Модуль 1 практика 2
Силантьев Дмитрий Сергеевич

Раздел 1

1. Создайте на сервере для 1 практики ключ ssh при помощи программы ssh-keygen

С помощью команды ssh-keygen

```
eltex-pg1-v19@eltex-16:02:~$ ssh-keygen
Generating public/private rsa key pair.
Enter file in which to save the key (/home/eltex-pg1-v19/.ssh/id_rsa):
/home/eltex-pg1-v19/.ssh/id_rsa already exists.
Overwrite (y/n)? y
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/eltex-pg1-v19/.ssh/id_rsa
Your public key has been saved in /home/eltex-pg1-v19/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:fCbdjhTdQ0jGKOjSCfmOYs8grD65xkCgGn6C9jWeWo4 eltex-pg1-v19@eltex
The key's randomart image is:
+---[RSA 3072]----+
|      . .   +o..  |
|.   o . . .ooo    |
|o    = . .. . o   |
|o.  . =. . o   . |
|*.   +  S = .     |
|==+..o.  = o      |
|=o==o.o   . .     |
|.= .*o            |
|oooE..            |
+----[SHA256]-----+
```

2. Скопируйте созданный ключ на сервер для 2 практики для пользователя root при помощи программы ssh-copy-id

```
eltex-pg1-v19@eltex-16:04:~$ ssh-copy-id root@172.16.9.193
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/eltex-pg1-
19/.ssh/id_rsa.pub"
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are promp
ed now it is to install the new keys
```

3. Подключитесь к серверу для 2 практики под пользователем root и сравните содержимое файла открытого ключа на сервере 1 ~/.ssh/*.pub и файла ~/.ssh/authorized_keys на сервере для 2 практики, а так же права доступа для каждого из файлов

С помощью команды ssh root@172.16.9.193 подключился к серверу 2

```
eltex-pg1-v19@eltex-16:12:~$ ssh root@172.16.9.193
root@172.16.9.193's password:
Welcome to Ubuntu 24.04.2 LTS (GNU/Linux 6.8.0-57-generic x86_64)

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

 System information as of Sun May 25 09:12:29 AM UTC 2025

  System load:  0.0               Processes:             110
  Usage of /:   41.1% of 14.66GB  Users logged in:       0
  Memory usage: 10%               IPv4 address for ens18: 172.16.9.193
  Swap usage:   0%

 * 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.

44 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

2 additional security updates can be applied with ESM Apps.
Learn more about enabling ESM Apps service at https://ubuntu.com/esm


*** System restart required ***
Last login: Sun May 25 07:48:06 2025 from 172.16.8.2
```

Содержимое файла на сервере 1 и права доступа

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDgkZZaD1WOuOW/ZaBX15GDgs3ZeeXt1aUSANqmV8gF9hm/2sU5SZ2maw2/kPH8mvRFQzqlMLfMWZ4
J8Jd91PRH0Pi/WJapccTRZEmGHzGGgJhdMkiYPuqDvxIoVDgdG40XEAciGDcBs6Aoukx4S9jMsAU1agvDPeZVG32k+L6Xy3g8cZ+i8pavYbXk8hfUWA
0YDx4hJh/4t5m35/RFjnyc1R3dyftl1gi8zea7Zu/hO8bvrqv6QbhKS0kU4qhP3lcXMgE0Ki0PyKj1ShiRXAq3cg1daotnK/PWPt2htMwgJUAadRJ3x
lf+Dzf5QMe0XOZ5co0TyEQDjKoTq0uBE2CK0BFieQD+cB5vx7eWvKYWZLKszF8sjJkfcxx7ZQl4E6U8lK4fjMM0a3mOZbhX2fnaafW/zsbS3EkGE8yv
3oFYQQ1jynXKzrrJT+pV9f6F87iEAt6uos38NYq/B+OdaLHXl/oNHAa3oguLQLAfXr2HKD4Rzcsnh0xfk5XOQiHhpnk= eltex-pg1-v19@eltex
eltex-pg1-v19@eltex-16:15:~$ ls -l ~/.ssh/*.pub
-rw-r--r-- 1 eltex-pg1-v19 eltex-pg1-v19 573 May 25 16:04 /home/eltex-pg1-v19/.ssh/id_rsa.pub
```

Содержимое файла на сервере 2 и права доступа

```
root@eltex-practice2-pg1-v19:~# cat ~/.ssh/authorized_keys
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQCflhC4gwPqAS7WlA5XmIKOpUH+BMAUAfz6d7MdzIU/tkh8euBcMzbYbX+OmssIHXi1q76DuiRzT2X
SKyrwgerU9x/gslQr7mhan//Vx9YDcDoCZ7MRbZ1nrYD19AxFJIdp+9IdjjmBXPazy0LNQ33efeSQ4ZnAhFEAeEu8MtPeRDFzVuUOCWcxbUjenA/cc/
dokFJs/qdYkWMsKO64QdTqW3HWPCIb1DBVs5feqUpFOjKPe54vqS0QTe4qLGQxEhpL4A2fLu034pHuxWZP0fNVBo1mu9SUaEp2RY4cQyZxDRjjeWJX+
gDpZT/lVduxqI8JQ0TjRizpDfwQQmBsxF1MT7emrbmAz+VyHnY+zuJKIOJpATKBftzQdQCG7+Ho2LtDgbjjOMhXKDS2SxULrJEsirq3aLQSSMloSk2
GKmGlHsn6087CrMyzk5mWHI9Jg+/LW9kiWh4AlpDu94e9p1GTQ8hugIltHM0S37FOdy7YORx+Wi6gQVCXR3tXEbtj0c= eltex-pg1-v19@eltex
root@eltex-practice2-pg1-v19:~# ls -l ~/.ssh/authorized_keys
-rw------- 1 root root 573 Mar 17 04:09 /root/.ssh/authorized_keys
```

Содержимое файлов одинаково, права отличаются. У первого сервера: у владельца права на чтение и запись, у группы и остальных только чтение. У второго сервера: запись и чтение только у владельца.

4. Создайте пользователя user1 при помощи команды useradd, укажите необходимость создания домашнего каталога и shell /bin/bash. Создайте пароль пользователю user1

Создаем командой useradd -m -d /home/user1 -s /bin/bash user1

Задаем пароль passwd user1

```
root@eltex-practice2-pg1-v19:/# useradd -m -d /home/user1 -s /bin/bash user1
root@eltex-practice2-pg1-v19:/# passwd user1
New password:
Retype new password:
No password has been supplied.
New password:
Retype new password:
passwd: password updated successfully
```

5. Создайте пользователя user2 и user3 при помощи команды adduser

```
root@eltex-practice2-pg1-v19:/# adduser user2
info: Adding user `user2' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `user2' (1002) ...
info: Adding new user `user2' (1002) with group `user2 (1002)' ...
info: Creating home directory `/home/user2' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user2
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] Y
info: Adding new user `user2' to supplemental / extra groups `users' ...
info: Adding user `user2' to group `users' ...
root@eltex-practice2-pg1-v19:/# adduser user3
info: Adding user `user3' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `user3' (1003) ...
info: Adding new user `user3' (1003) with group `user3 (1003)' ...
info: Creating home directory `/home/user3' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for user3
Enter the new value, or press ENTER for the default
        Full Name []:
        Room Number []:
        Work Phone []:
        Home Phone []:
        Other []:
Is the information correct? [Y/n] y
info: Adding new user `user3' to supplemental / extra groups `users' ...
info: Adding user `user3' to group `users' ...
```

6. Для пользователя user3 смените shell на /usr/sbin/nologin (man usermod), выполните вход под этим пользователем при помощи утилиты su, сначала без

дополнительных параметров, затем с явным указанием shell /bin/bash в параметрах su. Выполните logout

usermod -s /usr/bin/nologin user3

```
root@eltex-practice2-pg1-v19:/# usermod -s /usr/bin/nologin user3
usermod: Warning: missing or non-executable shell '/usr/bin/nologin'
```

su user3

```
root@eltex-practice2-pg1-v19:/# su user3
su: failed to execute /usr/bin/nologin: No such file or directory
```

su -s /bin/bash user3

```
su: using restricted shell /usr/bin/nologin
su: failed to execute /usr/bin/nologin: No such file or directory
```

7. Создайте новую группу и добавьте её для всех пользователей user* как дополнительную, посмотрите список групп всех пользователей user*

```
user3@eltex-practice2-pg1-v19:/$ usermod -a -G group1 user1
usermod: Permission denied.
usermod: cannot lock /etc/passwd; try again later.
user3@eltex-practice2-pg1-v19:/$ exit
exit
root@eltex-practice2-pg1-v19:/# usermod -a -G group1 user1
root@eltex-practice2-pg1-v19:/# usermod -a -G group1 user2
root@eltex-practice2-pg1-v19:/# usermod -a -G group1 user3
root@eltex-practice2-pg1-v19:/# id
uid=0(root) gid=0(root) groups=0(root)
root@eltex-practice2-pg1-v19:/# su user1
user1@eltex-practice2-pg1-v19:/$ id
uid=1001(user1) gid=1001(user1) groups=1001(user1),1004(group1)
user1@eltex-practice2-pg1-v19:/$ id -G
1001 1004
user1@eltex-practice2-pg1-v19:/$ logout
bash: logout: not login shell: use `exit'
user1@eltex-practice2-pg1-v19:/$ exit
exit
root@eltex-practice2-pg1-v19:/# su user2
user2@eltex-practice2-pg1-v19:/$ id
uid=1002(user2) gid=1002(user2) groups=1002(user2),100(users),1004(group1)
user2@eltex-practice2-pg1-v19:/$ exit
exit
root@eltex-practice2-pg1-v19:/# su user3
su: failed to execute /usr/bin/nologin: No such file or directory
root@eltex-practice2-pg1-v19:/# su -s /bin/bash user3
user3@eltex-practice2-pg1-v19:/$ id
uid=1003(user3) gid=1003(user3) groups=1003(user3),100(users),1004(group1)
```

9. Создайте каталог /opt/share и назначьте группу из предыдущего пункта его владельцем, установите на этот каталог бит SGID, права для группы rwx.

```
root@eltex-practice2-pg1-v19:~# mkdir -p ~/opt/share
root@eltex-practice2-pg1-v19:~# ls -ld ~/opt/share
drwxr-xr-x 2 root root 4096 May 25 09:42 /root/opt/share
root@eltex-practice2-pg1-v19:~# chgrp group1 ~opt/share
chgrp: cannot access '~opt/share': No such file or directory
root@eltex-practice2-pg1-v19:~# chgrp group1 ~/opt/share
root@eltex-practice2-pg1-v19:~# chmod g+s ~/opt/share
root@eltex-practice2-pg1-v19:~# ls -ld ~/opt/share
drwxr-sr-x 2 root group1 4096 May 25 09:42 /root/opt/share
```

Командой chmod g+rwx ~/opt/share выдадим права

```
root@eltex-practice2-pg1-v19:~# ls -ld ~/opt/share
drwxrwsr-x 2 root group1 4096 May 25 09:42 /root/opt/share
```

10. Для user1 задайте перманентно umask, снимающий право чтения для «прочих»

```
root@eltex-practice2-pg1-v19:~# umask -S u=rwx,g=rwx,o=
u=rwx,g=rwx,o=
```

11. Создайте каждым из пользователей новые файлы в каталоге /opt/share, удалите файлы созданные другими пользователями

```
root@eltex-practice2-pg1-v19:~# su user1
user1@eltex-practice2-pg1-v19:/root$ cd /root/opt/share
user1@eltex-practice2-pg1-v19:/root/opt/share$ touch test1.txt
user1@eltex-practice2-pg1-v19:/root/opt/share$ ls
test1.txt
user1@eltex-practice2-pg1-v19:/root/opt/share$ exit
exit
root@eltex-practice2-pg1-v19:~# su user2
user2@eltex-practice2-pg1-v19:/root$ cd opt/share
user2@eltex-practice2-pg1-v19:/root/opt/share$ rm test1.txt
user2@eltex-practice2-pg1-v19:/root/opt/share$ touch test2.txt
user2@eltex-practice2-pg1-v19:/root/opt/share$ ls
test2.txt
user2@eltex-practice2-pg1-v19:/root/opt/share$ exit
exit
root@eltex-practice2-pg1-v19:~# su -s /bin/bash user3
user3@eltex-practice2-pg1-v19:/root$ cd opt/share/
user3@eltex-practice2-pg1-v19:/root/opt/share$ rm test2.txt
user3@eltex-practice2-pg1-v19:/root/opt/share$ touch test1.txt
user3@eltex-practice2-pg1-v19:/root/opt/share$ ls
test1.txt
```

12. Повторите предыдущий пункт, предварительно установив sticky bit на каталоге /opt/share

Установка Sticky bit chmod +t /root/opt/share

При попытке удаления файла выдает ошибку

```
user1@eltex-practice2-pg1-v19:/root/opt/share$ rm test1.txt
rm: cannot remove 'test1.txt': Operation not permitted
```

13. Разрешите user1 выполнять привилегированную команду dmesg при помощи команды sudo, а user2 – при помощи скрипта на языке bash с установленным флагом SUID

User1

Командой sudo visudo зайдем в файл sudoers и добавим user1 ALL=(ALL) NOPASSWD: /bin/dmesg

```
# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "@include" directives:

@includedir /etc/sudoers.d
user1 ALL=(ALL) NOPASSWD: /bin/dmesg
```

Зайдем под пользователем и проверим

```
root@eltex-practice2-pg1-v19:~# su user1
user1@eltex-practice2-pg1-v19:/root$ sudo dmesg
[    0.000000] Linux version 6.8.0-57-generic (buildd@lcy02-amd64-040) (x86_64-linux-gnu-gcc-13 (Ubuntu 13.3.0-6ubu
ntu2~24.04) 13.3.0, GNU ld (GNU Binutils for Ubuntu) 2.42) #59-Ubuntu SMP PREEMPT_DYNAMIC Sat Mar 15 17:40:59 UTC 2
025 (Ubuntu 6.8.0-57.59-generic 6.8.12)
[    0.000000] Command line: BOOT_IMAGE=/vmlinuz-6.8.0-57-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   Hygon HygonGenuine
[    0.000000]   Centaur CentaurHauls
[    0.000000]   zhaoxin   Shanghai
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
[    0.000000] BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000100000000-0x000000013fffffff] usable
[    0.000000] BIOS-e820: [mem 0x000000fd00000000-0x000000ffffffffff] reserved
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] APIC: Static calls initialized
[    0.000000] SMBIOS 2.8 present.
[    0.000000] DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01
/2014
[    0.000000] Hypervisor detected: KVM
[    0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[    0.000000] kvm-clock: using sched offset of 465160743160 cycles
[    0.000002] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159059148
3 ns
[    0.000005] tsc: Detected 3399.996 MHz processor
[    0.001192] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.001196] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.048198] AGP: No AGP bridge found
```

User2

Используем команды для выдачи прав

```
root@eltex-practice2-pg1-v19:~# sudo nano /usr/local/bin/dmesg_suid.sh
root@eltex-practice2-pg1-v19:~# sudo chmod 755 /usr/local/bin/dmesg_suid.sh
root@eltex-practice2-pg1-v19:~# chown root:user2 /usr/local/bin/dmesg_suid.sh
root@eltex-practice2-pg1-v19:~# chmod u+s /usr/local/bin/dmesg_suid.sh
root@eltex-practice2-pg1-v19:~# ls -l /usr/local/bin/dmesg_suid.sh
-rwsr-xr-x 1 root user2 23 Mar 17 06:05 /usr/local/bin/dmesg_suid.sh
```

Разрешаем использование для всех пользователей

echo "kernel.dmesg_restrict=0" | sudo tee -a /etc/sysctl.conf

Проверяем

```
root@eltex-practice2-pg1-v19:~# su user2
user2@eltex-practice2-pg1-v19:/root$ /usr/local/bin/dmesg_suid.sh
[    0.000000] Linux version 6.8.0-57-generic (buildd@lcy02-amd64-040) (x86_64-linux-gnu-gcc-13 (Ubuntu 13.3.0-6ubu
ntu2~24.04) 13.3.0, GNU ld (GNU Binutils for Ubuntu) 2.42) #59-Ubuntu SMP PREEMPT_DYNAMIC Sat Mar 15 17:40:59 UTC 2
025 (Ubuntu 6.8.0-57.59-generic 6.8.12)
[    0.000000] Command line: BOOT_IMAGE=/vmlinuz-6.8.0-57-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro
[    0.000000] KERNEL supported cpus:
[    0.000000]   Intel GenuineIntel
[    0.000000]   AMD AuthenticAMD
[    0.000000]   Hygon HygonGenuine
[    0.000000]   Centaur CentaurHauls
[    0.000000]   zhaoxin   Shanghai
[    0.000000] BIOS-provided physical RAM map:
[    0.000000] BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
[    0.000000] BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
[    0.000000] BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
[    0.000000] BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
[    0.000000] BIOS-e820: [mem 0x0000000100000000-0x000000013fffffff] usable
[    0.000000] BIOS-e820: [mem 0x000000fd00000000-0x000000ffffffffff] reserved
[    0.000000] NX (Execute Disable) protection: active
[    0.000000] APIC: Static calls initialized
[    0.000000] SMBIOS 2.8 present.
[    0.000000] DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-prebuilt.qemu.org 04/01
/2014
[    0.000000] Hypervisor detected: KVM
[    0.000000] kvm-clock: Using msrs 4b564d01 and 4b564d00
[    0.000000] kvm-clock: using sched offset of 465160743160 cycles
[    0.000002] clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_idle_ns: 88159059148
3 ns
[    0.000005] tsc: Detected 3399.996 MHz processor
[    0.001192] e820: update [mem 0x00000000-0x00000fff] usable ==> reserved
[    0.001196] e820: remove [mem 0x000a0000-0x000fffff] usable
[    0.048198] AGP: No AGP bridge found
[    0.048617] last_pfn = 0x140000 max_arch_pfn = 0x400000000
[    0.048653] MTRR map: 4 entries (3 fixed + 1 variable; max 19), built from 8 variable MTRRs
[    0.048657] x86/PAT: Configuration [0-7]: WB  WC  UC- UC  WB  WP  UC- WT
[    0.048701] last_pfn = 0xbffda max_arch_pfn = 0x400000000
```

14. Для всех пользователей user* задайте время действия пароля – 10 дней.

Используем команду chage -M 10 $user

```
root@eltex-practice2-pg1-v19:~# chage -M 10 user1
root@eltex-practice2-pg1-v19:~# chage -M 10 user2
root@eltex-practice2-pg1-v19:~# chage -M 10 user3
```

15. Отредактируйте файл /etc/motd, вписав туда свое имя и фамилию

```
  GNU nano 7.2
Дмитрий Силантьев
```

16. Создайте копию содержимого каталога /etc в каталог /root/etc_backup при помощи программы rsync

```
root@eltex-practice2-pg1-v19:~# rsync etc/motd etc_backup/motd
root@eltex-practice2-pg1-v19:~# cat etc_backup/motd
Дмитрий Силантьев
```

17. Заархивируйте содержимое каталога /root/etc_backup архиватором tar, используйте алгоритмы сжатия gzip, bzip2, 7zip, сравните размеры полученных файлов

Создаем архив GZip командой tar -zcvf archive.tar.gz etc_backup/
Создаем архив BZip2 командой tar -jcvf archive.tar.bz2 etc_backup/

Создаем архив 7zip командой tar cf - etc_backup/ | 7z a -si archive.tar.7z

```
root@eltex-practice2-pg1-v19:~# tar -zcvf archive.tar.gz etc_backup/
etc_backup/
etc_backup/motd
root@eltex-practice2-pg1-v19:~#  tar -jcvf archive.tar.bz2 etc_backup/
etc_backup/
etc_backup/motd
root@eltex-practice2-pg1-v19:~# tar cf - etc_backup/ | 7z a -si archive.tar.7z

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_US.UTF-8 Threads:2 OPEN_MAX:1024

Creating archive: archive.tar.7z

Add new data to archive: 1 file


Files read from disk: 1
Archive size: 262 bytes (1 KiB)
Everything is Ok
```

С помощью ls -lh выводим информацию о файлах. Через 7zip файл весит 262 байта, через bzip2 191 байт, через gzip 192 байта

```
-rw-rw---- 1 root root  262 May 25 10:17 archive.tar.7z
-rw-rw---- 1 root root  191 May 25 10:17 archive.tar.bz2
-rw-rw---- 1 root root  192 May 25 10:17 archive.tar.gz
drwxrwx--- 2 root root 4.0K May 25 10:17 etc
drwxrwx--- 2 root root 4.0K May 25 10:17 etc_backup
drwxr-xr-x 3 root root 4.0K May 25 09:42 opt
```

18. Отредактируйте файл /etc/motd, вписав туда текущую дату и время, синхронизируйте каталог/root/etc_backup с каталогом /etc при помощи rsync, добавьте файл motd в архив, сжатый gzip

```
root@eltex-practice2-pg1-v19:~# nano /etc/motd
root@eltex-practice2-pg1-v19:~# sync etc/motd etc_backup/motd
```

Разархивирую архив gzip в motd добавил дату и время

```
Дмитрий Силантьев
25.05.2025
17:19
```

Архивируем измененный файл

```
total 40K
-rw-rw---- 1 root root  487 May 25 10:22 archive.tar.7z
-rw-rw---- 1 root root  10K May 25 10:23 archive.tar.bz2
-rw-rw---- 1 root root  10K May 25 10:21 archive.tar.gz
drwxrwx--- 2 root root 4.0K May 25 10:17 etc
drwxrwx--- 2 root root 4.0K May 25 10:17 etc_backup
drwxr-xr-x 3 root root 4.0K May 25 09:42 opt
```

19. Сравните содержимое архива, упакованного bzip2 с сорержимым каталога /root/etc_backup

Разархивировал и вывел содержимое двух файлов с помощью cat

```
root@eltex-practice2-pg1-v19:~# cat etc_backup_bzip2/etc_backup/motd
Дмитрий Силантьев
root@eltex-practice2-pg1-v19:~# cat etc_backup/motd
Дмитрий Силантьев
25.05.2025
17:19
```

20. Распакуйте архивы etc_backup, упакованные gzip и 7zip в каталоги /root/etc_backup_gzip и /root/etc_backup_7zip, сравните программой diff файлы motd в этих каталогах.

Командами tar -xvf archive.tar.gz -C ~/etc_backup_gzip
7z x archive.tar.7z -o./etc_backup_7zip/
Разархивировал в указынные каталоги, 7zip дополнительно разархивировал сам архив

```
root@eltex-practice2-pg1-v19:~# tar -xvf archive.tar.gz -C ~/etc_backup_gzip
etc_backup/
etc_backup/motd
root@eltex-practice2-pg1-v19:~# -o ./etc_backup_7zip/
-o: command not found
root@eltex-practice2-pg1-v19:~# 7z x archive.tar.7z -o./etc_backup_7zip/

7-Zip 23.01 (x64) : Copyright (c) 1999-2023 Igor Pavlov : 2023-06-20
 64-bit locale=en_US.UTF-8 Threads:2 OPEN_MAX:1024

Scanning the drive for archives:
1 file, 487 bytes (1 KiB)

Extracting archive: archive.tar.7z
--
Path = archive.tar.7z
Type = 7z
Physical Size = 487
Headers Size = 143
Method = LZMA2:24
Solid = -
Blocks = 2


Would you like to replace the existing file:
  Path:     ./etc_backup_7zip/archive.tar
  Size:     10240 bytes (10 KiB)
  Modified: 2025-05-25 10:17:50
with the file from archive:
  Path:     archive.tar
  Size:     10240 bytes (10 KiB)
  Modified: 2025-05-25 10:22:45
? (Y)es / (N)o / (A)lways / (S)kip all / A(u)to rename all / (Q)uit? y

Everything is Ok

Files: 2
Size:       20480
Compressed: 487
```

```
root@eltex-practice2-pg1-v19:~# cd etc_backup_7zip/
root@eltex-practice2-pg1-v19:~/etc_backup_7zip# tar -xvf archive.tar
etc_backup/
etc_backup/motd
```

Командой diff etc_backup_7zip/etc_backup/motd etc_backup_gzip/etc_backup/motd вывел различия(дата и время)

```
root@eltex-practice2-pg1-v19:~# diff etc_backup_7zip/etc_backup/motd etc_backup_gzip/etc_backup/motd
2,3d1
< 25.05.2025
< 17:19
```

Раздел 2

1. Найдите все записи из лога загрузки, доступного через команду journalctl с опцией -b в первые полторы секунды с момента загрузки

journalctl -b --until "2025-05-25 17:47:50"

```
root@eltex-practice2-pg1-v19:~# journalctl -b --until "2025-05-25 17:47:50"
Apr 07 02:13:17 localhost kernel: Linux version 6.8.0-57-generic (buildd@lcy02-amd64-040) (x86_64-linux-gnu-gcc-13>
Apr 07 02:13:17 localhost kernel: Command line: BOOT_IMAGE=/vmlinuz-6.8.0-57-generic root=/dev/mapper/ubuntu--vg-u>
Apr 07 02:13:17 localhost kernel: KERNEL supported cpus:
Apr 07 02:13:17 localhost kernel:   Intel GenuineIntel
Apr 07 02:13:17 localhost kernel:   AMD AuthenticAMD
Apr 07 02:13:17 localhost kernel:   Hygon HygonGenuine
Apr 07 02:13:17 localhost kernel:   Centaur CentaurHauls
Apr 07 02:13:17 localhost kernel:   zhaoxin   Shanghai
Apr 07 02:13:17 localhost kernel: BIOS-provided physical RAM map:
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x0000000000000000-0x000000000009fbff] usable
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x000000000009fc00-0x000000000009ffff] reserved
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x00000000000f0000-0x00000000000fffff] reserved
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x0000000000100000-0x00000000bffd9fff] usable
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x00000000bffda000-0x00000000bfffffff] reserved
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x00000000feffc000-0x00000000feffffff] reserved
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x00000000fffc0000-0x00000000ffffffff] reserved
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x0000000100000000-0x000000013fffffff] usable
Apr 07 02:13:17 localhost kernel: BIOS-e820: [mem 0x000000fd00000000-0x000000ffffffffff] reserved
Apr 07 02:13:17 localhost kernel: NX (Execute Disable) protection: active
Apr 07 02:13:17 localhost kernel: APIC: Static calls initialized
Apr 07 02:13:17 localhost kernel: SMBIOS 2.8 present.
Apr 07 02:13:17 localhost kernel: DMI: QEMU Standard PC (i440FX + PIIX, 1996), BIOS rel-1.16.3-0-ga6ed6b701f0a-pre>
Apr 07 02:13:17 localhost kernel: Hypervisor detected: KVM
Apr 07 02:13:17 localhost kernel: kvm-clock: Using msrs 4b564d01 and 4b564d00
Apr 07 02:13:17 localhost kernel: kvm-clock: using sched offset of 465160743160 cycles
Apr 07 02:13:17 localhost kernel: clocksource: kvm-clock: mask: 0xffffffffffffffff max_cycles: 0x1cd42e4dffb, max_>
Apr 07 02:13:17 localhost kernel: tsc: Detected 3399.996 MHz processor
```

2. Используя awk найдите все источники и их сообщения в файле auth.log (найдите его find), в названии источника удалите информацию об идентификаторе процесса при помощи sed, полученный результат отсортируйте по названию источника

find / -type f -name "auth.log" 2>/dev/null нашел файл auth.log

```
root@eltex-practice2-pg1-v19:~# find / -type f -name "auth.log" 2>/dev/null
/var/log/auth.log
```

Командой find /var/log -name "auth.log" -exec awk '{print $1, $2, $3, $5, $6, $7, $8, $9, $10}' {} \; | sed -E 's/\[[0-9]+\]//g' | sort -k4 нашел все источники

```
root@eltex-practice2-pg1-v19:~# find /var/log -name "auth.log" -exec awk '{print $1, $2, $3, $5, $6, $7, $8, $9, $1
0}' {} \; | sed -E 's/\[[0-9]+\]//g' | sort -k4
2025-05-25T09:12:04.286477+00:00 localhost sshd: 1 more authentication failure; logname= uid=0
2025-05-25T07:32:46.583795+00:00 localhost systemd-logind: 8263 logged out. Waiting for processes
2025-05-25T07:45:50.543017+00:00 localhost systemd-logind: 8267 logged out. Waiting for processes
2025-05-25T08:36:13.177211+00:00 localhost systemd-logind: 8270 logged out. Waiting for processes
2025-05-25T09:14:57.202368+00:00 localhost systemd-logind: 8281 logged out. Waiting for processes
2025-05-25T10:37:12.882663+00:00 localhost systemd-logind: 8284 logged out. Waiting for processes
2025-05-25T10:40:46.948023+00:00 localhost systemd-logind: 8296 logged out. Waiting for processes
2025-05-25T10:41:13.582979+00:00 localhost systemd-logind: 8298 logged out. Waiting for processes
2025-05-25T09:33:03.793077+00:00 localhost groupadd: added to /etc/group: name=user2, GID=1002
2025-05-25T09:33:29.495214+00:00 localhost groupadd: added to /etc/group: name=user3, GID=1003
2025-05-25T09:33:03.861785+00:00 localhost groupadd: added to /etc/gshadow: name=user2
2025-05-25T09:33:29.557668+00:00 localhost groupadd: added to /etc/gshadow: name=user3
2025-05-25T09:19:10.359092+00:00 localhost useradd: adding user 'user1', exit code: 9
2025-05-25T09:25:55.651514+00:00 localhost useradd: adding user 'user1', exit code: 9
2025-05-25T09:11:43.457875+00:00 localhost sshd: authentication failure; logname= uid=0 euid=0 tty=ssh
2025-05-25T09:05:10.889734+00:00 localhost sshd: closed by authenticating user root 172.16.8.2
2025-05-25T09:05:11.026808+00:00 localhost sshd: closed by authenticating user root 172.16.8.2
2025-05-25T09:10:13.188897+00:00 localhost sshd: closed by authenticating user root 172.16.8.2
2025-05-25T09:12:04.286286+00:00 localhost sshd: closed by authenticating user root 172.16.8.2
2025-05-25T07:45:50.541078+00:00 localhost sshd: disconnect from 172.16.8.2 port 40378:11: disconnected
2025-05-25T10:41:13.581359+00:00 localhost sshd: disconnect from 172.16.8.2 port 46734:11: disconnected
2025-05-25T10:37:12.873636+00:00 localhost sshd: disconnect from 172.16.8.2 port 47902:11: disconnected
2025-05-25T09:14:57.200504+00:00 localhost sshd: disconnect from 172.16.8.2 port 56846:11: disconnected
2025-05-25T10:40:46.946030+00:00 localhost sshd: disconnect from 172.16.8.2 port 58940:11: disconnected
2025-05-25T07:32:46.582383+00:00 localhost sshd: disconnect from 172.16.8.2 port 59362:11: disconnected
2025-05-25T08:36:12.782074+00:00 localhost sshd: disconnect from 172.16.8.2 port 60998:11: disconnected
2025-05-25T07:45:50.541229+00:00 localhost sshd: from user root 172.16.8.2 port 40378
2025-05-25T10:41:13.581432+00:00 localhost sshd: from user root 172.16.8.2 port 46734
2025-05-25T10:37:12.882519+00:00 localhost sshd: from user root 172.16.8.2 port 47902
2025-05-25T09:14:57.200655+00:00 localhost sshd: from user root 172.16.8.2 port 56846
2025-05-25T10:40:46.946139+00:00 localhost sshd: from user root 172.16.8.2 port 58940
2025-05-25T07:32:46.582531+00:00 localhost sshd: from user root 172.16.8.2 port 59362
2025-05-25T08:36:13.177009+00:00 localhost sshd: from user root 172.16.8.2 port 60998
2025-05-25T09:24:53.805347+00:00 localhost useradd: group: name=user1, GID=1001
2025-05-25T09:30:04.314316+00:00 localhost useradd: group: name=user1, GID=1001
2025-05-25T09:33:03.862595+00:00 localhost groupadd: group: name=user2, GID=1002
2025-05-25T09:33:29.558473+00:00 localhost groupadd: group: name=user3, GID=1003
2025-05-25T09:20:27.464318+00:00 localhost userdel: group 'user1' owned by 'user1'
2025-05-25T09:26:03.538450+00:00 localhost userdel: group 'user1' owned by 'user1'
2025-05-25T09:20:45.624513+00:00 localhost userdel: group 'user2' owned by 'user2'
2025-05-25T09:20:58.089566+00:00 localhost userdel: group 'user3' owned by 'user3'
2025-05-25T07:24:50.922282+00:00 localhost sshd: listening on :: port 22.
2025-05-25T09:33:15.553635+00:00 localhost gpasswd: of group users set by root
2025-05-25T09:33:42.399501+00:00 localhost gpasswd: of group users set by root
2025-05-25T09:31:08.178852+00:00 localhost passwd: password changed for user1
2025-05-25T09:33:08.216210+00:00 localhost passwd: password changed for user2
2025-05-25T09:33:35.587500+00:00 localhost passwd: password changed for user3
2025-05-25T10:01:50.571537+00:00 localhost chage: password expiry for user1
2025-05-25T10:01:55.269154+00:00 localhost chage: password expiry for user2
2025-05-25T10:01:58.492513+00:00 localhost chage: password expiry for user3
2025-05-25T09:11:45.055235+00:00 localhost sshd: password for root from 172.16.8.2 port
```

3. Для результата из предыдущего пункта найдите количество повторений для каждого источника и выведите их в виде списка «число_повторений источник», результат отсортируйте по убыванию количества повторений

Воспользуемся командой из предыдущего задания, изменим опции awk и добавим uniq -c и sort -nr

find /var/log -name "auth.log" -exec awk '{print $5}' {} \; | sed -E 's/\[[0-9]+\]//g' | sort -k4 | uniq -c | sort -nr

4. В файле /etc/passwd найдите всех пользователей в системе, у которых установлен shell /usr/sbin/nologin и выведите их в виде списка: «UID, username, список его групп»

Команда

awk -F: '$7 ~ "/usr/sbin/nologin$|/usr/bin/nologin$" {print $3, $1}' /etc/passwd | sort -nr | while read uid user; do

groups=$(grep -E "(:|,)$user(,|$)" /etc/group | cut -d: -f1 | paste -sd ",")

echo "$uid, $user, $groups"

done

5. Найдите в результате вывода dmesg все строки, содержащие слово 'kernel‘

Нашел строки с помощью grep -I (без учета регистра), итоговая команда: dmesg | grep -i "kernel"

```
root@eltex-practice2-pg1-v19:~# dmesg | grep -i "kernel"
[    0.000000] KERNEL supported cpus:
[    0.061675] Booting paravirtualized kernel on KVM
[    0.061982] Kernel command line: BOOT_IMAGE=/vmlinuz-6.8.0-57-generic root=/dev/mapper/ubuntu--vg-ubuntu--lv ro
[    0.062025] Unknown kernel command line parameters "BOOT_IMAGE=/vmlinuz-6.8.0-57-generic", will be passed to use
r space.
[    0.129923] Memory: 3933484K/4193760K available (22528K kernel code, 4444K rwdata, 14344K rodata, 4988K init, 47
16K bss, 260016K reserved, 0K cma-reserved)
[    0.312583] DMA: preallocated 512 KiB GFP_KERNEL pool for atomic allocations
[    0.312614] DMA: preallocated 512 KiB GFP_KERNEL|GFP_DMA pool for atomic allocations
[    0.312647] DMA: preallocated 512 KiB GFP_KERNEL|GFP_DMA32 pool for atomic allocations
[    0.642329] Loaded X.509 cert 'Build time autogenerated kernel key: 314db5b871207b67c6af73164cb9641e90a23972'
[    0.650159] Loaded X.509 cert 'Canonical Ltd. Kernel Module Signing: 88f752e560a1e0737e31163a466ad7b70a850c19'
[    1.817023] Loaded X.509 cert 'Build time autogenerated kernel key: 314db5b871207b67c6af73164cb9641e90a23972'
[    1.842214] Freeing unused kernel image (initmem) memory: 4988K
[    1.843103] Write protecting the kernel read-only data: 38912k
[    1.844495] Freeing unused kernel image (rodata/data gap) memory: 2040K
[   60.453177] systemd[1]: Listening on systemd-udevd-kernel.socket - udev Kernel Socket.
[   60.469014] systemd[1]: Mounting sys-kernel-debug.mount - Kernel Debug File System...
[   60.474780] systemd[1]: Mounting sys-kernel-tracing.mount - Kernel Trace File System...
[   60.535303] systemd[1]: Starting modprobe@configfs.service - Load Kernel Module configfs...
[   60.539905] systemd[1]: Starting modprobe@dm_mod.service - Load Kernel Module dm_mod...
[   60.548482] systemd[1]: Starting modprobe@drm.service - Load Kernel Module drm...
[   60.553397] systemd[1]: Starting modprobe@efi_pstore.service - Load Kernel Module efi_pstore...
[   60.562290] systemd[1]: Starting modprobe@fuse.service - Load Kernel Module fuse...
[   60.568805] systemd[1]: Starting modprobe@loop.service - Load Kernel Module loop...
[   60.635212] systemd[1]: Starting systemd-modules-load.service - Load Kernel Modules...
[   60.651096] systemd[1]: Starting systemd-remount-fs.service - Remount Root and Kernel File Systems...
[   60.671601] systemd[1]: Mounted sys-kernel-debug.mount - Kernel Debug File System.
[   60.672856] systemd[1]: Mounted sys-kernel-tracing.mount - Kernel Trace File System.
[   60.676499] systemd[1]: Finished modprobe@configfs.service - Load Kernel Module configfs.
[   60.678537] systemd[1]: Finished modprobe@dm_mod.service - Load Kernel Module dm_mod.
[   60.680663] systemd[1]: Finished modprobe@drm.service - Load Kernel Module drm.
[   60.683147] systemd[1]: Finished modprobe@fuse.service - Load Kernel Module fuse.
[   60.685158] systemd[1]: Finished modprobe@loop.service - Load Kernel Module loop.
[   60.691118] systemd[1]: Mounting sys-kernel-config.mount - Kernel Configuration File System...
[   60.711591] systemd[1]: Finished modprobe@efi_pstore.service - Load Kernel Module efi_pstore.
[   60.715647] systemd[1]: Mounted sys-kernel-config.mount - Kernel Configuration File System.
[1483137.705233] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483137.705778] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483260.583270] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483260.583779] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483260.584240] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483260.584639] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483260.585038] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483383.461329] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483383.461785] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483383.462301] "echo 0 > /proc/sys/kernel/hung_task_timeout_secs" disables this message.
[1483383.462476] Future hung task reports are suppressed, see sysctl kernel.hung_task_warnings
```

6. Подсчитайте количество строк в файле /var/log/kern.log

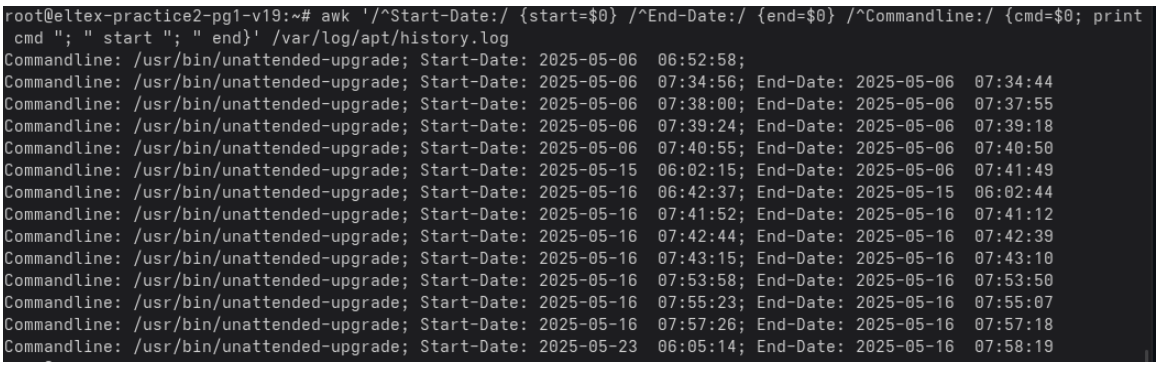
Подсчитал командой grep -c $ /var/log/kern.log

```
root@eltex-practice2-pg1-v19:~# grep -c $ /var/log/kern.log
11
```

7. Отформатируйте вывод записей в /var/log/apt/history.log в следующем порядке, построчно: Commandline: … ; Start-Date: … ; End-Date: …

С помощью awk отформатировал вывод

awk '/^Start-Date:/ {start=$0} /^End-Date:/ {end=$0} /^Commandline:/ {cmd=$0; print cmd "; " start "; " end}' /var/log/apt/history.log


root@eltex-practice2-pg1-v19:~# awk '/^Start-Date:/ {start=$0} /^End-Date:/ {end=$0} /^Commandline:/ {cmd=$0; print
cmd "; " start "; " end}' /var/log/apt/history.log
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-06 06:52:58;
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-06 07:34:56; End-Date: 2025-05-06 07:34:44
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-06 07:38:00; End-Date: 2025-05-06 07:37:55
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-06 07:39:24; End-Date: 2025-05-06 07:39:18
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-06 07:40:55; End-Date: 2025-05-06 07:40:50
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-15 06:02:15; End-Date: 2025-05-06 07:41:49
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-16 06:42:37; End-Date: 2025-05-15 06:02:44
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-16 07:41:52; End-Date: 2025-05-16 07:41:12
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-16 07:42:44; End-Date: 2025-05-16 07:42:39
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-16 07:43:15; End-Date: 2025-05-16 07:43:10
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-16 07:53:58; End-Date: 2025-05-16 07:53:50
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-16 07:55:23; End-Date: 2025-05-16 07:55:07
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-16 07:57:26; End-Date: 2025-05-16 07:57:18
Commandline: /usr/bin/unattended-upgrade; Start-Date: 2025-05-23 06:05:14; End-Date: 2025-05-16 07:58:19