МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ЛИПЕЦКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»

Институт Компьютерных наук
Кафедра Прикладной математики

ЛАБОРАТОРНАЯ РАБОТА

По дисциплине: «Операционные системы Linux».
На тему: «Работа с SSH».

Студент ПМ-22 (группа) _____ (подпись, дата) Борисов А. В. (фамилия, инициалы)

Руководитель

к. т. н. (ученая степень, ученое звание) _____ (подпись, дата) Кургасов В. В. (фамилия, инициалы)

Липецк 2024

Цель работы:

Ознакомление с программным обеспечением удаленного доступа к распределенным системам обработки данных.

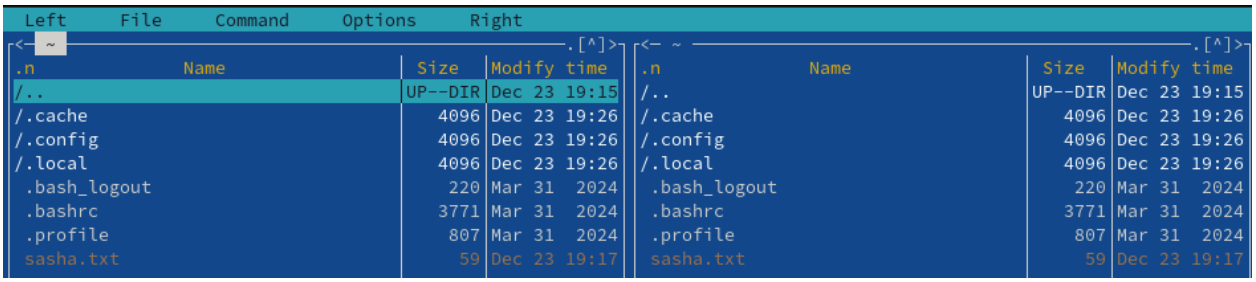
Ход работы:

1. **Подключимся к удаленному серверу используя ssh и просмотрим информацию о текущей системе с помощью команды uname -a.**

```
exerted@fedora:~$ ssh sasha@89.22.229.135
The authenticity of host '89.22.229.135 (89.22.229.135)' can't be established.
ED25519 key fingerprint is SHA256:F7Wb/ZpCycYqhmjri8d5iYw8yJW4BhF68BqIXb35Rsk.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? y
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '89.22.229.135' (ED25519) to the list of known hosts.
sasha@89.22.229.135's password:
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

 System information as of Mon Dec 23 06:50:54 PM UTC 2024

  System load:  0.0               Processes:             95
  Usage of /:   21.5% of 29.44GB  Users logged in:       0
  Memory usage: 17%               IPv4 address for ens3: 89.22.229.135
  Swap usage:   0%                IPv6 address for ens3: 2a0b:4140:38a2::2

 * Strictly confined Kubernetes makes edge and IoT secure. Learn how MicroK8s
   just raised the bar for easy, resilient and secure K8s cluster deployment.

   https://ubuntu.com/engage/secure-kubernetes-at-the-edge

Expanded Security Maintenance for Applications is not enabled.

0 updates can be applied immediately.

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status


*** System restart required ***

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.


The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

Last login: Mon Dec 23 18:04:57 2024 from 95.179.94.235
$ uname -a
Linux curved-twig.aeza.network 6.8.0-45-generic #45-Ubuntu SMP PREEMPT_DYNAMIC Fri Aug 30 12:02:04 UTC 2024 x86_64 x86_64 x86_64 GNU/Linux
$
```

2. **Создадим на локальном узле файл с моим фио и номером лабораторной работы и отправим через ssh соединение воспользовавшись командой и проверим содержимое файла на удаленной машине воспользовавшись midnight commander.**

```
exerted@fedora:~$ scp ./sasha.txt sasha2@89.22.229.135:/home/sasha2
sasha2@89.22.229.135's password:
Permission denied, please try again.
sasha2@89.22.229.135's password:
sasha.txt                                     100%   59     1.6KB/s   00:00
```



3. **Сгенерируем пару ключей на локальном хосте при помощи команды ssh-keygen и отправим на удаленную машину в папку .ssh под именем authorized_keys.**

```
exerted@fedora:~$ ssh-keygen
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/exerted/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/exerted/.ssh/id_ed25519
Your public key has been saved in /home/exerted/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:VZX/3sRvexgZ3j+3O/qCvG3QRVz0Lw6iHAraUDfpEZ4 exerted@fedora
The key's randomart image is:
+--[ED25519 256]--+
|       .     ..oo+|
|      . +    .  .o.|
|     . E     .   ...|
|    . o o .      ..o|
|   . . . S . o.o=o|
|    + . o o o ++.=|
|   . . . o . o .=+|
|            o.o.oO|
|            .oo+*O|
+----[SHA256]-----+
exerted@fedora:~$
```

```
exerted@fedora:~/.ssh$ ssh sasha2@89.22.229.135
Welcome to Ubuntu 24.04.1 LTS (GNU/Linux 6.8.0-45-generic x86_64)
```

```
exerted@fedora:~$ scp ./sasha.txt sasha2@89.22.229.135:/home/sasha2
sasha.txt                                     100%   59     1.3KB/s   00:00
```

Вывод

В этой лабораторной работе мы ознакомились с программным обеспечением удаленного доступа к распределенным системам обработки данных.

Контрольные вопросы:

1. Что такое ключ SSH? В чем преимущество их использования?

SSH-ключ — это пара криптографических ключей (публичный и приватный), которые используются для аутентификации при работе с протоколом SSH. Преимущества включают высокий уровень безопасности, удобство (например, безпарольный вход, что и продемонстрировано в лабораторной работе) и защиту от атак, таких как подбор паролей.

2. Как сгенерировать ключи SSH в разных ОС?

На Linux и macOS команда `ssh-keygen` в терминале. На Windows можно использовать PowerShell с `ssh-keygen` или утилиту PuTTYgen. Везде задается тип ключа и место его сохранения.

3. Возможно ли из «секретного» ключа сгенерировать «публичный» и/или наоборот?

Да, публичный ключ можно получить из приватного, а обратное невозможно из-за особенностей асимметричного шифрования.

4. Будут ли отличаться пары ключей, сгенерированные на одном ПК несколько раз с исходными условиями?

Да, они будут разными, так как при генерации используются случайные данные.

5. Перечислите доступные ключи для ssh-keygen.exe.

Основные: RSA, ED25519, ECDSA, DSA (последний устарел).

6. Можно ли использовать один «секретный» ключ доступа с разных ОС?

Да, можно, если приватный ключ перенести на другие устройства. Для безопасности рекомендуется создавать разные ключи для разных систем.

7. Возможно ли подключение «по ключу» SSH к системе с ОС Windows, где работает OpenSSH сервер?
Да, нужно настроить сервер OpenSSH, добавить публичный ключ в файл `authorized_keys` и убедиться, что аутентификация по ключу включена в настройках.

8. Какие известные сервисы позволяют использовать SSH-ключи?
GitHub, GitLab, AWS, DigitalOcean, Google Cloud Platform, Heroku и другие сервисы предоставляют эту возможность.