취약점 진단 (3)

작성일시	@2023년 4월 5일 오전 9:13
최종 편집 일시	@2023년 4월 7일 오후 11:37
강의 번호	보안
유형	강의
자료	주요정보통신기반시설_기술적_취약점_분석_평가_방법_상세가이드.pdf
복습	☐
5회독	☐
참고 링크	

5. 보안 관리
    W-36. 백신 프로그램 설치 (상)
    W-37. SAM 파일 접근 통제 설정 (상)
    W-38. 화면 보호기 설정 (상)
    W-39. 로그온 하지 않고 시스템 종료 허용 해제 (상)
    W-40. 원격 시스템에서 강제로 시스템 종료 (상)
    W-41. 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제 (상)
    W-42. SAM 계정과 공유의 익명 열거 허용 안 함 (상)
    W-43. Autologon 기능 제어 (상)
    W-44. 이동식 미디어 포맷 및 꺼내기 허용 (상)
    W-45. 디스크 볼륨 암호화 설정 (상)
    W-72. Dos 공격 방어 레지스트리 설정 (중)
    W-73. 사용자가 프린터 드라이버를 설치할 수 없게 함 (중)
    W-74. 세션 연결을 중단하기 전에 필요한 유휴 시간 (중)
    W-75. 경고 메시지 설정 (하)
    W-76. 사용자별 홈 디렉토리 권한 설정 (중)
    W-77. LAN Manager 인증 수준 (중)
    W-78. 보안 채널 데이터 디지털 암호화 또는 서명 (중)
    W-79. 파일 및 디렉토리 보호 (중)
    W-80. 컴퓨터 계정 암호 최대 사용 기간 (중)
    W-81. 시작 프로그램 목록 분석 (중)
6. DB 관리
    W-82. Windows 인증 모드 사용 (중)

- [ ] 1회독
- [ ] 2회독
- [ ] 3회독
- [ ] 4회독
- [ ] 5회독

점검 개요

- 서버 취약점 점검은 Unix, Windows 서버에 대해 가능
- 점검 시 자동화 진단 툴(스크립트)를 통해 보안 설정 값을 확인하고 담당자와의 인터뷰 필요
- 점검을 통해 발견된 취약점에 조치 계획을 수립하고 조치 이행을 해야 함

점검 방법

- 자동화 진단 툴 점검
- 수동 점검
- 담당자 인터뷰

서버 취약점 점검 절차

> 💡 **점검 계획 수립 → 점검 및 보고서 작성 → 결과 조치**

1. **점검 계획 수립**
    - 점검 범위 선정 → 점검 도구 선정 → 점검 일정 수립 → 점검 업무 착수
2. **점검 및 보고서 작성**
    - 설정 분석 → 정책 분석 → 보고서 작성
3. **결과 조치**
    - 조치 계획 수립 → 조치 이행

Unix 서버

취약점 분석-평가 항목

Unix 서버 취약점 분석평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정 관리	root 계정 원격 접속 제한	상	U-01
	패스워드 복잡성 설정	상	U-02
	계정 잠금 임계값 설정	상	U-03
	패스워드 파일 보호	상	U-04
	root 이외의 UID가 '0'금지	중	U-44
	root 계정 su 제한	하	U-45
	패스워드 최소 길이 설정	중	U-46
	패스워드 최대 사용기간 설정	중	U-47
	패스워드 최소 사용기간 설정	중	U-48
	불필요한 계정 제거	하	U-49
	관리자 그룹에 최소한의 계정 포함	하	U-50
	계정이 존재하지 않는 GID 금지	하	U-51
	동일한 UID 금지	중	U-52
	사용자 shell 점검	하	U-53
	Session Timeout 설정	하	U-54
2. 파일 및 디렉터리 관리	root 홈, 패스 디렉터리 권한 및 패스 설정	상	U-05
	파일 및 디렉터리 소유자 설정	상	U-06
	/etc/passwd 파일 소유자 및 권한 설정	상	U-07
	/etc/shadow 파일 소유자 및 권한 설정	상	U-08
	/etc/hosts 파일 소유자 및 권한 설정	상	U-09
	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	U-10
	/etc/syslog.conf 파일 소유자 및 권한 설정	상	U-11
	/etc/services 파일 소유자 및 권한 설정	상	U-12
	SUID, SGID, Sticky bit 설정 파일 점검	상	U-13
	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	U-14
	world writable 파일 점검	상	U-15
	/dev에 존재하지 않는 device 파일 점검	상	U-16
	$HOME/.rhosts, hosts.equiv 사용 금지	상	U-17
	접속 IP 및 포트 제한	상	U-18
	hosts.lpd 파일 소유자 및 권한 설정	하	U-55
	UMASK 설정 관리	중	U-56
	홈디렉토리 소유자 및 권한 설정	중	U-57
	홈디렉토리로 지정한 디렉토리의 존재 관리	중	U-58
	숨겨진 파일 및 디렉토리 검색 및 제거	하	U-59

분류	점검항목	항목 중요도	항목코드
3. 서비스 관리	finger 서비스 비활성화	상	U-19
	Anonymous FTP 비활성화	상	U-20
	r 계열 서비스 비활성화	상	U-21
	cron 파일 소유자 및 권한설정	상	U-22
	Dos 공격에 취약한 서비스 비활성화	상	U-23
	NFS 서비스 비활성화	상	U-24
	NFS 접근 통제	상	U-25
	automountd 제거	상	U-26
	RPC 서비스 확인	상	U-27
	NIS, NIS+ 점검	상	U-28
	tftp, talk 서비스 비활성화	상	U-29
	Sendmail 버전 점검	상	U-30
	스팸 메일 릴레이 제한	상	U-31
	일반사용자의 Sendmail 실행 방지	상	U-32
	DNS 보안 버전 패치	상	U-33
	DNS Zone Transfer 설정	상	U-34
	웹서비스 디렉토리 리스팅 제거	상	U-35
	웹서비스 웹 프로세스 권한 제한	상	U-36
	웹서비스 상위 디렉토리 접근 금지	상	U-37
	웹서비스 불필요한 파일 제거	상	U-38
	웹서비스 링크 사용 금지	상	U-39
	웹서비스 파일 업로드 및 다운로드 제한	상	U-40
	웹서비스 영역의 분리	상	U-41
	ssh 원격접속 허용	중	U-60
	ftp 서비스 확인	하	U-61
	ftp 계정 shell 제한	중	U-62
	Ftpusers 파일 소유자 및 권한 설정	하	U-63
	Ftpusers 파일 설정	중	U-64
	at 파일 소유자 및 권한 설정	중	U-65
	SNMP 서비스 구동 점검	중	U-66
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	U-67
	로그온 시 경고 메시지 제공	하	U-68
	NFS 설정파일 접근 제한	중	U-69
	expn, vrfy 명령어 제한	중	U-70
	Apache 웹 서비스 정보 숨김	중	U-71
4. 패치 관리	최신 보안패치 및 벤더 권고사항 적용	상	U-42
5. 로그 관리	로그의 정기적 검토 및 보고	상	U-43
	정책에 따른 시스템 로깅 설정	하	U-72

1. 계정 관리

U-01. root 계정 원격 접속 제한 (상)

U-02. 패스워드 복잡성 설정 (상)

U-03. 계정 잠금 임계값 설정 (상)

U-04. 패스워드 파일 보호 (상)

U-44. root 이외의 UID가 ‘0’ 금지 (중)

U-45. root 계정 su 제한 (하)

U-46. 패스워드 최소 길이 설정 (중)

U-47. 패스워드 최대 사용 기간 설정 (중)

U-48. 패스워드 최소 사용 기간 설정 (중)

U-49. 불필요한 계정 제거 (하)

U-50. 관리자 그룹에 최소한의 계정 포함 (하)

U-51. 계정이 존재하지 않는 GID 금지 (하)

U-52. 동일한 UID 금지 (중)

U-53. 사용자 shell 점검 (하)

U-54. Session Timeout 설정 (하)

2. 파일 및 디렉터리 관리

U-05. root 홈, 패스 디렉터리 권한 및 패스 설정 (상)

U-06. 파일 및 디렉터리 소유자 설정 (상)

U-07. /etc/passwd 파일 소유자 및 권한 설정 (상)

U-08. /etc/shadow 파일 소유자 및 권한 설정 (상)

U-09. /etc/hosts 파일 소유자 및 권한 설정 (상)

U-10. /etc/(x)inetd.conf 파일 소유자 및 권한 설정 (상)

U-11. /etc/syslog.conf 파일 소유자 및 권한 설정 (상)

U-12. /etc/services 파일 소유자 및 권한 설정 (상)

U-13. SUID, SGID, Sticky bit 설정 파일 점검 (상)

U-14. 사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정 (상)

U-15. world writable 파일 점검 (상)

U-16. /dev에 존재하지 않는 device 파일 점검 (상)

U-17. $HOME/.rhosts, hosts.equiv 사용 금지 (상)

U-18. 접속 IP 및 포트 제한 (상)

U-55. hosts.lpd 파일 소유자 및 권한 설정 (하)

U-56. UMASK 설정 관리 (중)

U-57. 홈디렉토리 소유자 및 권한 설정 (중)

U-58. 홈디렉토리로 지정한 디렉토리의 존재 관리 (중)

U-59. 숨겨진 파일 및 디렉토리 검색 및 제거 (하)

3. 서비스 관리

U-19. finger 서비스 비활성화 (상)

U-20. Anonymous FTP 비활성화 (상)

U-21. r 계열 서비스 비활성화 (상)

U-22. cron 파일 소유자 및 권한설정 (상)

U-23. Dos 공격에 취약한 서비스 비활성화 (상)

U-24. NFS 서비스 비활성화 (상)

U-25. NFS 접근 통제 (상)

U-26. automountd 제거 (상)

U-27. RPC 서비스 확인 (상)

U-28. NIS, NIS+ 점검 (상)

U-29. tftp, talk 서비스 비활성화 (상)

U-30. Sendmail 버전 점검 (상)

U-31. 스팸 메일 릴레이 제한 (상)

U-32. 일반 사용자의 Sendmail 실행 방지 (상)

U-33. DNS 보안 버전 패치 (상)

U-34. DNS Zone Transfer 설정 (상)

U-35. 웹서비스 디렉토리 리스팅 제거 (상)

U-36. 웹서비스 웹 프로세스 권한 제한 (상)

U-37. 웹서비스 상위 디렉토리 접근 금지 (상)

U-38. 웹서비스 불필요한 파일 제거 (상)

U-39. 웹서비스 링크 사용 금지 (상)

U-40. 웹서비스 파일 업로드 및 다운로드 제한 (상)

U-41. 웹서비스 영역의 분리 (상)

U-60. ssh 원격접속 허용 (중)

U-61. ftp 서비스 확인 (하)

U-62. ftp 계정 shell 제한 (중)

U-63. Ftpusers 파일 소유자 및 권한 설정 (하)

U-64. Ftpusers 파일 설정 (중)

U-65. at 파일 소유자 및 권한 설정 (중)

U-66. SNMP 서비스 구동 점검 (중)

U-67. SNMP 서비스 커뮤니티 스트링의 복잡성 설정 (중)

U-68. 로그온 시 경고 메시지 제공 (하)

U-69. NFS 설정파일 접근 제한 (중)

U-70. expn, vrfy 명령어 제한 (중)

U-71. Apache 웹 서비스 정보 숨김 (중)

4. 패치 관리

U-42. 최신 보안패치 및 벤더 권고사항 적용 (상)

5. 로그 관리

U-43. 로그의 정기적 검토 및 보고 (상)

U-72. 정책에 따른 시스템 로깅 설정 (하)

Windows 서버

취약점 분석-평가 항목

윈도우즈 서버 취약점 분석·평가 항목

분류	점검항목	항목 중요도	항목코드
1. 계정 관리	Administrator 계정 이름 변경 또는 보안성 강화	상	W-01
	Guest 계정 비활성화	상	W-02
	불필요한 계정 제거	상	W-03
	계정 잠금 임계값 설정	상	W-04
	해독 가능한 암호화를 사용하여 암호 저장 해제	상	W-05
	관리자 그룹에 최소한의 사용자 포함	상	W-06
	Everyone 사용권한을 익명 사용자에 적용 해제	중	W-46
	계정 잠금 기간 설정	중	W-47
	패스워드 복잡성 설정	중	W-48
	패스워드 최소 암호 길이	중	W-49
	패스워드 최대 사용 기간	중	W-50
	패스워드 최소 사용 기간	중	W-51
	마지막 사용자 이름 표시 안함	중	W-52
	로컬 로그온 허용	중	W-53
	익명 SID/이름 변환 허용 해제	중	W-54
	최근 암호 기억	중	W-55
	콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한	중	W-56
	원격터미널 접속 가능한 사용자 그룹 제한	중	W-57
2. 서비스 관리	공유 권한 및 사용자 그룹 설정	상	W-07
	하드디스크 기본 공유 제거	상	W-08
	불필요한 서비스 제거	상	W-09
	IIS 서비스 구동 점검	상	W-10
	IIS 디렉토리 리스팅 제거	상	W-11
	IIS CGI 실행 제한	상	W-12
	IIS 상위 디렉토리 접근 금지	상	W-13
	IIS 불필요한 파일 제거	상	W-14
	IIS 웹프로세스 권한 제한	상	W-15
	IIS 링크 사용 금지	상	W-16
	IIS 파일 업로드 및 다운로드 제한	상	W-17
	IIS DB 연결 취약점 점검	상	W-18
	IIS 가상 디렉토리 삭제	상	W-19
	IIS 데이터파일 ACL 적용	상	W-20
	IIS 미사용 스크립트 매핑 제거	상	W-21
	IIS Exec 명령어 쉘 호출 진단	상	W-22
	IIS WebDAV 비활성화	상	W-23

분류	점검항목	항목 중요도	항목코드
	NetBIOS 바인딩 서비스 구동 점검	상	W-24
	FTP 서비스 구동 점검	상	W-25
	FTP 디렉토리 접근 권한 설정	상	W-26
	Anonymous FTP 금지	상	W-27
	FTP 접근 제어 설정	상	W-28
	DNS Zone Transfer 설정	상	W-29
	RDS(Remonte Data Services) 제거	상	W-30
	최신 서비스팩 적용	상	W-31
	터미널 서비스 암호화 수준 설정	중	W-58
	IIS 웹 서비스 정보 숨김	중	W-59
	SNMP 서비스 구동 점검	중	W-60
	SNMP 서비스 커뮤니티스트링의 복잡성 설정	중	W-61
	SNMP Access control 설정	중	W-62
	DNS 서비스 구동 점검	중	W-63
	HTTP/FTP/SMTP 배너 차단	하	W-64
	Telnet 보안 설정	중	W-65
	불필요한 ODBC/OLE-DB 데이터소스와 드라이브 제거	중	W-66
	원격터미널 접속 타임아웃 설정	중	W-67
	예약된 작업에 의심스러운 명령이 등록되어 있는지 점검	중	W-68
3. 패치 관리	최신 HOT FIX 적용	상	W-32
	백신 프로그램 업데이트	상	W-33
	정책에 따른 시스템 로깅설정	중	W-69
4. 로그 관리	로그의 정기적 검토 및 보고	상	W-34
	원격으로 액세스 할 수 있는 레지스트리 경로	상	W-35
	이벤트 로그 관리 설정	하	W-70
	원격에서 이벤트 로그파일 접근 차단	중	W-71
5. 보안 관리	백신 프로그램 설치	상	W-36
	SAM 파일 접근 통제 설정	상	W-37
	화면보호기 설정	상	W-38
	로그온 하지 않고 시스템 종료 허용 해제	상	W-39
	원격 시스템에서 강제로 시스템 종료	상	W-40
	보안감사를 로그할 수 없는 경우 즉시 시스템 종료 해제	상	W-41
	SAM 계정과 공유의 익명 열거 허용 안함	상	W-42
	Autologon 기능 제어	상	W-43
	이동식 미디어 포맷 및 꺼내기 허용	상	W-44
	디스크 볼륨 암호화 설정	상	W-45
	Dos 공격 방어 레지스트리 설정	중	W-72
	사용자가 프린터 드라이버를 설치할 수 없게 함	중	W-73

분류	점검항목	항목 중요도	항목코드
	세션 연결을 중단하기 전에 필요한 유휴시간	중	W-74
	경고 메시지 설정	하	W-75
	사용자별 홈 디렉토리 권한 설정	중	W-76
	LAN Manager 인증 수준	중	W-77
	보안 채널 데이터 디지털 암호화 또는 서명	중	W-78
	파일 및 디렉토리 보호	중	W-79
	컴퓨터 계정 암호 최대 사용 기간	중	W-80
	시작 프로그램 목록 분석	중	W-81
6. DB 관리	Windows 인증 모드 사용	중	W-82

1. 계정 관리

W-01. Administrator 계정 이름 변경 또는 보안성 강화 (상)

W-02. Guest 계정 비활성화 (상)

W-03. 불필요한 계정 제거 (상)

W-04. 계정 잠금 임계값 설정 (상)

W-05. 해독 가능한 암호화를 사용하여 암호 저장 해제 (상)

W-06. 관리자 그룹에 최소한의 사용자 포함 (상)

W-46. Everyone 사용 권한을 익명 사용자에 적용 해제 (중)

W-47. 계정 잠금 기간 설정 (중)

W-48. 패스워드 복잡성 설정 (중)

W-49. 패스워드 최소 암호 길이 (중)

W-50. 패스워드 최대 사용 기간 (중)

W-51. 패스워드 최소 사용 기간 (중)

W-52. 마지막 사용자 이름 표시 안 함 (중)

W-53. 로컬 로그온 허용 (중)

W-54. 익명 SID/이름 변환 허용 해제 (중)

W-55. 최근 암호 기억 (중)

W-56. 콘솔 로그온 시 로컬 계정에서 빈 암호 사용 제한 (중)

W-57. 원격 터미널 접속 가능한 사용자 그룹 제한 (중)

2. 서비스 관리

W-07. 공유 권한 및 사용자 그룹 설정 (상)

W-08. 하드디스크 기본 공유 제거 (상)

W-09. 불필요한 서비스 제거 (상)

W-10. IIS 서비스 구동 점검 (상)

W-11. IIS 디렉토리 리스팅 제거 (상)

W-12. IIS CGI 실행 제한 (상)

W-13. IIS 상위 디렉토리 접근 금지 (상)

W-14. IIS 불필요한 파일 제거 (상)

W-15. IIS 웹프로세스 권한 제한 (상)

W-16. IIS 링크 사용 금지 (상)

W-17. IIS 파일 업로드 및 다운로드 제한 (상)

W-18. IIS DB 연결 취약점 점검 (상)

W-19. IIS 가상 디렉토리 삭제 (상)

W-20. IIS 데이터파일 ACL 적용 (상)

W-21. IIS 미사용 스크립트 매핑 제거 (상)

W-22. IIS Exec 명령어 쉘 호출 진단 (상)

W-23. IIS WebDAV 비활성화 (상)

W-24. NetBIOS 바인딩 서비스 구동 점검 (상)

W-25. FTP 서비스 구동 점검 (상)

W-26. FTP 디렉토리 접근 권한 설정 (상)

W-27. Anonymous FTP 금지 (상)

W-28. FTP 접근 제어 설정 (상)

W-29. DNS Zone Transfer 설정 (상)

W-30. RDS(Remonte Data Services) 제거 (상)

W-31. 최신 서비스팩 적용 (상)

W-58. 터미널 서비스 암호화 수준 설정 (중)

W-59. IIS 웹 서비스 정보 숨김 (중)

W-60. SNMP 서비스 구동 점검 (중)

W-61. SNMP 서비스 커뮤니티 스트링의 복잡성 설정 (중)

W-62. SNMP Access control 설정 (중)

W-63. DNS 서비스 구동 점검 (중)

W-64. HTTP/FTP/SMTP 배너 차단 (하)

W-65. Telnet 보안 설정 (중)

W-66. 불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거 (중)

W-67. 원격 터미널 접속 타임아웃 설정 (중)

W-68. 예약된 작업에 의심스러운 명령이 등록되어 있는지 점검 (중)

3. 패치 관리

W-32. 최신 HOT FIX 적용 (상)

W-33. 백신 프로그램 업데이트 (상)

W-69. 정책에 따른 시스템 로깅 설정 (중)

4. 로그 관리

W-34. 로그의 정기적 검토 및 보고 (상)

W-35. 원격으로 액세스 할 수 있는 레지스트리 경로 (상)

W-70. 이벤트 로그 관리 설정 (하)

W-71. 원격에서 이벤트 로그파일 접근 차단 (중)

5. 보안 관리

W-36. 백신 프로그램 설치 (상)

W-37. SAM 파일 접근 통제 설정 (상)

W-38. 화면 보호기 설정 (상)

W-39. 로그온 하지 않고 시스템 종료 허용 해제 (상)

W-40. 원격 시스템에서 강제로 시스템 종료 (상)

W-41. 보안 감사를 로그할 수 없는 경우 즉시 시스템 종료 해제 (상)

W-42. SAM 계정과 공유의 익명 열거 허용 안 함 (상)

W-43. Autologon 기능 제어 (상)

W-44. 이동식 미디어 포맷 및 꺼내기 허용 (상)

W-45. 디스크 볼륨 암호화 설정 (상)

W-72. Dos 공격 방어 레지스트리 설정 (중)

W-73. 사용자가 프린터 드라이버를 설치할 수 없게 함 (중)

W-74. 세션 연결을 중단하기 전에 필요한 유휴 시간 (중)

W-75. 경고 메시지 설정 (하)

W-76. 사용자별 홈 디렉토리 권한 설정 (중)

W-77. LAN Manager 인증 수준 (중)

W-78. 보안 채널 데이터 디지털 암호화 또는 서명 (중)

W-79. 파일 및 디렉토리 보호 (중)

W-80. 컴퓨터 계정 암호 최대 사용 기간 (중)

W-81. 시작 프로그램 목록 분석 (중)

6. DB 관리

W-82. Windows 인증 모드 사용 (중)