Лабораторная работа
Использование пакета OpenSSH

1 Генерация RSA ключа

Для генерации ключа используется утилита `ssh-keygen`. По умолчанию утилита генерирует RSA ключ. При указании аргумента `-d` генерируется DSA ключ. Секретный ключ защищается паролем и сохраняется в файле `.ssh/identity`, открытый ключ сохраняется в файле `.ssh/identity.pub`. Открытый ключ необходимо, затем, скопировать в файл `.ssh/authorized_keys` в домашнем каталоге пользователя на удаленной машине (т.е. на той машине, на которую пользователь собирается заходить с других компьютеров).

Задание 1: Сгенерируйте RSA ключ, скопируйте файл `.ssh/identity.pub` в файл `.ssh/authorized_keys` (Поскольку у Вас один и тот же домашний каталог на всех машинах, то данная операция аналогична копированию файла на удаленную машину).

2 Вход на удаленную машину

Для того, чтобы зайти на удаленную машину, т.е. запустить на ней командный интерпретатор, используется команда `ssh`. В простейшем виде команда имеет следующий синтаксис:

```
ssh [-l имя_пользователя] [хост|пользоатель@хост] [команда]
```

Если имя пользователя не указано, то используется имя пользователя запустившего программу `ssh`. Если не указана команда, то запускается командный интерпретатор пользователя, указанный в файле `/etc/passwd`.

Задание 2: Зайдите на любую другую машину при помощи команды `ssh`.

3 Использование ssh-agent

Программа `ssh` каждый раз запрашивает пароль пользователя, которым защищен секретный ключ. Для того, чтобы пароль не запрашивался постоянно, а сохранялся в памяти для последующего использования, служит программа `ssh-agent`. Программа создает локальный сокет UNIX и сообщает его другим приложениям при помощи переменных окружения. Режим доступа к сокету устанавливается таким образом, что чтение данных из сокета может производить только создавший его пользователь[1]. Синтаксис программы:

```
ssh-agent [-k] [комада]
```

Программа создает сокет, устанавливает переменные окружения и порождает процесс определенный командой. Этот процесс и его дочерние процессы наследуют переменные окружения указывающие на созданный сокет и на номер процесса `ssh-agent`. Для использования `ssh-agent` в текущем процессе можно выполнить команду:

```
eval `ssh-agent`
```

Ключ `-k` используется для завершения программы `ssh-agent`.

Для добавления ключей в хранилище `ssh-agent` используется команда `ssh-add`:

```
ssh-add [-ld] [file...]
```

Команда читает указанный файл, содержащий секретный ключ пользователя, запрашивает у пользователя пароль к ключу и передает ключ программе `ssh-agent`. Если файл ключа не указан, то программа использует файл `.ssh/identity`. Если в командной строке указан

[1] Данное ограничение не действует на пользователя root.

аргумент `-l`, то команда `ssh-add` выводит список ключей. Если указан аргумент `-d`, то команда удаляет ключ из хранилища `ssh-agent`.

Задание 3: Запустите программу ssh-agent при помощи команды `eval 'ssh-agent'`, добавьте в хранилище свой ключ. Зайдите при помощи программы `ssh` на другой компьютер.

4 Удаленный запуск программ

При запуске программы на другом компьютере программа `ssh` перенаправляет стандартные ввод и вывод программы на локальный компьютер. Это делает возможным включение команд запускаемых на удаленной машине в конвейеры выполняемые на локальной машине. Например:

```
ssh it-1 cat /var/log/messages | grep sshd | \
ssh cat >/tmp/ttt
```

Задание 4: Выполните команду `ls /etc` на компьютере `nix`, отсортируйте результат на любом другом компьютере и сохраните результат в файле отчета.

5 Копирование файлов при помощи ssh

Для копирование файлов с одного компьютера на другой можно использовать команду scp. Синтаксис команды следующий:

```
scp -pr [[user1@]host1:]file1 ... [[user2@]host2:]file2
```

Использование ключа `-p` позволяет сохранить время доступа и модификации файла и права доступа к нему, а ключ `-r` используется для рекурсивного копирования каталогов.

Спецификация файла может включать в себя имя компьютера, на котором хранится файл, и имя пользователя, под учетной записью которого будет осуществлен доступ к файлу.

Задание 5: Создайте в каталоге `/tmp` файл и скопируйте его на другую машину, также в каталог `/tmp`.

6 Пересылка протокола X11

Программа ssh позволяет перенаправлять вывод запускаемых на удаленном хосте программ X11 на локальный дисплей. Для использования этой возможности следует при запуске ssh указать ключ `-X`. Если используется ключ `-X` и определена переменная окружения `DISPLAY`, то ssh определит на удаленном хосте переменную `DISPLAY` таким образом, что запускаемые там программы X11 будут выводить информацию на локальный дисплей, пересылая ее через защищенный канал. При этом ssh самостоятельно осуществляет авторизацию удаленного клиента X11.

Например, для запуска на удаленном хосте программы xterm следует выполнить следующую команду:

```
ssh -X host xterm
```

Задание 6: Запустите на другом компьютере программу xterm.

Для того, чтобы запущенная программа выполнялась в фоновом режиме, следует добавить к команде ssh ключ `-f`:

```
ssh -f -X host xflame
```

Задание 7: Запустите на разных компьютерах программы xcalc, xclock, xeyes, xload

Необходимо заметить, что шифрование замедляет передачу данных и может заметно сказаться на работе программ активно выводящих графическую информацию.

Задание 8: Запустите на удаленном компьютере программу xflame при помощи ssh:

```
ssh -f -X host xflame
```

Теперь выполните следующие команды:

```
xhost +host
ssh -f host xflame -display $HOSTDISPLAY
xhost -host
```

При этом программа xflame будет использовать стандартный протокол X11 без шифрования. Наконец, запустите программу xflame на локальном компьютере.