ФЕДЕРАЛЬНОЕ АГЕНТСТВО ОБРАЗОВАНИЯ

ДИМИТРОВГРАДСКИЙ ИНСТИТУТ ТЕХНОЛОГИЙ,

УПРАВЛЕНИЯ И ДИЗАЙНА

Лабораторная работа №2
по курсу: “Методы и средства защиты информации”
“Усиление локальной защиты ОС Linux”

Выполнил студент гр.ВТ-41:
Потеренко А.Г.
Проверил преподаватель:
Петлинский В.П.

Димитровград 2006г.

1. Пользователи в ОС Linux

Наличие или отсутствие пользователя в системе определяется записью в файле **/etc/passwd**. Каждая запись представляет собой строку, состоящую из семи полей, разделенных двоеточиями.

```
#more /etc/passwd
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
news:x:9:13:news:/etc/news:
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
dbus:x:81:81:System message bus:/:/sbin/nologin
vcsa:x:69:69:virtual console memory owner:/dev:/sbin/nologin
rpm:x:37:37::/var/lib/rpm:/sbin/nologin
haldaemon:x:68:68:HAL daemon:/:/sbin/nologin
netdump:x:34:34:Network Crash Dump user:/var/crash:/bin/bash
nscd:x:28:28:NSCD Daemon:/:/sbin/nologin
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
rpc:x:32:32:Portmapper RPC user:/:/sbin/nologin
mailnull:x:47:47::/var/spool/mqueue:/sbin/nologin
smmsp:x:51:51::/var/spool/mqueue:/sbin/nologin
rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
nfsnobody:x:65534:65534:Anonymous NFS User:/var/lib/nfs:/sbin/nologin
pcap:x:77:77::/var/arpwatch:/sbin/nologin
apache:x:48:48:Apache:/var/www:/sbin/nologin
squid:x:23:23::/var/spool/squid:/sbin/nologin
webalizer:x:67:67:Webalizer:/var/www/usage:/sbin/nologin
xfs:x:43:43:X Font Server:/etc/X11/fs:/sbin/nologin
ntp:x:38:38::/etc/ntp:/sbin/nologin
gdm:x:42:42::/var/gdm:/sbin/nologin
dovecot:x:97:97:dovecot:/usr/libexec/dovecot:/sbin/nologin
named:x:25:25:Named:/var/named:/sbin/nologin
omen:x:500:502::/home/omen:/bin/bash
```

Поля, слева направо, имеют следующие значения:

USER - имя пользователя.

PASSWORD - в старых версиях Unix в этом поле хранился зашифрованный пароль пользователя; в современных версиях поле содержит "x", а зашифрованный пароль хранится в файле **/etc/shadow**, который доступен для чтения только суперпользователю.

UID - идентификатор пользователя - целое положительное число, 0 зарезервирован для суперпользователя.

GID - идентификатор группы, в которую входит пользователь.

GECOS - произвольный текстовый комментарий (как правило, имя и фамилия пользователя).

HOME - домашний каталог пользователя.

SHELL - шелл - программа, запускаемая для обслуживания сеанса работы пользователя в системе. Для обычных пользователей это - командный интерпретатор.

Если пользователь должен быть членом более одной группы, то для внесения его в другие группы, следует указать имя пользователя в соответствующей строке файла **/etc/group**.

```
#more /etc/group
root:x:0:root
bin:x:1:root,bin,daemon
daemon:x:2:root,bin,daemon
sys:x:3:root,bin,adm
adm:x:4:root,adm,daemon
tty:x:5:
disk:x:6:root
lp:x:7:daemon,lp
mem:x:8:
kmem:x:9:
wheel:x:10:root
mail:x:12:mail
news:x:13:news
uucp:x:14:uucp
```

```
man:x:15:
games:x:20:
gopher:x:30:
dip:x:40:
ftp:x:50:
lock:x:54:
nobody:x:99:
users:x:100:
dbus:x:81:
floppy:x:19:
vcsa:x:69:
rpm:x:37:
utmp:x:22:
haldaemon:x:68:
netdump:x:34:
nscd:x:28:
slocate:x:21:
sshd:x:74:
rpc:x:32:
mailnull:x:47:
smmsp:x:51:
rpcuser:x:29:
nfsnobody:x:65534:
pcap:x:77:
apache:x:48:
squid:x:23:
webalizer:x:67:
xfs:x:43:
ntp:x:38:
gdm:x:42:
dovecot:x:97:
named:x:25:
_123:x:500:
omen:x:502:
```

Группа, которая указана для пользователя в файле **/etc/passwd** называется первичной группой этого пользователя, остальные группы, в которые он внесен согласно файлу **/etc/group**, - вторичными. Первичная группа отличается от вторичных только в следующем: когда пользователь создает файл (и у каталога не установлен бит SGID), то группой-владельцем нового файла будет первичная группа пользователя (владельцем файла будет он сам).

Файл **/etc/group** таким образом выполняет две функции: во-первых, он определяет имена и идентификаторы групп; во-вторых, указывает участие пользователей во вторичных для них группах.

Чтобы определить, в каких группах вы участвуете, надо подать команду:

```
#groups
root bin daemon sys adm disk wheel
```

После входа пользователя в систему, текущим каталогом для него становится его домашний каталог (указанный в поле HOME в файле **/etc/passwd**). Перед выводом приглашения командной строки шелл sh выполняет команды, записанный в файле **.profile** (начинается с точки), находящемся в домашнем каталоге пользователя (bash выполняет файл **.bashrc**). В этом файле как правило устанавливаются переменные окружения (в первую очередь - переменная PATH) и какие-либо параметры сессии.

```
#more .bashrc
-------------------------------------------
# .bashrc

# User specific aliases and functions

# Source global definitions
if [ -f /etc/bashrc ]; then
        . /etc/bashrc
fi
```

Обратите внимание на команду **export**, которая помечает переменную как "экспортируемую", т.е. переменная будет передаваться в окружение дочерних процессов, запускаемых вашим шеллом; иначе она будет видна только внутри процесса шелла.

```
#echo $PATH
/usr/kerberos/sbin:/usr/kerberos/bin:/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin:/usr/X11R6/bin
:/root/bin
```

Изменить переменную PATH "на ходу", добавив в нее еще один путь можно следующим образом:

```
#PATH=$PATH:/root/omega
#export PATH
```

Изменять переменную PATH следует после создания нового поискового каталога, иначе могут появиться диагностические сообщения об ошибке значения переменной.

Для корректной работы клавиши *<Backspace>* (ASCII код 8 или Ctrl-H) может понадобиться установить соответствующий параметр терминала, задающий символ, используемый для стирания предыдущего символа:

```
#stty erase '^H'
```

Узнать, **какие пользователи работают в настоящий момент в системе** и чем занимаются, можно с помощью команд

```
#who
root     :0           Oct  3 21:04
root     pts/1        Oct  3 22:28 (:0.0)

#w
22:30:17 up  1:29,  2 users,  load average: 0,33, 0,18, 0,33
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     :0       -                21:04   ?xdm?   9:23   1.92s /usr/bin/gnome-
root     pts/1    :0.0             22:28    0.00s  0.09s  0.00s w
```

Получить сведения о сеансах работы пользователей за больший период (период определяется временем ротации регистрационного файла /var/log/wtmp) можно следующей командой:

```
#last
root     pts/1        :0.0             Tue Oct  3 22:28   still logged in
root     pts/1        :0.0             Tue Oct  3 21:46 - 22:28  (00:42)
root     pts/1        :0.0             Tue Oct  3 21:10 - 21:46  (00:35)
root     :0                            Tue Oct  3 21:04   still logged in
reboot   system boot  2.6.9-34.EL      Tue Oct  3 21:02          (01:27)
root     :0                            Tue Oct  3 20:54 - down   (00:05)
reboot   system boot  2.6.9-34.EL      Tue Oct  3 20:52          (00:08)
root     pts/1        :0.0             Tue Oct  3 20:36 - 20:39  (00:02)
root     pts/1        :0.0             Tue Oct  3 19:45 - 20:36  (00:50)
root     pts/1        :0.0             Tue Oct  3 19:43 - 19:44  (00:01)
root     pts/1        :0.0             Tue Oct  3 19:37 - 19:39  (00:01)
root     pts/1        :0.0             Tue Oct  3 19:32 - 19:37  (00:04)
root     :0                            Tue Oct  3 19:30 - down   (01:14)
reboot   system boot  2.6.9-34.EL      Tue Oct  3 19:28          (01:16)
root     pts/1        :0.0             Tue Oct  3 18:22 - crash  (01:05)
root     :0                            Tue Oct  3 18:20 - crash  (01:08)
reboot   system boot  2.6.9-34.EL      Tue Oct  3 18:16          (02:28)
omen     :0                            Wed Sep 27 11:18 - down   (00:00)
root     :0                            Wed Sep 27 11:14 - 11:18  (00:03)
reboot   system boot  2.6.9-34.EL      Wed Sep 27 11:07          (00:11)

wtmp begins Wed Sep 27 11:07:33 2006
```

2. Отключение все специальных учётных записей

Удалите из системы всех пользователей и все группы, которые не используются: например lp, sync, shutdown, halt, news, uucp, operator, games, gopher и т.д.

Для удаления пользователя используйте команду:

```
#userdel lp
```

Для удаления группы:

```
#groupdel lp
```

3. Выбор правильных паролей

Прежде чем выбирать пароль, выполните следующие рекомендации. Длина пароля: после установки Linux минимально возможная длина пароля по умолчанию - 5 символов. Этого недостаточно, должно быть 8.

Отредактируйте файл **"/etc/login.defs"**

```
#more /etc/login.defs
# *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
PASS_MIN_DAYS  0
PASS_MIN_LEN   8
PASS_WARN_AGE  7

#
# 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 ORed with the -m flag on
# useradd command line.
#
CREATE_HOME    yes
```

Используя утилиту **"useradd"**, создайте пользователя с учетным именем **test.**

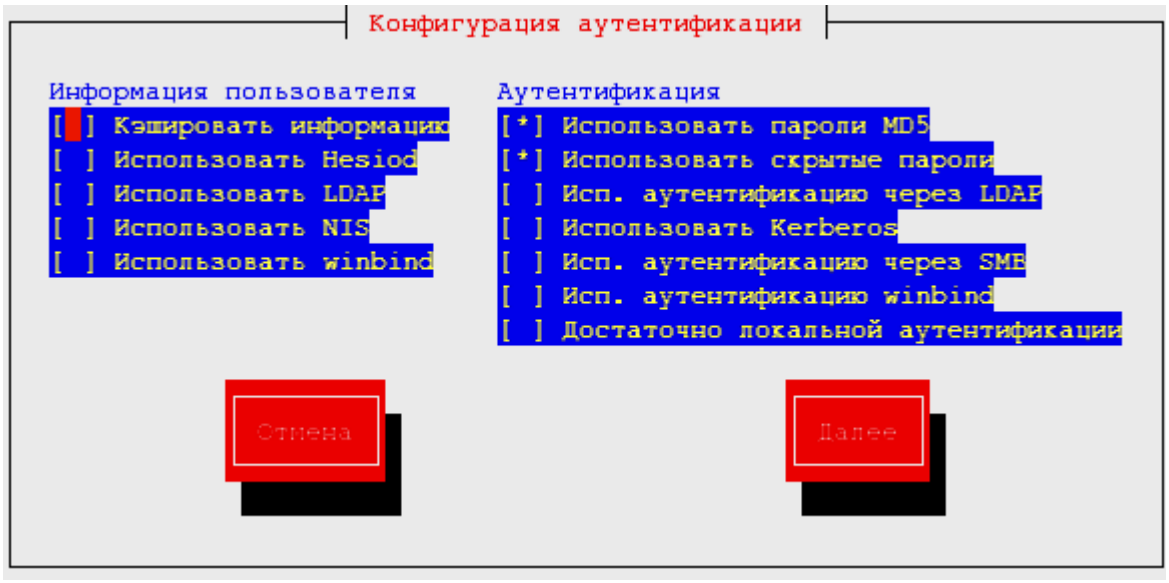
```
#useradd test
#passwd test
```

4. Включение поддержки теневых паролей

Включение возможности использования теневых **[shadow]** паролей позволяет хранить пароли в отдельном файле. Для включения поддержки теневых паролей в вашей системе можно использовать утилиту **"/usr/sbin/authconfig"**. Для конвертации существующих паролей и групп в теневые служат команды **pwconv, grpconv** соответственно.

Вызовите утилиту **"authconfig"** и убедитесь, что режим **shadow** включен. Запомните остальные схемы регистрации в системе, которые можно задавать посредством этой утилиты.

```
#/usr/sbin/authconfig
```



5. Учётная запись root'а

Учётная запись **"root"** -- наиболее привелигерованная в Unix. Когда администратор забывает выйти из системы, то система может автоматически закрыть консоль после заданного периода неактивности. Для того, чтобы этого добиться, нужно выставить значение в секундах в специальной переменной "TMOUT".

```
#more /etc/profile
----------------------------------------------------------------
# /etc/profile

# System wide environment and startup programs, for login setup
# Functions and aliases go in /etc/bashrc

pathmunge () {
        if ! echo $PATH | /bin/egrep -q "(^|:)$1($|:)" ; then
           if [ "$2" = "after" ] ; then
              PATH=$PATH:$1
           else
              PATH=$1:$PATH
           fi
        fi
}

# Path manipulation
if [ `id -u` = 0 ]; then
        pathmunge /sbin
        pathmunge /usr/sbin
        pathmunge /usr/local/sbin
fi

pathmunge /usr/X11R6/bin after


# No core files by default
ulimit -S -c 0 > /dev/null 2>&1

USER="`id -un`"
LOGNAME=$USER
MAIL="/var/spool/mail/$USER"

HOSTNAME=`/bin/hostname`
HISTSIZE=1000

if [ -z "$INPUTRC" -a ! -f "$HOME/.inputrc" ]; then
    INPUTRC=/etc/inputrc
fi

export PATH USER LOGNAME MAIL HOSTNAME HISTSIZE INPUTRC

for i in /etc/profile.d/*.sh ; do
    if [ -r "$i" ]; then
        . $i
    fi
```

```
done

TMOUT=10

unset i
unset pathmunge
```

Значение, указанное в переменной "TMOUT" в секундах. Если указать эту строку в **"/etc/profile"**, то консоль любого пользователя системы автоматически закроется после часа отсутствия активности. В файле **".bashrc"** вы можете установить эту переменную для каждого пользователя индивидуально. Для того чтобы изменения вступили в силу, необходимо выйти из системы и войти в нее снова.

6. Отключение консольного (console-equivalent) доступа для обычных пользователей к важным программам

На вашем сервере отключите консольный доступ обычных пользователей к таким программам, как **shutdown, reboot** и **halt** . Чтобы сделать это, выполните команду:

```
# rm -f /etc/security/console.apps/shutdown
# rm -f /etc/security/console.apps/reboot
# rm -f /etc/security/console.apps/halt
```

7. Запрещение для root входа с разных консолей

Файл **"/etc/securetty"** разрешает вам выбирать какие TTY-устройства пользователь **"root"** будет использовать для входа в систему. Отредактируйте файл **"/etc/securetty"** для отключения тех **tty**, которые вам не нужны.

```
#more /etc/securetty
console
vc/1
vc/2
vc/3
vc/4
vc/5
vc/6
vc/7
vc/8
vc/9
vc/10
vc/11
tty1
tty2
tty3
tty4
tty5
tty6
tty7
tty8
tty9
tty10
tty11
```

8. Блокирование получения прав "root" при помощи команды su

Команда **su (Substitute User)** предоставляет вам возможность становиться другими существующими пользователями системы. Если вы хотите, чтобы никто не мог получить права пользователя **"root"** или хотите ограничить использование команды **"su"** для определённых пользователей, то добавьте две следующие строки в начале файла конфигурации **"su"** в каталоге **"/etc/pam.d/"**.

Отредактируйте файл **su (/etc/pam.d/su)** и добавьте следующие строки в начале файла:

```
auth sufficient /lib/security/pam_rootok.so debug
auth sufficient /lib/security/pam_wheel.so trust use_uid
auth required   /lib/security/pam_wheel.so use_uid
```

Две последние строки подразумевают, что только пользователи группы **"wheel"** могут получить права **"root"** при помощи **su**. Вы можете добавить пользователей в группу wheel и только эти пользователи смогут получать через **su** права суперпользователя.

9. Ведение логов командной оболочки

Bash хранит до 500 введенных ранее команд в файле **“.bash_history”**, упрощая повторное использование команд. Каждый пользователь, который имеет в системе учётную запись, имеет и этот файл в домашнем каталоге. Bash может хранить меньшее число команд, чем указано выше и удалять их при выходе пользователя из системы.

Строки **HISTFILESIZE** и **HISTSIZE** в файле **"/etc/profile"** определяют размер файла **“.bash_history”** для всех пользователей системы.

```
HISTFILESIZE=30
HISTSIZE=30
```

Это позволит файлу **“.bash_history”** хранить не более 30 команд.

Администратор может добавить в файл **"/etc/skel/.bash_logout"** строку

```
rm -f $HOME/.bash_history
```

которая будет удалять файл **".bash_history"** каждый раз, когда пользователь будет выходить из системы. Эти изменения распространяются только на вновь регистрируемых пользователей. Для существующих пользователей следует отредактировать аналогичным образом файл **".bash_logout".**

10. Отключение команды перезагрузки системы с клавиатуры комбинацией (Control-Alt-Delete)

Чтобы сделать это закомментируйте следующую строку в файле **"/etc/inittab"**:

```
…
#ca::ctrlaltdel:/sbin/shutdown -t3 -r now
…
```

Для того, чтобы изменения вступили в силу, выполните команду:

```
#/sbin/init q
```

11. Сокрытие вашей системной информации

По умолчанию, когда вы входите в систему, вам сообщается название дистрибутива Linux, версию, версию ядра и имя сервера. Лучше оставить пользователю только приглашение "Login:" и всё.

- Отредактируйте файл **"/etc/rc.d/rc.local"** и поставьте "#" перед следующими строками:

```
# This will overwrite /etc/issue at every boot. So, make any changes you
# want to make to /etc/issue here or you will lose them when you reboot.
#echo "" > /etc/issue
#echo "$R" >> /etc/issue
#echo "Kernel $(uname -r) on $a $(uname -m)" >> /etc/issue
#
#cp -f /etc/issue /etc/issue.net
#echo >> /etc/issue
```

- Удалите также следующие файлы: **"issue.net"** и **"issue"** в каталоге **"/etc"**:

```
#rm -f /etc/issue
#rm -f /etc/issue.net
```

12. Отключите неиспользуемые программы с битами SUID/SGID

Постоянные пользователи имеют возможность запускать программы с правами "root", если у них выставлен бит SUID. Системный администратор должен минимизировать использование таких программ (SUID/SGID) и отключить те программы, которые не нужны.

• Чтобы найти программы с владельцем root и установленным битом 's', воспользуйтесь командой:

```
# find / -type f \( -perm -04000 -o -perm -02000 \) \-exec ls -lg {} \;
```

• Для отключения у выбранных программ бита suid выполните:

```
# chmod a-s [имя программы]
```

13. Проверка надежности паролей от взлома.

Для проверки надежности установленных паролей у зарегистрированных пользователей используются программы вскрытия паролей. В данной работе для проверки используется свободно распространяемая программа john-1.7.2.

С помощью john-1.7.2 вскройте пароли пользователей зарегистрированных вами в системе (test и test1). Для проверки сначала установите для них простые пароли, например, qwerty и 12345. Затем смените их на более сложные длиной - 8 символов и с использованием символов нижнего и верхнего регистров и цифровой клавиатуры. Оцените время вскрытия паролей в том и другом случае.

```
#cd /root
#tar zxvf john-1.7.2.tar.gz
#cd john-1.7.2
#cd src
# make clean linux-x86-any
# cd ../run
#./john --test
```