

| | |
|------|-------------------------|
| 문서번호 | J.W.P. MagicShop-250825 |
| 작성자 | 취약점진단팀 |
| 보안등급 | Confidential |
| Ver | ver 1.0 |

"J.W.P. MagicShop" 취약점 진단

DB OS 진단 상세결과

2025년 08월 25일

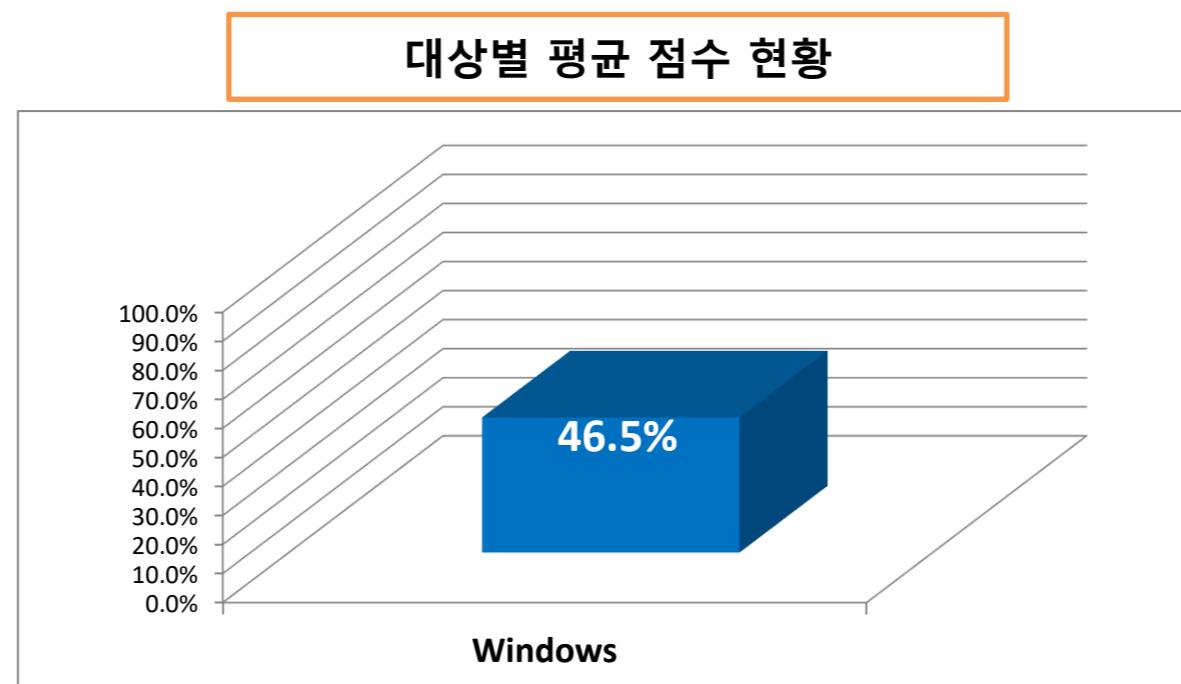


※ 진단 대상 리스트 - 서버 1대 (Windows 1대)

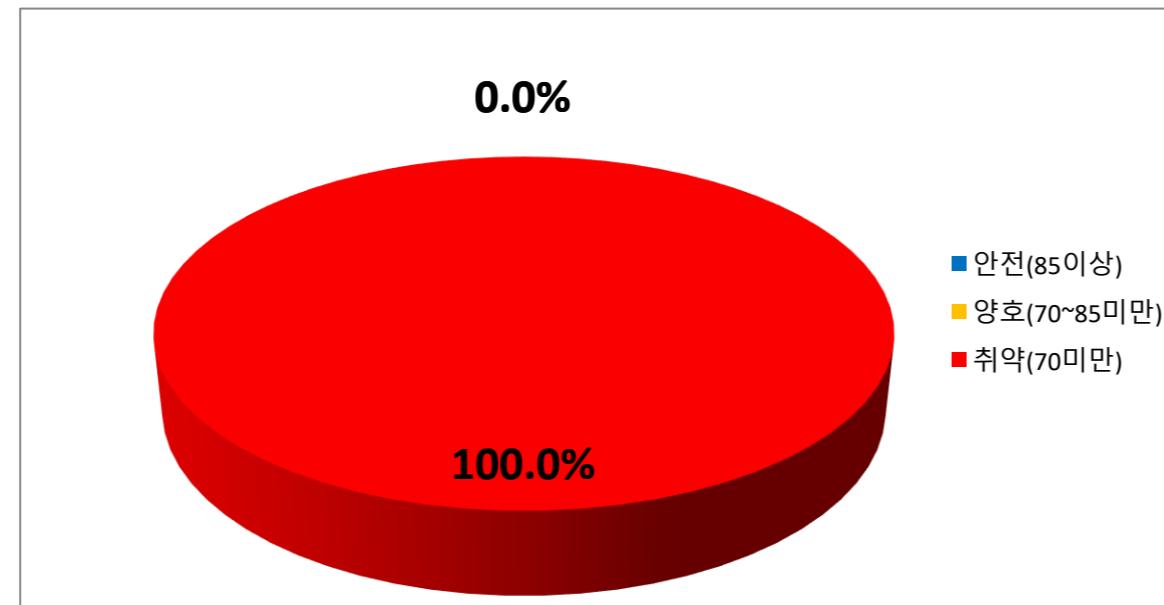
| 순번 | 진단 대상 | | | | 비고 |
|----------------|-----------|------------|---------------------|-------|----|
| | Hostname | IP Address | 버전정보 | 용도 | |
| Windows | | | | | |
| 1 | jwp-db-01 | 10.0.8.8 | Windows Server 2019 | DB OS | |

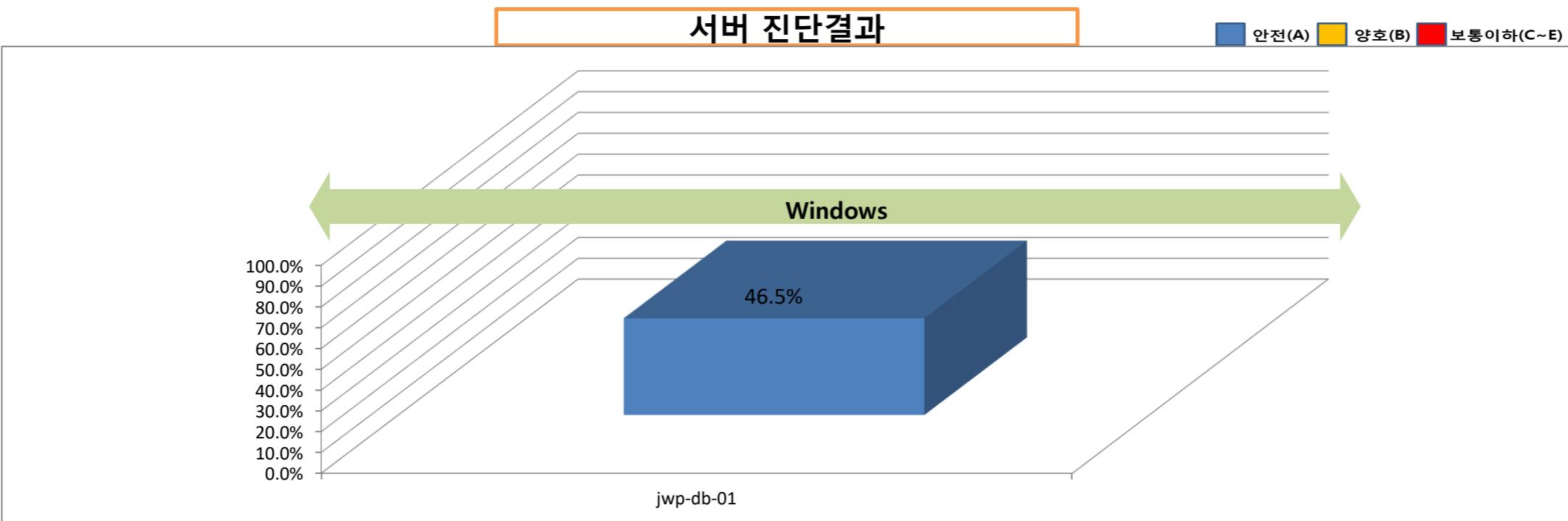
※ 대상별 평균 점수 그래프

| 진단 대상 | 평균 | 수량 |
|---------|-------|----|
| Windows | 46.5% | 1 |

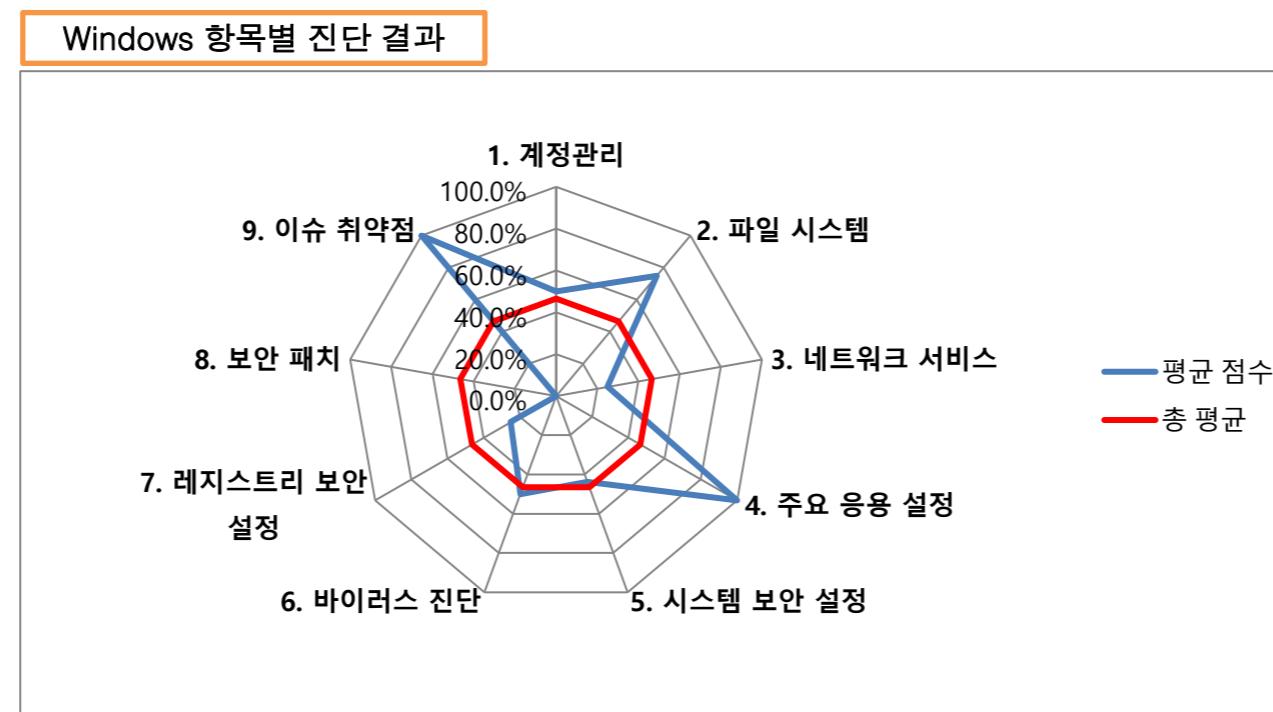


| | |
|-------------|--------|
| 전체 | 1 |
| 안전(85이상) | 0.0% |
| 양호(70~85미만) | 0.0% |
| 취약(70미만) | 100.0% |





| 진단 도메인 | 평균 점수 | 총 평균 |
|----------------|--------|-------|
| 1. 계정관리 | 50.0% | 46.5% |
| 2. 파일 시스템 | 75.0% | 46.5% |
| 3. 네트워크 서비스 | 25.0% | 46.5% |
| 4. 주요 응용 설정 | 100.0% | 46.5% |
| 5. 시스템 보안 설정 | 43.8% | 46.5% |
| 6. 바이러스 진단 | 50.0% | 46.5% |
| 7. 레지스트리 보안 설정 | 25.0% | 46.5% |
| 8. 보안 패치 | 0.0% | 46.5% |
| 9. 이슈 취약점 | 100.0% | 46.5% |

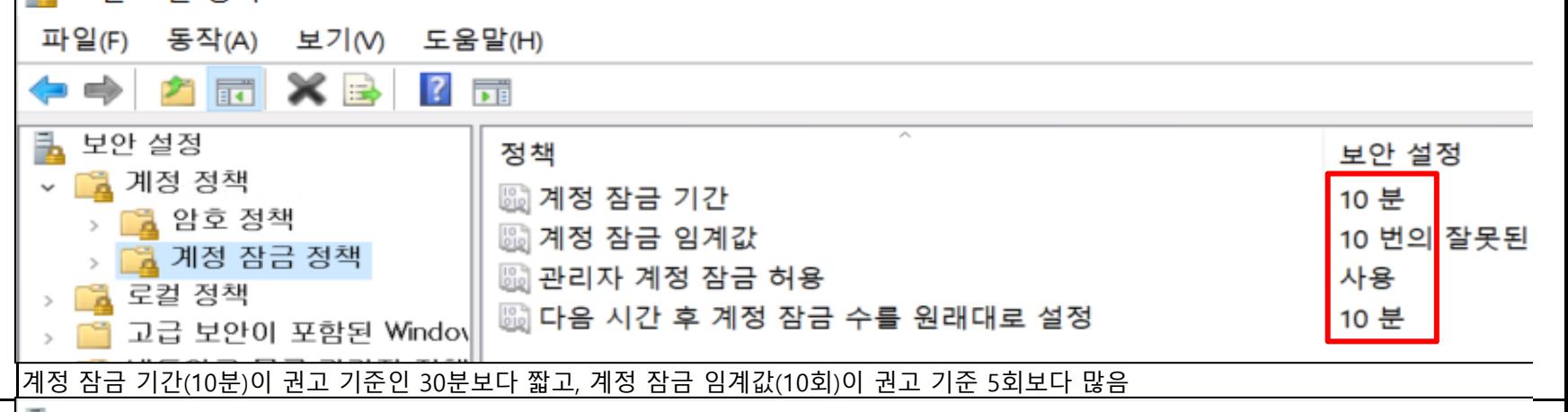
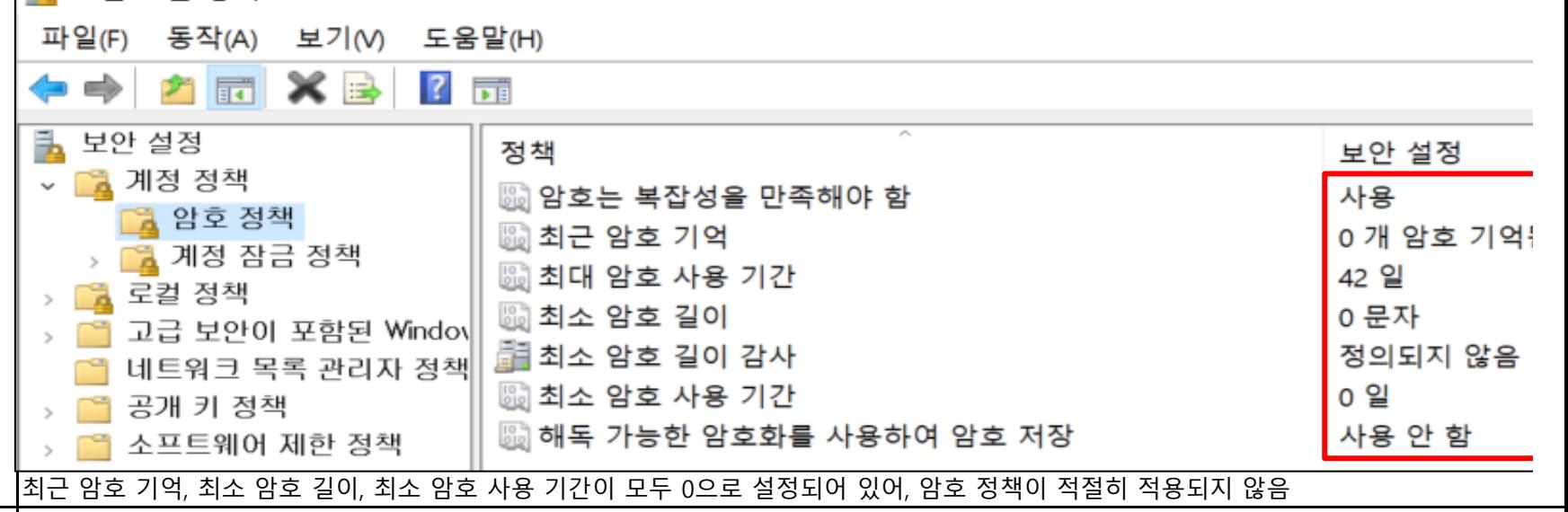


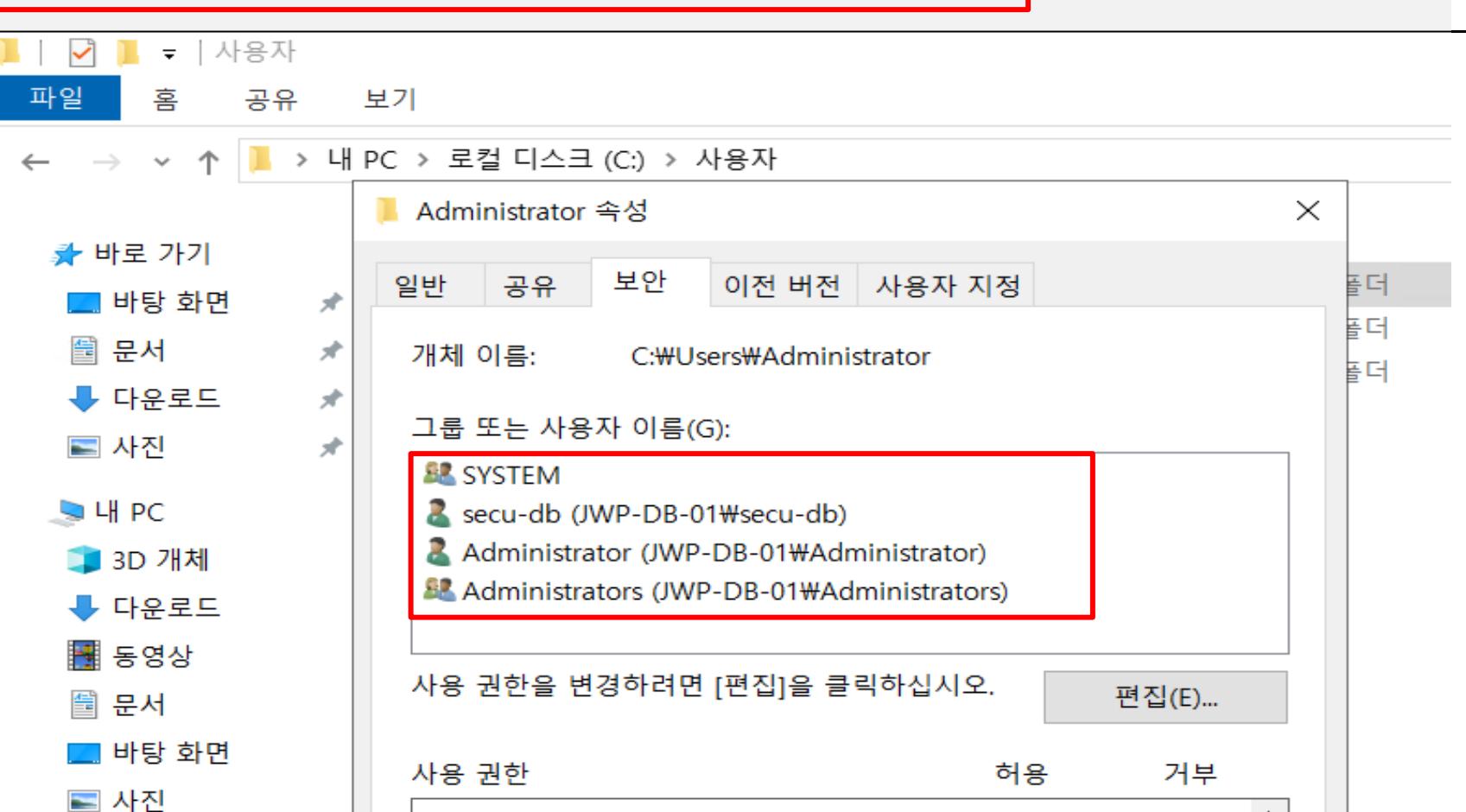
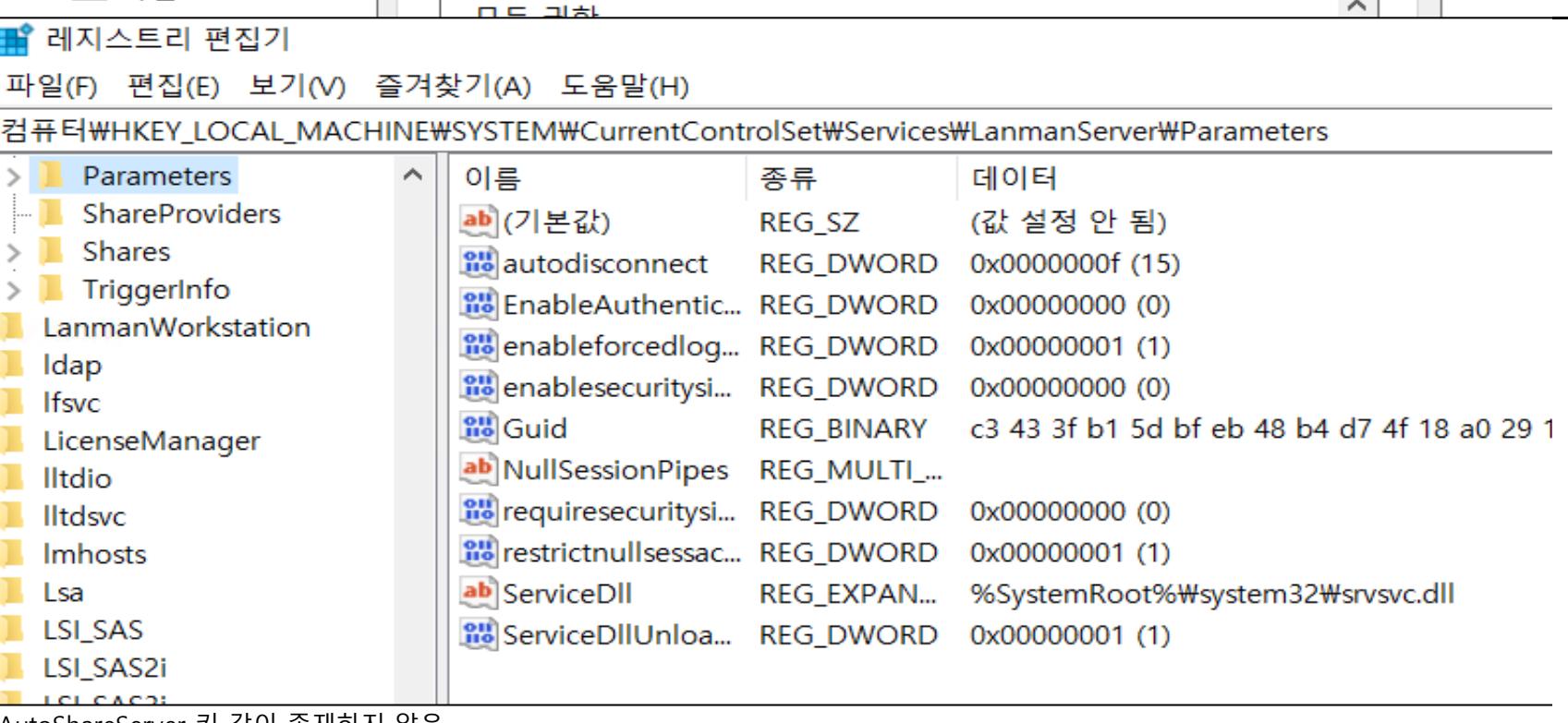
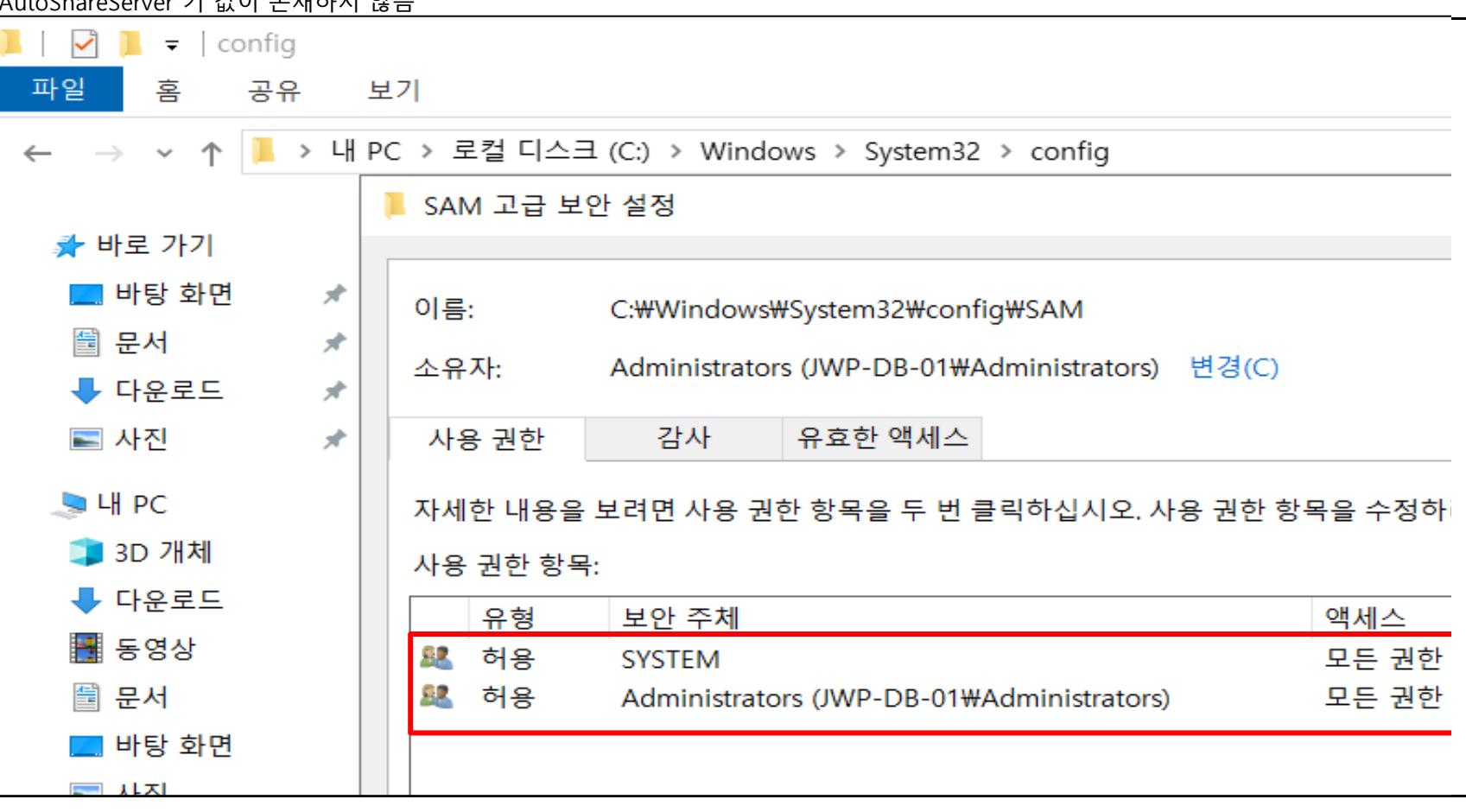
Windows 취약점 진단 요약결과(47항목)

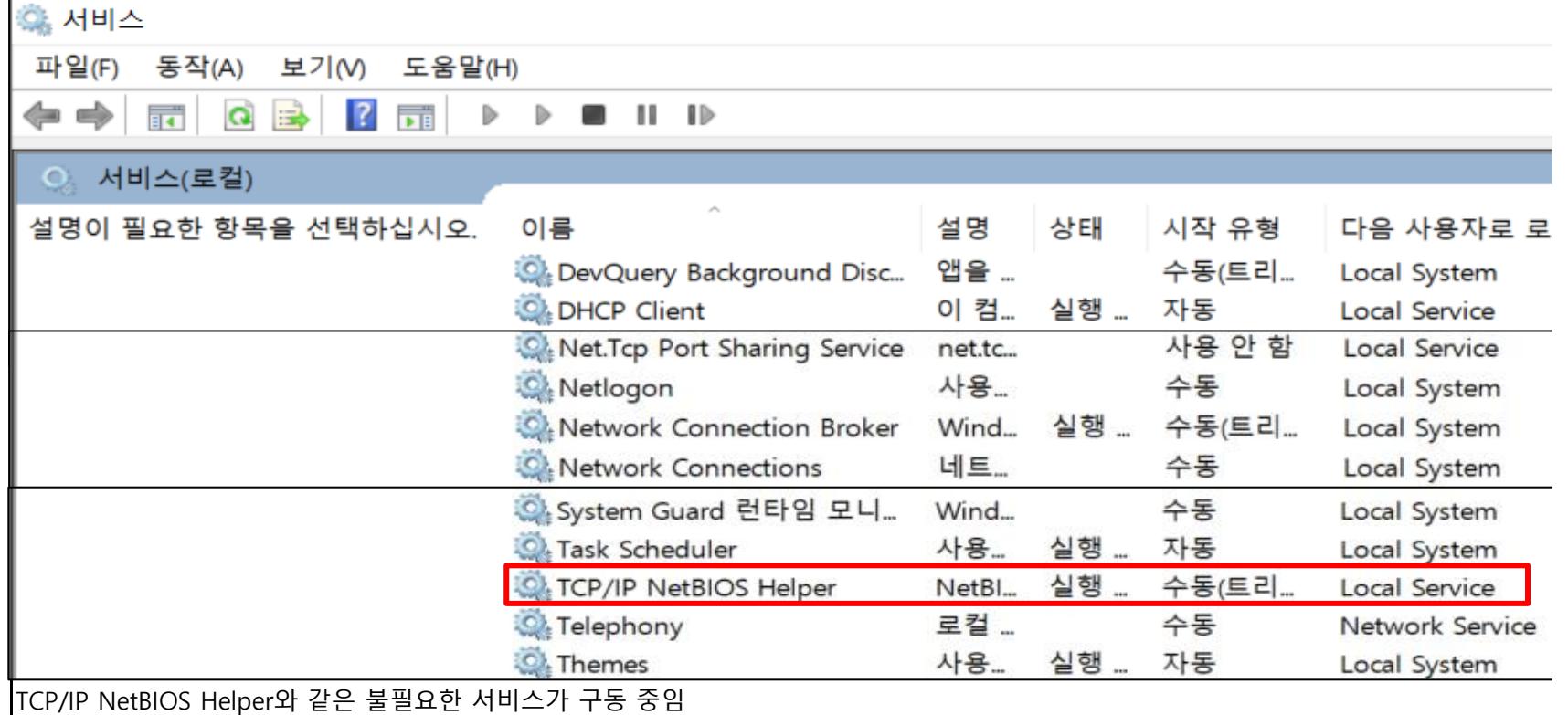
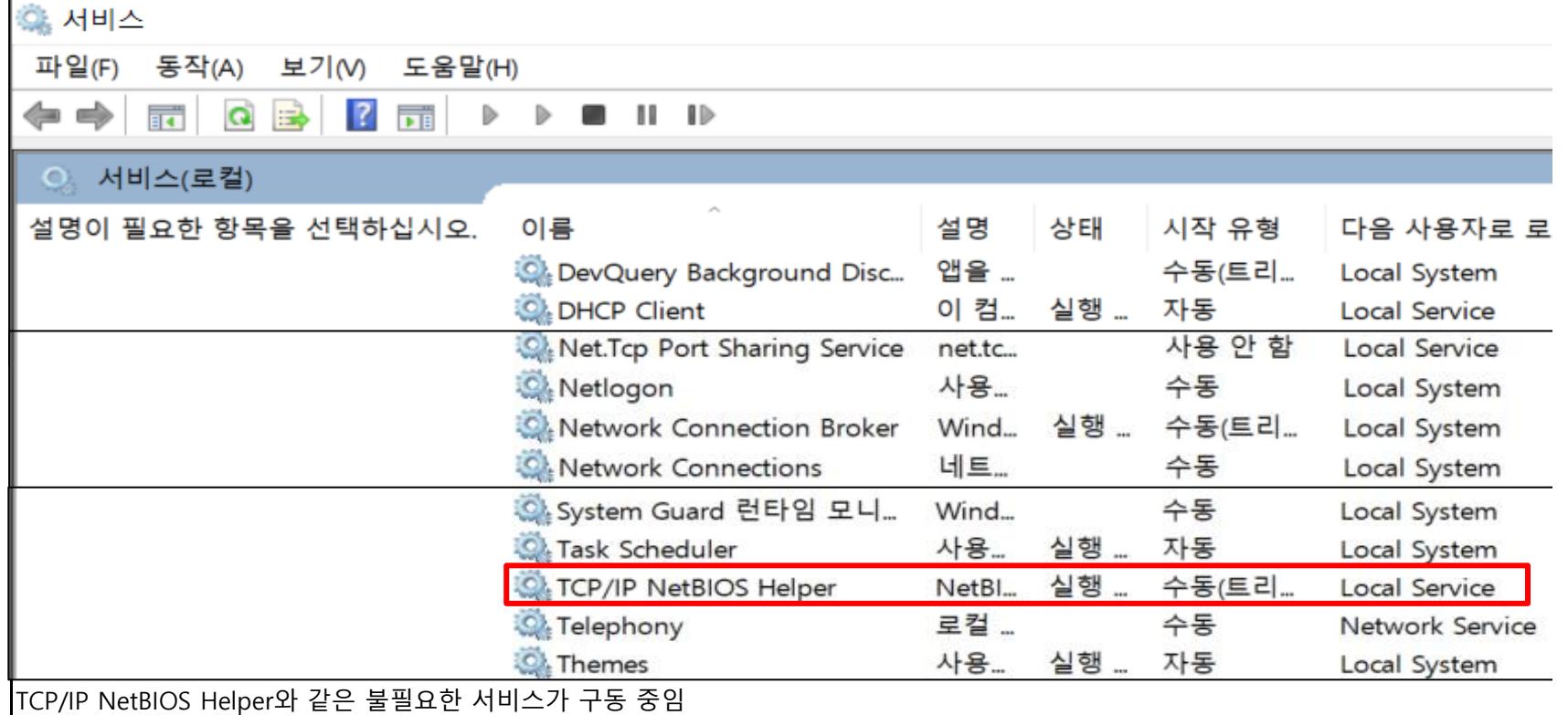
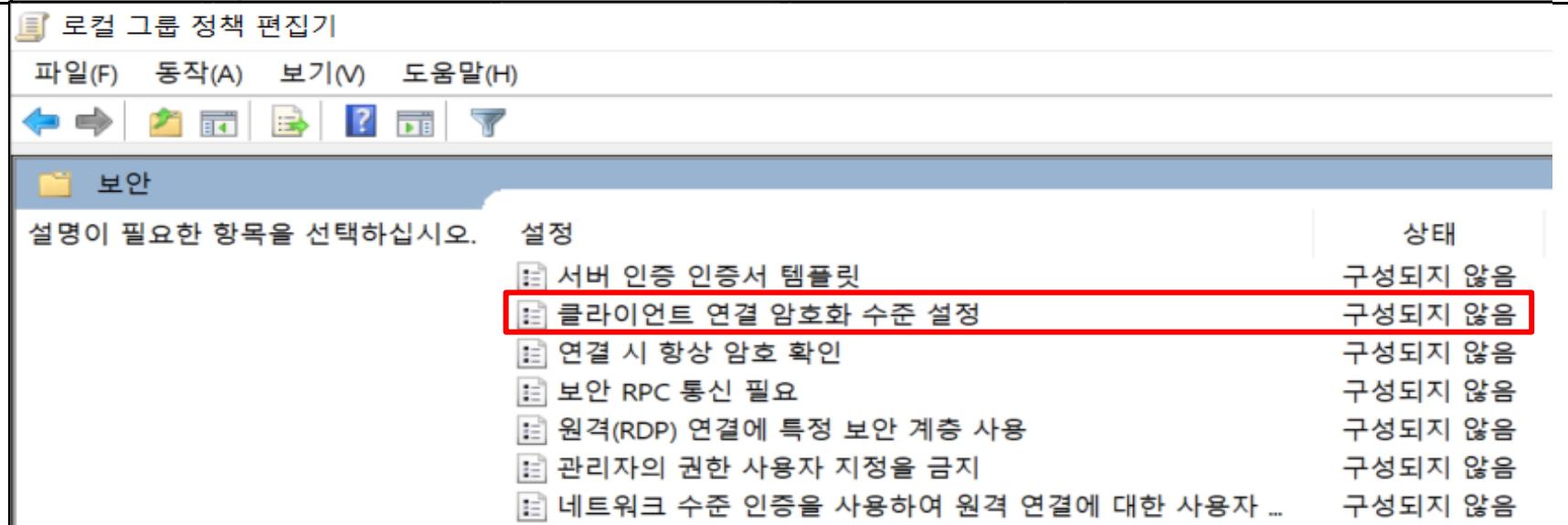
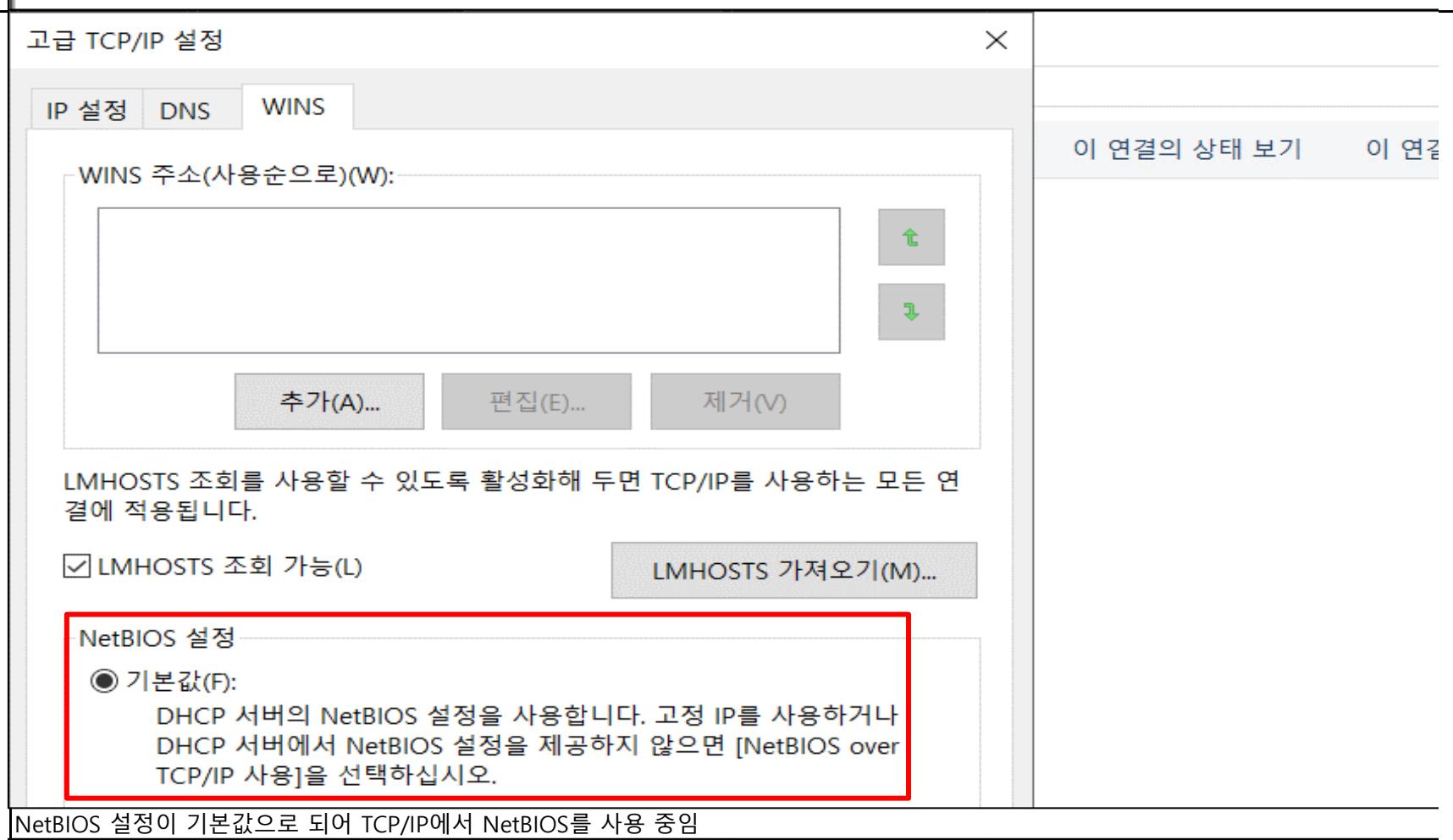
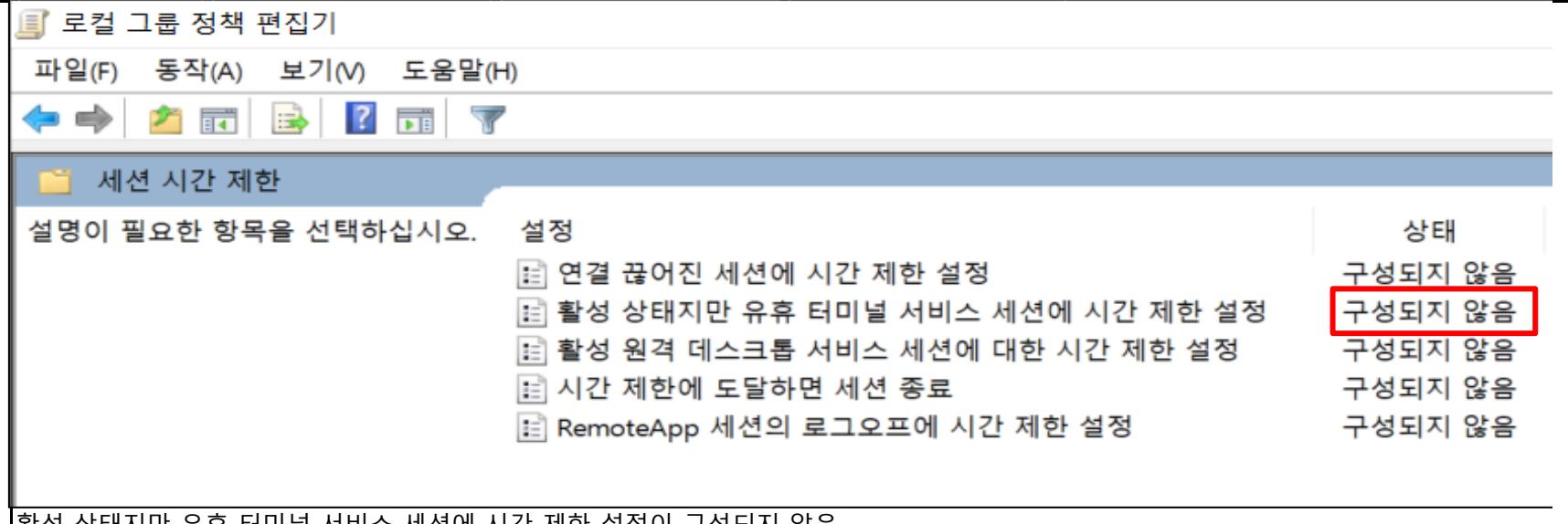
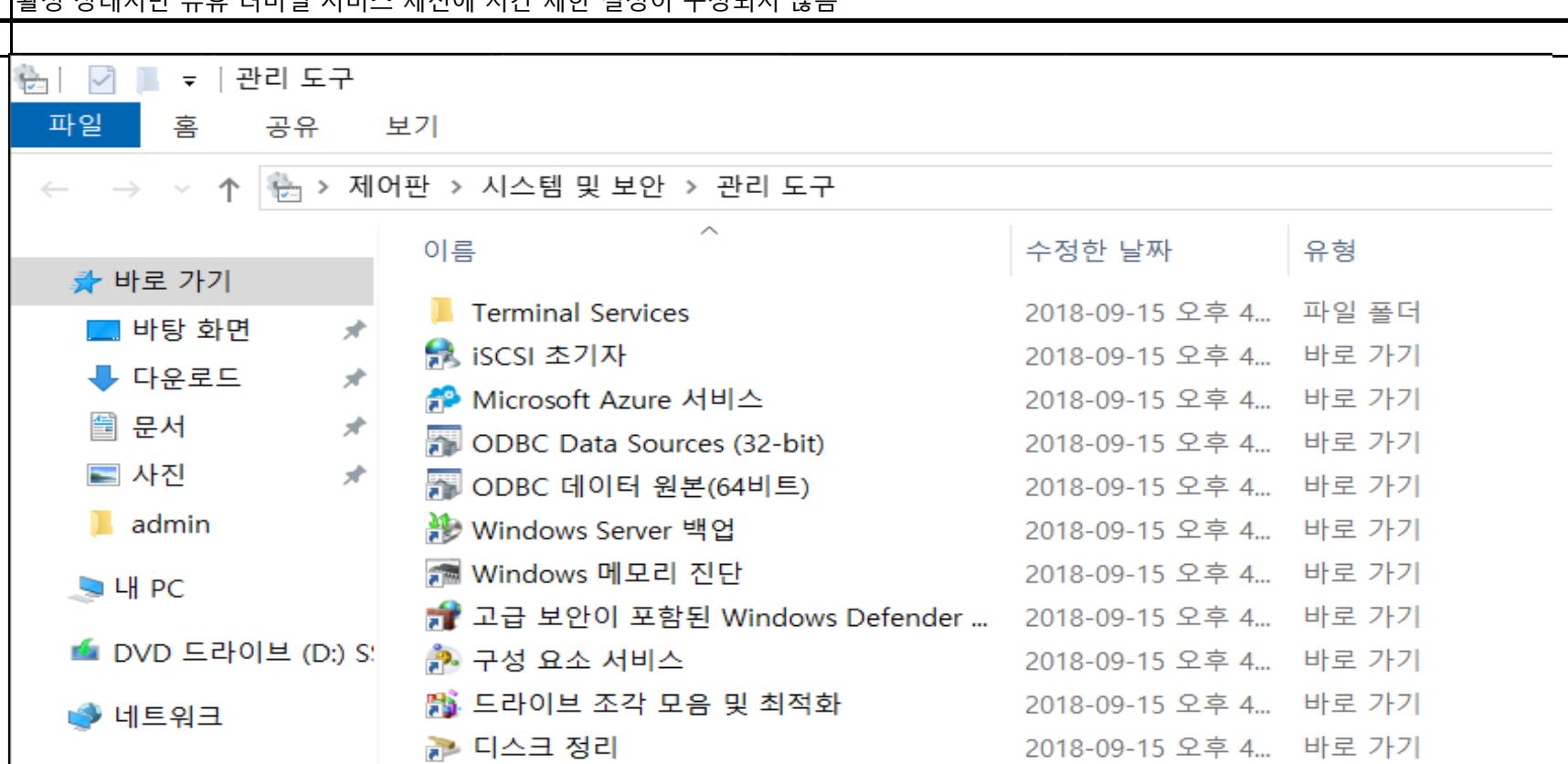
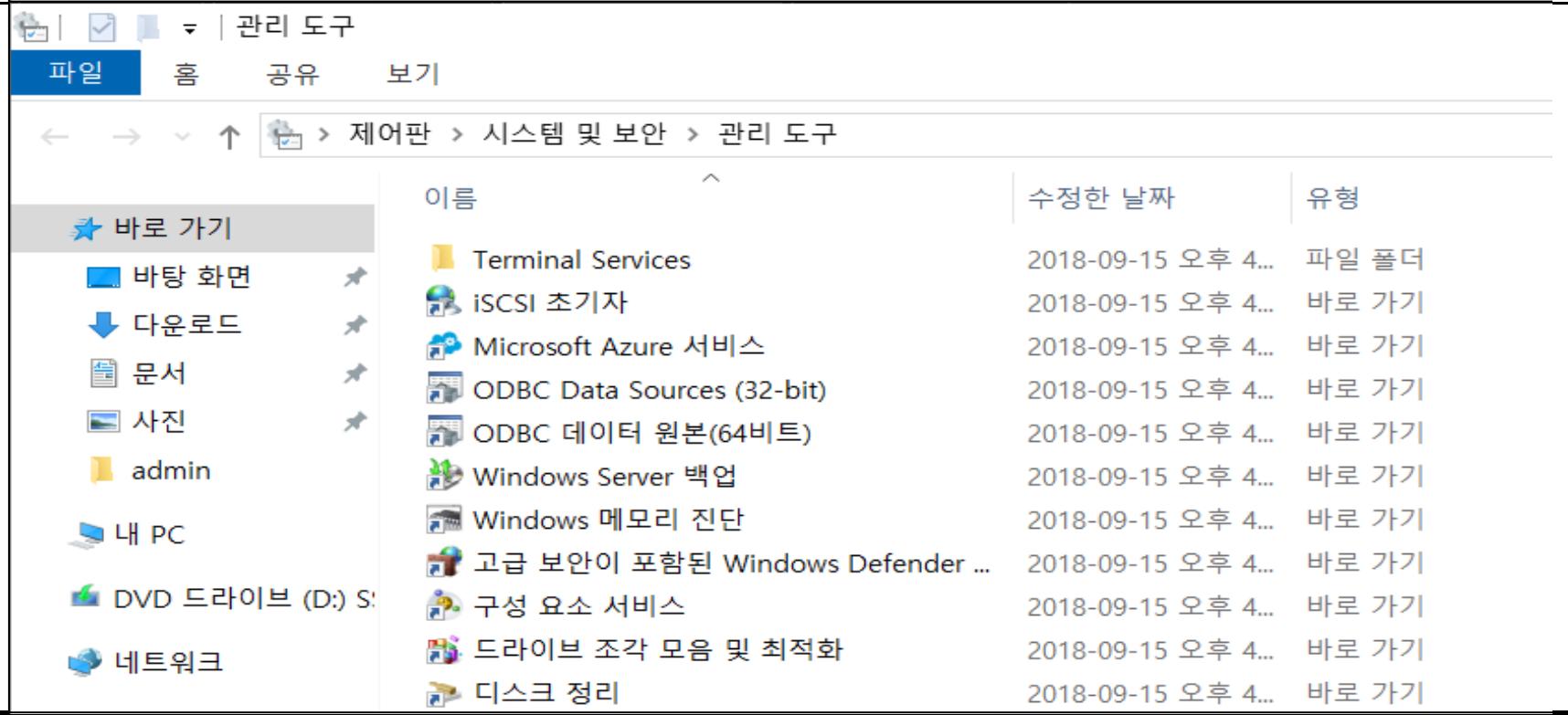
| 진단항목 | No. | 세부 진단항목 | 중 요 도 | 1 |
|----------------|-----|--|-------------|-----------|
| | | | | jwp-db-01 |
| | | | | 10.0.8.8 |
| 1. 계정관리 | 1 | 로컬 계정 사용 설정 | 상 | 취약 |
| | 2 | 계정 잠금 정책 설정 | 상 | 취약 |
| | 3 | 암호 정책 설정 | 상 | 취약 |
| | 4 | 취약한 패스워드 점검 | 상 | 취약 |
| | 5 | 사용자 계정 컨트롤(User Account Control) 설정 | 하 | 양호 |
| | 6 | 의명 SID/이름 변환 허용 정책 | 중 | 양호 |
| | 7 | 콘솔 로그온 시 로컬 계정에서 빙 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 | 취약 |
| | 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 | 취약 |
| | 2 | 터미널 서비스 암호화 수준 설정 | 중 | 양호 |
| | 3 | NetBIOS 서비스 보안 설정 | 상 | 취약 |
| | 4 | 터미널 서비스 Time Out 설정 | 중 | 취약 |
| 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 | 취약 |
| | 2 | 화면 보호기 설정 | 하 | 취약 |
| | 3 | 이벤트 뷰어 설정 | 상 | 양호 |
| | 4 | 로그인 시 경고 메시지 표시 설정 | 중 | 취약 |
| | 5 | 마지막 로그온 사용자 계정 숨김 | 중 | 취약 |
| | 6 | 로그온 하지 않은 사용자 시스템 종료 방지 | 중 | 취약 |
| | 7 | 로컬 감사 정책 설정 | 상 | 취약 |
| | 8 | 가상 매모리 페이지 파일 삭제 설정 | 하 | 취약 |
| | 9 | Lan Manager 인증 수준 | 하 | 취약 |
| | 10 | Everyone 사용 권한을 의명 사용자에게 적용 안함 | 하 | 양호 |
| | 11 | 이동식 미디어 포맷 및 꺼내기 admin만 허용 | 하 | 취약 |
| | 12 | 세션 연결 끊기 전 유회 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 | 취약 |
| 7. 레지스트리 보안 설정 | 1 | SAM(Security Account Manager) 보안 감사 설정 | 하 | 취약 |
| | 2 | Null Session 설정 | 상 | 취약 |
| | 3 | Remote Registry Service 설정 | 상 | 취약 |
| | 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 | 취약 |
| | 2 | 최신 HOT FIX 적용 | 상 | 취약 |
| 9. 이슈 취약점 | 1 | OpenSSL 취약점 | 상 | 양호 |
| 점검결과 | | | | 23 |
| | | 보안 적용율 (양호항목 / 진단항목) % | | 46.5% |

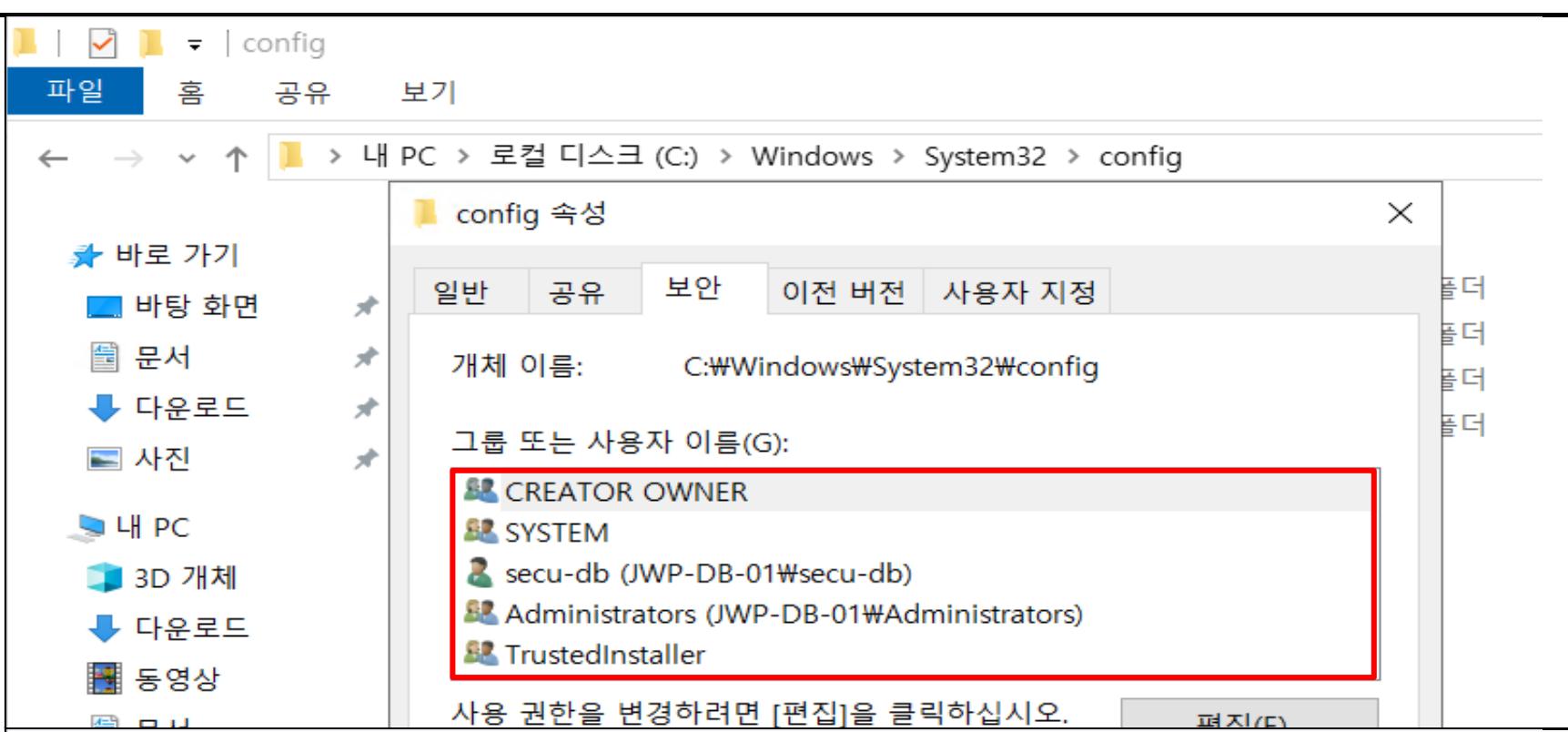
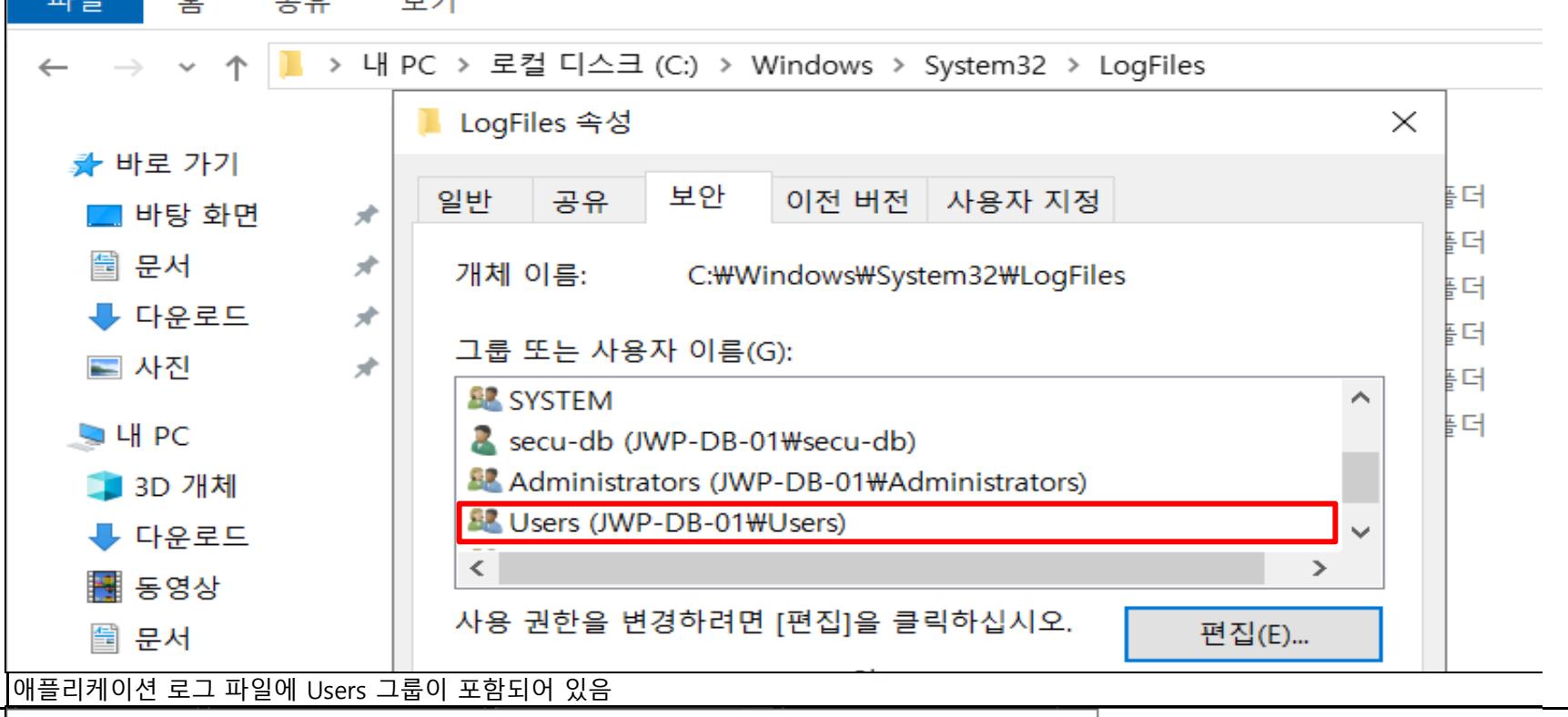
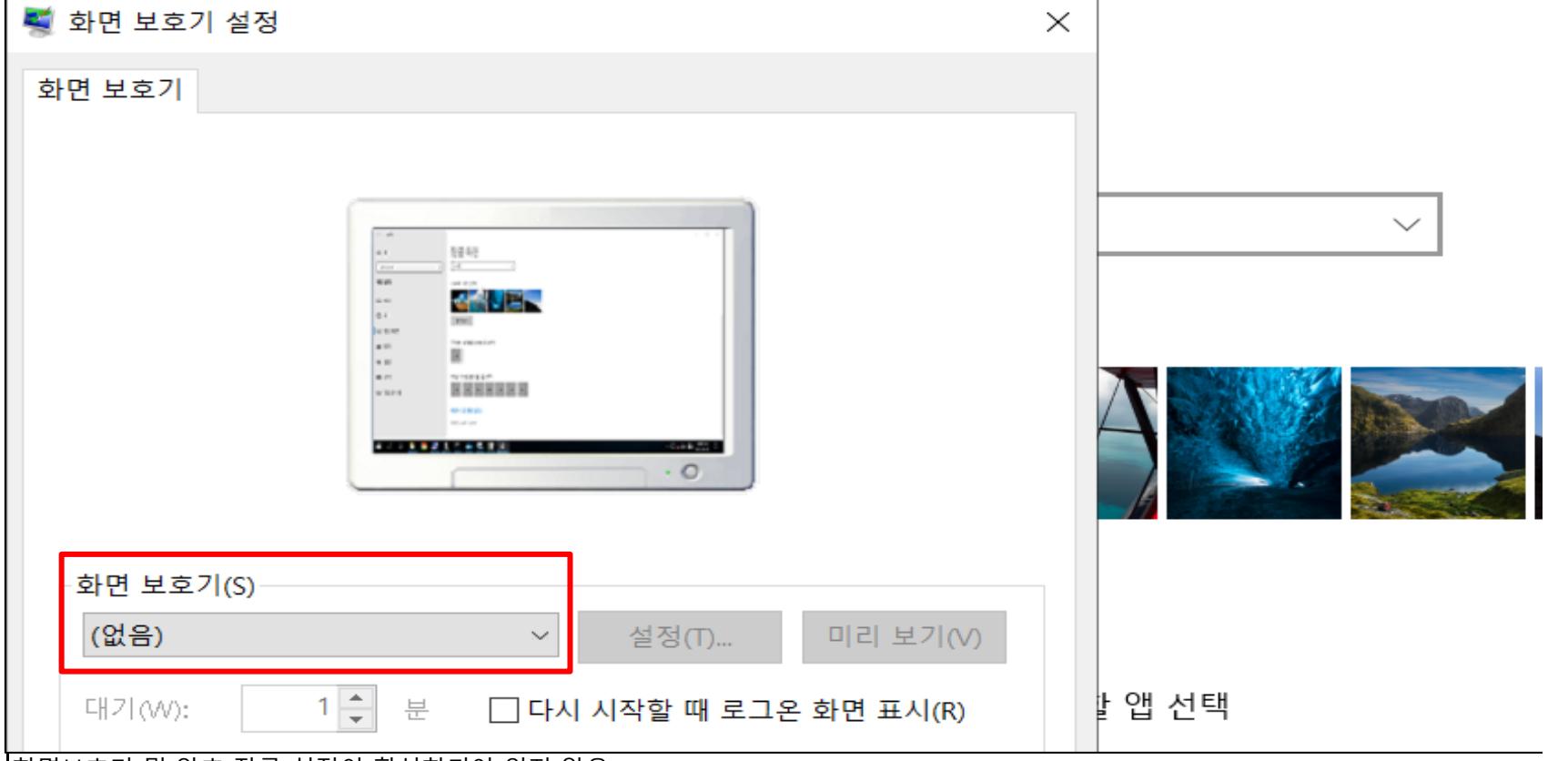
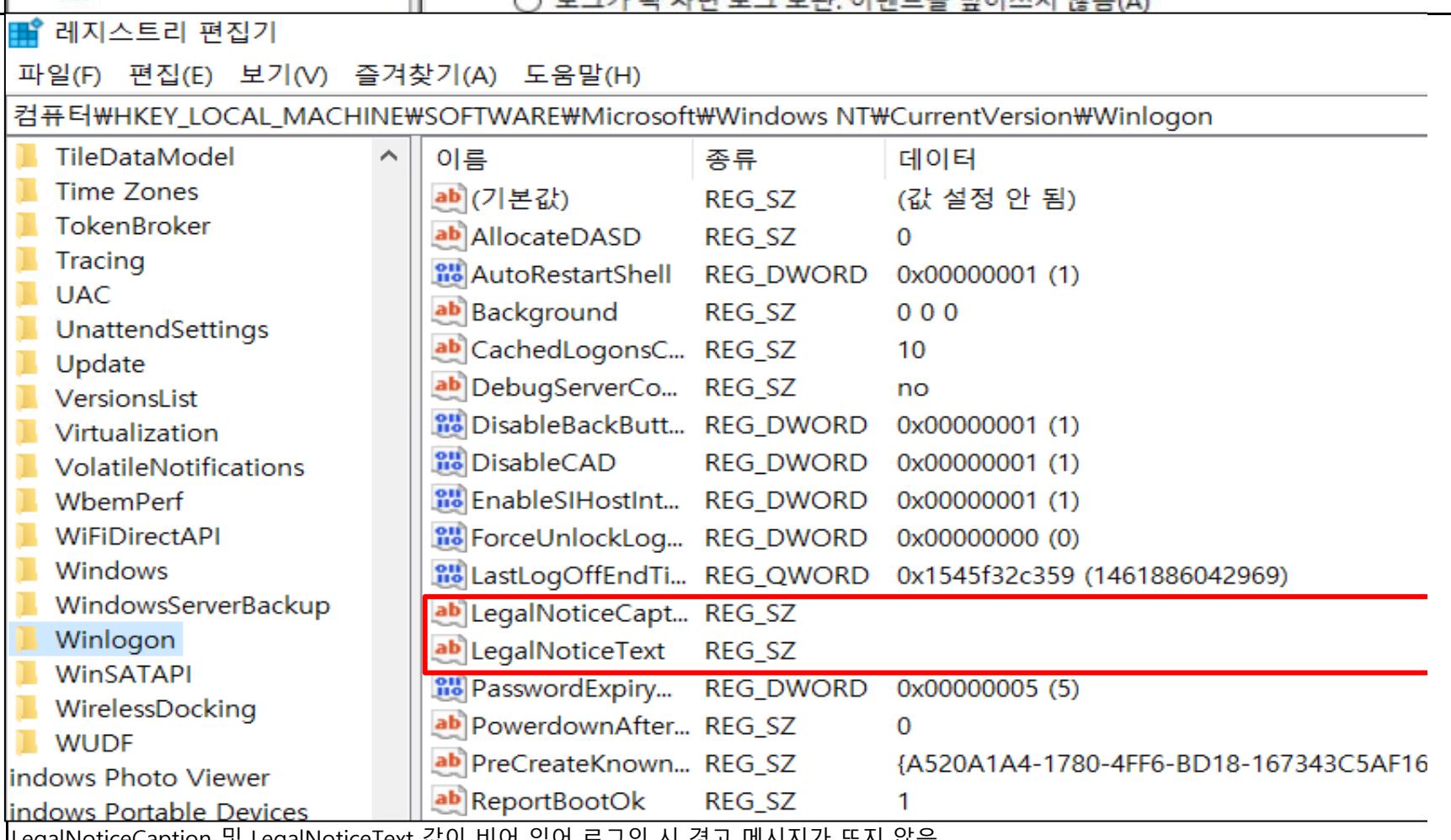
| 영역별점수 | 점수 | 양호 | 취약 | N/A |
|--------|--------|----|----|-----|
| 50.0% | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 100.0% | 1 | 0 | 0 |
| 75.0% | 100.0% | 1 | 0 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | N/A | 0 | 0 | 1 |
| 25.0% | 0.0% | 0 | 1 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| 100.0% | N/A | 0 | 0 | 1 |
| | 100.0% | 1 | 0 | 0 |
| | 100.0% | 1 | 0 | 0 |
| 43.8% | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 100.0% | 1 | 0 | 0 |
| | 100.0% | 1 | 0 | 0 |
| 50.0% | 100.0% | 1 | 0 | 0 |
| | 0.0% | 0 | 1 | 0 |
| 25.0% | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | 0.0% | 0 | 1 | 0 |
| | N/A | 0 | 0 | 1 |
| | 100.0% | 1 | 0 | 0 |
| 0.0% | N/A | 0 | 0 | 1 |
| | 0.0% | 0 | 1 | 0 |
| 100.0% | 100.0% | 1 | 0 | 0 |

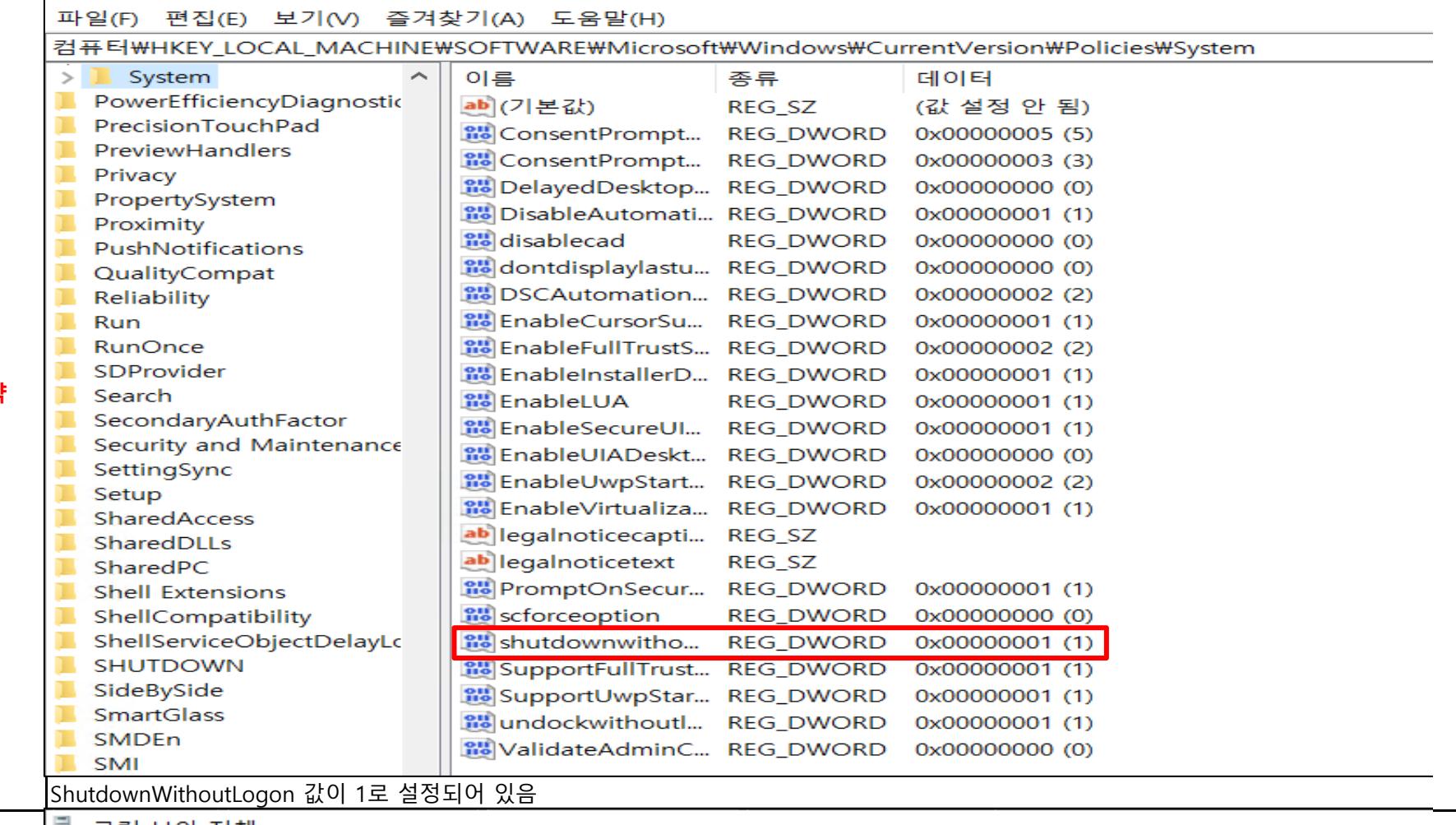
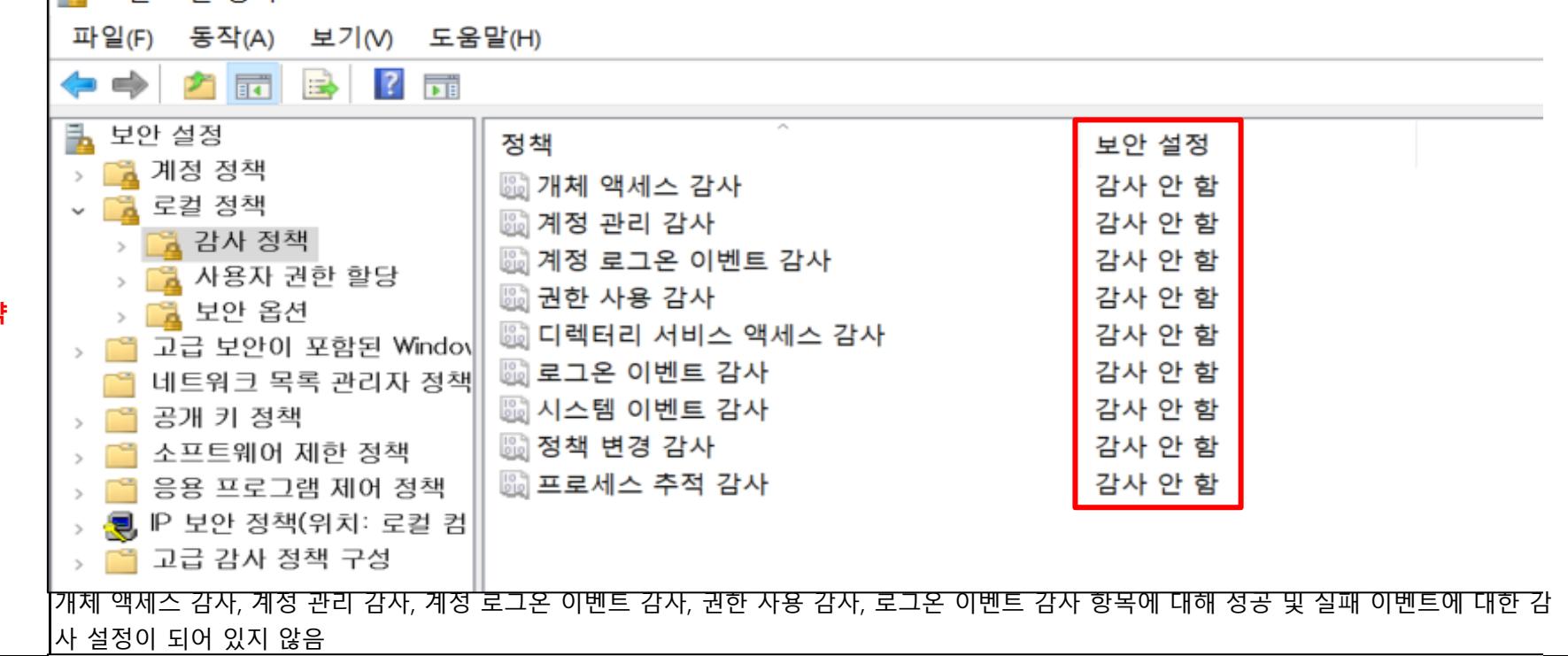
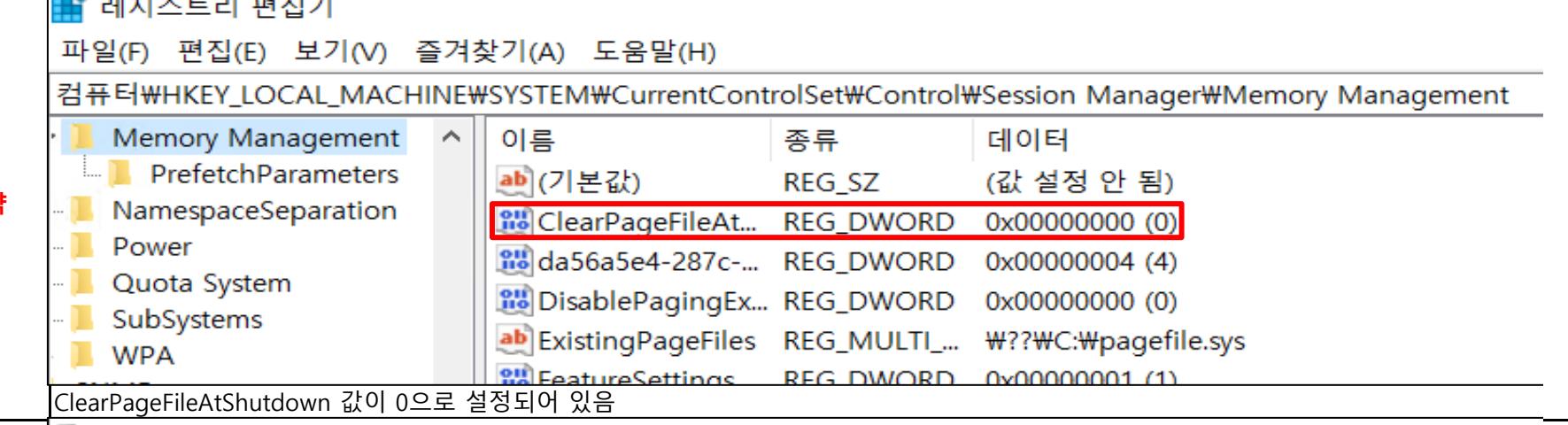
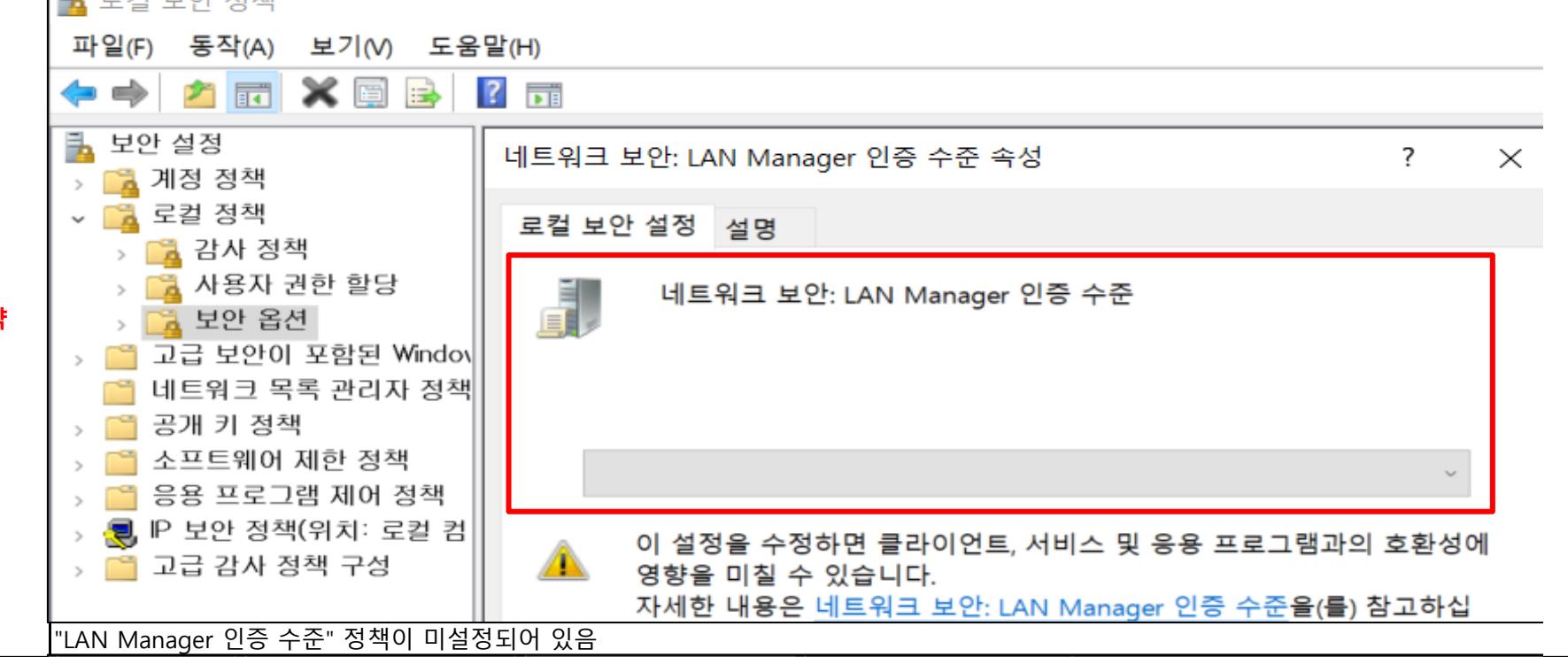
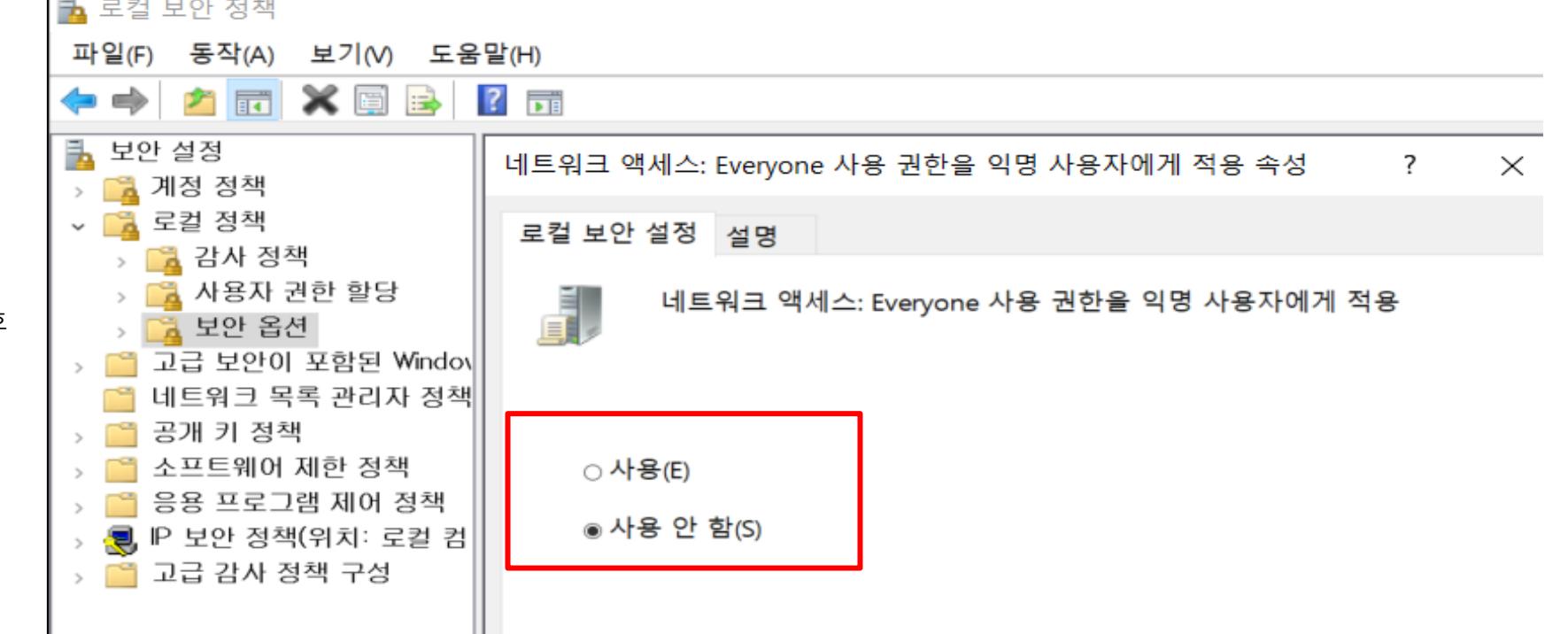
Windows 취약점 진단 상세결과(47항목)

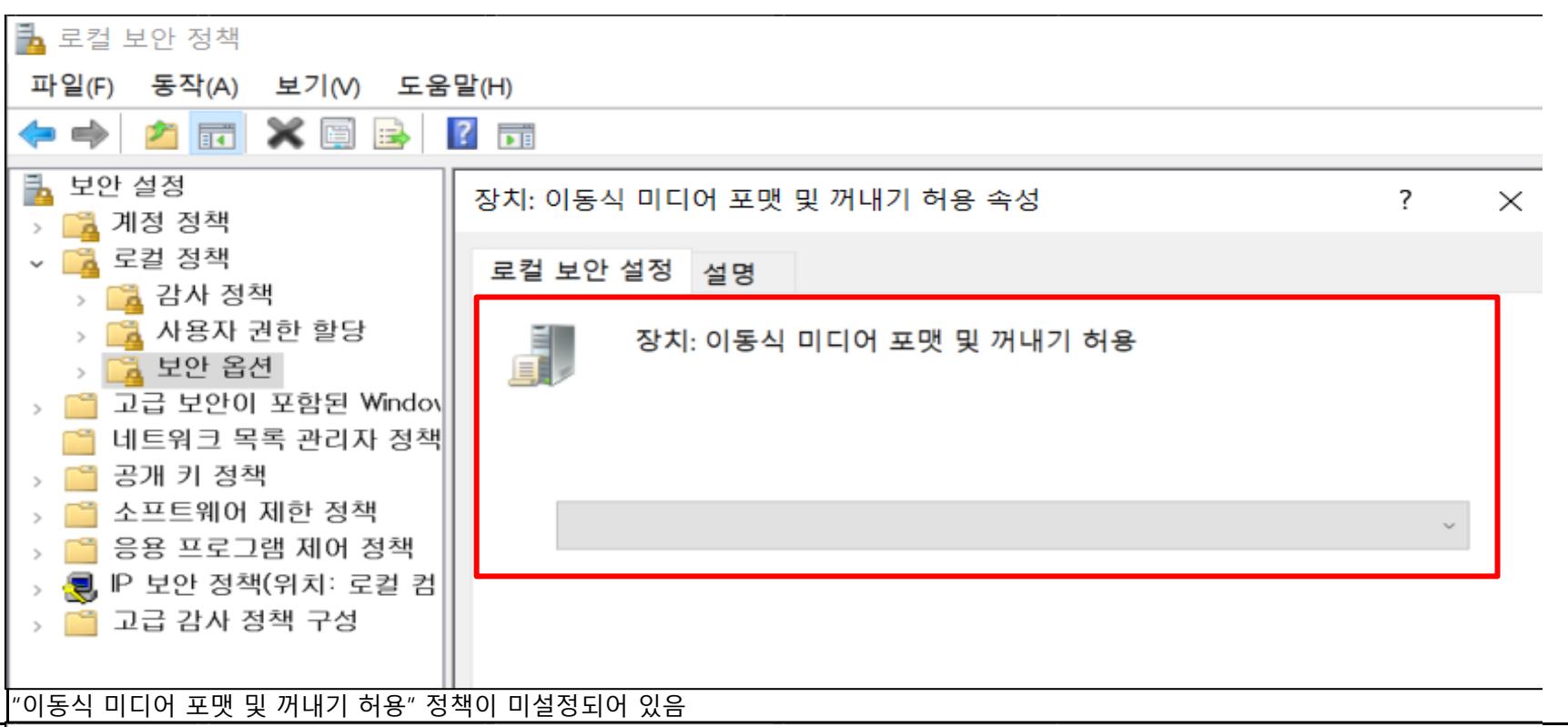
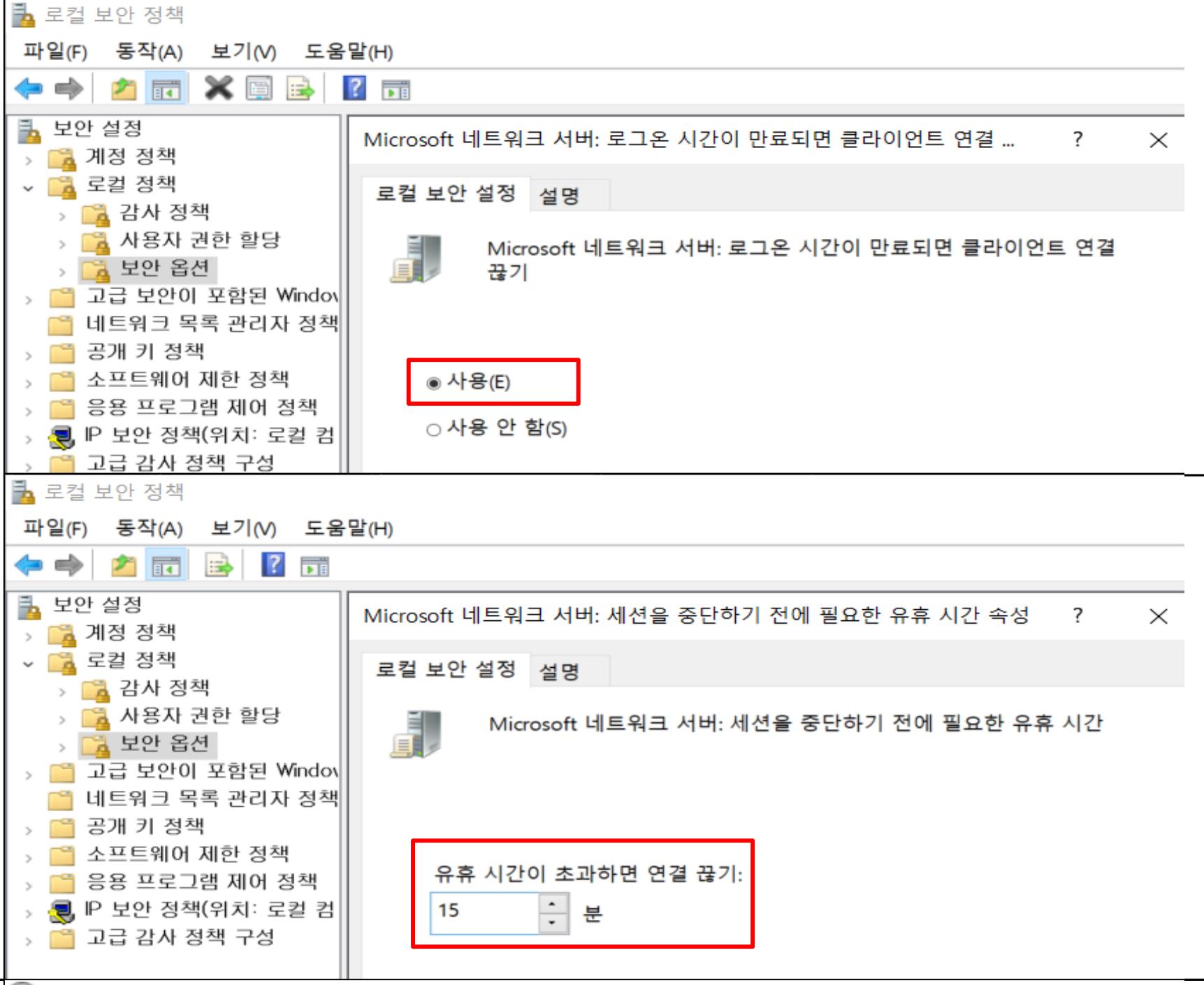
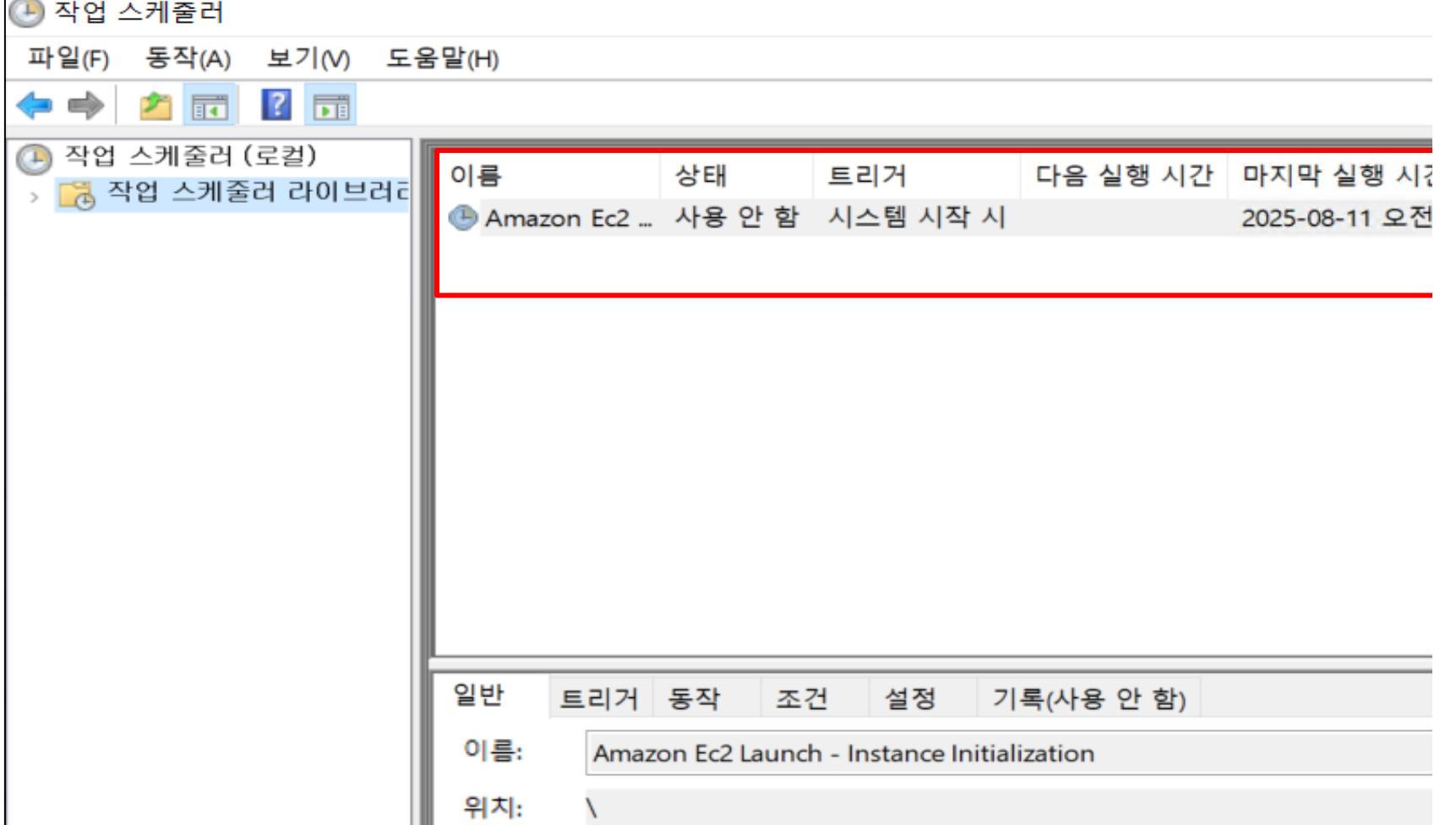
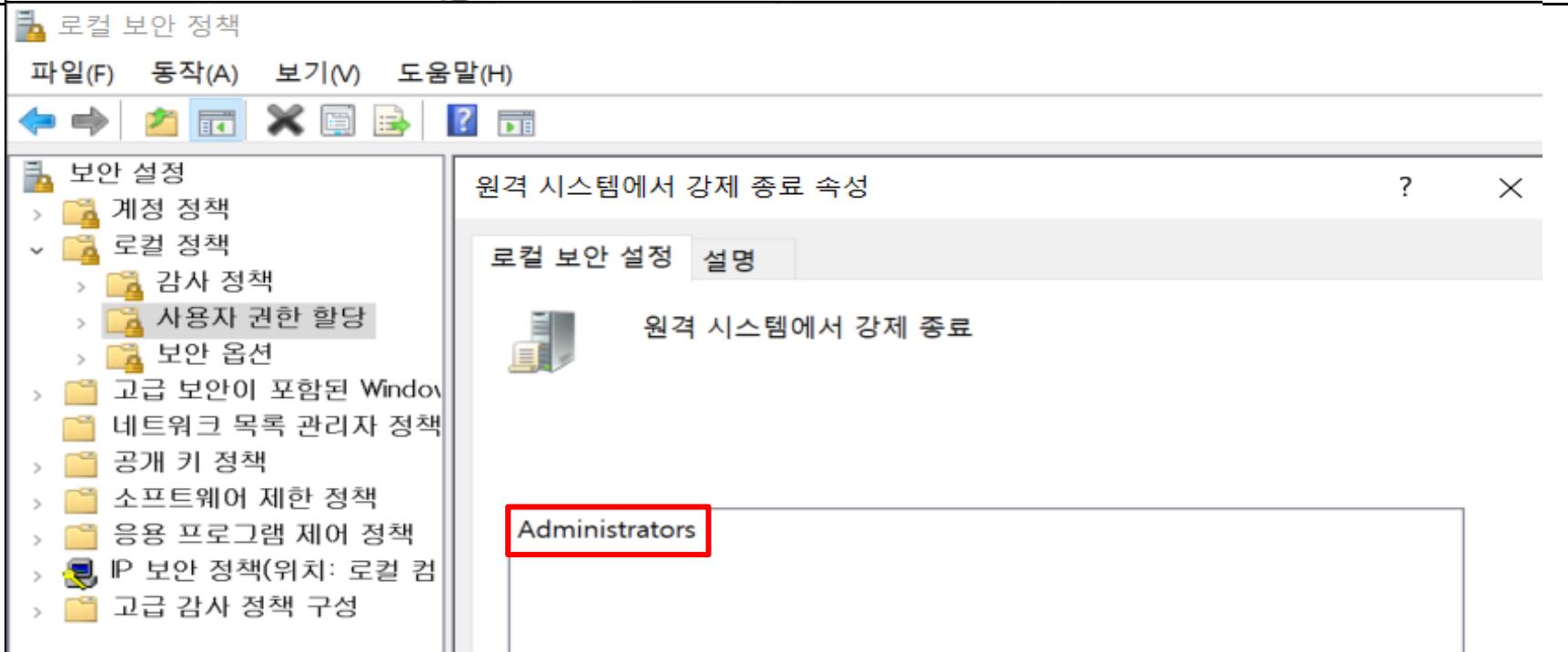
| 진단항목 | No. | 세부 진단항목 | 진단기준 | 1 | jwp-db-01 10.0.8.8 DB OS |
|---------|-----|-------------------------------------|---|----|---|
| 1. 계정관리 | 1 | 로컬 계정 사용 설정 | 양호 - Administrators 그룹에 관리자 계정인 Administrator의 이름을 바꾸어 사용하는 경우 Guest 계정 비활성화되어 있는 경우 / 불필요한 계정이 존재하지 않을 경우 취약 - Administrators 그룹에 관리자 계정인 Administrator가 존재하는 경우 Guest 계정 활성화되어 있는 경우 / 불필요한 계정이 존재할 경우 | 취약 |  |
| | 2 | 계정 잠금 정책 설정 | 양호 - 계정 잠금 기간 30분, 계정 잠금 기간 원래대로 설정 30분, 계정 잠금 임계 값 1 이상 5 이하인 경우 취약 - 계정 잠금 기간 및 잠금 기간 원래대로 설정 기간이 30분 보다 작거나, 계정 잠금 임계 값 설정이 없거나 5보다 큰 경우 | 취약 |  |
| | 3 | 암호 정책 설정 | 양호 - 진단 방법의 기준을 모두 만족하는 경우 취약 - 진단 방법의 기준을 하나라도 만족하지 않는 경우 | 취약 |  |
| | 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 | 취약 | 담당자와 인터뷰 결과 계정과 유사한 패스워드로 확인 |
| | 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 로그온 시 로컬 계정에서 빙 암호 사용 제한 정책 점검 | 양호 - "콘솔 로그온 시 로컬 계정에서 빙 암호 사용 제한" 정책이 "사용"으로 설정되어 있는 경우 취약 - "콘솔 로그온 시 로컬 계정에서 빙 암호 사용 제한" 정책이 "사용 안 함"으로 설정되어 있는 경우 | 양호 |  |

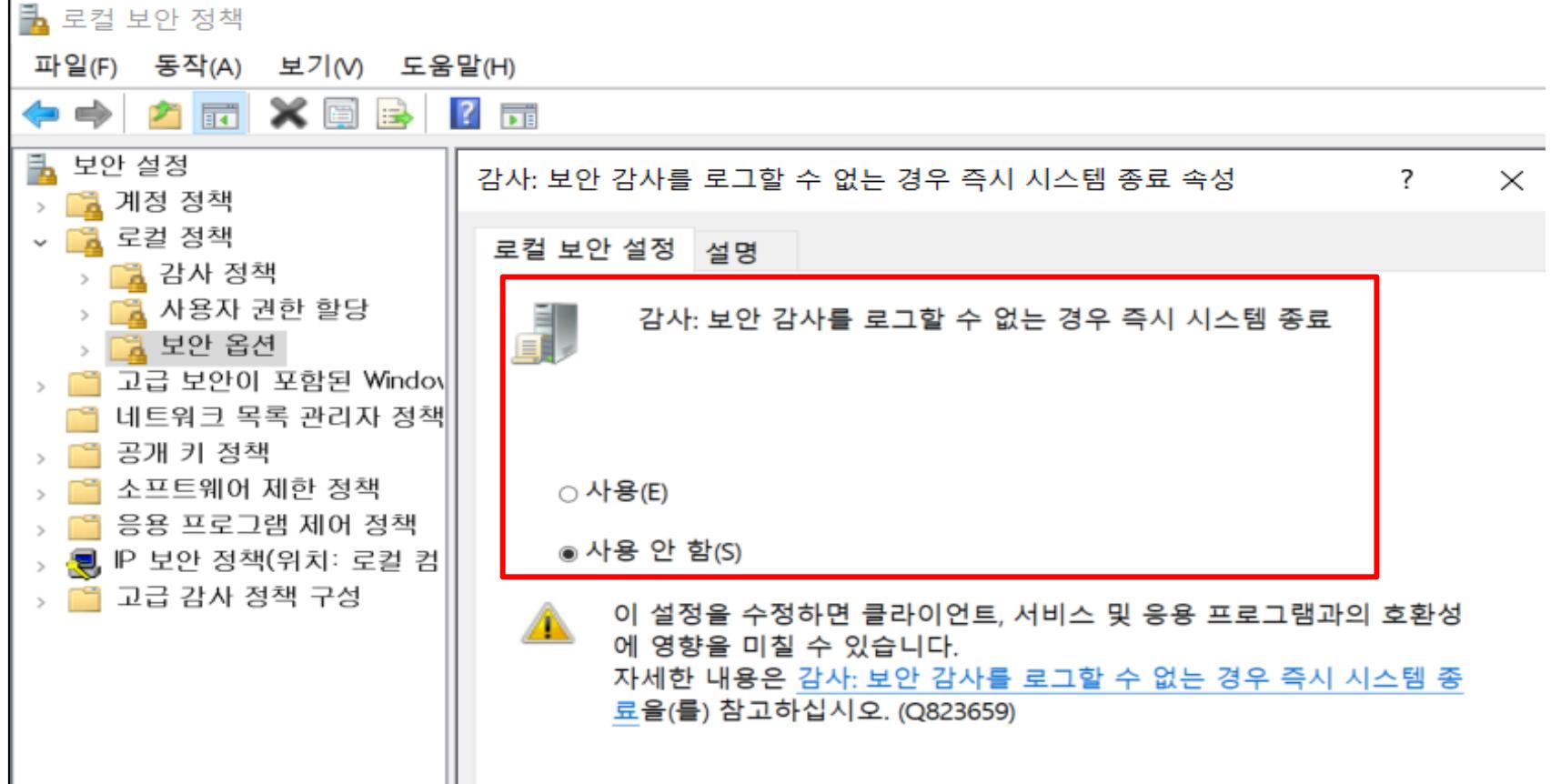
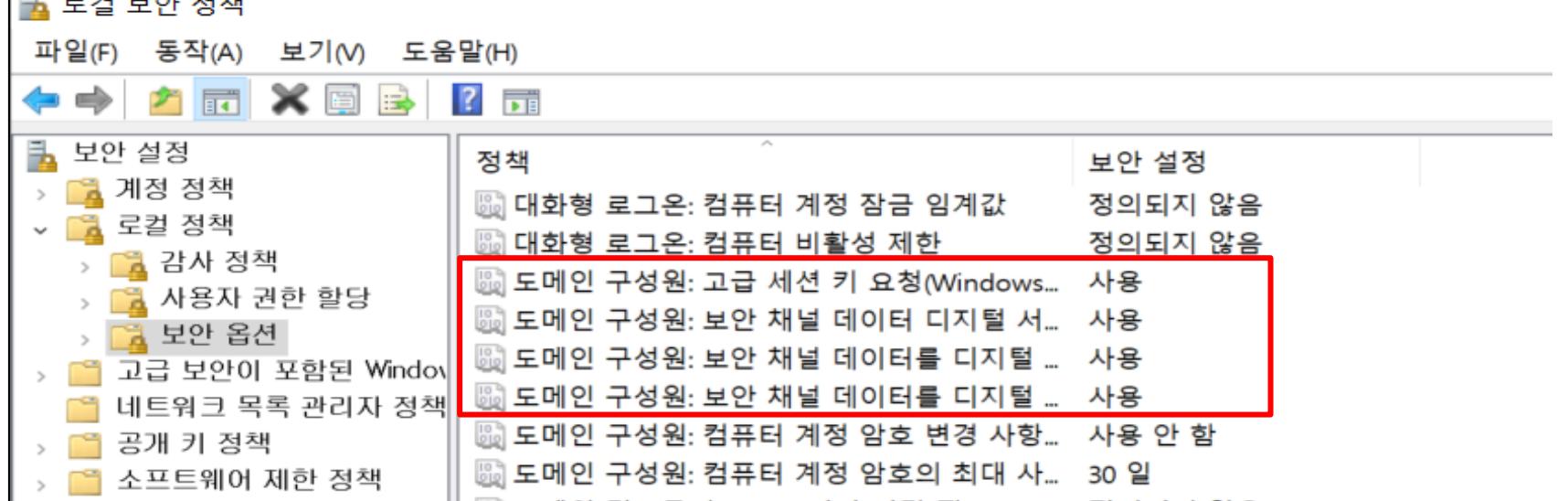
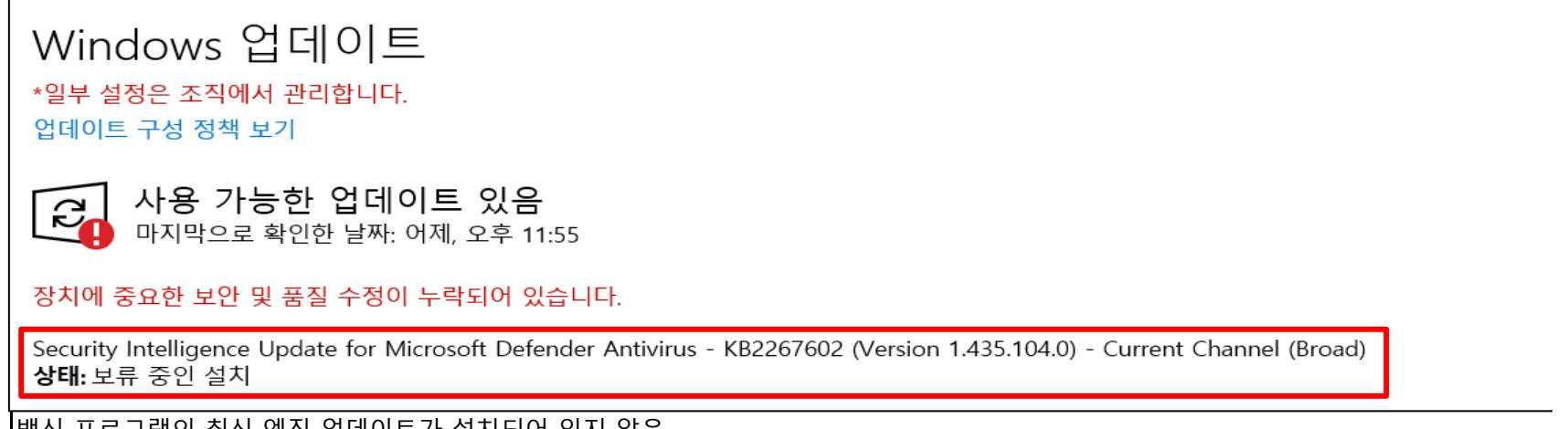
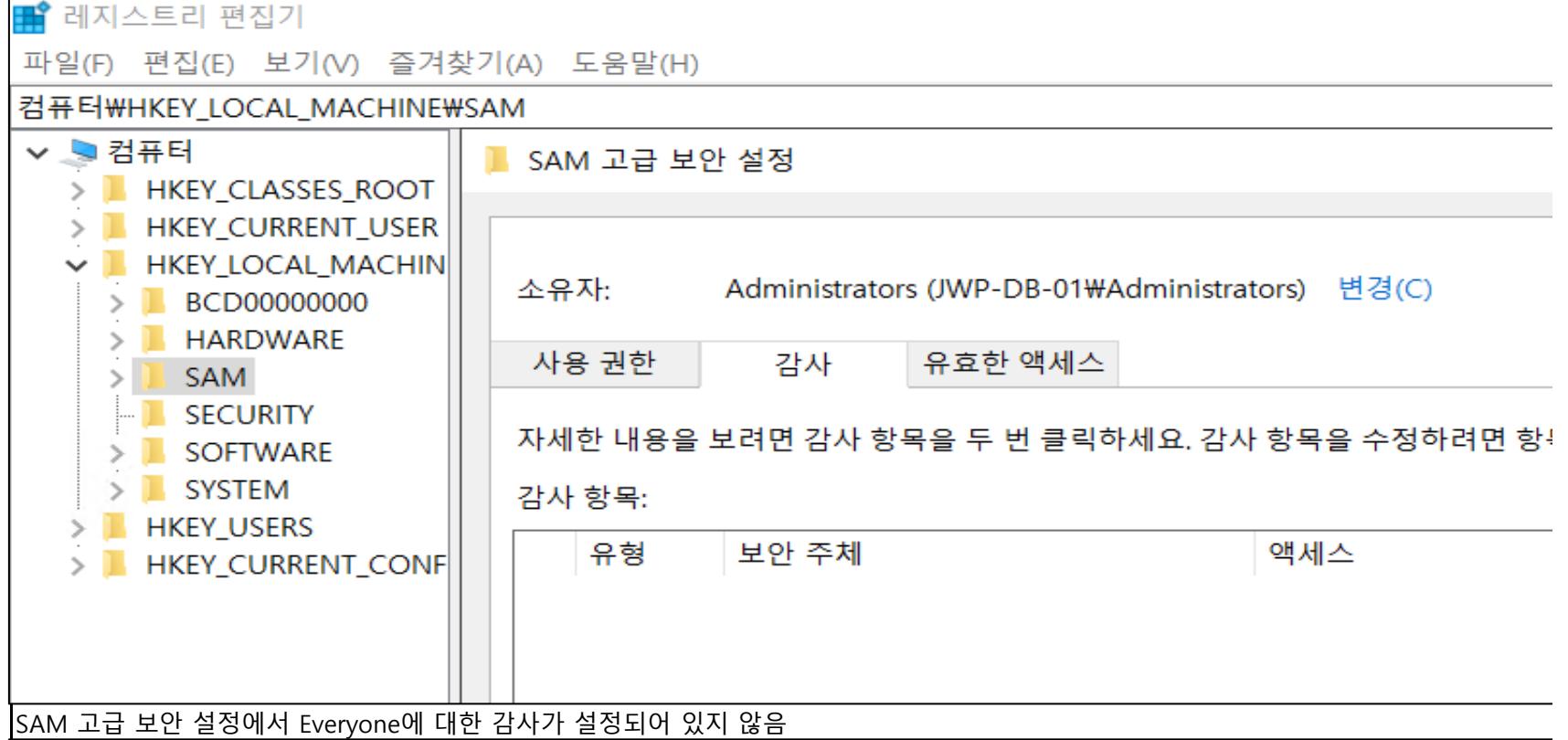
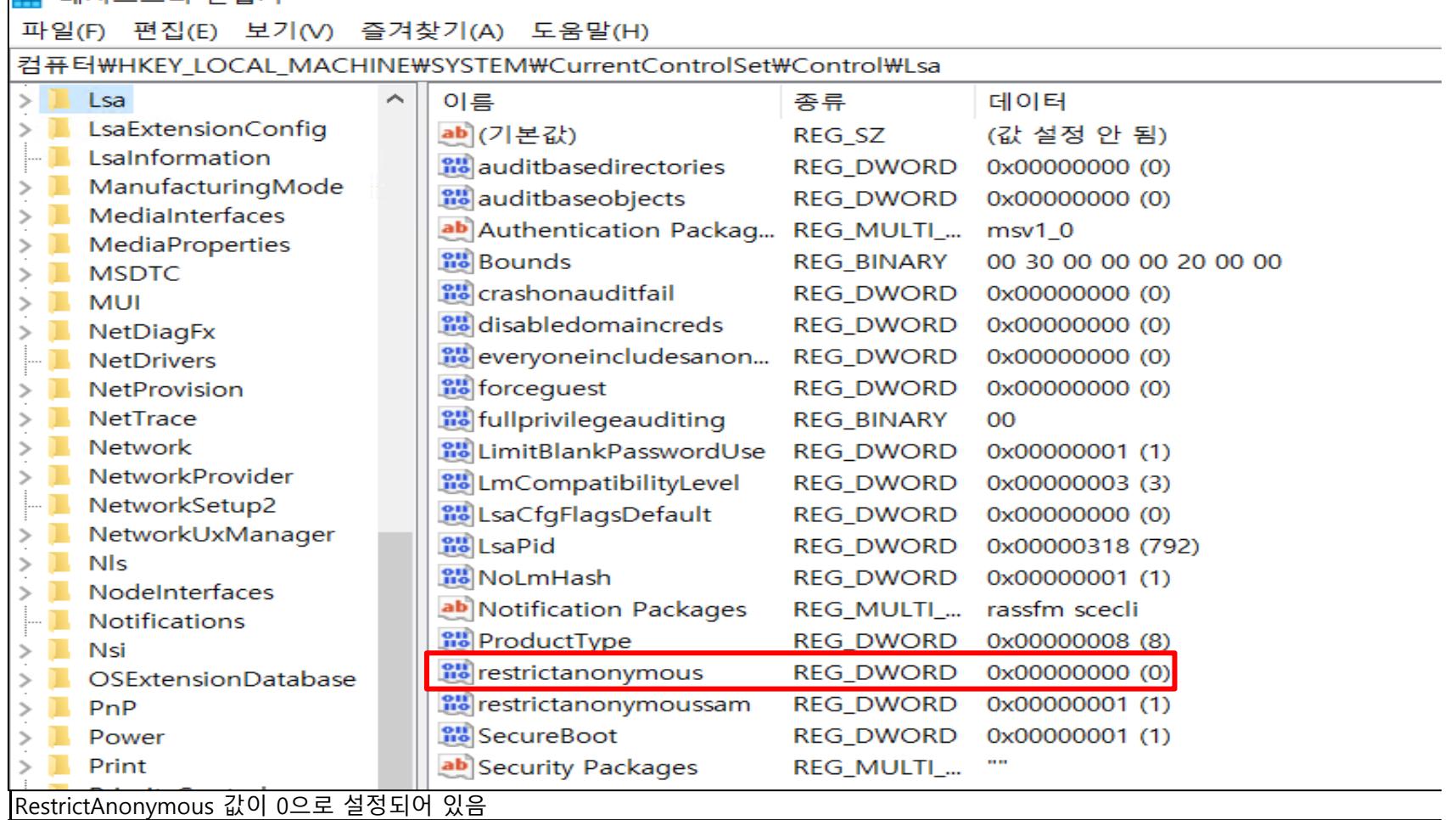
| | | | | |
|-----------|--|--|-----|---|
| | 8 관리자 그룹에 최소한의 사용자 포함 | 양호 - Administrator 그룹 구성원을 1명 이하로 유지하거나, 불필요한 관리자 계정이 존재하지 않는 경우 취약 - Administrator 그룹 구성원에 불필요한 관리자 계정이 존재하는 경우 | 양호 |  |
| | 1 CMD.EXE 파일 권한 설정 | 양호 - IIS 서비스가 실행 중이 아니거나, Administrator와 System, TrustedInstaller만 실행 권한이 설정되어 있을 경우 취약 - IIS가 실행 중이면서, Administrator와 System, TrustedInstaller 이 외에도 실행 권한이 설정되어 있을 경우 | 양호 |  |
| | 2 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 |  |
| 2. 파일 시스템 | 3 공유 폴더 설정 | 취약 - 기본 공유 디렉터리가 없거나 공유 디렉터리 접근 권한에 Everyone이 없을 경우 해당 레지스터리 AutoShareServer 값이 0, 암호 보호 공유가 설정되어 있는 경우 취약 - 기본 공유 디렉터리의 접근 권한에 Everyone이 있거나 암호 보호 공유가 해제되어 있는 경우 | 취약 |  |
| | 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 | |

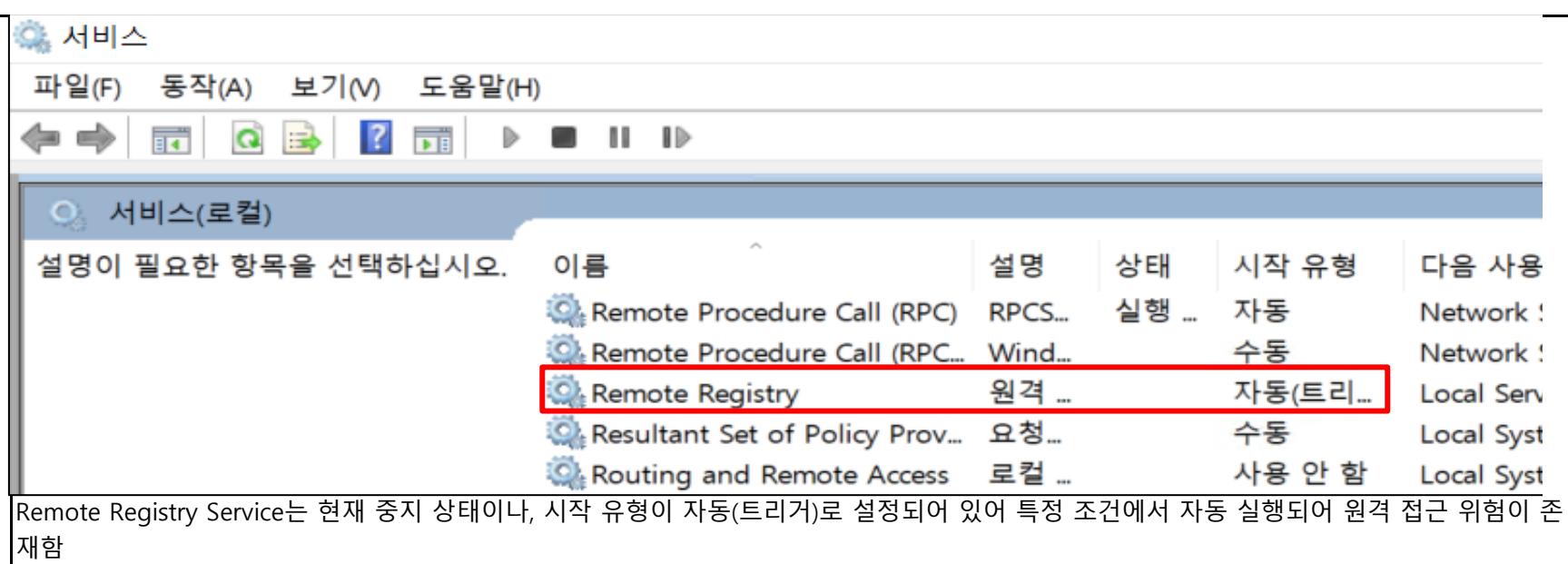
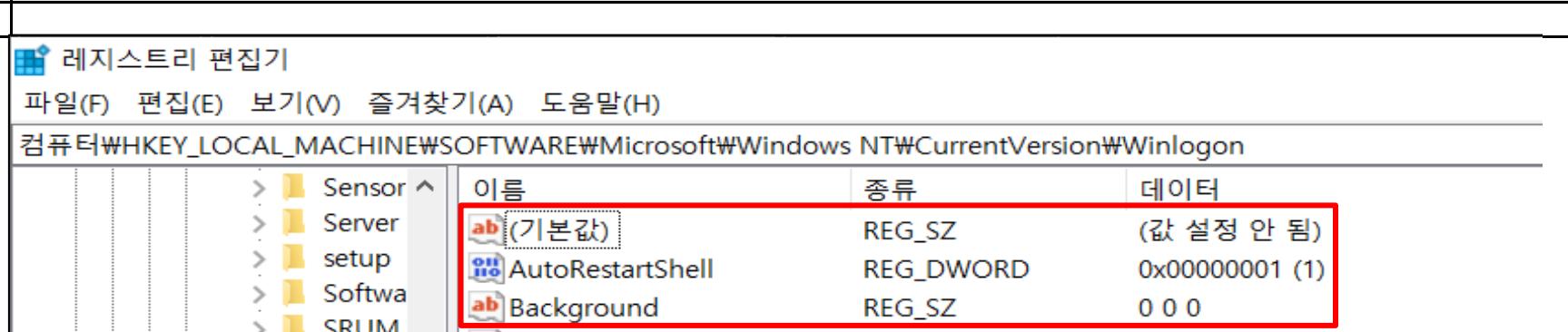
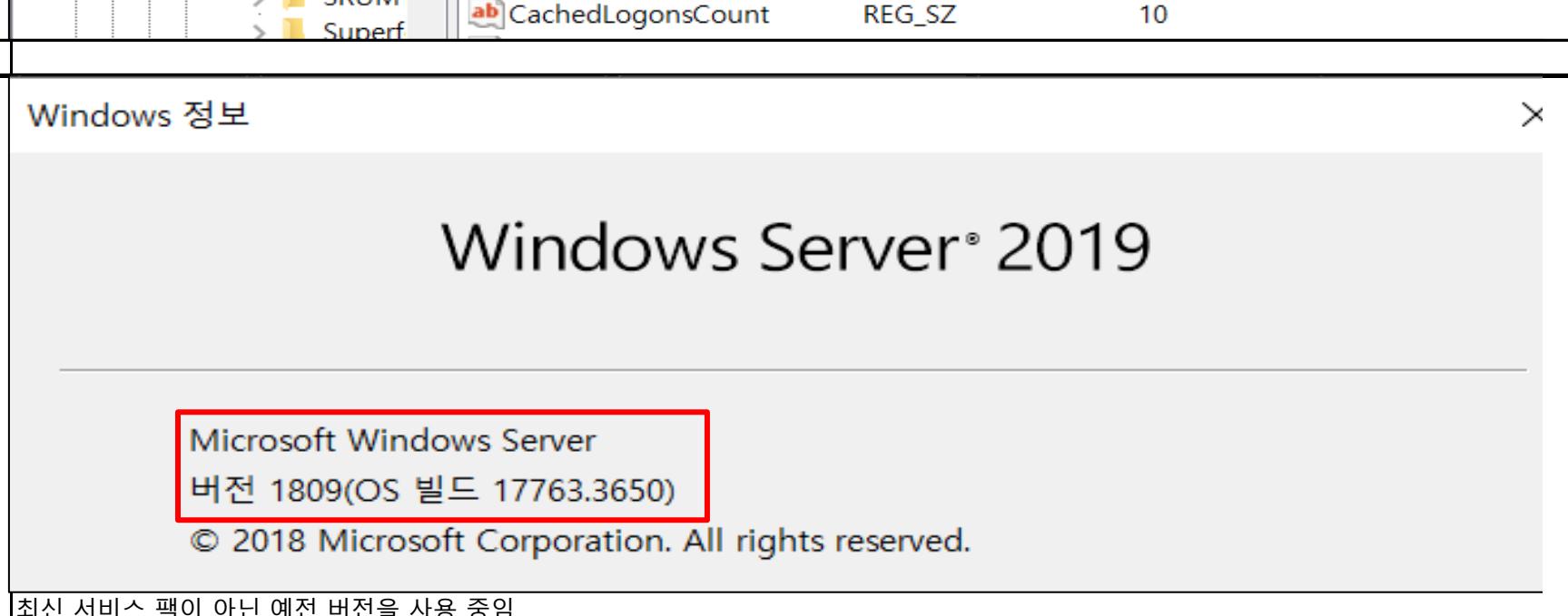
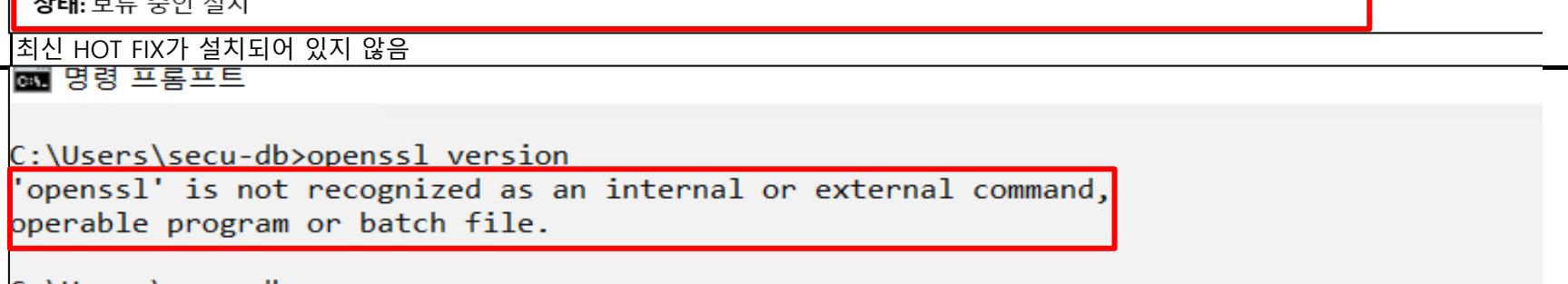
| | | | |
|-------------|--|--|---|
| | | |  |
| 1 | 불필요한 서비스 제거 | 양호 - White List에 포함되지 않거나 시스템 운영 부서와 협의되지 않은 불필요한 서비스가 구동 중이지 않을 경우 취약 - 시스템 운영 부서와 협의되지 않은 불필요한 서비스가 구동 중일 경우, 서버 진단 시 서비스 담당자 측 추가 확인을 거쳐 불필요한 서비스로 식별되는 경우 |  |
| 2 | 터미널 서비스 암호화 수준 설정 | 양호 - 터미널 서비스를 사용하지 않거나 사용 시 암호화 수준을 "클라이언트 호환 가능" 이상으로 설정한 경우 취약 - 터미널 서비스를 사용하고 암호화 수준을 "낮음"으로 설정한 경우 |  |
| 3. 네트워크 서비스 | 3. NetBIOS 서비스 보안 설정 | 양호 - NetBIOS 서비스를 사용하지 않거나 사용 시 "TCP/IP에서 NetBIOS 사용 안 함"으로 설정한 경우 취약 - NetBIOS 서비스를 사용하고 "TCP/IP에서 NetBIOS 사용 안 함"으로 설정하지 않은 경우 |  |
| | 4. 터미널 서비스 Time Out 설정 | 양호 - 터미널 서비스를 사용하지 않거나, 원격 제어 시 Timeout 제어 설정을 적용한 경우 취약 - 원격 제어 시 Timeout 제어 설정을 적용하지 않은 경우 |  |
| 4. 주요 응용 설정 | 1. Telnet 서비스 보안 설정 | ※ 해당 OS는 체크리스트에 포함하지 않음. |  |
| | 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 |  |
| 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 |  |

| | | | |
|---|--------------------|--|--|
| | | <p>양호 - 해당 디렉터리의 접근 권한에 Users / Everyone 그룹이 없는 경우 취약 - 해당 디렉터리의 접근 권한에 Users / Everyone 그룹이 있는 경우</p> | <p>취약</p>   <p>애플리케이션 로그 파일에 Users 그룹이 포함되어 있음</p> |
| 2 | 화면 보호기 설정 | <p>양호 - 화면보호기를 설정하고, 암호를 사용하며, 대기 시간이 5분일 경우 취약 - 화면보호기가 설정되어 있지 않거나, 암호를 사용하지 않거나, 대기시간이 5분 초과 일 경우</p> | <p>취약</p>  <p>화면보호기 및 암호 잠금 설정이 활성화되어 있지 않음</p> |
| 3 | 이벤트 뷰어 설정 | <p>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</p> | <p>양호</p>  |
| 4 | 로그인 시 경고 메시지 표시 설정 | <p>양호 - 로그인 시 경고 메시지가 뜨는 경우 취약 - 로그인 시 경고 메시지가 뜨지 않을 경우</p> | <p>취약</p>  <p>LegalNoticeCaption 및 LegalNoticeText 값이 비어 있어 로그인 시 경고 메시지가 뜨지 않음</p> |

| | | | |
|--------------|-------------------------------------|----|---|
| | | | |
| 5 | 마지막 로그온 사용자 계정 숨김 | 취약 |  <p>레지스트리 편집기 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Windows\System 이름 종류 데이터 ab(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) highlighted DSCAutomation... REG_DWORD 0x00000002 (2) EnableCursorSu... REG_DWORD 0x00000001 (1) EnableFullTrustC REG_DWORD 0x00000002 (2) RunOnce 레지스트리 DontDisplayLastUserName 값이 0으로 설정되어 있음</p> |
| 6 | 로그온 하지 않은 사용자 시스템 종료 방지 | 취약 |  <p>레지스트리 편집기 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Windows\System 이름 종류 데이터 ab(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) EnableUwpStart... REG_DWORD 0x00000000 (0) EnableVirtualiza... REG_DWORD 0x00000001 (1) legalnoticecapti... REG_SZ legalnoticetext REG_SZ PromptOnSecur... REG_DWORD 0x00000001 (1) sfcoreception REG_DWORD 0x00000000 (0) shutdownwithoutl... REG_DWORD 0x00000001 (1) highlighted 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</p> |
| 7 | 로컬 감사 정책 설정 | 취약 |  <p>로컬 보안 정책 파일(F) 동작(A) 보기(V) 도움말(H) 보안 설정 정책 보안 설정 개체 액세스 감사 계정 관리 감사 계정 로그온 이벤트 감사 권한 사용 감사 디렉터리 서비스 액세스 감사 로그온 이벤트 감사 시스템 이벤트 감사 정책 변경 감사 프로세스 주적 감사</p> <p>개체 액세스 감사, 계정 관리 감사, 계정 로그온 이벤트 감사, 권한 사용 감사, 로그온 이벤트 감사 항목에 대해 성공 및 실패 이벤트에 대한 감사 설정이 되어 있지 않음</p> |
| 5. 시스템 보안 설정 | 8. 가상 메모리 페이지 파일 삭제 설정 | 취약 |  <p>레지스트리 편집기 파일(F) 편집(E) 보기(V) 즐겨찾기(A) 도움말(H) 컴퓨터\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Memory Management 이름 종류 데이터 ab(기본값) REG_SZ (값 설정 안 됨) ClearPageFileAt... REG_DWORD 0x00000000 (0) highlighted da56a5e4-287c... REG_DWORD 0x00000004 (4) DisablePagingEx... REG_DWORD 0x00000000 (0) ExistingPageFiles REG_MULTI... W??WC:\pagefile.sys FeatureSettings REG_DWORD 0x00000001 (1) ClearPageFileAtShutdown 값이 0으로 설정되어 있음</p> |
| | 9. Lan Manager 인증 수준 | 취약 |  <p>로컬 보안 정책 파일(F) 동작(A) 보기(V) 도움말(H) 보안 설정 네트워크 보안: LAN Manager 인증 수준 속성 로컬 보안 설정 설명 네트워크 보안: LAN Manager 인증 수준 highlighted 이 설정을 수정하면 클라이언트, 서비스 및 응용 프로그램과의 호환성에 영향을 미칠 수 있습니다. 자세한 내용은 네트워크 보안: LAN Manager 인증 수준(를) 참고하십</p> <p>"LAN Manager 인증 수준" 정책이 미설정되어 있음</p> |
| | 10. Everyone 사용 권한을 익명 사용자에게 적용 안 함 | 양호 |  <p>로컬 보안 정책 파일(F) 동작(A) 보기(V) 도움말(H) 보안 설정 네트워크 액세스: Everyone 사용 권한을 익명 사용자에게 적용 속성 로컬 보안 설정 설명 네트워크 액세스: Everyone 사용 권한을 익명 사용자에게 적용 ○ 사용(E) ● 사용 안 함(S) highlighted</p> |

| | | | |
|----|----------------------------|---|--|
| 11 | 이동식 미디어 포맷 및 꺼내기 admin만 적용 | <p>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</p> <p style="color: red;">취약</p> |  <p>"이동식 미디어 포맷 및 꺼내기 허용" 정책이 미설정되어 있음</p> |
| 12 | 세션 연결 끊기 전 유회 시간 설정 | <p>양호 - "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책을 "사용"으로 설정하고 "세션 연결을 중단하기 전에 필요한 유회 시간" 정책이 "15분"으로 설정되어 있을 경우 취약 - "로그온 시간이 만료되면 클라이언트 연결 끊기" 정책이 "사용 안 함"으로 설정되어 있거나 "세션 연결을 중단하기 전에 필요한 유회 시간" 정책이 "15분"으로 설정되어 있지 않을 경우</p> <p style="color: green;">양호</p> |  |
| 13 | 예약된 작업 의심스런 명령어나 파일 점검 | <p>양호 - 예약된 작업에 불필요한 명령어나 파일이 있는지 확인하는 경우 취약 - 예약된 작업에 불필요한 명령어나 파일이 있는지 확인하지 않는 경우</p> <p style="color: green;">양호</p> |  |
| 14 | 원격 시스템 종료 권한 설정 | <p>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</p> <p style="color: green;">양호</p> |  |

| | | | |
|----------------|--|--|---|
| | | | |
| 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 |  |
| 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 |  |
| 6. 바이러스 진단 | 1 백신 프로그램 설치 | 양호 - 바이러스 백신 프로그램이 설치되어 있는 경우 취약 - 바이러스 백신 프로그램이 설치되어 있지 않은 경우 |  |
| | 2 최신 엔진 업데이트 | 양호 - 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있을 경우 취약 - 바이러스 백신 프로그램의 최신 엔진 업데이트가 설치되어 있진 않은 경우 |  |
| 7. 레지스트리 보안 설정 | 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 |  |
| | 2 Null Session 설정 | 양호 - 해당 레지스트리의 "RestrictAnonymous" 값이 "2"로 설정되어 있는 경우 취약 - 해당 레지스트리의 "RestrictAnonymous" 값이 "2"가 아니거나 설정되지 않은 경우 |  |

| | | | | |
|-----------|-------------------------------|---|------|---|
| | 3 Remote Registry Service 설정 | 양호 - Remote Registry Service 가 종지되어 있을 경우 취약 - Remote Registry Service 가 사용중인 경우 | 취약 |  |
| | 4 RDS(Remote Data Service) 제거 | ※ 해당 OS는 체크리스트에 포함하지 않음. | N/A | |
| | 5 AutoLogon 제한 설정 | 양호 - "AutoAdminLogon" 값이 없거나 "0"으로 설정되어 있는 경우 취약 - "AutoAdminLogon" 값이 "1"로 설정되어 있는 경우 | 양호 |  |
| | 6 DOS 공격에 대한 방어 레지스터리 설정 | ※ 해당 OS는 체크리스트에 포함하지 않음. | N/A | |
| 8. 보안패치 | 1 최신 서비스 팩 적용 | 양호 - 최신 서비스 팩이 설치되어 있는 경우 취약 - 최신 서비스 팩이 설치 되어 있지 않은 경우 | 취약 |  |
| | 2 최신 HOT FIX 적용 | 양호 - 최신 HOT FIX가 설치되어 있는 경우 취약 - 최신 HOT FIX가 설치되어 있지 않은 경우 | 취약 |  |
| 9. 이슈 취약점 | 1 OpenSSL 취약점 | 양호 - OpenSSL을 사용하지 않거나 최신버전의 OpenSSL을 설치하여 운영하는 경우 취약 - 최신버전의 OpenSSL을 설치하여 운영하지 않는 경우 | 양호 |  |
| 점검결과 | 보안 적용율 (양호항목 / 진단항목) % | | 23.0 | 46.5% |