목차

보안 취약점 점검 가이드(KISA 기준) 3
계정관리 3
root 계정 원격 접속 제한 3
패스워드 복잡성 설정 3
계정 잠금 임계값 설정 3
패스워드 파일 보호 3
root 이외의 UID가 '0' 금지 4
root 계정 su 제한 4
패스워드 최소 길이 설정 4
패스워드 최대 사용기간 설정 4
패스워드 최소 사용기간 설정 4
불필요한 계정 제거 4
관리자 그룹에 최소한의 계정 포함 4
계정이 존재하지 않는 GID 금지 4
동일한 UID 금지 5
사용자 shell 점검 5
session timeout 설정 5
파일 및 디렉터리 관리 5
root 홈, 패스 디렉터리 권한 및 패스 설정 5
파일 및 디렉터리 소유자 설정 5
/etc/passwd 파일 소유자 및 권한 설정 5
/etc/shadow 파일 소유자 및 권한 설정 5
/etc/hosts 파일 소유자 및 권한 설정 5
/etc/(x)inetd.conf 파일 소유자 및 권한 설정 6
/etc/syslog.conf 파일 소유자 및 권한 설정 6
/etc/services 파일 소유자 및 권한 설정 6
SUID, SGID, Sticky bit 설정 파일 점검 6
사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정 6
world writable 파일 점검 6
/dev에 존재하지 않는 device 파일 점검 6
$HOME/.rhosts, hosts.equiv 사용 금지 7
접속 IP 및 포트 제한 7
hosts.lpd 파일 소유자 및 권한 설정 7
UMASK 설정 관리 중 U-56 7
홈디렉토리 소유자 및 권한 설정 7
홈디렉토리로 지정한 디렉토리의 존재 관리 7
숨겨진 파일 및 디렉토리 검색 및 제거 7
finger 서비스 비활성화 7
Anonymous FTP 비활성화 8
r 계열 서비스 비활성화 8
cron 파일 소유자 및 권한설정 8
Dos 공격에 취약한 서비스 비활성화 8
NFS 서비스 비활성화 8
NFS 접근 통제 8
automountd 제거 8
RPC 서비스 확인 8
NIS, NIS+ 점검 8
tftp, talk 서비스 비활성화 9
Sendmail 버전 점검 9

스팸 메일 릴레이 제한 9
일반사용자의 Sendmail 실행 방지 9
DNS 보안 버전 패치 9
DNS Zone Transfer 설정 9
웹서비스 디렉토리 리스팅 제거 9
웹서비스 웹 프로세스 권한 제한 9
웹서비스 상위 디렉토리 접근 금지 10
웹서비스 불필요한 파일 제거 10
웹서비스 링크 사용 금지 10
웹서비스 파일 업로드 및 다운로드 제한 10
웹서비스 영역의 분리 10
ssh 원격접속 허용 10
ftp 서비스 확인 10
ftp 계정 shell 제한 10
Ftpusers 파일 소유자 및 권한 설정 10
Ftpusers 파일 설정 11
at 파일 소유자 및 권한 설정 11
SNMP 서비스 구동 점검 11
SNMP 서비스 커뮤니티스트링의 복잡성 설정 11
로그온 시 경고 메시지 제공 11
NFS 설정파일 접근 제한 11
expn, vrfy 명령어 제한 11
Apache 웹 서비스 정보 숨김 11
패치 관리 12
최신 보안패치 및 벤더 권고사항 적용 12
로그 관리 12
로그의 정기적 검토 및 보고 12
정책에 따른 시스템 로깅 설정 12

보안 취약점 점검 가이드(KISA 기준)

— *이강우 2024/10/22 04:29*

작성중

본 내용은 KISA 한국인터넷진흥원 제공 주요정보통신기반시설 기술적 취약점 분석 평가 상세 가이드에 기반한 **리눅스 시스템 보안 취약점 적용 방법**에 대해 기술한 문서입니다.

리눅스 배포판별(debian/ubuntu, RedHat/Rocky/CentOS), 또는 버전별로 취약점 조치를 진행하는 방법에 대해 설명합니다. **조치권장여부** 항목은 본 사이트에서 적용여부를 권장하는 항목으로 비권장으로 되어있는것은 적용하지 않는것을 권장합니다. 이는 해당 리눅스 벤더/커뮤니티에서 일반적으로 적용하지 않을 것을 권장하는 항목들이거나, 조치할 경우 운영상 또는 다른 SW등에 영향이 있을것으로 예상되는 항목입니다. 또한 조치 하지 않아도 보통 보안에 취약하지 않는 항목들로서 과거 아주 오래전 버전이나 유닉스에 존재하던 취약점이나 버그들로 인한것으로 현대의 리눅스에서는 취약하다고 평가되지 않습니다.

KISA에서 배포중인 문서또한 2021년 자료이므로 가급적 현재 사용중인 OS버전에 맞는 조치사항을 적용하는것을 권장한다.

계정관리

root 계정 원격 접속 제한

분류	점검항목	항목중요도	항목코드	조치권장여부
계정관리	**root 계정 원격 접속 제한**	상	U-01	**권장**

패스워드 복잡성 설정

분류	점검항목	항목중요도	항목코드	조치권장여부
계정관리	**패스워드 복잡성 설정**	상	U-02	**권장**

계정 잠금 임계값 설정

분류	점검항목	항목중요도	항목코드	조치권장여부
계정관리	**계정 잠금 임계값 설정**	상	U-03	**권장**

패스워드 파일 보호

분류	점검항목	항목중요도	항목코드	
계정관리	**패스워드 파일 보호**	상	U-04	**비권장**

root 이외의 UID가 '0' 금지

분류	점검항목	항목중요도	항목코드	
계정관리	**root 이외의 UID가 '0' 금지**	중	U-44	**권장**

root 계정 su 제한

분류	점검항목	항목중요도	항목코드	
계정관리	**root 계정 su 제한**	하	U-45	**권장**

패스워드 최소 길이 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**패스워드 최소 길이 설정**	중	U-46	**권장**

패스워드 최대 사용기간 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**패스워드 최대 사용기간 설정**	중	U-47	**비권장**

패스워드 최소 사용기간 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**패스워드 최소 사용기간 설정**	중	U-48	**비권장**

불필요한 계정 제거

분류	점검항목	항목중요도	항목코드	
계정관리	**불필요한 계정 제거**	하	U-49	**비권장**

관리자 그룹에 최소한의 계정 포함

분류	점검항목	항목중요도	항목코드	
계정관리	**관리자 그룹에 최소한의 계정 포함**	하	U-50	**비권장**

계정이 존재하지 않는 GID 금지

분류	점검항목	항목중요도	항목코드	
계정관리	**계정이 존재하지 않는 GID 금지**	중	U-51	**비권장**

동일한 UID 금지

분류	점검항목	항목중요도	항목코드	
계정관리	**동일한 UID 금지**	중	U-52	**권장**

사용자 shell 점검

분류	점검항목	항목중요도	항목코드	
계정관리	**사용자 shell 점검**	하	U-53	**권장**

session timeout 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**session timeout 설정**	하	U-54	**권장**

파일 및 디렉터리 관리

root 홈, 패스 디렉터리 권한 및 패스 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**root 홈, 패스 디렉터리 권한 및 패스 설정**	상	U-05	**권장**

파일 및 디렉터리 소유자 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**파일 및 디렉터리 소유자 설정**	상	U-06	**권장**

/etc/passwd 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**/etc/passwd 파일 소유자 및 권한 설정**	상	U-07	**권장**

/etc/shadow 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**/etc/shadow 파일 소유자 및 권한 설정**	상	U-08	**권장**

/etc/hosts 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**/etc/hosts 파일 소유자 및 권한 설정**	상	U-09	**권장**

/etc/(x)inetd.conf 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**/etc/(x)inetd.conf 파일 소유자 및 권한 설정**	상	U-10	**권장**

/etc/syslog.conf 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**/etc/syslog.conf 파일 소유자 및 권한 설정**	상	U-11	**권장**

/etc/services 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**/etc/services 파일 소유자 및 권한 설정**	상	U-12	**권장**

SUID, SGID, Sticky bit 설정 파일 점검

분류	점검항목	항목중요도	항목코드	
계정관리	**SUID, SGID, Sticky bit 설정 파일 점검**	상	U-13	**권장**

사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**사용자, 시스템 시작파일 및 환경파일 소유자 및 권한 설정**	상	U-14	**권장**

world writable 파일 점검

분류	점검항목	항목중요도	항목코드	
계정관리	**world writable 파일 점검**	상	U-15	**권장**

/dev에 존재하지 않는 device 파일 점검

분류	점검항목	항목중요도	항목코드	
계정관리	**/dev에 존재하지 않는 device 파일 점검**	상	U-16	**권장**

$HOME/.rhosts, hosts.equiv 사용 금지

분류	점검항목	항목중요도	항목코드	
계정관리	**$HOME/.rhosts, hosts.equiv 사용 금지**	상	U-17	권장

접속 IP 및 포트 제한

분류	점검항목	항목중요도	항목코드	
계정관리	**접속 IP 및 포트 제한**	상	U-18	권장

hosts.lpd 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**hosts.lpd 파일 소유자 및 권한 설정**	하	U-55	권장

UMASK 설정 관리 중 U-56

분류	점검항목	항목중요도	항목코드	
계정관리	**UMASK 설정 관리**	중	U-56	권장

홈디렉토리 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**홈디렉토리 소유자 및 권한 설정**	중	U-57	권장

홈디렉토리로 지정한 디렉토리의 존재 관리

분류	점검항목	항목중요도	항목코드	
계정관리	**홈디렉토리로 지정한 디렉토리의 존재 관리**	중	U-58	권장

숨겨진 파일 및 디렉토리 검색 및 제거

분류	점검항목	항목중요도	항목코드	
계정관리	**숨겨진 파일 및 디렉토리 검색 및 제거**	하	U-59	권장

finger 서비스 비활성화

분류	점검항목	항목중요도	항목코드	
계정관리	**finger 서비스 비활성화**	상	U-19	권장

Anonymous FTP 비활성화

분류	점검항목	항목중요도	항목코드	
계정관리	**Anonymous FTP 비활성화**	상	U-20	**권장**

r 계열 서비스 비활성화

분류	점검항목	항목중요도	항목코드	
계정관리	**r 계열 서비스 비활성화**	상	U-21	**권장**

cron 파일 소유자 및 권한설정

분류	점검항목	항목중요도	항목코드	
계정관리	**cron 파일 소유자 및 권한 설정**	상	U-22	**권장**

Dos 공격에 취약한 서비스 비활성화

분류	점검항목	항목중요도	항목코드	
계정관리	**Dos 공격에 취약한 서비스 비활성화**	상	U-23	**권장**

NFS 서비스 비활성화

분류	점검항목	항목중요도	항목코드	
계정관리	**NFS 서비스 비활성화**	상	U-24	**권장**

NFS 접근 통제

분류	점검항목	항목중요도	항목코드	
계정관리	**NFS 접근 통제**	상	U-25	**권장**

automountd 제거

분류	점검항목	항목중요도	항목코드	
계정관리	**automountd 제거**	상	U-26	**권장**

RPC 서비스 확인

분류	점검항목	항목중요도	항목코드	
계정관리	**RPC 서비스 확인**	상	U-27	**권장**

NIS, NIS+ 점검

분류	점검항목	항목중요도	항목코드	
계정관리	**NIS, NIS+ 점검**	상	U-28	**권장**

tftp, talk 서비스 비활성화

분류	점검항목	항목중요도	항목코드	
계정관리	**tftp, talk 서비스 비활성화**	상	U-29	**권장**

Sendmail 버전 점검

분류	점검항목	항목중요도	항목코드	
계정관리	**Sendmail 버전 점검**	상	U-30	**권장**

스팸 메일 릴레이 제한

분류	점검항목	항목중요도	항목코드	
계정관리	**스팸 메일 릴레이 제한**	상	U-31	**권장**

일반사용자의 Sendmail 실행 방지

분류	점검항목	항목중요도	항목코드	
계정관리	**일반사용자의 Sendmail 실행 방지**	상	U-32	**권장**

DNS 보안 버전 패치

분류	점검항목	항목중요도	항목코드	
계정관리	**DNS 보안 버전 패치**	상	U-33	**권장**

DNS Zone Transfer 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**DNS Zone Transfer 설정**	상	U-34	**권장**

웹서비스 디렉토리 리스팅 제거

분류	점검항목	항목중요도	항목코드	
계정관리	**웹서비스 디렉토리 리스팅 제거**	상	U-35	**권장**

웹서비스 웹 프로세스 권한 제한

분류	점검항목	항목중요도	항목코드	
계정관리	**웹서비스 웹 프로세스 권한 제한**	상	U-36	**권장**

웹서비스 상위 디렉토리 접근 금지

분류	점검항목	항목중요도	항목코드	
계정관리	**웹서비스 상위 디렉토리 접근 금지**	상	U-37	**권장**

웹서비스 불필요한 파일 제거

분류	점검항목	항목중요도	항목코드	
계정관리	**웹서비스 불필요한 파일 제거**	상	U-38	**권장**

웹서비스 링크 사용 금지

분류	점검항목	항목중요도	항목코드	
계정관리	**웹서비스 링크 사용 금지**	상	U-39	**권장**

웹서비스 파일 업로드 및 다운로드 제한

분류	점검항목	항목중요도	항목코드	
계정관리	**웹서비스 파일 업로드 및 다운로드 제한**	상	U-40	**권장**

웹서비스 영역의 분리

분류	점검항목	항목중요도	항목코드	
계정관리	**웹서비스 영역의 분리**	상	U-41	**권장**

ssh 원격접속 허용

분류	점검항목	항목중요도	항목코드	
계정관리	**ssh 원격접속 허용**	중	U-60	**권장**

ftp 서비스 확인

분류	점검항목	항목중요도	항목코드	
계정관리	**ftp 서비스 확인**	하	U-61	**권장**

ftp 계정 shell 제한

분류	점검항목	항목중요도	항목코드	
계정관리	**ftp 계정 shell 제한**	중	U-62	**권장**

Ftpusers 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**Ftpusers 파일 소유자 및 권한 설정**	하	U-63	**권장**

Ftpusers 파일 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**Ftpusers 파일 설정**	중	U-64	**권장**

at 파일 소유자 및 권한 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**at 파일 소유자 및 권한 설정**	중	U-65	**권장**

SNMP 서비스 구동 점검

분류	점검항목	항목중요도	항목코드	
계정관리	**SNMP 서비스 구동 점검**	중	U-66	**권장**

SNMP 서비스 커뮤니티스트링의 복잡성 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**SNMP 서비스 커뮤니티스트링의 복잡성 설정**	중	U-67	**권장**

로그온 시 경고 메시지 제공

분류	점검항목	항목중요도	항목코드	
계정관리	**로그온 시 경고 메시지 제공**	하	U-68	**권장**

NFS 설정파일 접근 제한

분류	점검항목	항목중요도	항목코드	
계정관리	**NFS 설정파일 접근 제한**	중	U-69	**권장**

expn, vrfy 명령어 제한

분류	점검항목	항목중요도	항목코드	
계정관리	**expn, vrfy 명령어 제한**	중	U-70	**권장**

Apache 웹 서비스 정보 숨김

분류	점검항목	항목중요도	항목코드	
계정관리	**Apache 웹 서비스 정보 숨김**	중	U-71	**권장**

패치 관리

최신 보안패치 및 벤더 권고사항 적용

분류	점검항목	항목중요도	항목코드	
계정관리	**최신 보안패치 및 벤더 권고사항 적용**	상	U-42	**권장**

로그 관리

로그의 정기적 검토 및 보고

분류	점검항목	항목중요도	항목코드	
계정관리	**로그의 정기적 검토 및 보고**	상	U-43	**권장**

정책에 따른 시스템 로깅 설정

분류	점검항목	항목중요도	항목코드	
계정관리	**정책에 따른 시스템 로깅 설정**	하	U-72	**권장**

From:
https://atl.kr/dokuwiki/ - **AllThatLinux!**

Permanent link:
https://atl.kr/dokuwiki/doku.php/%EB%B3%B4%EC%95%88_%EC%B7%A8%EC%95%BD%EC%A0%90_%EC%A0%90%EA%B2%80_%EA%B0%80%EC%9D%B4%EB%93%9C_kisa%EA%B8%B0%EC%A4%80

Last update: **2025/07/09 12:47**