

수업 내용 정리 보고서

작성일: 2026년 7월 1일

챕터 구성

- 계정 및 암호 정책 보안
- 시스템 레지스트리 및 LSA 보안 구성
- 사용자 권한 및 접근 제어 관리
- 보안 감사 및 취약점 점검 리스트

계정 및 암호 정책 보안

운영체제의 보안에서 **계정 및 암호 정책**은 시스템 접근 제어의 가장 기초적이면서도 중요한 요소입니다. 계정은 시스템을 사용하는 '주체'를 식별하고, 암호는 그 주체의 '신원'을 확인하는 수단입니다. 이 두 요소가 부실하게 관리될 경우, 공격자는 무차별 대입 공격(Brute-force Attack)이나 사전 공격(Dictionary Attack)을 통해 시스템 권한을 탈취할 수 있습니다. 본 보고서에서는 제공된 설정 자료를 바탕으로 계정 관리, 암호 정책, 접근 제어 관점에서의 보안 상태를 분석합니다.

1. 계정 관리 보안 (Account Management)

계정 관리 보안의 핵심은 기본 제공되는 관리자 계정의 노출을 최소화하고, 불필요한 계정(Guest 등)의 사용을 엄격히 제한하는 것입니다.

- **관리자 계정 명칭 변경 (W-01):** 공격자는 일반적으로 시스템에 존재하는 기본 관리자 계정명(예: Administrator)을 타겟으로 공격을 시도합니다. 설정 자료의 NewAdministratorName = "Administrator"는 기본값을 그대로 사용하고 있어, 공격자가 계정명을 예측하기 매우 쉬운 **[취약]** 상태입니다.
- **Guest 계정 관리 (W-02):** Guest 계정은 인증되지 않은 사용자에게 제한적인 권한을 부여하는 계정으로, 보안상 비활성화하는 것이 원칙입니다.
 - **계정 상태:** EnableGuestAccount = 0으로 설정되어 계정이 비활성화되어 있으므로 **[양호]**합니다.
 - **로그온 권한:** 하지만 SeInteractiveLogonRight(로컬 로그인 권한) 항목에 Guest가 포함되어 있습니다. 이는 계정이 비활성화되어 있더라도 정책적으로 권한이 열려 있는 상태이므로 보안 설정의 일관성 측면에서 주의가 필요합니다.

2. 암호 정책 보안 (Password Policy)

암호 정책은 암호의 '강도(Strength)'와 '유효 기간(Lifespan)'을 결정합니다. 강도가 낮은 암호는 쉽게 해독되며, 유효 기간이 없는 암호는 한 번 탈취되면 영구적으로 악용될 위험이 있습니다.

항목	설정값	보안 평가	상세 내용 및 위험성
암호 최소 길이 (W-07)	0	[취약]	최소 길이가 0이므로 단일 문자만으로도 암호 설정이 가능하여 매우 위험함.
암호 복잡성 (W-07)	0 (해제)	[취약]	대소문자, 숫자, 특수문자 조합을 강제하지 않아 단순한 암호 사용 가능성 높음.
최소 암호 사용 기간 (W-08)	0	[취약]	암호를 변경하자마자 즉시 다시 변경할 수 있어, 정책을 우회하여 이전 암호를 재사용하기 용이함.
최대 암호 사용 기간 (W-08)	42일	[양호]	정기적인 암호 변경을 유도하고 있으므로 권장 사항을 충족함.
최근 암호 기억 (W-08)	0	[취약]	이전 암호를 기억하지 않으므로, 사용자가 보안 강도가 낮은 암호로 계속 회전하며 재사용 가능함.
암호 저장 방식 (W-06)	0 (해제)	[양호]	해독 가능한 평문(Cleartext)으로 저장하지 않으므로 저장된 암호 탈취 시 피해 최소화.

3. 계정 잠금 및 익명 접근 제어

비정상적인 접근 시도를 차단하고, 시스템 정보의 노출을 막기 위한 제어 설정입니다.

- **계정 잠금 임계값 (W-05):** LockoutBadCount = 10으로 설정되어 있습니다. 이는 10회 로그인 실패 시 계정을 잠그는 설정입니다. 일반적으로 5회 이하를 권장하므로, 공격자가 시도할 수 있는 기회가 상대적으로 많을 수 있습니다.
- **익명 사용자 접근 제한 (W-10):**
 - **LSA 설정:** EveryoneIncludesAnonymous = 0으로 설정되어 익명 사용자가 Everyone 그룹에 포함되지 않도록 되어 있어 **[양호]**합니다.
 - **추가 제한:** 그러나 RestrictAnonymous = 0(허용)으로 설정되어 있습니다. 이는 익명 연결에 대한 추가적인 제한이 없음을 의미하며, 공격자가 시스템 정보를 수집하는 통로가 될 수 있어 **[취약]**합니다. (1 또는 2로 설정 권장)

4. 특수 권한 할당 (Privilege Rights)

사용자나 서비스가 시스템에서 수행할 수 있는 특수 작업(예: 백업, 로그인, 드라이버 로드 등)을 정의하는 권한입니다. 과도한 권한 부여는 권한 상승(Privilege Escalation) 공격의 대상이 됩니다.

주의사항: SID(Security Identifier) 분석

설정값에 나타나는 S-1-5-xxx 형태의 값은 사용자를 식별하는 고유 번호(SID)입니다. 예를 들어, S-1-5-32-544는 Administrators 그룹을 의미하며, S-1-1-0은 Everyone 그룹을 의미합니다. 특정 권한에 이러한 광범위한 SID가 포함되어 있는지 확인하는 것이 실무 점검의 핵심입니다.

- **네트워크 로그인 권한:** SeNetworkLogonRight에 S-1-1-0(Everyone)이 포함되어 있는지 확인이 필요합니다.
- **로컬 로그인 권한:** SeInteractiveLogonRight에 Guest 계정이 명시되어 있어, 앞서 언급한 계정 관리 보안 이슈와 맞물려 보안 약점으로 작용할 수 있습니다.

실무 점검 및 대응 가이드

시스템 관리자는 위 분석 결과를 바탕으로 다음과 같은 순서로 보안 설정을 강화해야 합니다.

1. **계정 식별성 강화:** Administrator 계정명을 예측 불가능한 이름으로 즉시 변경합니다.
2. **암호 강도 상향:** 최소 길이를 8자 이상으로 설정하고, 복잡성 요구 사항을 활성화하며, 암호 재사용 제한(최근 암호 기억)을 설정합니다.

3. **접근 차단 정교화:** 익명 연결 제한(RestrictAnonymous)을 활성화하고, 계정 잠금 임계값을 낮추어 무차별 대입 공격에 대비합니다.
4. **최소 권한 원칙 적용:** 특수 권한(Privilege Rights) 목록을 검토하여 Guest나 Everyone과 같은 광범위한 그룹이 불필요한 권한을 가지고 있지 않은지 점검합니다.

[확인 질문]

- 암호 복잡성 설정이 해제되었을 때 발생할 수 있는 가장 큰 보안 위험은 무엇인가?
- RestrictAnonymous 설정이 0(허용)일 때 공격자가 얻을 수 있는 정보는 무엇인가?
- 계정 잠금 임계값(LockoutBadCount)을 낮추는 것이 보안과 운영 편의성 사이에서 어떤 트레이드오프(Trade-off)를 가지는가?

시스템 레지스트리 및 LSA 보안 구성

운영체제의 보안을 강화하기 위해서는 단순히 백신 프로그램을 설치하는 것을 넘어, 시스템의 핵심 구성 요소인 **레지스트리(Registry)**와 **LSA(Local Security Authority, 로컬 보안 인증)**의 설정을 정밀하게 관리해야 합니다. 시스템 레지스트리는 운영체제의 설정 정보를 담고 있는 데이터베이스이며, LSA는 사용자의 인증 및 보안 정책을 관리하는 핵심 프로세스입니다. 본 장에서는 제공된 보안 설정 데이터를 바탕으로 계정 관리, 암호 정책, 익명 접근 제어, 그리고 사용자 권한 할당(Privilege Rights) 측면에서의 보안 취약점을 분석합니다.

1. 계정 및 암호 정책 관리 (System Access)

계정 및 암호 정책은 시스템에 접근하는 사용자의 신원을 확인하고, 탈취된 계정의 오남용을 방지하는 첫 번째 방어선입니다. 보안 설정 데이터 분석 결과, 암호의 강도와 계정의 식별성 측면에서 다수의 취약점이 발견되었습니다.

주요 점검 항목 및 분석 결과:

- 암호 복잡성 및 길이 (W-07):** MinimumPasswordLength = 0 및 PasswordComplexity = 0으로 설정되어 있습니다. 이는 암호의 최소 길이를 제한하지 않고 복잡성(대소문자, 숫자, 특수문자 조합)을 요구하지 않음을 의미합니다. 이 경우 공격자는 **무차별 대입 공격(Brute-force Attack)**이나 **사전 공격(Dictionary Attack)**을 통해 매우 쉽게 암호를 알아낼 수 있습니다.
- 암호 사용 기간 관리 (W-08):** MinimumPasswordAge = 0으로 설정되어 있어, 사용자가 암호를 변경한 직후 바로 다시 변경할 수 있습니다. 이는 암호 변경 정책을 우회하여 이전 암호를 계속 사용하려는 시도를 허용할 수 있어 보안상 취약합니다. 또한 PasswordHistorySize = 0 설정은 이전에 사용했던 암호를 기억하지 않으므로, 사용자가 보안성이 낮은 이전 암호로 즉시 회귀할 수 있는 환경을 제공합니다.
- 기본 계정 관리 (W-01, W-02):** NewAdministratorName = "Administrator"로 설정되어 관리자 계정명이 기본값 그대로 유지되고 있습니다. 공격자는 시스템 침투 시 가장 먼저 'Administrator'라는 이름을 타겟으로 삼기 때문에, 계정명을 변경하는 것이 권장됩니다. 반면, EnableGuestAccount = 0(Guest 계정 비활성화) 설정은 적절하게 관리되고 있습니다.

[보안 설정 요약표]

항목	설정값	상태	보안 영향
최소 암호 길이 (MinimumPasswordLength)	0	취약	단일 문자 암호 사용 가능 (Brute-force에 취약)
암호 복잡성 (PasswordComplexity)	0	취약	조합 규칙 미적용 (사전 공격에 취약)
관리자 계정명 (NewAdministratorName)	"Administrator"	취약	기본 계정명 노출로 인한 공격 표적화
최대 암호 사용 기간 (MaximumPasswordAge)	42	양호	주기적인 암호 교체 유도
Guest 계정 상태 (EnableGuestAccount)	0 (비활성)	양호	불필요한 Guest 계정 활용 차단

2. LSA 및 레지스트리를 통한 익명 접근 제어

LSA(Local Security Authority)는 시스템의 보안 정책을 강제하고 사용자의 로그인 과정을 관리합니다. 레지스트리 값을 통해 익명 사용자의 접근 범위를 제한함으로써 시스템 내부 정보의 유출을 막을 수 있습니다.

핵심 레지스트리 보안 분석:

- 익명 연결 제한 (W-10):** RestrictAnonymous = 0으로 설정되어 있습니다. 이는 익명 사용자가 시스템의 계정 정보나 공유 자원에 접근할 수 있도록 허용하는 설정입니다. 보안을 위해서는 이 값을 1 또는 2로 설정하여 익명 연결에 대한 추가적인 제한을 가해야 합니다. EveryoneIncludesAnonymous = 0 설정은 익명 사용자가 'Everyone' 그룹에 포함되지 않도록 차단하고 있으나, RestrictAnonymous 설정이 허용되어 있어 전체적인 보안 수준은 낮습니다.
- 암호 저장 방식 (W-06):** ClearTextPassword = 0 설정은 평문(Clear Text)으로 암호를 저장하지 않음을 의미하며, 이는 암호 해독 공격으로부터 안전한 **암호화**한 상태입니다.

주의사항: RestrictAnonymous 설정을 변경할 경우, 일부 오래된 네트워크 프로토콜이나 서비스가 익명 인증을 요구하여 정상적인 통신이 차단될 수 있습니다. 따라서 적용 전 반드시 서비스 영향도를 검토해야 합니다.

3. 사용자 권한 할당 (Privilege Rights)

사용자 권한 할당(User Rights Assignment)은 특정 사용자나 그룹이 시스템에서 수행할 수 있는 특수 작업(예: 시스템 시간 변경, 드라이버 로드, 로컬 로그인 등)을 정의합니다. 이 권한은 **SID(Security Identifier)**라는 고유 식별자를 통해 관리됩니다.

권한 설정 분석 및 취약점:

- **로컬 로그인 권한 (W-02):** SeInteractiveLogonRight 항목에 Guest 계정이 포함되어 있습니다. 이는 Guest 계정이 시스템에 직접 로그인하여 상호작용할 수 있음을 의미합니다. Guest 계정은 권한이 제한적이라 하더라도 시스템에 물리적으로 접근할 수 있는 통로가 되므로, 이를 로컬 로그인 허용 목록에서 제거해야 합니다.
- **네트워크 접근 및 거부 설정 (W-02, W-10):** SeDenyNetworkLogonRight = Guest 및 SeDenyInteractiveLogonRight = Guest 설정은 Guest 계정의 네트워크 및 로컬 로그인을 명시적으로 **거부**하고 있습니다. 이는 매우 적절한 보안 조치이며, 앞서 언급된 SeInteractiveLogonRight에 Guest가 포함된 설정과 충돌할 여지가 있으므로 권한 우선순위(Deny가 Allow보다 우선함)를 확인하고 설정을 정교화할 필요가 있습니다.
- **SID 식별 가이드:** 데이터에 등장하는 S-1-5-32-544는 'Administrators' 그룹을 의미하며, S-1-5-32-545는 'Users' 그룹을 의미합니다. 이러한 식별자를 통해 권한이 적절한 관리자 그룹에만 할당되어 있는지 확인하는 것이 실무의 핵심입니다.

실무 및 시험 대비 점검 포인트

시스템 보안 설정 감사(Audit)를 수행할 때는 다음의 순서와 기준을 적용하여 판단합니다.

1. **계정 식별성 확인:** 기본 관리자(Administrator) 및 Guest 계정의 이름이 변경되었는가? 계정은 비활성화되어 있는가?
2. **암호 정책 강도 검증:** 최소 길이가 충분한가(예: 8자 이상)? 복잡성 설정이 활성화되어 있는가? 이전 암호 재사용을 막기 위한 이력 관리(History)가 설정되어 있는가?
3. **익명 접근 차단 여부:** 레지스트리의 RestrictAnonymous 값이 1 이상인가? 익명 사용자가 시스템 정보에 접근할 수 없는 구조인가?
4. **권한 오남용 방지:** SeInteractiveLogonRight(로컬 로그인)나 SeNetworkLogonRight(네트워크 로그인)에 일반 사용자나 Guest 계정이 과도하게 포함되어 있지 않은가?

[학습 확인 질문]

- 암호 복잡성>Password Complexity)이 0으로 설정되었을 때 발생할 수 있는 가장 큰 보안 위협은 무엇인가?
- RestrictAnonymous 레지스트리 값을 0에서 1로 변경할 때 얻을 수 있는 보안 이점은 무엇인가?
- 사용자 권한 설정에서 'Deny(거부)' 권한과 'Allow(허용)' 권한이 충돌할 경우, Windows 시스템은 어떤 권한을 우선시하는가?

사용자 권한 및 접근 제어 관리

사용자 권한 및 접근 제어(Access Control)는 시스템의 자원(파일, 프로세스, 네트워크 등)에 대해 "누가(Who)", "어떤 권한으로(What)", "어떻게(How)" 접근할 수 있는지를 정의하는 보안의 핵심 요소입니다. 이번 학습에서는 시스템 설정 파일에 기록된 실제 값들을 바탕으로, 암호 정책, 계정 관리, 특권 권한(Privilege Rights), 그리고 익명 접속 제한 설정이 보안에 어떤 영향을 미치는지 분석합니다.

1. 암호 정책 및 계정 잠금 관리

암호 정책은 사용자의 신원을 확인하는 가장 기본적인 수단입니다. 강력한 암호 정책은 무작위 대입 공격(Brute-force Attack)이나 사전 공격(Dictionary Attack)으로부터 계정을 보호합니다. 분석 결과, 현재 설정은 여러 항목에서 취약점이 발견되었습니다.

항목	설정 값	보안 상태	설명 및 영향
최소 암호 사용 기간 (MinimumPasswordAge)	0	취약	암호를 변경한 후 즉시 다시 변경할 수 있어, 이전 암호를 재사용하려는 시도를 막지 못합니다.
최소 암호 길이 (MinimumPasswordLength)	0	취약	단일 문자만으로도 암호 설정이 가능하여 보안성이 매우 낮습니다.
암호 복잡성 설정 (PasswordComplexity)	0	취약	대소문자, 숫자, 특수문자 조합을 강제하지 않아 추측하기 쉬운 암호를 사용할 수 있습니다.
최근 암호 기억 (PasswordHistorySize)	0	취약	이전에 사용했던 암호를 기억하지 않으므로, 사용자가 동일한 암호를 반복해서 사용할 수 있습니다.
계정 잠금 임계값 (LockoutBadCount)	10	보통	10회 실패 시 잠금이 설정되어 있으나, 일반적으로 5회 이하로 설정하여 공격 노출을 줄이는 것이 권장됩니다.

실무 포인트: 암호 정책을 설정할 때는 '최소 암호 길이'와 '복잡성'을 우선적으로 확보해야 하며, '최근 암호 기억' 설정을 통해 사용자가 보안성이 낮은 구 암호를 다시 사용하는 것을 원천 차단해야 합니다.

2. 계정 관리 및 기본 계정 보호

시스템에는 운영체제 설치 시 기본적으로 생성되는 Administrator(관리자) 및 Guest(게스트) 계정이 존재합니다. 공격자는 이러한 기본 계정 명칭을 타겟으로 공격을 시작하므로, 이를 변경하거나 비활성화하는 것이 중요합니다.

- **Administrator 계정명 변경 (W-01):** 현재 NewAdministratorName = "Administrator"로 기본값이 유지되고 있습니다. 이는 공격자가 관리자 계정 이름을 이미 알고 있음을 의미하므로 **취약**한 상태입니다.
- **Guest 계정 관리 (W-02):** EnableGuestAccount = 0으로 설정되어 계정이 비활성화된 상태는 **양호**합니다. 다만, NewGuestName 설정 영역을 통해 이름을 변경하는 관리적 조치가 병행되어야 합니다.

3. 특권 권한(Privilege Rights) 할당 분석

특권 권한이란 특정 사용자가 시스템의 민감한 작업(예: 드라이버 로드, 시스템 시간 변경, 로그 파일 읽기 등)을 수행할 수 있도록 허용된 권한을 의미합니다. 권한 관리는 '최소 권한의 원칙(Principle of Least Privilege)'에 따라 꼭 필요한 사용자에게만 최소한의 권한을 부여해야 합니다.

분석된 설정 중 보안상 치명적인 오류는 다음과 같습니다.

[주의] 로컬 로그온 권한 내 Guest 포함 문제

SeInteractiveLogonRight = vmware, Guest, ... 설정에서 **Guest** 계정이 로컬 로그온(Interactive Logon) 권한을 가지고 있습니다. 이는 게스트 계정으로 시스템에 직접 접속할 수 있음을 의미하므로 매우 **취약한** 설정입니다.

반면, 다음과 같은 설정은 적절하게 관리되고 있습니다.

- **SeDenyNetworkLogonRight = Guest:** 게스트 계정의 네트워크 로그온을 명시적으로 거부하고 있어 **양호**합니다.
- **SeDenyInteractiveLogonRight = Guest:** 게스트 계정의 로컬 로그온을 거부하도록 설정되어 있으나, 앞서 언급한 SeInteractiveLogonRight와의 충돌 여부를 반드시 확인해야 합니다. (명시적 거부 권한이 허용 권한보다 우선하는 경우가 많으나, 설정의 일관성이 중요합니다.)

4. 시스템 익명성 및 접근 제한

익명 사용자가 시스템 정보(사용자 목록, 공유 자원 등)를 수집하지 못하도록 제한하는 설정은 공격의 전 단계인 '정찰(Reconnaissance)'을 차단하는 데 필수적입니다.

익명 연결 제한 (W-10):

레지스트리 값 MACHINE\System\CurrentControlSet\Control\Lsa\RestrictAnonymous = 0은 익명 연결에 대한 추가 제한을 **허용**하고 있음을 나타냅니다. 이는 공격자가 계정 이름이나 공유 폴더 목록을 익명으로 조회할 수 있게 하므로 보안상 매우 **취약**합니다. 일반적으로 이 값은 1 또는 2로 설정하여 익명 사용자의 접근을 엄격히 제한해야 합니다.

네트워크 접근 권한 (W-10):

SeNetworkLogonRight에 S-1-1-0 (Everyone) 그룹이 포함되어 있는지 확인하는 과정이 필요합니다. Everyone 그룹이 네트워크 접근 권한을 가지게 되면, 인증되지 않은 광범위한 사용자가 시스템에 접근을 시도할 수 있는 통로가 됩니다.

5. 보안 감사 정책 (Event Audit)의 결여

모든 보안 설정만큼 중요한 것이 '**감사(Audit)**'입니다. 감사는 시스템 내에서 발생하는 로그인 성공/실패, 파일 접근, 권한 변경 등의 이벤트를 기록하는 행위입니다.

현재 설정 자료를 보면 AuditSystemEvents, AuditLogonEvents를 포함한 모든 감사 항목이 **0**으로 설정되어 있습니다. 이는 시스템에 침입이 발생하거나 권한 오용이 일어나더라도 **어떠한 흔적도 남지 않음**을 의미합니다. 즉, 침해 사고 발생 시 원인 파악과 사후 대응이 불가능한 상태이므로 매우 심각한 보안 결함입니다.

학습 요약 및 실무 점검 체크리스트

시스템 보안 강화를 위해 관리자는 다음 항목을 우선순위에 따라 점검해야 합니다.

1. **암호 정책 강화:** 최소 길이(8자 이상), 복잡성 활성화, 최소 사용 기간 설정, 이전 암호 기억 기능을 반드시 적용했는가?
2. **기본 계정 보호:** Administrator 계정명을 변경했는가? Guest 계정은 비활성화되어 있는가?
3. **권한 최소화:** SeInteractiveLogonRight 등 특권 권한 목록에 Guest나 Everyone과 같은 광범위한 그룹이 포함되어 있지 않은가?
4. **익명성 차단:** RestrictAnonymous 레지스트리 값이 1 또는 2로 설정되어 익명 사용자의 정보 수집을 차단하고 있는가?
5. **가시성 확보:** 로그인, 로그아웃, 계정 관리, 객체 접근 등에 대한 감사 정책(Audit Policy)이 활성화되어 로그가 생성되고 있는가?

[시험/실무 포인트]

설정 파일에서 S-1-5-32-544는 **Administrators** 그룹을, S-1-1-0은 **Everyone** 그룹을 나타내는 SID(Security Identifier)입니다. 권한 설정 값을 해석할 때 이 SID들이 어떤 그룹에 부여되었는지를 파악하는 것이 문제 풀이와 실무의 핵심입니다.

보안 감사 및 취약점 점검 리스트

보안 감사는 시스템의 설정 상태가 보안 정책 및 가이드라인을 준수하고 있는지 확인하는 과정이며, 취약점 점검은 공격자가 이용할 수 있는 약점을 식별하는 행위입니다. Windows 운영체제 보안 감사에서는 주로 **계정 정책(Account Policy)**, **권한 할당(User Rights Assignment)**, **시스템 레지스트리(Registry)** 설정을 점검하여 공격 표면(Attack Surface)을 최소화하는 데 집중합니다.

1. 암호 정책 점검 (Password Policy)

암호 정책은 사용자 인증 단계에서 무차별 대입 공격(Brute-force Attack)이나 사전 공격(Dictionary Attack)을 방어하기 위한 핵심적인 통제 항목입니다. 암호의 수명과 복잡성을 관리하여 계정 탈취 위험을 낮춥니다.

점검 항목	설정 값 (예시)	판단 기준 및 보안 영향
최소 암호 사용 기간 (MinimumPasswordAge)	0	[취약] 사용자가 암호를 변경한 후 즉시 다시 변경할 수 있어, 암호 히스토리 기능을 우회하여 이전 암호를 재사용할 수 있습니다. 보통 1일 이상을 권장합니다.
최대 암호 사용 기간 (MaximumPasswordAge)	42	[양호] 일정 기간마다 암호를 강제로 변경하게 함으로써, 혹시 모를 암호 유출 시 피해 지속 기간을 제한합니다.
암호 최소 길이 (MinimumPasswordLength)	0	[취약] 암호 길이를 제한하지 않으면 단일 문자로도 설정이 가능해져 공격자가 암호를 알아내기가 매우 쉽습니다.
암호 복잡성 설정 (PasswordComplexity)	0 (해제)	[취약] 영문 대소문자, 숫자, 특수문자 조합을 강제하지 않으면 예측 가능한 단순한 암호가 사용될 위험이 큼니다.
최근 암호 기억 (PasswordHistorySize)	0	[취약] 이전에 사용했던 암호를 저장하지 않으면 사용자가 바로 직전에 썼던 암호를 다시 사용할 수 있습니다.

실무 포인트: 암호 정책 설정 시 '최소 사용 기간'과 '최근 암호 기억'을 함께 검토해야 합니다. 최소 사용 기간이 너무 길면 사용자가 불편을 느껴 포스트잇에 암호를 적어두는 등의 보안 사고가 발생할 수 있으므로, 조직의 운영 환경에 맞춘 균형 잡힌 설정이 필요합니다.

2. 계정 및 로그인 제어 (Account & Logon Control)

기본적으로 생성되는 관리자 계정이나 게스트(Guest) 계정은 공격자의 주요 타겟이 됩니다. 이들의 이름을 변경하거나 상태를 비활성화하는 것은 공격자가 침투 경로를 찾는 '정찰(Reconnaissance)' 단계를 방해하는 효과가 있습니다.

- **기본 관리자 계정명 변경 (W-01):** NewAdministratorName이 "Administrator"로 유지되어 있다면, 공격자는 사용자 이름을 찾는 수고 없이 바로 암호 크래킹을 시도할 수 있습니다.
- **게스트 계정 관리 (W-02):** EnableGuestAccount = 0 설정은 게스트 계정을 비활성화한 상태로, 보안상 [양호]합니다. 다만, 권한 할당(Privilege Rights) 단계에서 게스트 계정에 로컬 로그인 권한이 부여되어 있는지 별도로 확인해야 합니다.
- **계정 잠금 임계값 (W-05):** LockoutBadCount는 잘못된 암호 입력 시 계정을 잠그는 횟수입니다. 설정값(예: 10회)이 존재하더라도 보안 권고 수준(보통 5회 이하)보다 높다면 정책 재검토가 필요합니다.

3. 시스템 레지스트리 및 LSA 보안 (System Hardening)

LSA(Local Security Authority)는 Windows의 인증 프로세스를 담당하는 핵심 구성 요소입니다. 이와 관련된 레지스트리 설정은 익명 사용자의 접근을 제한하고 시스템의 무결성을 유지하는 데 결정적인 역할을 합니다.

주요 점검 사항:

- **익명 연결 제한 (W-10):** RestrictAnonymous 값이 0인 경우, 익명 사용자가 시스템 정보에 접근할 수 있어 보안에 [취약]합니다. 보안 강화를 위해 1 또는 2로 설정하여 익명 사용자의 정보 조회를 제한해야 합니다.
- **Everyone 그룹 포함 여부 (W-10):** EveryoneIncludesAnonymous가 0(해제)인 경우, 익명 사용자가 Everyone 그룹의 권한을 이용하지 못하므로 [양호]합니다.
- **암호 평문 저장 방지 (W-06):** ClearTextPassword = 0 설정은 암호가 해독 가능한 평문 형태로 저장되지 않음을 의미하며, 이는 매우 중요한 [양호] 사례입니다.

4. 권한 할당 점검 (Privilege Rights)

권한 할당은 특정 사용자나 그룹이 시스템에서 수행할 수 있는 작업(로그온, 파일 백업, 드라이버 로드 등)을 정의합니다. 불필요하게 넓은 권한이 부여되어 있는지 확인하는 것이 핵심입니다.

주의해야 할 권한 설정 사례:

- **로컬 로그인 권한 (SeInteractiveLogonRight):** 만약 이 목록에 Guest 계정이 포함되어 있다면, 게스트 계정이 시스템에 직접 로그인할 수 있어 [취약]합니다.
- **네트워크 액세스 권한 (SeNetworkLogonRight):** S-1-1-0(Everyone)과 같은 포괄적인 식별자가 포함되어 있는지 확인해야 합니다. 이는 모든 사용자가 네트워크를 통해 컴퓨터에 접근할 수 있게 하므로 권한 최소화 원칙에 어긋날 수 있습니다.
- **거부 정책(Deny Policy)의 활용:** SeDenyInteractiveLogonRight = Guest와 같이 특정 계정에 대해 명시적으로 '거부' 설정을 하는 것은 허용(Allow) 설정보다 우선순위가 높으므로 매우 강력한 방어 수단이 됩니다.

보안 감사 핵심 체크리스트 (요약)

실무에서 점검을 수행할 때 다음 순서에 따라 결과를 기록하고 조치 계획을 수립하십시오.

1. **인증 보안:** 암호 복잡성, 최소 길이, 히스토리, 사용 기간이 정책에 부합하는가?

2. **계정 관리:** 기본 관리자 계정명이 변경되었는가? 불필요한 Guest 계정은 비활성화되었는가?
3. **시스템 강화:** LSA 설정에서 익명 사용자의 접근(RestrictAnonymous)이 차단되어 있는가?
4. **권한 최소화:** 사용자 권한 할당 목록에 'Everyone'이나 'Guest'와 같은 과도한 권한이 포함되어 있지 않은가?

흔한 실수: "계정 잠금(Lockout) 설정이 되어 있으니 안전하다"라고 판단하는 것은 위험합니다. 잠금 임계값이 너무 높으면 공격자가 충분한 횟수의 로그인 시도를 할 수 있는 시간을 벌어주게 되므로, 반드시 권장되는 수치(예: 5회 이하)와 비교하여 점검해야 합니다.