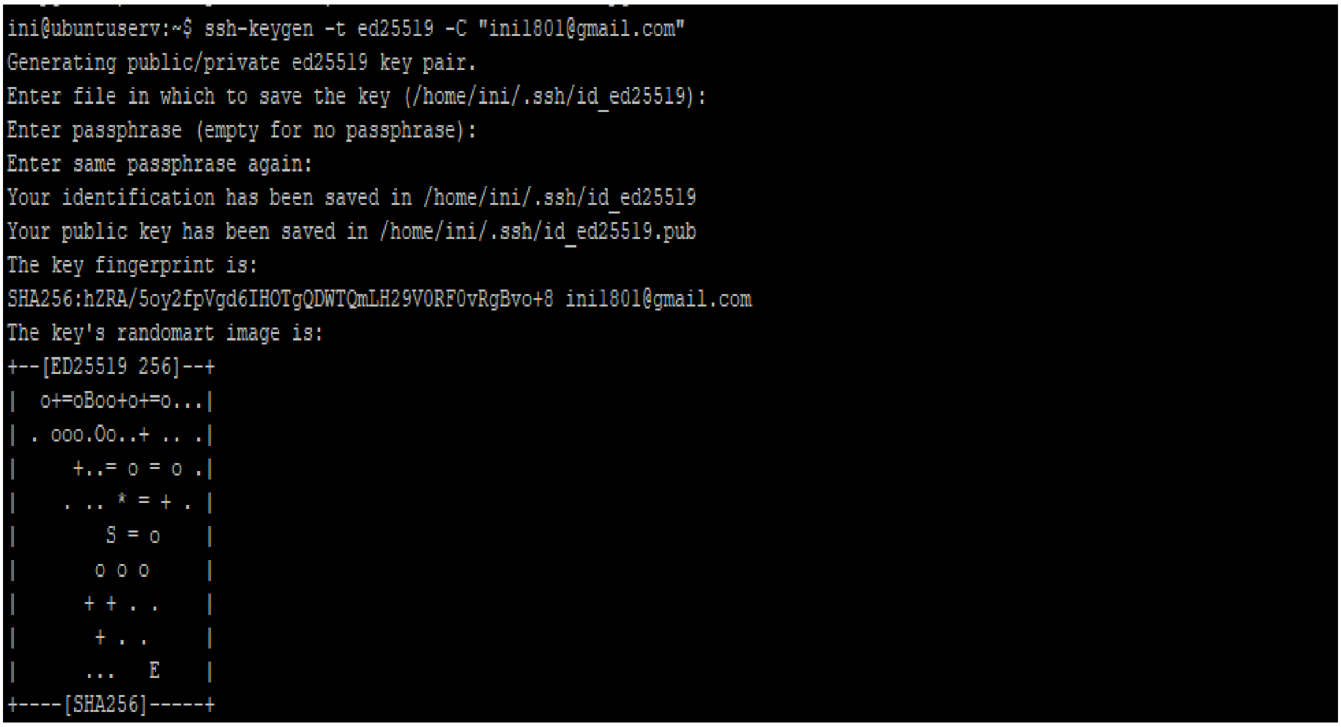
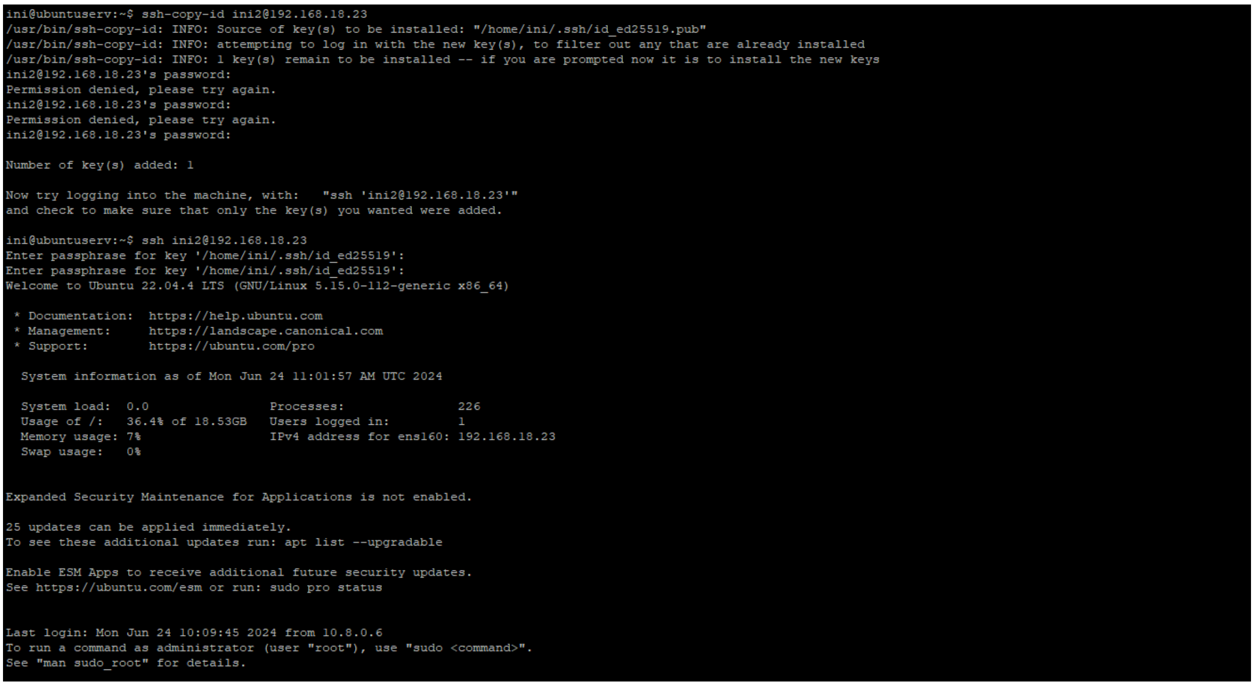
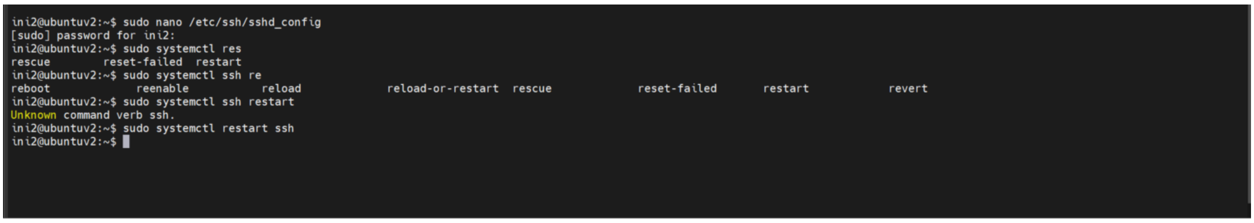
1. Создал 2 виртуальные машины на VMWare. Ubuntuserv 192.168.18.25 UbuntuV2 192.168.18.23
2. Создал на каждой разного пользователя.
3. 

```
ini@ubuntuserv:~$ ssh-keygen -t ed25519 -C "ini1801@gmail.com"
Generating public/private ed25519 key pair.
Enter file in which to save the key (/home/ini/.ssh/id_ed25519):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/ini/.ssh/id_ed25519
Your public key has been saved in /home/ini/.ssh/id_ed25519.pub
The key fingerprint is:
SHA256:hZRA/5oy2fpVgd6IHOTgQDWTQmLH29V0RF0vRgBvo+8 ini1801@gmail.com
The key's randomart image is:
+--[ED25519 256]--+
|  o+=oBoo+o+=o...|
| . ooo.Oo..+ .. .|
|     +..= o = o .|
|    . .. * = + . |
|        S = o    |
|       o o o     |
|      + + . .    |
|       + . .     |
|      ...   E    |
+----[SHA256]-----+
```

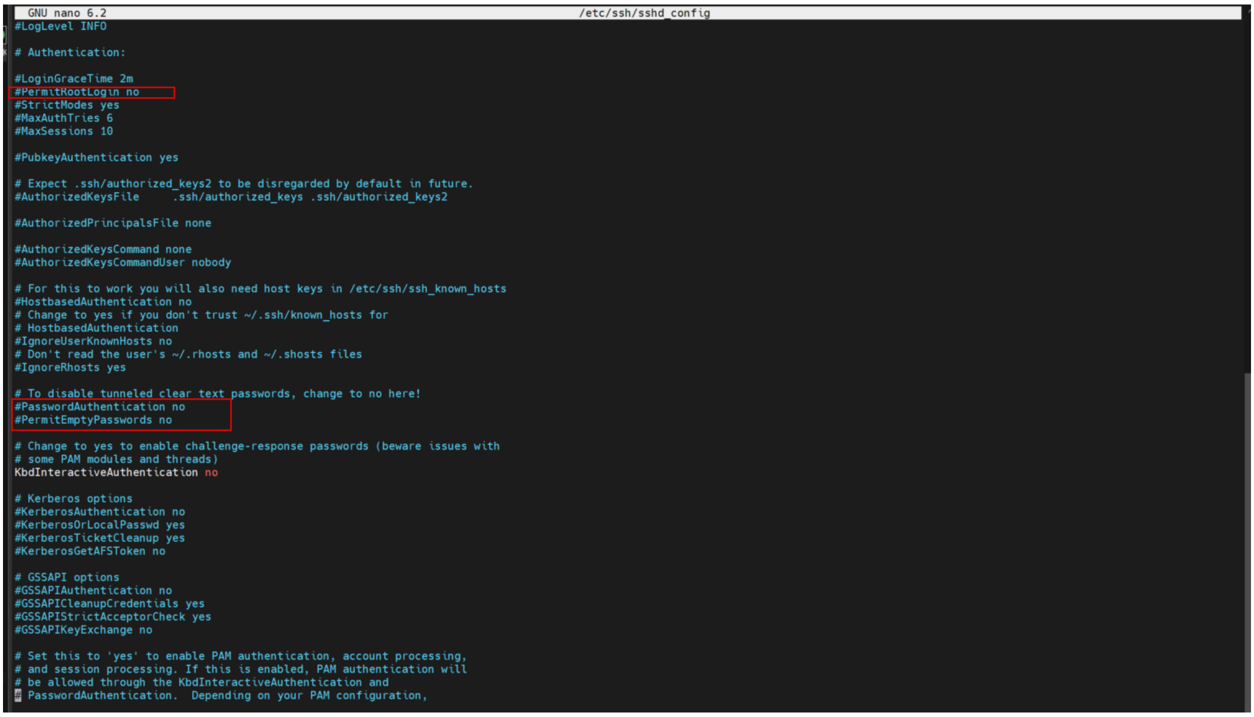
4. Подключаюсь с сервера1 на сервар2 по SSH по паролю пользователя с добавлением ключа.
5. 

```
ini@ubuntuserv:~$ ssh-copy-id ini2@192.168.18.23
/usr/bin/ssh-copy-id: INFO: Source of key(s) to be installed: "/home/ini/.ssh/id_ed25519.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 prompted now it is to install the new keys
ini2@192.168.18.23's password:
Permission denied, please try again.
ini2@192.168.18.23's password:
Permission denied, please try again.
ini2@192.168.18.23's password:

Number of key(s) added: 1

Now try logging into the machine, with:   "ssh 'ini2@192.168.18.23'"
and check to make sure that only the key(s) you wanted were added.

ini@ubuntuserv:~$ ssh ini2@192.168.18.23
Enter passphrase for key '/home/ini/.ssh/id_ed25519':
Enter passphrase for key '/home/ini/.ssh/id_ed25519':
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-112-generic x86_64)

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

  System information as of Mon Jun 24 11:01:57 AM UTC 2024

  System load:  0.0                Processes:               226
  Usage of /:   36.4% of 18.53GB   Users logged in:         1
  Memory usage: 7%                 IPv4 address for ens160: 192.168.18.23
  Swap usage:   0%


Expanded Security Maintenance for Applications is not enabled.

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

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


Last login: Mon Jun 24 10:09:45 2024 from 10.8.0.6
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
```

6. Подключаемся на второй сервер и редактируем файл sshd_config и запрещаем подключение по паролю. Сохраняем файл и делаем рестарт службы
7. 

```
ini2@ubuntuv2:~$ sudo nano /etc/ssh/sshd_config
[sudo] password for ini2:
ini2@ubuntuv2:~$ sudo systemctl res
rescue        reset-failed  restart
ini2@ubuntuv2:~$ sudo systemctl ssh re
reboot            reenable          reload            reload-or-restart  rescue            reset-failed      restart           revert
ini2@ubuntuv2:~$ sudo systemctl ssh restart
Unknown command verb ssh.
ini2@ubuntuv2:~$ sudo systemctl restart ssh
ini2@ubuntuv2:~$ █
```

8.

9. 

```
  GNU nano 6.2                                    /etc/ssh/sshd_config
#LogLevel INFO

# Authentication:

#LoginGraceTime 2m
#PermitRootLogin no
#StrictModes yes
#MaxAuthTries 6
#MaxSessions 10

#PubkeyAuthentication yes

# Expect .ssh/authorized_keys2 to be disregarded by default in future.
#AuthorizedKeysFile     .ssh/authorized_keys .ssh/authorized_keys2

#AuthorizedPrincipalsFile none

#AuthorizedKeysCommand none
#AuthorizedKeysCommandUser nobody

# For this to work you will also need host keys in /etc/ssh/ssh_known_hosts
#HostbasedAuthentication no
# Change to yes if you don't trust ~/.ssh/known_hosts for
# HostbasedAuthentication
#IgnoreUserKnownHosts no
# Don't read the user's ~/.rhosts and ~/.shosts files
#IgnoreRhosts yes

# To disable tunneled clear text passwords, change to no here!
#PasswordAuthentication no
#PermitEmptyPasswords no

# Change to yes to enable challenge-response passwords (beware issues with
# some PAM modules and threads)
KbdInteractiveAuthentication no

# Kerberos options
#KerberosAuthentication no
#KerberosOrLocalPasswd yes
#KerberosTicketCleanup yes
#KerberosGetAFSToken no

# GSSAPI options
#GSSAPIAuthentication no
#GSSAPICleanupCredentials yes
#GSSAPIStrictAcceptorCheck yes
#GSSAPIKeyExchange no

# Set this to 'yes' to enable PAM authentication, account processing,
# and session processing. If this is enabled, PAM authentication will
# be allowed through the KbdInteractiveAuthentication and
# PasswordAuthentication.  Depending on your PAM configuration,
```

10. Все. Подключение только по ключу.
11.