목차

Last update: 2015/12/10 01:15	rhel_서버_보안_점검_가이드	https://atl.kr/dokuwiki/doku.php/rhel_%EC%84%9C%EB%B2%84_%EB%B3%B4%EC%95%88_%EC%A0%90%EA%B2%80_%EA%B0%80%EC%9D%B4%EB%93%9C

RedHat Enterprise Linux Server 취약점 보안 가이드

계정관리 취약점 가이드

패스워드 복잡성 설정

패스워드 변경 시 해당 OS 버전에 따라 적용해야 하는 lib 가 따로 존재 한다.
해당 버전은 아래 경로에서 확인 할 수 있다.

```
[root@test ~]# cat /usr/share/doc/pam-1.1.1/txts/README*
```

* 주의 : /etc/pam.d/ 폴더 안에 있는 파일을 수정하게 되면, 로그인하는 계정 부터는 바로 적용이 됨
* 운영체제 별 모듈(lib파일) 확인하는 경로

운영체제	경로
32bit	cd /lib/security/
64bit	cd /lib64/security/

계정 잠금 임계 값 설정

system-auth

system-auth

```
[root@test ~]# cat /etc/pam.d/system-auth
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth        required      pam_env.so
auth        required      pam_tally2.so deny=3 onerr=fail
unlock_time=120 // 추가하는 부분
auth        sufficient    pam_fprintd.so
auth        sufficient    pam_unix.so nullok try_first_pass
auth        requisite     pam_succeed_if.so uid >= 500 quiet
auth        required      pam_deny.so

account     required      pam_unix.so
account     required      pam_tally2.so  // 추가하는 부분
account     sufficient    pam_localuser.so
account     sufficient    pam_succeed_if.so uid < 500 quiet
account     required      pam_permit.so
```

```
password    requisite     pam_cracklib.so try_first_pass retry=3 type=
password    sufficient    pam_unix.so sha512 shadow nullok
try_first_pass use_authtok
password    required      pam_deny.so

session     optional      pam_keyinit.so revoke
session     required      pam_limits.so
session     [success=1 default=ignore] pam_succeed_if.so service in
crond quiet use_uid
session     required      pam_unix.so
```

적용 후 테스트 방법
테스트 계정을 생성 한 후 유저 계정으로 로그인 시도합니다.

test

```
[test1@test ~]$ su - test1
Password:
su: incorrect password  // 1번째 틀림
[test1@test ~]$ su - test1
Password:
su: incorrect password  // 2번째 틀림
[test1@test ~]$ su - test1
Password:
su: incorrect password  // 3번째 틀림
[test1@test ~]$ su - test1
Account locked due to 4 failed logins // 4번째 틀림
Password:
su: incorrect password
[test1@test ~]$ su - test1
Account locked due to 5 failed logins // 5번째 정상적인 비밀번호 입력시에도 로그인이 되지 않는다.
Password:
su: incorrect password

[root@test ~]# pam_tally2  // 해당 명령어 입력 후 테스트한 계정의 실패 횟수를 확인한다.
Login           Failures Latest failure     From
test1               5    01/19/15 14:17:11  pts/0

[root@test ~]# pam_tally2 --reset  // 모든 유저의 failures 를 초기화 시켜 주는 명령어
Login           Failures Latest failure     From
test1               5    01/19/15 14:17:11  pts/0
[root@test ~]# pam_tally2          // 초기화 된 것을 확인한다.
```

계정 패스워드 최소길이 /최대사용 기간설정

password 설정

```
[root@test ~]# vim /etc/login.defs
#
# Please note that the parameters in this configuration file control the
# behavior of the tools from the shadow-utils component. None of these
# tools uses the PAM mechanism, and the utilities that use PAM (such as the
# passwd command) should therefore be configured elsewhere. Refer to
# /etc/pam.d/system-auth for more information.
#

# *REQUIRED*
#   Directory where mailboxes reside, _or_ name of file, relative to the
#   home directory.  If you _do_ define both, MAIL_DIR takes precedence.
#   QMAIL_DIR is for Qmail
#
#QMAIL_DIR  Maildir
MAIL_DIR    /var/spool/mail
#MAIL_FILE  .mail

# Password aging controls:
#
#   PASS_MAX_DAYS    Maximum number of days a password may be used.
#   PASS_MIN_DAYS    Minimum number of days allowed between password
changes.
#   PASS_MIN_LEN    Minimum acceptable password length.
#   PASS_WARN_AGE    Number of days warning given before a password expires.
#
PASS_MAX_DAYS   99999 // 패스워드 변경 없이 최대 사용기간 설정
PASS_MIN_DAYS   0     // 패스워드 변경 없이 최소 사용기간 설정
PASS_MIN_LEN    5     // 패스워드 최소 길이 설정
PASS_WARN_AGE   7     // 만료일전 경고 일자 만료일 -7일

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN           500
UID_MAX         60000

#
# Min/max values for automatic gid selection in groupadd
#
GID_MIN           500
GID_MAX         60000

#
```

```
# If defined, this command is run when removing a user.
# It should remove any at/cron/print jobs etc. owned by
# the user to be removed (passed as the first argument).
#
#USERDEL_CMD    /usr/sbin/userdel_local

#
# If useradd should create home directories for users by default
# On RH systems, we do. This option is overridden with the -m flag on
# useradd command line.
#
CREATE_HOME yes

# The permission mask is initialized to this value. If not specified,
# the permission mask will be initialized to 022.
UMASK           077

# This enables userdel to remove user groups if no members exist.
#
USERGROUPS_ENAB yes

# Use SHA512 to encrypt password.
ENCRYPT_METHOD SHA512
```