침입탐지 진단

01.Administrator 계정관리	
양호 기준	관리자 계정이 하나만 존재
진단 현황	별칭 administrators 설명 컴퓨터/도메인에 모든 액세스 권한을 가진 관리자 구성원 ---------- Administrator pc 명령을 잘 실행했습니다.
진단 결과	**양호**

02. Guest 계정관리	
양호 기준	관리자 계정이 비활성화
진단 현황	사용자 이름 Guest 전체 이름 설명 게스트가 컴퓨터/도메인을 액세스하도록 기본 제공된 계정 사용자 설명 국가 코드 000 (시스템 기본값) 활성 계정 아니요 계정 만료 날짜 기한 없음 마지막으로 암호 설정한 날짜 2018-12-06 오전 5:21:35 암호 만료 날짜 기한 없음 암호를 바꿀 수 있는 날짜 2018-12-06 오전 5:21:35 암호 필요 아니요 사용자가 암호를 바꿀 수도 있음 아니요 허용된 워크스테이션 전체 로그온 스크립트 사용자 프로필 홈 디렉터리 최근 로그온 아님 허용된 로그온 시간 전체 로컬 그룹 구성원 *Guests 글로벌 그룹 구성원 *None 명령을 잘 실행했습니다.
진단 결과	**양호**

03. 계정 잠금 정책 설정	
양호 기준	계정 잠금 기간 - 60분
진단 현황	

	잠금 임계값: 아님 잠금 기간 (분): 30 잠금 관찰 창 (분): 30
진단 결과	**취약**

04. 암호 정책 설정

양호 기준	최소 암호 사용기간 1일 이상
진단 현황	최소 암호 사용 기간 (일): 0 최대 암호 사용 기간 (일): 42 최소 암호 길이: 0 암호 기록 개수: 없음
진단 결과	**취약**

05. 사용자계정 컨트롤 설정

양호 기준	사용자 계정 컨트롤(UAC) 사용
진단 현황	REG_DWORD ConsentPromptBehaviorAdmin 5 REG_DWORD PromptOnSecureDesktop 1 REG_DWORD EnableLUA 1
진단 결과	**양호**

06. CMD 파일 권한 설정

양호 기준	Administrator와 System 과 TrustedInstaller 그룹만 실행 권한
진단 현황	C:\Windows\system32\cmd.exe NT SERVICE\TrustedInstaller:F BUILTIN\Administrators:R NT AUTHORITY\SYSTEM:R BUILTIN\Users:R
진단 결과	**양호**

07. CMD 파일 권한 설정

양호 기준	홈디렉터리 권한중 Users:F 또는 Everyone:F가 없음
진단 현황	c:\users\All Users NT AUTHORITY\SYSTEM:(OI)(CI)F BUILTIN\Administrators:(OI)(CI)F CREATOR OWNER:(OI)(CI)(IO)F BUILTIN\Users:(OI)(CI)R BUILTIN\Users:(CI)(특별 액세스:) FILE_WRITE_DATA FILE_APPEND_DATA FILE_WRITE_EA FILE_WRITE_ATTRIBUTES c:\users\Default NT AUTHORITY\SYSTEM:(OI)(CI)(ID)F

BUILTIN\Administrators:(OI)(CI)(ID)F
BUILTIN\Users:(ID)R
BUILTIN\Users:(OI)(CI)(IO)(ID)(특별 액세스:)

GENERIC_READ
GENERIC_EXECUTE

Everyone:(ID)R
Everyone:(OI)(CI)(IO)(ID)(특별 액세스:)

GENERIC_READ
GENERIC_EXECUTE

c:\users\Default User Everyone:(DENY)(특별 액세스:)

FILE_READ_DATA

Everyone:R
NT AUTHORITY\SYSTEM:F
BUILTIN\Administrators:F

c:\users\desktop.ini NT AUTHORITY\SYSTEM:(ID)F
BUILTIN\Administrators:(ID)F
BUILTIN\Users:(ID)R
Everyone:(ID)R

c:\users\pc NT AUTHORITY\SYSTEM:(OI)(CI)F
BUILTIN\Administrators:(OI)(CI)F
pc-PC\pc:(OI)(CI)F
pc-PC\HomeUsers:R

c:\users\Public BUILTIN\Administrators:(OI)(CI)F
CREATOR OWNER:(OI)(CI)(IO)F
NT AUTHORITY\SYSTEM:(OI)(CI)F
NT AUTHORITY\INTERACTIVE:(OI)(CI)(IO)(특별 액세스:)

DELETE
READ_CONTROL
SYNCHRONIZE
FILE_GENERIC_READ
FILE_GENERIC_WRITE
FILE_GENERIC_EXECUTE
FILE_READ_DATA
FILE_WRITE_DATA
FILE_APPEND_DATA
FILE_READ_EA
FILE_WRITE_EA
FILE_EXECUTE
FILE_DELETE_CHILD
FILE_READ_ATTRIBUTES
FILE_WRITE_ATTRIBUTES

NT AUTHORITY\INTERACTIVE:(특별 액세스:)

READ_CONTROL
SYNCHRONIZE
FILE_GENERIC_READ
FILE_GENERIC_EXECUTE
FILE_READ_DATA
FILE_WRITE_DATA
FILE_APPEND_DATA
FILE_READ_EA
FILE_EXECUTE
FILE_READ_ATTRIBUTES

NT AUTHORITY\SERVICE:(OI)(CI)(IO)(특별 액세스:)

	DELETE READ_CONTROL SYNCHRONIZE FILE_GENERIC_READ FILE_GENERIC_WRITE FILE_GENERIC_EXECUTE FILE_READ_DATA FILE_WRITE_DATA FILE_APPEND_DATA FILE_READ_EA FILE_WRITE_EA FILE_EXECUTE FILE_DELETE_CHILD FILE_READ_ATTRIBUTES FILE_WRITE_ATTRIBUTES NT AUTHORITY\SERVICE:(특별 액세스:) READ_CONTROL SYNCHRONIZE FILE_GENERIC_READ FILE_GENERIC_EXECUTE FILE_READ_DATA FILE_WRITE_DATA FILE_APPEND_DATA FILE_READ_EA FILE_EXECUTE FILE_READ_ATTRIBUTES NT AUTHORITY\BATCH:(OI)(CI)(IO)(특별 액세스:) DELETE READ_CONTROL SYNCHRONIZE FILE_GENERIC_READ FILE_GENERIC_WRITE FILE_GENERIC_EXECUTE FILE_READ_DATA FILE_WRITE_DATA FILE_APPEND_DATA FILE_READ_EA FILE_WRITE_EA FILE_EXECUTE FILE_DELETE_CHILD FILE_READ_ATTRIBUTES FILE_WRITE_ATTRIBUTES NT AUTHORITY\BATCH:(특별 액세스:) READ_CONTROL SYNCHRONIZE FILE_GENERIC_READ FILE_GENERIC_EXECUTE FILE_READ_DATA FILE_WRITE_DATA FILE_APPEND_DATA FILE_READ_EA FILE_EXECUTE FILE_READ_ATTRIBUTES Everyone:(OI)(CI)F Everyone:(OI)(CI)F 가 존재합니다. 불필요할 경우 삭제하시기 바랍니다.

진단 결과	취약

08. 하드디스크 기본공유 제거

양호 기준	레지스트리값 AutoShareWks가 0이며 기본공유가 존재하지 않을 경우(IPC$ 제외)
진단 현황	공유 이름 리소스 설명 --- C$ C:\ 기본 공유 ADMIN$ C:\Windows 원격 관리 Users C:\Users AutoShareWks 레지스트리 설정값 The system was unable to find the specified registry key.
진단 결과	취약

09. SAM 파일 접근통제

양호 기준	SAM파일 접근권한이 Administrator, System 그룹만 모든 권한으로 등록되어 있는 경우
진단 현황	C:\Windows\system32\config\SAM NT AUTHORITY\SYSTEM:(ID)F BUILTIN\Administrators:(ID)F pc-PC\pc:(ID)F
진단 결과	취약

10. 최신 서비스팩 적용

양호 기준	inciter mws client가 설치되어 있어 최신 서비스 팩이 설치되어 있음
진단 현황	Service pack: 0 서비스 팩이 설치되어 있지 않습니다.
진단 결과	취약

11. 공유권한 및 사용자그룹 설정

양호 기준	공유디렉터리가 없거나 공유 디렉터리 접근 권환에 everyone이 없음
진단 현황	공유 이름 리소스 설명 --- Users C:\Users
진단 결과	양호

12. 로그오프나 워크스테이션 잠김

양호 기준	화면보호기를 설정하고 암호를 사용하며 대기 시간이 5분
진단 현황	REG_SZ ScreenSaveActive 1 The system was unable to find the specified registry key. The system was unable to find the specified registry key.
진단 결과	취약

13. 이벤트 뷰어 설정

양호 기준	최대 로그크기 10240KB이상, 로그 덮어쓰지 않음
진단 현황	응용 프로그램 로그크기 REG_DWORD MaxSize 20971520 보안 로그크기 액세스가 거부되었습니다. 시스템 로그 크기 REG_DWORD MaxSize 20971520 응용프로그램 로그 덮어쓰기 설정 옵션 REG_DWORD Retention 0 보안 로그 덮어쓰기 설정 옵션 액세스가 거부되었습니다. 시스템로그 덮어쓰기 설정 옵션 REG_DWORD Retention 0 응용프로그램 로그 자동보관 설정 옵션 The system was unable to find the specified registry key. 보안 로그 자동보관 설정 옵션 액세스가 거부되었습니다. 시스템로그 자동보관 설정 옵션 The system was unable to find the specified registry key.
진단 결과	취약

14. 마지막 로그온 사용자 계정 숨김

양호 기준	마지막 로그온 사용자 숨김 설정이 “사용”으로 설정되어 있을 경우
진단 현황	REG_DWORD DontDisplayLastUserName 0
진단 결과	취약

15. 로그온하지 않은 사용자 시스템 종료 방지

양호 기준	로그온하지 않고 시스템 종료 허용'이 '사용안함'으로 설정되어 있을 경우
진단 현황	The system was unable to find the specified registry key.
진단 결과	**양호**

16. 백신 프로그램 설치

양호 기준	백신 프로그램이 설치되어 있음
진단 현황	
진단 결과	**취약**

17. Null Session 설정

양호 기준	해당 레지스트리 값이 설정되어 있음
진단 현황	REG_DWORD restrictanonymous 0
진단 결과	**취약**

18. 레즈스트리 보호차단

양호 기준	Remote Registry Service가 중지되어 있음
진단 현황	사용 중이지 않습니다.
진단 결과	**양호**

19. AutoLogon 기능제어

양호 기준	autoadminlogon 값이 없거나 0으로 설정되어있음
진단 현황	Listing of [SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon] REG_SZ ReportBootOk 1 REG_SZ Shell explorer.exe REG_SZ PreCreateKnownFolders {A520A1A4-1780-4FF6-BD18-167343C5AF16} REG_SZ DefaultDomainName REG_SZ DefaultUserName REG_SZ Userinit userinit.exe REG_SZ VMApplet SystemPropertiesPerformance.exe /pagefile [GPExtensions]
진단 결과	**취약**