Лабораторная работа № 1.
Управление пользователями, группами пользователей и правами на файлы и каталоги в Linux

Задачи

1) Научиться создавать, изменять и редактировать учетные записи пользователей и групп пользователей в Linux.
2) научиться задавать атрибуты прав и владения для файлов и каталогов под конкретные задачи

Подсказки

1) В работе используются следующие команды (в дополнение к изученным в предыдущих лабораторных работах): **`groupadd, useradd, groupdel, userdel, groupmod, usermod, openssl, chage, chmod, chgrp, chown, groups, id.`**
2) Сведения о пользователях системы и их идентификаторах (UID) хранятся в файле **`/etc/passwd`**
3) Для вывода результата работы команды или конвейера команд в новый файл используется конструкция: **`command > file`**
4) Для добавления результатов работы команды или конвейера команд в конец существующего файла используется конструкция: **`command >> file`**
5) Директория **`/etc/skel`** содержит копии различных установочных и других файлов, которые могут быть скопированы в новые домашние директории пользователей, когда программа **`useradd`** добавляет нового пользователя.
6) Для шифрования пароля можно использовать команду **`openssl passwd –crypt незашифрованный_пароль`**. Для того чтобы результат выполнения команды **`command2`** подставить в значение параметра **`p`** команды **`command1`** можно использовать конструкцию: **`command1 –p $(command2)`**
7) Для получения подробного справочного руководства по любой команде можно набрать в консоли «**`man название команды`**».
8) Для удобства работы можно пользоваться одновременно несколькими консолями. На одной консоли читать справочное руководство, на другой редактировать скрипт и т.п. Переключаться между ними можно нажатием комбинации клавиш Ctrl+Alt+Fn, где Fn – функциональная клавиша (F1 – для первой консоли, F2 – для второй, а вот 7-я консоль обычно занята графическим интерфейсом).
9) Для временного изменения контекста безопасности в Linux используются утилиты su и sudo. Они позволяют соответственно открыть шелл от имени другого пользователя или запустить команду в с повышенными привилегиями. Для безопасной работы в Linux рекомендуется использовать утилиту sudo. Она временно повышает привилегии до суперпользователя root или дот заданного в конфигурации пользователя. Обычно для использования sudo достаточно поставить пакет sudo и включить пользователя в группу sudo (в Debian) или weel (в CentOS). Существует файл sudoers для более тонкой настройки sudo. Для его редактирования используется редактор visudo, запускаемый от имени root.

Задание

Создать скрипт, который:

1) выводит в файл **`work3.log`** построчно список всех пользователей в системе в следующем формате: «**`user NNN has id MM`**»;
2) добавляет в файл **`work3.log`** строку, содержащую дату последней смены пароля для пользователя

root;

3) добавляет в файл **work3.log** список всех групп в системе (только названия групп) через запятую;
4) делает так, чтобы при создании нового пользователя у него в домашнем каталоге создавался файл **readme.txt** с текстом «**Be careful**!»;
5) создает пользователя **u1** с паролем **12345678**;
6) создает группу **g1**;
7) делает так, чтобы пользователь **u1** дополнительно входил в группу **g1**;
8) добавляет в файл **work3.log** строку, содержащую сведения об идентификаторе и имени пользователя **u1** и идентификаторах и именах всех групп, в которые он входит;
9) делает так, чтобы пользователь **user** дополнительно входил в группу **g1**
10) добавляет в файл **work3.log** строку с перечнем пользователей в группе **g1** через запятую;
11) делает так, что при входе пользователя **u1** в систему вместо оболочки **bash** автоматически запускается **/usr/bin/mc**, при выходе из которого пользователь возвращается к вводу логина и пароля;
12) создает пользователя **u2** с паролем **87654321**;
13) в каталоге **/home** создает каталог **test13,** в который копирует файл **work3.log** два раза с разными именами (**work3-1.log** и **work3-2.log**);
14) сделает так, чтобы пользователи **u1** и **u2** смогли бы просматривать каталог **test13** и читать эти файлы, только пользователь **u1** смог бы изменять и удалять их, а все остальные пользователи системы не могли просматривать содержимое каталога **test13** и файлов в нем. При этом никто не должен иметь права исполнять эти файлы;
15) создает в каталоге **/home** каталог **test14,** в который любой пользователь системы сможет записать данные, но удалить любой файл сможет только пользователь, который его создал или пользователь **u1**;
16) копирует в каталог **test14** исполняемый файл редактора **nano** и делает так, чтобы любой пользователь смог изменять с его помощью файлы, созданные в пункте 13;
17) создает каталог test15 и создает в нем текстовый файл /test15/secret_file. Делает так, чтобы содержимое этого файла можно было вывести на экран, только зная имя файла, но узнать имена файлов в каталоге кроме как подбором было бы невозможно.
18) Настроить sudo таким образом, чтобы пользователь u1 смог с помощью sudo и команды passwd менять пароли другим пользователям, но не смог бы использовать другие утилиты от имени root.

Отдельно создать второй скрипт, который полностью уничтожает результаты деятельности предыдущего: удаляет созданных пользователей и их домашние каталоги, удаляет созданные группы, удаляет все созданные в предыдущем скрипте файлы и каталоги.