U-01 (상)

1. 점검 내용

- 시스템 정책에 root 계정의 원격 터미널 접속 차단 설정이 적용 되어 있는지 점검

---

2. 점검 목적

- 관리자 계정 탈취로 인한 시스템 장악을 방지하기 위해 외부 비인가자의 root 계정 접근 시도를 원칙적으로 차단하기 위한 목적

---

3. 취약 판단 기준

- 원격 터미널 서비스 사용 시 root 직접 접속을 허용한 경우 취약하다고 판단

---

4. 점검 방법

- 우분투에는 기본적으로 SSH가 설치되어 있지 않음
- Telnet 관련 점검 기준
  - 현재 보안 상의 이유로 SSH로 바꿔 사용하는 것을 권장

4.1. OpenSSH 서버

설치

```
sudo apt install openssh-server
```

시작 및 활성화

```
sudo systemctl start ssh
sudo systemctl enable ssh
```

상태 확인

```
sudo systemctl status ssh
```

4.2. /etc/ssh/sshd_config 파일의 `PermitRootLogin` 설정 확인

```
sudo grep PermitRootLogin /etc/ssh/sshd_config
```

- PermitRootLogin no 라고 출력 되어야 양호하다고 판단한다

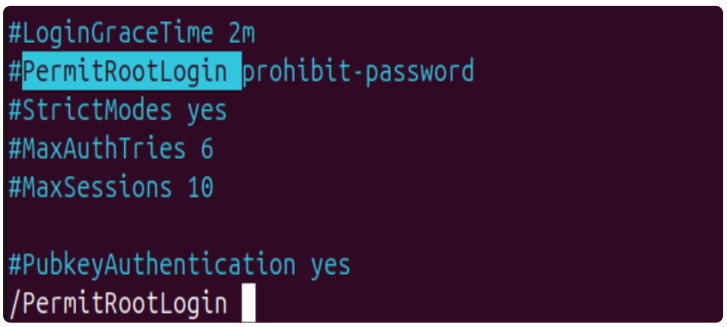
---

5. 보안 조치

- 원격 접속 시 root 계정으로 접속 할 수 없도록 파일을 수정하도록 조치
- Telnet 서비스 사용 시 사용하지 않도록 조치

5.1. /etc/ssh/sshd_config 파일 편집

```
sudo vim /etc/ssh/sshd_config
```



주석을 제거하고 PermitRootLogin 값을 no로 설정한다

SSH 서비스 재시작

```
sudo systemctl restart ssh
```

5.2. Telnet 삭제

```
sudo apt remove inetutils-telnet # 클라이언트 제거
sudo apt autoremove # 불필요한 의존성 패키지 정리
```

모든 Telnet 관련 패키지와 의존성 제거

```
sudo apt purge inetutils-telnet telnetd xinetd
sudo apt autoremove
```