

문서번호	J.W.P. MagicShop-250901
작성자	취약점진단팀
보안등급	Confidential
Ver	ver 1.0

"J.W.P. MagicShop" 취약점 조치 이행

DB OS 이행 점검 상세결과

2025년 09월 01일



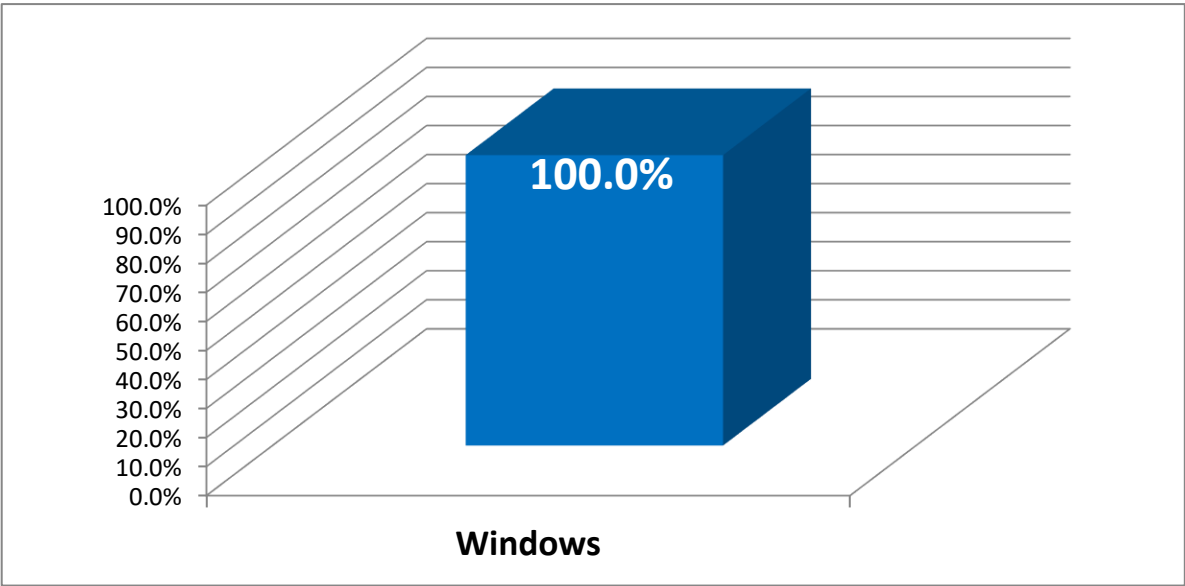
※ 진단 대상 리스트 - 서버 1대 (Windows 1대)

순번	진단 대상				비고
	Hostname	IP Address	버전정보	용도	
Windows					
1	jwp-db-01	10.0.8.8	Windows Server 2019	DB OS	

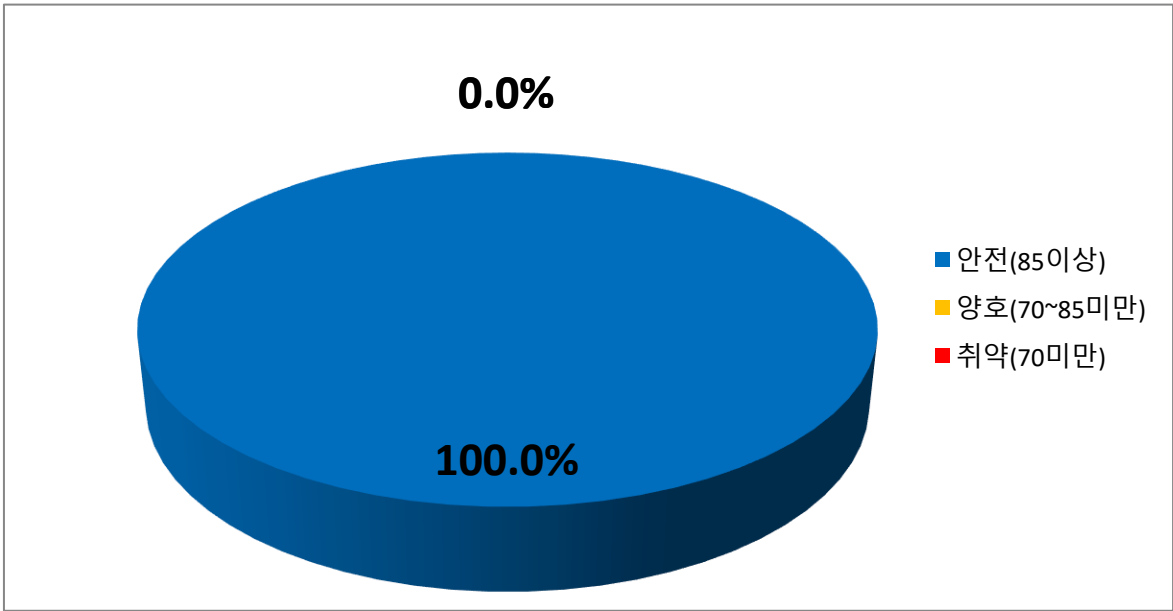
※ 대상별 평균 점수 그래프

진단 대상	평균	수량
Windows	100.0%	1

대상별 평균 점수 현황

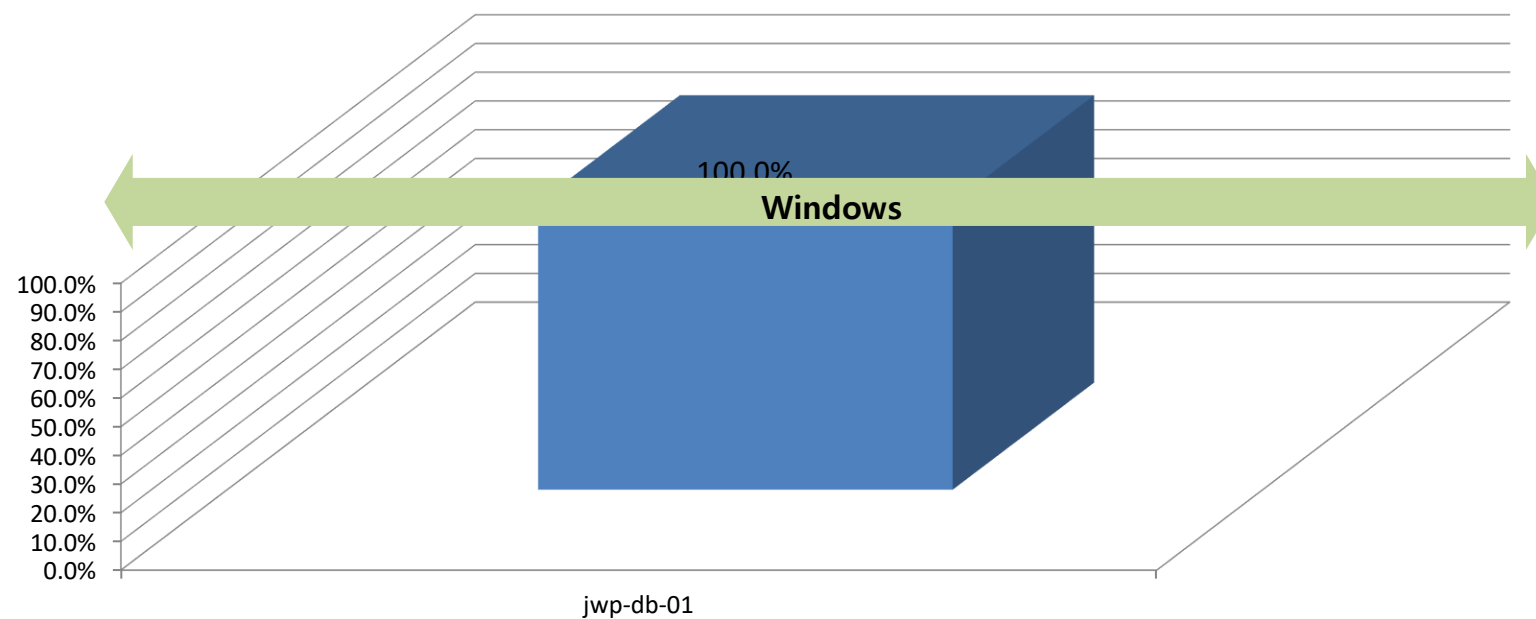


전체		수량
안전(85이상)	100.0%	1
양호(70~85미만)	0.0%	0
취약(70미만)	0.0%	0



서버 진단결과

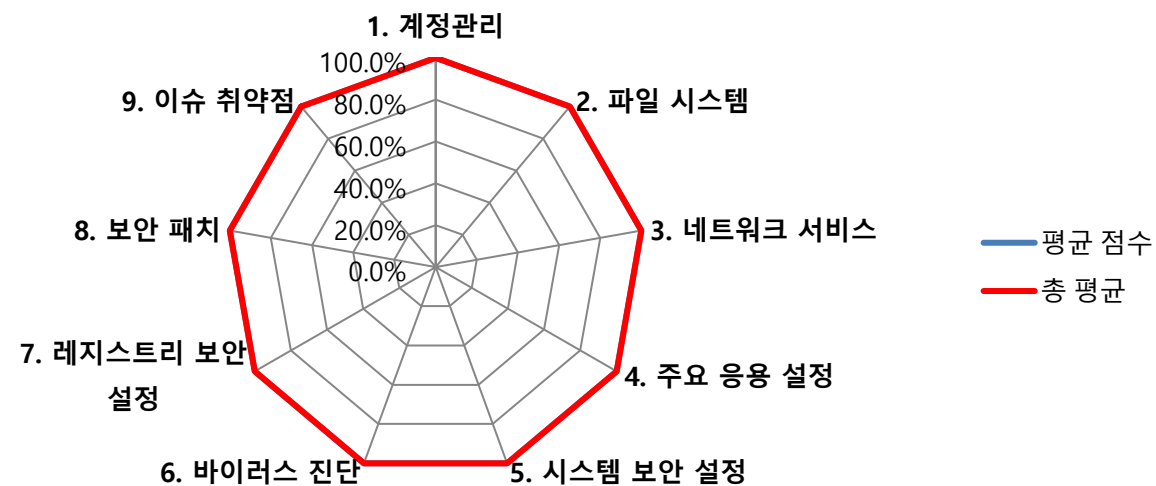
■ 안전(A) ■ 양호(B) ■ 보통이하(C~E)



Windows		
NO.	Hostname	점수
1	jwp-db-01	100.0%

진단 도메인	평균 점수	총 평균
1. 계정관리	100.0%	100.0%
2. 파일 시스템	100.0%	100.0%
3. 네트워크 서비스	100.0%	100.0%
4. 주요 응용 설정	100.0%	100.0%
5. 시스템 보안 설정	100.0%	100.0%
6. 바이러스 진단	100.0%	100.0%
7. 레지스트리 보안 설정	100.0%	100.0%
8. 보안 패치	100.0%	100.0%
9. 이슈 취약점	100.0%	100.0%

Windows 항목별 진단 결과

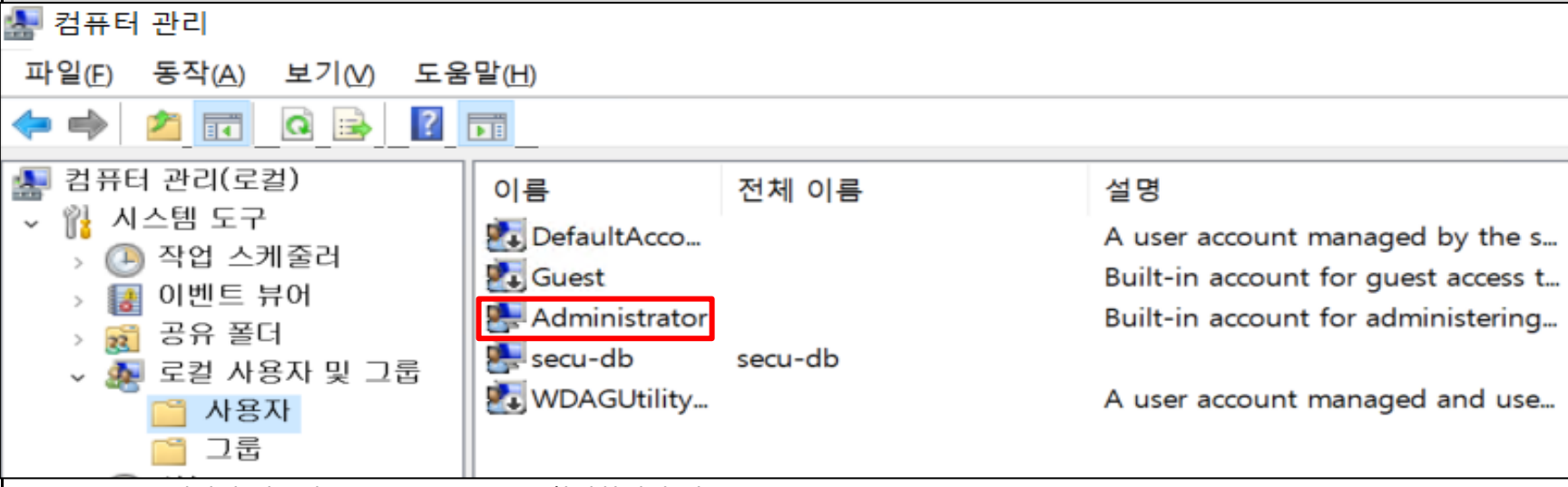
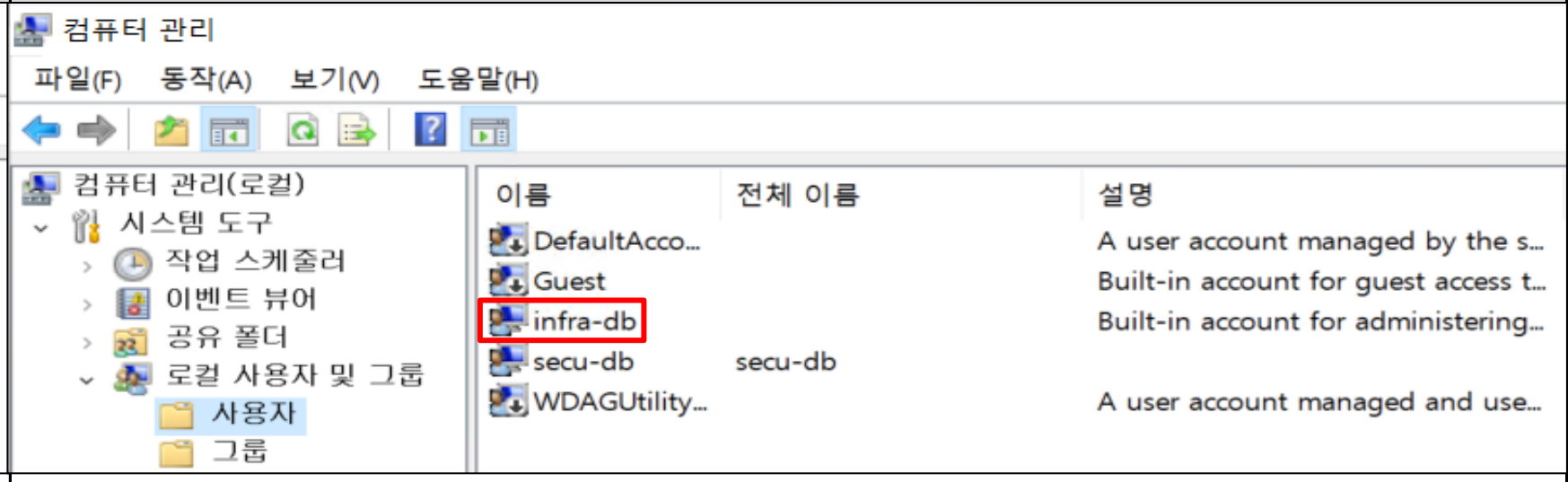
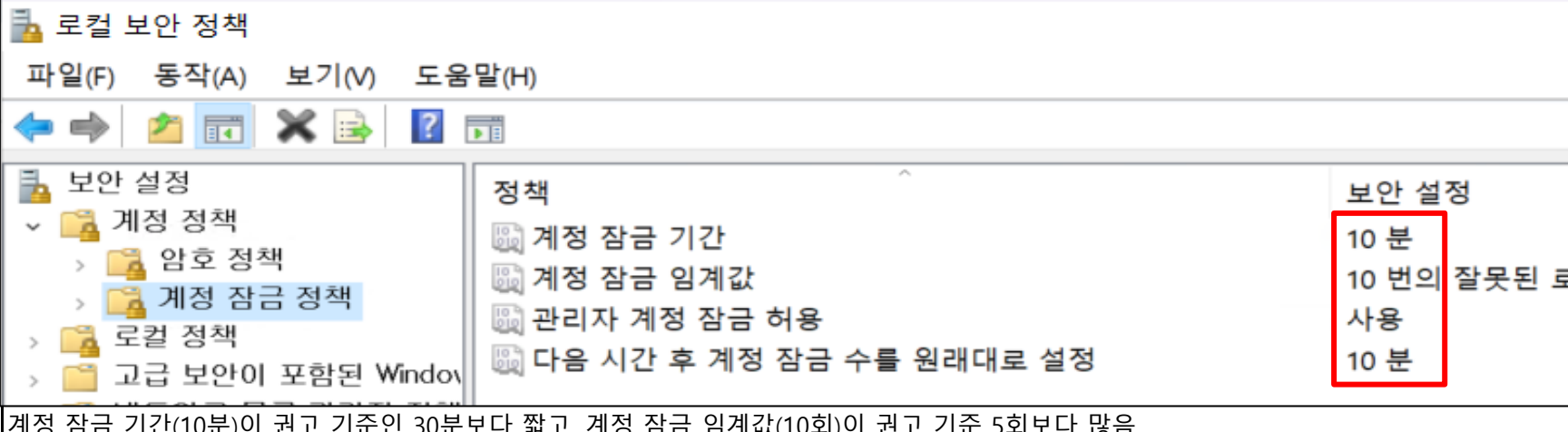
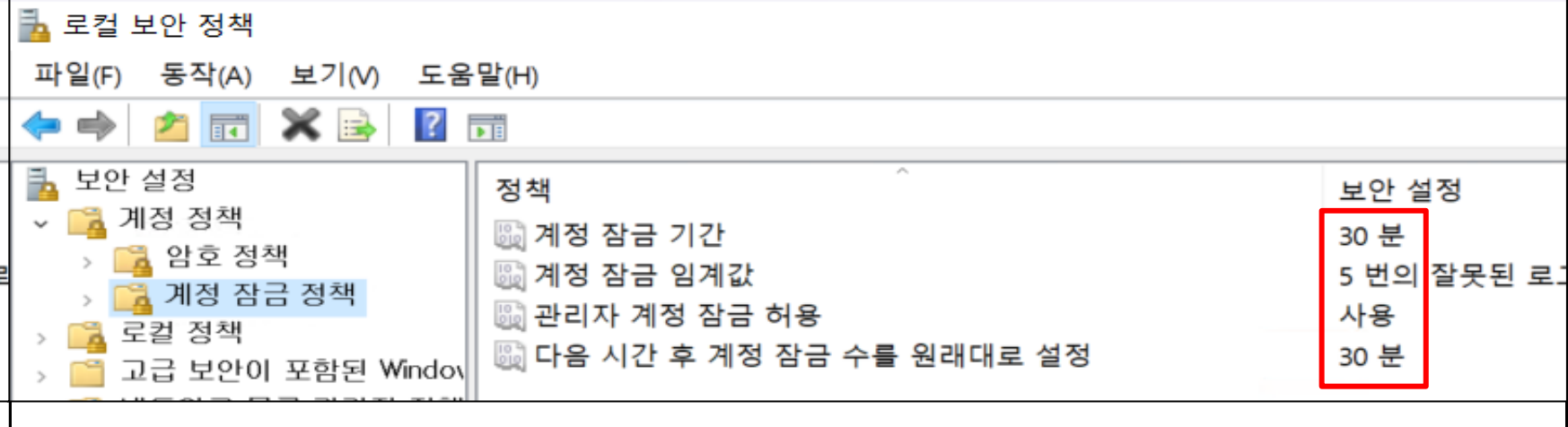
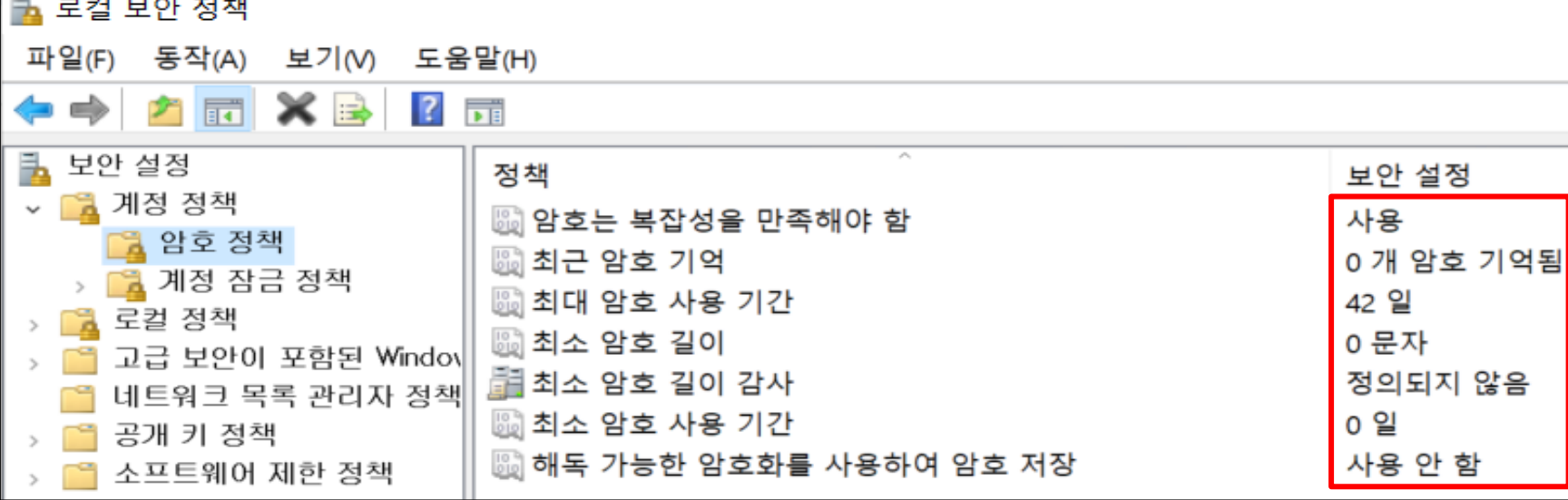
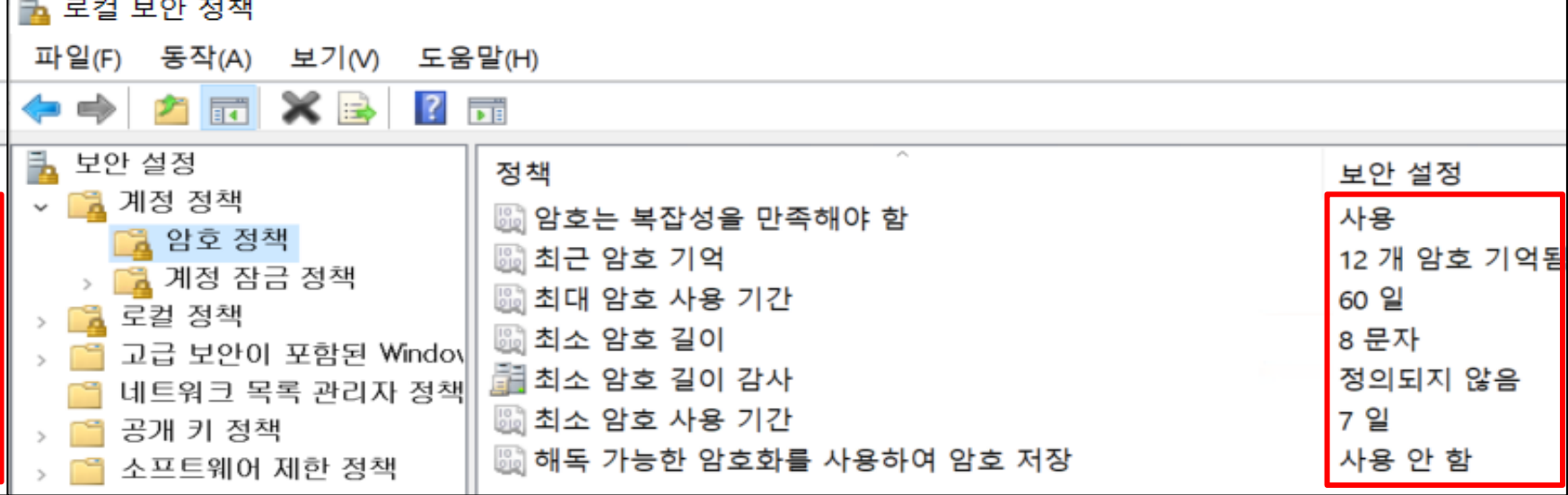
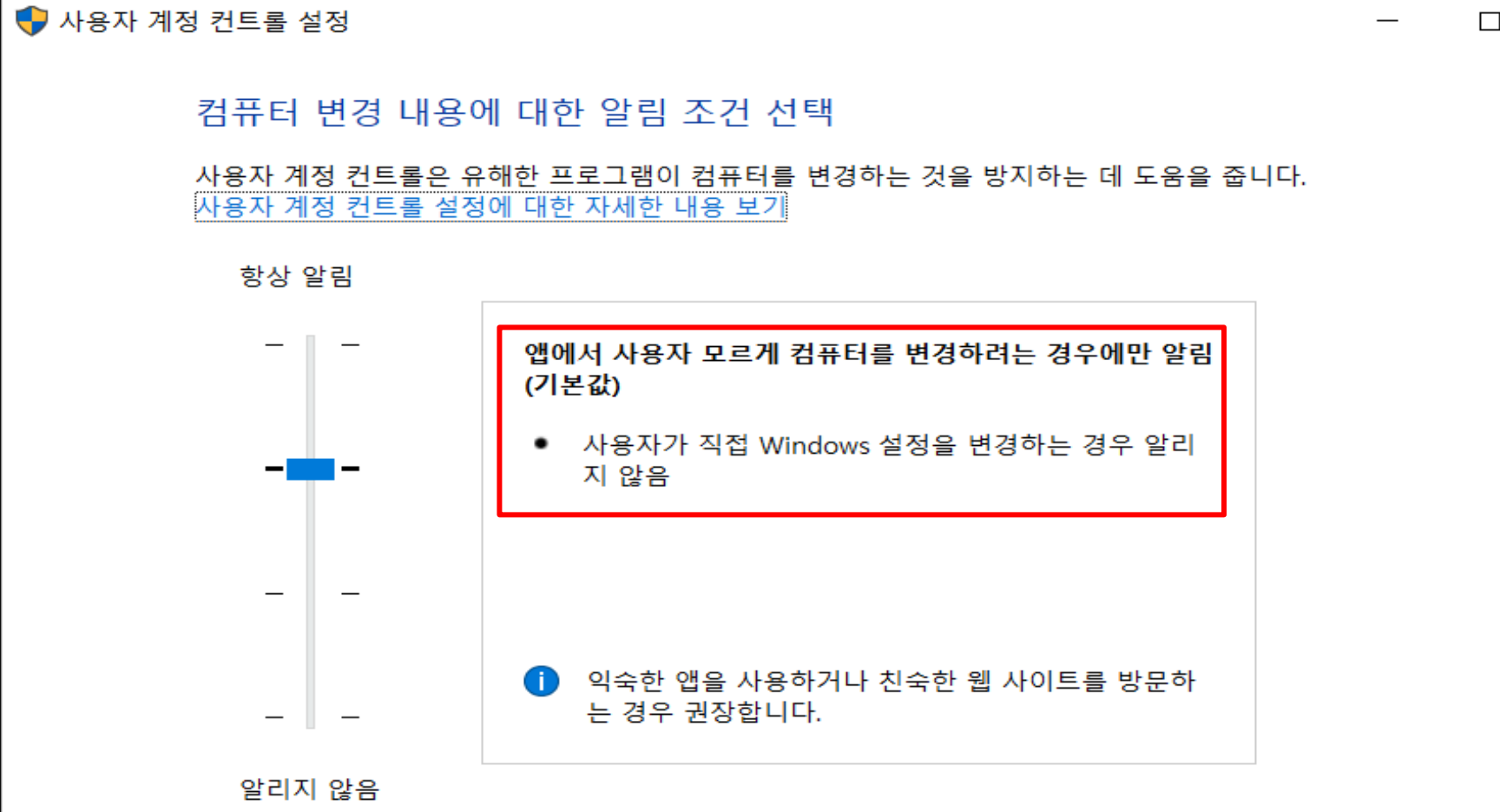



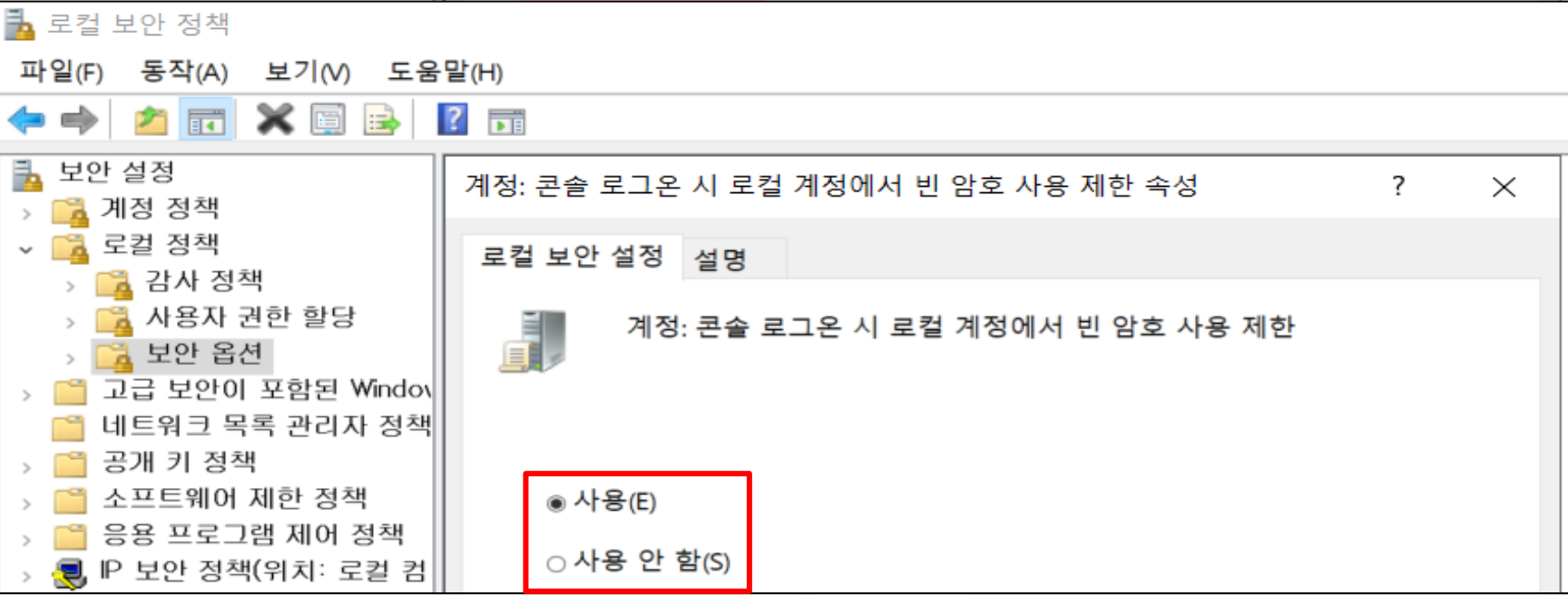

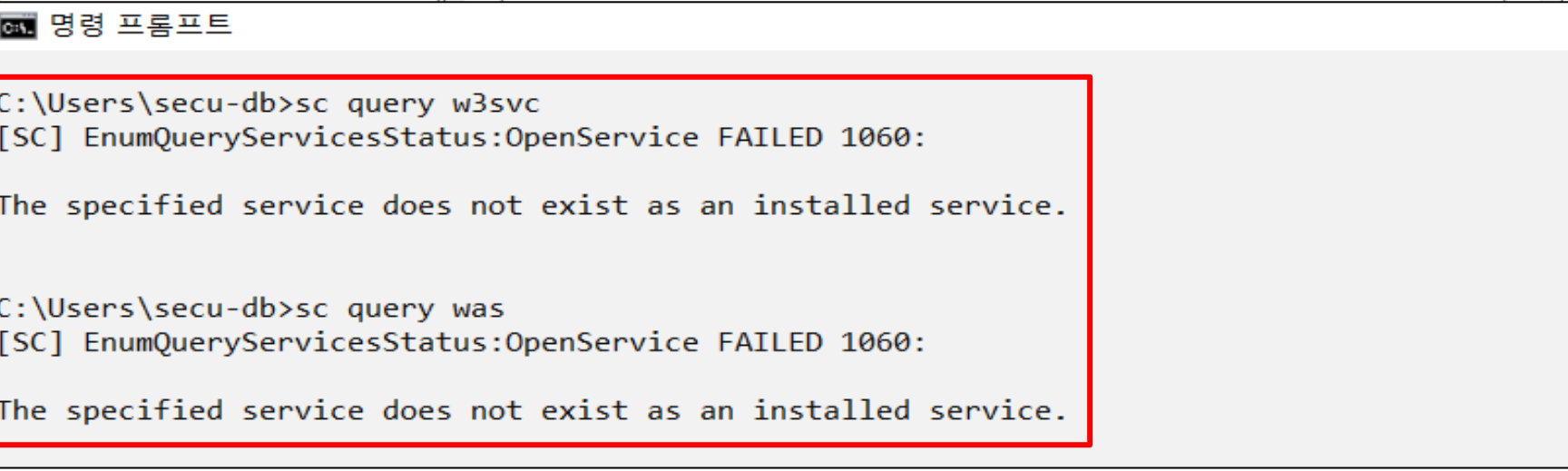
Windows 취약점 진단 요약결과(47항목)

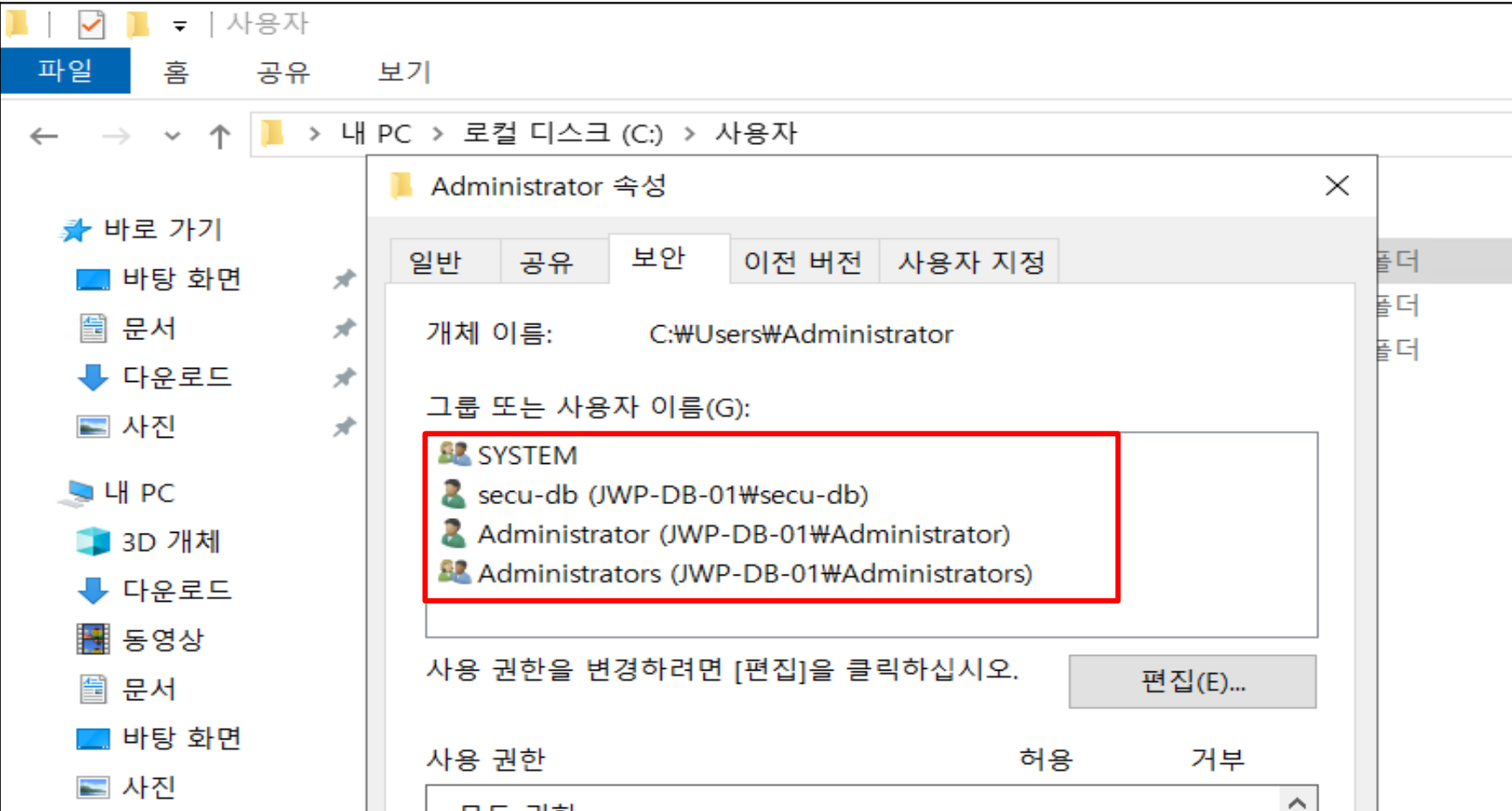
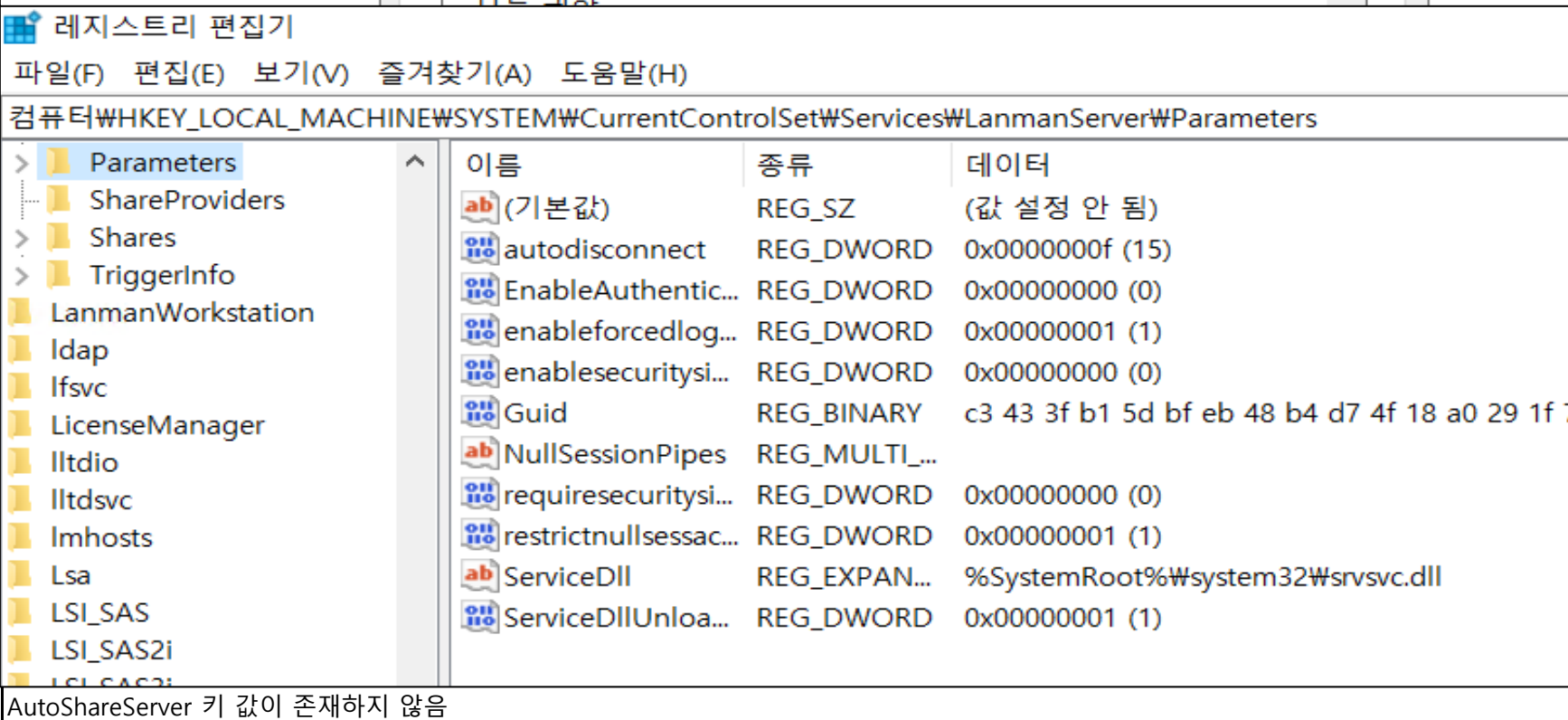
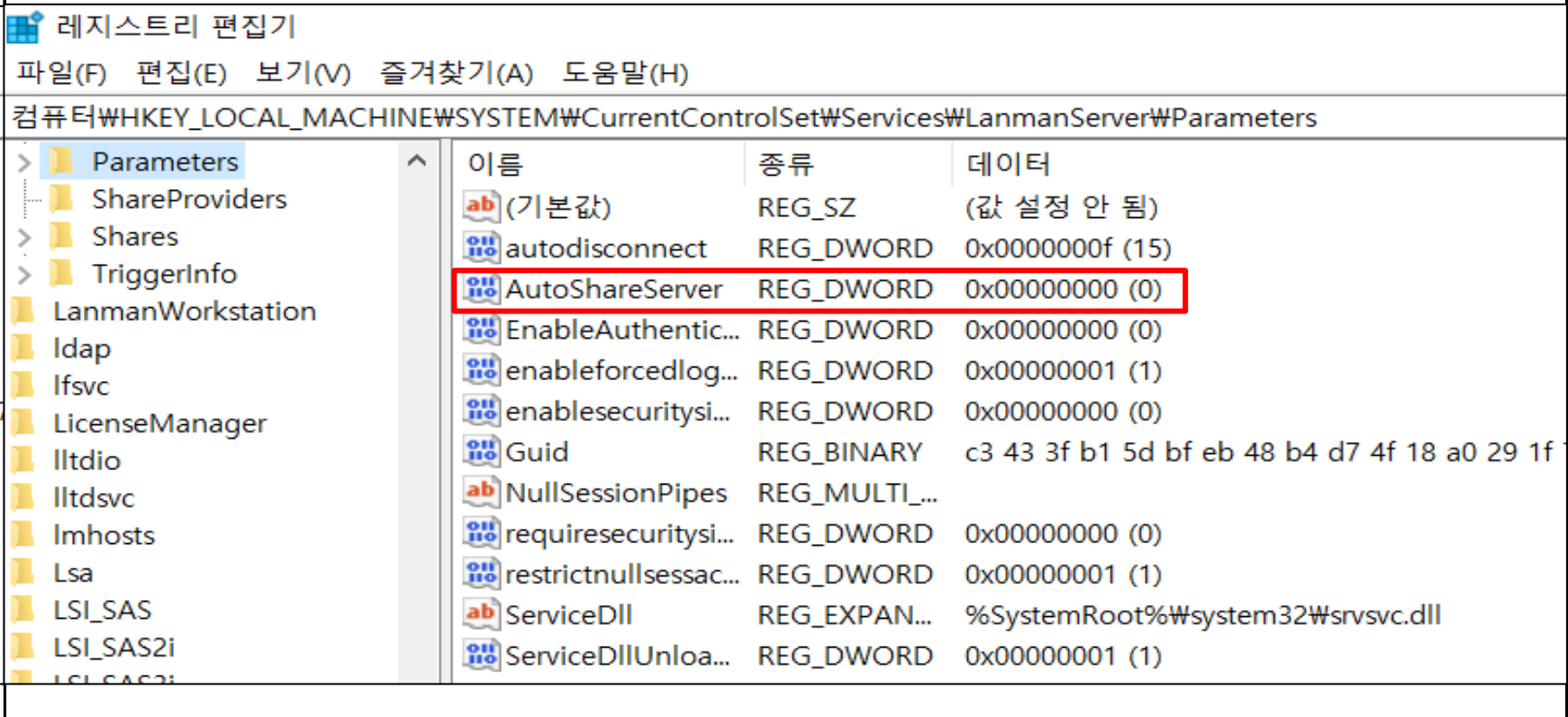
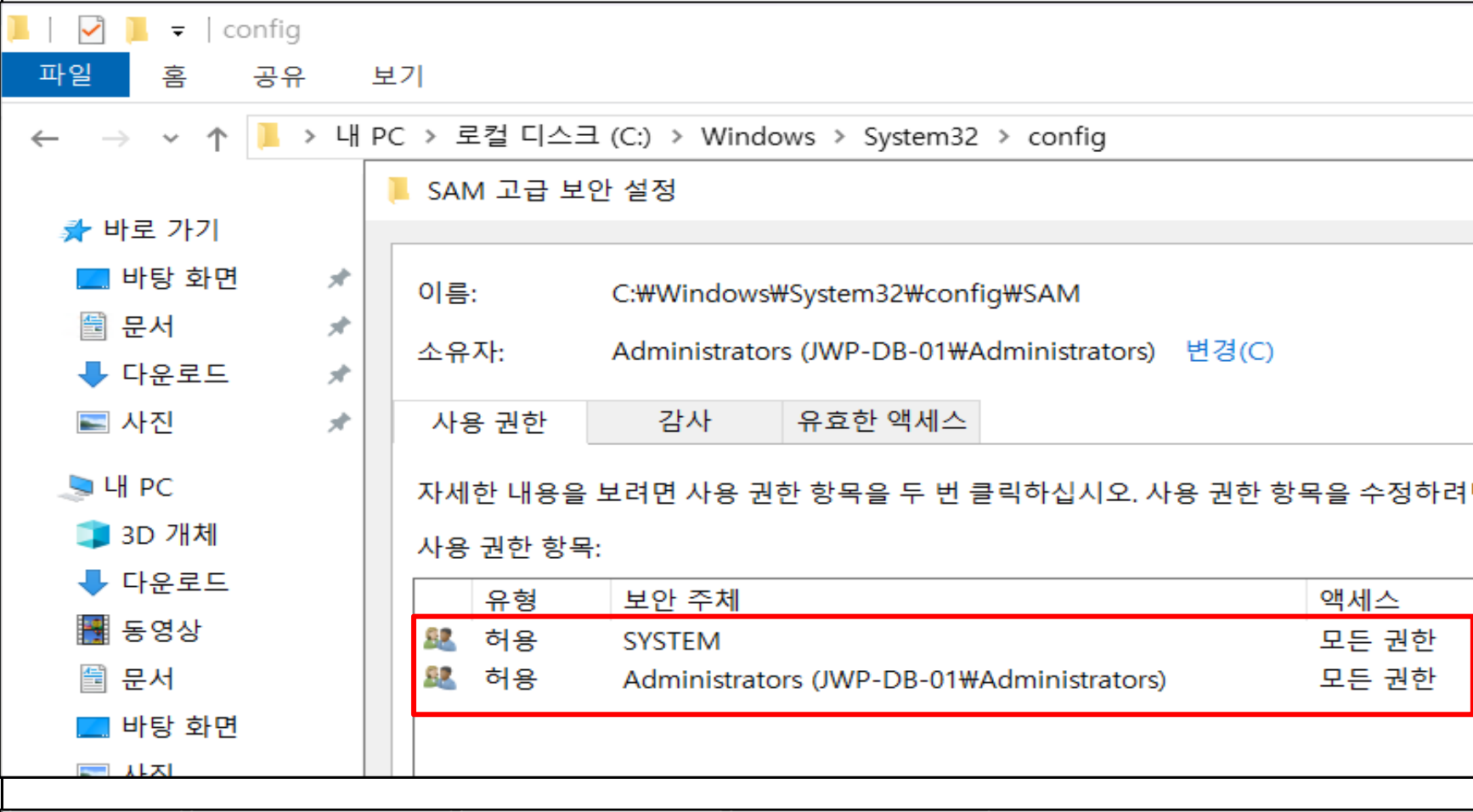
진단항목	No.	세부 진단항목	중 요 도	1
				jwp-db-01
				10.0.8.8
1. 계정관리	1	로컬 계정 사용 설정	상	양호
	2	계정 잠금 정책 설정	상	양호
	3	암호 정책 설정	상	양호
	4	취약한 패스워드 점검	상	양호
	5	사용자 계정 컨트롤(User Account Control) 설정	하	양호
	6	익명 SID/이름 변환 허용 정책	중	양호
	7	콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한 정책 점검	중	양호
	8	관리자 그룹에 최소한의 사용자 포함	상	양호
2. 파일 시스템	1	CMD.EXE 파일 권한 설정	중	양호
	2	사용자 홈 디렉터리 접근 제한	중	양호
	3	공유 폴더 설정	상	양호
	4	SAM(Security Account Manager) 파일 권한 설정	상	양호
	5	파일 및 디렉터리 보호	N/A	N/A
3. 네트워크 서비스	1	불필요한 서비스 제거	상	양호
	2	터미널 서비스 암호화 수준 설정	중	양호
	3	NetBIOS 서비스 보안 설정	상	양호
	4	터미널 서비스 Time Out 설정	중	양호
4. 주요 응용 설정	1	Telnet 서비스 보안 설정	N/A	N/A
	2	DNS(Domain Name Service) 보안 설정	중	양호
	3	SNMP(Simple Network Management Protocol) 서비스 보안 설정	상	양호
5. 시스템 보안 설정	1	원격 로그파일 접근 진단	하	양호
	2	화면 보호기 설정	하	양호
	3	이벤트 뷰어 설정	상	양호
	4	로그인 시 경고 메시지 표시 설정	중	양호
	5	마지막 로그인 사용자 계정 숨김	중	양호
	6	로그온 하지 않은 사용자 시스템 종료 방지	중	양호
	7	로컬 감사 정책 설정	상	양호
	8	가상 메모리 페이지 파일 삭제 설정	하	양호
	9	Lan Manager 인증 수준	하	양호
	10	Everyone 사용 권한을 익명 사용자에게 적용 안함	하	양호
	11	이동식 미디어 포맷 및 꺼내기 admin만 허용	하	양호
	12	세션 연결 끊기 전 유희 시간 설정	하	양호
	13	예약된 작업 의심스런 명령어나 파일 점검	중	양호
	14	원격 시스템 종료 권한 설정	상	양호
	15	보안 감사를 로그 할 수 없는 경우 즉시 시스템 종료 방지	상	양호
	16	보안 채널 데이터 디지털 암호화 또는 서명 설정	중	양호
6. 바이러스 진단	1	백신 프로그램 설치	중	양호
	2	최신 엔진 업데이트	중	양호
7. 레지스트리 보안 설정	1	SAM(Security Account Manager) 보안 감사 설정	하	양호
	2	Null Session 설정	상	양호
	3	Remote Registry Service 설정	상	양호
	4	RDS(Remote Data Service) 제거	N/A	N/A
	5	AutoLogon 제한 설정	중	양호
	6	DOS 공격에 대한 방어 레지스트리 설정	N/A	N/A
8. 보안 패치	1	최신 서비스 팩 적용	상	양호
	2	최신 HOT FIX 적용	상	양호
9. 이슈 취약점	1	OpenSSL 취약점	상	양호
점검결과			0	
	보안 적용율 (양호항목 / 진단항목) %		100.0%	

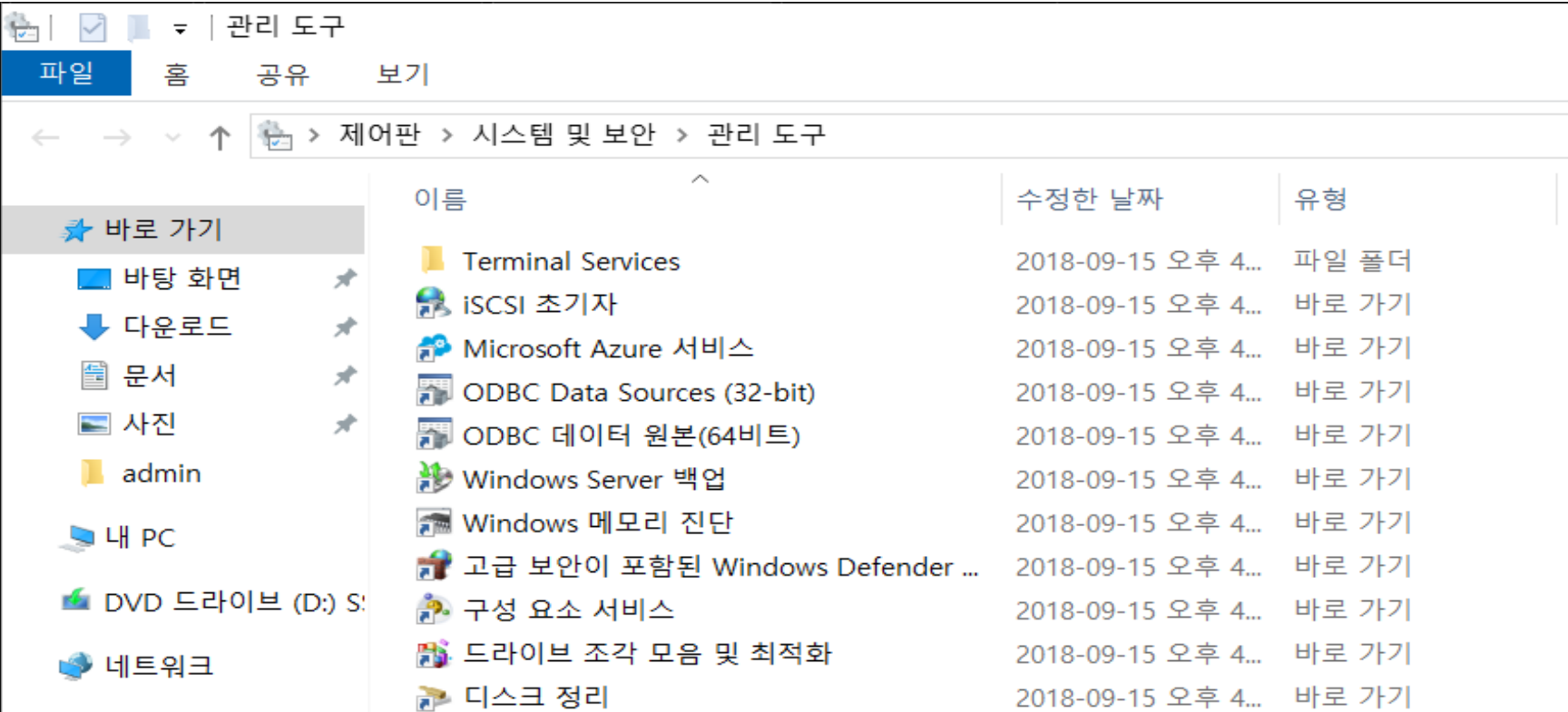
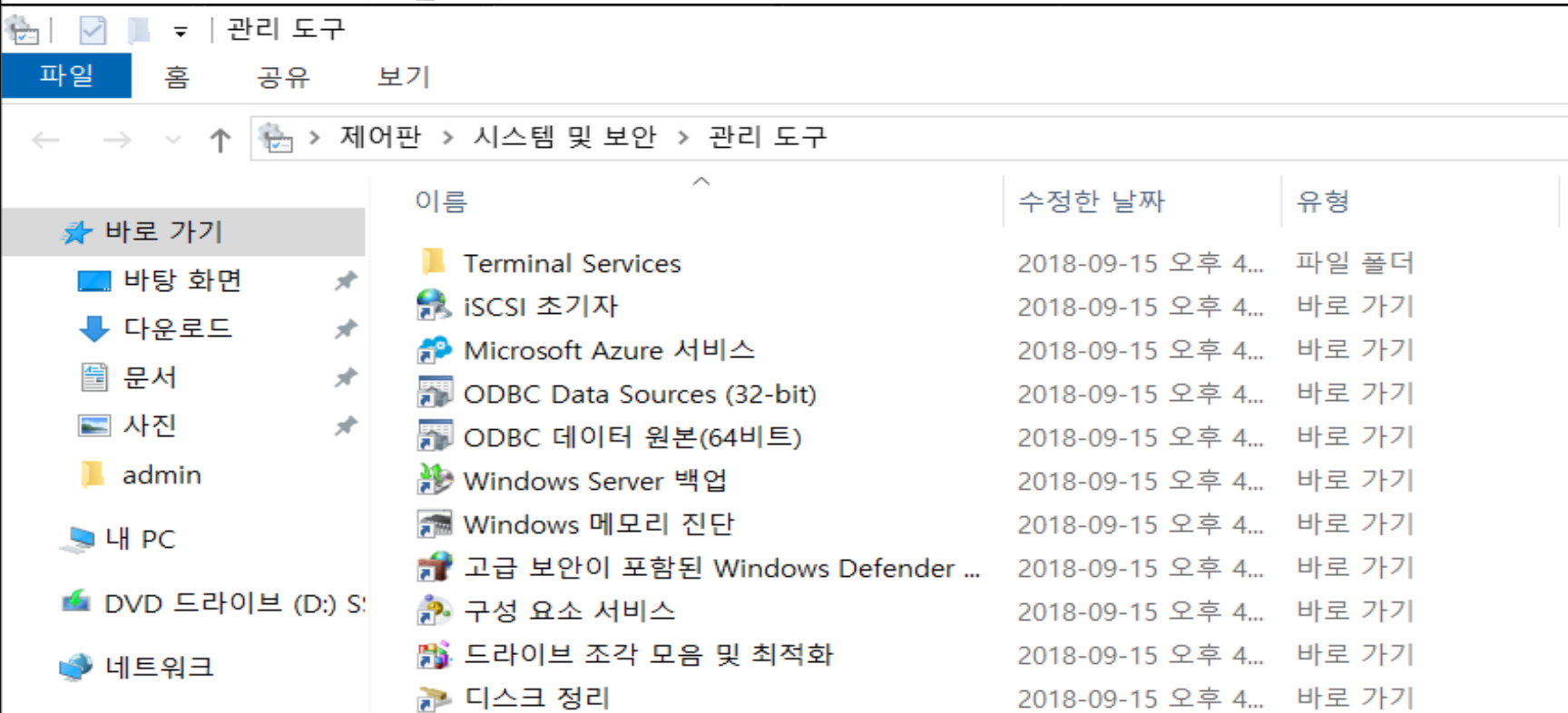
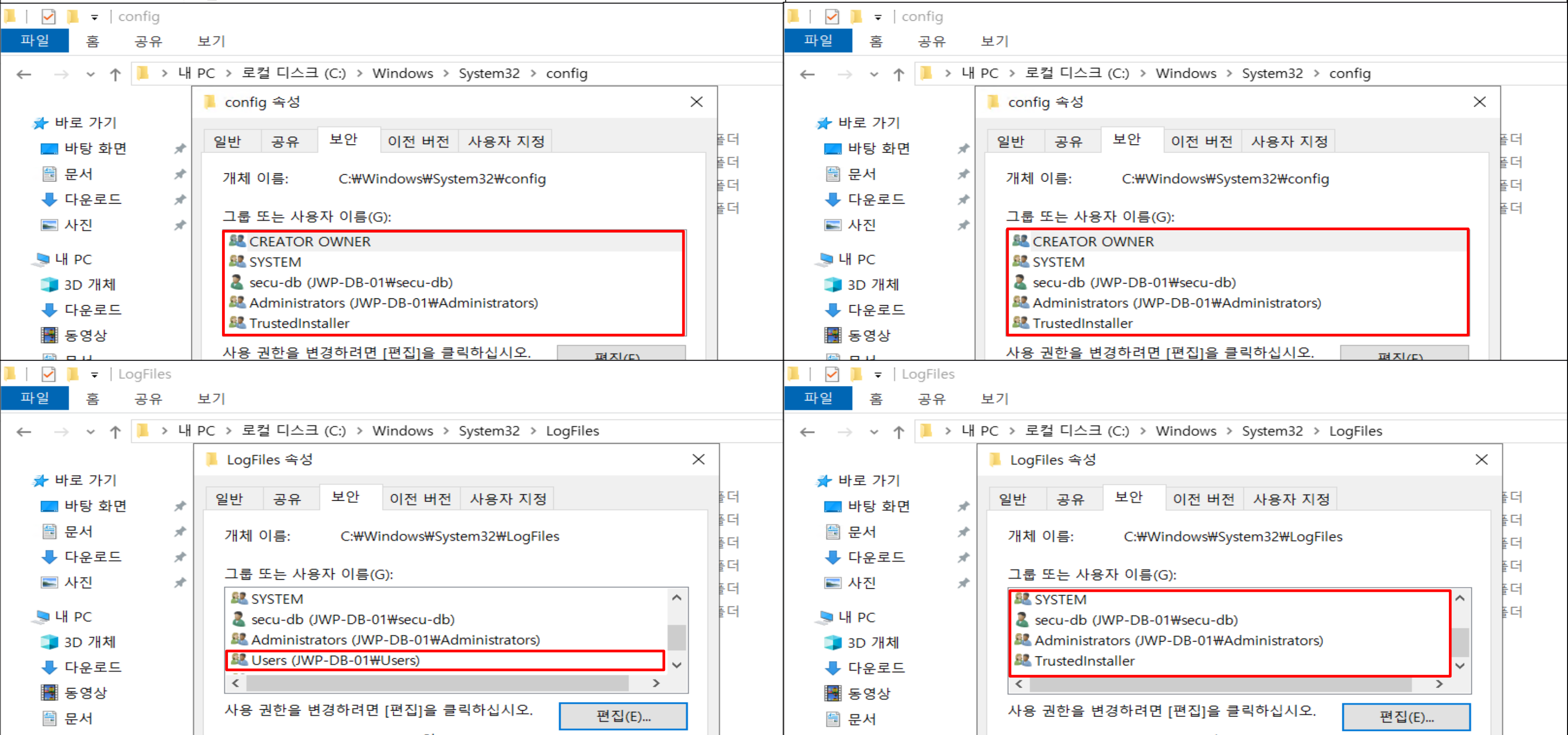
영역별점수	점수	양호	취약	N/A
100.0%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
100.0%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	N/A	0	0	1
100.0%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
100.0%	N/A	0	0	1
	100.0%	1	0	0
	100.0%	1	0	0
100.0%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
100.0%	100.0%	1	0	0
	100.0%	1	0	0
100.0%	100.0%	1	0	0
	100.0%	1	0	0
	100.0%	1	0	0
	N/A	0	0	1
	100.0%	1	0	0
	N/A	0	0	1
100.0%	100.0%	1	0	0
	100.0%	1	0	0
100.0%	100.0%	1	0	0

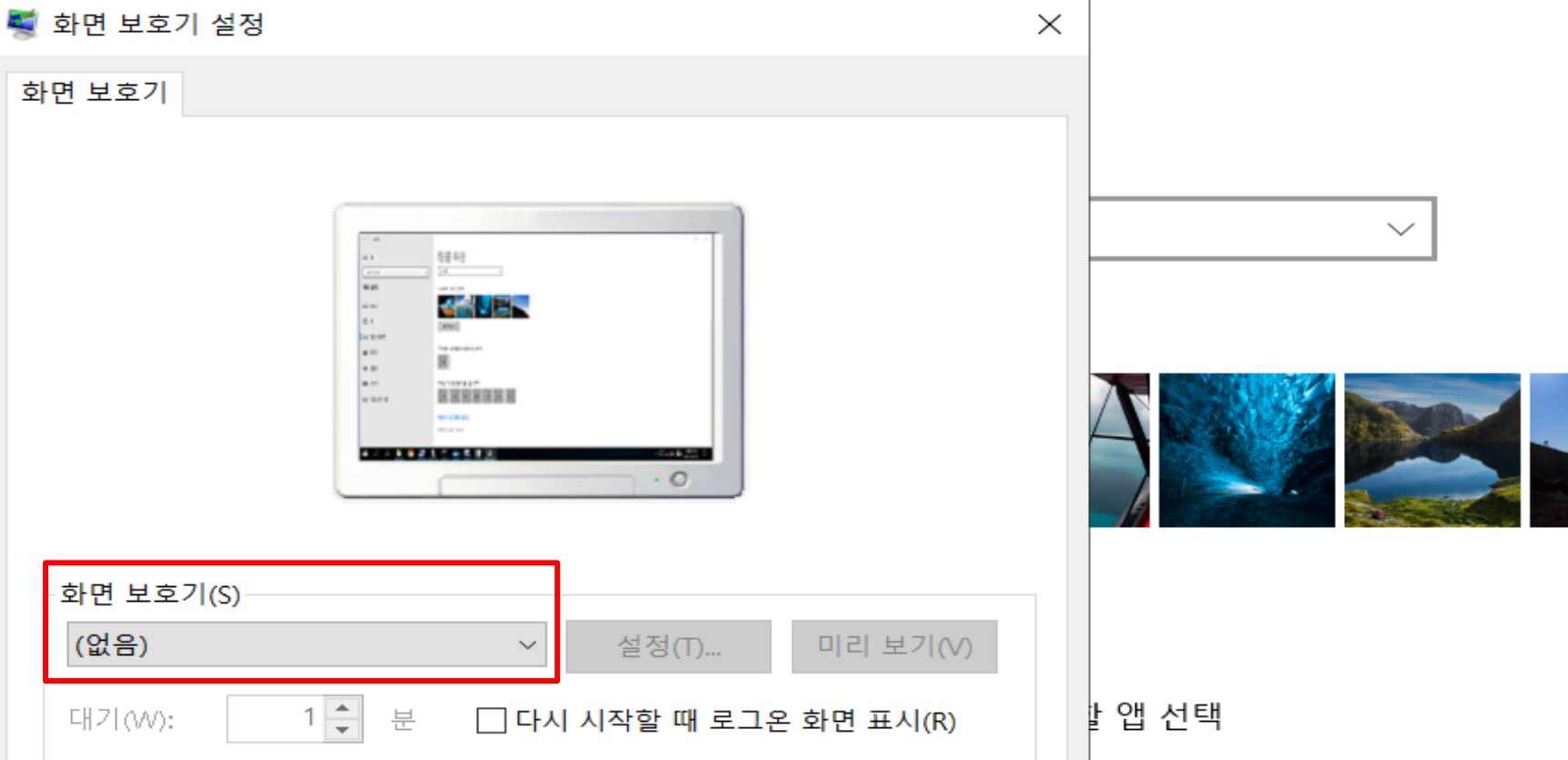
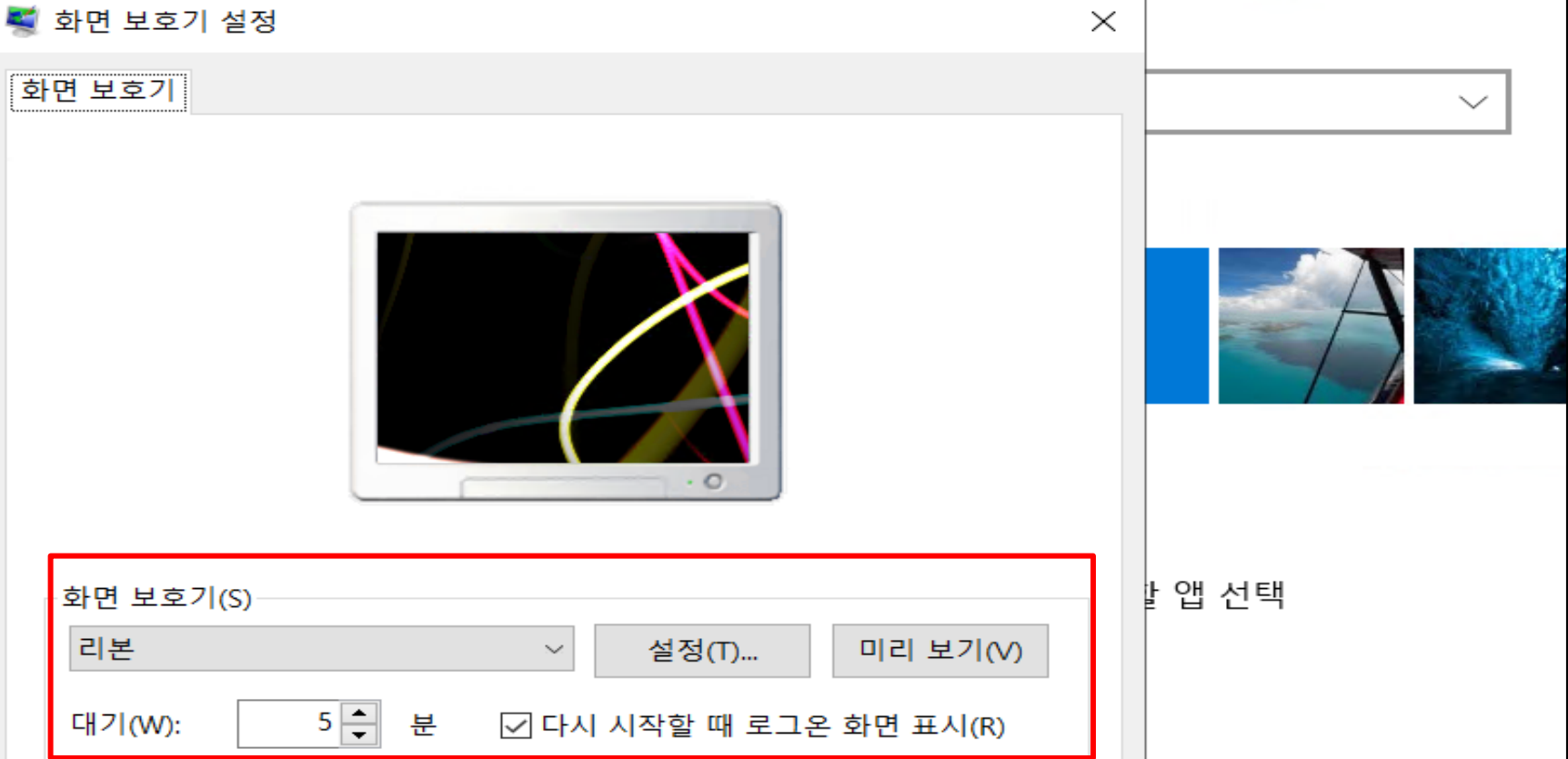
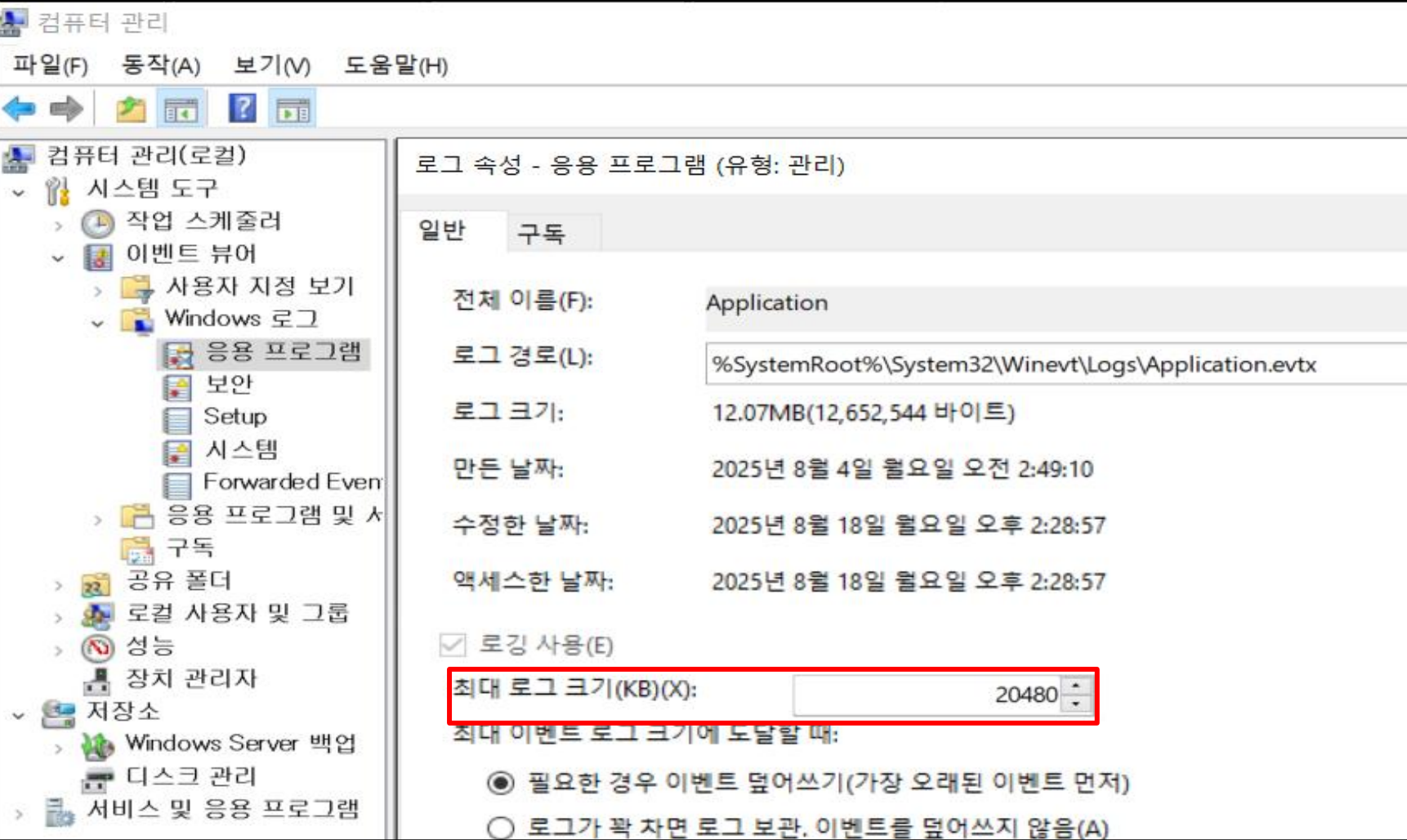
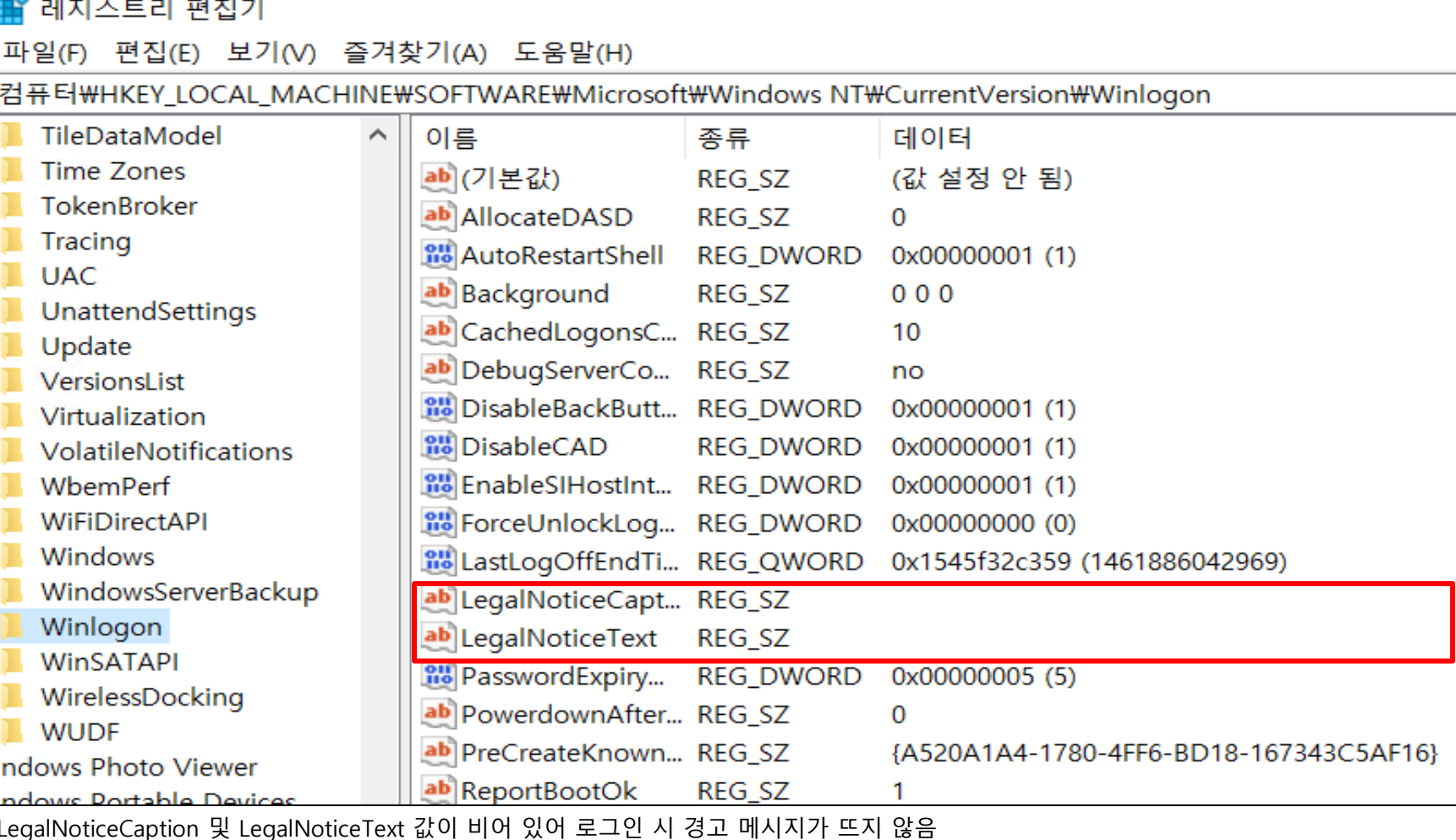
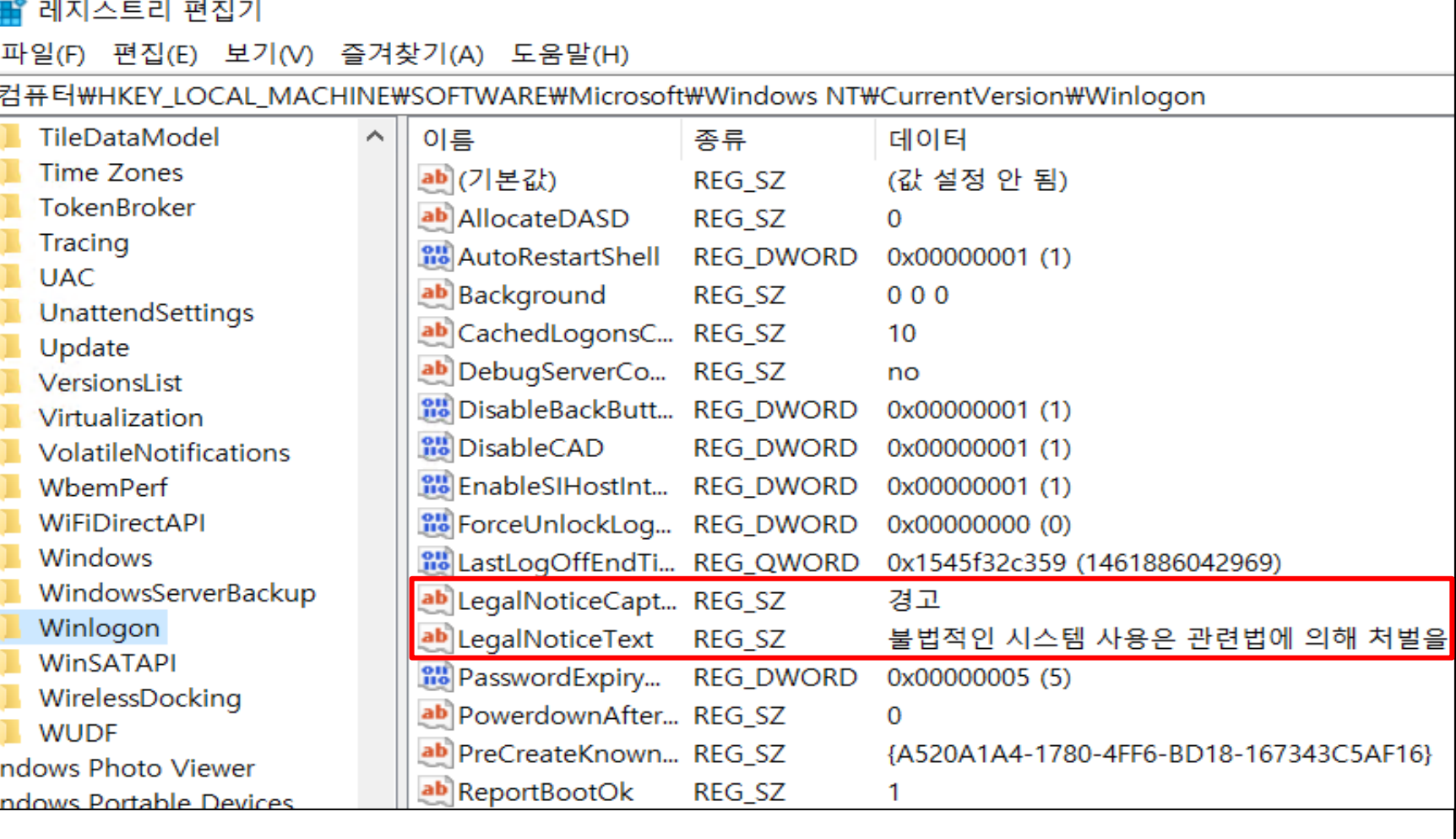
Windows 취약점 진단 상세결과(47항목)

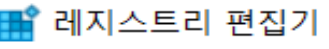
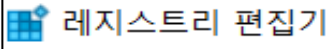
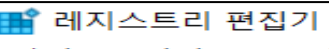
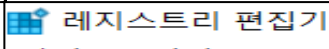
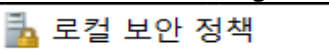
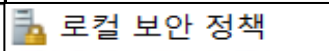
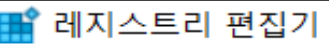
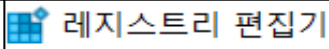
진단항목	No.	세부 진단항목	진단기준	1	jwp-db-01	jwp-db-01
					10.0.8.8	10.0.8.8
					DB OS	DB OS
1. 계정관리	1	로컬 계정 사용 설정	양호 - Administrators그룹에 관리자 계정인 Administrator의 이름을 바꾸어 사용하는 경우 Guest 계정 비활성화되어 있는 경우 / 불필요한 계정이 존재하지 않을 경우 취약 - Administrators그룹에 관리자 계정인 Administrator가 존재하는 경우 Guest 계정 활성화되어 있는 경우 / 불필요한 계정이 존재할 경우	양호	 <p>Administrator 계정이 기본값(Administrator)으로 활성화되어 있음</p>	
	2	계정 잠금 정책 설정	양호 - 계정 잠금 기간 30분, 계정 잠금 기간 원래 대로 설정 30분, 계정 잠금 임계 값 1 이상 5 이하 인 경우 취약 - 계정 잠금 기간 및 잠금 기간 원래대로 설정 기간이 30분 보다 작거나, 계정 잠금 임계 값 설정이 없거나 5보다 큰 경우	양호	 <p>계정 잠금 기간(10분)이 권고 기준인 30분보다 짧고, 계정 잠금 임계값(10회)이 권고 기준 5회보다 많음</p>	
	3	암호 정책 설정	양호 - 진단 방법의 기준을 모두 만족하는 경우 취약 - 진단 방법의 기준을 하나라도 만족하지 않는 경우	양호	 <p>최근 암호 기억, 최소 암호 길이, 최소 암호 사용 기간이 모두 0으로 설정되어 있어, 암호 정책이 적절히 적용되지 않음</p>	
	4	취약한 패스워드 점검	양호 - 계정과 유사하지 않은 8자 이상의 영문/숫자/특수문자의 조합으로 암호가 설정된 경우 취약 - 계정과 유사하지 않은 8자 이상의 영문/숫자/특수문자의 조합으로 암호가 설정되지 않은 경우	양호	담당자와 인터뷰 결과 계정과 유사한 패스워드로 확인	패스워드 정책 수립 (담당자 협의 완료) 1. 패스워드는 영문, 숫자, 특수문자를 조합하여 10자 이상으로 설정 2. 전화번호, 생년월일, 계정명 등 추측 또는 유추하기 쉬운 패스워드 사용 금지 3. 연속되거나 동일한 문자 및 숫자 사용 금지 4. 위 사항을 모두 충족해야 함
	5	사용자 계정 컨트롤(User Account Control) 설정	양호 - 사용자 계정 컨트롤(UAC)을 사용하는 경우 취약 - 사용자 계정 컨트롤(UAC)을 사용하지 않는 경우	양호		

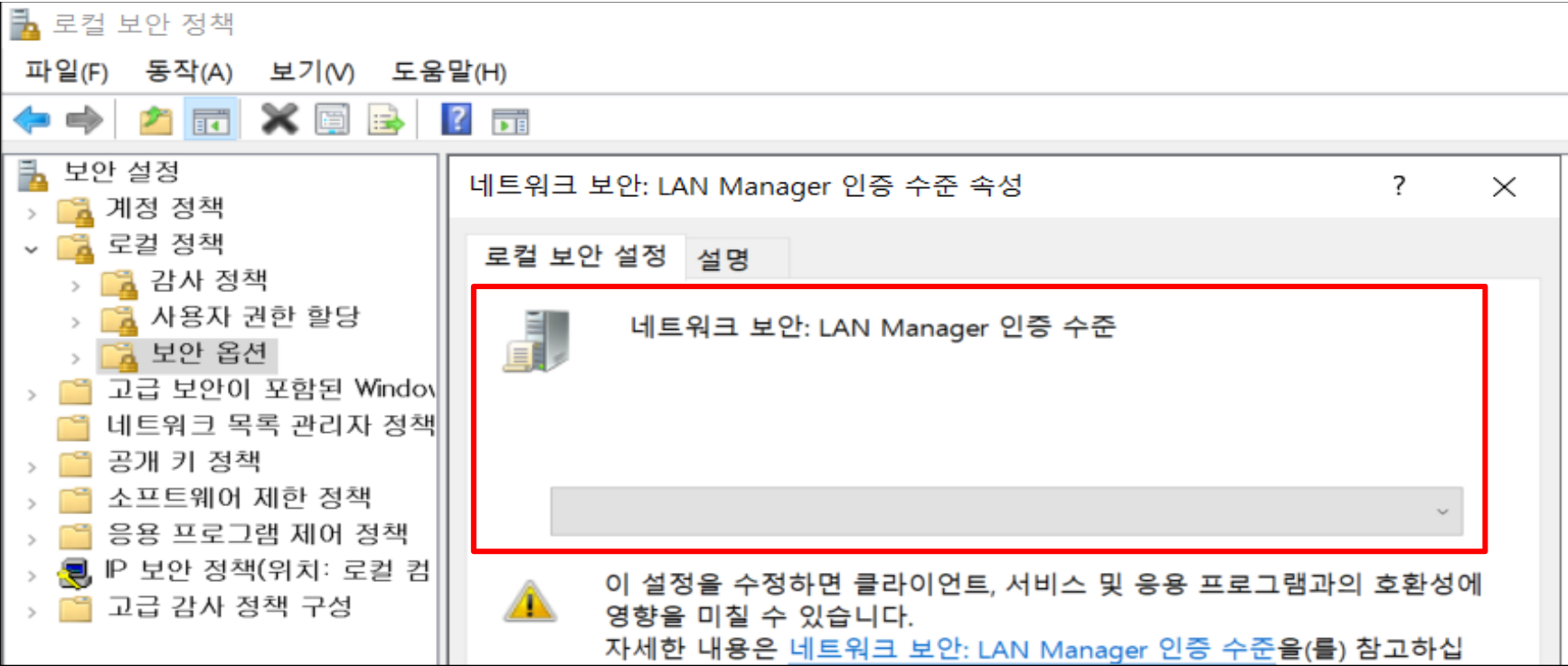
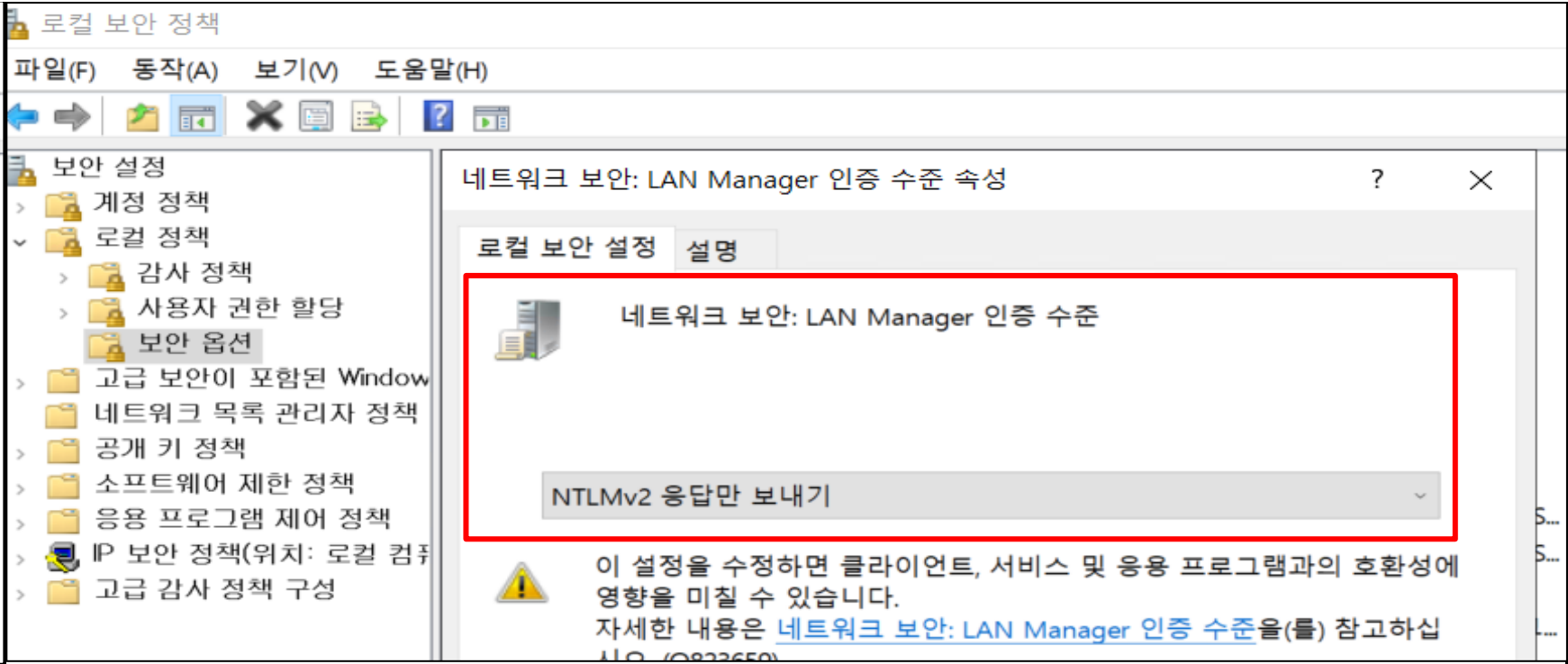
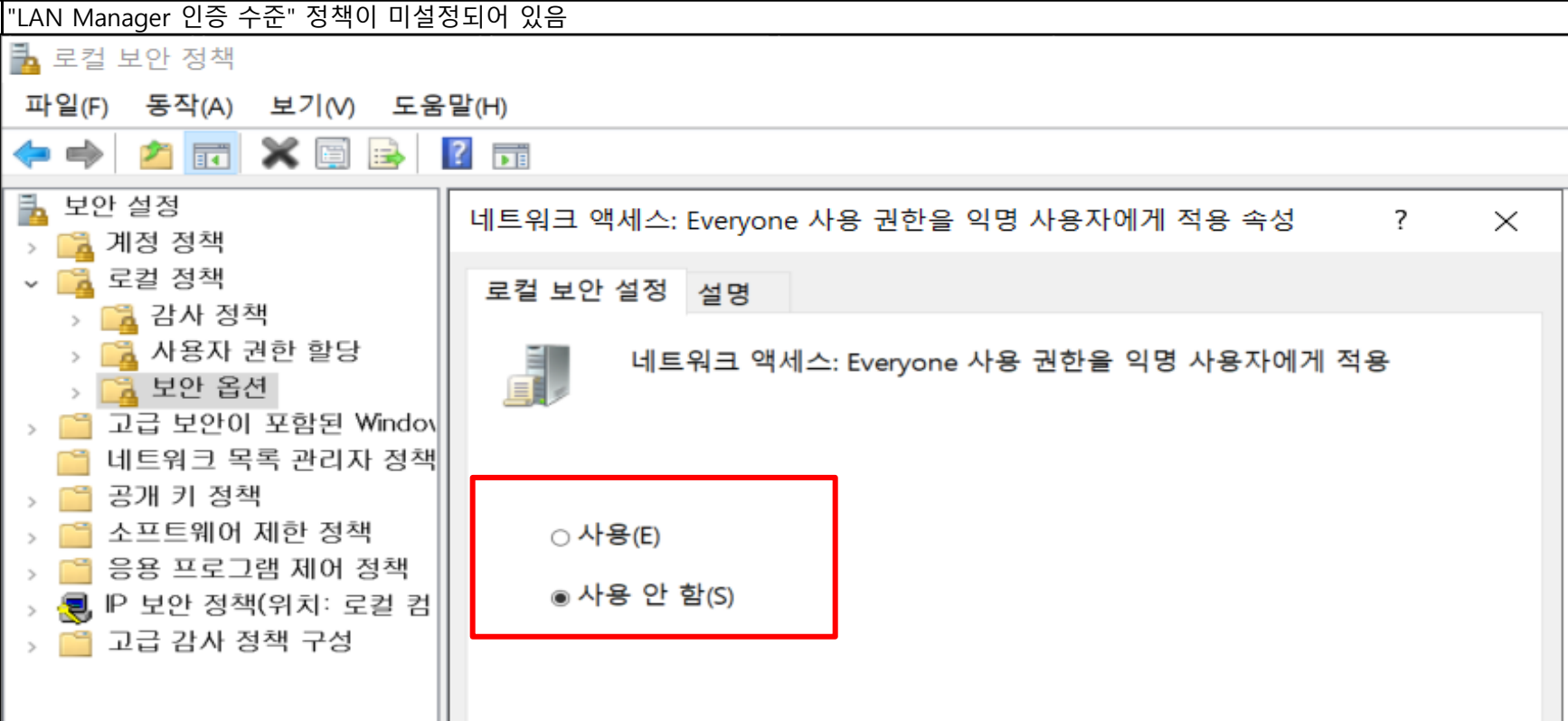
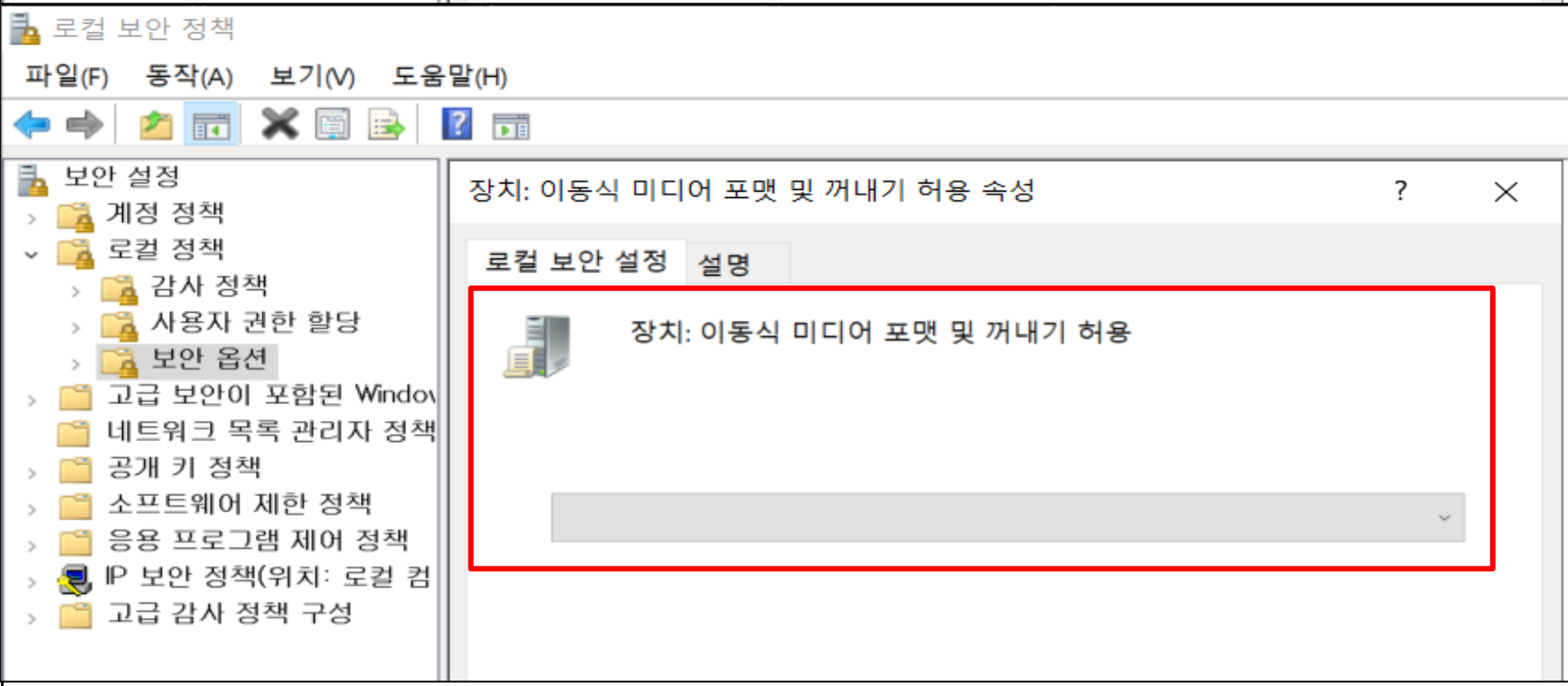
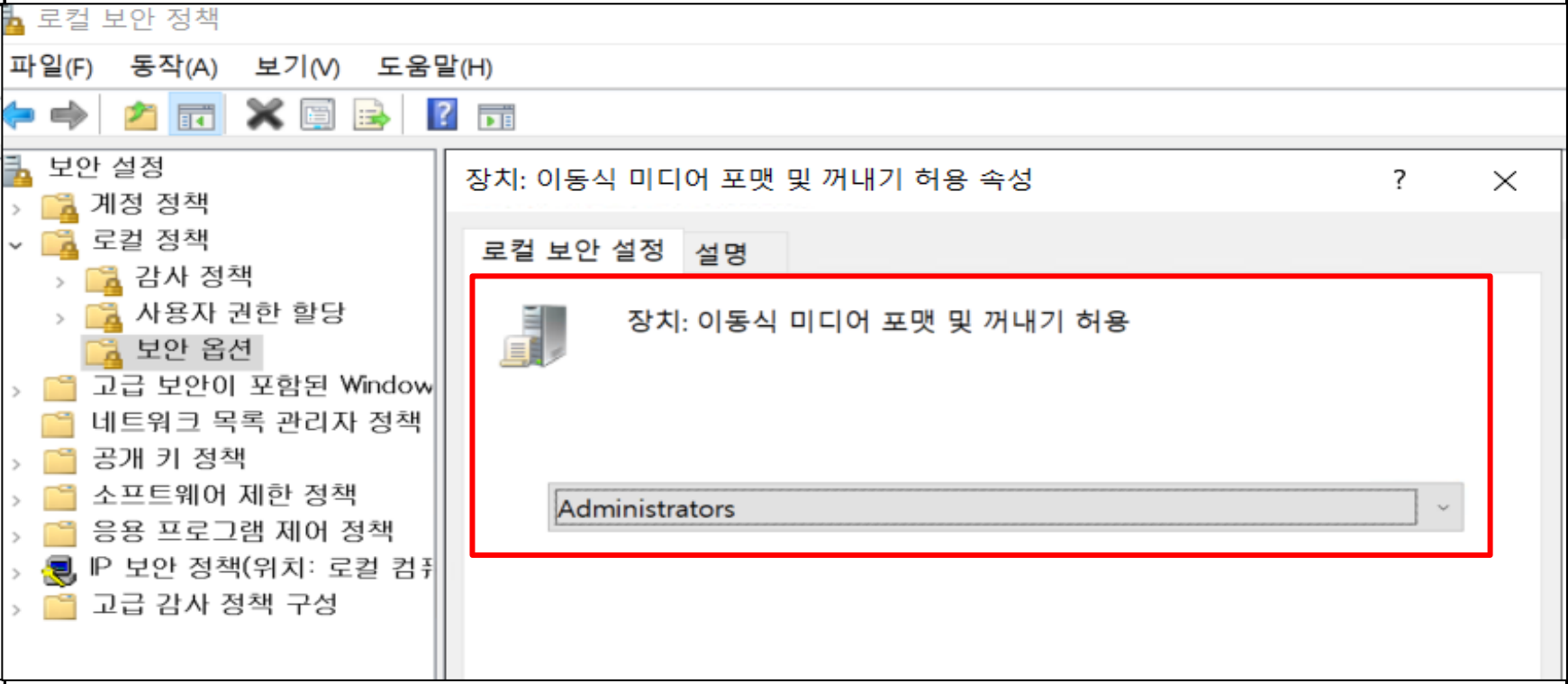
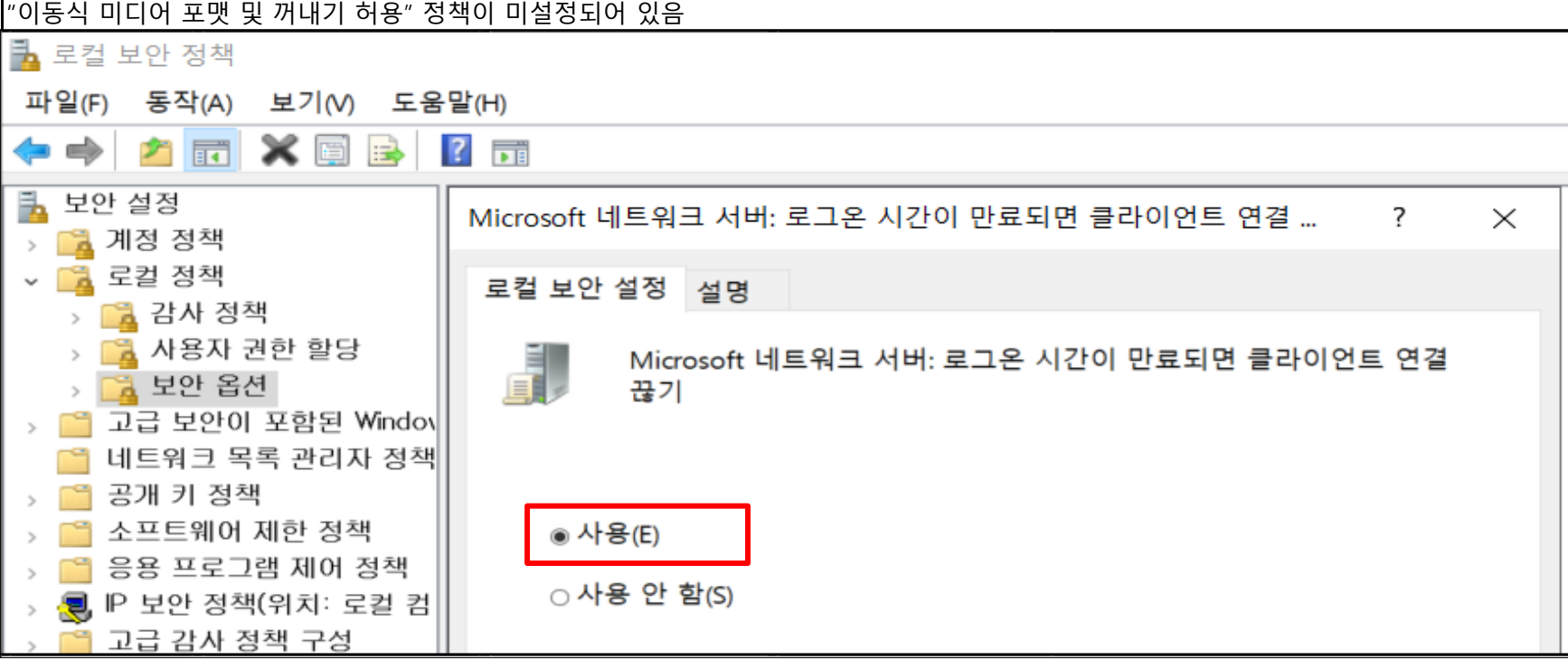
	6	익명 SID/이름 변환 허용 정책	양호 - "익명 SID/이름 변환 허용" 정책이 "사용 안 함"으로 설정되어 있는 경우 취약 - "익명 SID/이름 변환 허용" 정책이 "사용"으로 설정되어 있는 경우	양호		
	7	콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한 정책 점검	양호 - "콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용"으로 설정되어 있는 경우 취약 - "콘솔 로그인 시 로컬 계정에서 빈 암호 사용 제한" 정책이 "사용 안 함"으로 설정되어 있는 경우	양호		
	8	관리자 그룹에 최소한의 사용자 포함	양호 - Administrator 그룹 구성원을 1명 이하로 유지하거나, 불필요한 관리자 계정이 존재하지 않는 경우 취약 - Administrator 그룹 구성원에 불필요한 관리자 계정이 존재하는 경우	양호		
	1	CMD.EXE 파일 권한 설정	양호 - IIS 서비스가 실행 중이 아니거나, Administrator와 System, TrustedInstaller만 실행 권한이 설정되어 있을 경우 취약 - IIS가 실행 중이면서, Administrator와 System, TrustedInstaller 이 외에도 실행 권한이 설정되어 있을 경우	양호		

2. 파일 시스템	2	사용자 홈 디렉터리 접근 제한	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	양호		
	3	공유 폴더 설정	양호 - 기본 공유 디렉터리가 없거나 공유 디렉터리 접근 권한에 Everyone이 없을 경우 해당 레지스트리 AutoShareServer 값이 0, 암호 보호 공유가 설정되어 있는 경우 취약 - 기본 공유 디렉터리의 접근 권한에 Everyone이 있거나 암호 보호 공유가 해제되어 있는 경우	양호		
	4	SAM(Security Account Manager) 파일 권한 설정	양호 - SAM 파일 접근 권한이 Administrator, System 그룹만 모든 권한으로 등록되어 있는 경우 취약 - SAM 파일에 Administrator, System 그룹 외 다른 그룹에 권한이 설정되어 있을 경우	양호		
	5	파일 및 디렉터리 보호	※ 해당 OS는 체크리스트에 포함하지 않음.	N/A		

4. 주요 응용 설정	2	DNS(Domain Name Service) 보안 설정	양호 - DNS 서비스를 사용하지 않거나, 사용 시 영역 전송이 "특정 서버로만" 설정되어 있을 경우 취약 - DNS 서비스를 사용하고 영역 전송이 "특정 서버로만" 설정되어 있지 않을 경우	양호		
	3	SNMP(Simple Network Management Protocol) 서비스 보안 설정	양호 - SNMP 서비스를 사용하지 않거나 Community 스트링이 public, private이 아닐 경우 (SNMP Brute Force Attack 또는 SNMP Dictionary Attack이 가능하므로 반드시 8자리 이상의 자릿수와 숫자, 기호를 혼합하여 강력한 패스워드 형식으로 설정) 취약 - SNMP 서비스를 사용하고 Community 스트링이 public, private 인 경우	양호		
	1	원격 로그파일 접근 진단	양호 - 해당 디렉터리의 접근 권한에 Users / Everyone 그룹이 없는 경우 취약 - 해당 디렉터리의 접근 권한에 Users / Everyone 그룹이 있는 경우	양호	 애플리케이션 로그 파일에 Users 그룹이 포함되어 있음	



	2	화면 보호기 설정	양호 - 화면보호기를 설정하고, 암호를 사용하며, 대기 시간이 5분일 경우 취약 - 화면보호기가 설정되어 있지 않거나, 암호를 사용하지 않거나, 대기시간이 5분 초과 일 경우	양호		취약	
	3	이벤트 뷰어 설정	양호 - 최대 로그 크기 10240KB 이상이고 "필요한 경우 이벤트 덮어쓰기" 설정되어 있는 경우 취약 - 최대 로그 크기 10240KB 미만이고 "필요한 경우 이벤트 덮어쓰기" 설정되지 않은 경우	양호			
	4	로그인 시 경고 메시지 표시 설정	양호 - 로그인 시 경고 메시지가 뜨는 경우 취약 - 로그인 시 경고 메시지가 뜨지 않을 경우	양호		취약	
					LegalNoticeCaption 및 LegalNoticeText 값이 비어 있어 로그인 시 경고 메시지가 뜨지 않음		

5. 시스템 보안 설정	5	마지막 로그인 사용자 계정 숨김	양호 - "DontDisplayLastUserName"이 "1"로 설정되어 있을 경우 취약 - "DontDisplayLastUserName"이 "1"로 설정되어 있지 않을 경우	양호	 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System System 이름 이름 종류 데이터 (기본값) REG_SZ (값 설정 안 됨) ConsentPrompt... REG_DWORD 0x00000005 (5) ConsentPrompt... REG_DWORD 0x00000003 (3) DelayedDesktop... REG_DWORD 0x00000000 (0) DisableAutomati... REG_DWORD 0x00000001 (1) disablecad REG_DWORD 0x00000000 (0) dontdisplaylastu... REG_DWORD 0x00000000 (0) DSCAutomation... REG_DWORD 0x00000002 (2) EnableCursorSu... REG_DWORD 0x00000001 (1) EnableFullTrustS... REG_DWORD 0x00000002 (2) RunOnce 레지스트리 DontDisplayLastUserName 값이 0으로 설정되어 있음	 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System System 이름 이름 종류 데이터 (기본값) REG_SZ (값 설정 안 됨) ConsentPrompt... REG_DWORD 0x00000005 (5) ConsentPrompt... REG_DWORD 0x00000003 (3) DelayedDesktop... REG_DWORD 0x00000000 (0) DisableAutomati... REG_DWORD 0x00000001 (1) disablecad REG_DWORD 0x00000000 (0) dontdisplaylastu... REG_DWORD 0x00000001 (1) DSCAutomation... REG_DWORD 0x00000002 (2) EnableCursorSu... REG_DWORD 0x00000001 (1) EnableFullTrustS... REG_DWORD 0x00000002 (2) RunOnce
	6	로그온 하지 않은 사용자 시스템 종료 방지	양호 - "ShutdownWithoutLogon"이 "0"으로 설정되어 있을 경우 취약 - "ShutdownWithoutLogon"이 "1"으로 설정되어 있을 경우	양호	 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System System 이름 이름 종류 데이터 (기본값) REG_SZ (값 설정 안 됨) ConsentPrompt... REG_DWORD 0x00000005 (5) ConsentPrompt... REG_DWORD 0x00000003 (3) DelayedDesktop... REG_DWORD 0x00000000 (0) DisableAutomati... REG_DWORD 0x00000001 (1) disablecad REG_DWORD 0x00000000 (0) dontdisplaylastu... REG_DWORD 0x00000000 (0) DSCAutomation... REG_DWORD 0x00000002 (2) EnableCursorSu... REG_DWORD 0x00000001 (1) EnableFullTrustS... REG_DWORD 0x00000002 (2) EnableInstallerD... REG_DWORD 0x00000001 (1) EnableLUA REG_DWORD 0x00000001 (1) EnableSecureUI... REG_DWORD 0x00000001 (1) EnableUIAdesk... REG_DWORD 0x00000000 (0) EnableUwpStart... REG_DWORD 0x00000002 (2) EnableVirtualiza... REG_DWORD 0x00000001 (1) legalnoticecapti... REG_SZ legalnoticetext REG_SZ PromptOnSecur... REG_DWORD 0x00000001 (1) scforceoption REG_DWORD 0x00000000 (0) shutdownwitho... REG_DWORD 0x00000001 (1) SupportFullTrust... REG_DWORD 0x00000001 (1) SupportUwpStar... REG_DWORD 0x00000001 (1) undockwithoutl... REG_DWORD 0x00000001 (1) ValidateAdminC... REG_DWORD 0x00000000 (0) ShutdownWithoutLogon 값이 1로 설정되어 있음	 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System System 이름 이름 종류 데이터 (기본값) REG_SZ (값 설정 안 됨) ConsentPrompt... REG_DWORD 0x00000005 (5) ConsentPrompt... REG_DWORD 0x00000003 (3) DelayedDesktop... REG_DWORD 0x00000000 (0) DisableAutomati... REG_DWORD 0x00000001 (1) disablecad REG_DWORD 0x00000000 (0) dontdisplaylastu... REG_DWORD 0x00000001 (1) DSCAutomation... REG_DWORD 0x00000002 (2) EnableCursorSu... REG_DWORD 0x00000001 (1) EnableFullTrustS... REG_DWORD 0x00000002 (2) EnableInstallerD... REG_DWORD 0x00000001 (1) EnableLUA REG_DWORD 0x00000001 (1) EnableSecureUI... REG_DWORD 0x00000001 (1) EnableUIAdesk... REG_DWORD 0x00000000 (0) EnableUwpStart... REG_DWORD 0x00000002 (2) EnableVirtualiza... REG_DWORD 0x00000001 (1) legalnoticecapti... REG_SZ legalnoticetext REG_SZ PromptOnSecur... REG_DWORD 0x00000001 (1) scforceoption REG_DWORD 0x00000000 (0) shutdownwitho... REG_DWORD 0x00000000 (0) SupportFullTrust... REG_DWORD 0x00000001 (1) SupportUwpStar... REG_DWORD 0x00000001 (1) undockwithoutl... REG_DWORD 0x00000001 (1) ValidateAdminC... REG_DWORD 0x00000000 (0) SMI
	7	로컬 감사 정책 설정	양호 - 상기 이벤트 감사 항목에 대해서는 반드시 "성공\실패" 감사 설정이 되어있는 경우 취약 - 상기 이벤트 감사 항목에 "성공\실패" 설정이 되어있지 않은 경우	양호	 파일(F) 동작(A) 보기(V) 도움말(H) 보안 설정 계정 정책 로컬 정책 감사 정책 사용자 권한 할당 보안 옵션 고급 보안이 포함된 Window 네트워크 목록 관리자 정책 공개 키 정책 소프트웨어 제한 정책 응용 프로그램 제어 정책 IP 보안 정책(위치: 로컬 컴 고급 감사 정책 구성 정책 개체 액세스 감사 계정 관리 감사 계정 로그인 이벤트 감사 권한 사용 감사 디렉터리 서비스 액세스 감사 로그온 이벤트 감사 시스템 이벤트 감사 정책 변경 감사 프로세스 추적 감사 보안 설정 감사 안 함 감사 안 함 감사 안 함 감사 안 함 감사 안 함 감사 안 함 감사 안 함 감사 안 함 감사 안 함 개체 액세스 감사, 계정 관리 감사, 계정 로그인 이벤트 감사, 권한 사용 감사, 로그인 이벤트 감사 항목에 대해 '성공' 및 '실패' 이벤트에 대한 감사가 설정이 되어 있지 않음	 파일(F) 동작(A) 보기(V) 도움말(H) 보안 설정 계정 정책 로컬 정책 감사 정책 사용자 권한 할당 보안 옵션 고급 보안이 포함된 Window 네트워크 목록 관리자 정책 공개 키 정책 소프트웨어 제한 정책 응용 프로그램 제어 정책 IP 보안 정책(위치: 로컬 컴 고급 감사 정책 구성 정책 개체 액세스 감사 계정 관리 감사 계정 로그인 이벤트 감사 권한 사용 감사 디렉터리 서비스 액세스 감사 로그온 이벤트 감사 시스템 이벤트 감사 정책 변경 감사 프로세스 추적 감사 보안 설정 성공, 실패 성공, 실패 성공, 실패 성공, 실패 감사 안 함 감사 안 함 감사 안 함 감사 안 함 감사 안 함 감사 안 함
	8	가상 메모리 페이지 파일 삭제 설정	양호 - "ClearPageFileAtShutdown"이 "1"로 설정되어 있을 경우 취약 - "ClearPageFileAtShutdown"이 "1"로 설정되어 있지 않을 경우	양호	 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management Memory Management 이름 이름 종류 데이터 (기본값) REG_SZ (값 설정 안 됨) ClearPageFileAt... REG_DWORD 0x00000000 (0) da56a5e4-287c-... REG_DWORD 0x00000004 (4) DisablePagingEx... REG_DWORD 0x00000000 (0) ExistingPageFiles REG_MULTI... \\??\C:\pagefile.sys FeatureSettings REG_DWORD 0x00000001 (1) ClearPageFileAtShutdown 값이 0으로 설정되어 있음	 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management Memory Management 이름 이름 종류 데이터 (기본값) REG_SZ (값 설정 안 됨) ClearPageFileAt... REG_DWORD 0x00000001 (1) da56a5e4-287c-... REG_DWORD 0x00000004 (4) DisablePagingEx... REG_DWORD 0x00000000 (0) ExistingPageFiles REG_MULTI... \\??\C:\pagefile.sys FeatureSettings REG_DWORD 0x00000001 (1)

	9	Lan Manager 인증 수준	양호 - "LAN Manager 인증 수준" 정책이 "NTLMv2 응답만 보냄"으로 설정되어 있을 경우 취약 - "LAN Manager 인증 수준" 정책이 "LM" 및 "NTLM"으로 설정되어 있을 경우	양호		
	10	Everyone 사용 권한을 익명 사용자에게 적용 안함	양호 - "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용 안 함"으로 설정되어 있을 경우 취약 - "Everyone 사용 권한을 익명 사용자에게 적용" 정책이 "사용"으로 설정되어 있을 경우	양호		
	11	이동식 미디어 포맷 및 꺼내기 admin만 허용	양호 - "이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrators"로 되어 있을 경우 취약 - "이동식 미디어 포맷 및 꺼내기 허용" 정책이 "Administrators"로 되어 있지 않을 경우	양호		
			양호 - "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책을 "사용"으로 설정하고 "세션 연결을 중단하기 전에 필요한 유휴 시간" 정책이 "15분"으로 설정되어 있을 경우			

	12	세션 연결 끊기 전 유휴 시간 설정	양호	<div><div>15분 - 세션 연결을 끊기 전에 유휴 시간이 만료되면 클라이언트 연결 끊기" 정책이 "사용 안 함" 으로 설정되어 있거나 "세션 연결을 중단하기 전에 필요한 유휴 시간" 정책이 "15분"으로 설정되어 있지 않을 경우</div><div><div>로컬 보안 정책</div><div>파일(F) 동작(A) 보기(V) 도움말(H)</div><div><div>보안 설정</div><div>계정 정책</div><div>로컬 정책</div><div>감사 정책</div><div>사용자 권한 할당</div><div>보안 옵션</div><div>고급 보안이 포함된 Windows</div><div>네트워크 목록 관리자 정책</div><div>공개 키 정책</div><div>소프트웨어 제한 정책</div><div>응용 프로그램 제어 정책</div><div>IP 보안 정책(위치: 로컬 컴</div><div>고급 감사 정책 구성</div></div><div><div>Microsoft 네트워크 서버: 세션을 중단하기 전에 필요한 유휴 시간 속성</div><div>로컬 보안 설정 설명</div><div>Microsoft 네트워크 서버: 세션을 중단하기 전에 필요한 유휴 시간</div><div>유휴 시간이 초과하면 연결 끊기:</div><div>15 분</div></div></div></div> <tr><td>13</td><td>예약된 작업 의심스런 명령어나 파일 점검</td><td>양호</td><td><div><div>작업 스케줄러</div><div>파일(F) 동작(A) 보기(V) 도움말(H)</div><div><div>작업 스케줄러 (로컬)</div><div>작업 스케줄러 라이브러리</div></div><div><table><thead><tr><th>이름</th><th>상태</th><th>트리거</th><th>다음 실행 시간</th><th>마지막 실행 시간</th></tr></thead><tbody><tr><td>Amazon Ec2 ...</td><td>사용 안 함</td><td>시스템 시작 시</td><td></td><td>2025-08-11 오전 1</td></tr></tbody></table></div><div><div>일반</div><div>트리거</div><div>동작</div><div>조건</div><div>설정</div><div>기록(사용 안 함)</div></div><div><div>이름:</div><div>Amazon Ec2 Launch - Instance Initialization</div></div><div><div>위치:</div><div>\</div></div></div></td></tr>	13	예약된 작업 의심스런 명령어나 파일 점검	양호	<div><div>작업 스케줄러</div><div>파일(F) 동작(A) 보기(V) 도움말(H)</div><div><div>작업 스케줄러 (로컬)</div><div>작업 스케줄러 라이브러리</div></div><div><table><thead><tr><th>이름</th><th>상태</th><th>트리거</th><th>다음 실행 시간</th><th>마지막 실행 시간</th></tr></thead><tbody><tr><td>Amazon Ec2 ...</td><td>사용 안 함</td><td>시스템 시작 시</td><td></td><td>2025-08-11 오전 1</td></tr></tbody></table></div><div><div>일반</div><div>트리거</div><div>동작</div><div>조건</div><div>설정</div><div>기록(사용 안 함)</div></div><div><div>이름:</div><div>Amazon Ec2 Launch - Instance Initialization</div></div><div><div>위치:</div><div>\</div></div></div>	이름	상태	트리거	다음 실행 시간	마지막 실행 시간	Amazon Ec2 ...	사용 안 함	시스템 시작 시		2025-08-11 오전 1
	13	예약된 작업 의심스런 명령어나 파일 점검	양호	<div><div>작업 스케줄러</div><div>파일(F) 동작(A) 보기(V) 도움말(H)</div><div><div>작업 스케줄러 (로컬)</div><div>작업 스케줄러 라이브러리</div></div><div><table><thead><tr><th>이름</th><th>상태</th><th>트리거</th><th>다음 실행 시간</th><th>마지막 실행 시간</th></tr></thead><tbody><tr><td>Amazon Ec2 ...</td><td>사용 안 함</td><td>시스템 시작 시</td><td></td><td>2025-08-11 오전 1</td></tr></tbody></table></div><div><div>일반</div><div>트리거</div><div>동작</div><div>조건</div><div>설정</div><div>기록(사용 안 함)</div></div><div><div>이름:</div><div>Amazon Ec2 Launch - Instance Initialization</div></div><div><div>위치:</div><div>\</div></div></div>	이름	상태	트리거	다음 실행 시간	마지막 실행 시간	Amazon Ec2 ...	사용 안 함	시스템 시작 시		2025-08-11 오전 1				
이름	상태	트리거	다음 실행 시간	마지막 실행 시간														
Amazon Ec2 ...	사용 안 함	시스템 시작 시		2025-08-11 오전 1														

	15	보안 감사를 로그 할 수 없는 경우 즉시 시스템 종료 방지	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	양호	<div><div><div>로컬 보안 정책</div><div>파일(F) 동작(A) 보기(V) 도움말(H)</div><div><div>보안 설정</div><div>계정 정책</div><div>로컬 정책</div><div>감사 정책</div><div>사용자 권한 할당</div><div>보안 옵션</div><div>고급 보안이 포함된 Windows</div><div>네트워크 목록 관리자 정책</div><div>공개 키 정책</div><div>소프트웨어 제한 정책</div><div>응용 프로그램 제어 정책</div><div>IP 보안 정책(위치: 로컬 컴</div><div>고급 감사 정책 구성</div></div><div>감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 속성</div><div><div>로컬 보안 설정</div><div>설명</div><div>감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료</div><div><div><input type="radio"/> 사용(E)</div><div><input checked="" type="radio"/> 사용 안 함(S)</div></div><div><div>이 설정을 수정하면 클라이언트, 서비스 및 응용 프로그램과의 호환성에 영향을 미칠 수 있습니다.</div><div>자세한 내용은 감사: 보안 감사를 로그할 수 없는 경우 즉시 시스템 종</div><div>트을(들) 참고하십시오. (Q823659)</div></div></div></div></div>	
	16	보안 채널 데이터 디지털 암호화 또는 서명 설정	양호 - 보안 채널 데이터 디지털 암호화 또는 서명 정책이 모두 "사용"으로 되어 있는 경우 취약 - 보안 채널 데이터 디지털 암호화 또는 서명 정책이 모두 "사용 안 함"으로 되어 있는 경우	양호	<div><div><div>로컬 보안 정책</div><div>파일(F) 동작(A) 보기(V) 도움말(H)</div><div><div>보안 설정</div><div>계정 정책</div><div>로컬 정책</div><div>감사 정책</div><div>사용자 권한 할당</div><div>보안 옵션</div><div>고급 보안이 포함된 Windows</div><div>네트워크 목록 관리자 정책</div><div>공개 키 정책</div><div>소프트웨어 제한 정책</div><div>응용 프로그램 제어 정책</div></div><div><div>정책</div><div>대화형 로그인: 컴퓨터 계정 잠금 임계값</div><div>대화형 로그인: 컴퓨터 비활성 제한</div><div>도메인 구성원: 고급 세션 키 요청(Windows...</div><div>도메인 구성원: 보안 채널 데이터 디지털 서...</div><div>도메인 구성원: 보안 채널 데이터를 디지털 ...</div><div>도메인 구성원: 보안 채널 데이터를 디지털 ...</div><div>도메인 구성원: 컴퓨터 계정 암호 변경 사항...</div><div>도메인 구성원: 컴퓨터 계정 암호의 최대 사...</div><div>도메인 컨트롤러: LDAP 서버 서명 필요</div><div>보안 설정</div><div>정의되지 않음</div><div>정의되지 않음</div><div>사용</div><div>사용</div><div>사용</div><div>사용</div><div>사용 안 함</div><div>30 일</div><div>정의되지 않음</div></div></div></div>	
6. 바이러스 진단	1	백신 프로그램 설치	양호 - 바이러스 백신 프로그램이 설치되어 있는 경우 취약 - 바이러스 백신 프로그램이 설치되어 있지 않은 경우	양호	<div><div>Windows 보안</div><div>←</div><div>보안 한 눈에 보기</div><div>장치의 보안 및 상태를 확인하고 필요한 모든 작업을 수행하세요.</div><div><div><div>총</div><div>바이러스 및 위협 방지</div><div>방화벽 및 네트워크 보호</div><div>앱 및 브라우저 컨트롤</div><div>장치 보안</div></div><div><div><div>바이러스 및 위협 방지</div><div>추가 작업이 필요 없습니다.</div></div><div><div><div>방화벽 및 네트워크 보호</div><div>추가 작업이 필요 없습니다.</div></div><div><div><div>앱 및 브라우저 컨트롤</div><div>추가 작업이 필요 없습니다.</div></div><div><div><div>장치 보안</div><div>장치 보기 및 하드웨어 보안 기능 관리</div></div></div></div></div></div></div></div>	
	2	최신 엔진 업데이트	양호 - 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있을 경우 취약 - 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있지 않은 경우	양호	<div><div>Windows 업데이트</div><div>*일부 설정은 조직에서 관리합니다.</div><div>업데이트 구성 정책 보기</div><div><div>사용 가능한 업데이트 있음</div><div>마지막으로 확인한 날짜: 어제, 오후 11:55</div><div>장치에 중요한 보안 및 품질 수정이 누락되어 있습니다.</div><div>Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.435.104.0) - Current Channel (Broad)</div><div>상태: 보류 중인 설치</div></div></div>	<div><div>Windows 업데이트</div><div>*일부 설정은 조직에서 관리합니다.</div><div>업데이트 구성 정책 보기</div><div><div>현재 최신 상태입니다.</div><div>마지막으로 확인한 날짜: 2025-08-27, 오후 2:15</div><div>업데이트 확인</div><div>*조직에서 자동 업데이트를 켜습니다.</div></div></div>
	1	SAM(Security Account Manager) 보안 감사 설정	양호 - 해당 레지스트리 값에 Everyone에 대한 감사 설정이 되어 있을 경우 취약 - 해당 레지스트리 값에 Everyone에 대한 감사 설정이 되어 있지 않을 경우	양호	<div><div>레지스트리 편집기</div><div>파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)</div><div>컴퓨터\HKEY_LOCAL_MACHINE\SAM</div><div><div>컴퓨터</div><div>HKEY_CLASSES_ROOT</div><div>HKEY_CURRENT_USER</div><div>HKEY_LOCAL_MACHINE</div><div>BCD00000000</div><div>HARDWARE</div><div>SAM</div><div>SECURITY</div><div>SOFTWARE</div><div>SYSTEM</div><div>HKEY_USERS</div><div>HKEY_CURRENT_CONF</div></div><div><div>SAM 고급 보안 설정</div><div>소유자: Administrators (JWP-DB-01\Administrators) 변경(C)</div><div>사용 권한</div><div>감사</div><div>유효한 액세스</div><div>자세한 내용을 보려면 감사 항목을 두 번 클릭하세요. 감사 항목을 수정하려면 항목을</div><div>감사 항목:</div><div><div>유형</div><div>보안 주제</div><div>액세스</div></div></div></div>	<div><div>레지스트리 편집기</div><div>파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H)</div><div>컴퓨터\HKEY_LOCAL_MACHINE\SAM</div><div><div>컴퓨터</div><div>HKEY_CLASSES_ROOT</div><div>HKEY_CURRENT_USER</div><div>HKEY_LOCAL_MACHINE</div><div>BCD00000000</div><div>HARDWARE</div><div>SAM</div><div>SECURITY</div><div>SOFTWARE</div><div>SYSTEM</div><div>HKEY_USERS</div><div>HKEY_CURRENT_CONF</div></div><div><div>SAM 고급 보안 설정</div><div>소유자: Administrators (JWP-DB-01\Administrators) 변경(C)</div><div>사용 권한</div><div>감사</div><div>유효한 액세스</div><div>자세한 내용을 보려면 감사 항목을 두 번 클릭하세요. 감사 항목을 수정하려면 항목을</div><div>감사 항목:</div><div><div>유형</div><div>보안 주제</div><div>액세스</div><div>성공</div><div>Everyone</div><div>모든 권한</div></div></div></div>
					<div>SAM 고급 보안 설정에서 Everyone에 대한 감사가 설정되어 있지 않음</div>	

8. 보안패치				Windows 업데이트 *일부 설정은 조직에서 관리합니다. 업데이트 구성 정책 보기 <div> 사용 가능한 업데이트 있음 마지막으로 확인한 날짜: 어제, 오후 11:55</div> <div>장치에 중요한 보안 및 품질 수정이 누락되어 있습니다.</div> <div>Security Intelligence Update for Microsoft Defender Antivirus - KB2267602 (Version 1.435.104.0) - Current Channel (Broad) 상태: 보류 중인 설치 2025-07 Cumulative Update for .NET Framework 3.5, 4.7.2 and 4.8 for Windows Server 2019 for x64 (KB5062152) 상태: 보류 중인 설치 2025-07 Cumulative Update for Windows Server 2019 (1809) for x64-based Systems (KB5062557) 상태: 보류 중인 설치 Windows Malicious Software Removal Tool x64 - v5.134 (KB890830) 상태: 보류 중인 설치 2022-08 Security Update for Windows Server 2019 for x64-based Systems (KB5012170) 상태: 보류 중인 설치</div> <div>최신 HOT FIX가 설치되어 있지 않음</div>	
	2	최신 HOT FIX 적용	양호 - 최신 HOT FIX가 설치되어 있는 경우 취약 - 최신 HOT FIX가 설치되어 있지 않은 경우	양호	Windows 업데이트 *일부 설정은 조직에서 관리합니다. 업데이트 구성 정책 보기 <div> 현재 최신 상태입니다. 마지막으로 확인한 날짜: 2025-08-27, 오후 2:15</div> <div>업데이트 확인</div> <div>*조직에서 자동 업데이트를 켜습니다.</div> <div>사용 시간 변경 업데이트 기록 보기 고급 옵션</div>
9. 이슈 취약점	1	OpenSSL 취약점	양호 - OpenSSL을 사용하지 않거나 최신버전의 OpenSSL를 설치하여 운영하는 경우 취약 - 최신버전의 OpenSSL을 설치하여 운영하지 않는 경우	양호	<div>C:\Users\secu-db>openssl version</div> <div>'openssl' is not recognized as an internal or external command, operable program or batch file.</div> <div>C:\Users\secu-db>_</div>
점검결과				0.0	
	보안 적용율 (양호항목 / 진단항목) %			100.0%	