

U-50 (하)

1. 점검 내용

- 시스템 관리자 그룹에 최소한 (root 계정과 시스템 관리에 허용된 계정) 의 계정만 존재하는지 점검
-

2. 점검 목적

- 관리자 그룹에 최소한의 계정만 존재하는지 점검하여 불필요하게 권한이 남용 되고 있는지 확인하기 위한 목적
-

3. 취약 판단 기준

- 관리자 그룹에 불필요한 계정이 등록되어 있는 경우 취약하다고 판단
-

4. 점검 방법

4.1. /etc/group 파일 확인

```
grep '^root:' /etc/group
```

- 루트 그룹에 불필요한 계정이 있는지 확인

system 계정에 불필요한 계정 확인

```
grep '^system:' /etc/group
```

- 시스템 그룹에 불필요한 계정이 있는지 확인
-

5. 보안 조치 방법

5.1. 불필요한 계정 삭제

```
sudo userdel username
```

5.2. 사용자 홈 디렉토리를 포함한 사용자의 모든 데이터 삭제

```
sudo userdel -r username
```