os.md 5.1 KB

목차(Ubuntu 기준)

접속과 로그인에 대한 관리 정책 수립

- 안 1) 주기적으로 비정상적인 접속 IP와 로그인 ID가 존재하는지 관리
- 안 2) 실시간으로 비정상적인 접속 IP와 로그인 ID가 존재하는지 관리
- 안 3) [권장] 주기적으로 그리고 실시간으로 비정상적인 접속 IP와 로그인 ID가 존재하는지 관리

로그인 관리

비정상적인 로그인 이력

```
$ sudo lastb                                    # /var/log/btmp 파일을 통하여 실패 정보
```

정상적인 로그인 및 재부팅 이력

```
$ last                                          # /var/log/wtmp 파일(Unix의 경우 /var/adm/wtmp)을 통하여 성공한 로그인과 재부팅 정보
$ last | grep -a -v x.x.x.x | grep -a -v y.y.y.y  # 특정(예: 정상적인 로그인) IP(x.x.x.x, y.y.y.y)를 제외(-v, 바이너리를 텍스트로 처리: -a)
$ last -1000 -R | grep -a -v x.x.x.x | grep -a -v y.y.y.y  # 최근 1,000개(-1000)의 접속 이력(심볼릭 링크 포함: -R)에서 특정 IP를 제외
```

마지막 접속 이력

```
$ lastlog                                       # /var/log/lastlog 파일을 통하여 마지막 접속 정보(ID, Port, IP, Time)
```

인증 이력

```
$ cat /var/log/auth.log                                                          # 인증 정보
$ grep "Failed password" /var/log/auth.log | head -3                             # 최초 암호가 틀린 3개(head -3) 로그인 정보
$ grep "Failed password" /var/log/auth.log | grep -v COMMAND | awk '{print $9}' | sort | uniq -c   # 암호가 틀린 로그인 ID별 요약 정보
$ grep "Failed password" /var/log/auth.log | grep -v COMMAND | awk '{print $11}' | sort | uniq -c  # 암호가 틀린 로그인 IP별 요약 정보
$ faillog -a                                                                     # 실패한 인증 정보
```

로그인 실패 시 접속 차단

```
$ sudo vi /etc/pam.d/common-auth
...
auth    required    pam_tally2.so deny=5 unlock_time=300   # [추가] 5회 로그인 실패 시 300초(5분) 접속 차단
...
$ sudo pam_tally2 -u ID -r                                 # 계정(ID) 로그인 실패 횟수 초기화
```

계정 관리

```
$ cat /etc/passwd                               # 계정 및 암호 정보(계정:암호:UID:GID:설명:Home:Shell) 확인
$ cat /etc/passwd | grep :0:                    # [중요] UID 혹은 GID가 0(root 권한)인 계정 확인
$ diff -d passwd passwd-                        # 기존과 이전 계정 정보를 통해 신규 계정 확인
$ cat /etc/shadow                               # 계정 암호 정보(계정:암호:생성일자:변경가능최소기간:유효기간:경고일수)
$ cat /etc/group                                # 그룹 정보
$ gpasswd GROUP                                 # 필요 시 GROUP 그룹에 대한 암호 설정
$ cat /etc/gshadow                              # 그룹 암호 정보
```

명령어 관리

```
$ history | grep COMMAND                        # 주요 권한 관련 COMMAND(useradd, adduser, setUID, umask, chmod, chown 등) 확인
$ sudo find / -name .bash_history -exec ls -al {} \;   # 모든(/) 경로에서 .bash_history 파일를 찾아서 명령 실행
```

```
# [참고] -exec 명령어 {} \;
# - {}: find로 찾은 파일들
# - \;: -exec 옵션의 끝 표시
# find / -name HelloWorld.txt -exec cat {} > /HelloWorld-All.txt \;     # 모든 경로에서 HelloWorld.txt를 찾아서 HelloWorld-All.txt에 저장
$ cat /etc/profile                                                      # 시스템 프로파일 정보 변경 확인
$ cat ~/.profile                                                        # 계정 프로파일 정보 변경 확인
$ sudo vi /etc/profile
declare -r HISTFILE                                                     # [추가] unset HISTFILE(사용된 명령어 미기록)를 차단
...
```

시스템 관리

```
$ cat /var/log/dmesg                                                    # 전체 이벤트(시스템, 네트워크, 장치 등) 정보
```