Санкт-Петербургский Национальный Исследовательский
Университет ИТМО
Факультет Программной Инженерии и Компьютерной Техники

Практическая работа №2
по дисциплине
'Современные инструменты анализа данных'

Выполнили Студенты
Пономарев Вадим
Птицын Максим
Воронина Дарья
Коновалов Арсений
Преподаватель:
Береснев Артем Дмитриевич

г. Санкт-Петербург
2022г.

Часть 2

```
c7-1
sshd
PMEuser
```

```
Sep 27 18:11:11 c7-2 groupadd[1883]: group added to /etc/group: name=PMEuser, G
ID=1001
Sep 27 18:11:11 c7-2 groupadd[1883]: group added to /etc/gshadow: name=PMEuser
Sep 27 18:11:11 c7-2 groupadd[1883]: new group: name=PMEuser, GID=1001
Sep 27 18:11:11 c7-2 useradd[1889]: new user: name=PMEuser, UID=1001, GID=1001,
 home=/home/PMEuser, shell=/bin/bash, from=/dev/pts/1
Sep 27 18:11:24 c7-2 passwd[1900]: pam_unix(passwd:chauthtok): password changed
 for PMEuser
Sep 27 18:11:24 c7-2 passwd[1900]: gkr-pam: couldn't update the login keyring p
assword: no old password was entered
Sep 27 18:11:42 c7-2 chfn[1901]: changed user 'PMEuser' information
Sep 27 18:14:02 c7-2 sshd[2096]: Accepted password for PMEuser from 10.0.0.1 po
rt 56486 ssh2
Sep 27 18:14:02 c7-2 sshd[2096]: pam_unix(sshd:session): session opened for use
r PMEuser(uid=1001) by (uid=0)
Sep 27 18:14:02 c7-2 systemd-logind[567]: New session 3 of user PMEuser.
Sep 27 18:14:02 c7-2 systemd: pam_unix(systemd-user:session): session opened fo
r user PMEuser(uid=1001) by (uid=0)
```

Конфигурим ssh

```
33 PermitRootLogin no
32 LoginGraceTime 30s
35 MaxAuthTries 3
```

Состояние сервиса

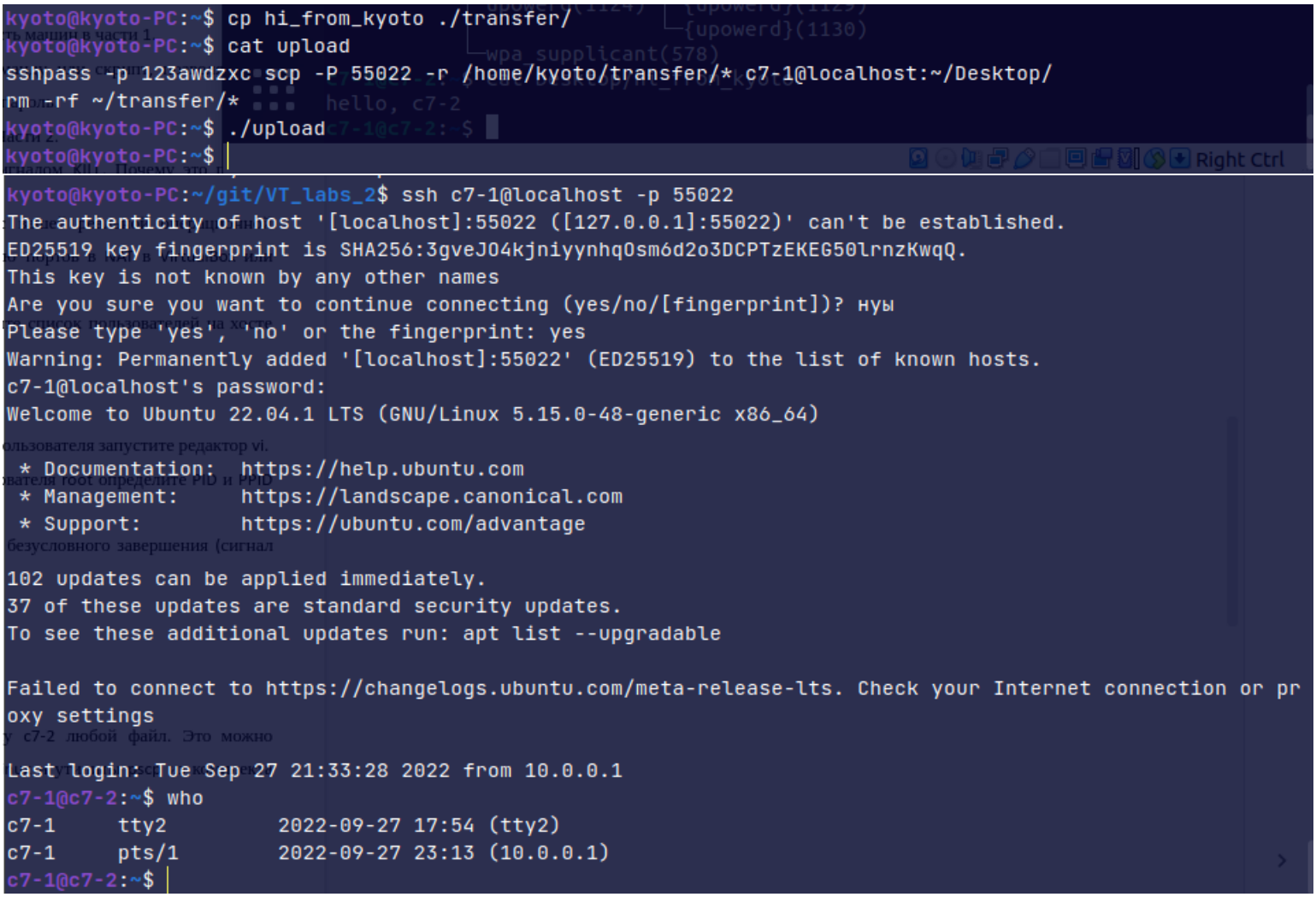
```
сен 27 19:19:11 c7-2 systemd[1]: Stopping OpenBSD Secure Shell server..
сен 27 19:19:11 c7-2 sshd[4067]: Received signal 15; terminating.
сен 27 19:19:11 c7-2 systemd[1]: ssh.service: Deactivated successfully.
сен 27 19:19:11 c7-2 systemd[1]: Stopped OpenBSD Secure Shell server.
сен 27 19:19:11 c7-2 systemd[1]: Starting OpenBSD Secure Shell server..
сен 27 19:19:11 c7-2 sshd[4071]: Server listening on 0.0.0.0 port 22.
сен 27 19:19:11 c7-2 sshd[4071]: Server listening on :: port 22.
сен 27 19:19:11 c7-2 systemd[1]: Started OpenBSD Secure Shell server.
```

Добавление в групу sudo юзеров(на нашей убунту не было wheel)

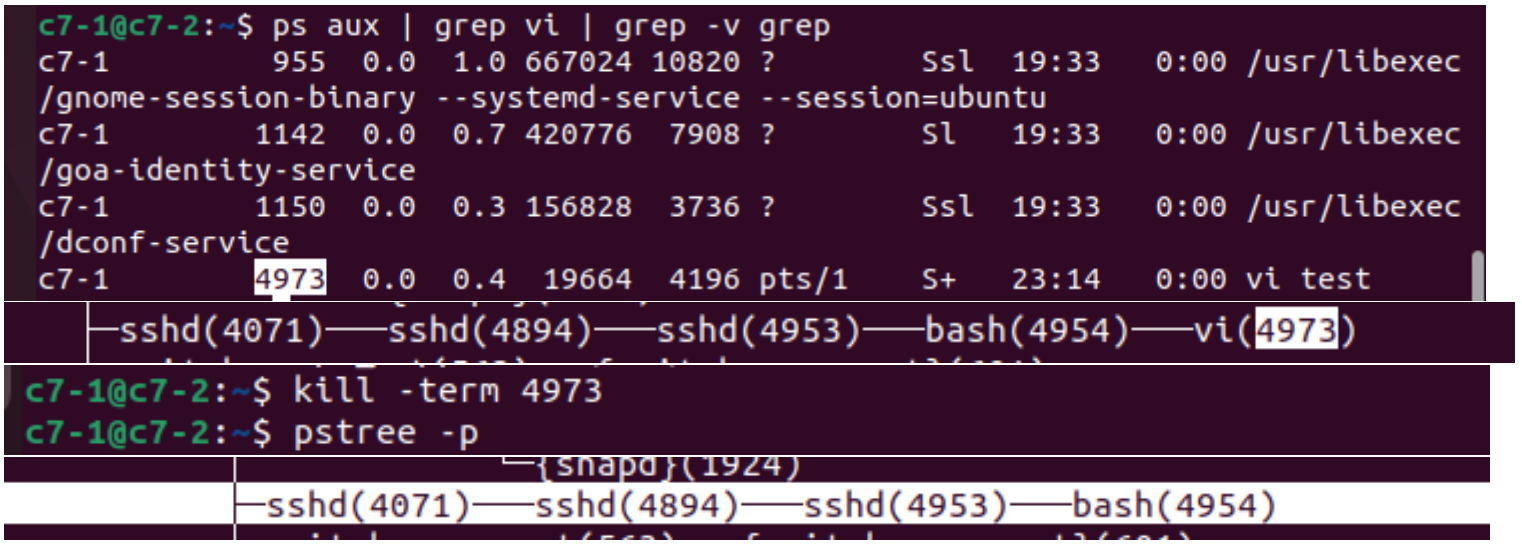
```
root@c7-2:~# usermod -aG sudo PMEuser
root@c7-2:~# sudo - PMEuser
sudo: -: command not found
root@c7-2:~# su - PMEuser
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

Show Applications
PMEuser@c7-2:~$
```

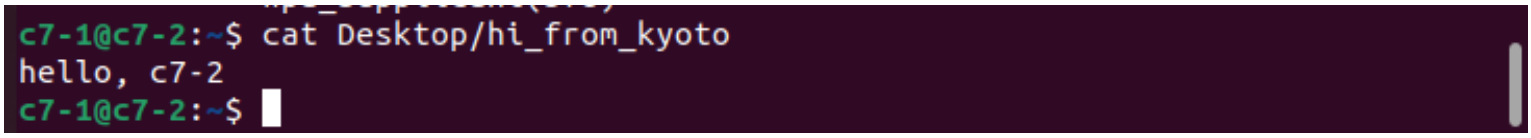
Часть 3


kyoto@kyoto-PC:~$ cp hi_from_kyoto ./transfer/
kyoto@kyoto-PC:~$ cat upload
sshpass -p 123awdzxc scp -P 55022 -r /home/kyoto/transfer/* c7-1@localhost:~/Desktop/
rm -rf ~/transfer/*
kyoto@kyoto-PC:~$ ./upload
kyoto@kyoto-PC:~$
kyoto@kyoto-PC:~/git/VT_labs_2$ ssh c7-1@localhost -p 55022
The authenticity of host '[localhost]:55022 ([127.0.0.1]:55022)' can't be established.
ED25519 key fingerprint is SHA256:3gveJO4kjniyynhqOsm6d2o3DCPTzEKEG50lrnzKwqQ.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? нуы
Please type 'yes', 'no' or the fingerprint: yes
Warning: Permanently added '[localhost]:55022' (ED25519) to the list of known hosts.
c7-1@localhost's password:
Welcome to Ubuntu 22.04.1 LTS (GNU/Linux 5.15.0-48-generic x86_64)
* Documentation: https://help.ubuntu.com
* Management: https://landscape.canonical.com
* Support: https://ubuntu.com/advantage
102 updates can be applied immediately.
37 of these updates are standard security updates.
To see these additional updates run: apt list --upgradable
Failed to connect to https://changelogs.ubuntu.com/meta-release-lts. Check your Internet connection or pr
oxy settings
Last login: Tue Sep 27 21:33:28 2022 from 10.0.0.1
c7-1@c7-2:~$ who
c7-1 tty2 2022-09-27 17:54 (tty2)
c7-1 pts/1 2022-09-27 23:13 (10.0.0.1)
c7-1@c7-2:~$

Часть 4


c7-1@c7-2:~$ ps aux | grep vi | grep -v grep
c7-1 955 0.0 1.0 667024 10820 ? Ssl 19:33 0:00 /usr/libexec
/gnome-session-binary --systemd-service --session=ubuntu
c7-1 1142 0.0 0.7 420776 7908 ? Sl 19:33 0:00 /usr/libexec
/goa-identity-service
c7-1 1150 0.0 0.3 156828 3736 ? Ssl 19:33 0:00 /usr/libexec
/dconf-service
c7-1 4973 0.0 0.4 19664 4196 pts/1 S+ 23:14 0:00 vi test
├─sshd(4071)──sshd(4894)──sshd(4953)──bash(4954)──vi(4973)
c7-1@c7-2:~$ kill -term 4973
c7-1@c7-2:~$ pstree -p
└─{snapd}(1924)
├─sshd(4071)──sshd(4894)──sshd(4953)──bash(4954)

Часть 5



Ответы на вопросы

1)С помощью команды **ping**(пинганули ip-шник)
2)sudo useradd -p $(openssl passwd -1 **password**) **username**
3)Чтение файла с паролями пользователей без root доступа звучит весьма странно :)

```
PMEuser@c7-2:~$ cat /etc/shadow
cat: /etc/shadow: Permission denied
PMEuser@c7-2:~$ sudo -i
[sudo] password for PMEuser:
root@c7-2:~# cat /etc/shadow
root:!:19262:0:99999:7:::
daemon:*:19213:0:99999:7:::
bin:*:19213:0:99999:7:::
sys:*:19213:0:99999:7:::
sync:*:19213:0:99999:7:::
games:*:19213:0:99999:7:::
man:*:19213:0:99999:7:::
lp:*:19213:0:99999:7:::
mail:*:19213:0:99999:7:::
news:*:19213:0:99999:7:::
uucp:*:19213:0:99999:7:::
proxy:*:19213:0:99999:7:::
www-data:*:19213:0:99999:7:::
backup:*:19213:0:99999:7:::
list:*:19213:0:99999:7:::
irc:*:19213:0:99999:7:::
gnats:*:19213:0:99999:7:::
nobody:*:19213:0:99999:7:::
systemd-network:*:19213:0:99999:7:::
systemd-resolve:*:19213:0:99999:7:::
messagebus:*:19213:0:99999:7:::
systemd-timesync:*:19213:0:99999:7:::
```

4)Убивание процесса через kill может вызвать ситуацию, когда дочерние процессы станут осиротевшими. Тогда они будут висеть и тратить ресурсы пк