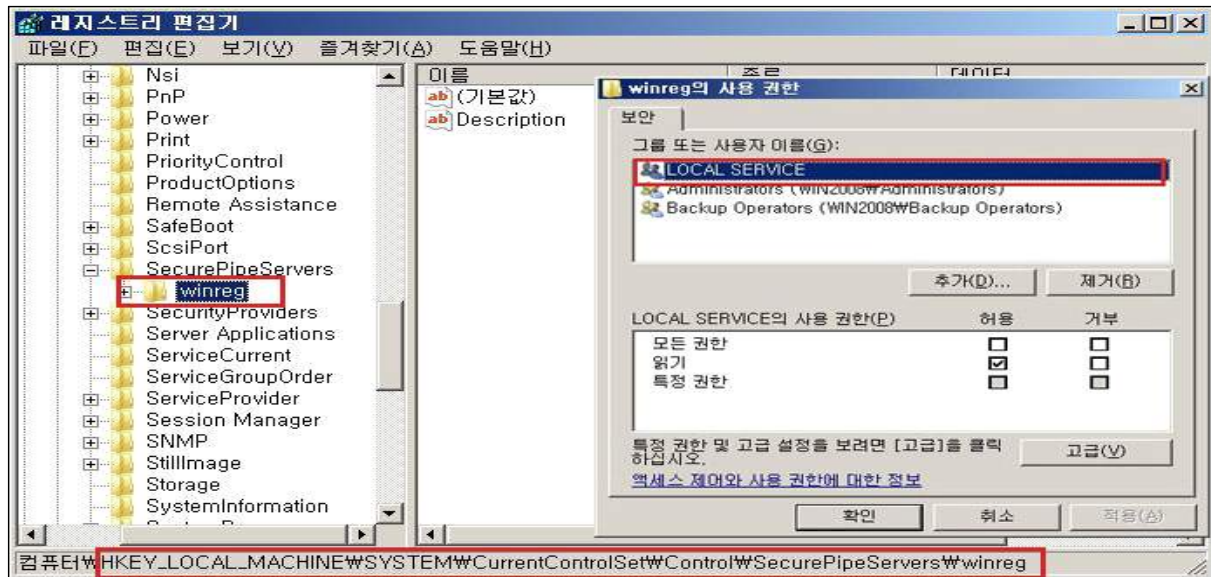
반드시 필요한 경우를 제외하고는 “불필요한 서비스제거” 항목을 참조하여 “Remote Registry Service” 를 중지시켜야 함

시작>설정>제어판>관리도구>서비스 에서 해당 서비스 중지



꼭 필요한 경우 다음과 같은 방법으로 원격 레지스트리 접근을 제한

1. 시작>실행>regedit 실행 다음 winreg 선택 (존재하지 않는 경우 생성)
HKEY_LOCAL_MACHINE\ SYSTEM\CurrentControlSet\Control\SecurePipeServers\winreg
Name : Description
Value : Registry Server (한글로 “레지스트리 서버”도 동일한 설정)
2. winreg키를 선택하고, “편집” 메뉴를 선택한 다음, “사용 권한”을 선택
3. 원격 레지스트리 접근을 허용할 계정 추가



■ 상세설명

Windows에 의해 사용되는 모든 초기화와 환경설정 정보는 레지스트리에 저장되어 있음.

일반 사용자들은 쉽게 레지스트리를 읽을 수 있지만 레지스트리를 수정하기 위해서는 HKEY_CURRENT_USER를 제외하고는 관리자의 권한이 필요함.

레지스트리 편집기는 원격접속으로도 그 키를 바꿀 수 있는데 이는 대단히 위험한 것으로 네트워크를 통한 레지스트리 접속을 차단해야 됨.

원격에서 레지스트리로의 접근을 위해서는 관리자의 권한 또는 원격에서 접근을 하기 위한 특별한 계정이 필요함.

윈도우에서는 원격에서 레지스트리 접근에 대한 요구를 다루기 위해 원격 레지스트리 서비스를 제공하고 있는 데 이 서비스를 중지시키면 레지스트리에 대한 어떠한 원격 접근도 막을 수 있음.

원격 레지스트리 서비스를 중지시키지 않고 레지스트리에 대한 원격 접근을 제어하기 위해 윈도우에서는 winreg라는 키를 생성하여 레지스트리 접근에 대한 사용자, 그룹, 서비스를 제어함.

비고

단기 적용(적용 시 개발자 및 운영자 협의)

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

7.4. AutoLogon 제한 설정

분류	레지스트리 보안 설정	보안항목	Autologon 제한 설정
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도
내용 및 적용방법			중

해킹 방지를 위한 AutoLogon 사용 제한 설정

■ 기준

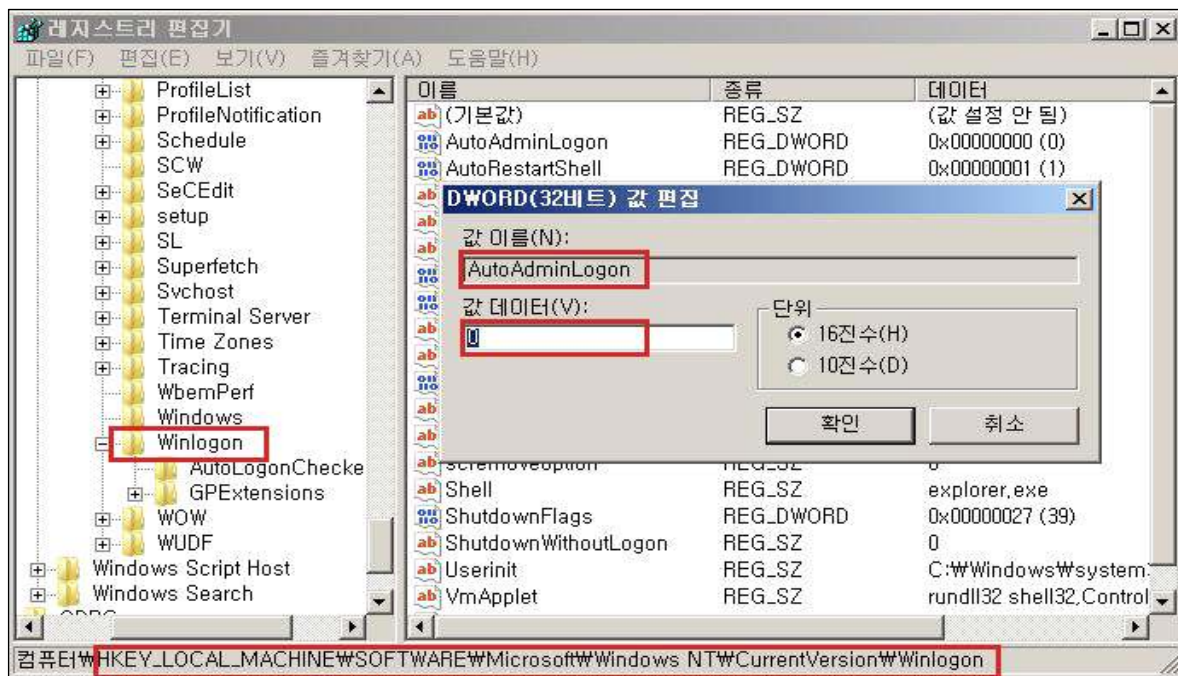
가. 해당 레지스트리의 “AutoAdminLogon” 값이 없거나 “0”으로 설정

양호 - AutoAdminLogon 값이 없거나 0으로 설정되어 있는 경우

취약 - AutoAdminLogon 값이 1로 설정되어 있는 경우

■ 조치방법

1. 시작>실행>regedt32를 실행
2. HKLM\ Software\Microsoft\Windows NT\CurrentVersion\Winlogon
3. AutoAdminLogon 값을 0으로 세팅
4. DefaultPassword 엔트리가 존재한다면 삭제



■ 상세설명

Autologon 기능을 사용하면 침입자가 해킹 도구를 이용하여 레지스트리에서 로그인 계정 및 암호를 확인할 수 있으므로 Autologon 기능을 사용하지 말아야 함.

비고	단기 적용(적용 시 개발자 및 운영자 협의)
----	--------------------------

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

8. 보안 패치

8.1. 최신 서비스 팩 적용

분류	보안 패치	보안항목	최신 서비스 팩 적용	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	상
내용 및 적용방법	<p>시스템 안정 및 보안성 향상을 위한 최신 서비스팩 적용여부 점검</p> <p>■ 기준</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">가. 최신 서비스팩 설치</div> <p>양호 - 최신 서비스팩이 설치되어 있는 경우 취약 - 최신 서비스팩이 설치 되어 있지 않은 경우</p> <p>■ 조치방법</p> <p>설치되어 있는 Service Pack 을 확인하기 위해 'Winver' 명령어를 이용해 확인 할 수 있음. 또한 만약 O/S가 필요에 의하여 재설치 되어 진다면 네트워크에 연결하기 이전에 최신 서비스팩 및 각종 보안 패치를 적용</p> <p>Service Pack 설치 시에는 네트워크와 분리된 상태에서 설치 할 것을 권장 함. 현재 많은 인터넷 웜(Worm)이 Windows 의 취약점을 이용하여 공격을 하기 때문에 O/S를 설치한 후 곧바로 네트워크에 연결하는 것은 곧바로 서버에 피해를 입을 수 있기 때문 임</p> <p>현재까지 발표된 Windows 2008 Server의 가장 최신 Service Pack은 SP2 이며 Microsoft® 홈페이지에서 다운로드 받을 수 있음 http://www.microsoft.com/downloads/details.aspx?FamilyID=891ab806-2431-4d00-afa3-99ff6f22448d&displaylang=ko</p> <p>현재까지 발표된 Windows 2008 R2의 가장 최신 Service Pack은 SP1 이며 Microsoft® 홈페이지에서 다운로드 받을 수 있음 http://www.microsoft.com/downloads/ko-kr/details.aspx?FamilyID=c3202ce6-4056-4059-8a1b-3a9b77cdfdda&displaylang=ko</p> <p>■ 상세설명</p> <p>서비스 팩은 Windows 시스템을 마이크로소프트에서 출시하고 난 뒤 Windows와 관련된 응용프로그램, 서비스, 실행파일 등 여러 수정 파일들을 모아 놓은 프로그램 임.</p>			
비고	장기 적용(적용 시 개발자 및 운영자 협의)			

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

8.2. 최신 HOT FIX 적용

분류	보안 패치	보안항목	최신 HOT FIX 적용	
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)		중요도	상
내용 및 적용방법	<p>시스템 안정 및 보안성 향상을 위한 최신 HOT FIX적용여부 점검</p> <p>■ 기준</p> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;">가. 최신 HOT FIX가 설치</div> <p>양호 - 최신 HOT FIX가 설치되어 있는 경우 취약 - 최신 HOT FIX가 설치되어 있지 않은 경우</p> <p>■ 조치방법</p> <p>1. 아래의 패치 리스트를 조회하여, 서버에 필요한 패치를 선별하여 수동으로 설치 하는 것을 권장 Microsoft 제공 최신 패치 리스트 http://technet.microsoft.com/ko-kr/security/bulletin/</p> <p>2. Windows 자동 업데이트 기능을 이용한 설치 수동 업데이트의 부담을 덜어주기 위하여 Microsoft에서는 자동으로 시스템에 필요한 Hot Fix 및 소프트웨어 업그레이드를 보여주고 다운로드 및 적용을 쉽게 하기 위한 사이트를 마련해 놓고 있음 Internet Explorer 도구 메뉴 중 “Windows Update” 라는 것을 선택하여 주면 자동으로 Windows Update 사이트로 이동하게 되며 또한 다음의 URL 을 직접 주소 입력 창에 입력 http://windowsupdate.microsoft.com/?IE</p> <p>주의) 보안패치 및 Hot Fix의 경우는 적용 후 시스템 재시작을 요하는 경우가 대부분이므로 관리자는 서비스에 지장이 없는 시간대에 적용을 하는 것을 권장 시스템에 알맞은 Hot Fix는 수행되고 있는 OS프로그램 및 특히 개발되거나 구매한 Application 프로그램에 영향을 줄 수 있음. 따라서 패치 적용 전 Application 프로그램을 구분하고, 필요하다면 OS 벤더 또는 Application 엔지니어의 확인 하에 패치를 수행</p> <p>■ 상세설명</p> <p>Hot Fix는 즉시 교정되어야만 하는 주요한 취약점(주로 보안과 관련된)을 패치하기 위해 배포되는 프로그램 임. Hot Fix는 각각의 Service Pack 이 발표된 이후 패치가 추가될 필요가 있을 때 별도로 발표 됨. 때론, Hot Fix 보다 취약성을 이용한 공격도구가 먼저 출현 할 수 있으므로 Hot Fix는 발표 후 가능한 빨리 설치 할 것을 권장함.</p>			
비고	장기 적용(적용 시 개발자 및 운영자 협의)			

 서울대학교 SEOUL NATIONAL UNIVERSITY	서버 보안 가이드라인		
	Windows 2008	Ver. 2.0	작성일: 2017. 4. 14.

9. 이슈 취약점

9.1. HeartBleed 취약점

분류	이슈 취약점	보안항목	OpenSSL 버전 취약성
대상 OS	Windows 2008 Standard / EnterpriseEdition(R2포함)	중요도	상
내용 및 적용방법			

OpenSSL 버전 확인 및 HeartBleed 취약점 점검

■ 기준

가. OpensSSL을 사용하지 않거나 최신버전의 OpenSSL를 설치 (OpenSSL 1.0.2k 이상)

양호 - OpensSSL을 사용하지 않거나 최신버전의 OpenSSL를 설치하여 운영하는 경우

취약 - 최신버전의 OpenSSL을 설치하여 운영하지 않는 경우

■ 조치방법

<OpenSSL 버전 및 업데이트 버전 설치>

Heartbleed 취약점의 영향을 받는 OpenSSL 버전은 1.0.1 ~ 1.0.1f, 1.0.2-beta, 1.0.2-beta1 버전으로 현재(2017.04)기준으로 최신 버전인 OpenSSL 1.0.2k 이상의 버전을 사용할 것을 권장

1) OpenSSL 버전 확인

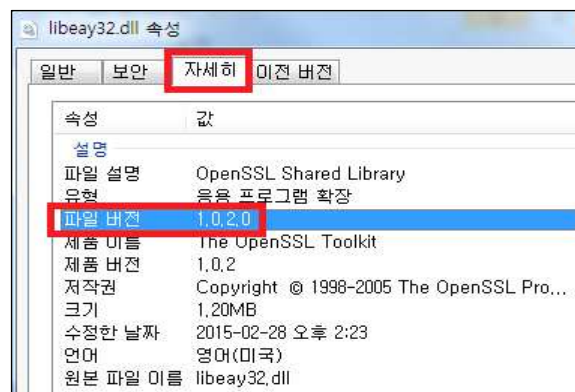
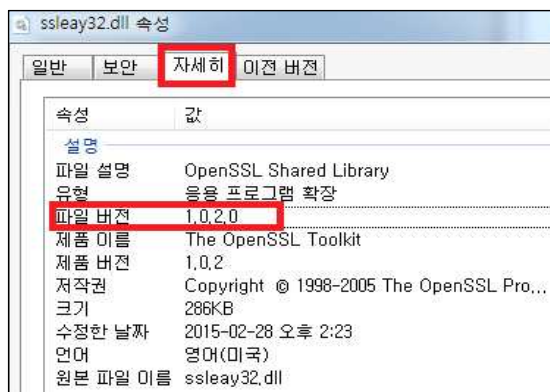
1. cmd창에 openssl version 명령어를 이용한 버전확인

cmd창 실행 후 OpenSSL이 설치된 경로의 bin 폴더로 이동 (디폴트 설치 경로 C:\OpenSSL-Win32\bin) openssl version 입력 후 확인

```
C:\OpenSSL-Win32\bin>openssl version
OpenSSL 1.0.2 22 Jan 2015
```

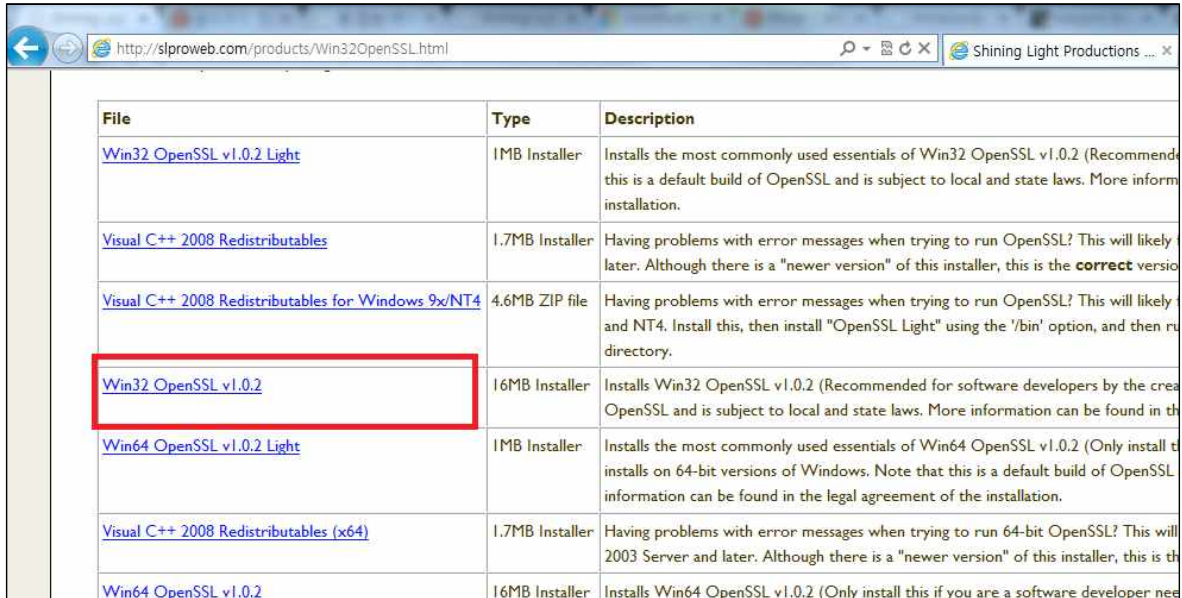
2. 라이브러리 파일의 속성 정보를 이용한 버전확인

OpenSSL이 설치된 경로의 bin 폴더로 이동 (디폴트 설치 경로 C:\OpenSSL-Win32\bin)로 이동
OpenSSL 라이브러리 파일(ssleay32.dll, libeay32.dll)의 우클릭 속성 > 자세히 > 파일버전 확인



2) OpenSSL 보안 패치 방법

취약점에 영향을 받는 버전을 사용할 경우 아래 홈페이지에 접속하여 윈도우 용 최신버전(2017년 4월기준 1.0.2k)을 다운로드 하여 업데이트를 수행하고 서비스 재시작
다운로드 경로 : <http://slproweb.com/products/Win32OpenSSL.html>



File	Type	Description
Win32 OpenSSL v1.0.2 Light	1MB Installer	Installs the most commonly used essentials of Win32 OpenSSL v1.0.2 (Recommended for software developers by the creator of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Visual C++ 2008 Redistributables	1.7MB Installer	Having problems with error messages when trying to run OpenSSL? This will likely fix it. Although there is a "newer version" of this installer, this is the correct version for Windows 9x/NT4.
Visual C++ 2008 Redistributables for Windows 9x/NT4	4.6MB ZIP file	Having problems with error messages when trying to run OpenSSL? This will likely fix it. Although there is a "newer version" of this installer, this is the correct version for Windows 9x/NT4. Install this, then install "OpenSSL Light" using the '/bin' option, and then run the installer.
Win32 OpenSSL v1.0.2	16MB Installer	Installs Win32 OpenSSL v1.0.2 (Recommended for software developers by the creator of OpenSSL and is subject to local and state laws. More information can be found in the legal agreement of the installation.
Win64 OpenSSL v1.0.2 Light	1MB Installer	Installs the most commonly used essentials of Win64 OpenSSL v1.0.2 (Only install this on 64-bit versions of Windows. Note that this is a default build of OpenSSL. More information can be found in the legal agreement of the installation.
Visual C++ 2008 Redistributables (x64)	1.7MB Installer	Having problems with error messages when trying to run 64-bit OpenSSL? This will likely fix it. Although there is a "newer version" of this installer, this is the correct version for Windows 2003 Server and later.
Win64 OpenSSL v1.0.2	16MB Installer	Installs Win64 OpenSSL v1.0.2 (Only install this if you are a software developer needing a full build).

■ 상세설명

OpenSSL은 통신구간 암호화에 사용하는 TLS(Transport Layer Security), SSL(Secure Socket Layer) 프로토콜을 구현한 오픈 소스 라이브러리로 거의 모든 버전의 유닉스 계열 운영체제(솔라리스, 맥 OS X, 리눅스) 및 윈도우 등 널리 이용되고 있음.

2014년 4월 7일 발견된 HeartBleed 취약점(CVE-2014-0610)은 OpenSSL에서 사용하는 확장규격중 하나인 HeartBeat에 버그를 악용하여, 프로토콜에서 클라이언트 요청메시지를 처리할 때 데이터 길이 검증을 수행하지 않아 시스템 메모리에 저장된 64kb 데이터를 외부에서 아무런 제한 없이 탈취 할 수 있는 취약점이다. 예를 들어 이 취약점을 알고 있는 공격자가 서버에 하트비트 프로토콜을 악용해 서버에 저장된 정보들 중 최대 64kb의 내용을 반복해서 요청하면 저장된 개인ID, 패스워드, 주민등록 번호 등 민감한 개인정보 탈취가 가능함.

HeartBeat은 서버와 클라이언트의 안정적인 연결을 유지하기 위해 클라이언트에서 임의의 정보를 전달하면 서버에서 응답하여 연결상태를 알려주는 기능으로 2012년 3월 14일 OpenSSL 1.0.1 버전부터 HeartBleed 취약점이 발견되어 수정되기 전 버전인 1.0.1f까지 탑재되어 배포되었으며, 배포당시 취약하게 구현되어 있는 HeartBeat 기능이 기본적으로 활성화 되어 있기 때문에 취약한 버전의 OpenSSL을 사용하는 시스템의 경우 HeartBleed취약점에 노출되어 있을 가능성이 높기 때문에 취약점 확인과 OpenSSL 최신 업데이트가 필요함.

비고

장기 적용(적용 시 개발자 및 운영자 협의)