U_45 (하)

1. 점검 내용

- su 명령어 사용을 허용하는 사용자를 지정한 그룹이 설정되어 있는지 점검

---

2. 점검 목적

- su 관련 그룹만 su 명령어 사용 권한이 부여되어 있는지 점검하여 su 그룹에 포함되지 않은 일반 사용자의 su 명령 사용을 원칙적으로 차단하기 위한 목적

---

3. 취약 판단 기준

- su 명령어를 모든 사용자가 사용하도록 설정되어 있는 경우 취약하다고 판단

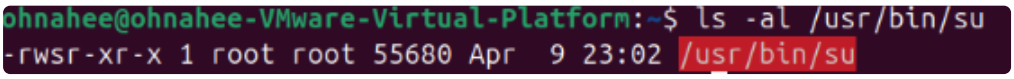
---

4. 점검 방법

4.1. su 명령어의 파일 권한 확인

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

4.2. 파일 권한 분석



-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

모든 사용자가 su 명령을 사용할 수 있도록 설정되어 있다

---

5. 보안 조치 방법

5.1. wheel 그룹 생성

```
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 사용자아이디
```

---

5. 보안 조치 방법 (2)

5.1. 리눅스 PAM 모듈 이용

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

5.2. PAM 모듈 설치 확인

```
sudo apt list --installed | grep pam
```

5.3. pam_wheel.so 모듈을 이용한 설정

PAM 설정 파일 텍스트 편집기로 열기

```
sudo vim /etc/pam.d/su
```

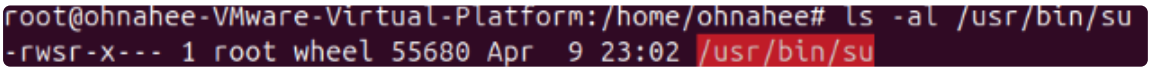
설정 추가

```
auth sufficient pam_rootok.so
auth required pam_wheel.so 사용자아이디 group=wheel
```

- wheel 그룹에 속한 사용자만 su 명령을 사용할 수 있도록 제한

---

6. 보안 조치 확인



- 지정한 그룹 사용자 외의 su 명령어 실행이 제한 되었다