# SSH

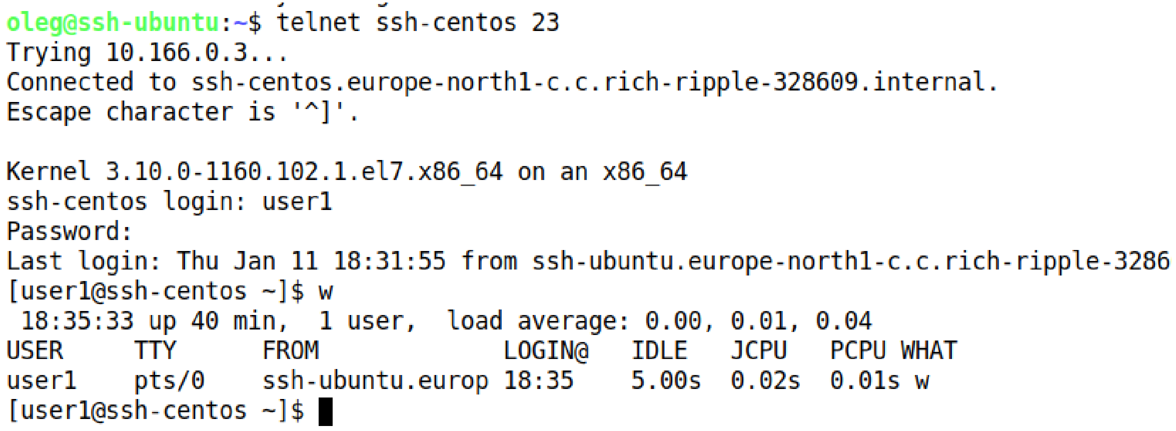
**S**ECURE

**SH**ELL

# Before SSH

```
yum install telnet-server

useradd user1
echo 'passwordforuser1' | passwd user1 --stdin

firewall-cmd --add-service=telnet --zone=public --permanent
setenforce permissive
systemctl enable telnet.socket
systemctl start telnet.socket
```

- telnet as remote console/shell
  - Insecure plaintext
  - Server spoofing



```
oleg@ssh-ubuntu:~$ telnet ssh-centos 23
Trying 10.166.0.3...
Connected to ssh-centos.europe-north1-c.c.rich-ripple-328609.internal.
Escape character is '^]'.

Kernel 3.10.0-1160.102.1.el7.x86_64 on an x86_64
ssh-centos login: user1
Password:
Last login: Thu Jan 11 18:31:55 from ssh-ubuntu.europe-north1-c.c.rich-ripple-3286
[user1@ssh-centos ~]$ w
 18:35:33 up 40 min,  1 user,  load average: 0.00, 0.01, 0.04
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
user1    pts/0    ssh-ubuntu.europ 18:35    5.00s  0.02s  0.01s w
[user1@ssh-centos ~]$ 
```

# ssh

- шифрований канал на між tcp-з'єданням на трафіком всередині.
- аутентифікація не тількі на рівні того що надає система входу термінал:
  - логін + пароль
  - файлові ключі
  - gssapi (kerberos – SSO)
  - hostbased
- налаштування, обмеження на рівні логіна, або ключа який використовує клієнт
- клієнт може запам'ятати fingerprint сервера, та має реакцію на його зміну

# ssh configuration

- конфігуація сервера:

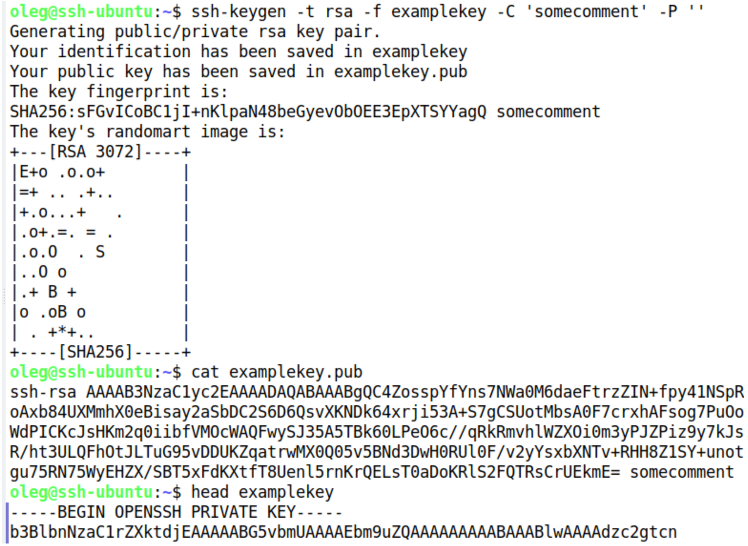
```
/etc/ssh/sshd_config
/etc/ssh/ssh_host_*_key
```

- конфігуація клієнта:

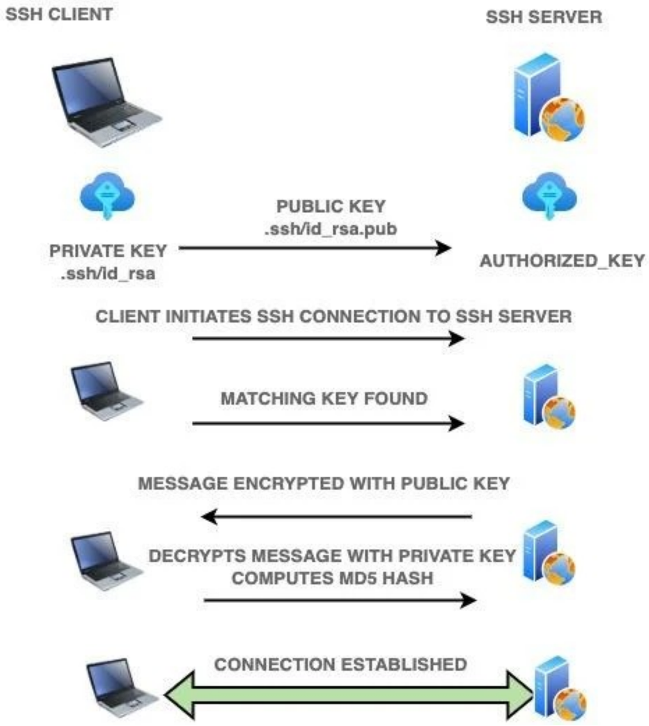
```
/etc/ssh/ssh_config

~/.ssh/config
```

# Key based auth

```
ssh-keygen -t type -b bits
-f filename -C comment
-P passphrase
```



```
oleg@ssh-ubuntu:~$ ssh-keygen -t rsa -f examplekey -C 'somecomment' -P ''
Generating public/private rsa key pair.
Your identification has been saved in examplekey
Your public key has been saved in examplekey.pub
The key fingerprint is:
SHA256:sFGvICoBC1jI+nKlpaN48beGyevObOEE3EpXTSYYagQ somecomment
The key's randomart image is:
+---[RSA 3072]----+
|E+o .o.o+        |
|=+ .. .+..       |
|+.o...+   .      |
|.o+.=. = .       |
|.o.O  . S        |
|..O o            |
|.+ B +           |
|o .oB o          |
| . +*+..         |
+----[SHA256]-----+
oleg@ssh-ubuntu:~$ cat examplekey.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQC4ZosspYfYns7NWa0M6daeFtrzZIN+fpy41NSpR
oAxb84UXMmhX0eBisay2aSbDC2S6D6QsvXKNDk64xrji53A+S7gCSUotMbsA0F7crxhAFsog7PuOo
WdPICKcJsHKm2q0iibfVMOcWAQFwySJ35A5TBk60LPeO6c//qRkRmvhlWZXOi0m3yPJZPiz9y7kJs
R/ht3ULQFhOtJLTuG95vDDUKZqatrwMX0Q05v5BNd3DwH0RUl0F/v2yYsxbXNTv+RHH8Z1SY+unot
gu75RN75WyEHZX/SBT5xFdKXtfT8Uenl5rnKrQELsT0aDoKRlS2FQTRsCrUEkmE= somecomment
oleg@ssh-ubuntu:~$ head examplekey
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
```



SSH CLIENT

SSH SERVER

PUBLIC KEY
.ssh/id_rsa.pub

PRIVATE KEY
.ssh/id_rsa

AUTHORIZED_KEY

CLIENT INITIATES SSH CONNECTION TO SSH SERVER

MATCHING KEY FOUND

MESSAGE ENCRYPTED WITH PUBLIC KEY

DECRYPTS MESSAGE WITH PRIVATE KEY
COMPUTES MD5 HASH

CONNECTION ESTABLISHED

# Key based auth

```
client: ssh-copy-id -i filename username@remote_host

username@server: ~/.ssh/authorized_keys
```

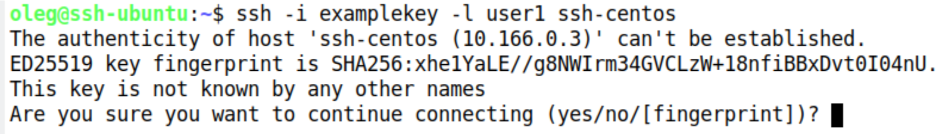
Аутентифікація:

```
client: ssh -i path/to/privatekey username@remote_host
```

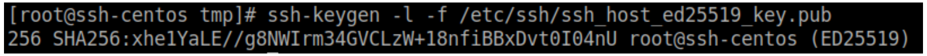
# Ssh fingerprint

- `ssh-kegen -l -f file`
- `~/.ssh/known_host`

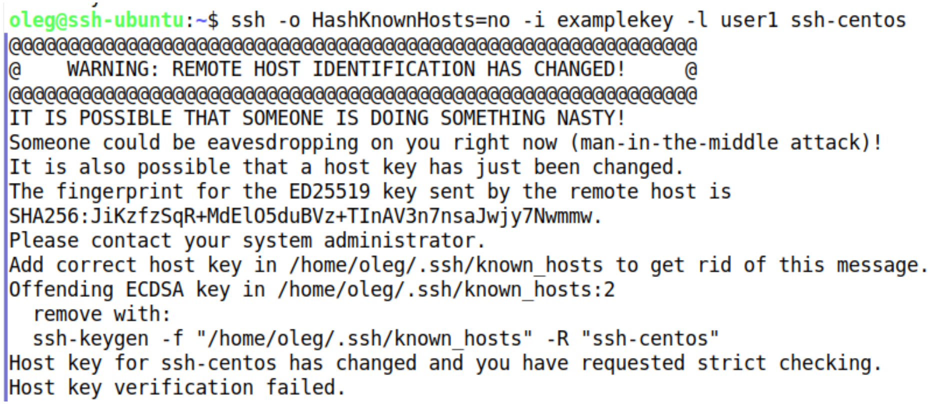
-
  ```
  -o StrictHostKeyChecking=no
  -o StrictHostKeyChecking=accept-new
  -o UserKnownHostsFile=known_hosts

  -o StrictHostKeyChecking=no
  -o UserKnownHostsFile=/dev/null
  ```



```
oleg@ssh-ubuntu:~$ ssh -i examplekey -l user1 ssh-centos
The authenticity of host 'ssh-centos (10.166.0.3)' can't be established.
ED25519 key fingerprint is SHA256:xhe1YaLE//g8NWIrm34GVCLzW+18nfiBBxDvt0I04nU.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? █
```



```
[root@ssh-centos tmp]# ssh-keygen -l -f /etc/ssh/ssh_host_ed25519_key.pub
256 SHA256:xhe1YaLE//g8NWIrm34GVCLzW+18nfiBBxDvt0I04nU root@ssh-centos (ED25519)
```



```
oleg@ssh-ubuntu:~$ ssh -o HashKnownHosts=no -i examplekey -l user1 ssh-centos
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the ED25519 key sent by the remote host is
SHA256:JiKzfzSqR+MdElO5duBVz+TInAV3n7nsaJwjy7Nwmmw.
Please contact your system administrator.
Add correct host key in /home/oleg/.ssh/known_hosts to get rid of this message.
Offending ECDSA key in /home/oleg/.ssh/known_hosts:2
  remove with:
  ssh-keygen -f "/home/oleg/.ssh/known_hosts" -R "ssh-centos"
Host key for ssh-centos has changed and you have requested strict checking.
Host key verification failed.
```

# ~/.ssh/config

```
~/.ssh/config
GSSAPIAuthentication no
IdentityFile ~/.ssh/default_key

Host hostalias
  HostName realhost_ip
  User user1
  Port     2222
  IdentityFile ~/.ssh/custom_key
  UserKnownHostsFile=/dev/null
  StrictHostKeyChecking=no

$ ssh hostalias
```

- Configuration data is parsed as follows:
  1) command line options
  2) user-specific file
     ssh -F ~/.ssh/ssh_config
  3) system-wide file
     /etc/ssh/ssh_config

- man 5 ssh_config

# Verbose logging

- ssh -v

```
debug1: Reading configuration data
/home/oleg/.ssh/config
debug1: /home/oleg/.ssh/config line 5: Applying
options for 10.166.*
debug1: Authenticating to 10.166.0.3:22 as 'ec2'
debug1: Trying private key:
/home/oleg/.ssh/default_key
debug1: Authentications that can continue:
publickey,gssapi-keyex,gssapi-with-mic,password
```

- `ssh -vv -vvv`

- /etc/ssh/sshd_config:
  LogLevel INFO
  INFO, VERBOSE, DEBUG
- /var/log/secure (rhel-based)
- /var/log/auth.log (debian-based)

# scp

- scp – ssh copy

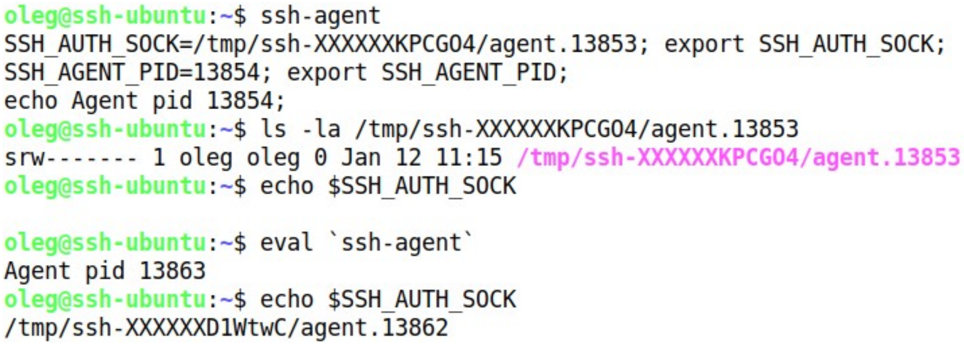
```
scp localfile remote:file

scp remote:file localfile

scp -p -r ...
-p permission
-r recursive
```

- rsync over ssh

```
rsync [OPTS] [USER@]HOST:SRC [DEST]

rsync [OPTS] SRC [USER@]HOST:DEST

-a - archive mode (-rlptgoD)
recursive, symlinks,
permission, timestamps etc

-z - compression

-v – verbose

-n – dry run
```

# ssh-agent

- `eval $(ssh-agent)`
  `eval `ssh-agent``
- `ssh-add key # add key`
- `ssh-add -l # list`



```
oleg@ssh-ubuntu:~$ ssh-agent
SSH_AUTH_SOCK=/tmp/ssh-XXXXXXKPCGO4/agent.13853; export SSH_AUTH_SOCK;
SSH_AGENT_PID=13854; export SSH_AGENT_PID;
echo Agent pid 13854;
oleg@ssh-ubuntu:~$ ls -la /tmp/ssh-XXXXXXKPCGO4/agent.13853
srw------- 1 oleg oleg 0 Jan 12 11:15 /tmp/ssh-XXXXXXKPCGO4/agent.13853
oleg@ssh-ubuntu:~$ echo $SSH_AUTH_SOCK

oleg@ssh-ubuntu:~$ eval `ssh-agent`
Agent pid 13863
oleg@ssh-ubuntu:~$ echo $SSH_AUTH_SOCK
/tmp/ssh-XXXXXXD1WtwC/agent.13862
```