VM 접속 보안 강화 방법 – sshd config에서 root 로그인 제한

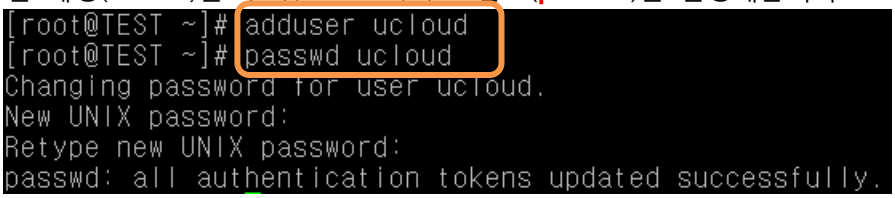
서비스 개요 >>>

Linux가 설치 된 후에는 default로 시스템 관리자인 root 사용자 계정만 존재하고 있습니다. 또한 기본적인 ssh설정으로 root로 바로 접속이 가능하도록 설정되어 있습니다. 이러한 상황에서 root 사용자로만 로그인하여 시스템을 사용하게 되면 많은 위험에 노출되기 쉽습니다. 무한 스캐닝 방법을 사용하여 root 계정을 통해 악의적인 접속을 시도하는 것이 그 예입니다.

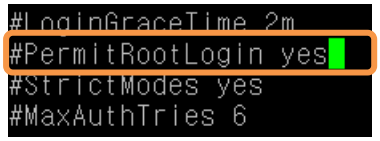
그리하여 root 계정의 ssh 원격접속을 허용하지 않도록 설정하고, 일반 사용자 계정으로 로그인하여 root 권한의 작업이 필요할 때마다 root 권한을 얻어 작업하는 것이 바람직합니다.

과 정 >>>

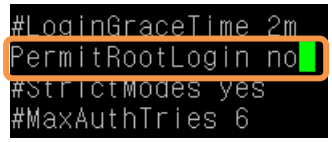
1. 우선 일반 사용자 계정을 추가해야 하므로 root계정으로 로그인한 후 다음과 같이 새로운 계정(ucloud)을 추가(**adduser**)하고 암호(**passwd**)를 설정해줍니다.



2. **vi /etc/ssh/sshd_config** 명령어를 통해 **#PermitRootLogin yes** 항목을 찾습니다.



3. **PermitRootLogin no** 로 수정하고 저장합니다.



수정이 완료되면 esc를 누르고 :wq로 저장하여 vi를 빠져나옵니다.

4. **Service sshd restart**로 수정한 sshd demon을 다시 시작합니다.

5. root 계정으로 로그인을 시도하면 Access denied란 메시지가 뜨면서 접속이 제한됩니다.

6. root 계정 접속이 제한되었으므로, 새로 생성했던 ucloud계정으로 로그인하여 사용합니다.

```
login as: ucloud
ucloud@                's password:
[ucloud@TEST ~]$
```

7. root 계정의 권한이 필요할 경우 **su –** 명령으로 root 계정에 로그인하여 권한을 획득합니다.

```
[ucloud@TEST ~]$ su -
Password:
[root@TEST ~]#
```

8. 다시 root 계정의 접속을 허용하고 싶을 경우, **vi /etc/ssh/sshd_config** 명령어를 사용하여 **PermitRootLogin no** 항목을 **PermitRootLogin yes** 로 수정하고, **Service sshd restart** 로 수정한 sshd demon을 다시 시작하여 원래 상태로 복구하시면 됩니다.

- **참고**

  특정 사용자 계정에게만 su 명령어를 사용하도록 설정하는 방법입니다.

  1. root 계정으로 로그인 한 후 **vi /etc/pam.d/su** 실행
  2. **#**auth required pam_wheel.so use_uid 항목의 주석(#) 제거
  3. **vi /etc/group** 를 실행하여 "whee"그룹에 "su –"명령 사용가능한 계정 추가
     wheel:x:10:root**,ucloud**
  4. "wheel" 그룹에 추가된 계정들만 "su"명령어 사용 가능