U-45 (하)

1. 점검 내용

- su 명령어 사용을 허용하는 사용자를 지정한 그룹이 설정되어 있는지 점검

---

2. 점검 목적

- su 그룹에 포함되지 않은 일반 사용자의 su 명령을 원칙적으로 차단하는지 확인하기 위함

---

3. 점검 전 지식

3.1. wheel 그룹

- 특별한 권한을 가진 사용자들을 모아 놓은 그룹
- 이 그룹에 속한 사용자는 관리자 권한(루트 권한) 을 사용할 수 있다
  - 관리자 권한은 컴퓨터에서 모든 작업을 가능하게 할 수 있는 권한을 말한다

3.2. sudo 그룹

- 위 그룹의 설명과 같다

---

4. 점검 방법 및 결과 값

4.1. sudo 그룹 내 구성원 확인

```
cat /etc/group | grep sudo
```

- /etc/group 은 리눅스 시스템에서 모든 그룹 정보를 저장하는 파일
- 특정 문자열을 검색하는 명령어인 grep 을 사용하여 wheel 을 검색하자

- sudo : 그룹이름
- x : 암호화 된 비밀번호 나타낸다 (현대 리눅스에서는 사용되지 않아서 x로 표시)
- 27 : 그룹 ID (GID) 로 그룹의 고유한 식별번호
- ohnahee : 그룹에 속한 사용자이다
  - sudo 그룹에 속해있으므로 sudo 명령어를 사용하여 관리자 권한으로 명령을 실행할 수 있다
- root 는 왜 sudo 그룹에 포함되지 않는 건가
  - root 는 기본적으로 모든 권한을 가지고 있으므로 sudo 그룹에 속할 필요가 없다
- sudo : 특정 명령어를 관리자 권한 (root) 로 실행한다
- sudo su : 관리자 권한 (root) 로 전환한다

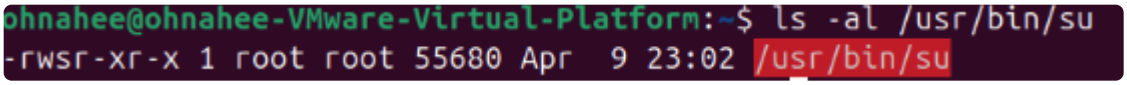
4.2. su 명령어 사용 설정 여부 확인

- su 명령어는 기본적으로 모든 사용자가 접근 할 수 있지만 이를 sudo 그룹 사용자로 제한할 수 있다

su 그룹이 명령어를 사용할 수 있는지 현재 설정 여부 확인

```
ls -al /usr/bin/su
```

4.3. 파일 권한 확인



- -rwsr-xr-x
  - '-' : 일반 파일
  - rws : 소유자의 권한은 읽기, 쓰기, 실행 가능 (s: 소유자 권한으로 실행)
  - r-x : 그룹의 권한은 읽기, 실행 가능
  - r-x : 다른 사용자의 권한은 읽기, 실행만 가능
- 1
  - 하드 링크의 수

    - 이 파일의 다른 이름이 있거나 다른 위치에서 동일한 파일을 참조하는 경우
- root root
    - 파일 소유자 root
    - 파일 그룹 root
- 55680
    - 파일 크기가 55680 바이트
- Apr 9 23:02
    - 마지막 수정 날짜
    - 4월 9일 23:03 시에 마지막으로 수정됨
- /usr/bin/su
    - 파일 경로

결론 : su 명령어의 권한 설정이 su 그룹에 들어가 있지 않은 사람도 실행 가능하다

---

5. 보안 조치 방법

5.1. wheel 그룹 생성

- sudo 권한을 이용하여 생성 해야 함

```
groupadd 그룹이름
```

5.2. su 명령어 그룹 변경

- su 명령어의 실행 권한을 제한된 그룹에만 허용하도록 설정한다

```
chgrp wheel /bin/su
```

5.3. su 명령어 사용 권한 변경

- su 명령어의 파일 권한을 설정하여 그룹에 속한 사용자들만 사용할 수 있도록 설정한다

```
chmod 4750 /bin/su
```

5.4. wheel 그룹에 su 명령 허용 계정 등록 or 직접 etc/group 파일을 수정하여 필요한 계정 등록

- su 명령을 사용할 수 있도록 해야 하는 사용자 계정을 새로 생성한 그룹에 추가한다

```
usermod -aG wheel 사용자명
```

+ 추가적으로 리눅스 PAM 모듈을 이용하여도 가능하다

https://www.igloo.co.kr/security-information/%EB%A6%AC%EB%88%85%EC%8A%A4-pam-%EB%AA%A8%EB%93%88%EC%9D%98-%EC%9D%B4%ED%95%B4/

PAM 모듈

- Pluggable Authentication Modules, 인증모듈
- 응용 프로그램 (서비스) 에 대한 사용자의 사용 권한을 제어하는 모듈
- 단순히 한 줄 수정한다고 되는 것이 아니라 위, 아래 줄 선언된 설정에 의해 그 결과값이 달라지기 때문에 주의가 필요하다

1. etc/pam.d/su 파일을 아래와 같이 설정 (주석 제거)
   - auth sufficient /lib/security/pam_rootok.so auth required /lib/security/pam_wheel.so debug group=wheel
   - auth sufficient /lib/security/$ISA/pam_rootok.so auth required /lib/security/$ISA/pam_wheel.so use_uid
2. wheel 그룹에 su 명령어를 사용할 사용자 추가 or 직접 etc/group 파일을 수정하여 필요한 계정 추가

---

6. 보안 조치 확인

```
root@ohnahee-VMware-Virtual-Platform:/home/ohnahee# ls -al /usr/bin/su
-rwsr-x--- 1 root wheel 55680 Apr  9 23:02 /usr/bin/su
```

- 지정한 그룹 사용자 외의 su 명령어 실행이 제한 되었다