JANT 한국항행학회논문지
Journal of Advanced Navigation Technology

기반 기술

J. Adv. Navig. Technol. 19(6): 587-594, Dec. 2015

리눅스 서버의 사용자 관리 및 보안

Management and Security of User in Linux Server

정 성 재[1] · 성 경[2*]
[1](주)엔버 기업부설연구소
[2]목원대학교 융합컴퓨터미디어학부

Sung-Jae Jung[1] · Kyung Sung[2*]
[1]ScomCNS Co., Ltd., Seoul 138-953, Korea
[2]Division of Convergence Computer & Media, Mokwon University, Daejeon 302-729, Korea

[요 약]

개방형 운영체제인 리눅스는 전통적인 웹, 메일, DNS, FTP 등의 서버뿐만 아니라, 클라우드 및 빅데이터 인프라 구축에도 사용되고 있다. 또한 데스크톱이나 모바일 기기, 스마트 TV 및 자동차 등에도 탑재되고 있다. 특히, 사물인터넷 시대로 접어드는 현 시점에서는 리눅스가 차지하는 비중이 더 커질 것으로 예상되고 있다. 리눅스의 사용이 증가함에 따라 보안이 중요한 요소로 부각되고 있고, 리눅스 시스템 보안의 핵심은 사용자 관리에 있다. 본 논문에서는 리눅스의 사용자를 분류하고, 사용자 관련 파일의 역할을 분석하였다. 마지막으로 리눅스의 사용자별 보안 관리 기법에 대해 알아보고, 유용한 사용자 보안 도구에 대해 분석하였다.

[Abstract]

Open operating system, Linux is the traditional Web, E-mail, DNS, FTP server, as well as being used in Cloud and Big data infrastructure. In addition, Linux is also used like a desktop or mobile devices, smart TV and cars. In particular, stepping up to the IoT era at this time is expected to be greater proportion occupied by Linux. As the use of Linux has increased security has emerged as an important factor. User management is core of Linux system security. In this paper, Classifying Linux user and analyzed the role of the user-specific file. Finally, we analyzed the linux management technologies and useful user security tools.

Key word : Linux, System security, User management, User security, Security tools.

http://dx.doi.org/10.12673/jant.2015.19.6.587

Received 15 October 2015; **Revised** 25 November 2015
Accepted (Publication) 9 December 2015 (30 December 2015)

***Corresponding Author; Kyung Sung**

Tel: +82-42-829-7640
Email: skyys04@mokwon.ac.kr

Ⅰ. 서 론

1991년에 핀란드 헬싱키 대학의 대학원생인 리누스 토발즈(Linus Torvalds)는 포직스(posix)와 호환되는 운영체제 커널을 만들기로 하고, 리눅스의 첫 번째 버전인 0.01을 1991년 9월 17일에 인터넷에 공개하였다. 첫 공식버전인 0.02는 같은 해 10월에 발표한 이후로 전 세계 많은 개발자와 전문가의 도움을 받아 지속적으로 개발을 진행하게 되었다. 그 후 개발자들은 몇 년 동안 리눅스를 자유소프트웨어 관련 프로젝트인 GNU(gnu is not unix) 프로그램에 적용시키는 작업을 수행하였다. 1994년에 리눅스 커널 버전 1.0을 발표하였고, 1996년 리눅스 커널 버전 2.0을 발표하였다. 1990년대 중반에 접어들면서 레드햇, 칼데라와 같은 리눅스 배포판들이 전 세계로 퍼져 나가기 시작했고, 그 이후 순수 비영리 배포판인 데비안이 GUI (graphic user interface)를 탑재하여 배포되기 시작했다. 현재 리눅스 커널은 소스가 공개되어 있고 누구나 커널을 수정할 수 있는 특징으로 약 300여개 이상의 리눅스 배포판이 만들어졌다. 리눅스를 활용하는 분야도 데스크톱이나 서버뿐만 아니라, 구글에서 만든 모바일 운영체제인 안드로이드에도 사용되고 있으며, 자동차에 장착되는 IVI (in-vehicle infotainment)에도 사용될 만큼 다양한 분야로 영역을 넓혀가고 있다. 최근 IT의 인프라가 클라우드 및 빅데이터 기반으로 바뀌고, 사물인터넷 (IoT; internet of things) 시대로 진입하면서 리눅스 같은 개방형 운영체제의 사용이 증가하고 있다. 특히 서버 시장에서는 유닉스(unix)에서 x86 기반의 리눅스 서버로 많이 대체되고 있다.

본 논문에서는 리눅스 서버 보안의 가장 큰 요소라 할 수 있는 사용자에 대해 살펴보고, 안전한 시스템 운영을 위한 사용자 관리 및 보안 방법에 대해 알아본다.

Ⅱ. 리눅스 사용자의 개요

2-1 사용자의 분류

리눅스의 사용자는 크게 root 사용자와 일반 사용자로 구분하고, 일반 사용자는 로그인이 가능한 사용자와 로그인은 되지 않고 시스템의 필요에 의해 생성된 시스템 계정으로 나눈다[1]. root는 시스템운영에 있어서 모든 권한을 행사하므로 권한이 있는 사용자 (privileged user) 또는 슈퍼 유저 (super user)라고 한다. 일반 사용자는 권한이 없는 사용자 (unprivileged user) 또는 보통 사용자 (normal user)라고 부르는데, 시스템에 대해 제한적인 권한을 행사한다. 일반적으로는 root라는 계정 자체를 슈퍼 유저라 인식하는데, 리눅스 시스템 내부에서는 사용자를 흔히 말하는 ID(identity)로 관리하는 것이 아니라 숫자값 형태의 UID (user identity)로 관리한다. 사용자의 UID는 0번부터 정수값으로 배분되는데, root는 0이 할당되고 0번 사용자를 슈퍼 유저로 인식한다. 일반 사용자는 1번부터 부여되는데, 사용자 생성 시에 보통 레드햇 리눅스 계열은 500번부터 할당되고 데비안 리눅스 계열은 1000번부터 할당된다.

사용자를 역할에 따라 분류하면 root, 일반 사용자, 시스템 계정으로 분류할 수 있다. root는 리눅스 시스템에서 절대적인 권한을 행사하는 계정으로 사용자 생성 및 삭제, 디스크 및 파티션 관리, 프로세스 제어 등 시스템 관리와 관련된 모든 것을 통제할 수 있다. root는 시스템에 운영체제 설치할 때 기준이 되는 계정이다. 일반 사용자는 root에 의해 useradd 및 passwd 명령을 이용해서 생성되는 계정으로 제한된 범위 내에서 파일의 생성 및 삭제, 프로세스 생성 등을 할 수 있다. 시스템 계정은 말 그대로 시스템의 필요에 의해 생성된 계정이다. 리눅스 사용자 계정의 정보는 /etc/passwd 파일에 기록되는데, 이 파일에 등록된 계정을 보면 root 이외에 bin, daemon, adm, game 등 관리자가 생성하지 않는 계정들이 존재한다. 리눅스는 유닉스의 영향을 받아 파일 생성할 때나 프로세스 생성 시에 반드시 소유자를 명시하도록 되어 있고, 해당 소유자의 권한을 승계하는 형태로 운영된다. 즉, root가 만든 파일이면 root 권한이고, root가 실행한 프로세스는 root 권한이 부여된다고 볼 수 있다. 시스템 계정이 없다면 모든 파일 생성과 프로세스 생성 시에 root 권한이 부여되어야 한다. 구체적으로 예를 들면 리눅스에 있는 하나의 게임을 실행하여 게임의 점수를 /etc/highscore 라는 파일에 기록하도록 구성했다고 가정 했을 때, root만 존재한다면 게임 실행 시에 root 권한으로 실행되고 관련 점수는 /etc/highscore에 root 권한으로 저장이 된다. 정상적으로 동작한다면 문제가 없겠지만, 만약 프로그램의 오류로 인해 /etc/highscore 파일에 기록되어야할 정보를 시스템 부팅과 연관되어 있는 /etc/inittab에 기록한다면 시스템이 부팅되지 않는 최악의 상황을 맞이하게 된다. 만약 games라는 계정을 만들어서 게임을 실행할 때 games라는 사용자 권한으로 프로세스를 생성하고, /etc/highscore에 기록하도록 한다면 시스템 상에 발생할 수 있는 문제점을 줄일 수 있게 된다.

2-2 사용자 정보의 확인

리눅스는 대부분의 정보를 텍스트파일에 저장해서 관리하는데, 사용자 계정 정보 역시 파일로 저장되고 사용자를 생성할 때도 관련 파일에서 정보를 가져온다. 따라서 관련 파일을 텍스트 관련 명령어인 cat, tail, head 등을 이용해서 확인하거나 vi, emacs 등의 편집기를 이용해서 확인 및 편집이 가능하다. 사용자 생성 명령어인 useradd와 관련된 파일을 정리해보면 그림 1과 같다. useradd 명령을 실행하면 기본 설정은 /etc/default/useradd에서 정보를 가져오고, /etc/skel에 들어있는 파일 및 디렉터리를 사용자에게 제공한다. 생성된 사용자의 정보는 /etc/passwd와 /etc/shadow에 기록된다. 또한, ‘/home/사용자아이디’에 홈 디렉터리를 부여받아서 파일을 생성 삭제할 수 있고, ‘/var/spool/mail/사용자아이디’에 메일 파일을 생성해준다.

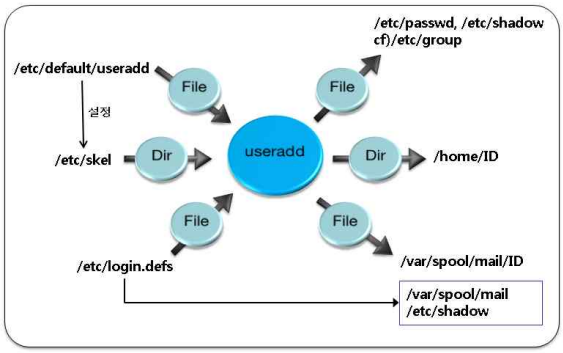

그림 1. useradd 명령어와 관련 파일
Fig. 1. useradd command and related files.

2-3 사용자 관련 파일

1) /etc/passwd

/etc/passwd는 시스템에 로그인하여 자원을 이용할 수 있는 사용자의 목록을 저장하고 있는 정보파일이다. 이 파일에 기록된 사용자 정보는 그 사용자가 로그인하고, 로그아웃할 때까지 항상 시스템이 사용자를 감시하기 위한 근거가 되는 파일이다. /etc/passwd에는 콜론(:)을 구분자로 하여 'useranme:password:UID:GID:fullname:home-directory:shell' 과 같이 7개의 기본적인 정보를 기록한다.

그림 2. /etc/passwd 파일의 예
Fig. 2. Examples of /etc/passwd.

표 1. /etc/passwd의 항목 설명
Table 1. Field description of /etc/passwd.

Field	Descriptions
posein	Account, the name of the user on system. ID called a one people
x	The encrypted user password. Currently managed separately from the /etc/shadow
500	The numerical user ID
500	The numerical primary group ID for this user
System Engineer	This filed is optional and only used fro informational purposes.
/home/posein	The user's Home Directory
/bin/bash	The program to run at login

2) /etc/shadow

/etc/passwd는 사용자의 아이디 및 패스워드 등의 정보를 담고 있는 중요한 파일이나 모든 사용자가 이 파일의 내용을 볼 수 있도록 접근 권한이 설정되어 있다. 사용자의 패스워드의 경우에는 암호화(encryption)해서 저장되기는 하나 잠재적으로 노출될 위험이 존재하였다. /etc/shadow는 /etc/passwd의 두 번째 필드인 패스워드 부분을 암호화여 관리하는 파일로 root 사용자 이외에는 접근이 불가능하도록 설정되어 있다. 이 파일은 'username:password:last:may:must:warn:expire:disable:reserved' 와 같이 9개의 필드로 구성되어 있다.

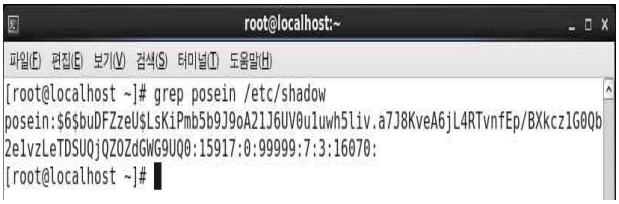

그림 3. /etc/shadow 파일의 예
Fig. 3. Examples of /etc/shadow.

표 2. /etc/shadow의 항목 설명
Table 2. Field description of /etc/shadow.

Field	Descriptions
posein	Login name.
6.....	Encrypted password. Initially, the hash algorithm is MD5 that was used, in recent years, the hash algorithm is used that SHA512.
15917	Date of last password change, expressed as the number of since Jan 1, 1970
0	Minimum password age, An empty filed and value 0 mean that there are no minimum password age.
99999	Maximum password age.
7	Password warning period
3	Password inactivity period
16070	Account expiration date
reserved field	This field is reserved for future use.

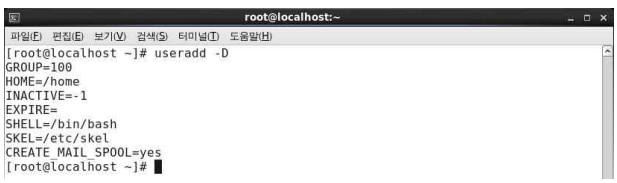

그림 4. /etc/default/useradd 파일의 예
Fig. 4. Examples of /etc/default/useradd.

3) /etc/default/useradd

/etc/default/useradd는 별도의 옵션 없이 'useradd 사용자명' 으로 계정 생성 시에 기본적으로 적용되는 설정이 들어있는 파일이다. 텍스트 파일의 전체 내용을 출력할 때 하는 사용 명령인 cat 으로 확인하거나 'useradd -D'를 입력하면 확인가능하다.

4) /etc/login.defs

/etc/login.defs에는 메일 디렉터리, 패스워드 관련 설정(최대 사용기한, 최소 사용기한, 최소 길이, 만기 이전 경고 주는 날짜), UID의 최솟값 및 최댓값, GID의 최솟값 및 최댓값, 홈 디렉터리 생성 여부, 기본 UMASK 값, 패스워드에 적용하는 암호화 알고리즘 등이 정의되어 있다.

표 3. /etc/default/useradd의 항목 설명
Table 3. Field description of /etc/default/useradd.

ITEM	Descriptions
GROUP=100	The groue name of ID for a new user's initial group. The named group must exist, and a numerical group ID must have an existing entry.
HOME=/home	The path prefix for a new user's home directory. The user's name will be affixed to the end of BASE_DIR to form the new user's home directory name, if the -d option is not used when creating a new account.
INACTIVE=-1	The number of days after a password has expired before the account will be disabled.
EXPIRE=	The date on which the user account is disabled.
SHELL=/bin/bash	The name of a new user's login shell.
SKEL=/etc/skel	he system administrator is responsible for placing the default user files in the /etc/skel/ directory
CREATE_MAIL_SPOOL=yes	The entry that specifies whether to create a mail file during user creation. If set to yes the mail related files are created in the '/var/spool/mail/username'

III. 사용자 보안 관리

3-1 root 계정 관리

리눅스와 같은 UNIX 계열 운영체제에서 root 계정이 갖는 권한은 절대적이라고 볼 수 있다. 따라서 root 계정을 잘 관리하

표 4. /etc/login.defs의 항목 설명
Table 4. Field description of /etc/login.defs.

ITEM	MAIL_DIR /var/spool/mail
Desc	The mail spool directory. This is need to manipulate the mailbox when its corresponding user account is modified or deleted. If not specified, a compile-time default is used.
ITEM	PASS_MAX_DAYS 99999
Desc	The maximum number of days a password may be used. If the password is older than this, a password change will be forced. If not specified, -1 will be assumed (which disables the restriction)
ITEM	PASS_MIN_DAYS 0
Desc	The minimum number of days allowed between password changes. Any password changes attempted sooner than this will be rejected. If not specified, -1 will be assumed (which disables the restriction).
ITEM	PASS_MIN_LEN 5
Desc	Specifies the minimum length of the password
ITEM	PASS_WARN_AGE 7
Desc	The number of days warning given before a password expires. A zero means warning is given only upon the day of expiration, a negative value means no warning is given. If not specified, no warning will be provided.
ITEM	UID_MIN 500
Desc	Specifies the minimum value of UID
ITEM	UID_MAX 60000
Desc	Specifies the maximum value of UID
ITEM	GID_MIN 500
Desc	Specifies the minimum value of GID
ITEM	GID_MAX 60000
Desc	Specifies the maximum value of GID
ITEM	CREATE_HOME yes
Desc	Indicate if a home directory should be created by default for new users. This setting does not apply to system users, and can be overridden on the command line.
ITEM	UMASK 077
Desc	The file mode creation mask is initialized to this value. If not specified, the mask will be initialized to 022.
ITEM	USERGROUPS_ENAB yes
Desc	Enable setting of the umask group bits to be the same as owner bits (examples: 022 -> 002, 077 -> 007) for non-root users, if the uid is the same as gid, and username is the same as the primary group name.
ITEM	ENCRYPT_METHOD SHA512
Desc	Specifies the hash algorithm to be used for password

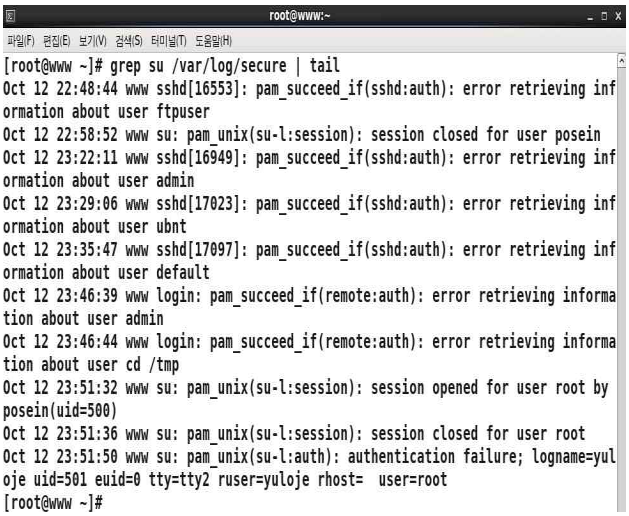

그림 5. 시스템 로그 파일 확인 예
Fig. 5. Confirmation of system log file.

는 것이 시스템 보안에서 중요한 요소라고 볼 수 있는데, root 계정 관리를 위한 방법으로 크게 네 가지 손꼽을 수 있다. 첫 번째는 root 계정 이외에 다른 슈퍼유저가 존재하는 지를 점검한다. 리눅스에서는 root 계정을 슈퍼유저로 취급한다기보다는 root에 부여된 UID가 0인 사용자를 슈퍼유저로 취급한다. 해커들이 로컬의 익스플로잇(exploit) 코드를 사용해서 root 권한을 획득 후에 일반 계정사용자의 UID를 0번으로 변경함으로서 또 하나의 슈퍼유저를 만드는 경우가 있으므로 반드시 점검해야 한다. 두 번째는 리눅스 시스템에 root 계정으로 직접 로그인하는 것을 최대한 막는다. 로컬의 시스템 로그인을 비롯하여 X 윈도, 텔넷, SSH 등과 같은 인증 서비스를 이용할 경우에 root를 이용한 로그인을 막고, 일반 사용자로 접근하도록 설정한다. 일반 사용자로 로그인한 후 root 권한이 필요하다면 su 명령 등을 이용해서 일시적으로 root 권한을 획득하도록 한다. 세 번째는 root 계정으로 불필요하게 장시간 로그인되어 있는 것을 막는다. root 계정으로 불필요하게 로그인되어 있다면 자원 낭비를 초래하고 특히 시스템이 물리적으로 접근 가능한 곳에 있다면 아주 큰 보안상의 문제를 야기할 수 있다. 환경 변수인 TMOUT를 사용하면 지정한 시간 이외에 작업을 하지 않을 경우에 자동 로그아웃시킬 수 있다. 네 번째는 일반 사용자에게 root 권한 획득할 때에 su보다는 sudo 명령어를 사용하도록 권장한다. su 명령은 일반 사용자로 로그인한 후에 root나 다른 사용자로 전환할 때 사용하는 명령으로 관련 사용자의 패스워드를 알고 있어야 한다. 즉, 일반 사용자가 root 사용자로 전환하기 위해서는 root의 패스워드를 알고 있어야 한다. 해당 사용자가 root의 모든 권한을 행사하는 경우라면 문제가 없지만, 일부 명령어만 할당하려는 경우에는 보안상의 문제점을 가지고 있다. 이러한 문제점을 해결할 수 있는 것이 sudo이다. sudo 명령은 모든 명령어뿐만 아니라, 특정 명령어만 root 권한을 대행할 수 있도록 설정할 수 있다. 아울러, root의 패스워드를 노출시킬 염려도 없어 su 명령에 비해 안전하다고 볼 수 있다.

3-2 시스템 계정 관리

시스템 계정은 시스템 운영에 필요한 계정으로 리눅스를 설치하게 되면 배포판에 따라 30 ~ 40여개의 계정이 생성된다. 보통 500번 이하의 UID를 부여받고 프로세스나 파일 권한 부여의 역할만 수행해서 로그인이 되지 않도록 설정한다. 즉 /etc/passwd의 일곱 번째 필드에는 로그인후 사용되는 셸의 경로가 명기되는데, 시스템 계정은 '/sbin/nologin'과 같이 설정하여 로그인을 막는다. 그러나 해커들은 game이나 games 등과 같은 시스템 계정으로 위장하여 셸(shell)을 부여하고 로그인이 되도록 설정하는 경우도 있다. 따라서 해당 계정들을 지속적으로 관리해야 한다. 시스템 계정 관리의 가장 좋은 방법은 불필요한 서비스를 제거하여 시스템 계정을 최소화하는 것이지만, 초보 관리자들에게는 쉬운 방법은 아니다. 초보 관리자에게 있어서 현실적인 시스템 계정 관리 방법은 처음 리눅스 설치 시에 기본적으로 생성되는 계정의 목록을 만들어 기록하고, 시스템

그림 6. 사용자 히스토리 파일 확인 예
Fig. 6. Confirmation of user history file.

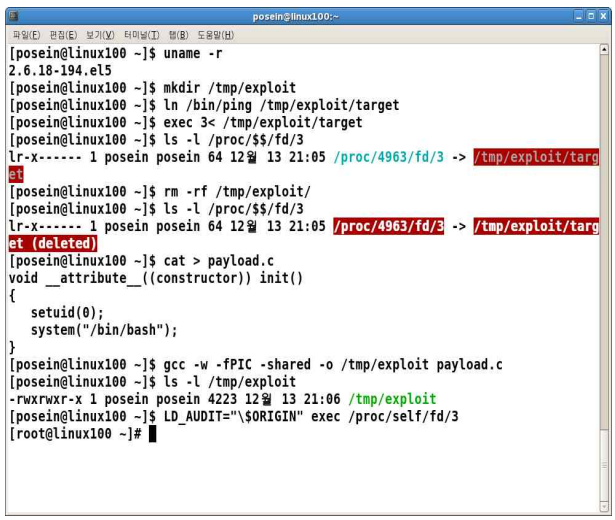

그림 7. GNU C 라이브러리 취약점
Fig. 7. GNU C library dynamic linker $ORIGIN expansion vulnerability.

운영 중에 설치되는 프로그램에 의해 생성되는 계정들을 추가로 기입하여 지속적으로 감시하는 것이다.

3-3 일반 사용자 관리

일반 사용자들은 시스템에 로그인하여 명령을 실행하고 파일 및 프로세스를 생성하므로 잠재적으로 보안상의 위험 요소를 가지고 있다. 따라서 일반 사용자의 관리가 시스템 보안에 가장 큰 요소라고 할 수 있는데, 크게 3가지 방법으로 예를 들 수 있다.

첫 번째는 root 권한을 획득할 수 있는 명령어를 사용하는지를 감시한다. 예를 들면 root 사용자를 전환할 수 있는 su가 대표적인 명령어에 해당하는 데, 해당 명령어의 사용한 기록은 /var/log/secure를 조회하거나 각 사용자의 홈 디렉터리 내에 생성되는 히스토리(history) 파일을 조회함으로서 알 수 있다.

두 번째는 root 권한을 획득할 수 있는 명령어를 사용자에 따라 제한을 설정한다. su 명령어를 비롯하여 일반 사용자가 root local exploit 코드를 이용하여 root 권한을 획득할 때 사용하는 gcc 등도 사용자 제한을 설정해두는 것이 좋다. 그림 7은 현재 서버에서도 많이 사용되는 리눅스 버전인 레드햇 엔터프라이즈 리눅스 5 와 6의 GNU C 라이브러리 취약점을 이용해서 일반 사용자가 root 계정을 획득하는 과정이다[2]-[5].

그림 7과 같이 일반 사용자가 간단히 C 언어로 작성된 소스코드를 gcc로 컴파일하여 실행 명령을 만든 후에 쉽게 root 권한을 획득하는 것을 알 수 있다. 사용자의 특정 명령어 제한은 보안 도구를 사용해도 되나, 손쉽게 그룹 생성과 허가권(permission) 설정으로 해결할 수도 있다. 예를 들면 admin과 같은 그룹을 생성하고, root 권한 획득과 연관 있는 명령어들을 admin 그룹에 속한 사용자만 실행 가능하도록 허가권을 설정한다. 그 뒤에 해당 명령을 실행할 사용자를 admin 그룹으로 묶어주는 작업을 통해 쉽게 해결 가능하다.

세 번째는 사용자의 패스워드를 관리한다. 해커가 유출된 일반 사용자의 패스워드를 이용하여 시스템에 로그인하게 되면 그림 7의 사례처럼 root 권한을 획득할 확률이 상당히 높아지게 된다. 따라서 사용자의 패스워드 관리는 시스템 보안에 있어서 상당히 중요한 요소이다. 먼저 별도의 패스워드 관리 파일인 /etc/shadow를 반드시 사용하도록 한다. 리눅스에서는 pwconv 및 pwunconv 명령을 이용해서 사용자 관리를 /etc/passwd 파일에서만 관리하거나 /etc/shadow를 같이 사용하도록 설정할 수 있다. 반드시 pwconv 명령을 통한 /etc/shadow 파일을 사용하도록 하고, pwck 명령을 이용해서 /etc/passwd 및 /etc/shadow 파일을 점검하도록 한다. 아울러, /etc/shadow에서 암호화된 패스워드가 기록되는 영역인 두 번째 필드가 공백인 경우에는 패스워드 입력 없이 로그인이 되니 수시로 점검이 필요하다.

Ⅳ. 사용자 보안 관련 도구

사용자에 대한 보안을 위해 관련 도구를 이용하면 더욱 손쉽게 관리할 수 있다. 본 장에서는 3장에서 언급된 사용자 관리와 관련하여 유용한 보안 도구 몇 가지를 살펴보도록 한다.

4-1 sudo

sudo(superuser do)는 특정 사용자 또는 특정 그룹에 root 사용자 권한을 가질 수 있도록 일부 명령 또는 모든 명령을 실행할 수 있도록 해주는 도구로 대부분의 리눅스 배포판에 기본적으로 설치되어 있다[6]. 관리자가 visudo 명령을 실행하면 vi 편집기가 /etc/sudoers 파일을 열면서 설정하도록 되어 있다. 적용된 사용자는 'sudo 명령어' 형태로 실행하여 root 권한을 대행한다. su 명령은 일반 사용자에게 root의 패스워드를 알려줘야 하고, 일부 명령어만 가능하도록 하는 설정이 불가능하다. 예를 들면 posein이라는 계정에 다른 사용자를 추가하고 패스워드를 부여하는 2가지 권한만을 할당하기 위해 useradd 및 passwd 명령어만 사용가능하도록 할 때 sudo 명령은 매우 유용하다.

4-2 PAM

PAM (pluggable authentication module)은 사용자를 인증하고 그 사용자의 서비스에 대한 접근을 제어하는 모듈화된 방법을 말한다. PAM은 응용 프로그램들에게 사용자 인증 방법을 선택할 수 있는 공유 라이브러리의 묶음을 제공한다. 리눅스에서 PAM 프로젝트의 목적은 소프트웨어 개발과 안전한 권한 부여 및 인증 체계를 분리하는데 있다[7]. 현재 PAM은 대부분의 배포판 리눅스에 기본적으로 설치되어 있고 특정 서비스에 대한 사용자(또는 그룹)들의 허가 목록 파일, 특정 서비스에 대한 사용자(또는 그룹)들의 거부 목록 파일, 사용자의 패스워드 길이 제한 등에 사용되고 있다. 보편적으로 사용되는 첫 번째 방법에는 로컬 로그인, X 윈도, ssh, 텔넷 등과 같은 인증 서비스에 root 사용자의 접근을 들 수 있다. 두 번째 방법에는 텔넷, ssh, ftp와 같은 서비스를 이용하는 사용자의 거부 목록을 만들거나 허가 목록을 만들 때 사용한다. 세 번째 방법에는 su, sudo와 같이 root 권한 획득이 가능한 명령어에 대한 사용자 거부 또는 허가 목록 파일도 만들 수 있다.

4-3 John The Ripper

John The Ripper는 Solar Designer가 개발한 유닉스 계열 패스워드 크랙 도구 (password crack tool)로 시작했지만, 현재는 유닉스 계열 이외에도 Windows 계열, DOS, BeOS, OpenVMS 등 다양한 운영체제를 지원한다[8]. 기본적인 원리는 암호로 사용될 만한 목록이 들어 있는 텍스트 형태의 사전 파일(dictionary file) 을 이용해서 일일이 대입한 후에 암호화된 패스워드가 들어 있는 /etc/shadow와 비교해서 사용자의 패스워드를 알아내는 방식이다. 관리자가 사전 파일에 유추가 될 만한 패스워드를 추가로 기입할 수도 있고, 텍스트로 저장된 다른 사

전 파일을 이용할 수 있다. 이 도구를 사용하면 일반 사용자들이 보편적으로 설정해서 사용하는 알기 쉬운 패스워드를 걸러낼 수 있고, 보안상 가장 위험한 패스워드를 설정하지 않은 사용자도 쉽게 찾아낼 수 있다.

Ⅴ. 보안 도구를 활용한 관리 기법

5-1 sudo 활용

sudo(superuser do)는 root 패스워드의 노출 없이 일반 사용자들에게 root의 관리자 권한을 할당할 때 매우 유용하다. 설정도 매우 쉬워 visudo라는 명령을 실행하면 vi편집기로 /etc/sudoers 파일을 열게 되고 '사용자명 접속한 곳=명령어' 순으로 기입하면 된다. 예를 들어 posein은 root와 동일하게 모든 명령을 사용가능하게 하고, yuloje는 사용자 관리를 위해 useradd와 passwd 명령만 이용할 수 있도록 설정한다면 다음과 같이 설정하면 된다.

```
# visudo
posein    ALL=ALL
yujoje    ALL=/usr/local/sbin/useradd, /usr/bin/passwd
```

sudo가 root의 권한 일부 또는 전체를 손쉽게 할당할 수 있지만, 악용될 소지가 있으므로 주시해야 한다. 예를 들어 아래와 같이 설정한다면 hacker 사용자는 sudo 명령 이용할 때 어떠한 패스워드의 입력 없이도 아주 손쉽게 root로의 전환이 가능하다.

```
# visudo
hacker   ALL=(ALL)      NOPASSWD: ALL
```

그림 8은 관련 설정 후에 실행한 결과이다.

5-2 PAM 활용

PAM은 사용자명을 기반으로 특정 서비스에 대한 허가 목록을 만들거나 거부 목록을 만들 때 유용하다. 예를 들면 텔넷(telnet) 서비스를 posein 및 yuloje 사용자만 허가하도록 한다면 /etc/pam.d/remote 에 아래의 설정을 추가한 뒤에 관련 목록 파

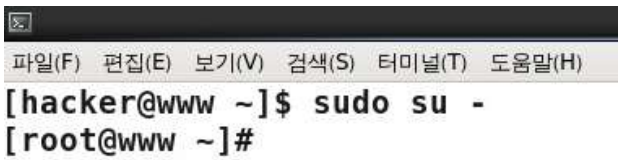

그림 8. sudo 사용 예
Fig. 8. Examples of sudo.

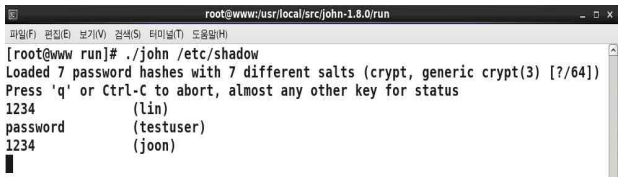

그림 9. John The Ripper 사용 예
Fig. 9. Examples of John The Ripper.

일을 생성하면 된다.

```
# vi /etc/pam.d./remote
auth    required    pam_listfile.so item=user sense=allow file=/etc/loginusers

# vi /etc/loginusers
posein
yuloje
```

또한, ssh 서비스를 posein 및 yuloje 사용자만 접속을 불허한다면 /etc/pam.d/sshd에 아래의 설정을 추가한 뒤에 관련 목록 파일을 생성하면 된다.

```
# vi /etc/pam.d./sshd
auth    required    pam_listfile.so item=user sense=deny file=/etc/ssh_nologin

# vi /etc/ssh_nologin
posein
yuloje
```

5-3 John The Ripper 활용

John The Ripper는 단순하고 쉽게 유추가 가능한 패스워드를 설정한 사용자를 찾아낼 때 용이한 도구로 실행 명령도 매우 간단하다. 그림 9의 결과를 살펴보면 lin 및 joon이라는 계정의 패스워드는 1234로 설정되어 있고, testuser의 패스워드는 password로 설정되어 있다는 것을 보여준다. 많은 사용자가 등록되어 사용되는 시스템인 경우에는 /etc/shadow 파일의 변경 여부를 확인해서 주기적으로 검사한다면 보안 강화를 위해 상당한 효과를 거둘 수 있다.

Ⅵ. 결 론

리눅스는 전통적인 웹 , 메일, DNS, FTP 등의 서버뿐만 아니라, 클라우드 및 빅데이터 인프라 구축에도 사용되고 있다. 또한, 데스크톱이나 모바일 기기, 스마트 TV나 자동차 등 에도 탑재되고 있다. 특히, 본격적인 IoT 시대를 앞 둔 현 시점에서는

데이터 수집 및 분석 등의 시스템에도 개방형 운영체제인 리눅스가 가장 큰 비중을 차지하리라고 예상되고 있다. 리눅스의 사용이 증가함에 따라 보안이 중요한 요소로 부각되고 있고, 리눅스 시스템 보안의 핵심은 사용자 관리에 있다고 볼 수 있다. 수많은 사용자 계정을 생성하는 서버뿐만 아니라 일반적인 리눅스 시스템에서도 보안을 이유로 절대권한자인 root 계정으로 접근을 막고 일반 사용자 계정으로 접근을 권장하고 있다.

본 논문에서 분석한 리눅스 사용자 및 관련 파일을 토대로 제시한 사용자 관리 기법을 활용한다면 안전한 리눅스 시스템 운영에 있어서 하나의 지침이 되는 역할을 수행할 것으로 사료된다.

감사의 글

이 논문은 2104년도 목원대학교 연구년 지원에 의하여 연구되었습니다.

참고 문헌

[1] S. J Jung, and Y. M. Bae, *To conquer Linux Master First Class*, Seoul, Korea: Booksholic publishing, 2015.

[2] Exploit Database [Internet]. Available: http://www.exploit-db.com/exploits/15274/.

[3] Common Vulnerabilities and Exposures [Internet]. Available: http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-CVE-2010-3847/.

[4] Red Hat, Red Hat Customer Portal [Internet]. Available: https://www.redhat.com/security/data/cve/CVE-2010-3847.html/.

[5] S. J Jung, and Y. M. Bae, "A study on the Linux Partition Considering Security," *Journal of Security Engineering*, Vol. 8, No. 1, pp. 67-76, Feb. 2011.

[6] Common Vulnerabilities and Exposures [Internet]. Available: http://www.courtesan.com/sudo/.

[7] Linux-PAM project [Internet]. Available: http://www.linux-pam.org/.

[8] Openwall, John the Ripper password cracker[Internet]. Available: http://www.openwall.com/john/.

정 성 재 (Sung-Jae Jung)
1998년 2월 : 한남대학교 컴퓨터공학과 (공학사)
2003년 8월 : 한남대학교 컴퓨터공학과 (공학석사)
2011년 2월 : 한남대학교 컴퓨터공학과 (공학박사)
2005년 3월 ~ 2010년 2월: 한남대학교 국제IT교육센터 전임강사
2015년 11월 ~ 현재 : ㈜엔버 기업부설연구소 소장
※ 관심분야 : 리눅스, 정보보호, 시스템보안, 클라우드 컴퓨팅, 서버 가상화

성 경 (Kyung Sung)
1994년 3월 ~ 2004년 2월 : 동해대학교 컴퓨터공학과 교수
2004년 3월 ~ 2014년 2월 : 목원대학교 컴퓨터교육과 교수
2014년~현재 : 목원대학교 공과대학 융합컴퓨터미디어학부 교수
※ 관심분야 : 정보보호 및 정보관리,가상현실,컴퓨터네트워크, 신경회로망, 컴퓨터교육