침입탐지 진단

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
진단 결과	**양호**

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 REG_SZ ScreenSaverIsSecure 1 REG_SZ ScreenSaveTimeOut 1
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	REG_DWORD ShutdownWithoutLogon 1
진단 결과	**취약**
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**