Linux 진단결과 (페이지 1)

구분	진단코드	진단항목	취약도	점검결과
계정관리	U-01	root 계정 원격 접속 제한	상	취약
계정관리	U-02	패스워드 복잡성 설정	상	양호
계정관리	U-03	계정 잠금 임계값 설정	상	취약
계정관리	U-04	패스워드 최대 사용 기간 설정	중	취약
계정관리	U-05	패스워드 파일 보호	상	양호
파일 및 디렉토리 관리	U-06	root 홈 패스 디렉터리 권한 및 패스 설정	상	양호
파일 및 디렉토리 관리	U-07	파일 및 디렉터리 소유자 설정	상	취약
파일 및 디렉토리 관리	U-08	/etc/passwd 파일 소유자 및 권한 설정	상	양호
파일 및 디렉토리 관리	U-09	/etc/shadow 파일 소유자 및 권한 설정	상	취약
파일 및 디렉토리 관리	U-10	/etc/hosts 파일 소유자 및 권한 설정	상	양호
파일 및 디렉토리 관리	U-11	/etc/(x)inetd.conf 파일 소유자 및 권한 설정	상	N/A
파일 및 디렉토리 관리	U-12	/etc/(r)syslog.conf 파일 소유자 및 권한 설정	상	양호
파일 및 디렉토리 관리	U-13	/etc/services 파일 및 권한 설정	상	양호
파일 및 디렉토리 관리	U-14	SUID SGID Sticy bit 설정 파일 점검	상	양호
파일 및 디렉토리 관리	U-15	사용자 시스템 시작파일 및 환경파일 소유자 및 권한 설정	상	취약
파일 및 디렉토리 관리	U-16	world writable 파일 점검	상	취약
파일 및 디렉토리 관리	U-17	$HOME/.rhosts hosts.equiv 사용금지	상	양호
파일 및 디렉토리 관리	U-18	접속 IP 및 포트 제한	상	N/A
파일 및 디렉토리 관리	U-19	cron 파일 소유자 및 권한 설정	상	취약
서비스 관리	U-20	Finger 서비스 비활성화	상	N/A

Linux 진단결과 (페이지 2)

구분	진단코드	진단항목	취약도	점검결과
서비스 관리	U-21	Anonymous FTP 비활성화	상	양호
서비스 관리	U-22	r 계열 서비스 비활성화	상	N/A
서비스 관리	U-23	DOS 공격에 취약한 서비스 비활성화	상	N/A
서비스 관리	U-24	NFS 서비스 비활성화	상	취약
서비스 관리	U-25	NFS 접근통제	상	N/A
서비스 관리	U-26	automountd	상	양호
서비스 관리	U-27	RPC 서비스 확인	상	N/A
서비스 관리	U-28	NIS NIS+ 점검	상	양호
서비스 관리	U-29	tftp talk 서비스 비활성화	상	양호
서비스 관리	U-30	Sendmail 버전 점검	상	N/A
서비스 관리	U-31	스팸 메일 릴레이 제한	상	양호
서비스 관리	U-32	일반사용자의 Sendmail 실행 방지	상	양호
서비스 관리	U-33	DNS 보안 버전 패치	상	양호
서비스 관리	U-34	DNS ZoneTransfer 설정	상	양호
패치 및 로그관리	U-35	최신 보안패치 및 벤더 권고사항 적용	상	N/A
패치 및 로그관리	U-36	로그의 정기적 검토 및 보고	상	N/A

Linux 조치사항 (페이지 1)

진단코드	진단항목	조치방법
U-01	root 계정 원격 접속 제한	Telnet의 경우 /etc/securetty 파일에서 pts/0 ~ pts/x 설정 제거 또는, 주석 처리 | SSH의 경우 vi /etc/ssh/sshd_config 에서 PermitRootLogin no 로 설정
U-03	계정 잠금 임계값 설정	Debian 계열의 경우 /etc/pam.d/common-auth 파일 내 설정 값을 변경 RHEL 계열의 경우 /etc/pam.d/system-auth 및 /etc/pam.d/password-auth 파일 내 설정값을 변경
U-04	패스워드 최대 사용 기간 설정	User 생성 시에 vi /etc/login.defs 파일에서 PASS_MAX_DAYS를 90으로 설정 또는 현재 User의 최대 사용기간을 적용 chage -M 90 < 계정명 >
U-07	파일 및 디렉토리 소유자 설정	소유자가 존재하지 않는 파일이나 디렉터리가 불필요한 경우 rm 명령으로 삭제, 필요한 경우 chown 명령으로 소유자 및 그룹 변경
U-09	/etc/shadow 파일 소유자 및 권한 설정	/etc/shadow 파일의 소유자 및 권한 변경 (소유자 root, 권한 400)
U-15	사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정	chown 명령을 통해 소유자를 변경하거나 chmod 명령을 통해 일반 사용자 쓰기 권한 제거
U-16	world writable 파일 점검	chmod 명령을 통해 일반 사용자 쓰기 권한 제거하거나 파일을 삭제
U-19	cron 파일 소유자 및 권한 설정	/etc/cron.allow 및 /etc/cron.deny 파일의 소유자 및 권한 변경
U-24	NFS 서비스 비활성화	NFS 데몬(nfsd)을 중지