

4주차 3차시. 리눅스/유닉스 인증과 패스워드

【학습목표】

1. 리눅스/유닉스 인증 및 패스워드 관리에 대해 설명할 수 있다.

학습내용1 : 리눅스/유닉스 인증

1. 리눅스/유닉스의 인증 방식

윈도우의 인증 방식보다 단순하지만 윈도우 인증 방식보다 취약하지는 않음

리눅스에서 인증 필수 요소

패스워드 파일 : 패스워드는 shadow 파일에 암호화되어 저장

shadow 파일: shadow 파일에서 root 계정에 대한 정보 확인

```
# cat /etc/shadow
```

```
wishfree@localhost:/
File Edit View Search Terminal Help
[root@localhost ~]# cat /etc/shadow
root:$6$LLA8959yh6FPZ6j5:ohP0kx9NkTFtF88T2gB1vpepGlpU9.u5XKtaC1l03TjG58o/XgU8l?
80IXK1rtFK67oAtdXPaZr/uKuAuaFT0:14923:0:99999:7:::
bin:*:14789:0:99999:7:::
daemon:*:14789:0:99999:7:::
adm:*:14789:0:99999:7:::
lp:*:14789:0:99999:7:::
sync:*:14789:0:99999:7:::
shutdown:*:14789:0:99999:7:::
halt:*:14789:0:99999:7:::
mail:*:14789:0:99999:7:::
uucp:*:14789:0:99999:7:::
operator:*:14789:0:99999:7:::
games:*:14789:0:99999:7:::
gopher:*:14789:0:99999:7:::
ttp:*:14789:0:99999:7:::
nobody:*:14789:0:99999:7:::
avahi:autouid{1,14923}:
usbmuxd:{1,14923}:
dbus:{1,14923}:
rpc:{1,14923:0:99999:7:::
```

root : \$6\$LL489S99Pyh6~중략~Pazr/uKuAkuFT0/ : 14923 : 0 : 99999 : 7 : : :

- ① ② ③ ④ ⑤ ⑥ ⑦ ⑧ ⑨

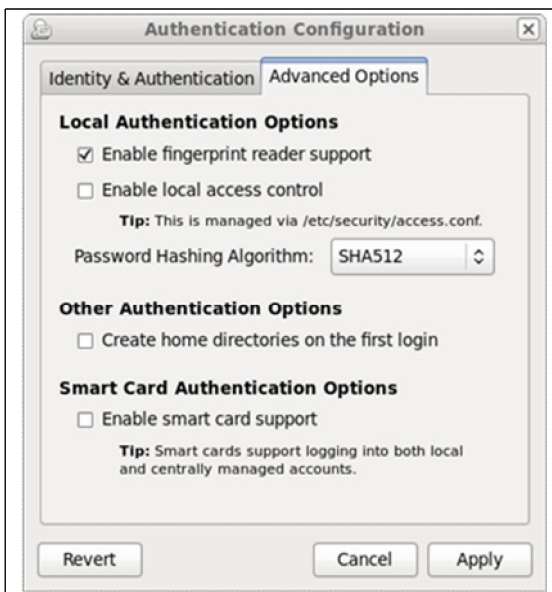
- ① 사용자 계정
- ② 암호화된 사용자의 패스워드 저장
 - \$1\$로 시작하면 MD5
 - \$5\$로 시작하면 SHA256
 - \$6\$로 시작하면 SHA512를 나타냄
- ③ 1970년 1월 1일부터 마지막으로 패스워드 변경한 날까지 계산 값
14923일은 약 41년
- ④ 패스워드 변경하기 전 패스워드 사용한 기간
최초 설정 후 바꾸지 않았으므로 0
- ⑤ 패스워드 바꾸지 않고 최대한 사용할 수 있는 기간
이 값은 보안 정책에 따라 변경 됨
보통 패스워드의 최대 사용 기간을 60일로 권고
- ⑥ 패스워드 최대 사용 기간에 가까워질 경우 사용자에게 미리 통지
패스워드 사용 기한 며칠 전에 경고를 보낼지 지정

- ⑦ 계정에 대한 사용 제한을 설정
며칠 후에 완전히 사용 정지할지 설정
- ⑧ 1970년 1월 1일부터 계정이 완전 사용 정지된 기간 계산 값 기록
- ⑨ 관리자 임의 사용 부분

- 로직이 정형화되어 있지 않음
- 운영체제로 다르며 기본적으로 대부분 Salt와 해시를 이용

2. 페도라 14의 인증 방식

- 기본적으로 SHA512 해시 알고리즘 사용
- [System]-[Administration]-[Authentication] 메뉴 선택 하면 ‘Advanced option’에서 추가적으로 MD5, SHA256 등의 알고리즘 선택 가능



3. 전형적인 리눅스의 인증 방식

passwd 파일과 shadow 파일을 이용

- /etc/passwd: passwd 파일은 대부분 /etc/passwd 파일로 동일
- /etc/shadow: shadow 파일은 운영체제별로 고유한 경로와 파일명을 사용하는 경우도 많음

4. 운영체제별 passwd와 shadow 파일 위치

운영체제	Shadow 파일 위치
IBM AIX	/etc/security/passwd
IBM A/ux 3.0.3 (RS-6000)	/tcblfile/auth/??/*
BSD 4.3 - Reno	/etc/master.passwd
DEC DG/ux (Digital Unix)	/etc/tcblaa/user
DEC EP/ux	/etc/shadow
HP/ux	/secure/etc/passwd
IRIX 5	/etc/shadow
Free BSD	/etc/shadow
SunOS 4.1 + C2	/etc/security/passwd.adjunct
SunOS 5.x	/etc/shadow, passwd
System V Release 4.0	/etc/shadow, passwd

학습내용2 : 리눅스 패스워드 크래킹

1. 주제

리눅스 패스워드 크래킹

2. 참고

- 한빛미디어
- 정보 보안 개론과 실습 : 시스템 해킹과 보안
- 199페이지
- 실습 4-2. 리눅스 패스워드 크래킹하기

3. 실습 환경 및 내용

- 페도라 14
- John-the-ripper를 이용한 무작위 대입 공격

4. John-the-ripper 설치

Yum(Yellow dog Updater, Modified)을 이용한 설치

Yum이란?

RPM 기반의 시스템을 위한 자동 업데이트 및 패키지 설치/제거 도구

패키지 설치 : yum install 패키지명

패키지 삭제 : yum remove 패키지명

패키지 업그레이드 : yum update 패키지명

```

root@fedora14:~# yum install john.i686
Loaded plugins: langpacks, presto, refresh-packagekit
Adding en_US to language list
Setting up Install Process
Resolving Dependencies
--> Running transaction check
--> Package john.i686 0:1.7.6-1.fc14 set to be installed
--> Finished Dependency Resolution

Dependencies Resolved

Package Arch Version Repository Size
-----
Installing:
john i686 1.7.6-1.fc14 updates 632 k

Transaction Summary
Install 1 Package(s)

Total download size: 632 k
Installed size: 1.5 M
Is this ok [y/N]:

```

5. John-the-ripper 명령어

```

root@fedora14:~# john
Created directory: /root/.john
John the Ripper password cracker, version 1.7.6
Copyright (c) 1996-2010 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single "single crack" mode
--wordlist=FILE --stdin wordlist mode, read words from FILE or stdin
--rules enable word mangling rules for wordlist mode
--incremental[=MODE] "incremental" mode [using section MODE]
--external=MODE external mode or word filter
--stdout[=LENGTH] just output candidate passwords [cut at LENGTH]
--restore[=NAME] restore an interrupted session [called NAME]
--session=NAME give a new session the NAME
--status[=NAME] print status of a session [called NAME]
--make-charset=FILE make a charset, FILE will be overwritten
--show show cracked passwords
--test[=TIME] run tests and benchmarks for TIME seconds each
--users=[-]LOGIN[UID[,...]] [do not] load this (these) user(s) only
--groups=[-]GID[,...] load users [not] of this (these) group(s) only
--shells=[-]SHELL[,...] load users with[out] this (these) shell(s) only
--salts=[-]COUNT load salts with[out] at least COUNT passwords only
--format=NAME force hash type NAME: DES/BSDF/MD5/BF/AFS/LM/crypt
--save-memory=LEVEL enable memory saving, at LEVEL 1..3

```

6. 테스트 계정 생성

useradd user

7. 테스트 계정 패스워드 설정

passwd user

```

root@fedora14:~# useradd user
root@fedora14:~# passwd user
Changing password for user user.
New password:
Retype new password:
passwd: all authentication tokens updated successfully.
root@fedora14:~#

```

8. 테스트 계정의 비밀번호 정보 확인

```
# cat /etc/shadow
```

```
root@fedora14:~# cat /etc/shadow
ntp:!:14976:::::::
nm-openconnect:!:14976:::::::
mailnull:!:14976:::::::
smmsp:!:14976:::::::
sshd:!:14976:::::::
smolt:!:14976:::::::
pulse:!:14976:::::::
gdm:!:14976:::::::
wishfree:$6$5/dV7bouH.nzNafZ5i58DTsWLF79qnfX4ITSwschsvz1Rof/n.338c9ZBLH7Wxk0LWKS
G8Emx1B2K/Z6T1AxkoKL8deXL7nLYD7T08:14976:0:99999:7:::
user:$6$5f/AtZ0$1EVdsUG5V3snW5SugjxHWCKCEH60N50TU/7HFQawyRiM1XiVq3pq4ijWX1oERIA
Hm8k8IMWec8c5InHiB6Jc/1:14976:0:99999:7:::
user0:$6$cSdHzvULsXrupNSYCSe495p51hIyhLNFE0y56thexVuB/SpfjEw7uwcYB12.tQwI3B0cZ.P
4bUyW64tt0N7B8Mk/TgTbk/:14976:0:99999:7:::
user1:$6$5qG6AdFw5AFs1CDVgF.cLKncLDxPbwYl1d8ZbPshRDswacAbLjfxGVKtEv4Zr1fd.7QeSM
6u9qB.GkHxscWvtyTt8N5m:/:14976:0:99999:7:::
user2:$6$yAxcLLl/SVKCS1hTAP1SFXHDKHr046Un0gm0sV6spPdQ9ZBgMyycgwxEtCzZEM/0cTv3
x20V5I/qYclwT2KxL0uJaLo/:14976:0:99999:7:::
[root@fedora14 ~]#
```

9. 사전 대입법을 이용한 비밀번호 크래킹

John-the-ripper를 이용

‘dideodlf’이라는 단어를 입력해둔 사전파일을 이용

```
# john --wordlist=dic /etc/shadow
```

```
root@fedora14:~# john --wordlist=dic /etc/shadow
Loaded 6 password hashes with 6 different salts (generic crypt(3) [7/32])
dideodlf (user)
dideodlf (root)
1234 (user0)
guesses: 4 time: 0:00:00 100% c/s: 26.66 trying: 1234 - dideodlf
[root@fedora14 ~]#
```

10. 무작위 대입법을 이용한 비밀번호 크래킹

사전 대입 공격이 실패할 경우 사용

--wordlist 옵션 없이 실행

```
# john --show /etc/shadow
```

```
root@fedora14:~# john --show /etc/shadow
root:dideodlf:14976:0:99999:7:::
wishfree:dideodlf:14976:0:99999:7:::
user:dideodlf:14976:0:99999:7:::
user0:1234:14976:0:99999:7:::
4 password hashes cracked, 2 left
[root@fedora14 ~]#
```

학습내용3 : 리눅스 패스워드 복구

1. 주제

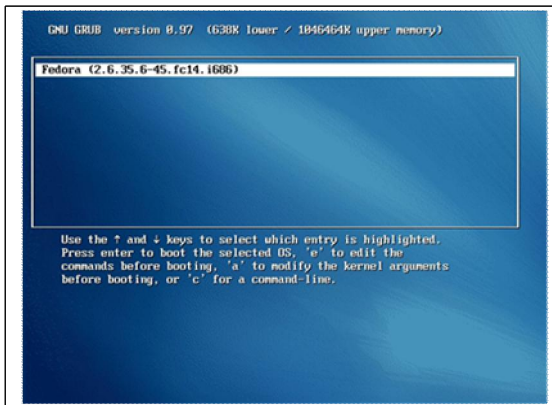
리눅스 패스워드 복구

2. 참고

- 한빛미디어
- 정보 보안 개론과 실습: 시스템 해킹과 보안
- 212페이지
- 실습 4-5. 리눅스 패스워드 복구하기

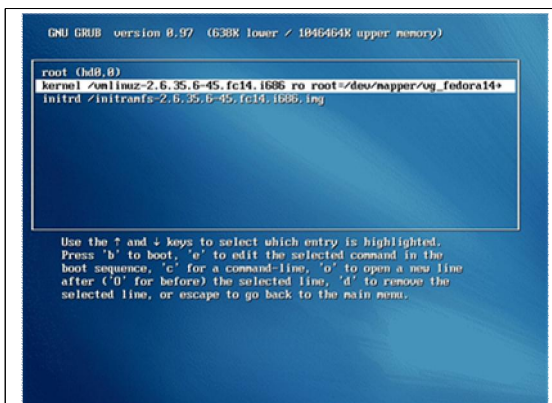
3. GRUB을 이용한 싱글 모드 부팅

GRUM 화면에서 e를 누름



5. 싱글 모드 부팅 설정

Kernel 선택 후 e를 누름



6. 싱글 모드 부팅

패스워드 입력 없이 셸을 획득할 수 있음

```

5.385340] sd 2:0:0:0: [sda] Assuming drive cache: write through
5.386163] sd 2:0:0:0: [sda] Assuming drive cache: write through
5.389579] sd 2:0:0:0: [sda] Assuming drive cache: write through
Welcome to
Starting udev: [ 10.756933] microcode: CPU0 update to revision 8xa3 failed
[ 10.757123] microcode: CPU0 update to revision 8xa3 failed
[ 10.758120] microcode: CPU0 update to revision 8xa3 failed
Setting hostname fedora14: [ OK ]
Setting up Logical Volume Management: 2 logical volume(s) in volume group "vg_
fedora14" now active [ OK ]
Checking filesystems
/dev/mapper/vg_fedora14-lv_root: clean, 146879/1152816 files, 971652/4683984 blo
cks
/dev/sda1: clean, 36/128016 files, 45179/512800 blocks [ OK ]
Remounting root filesystem in read-write mode: [ OK ]
Mounting local filesystems: [ OK ]
Enabling local filesystem quotas: [ OK ]
Enabling /etc/fstab swaps: [ OK ]
error: unexpectedly disconnected from boot status daemon
[root@fedora14 ~]#
[root@fedora14 ~]#
[root@fedora14 ~]#

```

7. 패스워드 파일 수정

편집기를 이용하여 /etc/shadow 내용 중 패스워드를 새로 설정할 계정의 x를 지우고 저장 후 부팅 이후 로그인할 때 패스워드를 물어보지 않음

```

root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:x:11:0:operator:/root:/sbin/nologin
games:x:12:100:games:/usr/games:/sbin/nologin
gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
ftp:x:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:x:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:x:170:170:Avahi IPoLL Stack:/var/lib/avahi-autoipd:/sbin/nologin
usbmuxd:x:113:113:usbmuxd user:/:/sbin/nologin
dbus:x:81:81:system message bus:/:/sbin/nologin
pcmcia:x:32:32:pcmcia:/var/lib/pcmcia:/sbin/nologin
rtkit:x:172:172:RealtimeKit:/proc:/sbin/nologin
oprofile:x:16:16:Special user account to be used by OProfile:/home/oprofile:/sbi
n/nologin

```

편집기를 이용하여 /etc/shadow 내용 중 패스워드를 새로 설정할 계정의 x를 지우고 저장 후 부팅 이후 로그인할 때 패스워드를 물어보지 않음

```

root:!:0:0:root:/root:/bin/bash
bin:!:1:1:bin:/bin:/sbin/nologin
daemon:!:2:2:daemon:/sbin:/sbin/nologin
adm:!:3:4:adm:/var/adm:/sbin/nologin
lp:!:4:7:lp:/var/spool/lpd:/sbin/nologin
sync:!:5:0:sync:/sbin:/bin/sync
shutdown:!:6:0:shutdown:/sbin:/sbin/shutdown
halt:!:7:0:halt:/sbin:/sbin/halt
mail:!:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:!:10:14:uucp:/var/spool/uucp:/sbin/nologin
operator:!:11:0:operator:/root:/sbin/nologin
games:!:12:100:games:/usr/games:/sbin/nologin
gopher:!:13:30:gopher:/var/gopher:/sbin/nologin
ftp:!:14:50:FTP User:/var/ftp:/sbin/nologin
nobody:!:99:99:Nobody:/:/sbin/nologin
avahi-autoipd:!:170:170:Avahi IPoLL Stack:/var/lib/avahi-autoipd:/sbin/nologin
usbmuxd:!:113:113:usbmuxd user:/:/sbin/nologin
dbus:!:81:81:system message bus:/:/sbin/nologin
pcmcia:!:32:32:pcmcia:/var/lib/pcmcia:/sbin/nologin
rtkit:!:172:172:RealtimeKit:/proc:/sbin/nologin
oprofile:!:16:16:Special user account to be used by OProfile:/home/oprofile:/sbi
n/nologin

```

【학습정리】

1. 윈도우의 패스워드를 분실한 경우 복구용 CD를 이용하여 패스워드를 초기화하는 방법을 사용한다.
2. 리눅스/유닉스 시스템에서 패스워드를 분실한 경우 싱글모드 부팅을 통해 비밀번호를 삭제하는 방법이 있다.