Linux 서버 취약점 점검 자동화 스크립트

ASC 25-2 프로젝트 최종 발표

Team : Croncrew

이예빈 김동후 김레빈 양상윤 정태영 최재웅

프로젝트 개요

리눅스 서버 보안 사고의 지속적 증가 및 고도화

계정 관리 미흡 및 설정 오류 등 기초 보안 설정 부재

수동 점검의 한계 : 누락 발생 및 판단 오류 가능성

자동화 스크립트를 통한 보안 점검의 효율성 극대화

관리자가 즉시 이해 가능한 직관적인 결과 및 위험 제시

KISA 보안 가이드라인, CIS 기준 기반의 체계적인 보안 기준 수립

취약점 분류(1)

// 주요 점검 항목 : 계정 및 권한 관리

항목 코드	점검 내용	주요 위협 요소
U-01	sudo 명령어 과다 허용	비인가 사용자의 루트 권한 획득 및 시스템 설정 무단 변경
U-02	비밀번호 복잡도 설정	단순한 비밀번호 사용으로 인한 무차별 대입(brute force) 취약
U-03	계정 잠금 임계값 설정	반복적인 로그인 시도 차단 불가로 인한 계정 탈취 위험
U-08	/etc/shadow 권한 설정	비밀번호 해시값 노출로 인한 오프라인 크래킹 공격 가능성
U-09	파일/디렉터리 소유자 설정	시스템 핵심 파일 변조를 통한 권한 상승 및 서비스 조작

취약점 분류(2)

// 주요 점검 항목 : 서비스 및 파일 시스템 보안

항목 코드	점검 내용	주요 위협 요소
U-10	xinetd.conf 권한 설정	비인가자의 악의적인 서비스 등록 및 임의 명령 실행 위험
U-13	SUID/SGID 설정 점검	불필요한 권한 획득을 통한 시스템 보안 정책 우회 및 탈취
U-14	사용자 환경 파일 권한	환경 파일 변조를 통한 악성 스크립트 실행 및 계정 탈취
U-16	/dev 내 device 파일 점검	루트킷(Rootkit) 또는 백도어 프로그램의 은닉 여부 탐지
U-19	finger 서비스 활성화	사용자 정보 노출을 통한 추가 공격 정보(계정명 등) 제공
U-20	Anonymous FTP 비활성화	익명 접속을 통한 정보 유출 및 악성코드 유포 경로 활용
U-71	Apache 설정 파일 점검	웹 서버 비전 및 시스템 민감 정보 노출로 인한 타겟 공격

전체 시스템 구조

// 점검 및 개선 프로세스(workflow)

1. **초기 점검 수행**

   루트 권한으로 sudo ./uni.sh 실행 및 환경 초기화

2. **취약 항목 확인**

   항목별 OK/WARN 판정 및 unified_check_result.txt 생성

3. **보안 설정 수정**

   가이드라인에 따라 /etc, pam 등 설정 파일 조정

4. **점검 재수행**

   수정 사항 반영 여부 확인 및 최종 통계(양호/취약 건수) 출력

점검 기준 및 구현 (1)

// 핵심 보안 설정 기준 : 계정 및 인증

U-01 sudo 권한 제한

> NOPASSWD 옵션 사용 여부 전수 조사

> 비루트 사용자의 ALL=(ALL) ALL 권한 허용 점검

> 불필요한 관리자 권한 부여 항목 식별 및 로그 기록

Target : /etc/sudoers, /etc/sudoers.d/*

U-02 비밀번호 복잡도 설정

> 최소 길이 10자 이상 준수 여부 확인

> 숫자, 대문자, 소문자, 특수문자 각 2개 이상 포함 강제화

> PASS_MAX_DAYS, PASS_MIN_DAYS 등 유효기간 정책 점검

Target : /etc/login.defs, /etc/security/pwquality.conf*

U-03 계정 잠금 임계값

> 로그인 실패 시 계정 잠금 활성화 여부 확인

> 임계값을 10회 이하로 설정하여 무차별 대입 방어

> PAM 모듈(pam_tally2 또는 faillock) 설정 대조

Target : /etc/pam.d/system-auth,
/etc/pam.d/password-auth

점검 기준 및 구현 (2)

// 핵심 보안 설정 기준 : 권한 관리

U-08 shadow 파일 권한

> 소유자가 root로 설정되어 있는지 점검

> 권한이 400 또는 000으로 설정되어있는지 확인

> group/other에게 부여된 불필요한 권한 제거

Target : /etc/shadow

U-09 중요 파일 소유자 및 권한

> passwd, shadow, group 등 핵심 파일 소유자 root 통일

> 불필요한 실행 권한 및 쓰기 권한 부여 여부 전수 조사

> 잘못된 권한으로 인한 권한 상승 및 서비스 조작 방지

Target : /etc/passwd, /etc/group, /etc/hosts, /etc/services

U-14 환경 파일 권한

> 홈 디렉터리 시작 파일의 소유자 root 여부 확인

> 타 사용자의 수정 및 접근 제한(권한 644/600)

> 파일 무결성 보장을 위한 권한 설정 상태 점검

Target : /etc/profile.d/*, ~/.bashrc 등

점검 기준 및 구현 (3)

// 핵심 보안 설정 기준 : 계정 및 인증

U-10/13 특수 권한 및 설정

> xinetd.conf 소유자 root 및 권한 설정 점검

> 불필요한 SUID/SGID 바이너리(dump, lpr 등) 제거

> 비인가 서비스 등록 및 권한 상승 경로 원천 차단

Target : /etc/xinetd.conf, /usr/bin/*, /usr/sbin/*

U-16/19 무결성 및 정보 노출

> /dev 디렉터리 내 비정상 일반 파일 존재 여부 탐지

> finger 서비스 비활성화 상태 점검(사용자 정보 보호)

> 백도어 은닉 방지 및 공격 정보 수집 경로 차단

Target : /dev/, /etc/xinetd.d/finger

U-20/71 FTP 및 웹 서버 보안

> Anonymous FTP 익명 로그인 차단 및 디렉터리 권한 강화

> Apache ServerTokens(Prod), ServerSignature(Off) 설정 확인

> 익명 접속을 통한 정보 유출 방지 및 서버 민감 정보 노출 최소화

Target : /etc/login.defs, /etc/security/pwquality.conf*

테스트 및 검증

// 다양한 시나리오 기반 실효성 확인

#01. 완전 취약 상태(Full Vulnerable)

> 모든 점검 항목에 취약 설정 적용 : 스크립트의 탐지 정확도 검증; WARN 판정 및 원인 출력 확인

```
[H[2J[3J==========================================
리눅스 서버 점검 자동화 통합 프로그램
실행 시각: 2025-12-20 17:22:24
==========================================

================================================
[U-01. sudo 명령어 과다 허용 점검]
================================================
INFO: /etc/sudoers 파일이 존재합니다.
INFO: /etc/sudoers.d 디렉터리가 존재합니다.
OK: NOPASSWD 설정이 발견되지 않았습니다.
WARN: root 이외 사용자/그룹에 대해 ALL=(ALL) ALL 이 허용된 설정이 발견되었습니다:
      /etc/sudoers:50:%admin ALL=(ALL) ALL
INFO: /var/log/auth.log 파일이 존재합니다. sudo 로그 기록 여부를 확인합니다.
OK: sudo 실행 로그가 /var/log/auth.log 에 기록되고 있습니다.
================================================
결과: 취약
권장 조치: sudo visudo 명령으로 /etc/sudoers 편집
          - NOPASSWD 설정 제거
          - 최소 권한 원칙 적용 (화이트리스트 방식)
          예시: username ALL=(ALL) /usr/bin/systemctl, /usr/bin/ls
```

```
================================================
[최종 점검 요약]
================================================
INFO  : 총 점검 항목: 12
OK    : 양호 항목: 1
WARN  : 취약 항목: 12
================================================


==========================================
점검 완료
상세 결과는 다음 파일에서 확인할 수 있습니다:
  - 화면 출력: /home/redmint/asd/asc/vul_check/unified_check_result.txt
  - 로그 파일: /home/redmint/asd/asc/vul_check/unified_check.log
==========================================
```

테스트 및 검증

// 다양한 시나리오 기반 실효성 확인

#02. 완전 양호 상태(Full Secure)

> 보안 가이드라인 준수 환경 구성 : 오탐(False Positive) 여부 확인, 모든 항목 OK 판정 확인

```
================================================
[U-06: 파일 및 디렉터리 소유자 점검]
================================================
INFO  : 실행 시각: 2025-12-21 10:38:34
파일명                          소유자:그룹      권한      결과      조치
------------------------------------------------------------------------
/etc/passwd                     root:root          644        양호      -
/etc/shadow                     root:root          400        양호      -
/etc/group                      root:root          644        양호      -
/etc/profile                    root:root          644        양호      -
/etc/hosts                      root:root          644        양호      -
/etc/services                   root:root          644        양호      -
/etc/bashrc                     파일 없음        -          제외      -
================================================
결과: 양호
```

```
================================================
[U-71. Apache 웹 서비스 정보 노출 점검 (ServerTokens/Signature)]
================================================
OK: ServerTokens 설정이 'Prod'로 적절합니다. (기준: Prod)
OK: ServerSignature 설정이 'Off'로 적절합니다. (기준: Off)
INFO: 파일 상세 정보: -rw-r--r-- 1 root root 1830 Dec 21 10:14 /etc/apache2/conf-available
INFO: 서버 버전 및 OS 정보 표시로 공격 표면 노출 가능성
INFO: 불필요한 정보 노출을 최소화(Prod/Off)하기
================================================
결과: 양호


================================================
[최종 점검 요약]
================================================
INFO  : 총 점검 항목: 12
OK    : 양호 항목: 12
OK    : 취약 항목: 0
================================================


========================================
점검 완료
상세 결과는 다음 파일에서 확인할 수 있습니다:
  - 화면 출력: /home/redmint/asd/asc/vul_check/unified_check_result.txt
  - 로그 파일: /home/redmint/asd/asc/vul_check/unified_check.log
========================================
```

테스트 및 검증

// 다양한 시나리오 기반 실효성 확인

#03. 특정 취약점 발생(Partial Vulnerable)

> Apache(U-71) 항목만 취약 설정: 선별적 탐지 성공 검증; 해당 항목만 WARN 판정 확인

```
================================================
[U-71. Apache 웹 서비스 정보 노출 점검 (ServerTokens/Signature)]
================================================
OK: ServerTokens 설정이 'Prod'로 적절합니다. (기준: Prod)
WARN: ServerSignature 설정이 'On'로 취약합니다. (기준: Off)
INFO: 파일 상세 정보: -rw-r--r-- 1 root root 1829 Dec 21 10:40 /etc/apache2/conf-available
INFO: 서버 버전 및 OS 정보 표시로 공격 표면 노출 가능성
INFO: 불필요한 정보 노출을 최소화(Prod/Off)하기
================================================
결과: 취약
권장 조치: /etc/apache2/conf-available/security.conf 파일을 다음과 같이 수정
          ServerTokens Prod
          ServerSignature Off
          설정 후 Apache 재시작: sudo systemctl restart apache2
```

```
================================================
[최종 점검 요약]
================================================
INFO  : 총 점검 항목: 12
OK    : 양호 항목: 11
WARN  : 취약 항목: 1
================================================


========================================
점검 완료
상세 결과는 다음 파일에서 확인할 수 있습니다:
  - 화면 출력: /home/redmint/asd/asc/vul_check/unified_check_result.txt
  - 로그 파일: /home/redmint/asd/asc/vul_check/unified_check.log
========================================
```

결론 및 성과

주요 성과(Key Achievements)

[*] 자동 점검 로직 구현

리눅스 서버 핵심 12개 항목 자동 점검 스크립트 완성

[*] 객관적 기준 수립

KISA, CIS 기준을 반영한 신뢰성 있는 점검 규칙 적용

[*] 대응 가이드 제공

관리자를 위한 우선순위별 구체적 조치 안내 제공

기대 효과(Expected Effects)

[*] 운영 효율성 증대

수동 대비 점검 시간 단축 및 관리자 부담 경감

[*] 인적 오류 예방

점검 누락, 판단 착오 감소로 보안 신뢰도 향상

[*] 보안 수준 상향 평준화

정기 자동 점검으로 인프라 보안 거버넌스 강화

향후 발전 방향

기술적 확장(Technical Expansion)

[*] 결과 리포트 고도화 : HTML/PDF 시각화 보고서 자동 생성

[*] 환경 확장 : Cloud 인프라 및 Docker/K8s 컨테이너 점검 추가

[*] DB 연계 : 점검 이력 관리 및 보안 추이 분석 대시 보드 구현

실효성 검증(Validation)

[*] 공격 시뮬레이션 연계 : react2shell 활용 실제 위협 검증

[*] 대응 자동화 : 취약점 발견 시 즉각적인 보안 패치 적용 기능

[*] 인식 제고 : 실제 공격 시나리오를 통한 보안 교육 도구 활용