DNA Lab OS Security Scan Report

Date: 2026-01-04 19:57:12

Target: http://35.166.49.142/

50	14	36	79
Total Scans	Vulnerable	Safe	Total Findings

1. OS: Root 원격 로그인 제한 — SAFE

DETAILS

- [OS] SSH가 실행되고 있지 않음
- [OS] Telnet이 실행되고 있지 않음

RECOMMENDATION

안전 - Root 원격 로그인이 제한되어 있음

2. OS: 비밀번호 관리정책 설정 — VULNERABLE

DETAILS

- [OS] PASS_MAX_DAYS: 양호 (현재값: 99999)
- [OS] PASS_MIN_DAYS: 양호 (현재값: 0)
- [OS] minlen 설정이 없음
- [OS] dcredit 설정이 없음
- [OS] ucredit 설정이 없음
- [OS] lcredit 설정이 없음
- [OS] ocredit 설정이 없음
- [OS] enforce_for_root 설정이 없음
- [OS] pam_pwquality.so 위치가 pam_unix.so보다 뒤에 있음
- [OS] pam_pwhistory.so 위치가 pam_unix.so보다 뒤에 있음

RECOMMENDATION

ocredit를 -1 이상으로 설정 | lcredit를 -1 이상으로 설정 | pam_pwhistory.so를 pam_unix.so 위로 이동 | pwquality.conf에 enforce_for_root 추가 | ucredit를 -1 이상으로 설정 | pam_pwquality.so를 pam_unix.so 위로 이동 | dcredit를 -1 이상으로 설정 | minlen를 8 이상으로 설정

3. OS: 계정 잠금 임계값 설정 VULNERABLE

DETAILS

- [OS] pam_tally/pam_tally2 auth 설정이 없음
- [OS] pam_tally/pam_tally2 account 설정이 없음

RECOMMENDATION

common-auth에 pam_tally(2).so deny=10 unlock_time=120 no_magic_root 설정 추가 | account required pam_tally(2).so no_magic_root reset 설정 추가

4. OS: 패스워드 파일 보호 SAFE

DETAILS

- [OS] 패스워드 파일 보호: 양호 (모든 계정이 shadow 파일 사용)

RECOMMENDATION

안전 - 패스워드 파일이 적절히 보호되어 있음

5. OS: root 이외 UID 0 금지 SAFE

DETAILS

- [OS] root 이외 UID 0 계정 없음 (양호)

RECOMMENDATION

안전 - root 이외 UID 0 계정이 없음

6. OS: 사용자 계정 su 기능 제한 VULNERABLE

DETAILS

- [OS] pam_wheel.so 설정이 없음

RECOMMENDATION

/etc/pam.d/su에 pam_wheel.so 설정 추가

7. OS: 계정이 존재하지 않는 GID SAFE

DETAILS

- [OS] 존재하지 않는 GID 사용 계정 없음 (양호)

RECOMMENDATION

안전 - GID 설정이 유효함

8. OS: 동일한 UID 금지 SAFE

DETAILS

- [OS] 동일한 UID 없음 (양호)

RECOMMENDATION

안전 - 동일한 UID가 없음

9. OS: 사용자 shell 점검 SAFE

DETAILS

- [OS] 로그인 불필요 계정 쉘 설정: 양호

RECOMMENDATION

안전 - 로그인 불필요 계정의 쉘이 제한됨

10. OS: 세션 종료 시간 설정 VULNERABLE

DETAILS

- [OS] TMOUT 설정이 없음

RECOMMENDATION

TMOUT을 600 이하로 설정

11. OS: 안전한 비밀번호 암호화 알고리즘 사용 SAFE

DETAILS

- [OS] ENCRYPT_METHOD: 양호 (SHA512)
- [OS] pam_unix.so SHA-2/YESCRYPT 설정: 양호

RECOMMENDATION

안전 - 안전한 비밀번호 암호화 알고리즘이 설정됨

12. OS: Root 홈, PATH 설정 SAFE

DETAILS

- [OS] PATH에 현재 디렉터리가 포함되지 않음 (양호)

RECOMMENDATION

안전 - PATH 설정이 적절함

13. OS: 파일 및 디렉터리 소유자 설정 SAFE

DETAILS

- [OS] 소유자/그룹 미지정 파일 없음 (양호)

RECOMMENDATION

안전 - 소유자 및 그룹이 적절히 설정됨

14. OS: /etc/passwd 파일 소유자 및 권한 설정 SAFE

DETAILS

- [OS] /etc/passwd 소유자: 양호 (root)
- [OS] /etc/passwd 권한: 양호 (644)

RECOMMENDATION

안전 - /etc/passwd 권한이 적절함

15. OS: 시스템 시작 스크립트 권한 설정 SAFE

DETAILS

- [OS] 시스템 시작 스크립트 권한: 양호

RECOMMENDATION

안전 - 시스템 시작 스크립트 권한이 적절함

16. OS: /etc/shadow 파일 소유자 및 권한 설정 VULNERABLE

DETAILS

- [OS] /etc/shadow 소유자: 양호 (root)
- [OS] /etc/shadow 권한: 취약 (640)

RECOMMENDATION

/etc/shadow 권한을 400 이하로 설정

17. OS: /etc/hosts 파일 소유자 및 권한 설정 SAFE

DETAILS

- [OS] /etc/hosts 소유자: 양호 (root)
- [OS] /etc/hosts 권한: 양호 (644)

RECOMMENDATION

안전 - /etc/hosts 권한이 적절함

18. OS: /etc/inetd.conf 파일 소유자 및 권한 설정 SAFE

DETAILS

- [OS] /etc/inetd.conf 파일 없음 (양호)

RECOMMENDATION

안전 - /etc/inetd.conf 권한이 적절함

19. OS: /etc/(r)syslog.conf 파일 소유자 및 권한 설정 VULNERABLE

DETAILS

- [OS] /etc/rsyslog.conf 소유자: 양호 (root)
- [OS] /etc/rsyslog.conf 권한: 취약 (644)

- [OS] /etc/rsyslog.d/50-default.conf 소유자: 양호 (root)
- [OS] /etc/rsyslog.d/50-default.conf 권한: 취약 (644)

RECOMMENDATION

/etc/rsyslog.conf 권한을 640 이하로 설정 | /etc/rsyslog.d/50-default.conf 권한을 640 이하로 설정

20. OS: /etc/services 파일 소유자 및 권한 설정 SAFE

DETAILS

- [OS] /etc/services 소유자: 양호 (root)
- [OS] /etc/services 권한: 양호 (644)

RECOMMENDATION

안전 - /etc/services 권한이 적절함

21. OS: SUID, SGID 설정 파일 점검 SAFE

DETAILS

- [OS] SUID/SGID 설정 파일 없음 (양호)

RECOMMENDATION

안전 - SUID/SGID 설정이 적절히 관리됨

22. OS: 사용자 환경변수 파일 소유자 및 권한 설정 SAFE

DETAILS

- [OS] 사용자 환경변수 파일 권한: 양호

RECOMMENDATION

안전 - 사용자 환경변수 파일 권한이 적절함

23. OS: .rhosts/hosts.equiv 사용 금지 SAFE

DETAILS

- [OS] /etc/hosts.equiv 파일 없음 (양호)
- [OS] .rhosts 파일 없음 (양호)

RECOMMENDATION

안전 - .rhosts/hosts.equiv 사용 금지

24. OS: 접속 IP 및 포트 제한 SAFE

DETAILS

- [OS] 접속 IP/포트 제한 설정: 양호

RECOMMENDATION

안전 - 접속 IP 및 포트 제한이 설정됨

25. OS: hosts.lpd 파일 소유자 및 권한 설정 SAFE

DETAILS

- [OS] /etc/hosts.lpd 파일 없음 (양호)

RECOMMENDATION

안전 - hosts.lpd 권한이 적절함

26. OS: UMASK 설정 관리 VULNERABLE

DETAILS

- [OS] /etc/profile umask 설정 없음
- [OS] /etc/login.defs UMASK: 양호 (022)

RECOMMENDATION

/etc/profile에 umask 022 이상 설정

27. OS: 홈디렉토리 소유자 및 권한 설정 SAFE

DETAILS

- [OS] 홈디렉토리 소유자 및 권한: 양호

RECOMMENDATION

안전 - 홈디렉토리 권한이 적절함

28. OS: 홈 디렉토리 존재 여부 SAFE

DETAILS

- [OS] 홈 디렉토리 존재 여부: 양호

RECOMMENDATION

안전 - 홈 디렉토리가 모두 존재함

29. OS: Finger 서비스 비활성화 SAFE

DETAILS

- [OS] Finger 서비스 비활성화: 양호

RECOMMENDATION

안전 - Finger 서비스가 비활성화됨

30. OS: 공유 서비스 익명 접근 제한 SAFE

DETAILS

- [OS] 익명 접근 설정 없음 (양호)

RECOMMENDATION

안전 - 공유 서비스 익명 접근이 제한됨

31. OS: r 계열 서비스 비활성화 SAFE

DETAILS

- [OS] r 계열 서비스 비활성화: 양호

RECOMMENDATION

안전 - r 계열 서비스가 비활성화됨

32. OS: crontab 설정파일 권한 설정 미흡 VULNERABLE

DETAILS

- [OS] cron/at 관련 파일 권한 취약
- - /etc/crontab (owner=root, perm=644)

RECOMMENDATION

cron/at 관련 파일 소유자 root 및 권한 640 이하 설정

33. OS: DoS 서비스 비활성화 SAFE

DETAILS

- [OS] DoS 취약 서비스 비활성화: 양호

RECOMMENDATION

안전 - DoS 취약 서비스가 비활성화됨

34. OS: 불필요한 NFS 서비스 비활성화 VULNERABLE

DETAILS

- [OS] NFS 관련 서비스가 활성화되어 있음
- [OS] 활성 서비스: nfs-server, nfs, rpcbind, nfs-mountd

RECOMMENDATION

불필요한 NFS 서비스 비활성화

35. OS: NFS 접근 통제 SAFE

DETAILS

- [OS] /etc/exports 파일 없음 (양호)

RECOMMENDATION

안전 - NFS 접근 통제가 적절함

36. OS: 불필요한 automountd 제거 SAFE

DETAILS

- [OS] automount/autofs 서비스 비활성화: 양호

RECOMMENDATION

안전 - automount/autofs 서비스가 비활성화됨

37. OS: RPC 서비스 비활성화 SAFE

DETAILS

- [OS] RPC 서비스 비활성화: 양호

RECOMMENDATION

안전 - RPC 서비스가 비활성화됨

38. OS: NIS/NIS+ 점검 SAFE

DETAILS

- [OS] NIS/NIS+ 서비스 비활성화: 양호

RECOMMENDATION

안전 - NIS/NIS+ 서비스가 비활성화됨

39. OS: tftp/talk 서비스 비활성화 SAFE

DETAILS

- [OS] tftp/talk 서비스 비활성화: 양호

RECOMMENDATION

안전 - tftp/talk 서비스가 비활성화됨

40. OS: Telnet 서비스 비활성화 SAFE

DETAILS

- [OS] Telnet 서비스 비활성화: 양호

RECOMMENDATION

안전 - Telnet 서비스가 비활성화됨

41. OS: FTP 배너 정보 노출 제한 SAFE

DETAILS

- [OS] vsftpd 설정 파일 없음 (FTP 미사용)

RECOMMENDATION

안전 - FTP 배너 정보 노출이 제한됨

42. OS: 암호화되지 않는 FTP 서비스 비활성화 VULNERABLE

DETAILS

- [OS] FTP 서비스가 활성화되어 있음
- [OS] 활성 서비스: vsftpd, proftpd, pure-ftpd, ftp

RECOMMENDATION

암호화되지 않는 FTP 서비스 비활성화

43. OS: FTP 계정 shell 제한 SAFE

DETAILS

- [OS] FTP 계정 쉘 제한: 양호

RECOMMENDATION

안전 - FTP 계정 쉘이 제한됨

44. OS: FTP 접근 제어 설정 VULNERABLE

DETAILS

- [OS] ftpusers 파일 없음

RECOMMENDATION

ftpusers 파일 생성 및 권한 설정

45. OS: Ftpusers 파일 설정 VULNERABLE

DETAILS

- [OS] ftpusers 파일 없음

RECOMMENDATION

ftpusers 파일에 root 계정 차단 설정 추가

46. OS: 불필요한 SNMP 서비스 구동 점검 VULNERABLE

DETAILS

- [OS] snmpd 서비스가 활성화되어 있음

RECOMMENDATION

불필요한 snmpd 서비스 비활성화

47. OS: sudo 명령어 접근 관리 SAFE

DETAILS

- [OS] /etc/sudoers 소유자: 양호 (root)
- [OS] /etc/sudoers 권한: 양호 (440)

RECOMMENDATION

안전 - /etc/sudoers 권한이 적절함

48. OS: NTP 및 시각 동기화 설정 SAFE

DETAILS

- [OS] NTP 동기화 서비스 활성화: chronyd, ntpd, ntp, systemd-timesyncd, timedatectl

RECOMMENDATION

안전 - 시각 동기화 설정이 적용됨

49. OS: 정책에 따른 시스템 로깅 설정 SAFE

DETAILS

- [OS] 로깅 정책 설정: 양호

RECOMMENDATION

안전 - 로깅 정책이 설정됨

50. OS: 로그 디렉터리 소유자 및 권한 설정 VULNERABLE

DETAILS

- [OS] 로그 파일 소유자/권한 문제 발견
- - /var/log/cloud-init.log (owner=syslog, perm=640)
- - /var/log/auth.log (owner=syslog, perm=640)
- - /var/log/kern.log (owner=syslog, perm=640)
- - /var/log/syslog (owner=syslog, perm=640)

RECOMMENDATION

로그 파일 소유자를 root로, 권한을 644 이하로 설정