

Start two parallel SSH servers

1. Створюємо користувача john із домашньою папкою за типовим шляхом.

```
dmytro@ubuntu22:~$ sudo useradd -m -d /home/john -s /bin/bash john
dmytro@ubuntu22:~$
```

2. Встановіть і налаштуйте SSH-сервер, який прослуховує порт 2222, обмежуючи кореневий доступ і забороняючи авторизації
- Встановлюємо та налаштовуємо SSH сервер

```
dmytro@ubuntu22:~$ sudo apt-get update
```

```
dmytro@ubuntu22:~$ sudo apt-get install openssh-server
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
openssh-server is already the newest version (1:8.9p1-3ubuntu0.10).
0 upgraded, 0 newly installed, 0 to remove and 11 not upgraded.
dmytro@ubuntu22:~$
```

- Відредагуємо конфігураційний файл **etc/ssh/sshd_config**
Змінимо у файлі наступні параметри

- Port 2222
- AllowUsers john
- PermitRootLogin no
- PasswordAuthentication no

```
include /etc/ssh/sshd_config.d/*.conf

Port 2222
#AddressFamily any
#ListenAddress 0.0.0.0
#ListenAddress ::
AllowUsers john

#HostKey /etc/ssh/ssh_host_rsa_key
#HostKey /etc/ssh/ssh_host_ecdsa_key
#HostKey /etc/ssh/ssh_host_ed25519_key

# Ciphers and keying
#RekeyLimit default none

# Logging
#SyslogFacility AUTH
#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
```

Генеруємо SSH ключі для користувача "john"

```
john@ubuntu22:~$ sudo -u john ssh-keygen -t rsa -b 4096
Generating public/private rsa key pair.
Enter file in which to save the key (/home/john/.ssh/id_rsa):
Created directory '/home/john/.ssh'.
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /home/john/.ssh/id_rsa
Your public key has been saved in /home/john/.ssh/id_rsa.pub
The key fingerprint is:
SHA256:RNk/Nzewz6Z826oLcG/nfLxbZF2rpS/P+y4xnKqdfU john@ubuntu22
The key's randomart image is:
[-----[RSA 4096]-----+
    ..
    .  .
    .   .
    .    E .
    .   .
    .  .oo..=
    .   .oo==
    .    o o  +*
    .   .o.+++..
    .    .o=B+o=
    .   .++B%X
    .
+-----[SHA256]-----+
john@ubuntu22:~$
```

Створюємо директорію «.ssh» для користувача john. Після чого додаємо публічний ключ до файлу “authorized keys”

```
john@ubuntu22:~$ sudo -u john mkdir -p /home/john/.ssh
john@ubuntu22:~$ sudo -u john cat /home/john/.ssh/id_rsa.pub > /home/john/.ssh/authorized_keys
```

Налаштовуємо права доступу до файлу "authorized_keys"

```
john@ubuntu22:~$ sudo -u john chmod 600 /home/john/.ssh/authorized_keys
john@ubuntu22:~$
```

Перезапускаємо SSH сервер

```
john@ubuntu22:~$ sudo systemctl restart ssh
[sudo] password for john:
john@ubuntu22:~$
```

Налаштування SSH у режимі налагодження для порту 3333

Створимо додатковий конфігураційний файл для налагодження

```
john@ubuntu22:~$ sudo vi /etc/ssh/sshd_config_debug
john@ubuntu22:~$
```

Внесемо у файл деякі дані:

Port 3333 – ssh сервер буде слухати з'єднання на порту 3333

PermitRootLogin no – Забороняє вхід користувачу root

PasswordAuthentication yes – Дозволяє аутентифікацію за паролем

AllowUsers * - дозволяє всім користувачам підключатися через SSH

```
Port 3333
PermitRootLogin no
PasswordAuthentication yes
AllowUsers *
```

Запустимо SSH у режимі налагодження (`sudo /usr/sbin/sshd -f /etc/ssh/sshd_config debug -d`)

```
john@ubuntu22:~$ sudo /usr/sbin/sshd -f /etc/ssh/sshd_config_debug -d
debug1: sshd version OpenSSH 8.9, OpenSSL 3.0.2 15 Mar 2022
debug1: private host key #0: ssh-rsa SHA256:KcUg2dLP0PY/tpYoQJSnLBhZY9ToeyLFhNnb0vGoU
debug1: private host key #1: ecdsa-sha2-nistp256 SHA256:X+mRY6Jx8qpv3RBBi5PcdyDgP3EAo03//sp/s1iYi0
debug1: private host key #2: ssh-ed25519 SHA256:g+LzcPqyqeUNPcdxK0edHlJvseI3v7rM93T31VfzOI
debug1: rexec_argv[0]='/usr/sbin/sshd'
debug1: rexec_argv[1]='-f'
debug1: rexec_argv[2]='/etc/ssh/sshd_config_debug'
debug1: rexec_argv[3]='-d'
debug1: Set /proc/self/oom_score_adj from 0 to -1000
debug1: Bind to port 3333 on 0.0.0.0.
Server listening on 0.0.0.0 port 3333.
debug1: Bind to port 3333 on ::.
Server listening on :: port 3333.
```

Підключення до серверів та перевірка статусу

Підключення до серверу на порту 2222

```
john@ubuntu22:~$ ssh -p 2222 john@192.168.112.128
The authenticity of host '[192.168.112.128]:2222 ([192.168.112.128]:2222)' can't be established.
ED25519 key fingerprint is SHA256:g+LzcPqyjeUNPcdxKmOedHJlvseI3v7rm93T31Vfz0I.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.112.128]:2222' (ED25519) to the list of known hosts.
Enter passphrase for key '/home/john/.ssh/id_rsa':
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-113-generic x86_64)

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

System information as of Thu Jul  4 01:00:40 PM UTC 2024

System load:  0.41          Processes:           260
Usage of /:   45.9% of 18.53GB Users logged in:    1
Memory usage: 13%          IPv4 address for ens33: 192.168.112.128
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

9 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

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.

john@ubuntu22:~$
```

Підключення до серверу на порту 3333

```
john@ubuntu22:~$ ssh -p 3333 john@192.168.112.128
The authenticity of host '[192.168.112.128]:3333 ([192.168.112.128]:3333)' can't be established.
ED25519 key fingerprint is SHA256:g+LzcPqyjeUNPcdxKmOedHJlvseI3v7rm93T31Vfz0I.
This host key is known by the following other names/addresses:
  ~/.ssh/known_hosts:1: [hashed name]
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.112.128]:3333' (ED25519) to the list of known hosts.
Enter passphrase for key '/home/john/.ssh/id_rsa':
Welcome to Ubuntu 22.04.4 LTS (GNU/Linux 5.15.0-113-generic x86_64)

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

System information as of Thu Jul  4 01:24:36 PM UTC 2024

System load:  0.17          Processes:           264
Usage of /:   45.9% of 18.53GB Users logged in:    2
Memory usage: 14%          IPv4 address for ens33: 192.168.112.128
Swap usage:   0%

Expanded Security Maintenance for Applications is not enabled.

9 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: Thu Jul  4 13:24:37 2024 from 192.168.112.128
john@ubuntu22:~$
```

Перевірка статусу SSH-сервера

```
john@ubuntu22:~$ sudo systemctl status ssh
[sudo] password for john:
● ssh.service - OpenBSD Secure Shell server
   Loaded: loaded (/lib/systemd/system/ssh.service; enabled; vendor preset: enabled)
   Active: active (running) since Thu 2024-07-04 13:23:22 UTC; 5min ago
     Docs: man:sshd(8)
           man:sshd_config(5)
   Process: 10070 ExecStartPre=/usr/sbin/sshd -t (code=exited, status=0/SUCCESS)
   Main PID: 10071 (sshd)
     Tasks: 1 (limit: 4514)
    Memory: 6.2M
       CPU: 224ms
   CGroup: /system.slice/ssh.service
           └─10071 "sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups"

Jul 04 13:23:22 ubuntu22 systemd[1]: Starting OpenBSD Secure Shell server...
Jul 04 13:23:22 ubuntu22 sshd[10071]: Server listening on 0.0.0.0 port 3333.
Jul 04 13:23:22 ubuntu22 sshd[10071]: Server listening on :: port 3333.
Jul 04 13:23:22 ubuntu22 systemd[1]: Started OpenBSD Secure Shell server.
Jul 04 13:23:22 ubuntu22 sshd[10071]: Server listening on 0.0.0.0 port 2222.
Jul 04 13:23:22 ubuntu22 sshd[10071]: Server listening on :: port 2222.
Jul 04 13:24:36 ubuntu22 sshd[10077]: Accepted publickey for john from 192.168.112.128 port 47676 ssh2: RSA SHA256:RNk/Nzewz6Z826oLcG/nfLxbZF2rpS/P+yy4xnKqdfU
Jul 04 13:24:36 ubuntu22 sshd[10077]: pam_unix(sshd:session): session opened for user john(uid=1007) by (uid=0)
Jul 04 13:25:06 ubuntu22 sshd[10045]: Accepted publickey for john from 192.168.112.128 port 46694 ssh2: RSA SHA256:RNk/Nzewz6Z826oLcG/nfLxbZF2rpS/P+yy4xnKqdfU
Jul 04 13:25:06 ubuntu22 sshd[10045]: pam_unix(sshd:session): session opened for user john(uid=1007) by (uid=0)
```

Перевіримо процес у режимі налагодження

```
john@ubuntu22:~$ ps aux | grep sshd
root      9422  0.0  0.2 17180 10956 ?        Ss   10:22   0:00 sshd: dmytro [priv]
dmytro    9502  0.0  0.2 17472  8532 ?        S    10:22   0:02 sshd: dmytro@pts/2
root     10310  0.0  0.2 17184 10904 ?        Ss   11:58   0:00 sshd: dmytro [priv]
root     10313  0.0  0.2 17180 11020 ?        Ss   11:58   0:00 sshd: dmytro [priv]
dmytro   10442  0.0  0.2 17472  8436 ?        S    11:58   0:02 sshd: dmytro@pts/6
dmytro   10470  0.0  0.2 17312  7960 ?        S    11:58   0:00 sshd: dmytro@notty
root     10607  0.0  0.2 16920 11112 ?        Ss   12:59   0:00 sshd: john [priv]
john     10713  0.0  0.2 17224  8104 ?        S    13:00   0:00 sshd: john@pts/0
root     10782  0.0  0.2 16920 10808 ?        Ss   13:16   0:00 sshd: john [priv]
john     10839  0.0  0.2 17220  8076 ?        R    13:16   0:00 sshd: john@pts/1
root     10871  0.0  0.2 15432  9464 ?        Ss   13:23   0:00 sshd: /usr/sbin/sshd -D [listener] 0 of 10-100 startups
root     10877  0.0  0.2 17048 10884 ?        Ss   13:24   0:00 sshd: john [priv]
john     10934  0.0  0.2 17192  7992 ?        S    13:24   0:00 sshd: john@pts/8
root     10945  0.0  0.2 17048 10752 ?        Ss   13:24   0:00 sshd: john [priv]
john     10992  0.0  0.2 17192  7980 ?        S    13:25   0:00 sshd: john@pts/9
john     11013  0.0  0.0   612   224 pts/9    S+   13:31   0:00 grep --color=auto sshd
john@ubuntu22:~$
```