취약점 진단(Windows) 관련 전체 항목(~가이드) 및 관련 내용

대상 시스템(OS) : Windows server 2012 R2

서비스팩 여부 : 없음 > 기능 패치 및 보안 업데이트로 대체

1. 계정 관리

W-01 : Administrator 계정 이름 변경 또는 보안성 강화

W-02 : Guest 계정 비활성화

Default 로 생성되어 있는 계정 > 비활성화

W-03 : 불필요한 계정 제거

관리적 측면의 내용

오래 사용될수록 ~수십개의 계정이 있을 수 있음.

새로운 관리자가 모르는 계정도 존재할 수 있음.

W-04 : 계정 잠금 임계값 설정

레인보우 공격을 막기 위한 로그인 시도 횟수 제한

W-05 : 해독 가능한 암호화를 사용하여 암호 저장 해제

'복호화 가능한 암호화' 설정 비활성화

W-06 : 관리자 그룹에 최소한의 사용자 포함

관리자 그룹에 소속되어 있는 불필요한 사용자 계정의 권한 제거

리눅스에도 동일한 항목이 있음.

? 계정별 로그인 가능여부 확인해야하는가

W-46 : Everyone 사용권한을 익명 사용자에 적용 해제

ID,PW 없이 로그인 할 수 있는 기능이기 때문에 "사용 안함"으로 설정해야함.

W-47 : 계정 잠금 기간 설정

"W-04" 항목과 연관성

"계정 잠금 임계값" 이상 로그인 실패하였을 시 어느 정도의 시간동안 로그인이 불가능해질지에 대한 내용

W-48 : 패스워드 복잡성 설정

W-49 : 패스워드 최소 암호 길이

W-50 : 패스워드 최대 사용 기간

W-51 : 패스워드 최소 사용 기간

변경된 패스워드를 일정 기간 이상 사용하도록 하여, 익숙한 패스워드 혹은 기존에 사용하던 패스워드로 바로 변경할 수 있음 > 비활성화 하여야함.

W-52 : 마지막 사용자 이름 표시 안함

W-53 : 로컬 로그온 허용

교육환경은 로컬 로그온이라고 보면 되지만, 실무에서는 로컬 로그온 하지는 않음. > 보통 원격으로 접속함.

관리 목적으로 허용하지 않는 것이 맞음

W-54 : 익명 SID/이름 변환 허용 해제

계정에 따른 계정번호(SID)가 부여되어 있는데 이 SID를 사용하면 계정 아이디를 알 수 있음.

W-55 : 최근 암호 기억

W-56 : 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한

W-57 : 원격 터미널 접속 가능한 사용자 그룹 제한

? "원격 연결 허용 안함"으로 설정되어 있다면 더 볼 필요없나. > 없을 것 같음. 많은 경우에서 원격 접속을 허용한 채로 서버를 사용하겠지만 원격 접속 자체가 비활성화 되어 있는 대상에 대해서는 진단할 필요가 없을 것 같음.

2. 서비스 관리

W-07 : 공유 권한 및 사용자 그룹 설정

기업에서도 사용의 편의를 위해 윈도우 서버 간 공유 폴더를 쓰는 경우도 꽤 있음.

권한 제어가 되어 있지 않은 공유 폴더를 쓰는 것은 보안 취약점임.

? 읽기, 변경, 모든 권한 설정이 가능한데 "읽기" 옵션만 설정되어 있어도 "취약"으로 판단하시는지 > "읽기" 권한만으로도 익명 사용자의 접근이 가능하여 내부 데이터 유출 및 악성코드 감염의 우려가 있음.

? "SYSVOL", "NETLOGON"이 시스템에서 필요한 공유 폴더는 아닌지. > 명확한 레퍼런스를 찾을 수 없으며, 찾았다고 하더라도 해당 서비스를 명확하게 사용하고 있는지에 대해 담당자와의 커뮤니케이션이 필요함.

W-08 : 하드디스크 기본 공유 제거

? 기본 공유 폴더 3가지(ADMIN$,C$,IPC$) 전부 공유 중지가 불가능 하거나, 시스템 재부팅 시 공유 기능이 다시 시작된다고 합니다.

> 공유 중지가 불가능한 기본 공유 설정은 수정이 가능한지, 가능하다면 어떻게 수정하는지

> 공유 중지가 일시적인 기본 공유 설정은 레지스트리 AutoShareServer으로 수정할 수 있는 건지

W-09 : 불필요한 서비스 제거

? 매번 MS 가이드와 구동중인 서비스 간 비교 및 분석으로 진단을 결정하시는지(실무에서)

? 가이드에 없는 서비스에 대해서는 인터뷰?

W-10 : IIS 서비스 구동 점검

쓰냐 or 안쓰냐

W-11 : IIS 디렉토리 리스팅 제거

ex ) mirrorlist 혹은 비슷한 양식의 다운로드 페이지 양식 참고

? 미러리스트는 해당 취약점에 취약 판단을 받나, 아니면 사용 목적에 따라 "양호"판단이 가능한가

W-12 : IIS CGI 실행 제한

W-13 : IIS 상위 디렉토리 접근 금지

"W-11" 항목의 디렉터리 리스팅과의 연관성

해당하는 설정 못 찾겠다

W-14 : IIS 불필요한 파일 제거

Defalut 설정 중 불필요한 디렉터리 및 파일에 대한 점검

진단 대상이 아님.

W-15 : IIS 웹프로세스 권한 제한

관리자 권한으로 IIS가 구현되어 있으면 IIS에 권한을 가진 모든 사용자의 정보를 탈취할 수 있음.

W-16 : IIS 링크 사용 금지

자주 발생하는 취약점은 아님.

SymLink, Alias, 바로가기 등

ex) 우리가 자주 사용하는 "바로가기" 기능과 같은 의미임.

W-17 : IIS 파일 업로드 및 다운로드 제한

W-18 : IIS DB 연결 취약점 점검

> 오래된 항목, 가이드에 있는 것처럼 처리하지는 않음 > 옛 서버를 점검할 때 참고하는 내용

W-19 : IIS 가상 디렉토리 삭제

대상 시스템의 버전(2012)은 해당 없음.

상위 버전에서는 제공되지 않는 기능임 > 진단 대상 항목이 아님.

W-20 : IIS 데이터파일 ACL 적용

W-21 : IIS 미사용 스크립트 매핑 제거(실습)

특정 확장자를 사용하지말라

IIS관리자-IIS-처리기매핑

W-22 : IIS Exec 명령어 쉘 호출 진단

진단 대상 항목이 아님.

W-23 : IIS WebDAV 비활성화(실습)

취약점 진단 공부에 많이 사용하는 기능 > 샌드백

대상 항목에는 있지만 실제로 사용되지는 않는 기능임.

"양호" 진단 기준이 자세하게 나와있는 편임.

IIS관리자-상위디렉터리-ISAPI 및 CGI 제한-WebDAV

W-24 : 바인딩 서비스 구동 점검(실습)

실무에서는 사내 서버 혹은 PC 간 자원 공유를 위해 사용하는 경우가 있음.

> 사용 조건을 충분히 설정하였는지를 기준으로 진단함.

이더넷 속성-IPv4 속성-고급 TCP/IP 설정.

W-25 : FTP 서비스구동점검

보통 vsftp, sftp를 많이 사용함

W-26 : FTP 디렉토리접근권한설정

W-27 : Anonymous FTP 금지

W-28 : FTP 접근제어설정

W-29 : DNS Zone Transfer 설정

Domain Name Server의 데이터를 오염 시킨다거나 악성코드 등을 삽입할 수 있음.> 특정 서버로만 영역전송이 가능하도록 설정해야함.

W-30 RDS(Remonte Data Services) 제거

진단 대상 항목이 아님. 경로 자체가 존재하지 않음.

W-31 최신 서비스팩 적용

리눅스에는 "서비스팩" 개념이 없음.

16,19 등 이후 버전은 서비스팩 개념이 없음.

W-58 터미널 서비스 암호화 수준 설정

원격지에서 서버에 접속할 때 "터미널" 사용함.

W-59 IIS 웹 서비스 정보 숨김

에러 페이지를 별도로 지정하여 "Defalut 에러 페이지"에 들어있는 중요 정보가 노출되지 않도록 해야함.

공통의 에러 페이지를 생성하여, 에러의 종류도 노출되지 않도록 해야함.

W-60 SNMP 서비스 구동 점검

NMS 또는 별도의 툴(솔루션 등)에서 모니터링을 위해 SNMP 서비스를 많이 이용함.

W-61 SNMP 서비스 커뮤니티스트링의 복잡성 설정

Defalut 인 "public" 또는 "private"로 설정되어 있지 않도록 하여야함.

W-62 SNMP Access control 설정

W-63 DNS 서비스 구동 점검

버전 등에 따른 DNS 관련 CVE 취약점 및 잘 알려진 취약점이 많이 있는 상태임.

사용하지 않는 것을 추천하거나 사용해야한다면 필요한 보안 업데이트를 지속적으로 하고 있는지 확인함.

W-64 HTTP/FTP/SMTP 배너 차단

서비스 및 계정에 따른 Defalut Message 배너를 삭제하여 정보 노출을 막아야함.

W-65 Telnet 보안 설정

암호화 기능이 없어 잘 사용되지 않는 서비스임.

텔넷을 사용하지 않으면 "양호" 진단

W-66 불필요한 ODBC/OLE-DB 데이터소스와 드라이브 제거

ODBC (Open Database Connectivity) : DB에 접근하기 위한 ANSI/ISO 표준 API.

OLE DB (Object Linking and Embedding Database) : MS COM 기반 API.

> RDB,mail,sheet,txt 등 다양한 형식의 파일에 일관된 방식으로 접근하도록 설계됨.

W-67 원격 터미널 접속 타임아웃 설정

세션 타임아웃 설정 필요.

W-68 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검

대표적인 예제는 로그 관리, 주요 데이터 백업 등이 있음.

"예약작업" 기능이 노출될 시 다양한 공격루트로 사용됨.

잘 알려지거나 간단한 "예약작업"에 대해서는 확인 가능하지만,

> 자체적으로 사용하는 "예약작업"에 대해서는 보통 담당자 확인이 필요한 경우가 많음.

W-32 최신 HOT FIX 적용

기업에서는 보통 "자동 업데이트" 기능을 사용하지 않음.

> 기업 입장에서는 서비스의 문제 발생가능성을 무시할 수 없음.

>> 그래서 아예 하지 않거나 패치 서버를 따로 두고 테스트 후에 적용함.

W-33 백신 프로그램 업데이트

W-69 정책에 따른 시스템 로깅 설정

W-34 로그의 정기적 검토 및 보고

가이드 기준 일정 크기 이상의 데이터가 진단 대상 기준임.

W-35 원격으로 액세스 할 수 있는 레지스트리 경로

W-70 이벤트 로그 관리 설정

W-71 원격에서 이벤트 로그파일 접근 차단

W-36 백신 프로그램 설치

W-37 SAM 파일 접근 통제 설정

W-38 화면보호기 설정

W-39 로그온 하지 않고 시스템 종료 허용 해제

W-40 원격 시스템에서 강제로 시스템 종료

W-41 보안감사를 로그할 수 없는 경우 즉시 시스템 종료 해제

W-42 SAM 계정과 공유의 익명 열거 허용 안함

W-43 Autologon 기능 제어

W-44 이동식 미디어 포맷 및 꺼내기 허용

W-45 디스크 볼륨 암호화 설정

W-72 Dos 공격 방어 레지스트리 설정

W-73 사용자가 프린터 드라이버를 설치할 수 없게 함

W-74 세션 연결을 중단하기 전에 필요한 유휴시간

W-75 경고 메시지 설정

W-76 사용자별 홈 디렉토리 권한 설정

W-77 LAN Manager 인증 수준

W-78 보안 채널 데이터 디지털 암호화 또는 서명

W-79 파일 및 디렉토리 보호

W-80 컴퓨터 계정 암호 최대 사용 기간

W-81 시작 프로그램 목록 분석

W-82 Windows 인증 모드 사용