

# Hướng dẫn tổng hợp cài đặt SSH Server trên Kali Linux

Tài liệu này tổng hợp **mọi mô hình** (password / key-based / root / custom paths / scp / ssh-copy-id / fail2ban / ufw / đổi port / troubleshooting) và hướng dẫn **chi tiết từng bước** để bạn có thể copy — dán chạy ngay. Kèm emoji và sơ đồ nhỏ để dễ hình dung.

## Mục lục

1. Giới thiệu nhanh 📌
2. Các mô hình (use-cases) 🛠️
3. Cài đặt OpenSSH Server cơ bản 🛠️
4. Cấu hình an toàn cơ bản (sshd\_config) 🔒
5. Thiết lập **SSH key-based authentication** (chi tiết) 🔑
6. Tạo key trên client
7. Copy key: `ssh-copy-id`, `scp`, thủ công
8. Quyền file & thư mục
9. Sao lưu & thay đổi `AuthorizedKeysFile` 📁
10. Đổi port / chặn root / giới hạn user 🛡️
11. Firewall (ufw) và fail2ban 🕒
12. Kiểm tra & debug (logs, sshd -T, journalctl) 📖
13. Các lệnh `scp` thường dùng (2 chiều) 📁
14. Sơ đồ minh họa (ASCII + mô tả) 📖
15. Checklist nhanh trước khi tắt password auth 🔗
16. FAQ & lỗi thường gặp 📝
17. Tóm tắt và tài nguyên nhanh 📚

## 1) Giới thiệu nhanh 📌

- **SSH (OpenSSH)** là giao thức an toàn để đăng nhập shell và copy file. Kali Linux thường đã có OpenSSH client, nhưng server (`openssh-server`) có thể chưa cài.
- Bài này giả định bạn có quyền `sudo` trên máy Kali (hoặc root).

## 2) Các mô hình (use-cases) 🛠️

- **Mô hình A — Password-based (mặc định, tạm dùng để test):** dễ thiết lập nhưng kém an toàn.
- **Mô hình B — Key-based (khuyến nghị):** đăng nhập bằng public/private key → an toàn hơn.
- **Mô hình C — Root login disabled:** dùng user thường + sudo.
- **Mô hình D — Port non-standard + fail2ban + ufw:** giảm lượng scan tự động.
- **Mô hình E — Custom AuthorizedKeysFile:** khi admin muốn đặt file ở vị trí khác.

## 3) Cài OpenSSH Server cơ bản 🛠️

```
sudo apt update
sudo apt install -y openssh-server

# bật service và kích hoạt khi boot
sudo systemctl enable --now ssh

# kiểm tra trạng thái
sudo systemctl status ssh
```

Nếu `active (running)` → server đang hoạt động.

---

## 4) Cấu hình an toàn cơ bản ( `/etc/ssh/sshd_config` )

Mở file:

```
sudo nano /etc/ssh/sshd_config
```

Các tham số nên chỉnh (bỏ `#` nếu bị comment):

```
Port 22                # đổi nếu muốn (ví dụ 2222)
PermitRootLogin no      # KHÔNG bật root trực tiếp
PubkeyAuthentication yes # cho rõ (mặc định thường là yes)
AuthorizedKeysFile .ssh/authorized_keys
PasswordAuthentication yes # tạm bật để test, sau khóa lại
PermitEmptyPasswords no
ClientAliveInterval 300
ClientAliveCountMax 2
AllowUsers youruser anotheruser # giới hạn user (tùy chọn)
```

Sau khi sửa: `sudo systemctl restart ssh`.

**Lưu ý:** nhiều bản hệ thống có dòng `Include /etc/ssh/sshd_config.d/*.conf` — cấu hình có thể phân mảnh ở đó.

---

## 5) Thiết lập SSH key-based authentication (chi tiết)

### 5.1 Tạo key trên client

Trên máy client (Linux/macOS/WSL):

```
ssh-keygen -t ed25519 -C "your_email@example.com"
# hoặc
ssh-keygen -t rsa -b 4096 -C "your_email@example.com"
```

Nhấn Enter để dùng đường dẫn mặc định ( `~/.ssh/id_ed25519` ). Nếu muốn passphrase thì nhập, không thì Enter để bỏ.

## 5.2 Copy key sang server

**Cách A — Dùng `ssh-copy-id` (nhANH & tự động)**

```
ssh-copy-id user@server_ip
# nếu port khác
ssh-copy-id -p 2222 user@server_ip
```

**Cách B — Dùng `scp`**

```
scp ~/.ssh/id_ed25519.pub user@server_ip:/home/user/
# trên server:
ssh user@server_ip
mkdir -p ~/.ssh
cat ~/id_ed25519.pub >> ~/.ssh/authorized_keys
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
rm ~/id_ed25519.pub
```

**Cách C — Thủ công (copy/paste)** Trên client: `cat ~/.ssh/id_ed25519.pub` → copy dòng Trên server: `mkdir -p ~/.ssh && nano ~/.ssh/authorized_keys` → dán → lưu Rồi `chmod 700 ~/.ssh && chmod 600 ~/.ssh/authorized_keys`.

## 5.3 Quyền file & folder (chính xác!)

Trên server (user tương ứng):

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
chown -R $(whoami):$(whoami) ~/.ssh
```

**Sai quyền** là nguyên nhân phổ biến nhất khiến publickey không hoạt động.

## 5.4 Test

Trên client:

```
ssh user@server_ip
```

Nếu vào được mà **không hỏi mật khẩu** → thành công. Nếu vẫn yêu cầu mật khẩu thì kiểm tra logs.

## 6) AuthorizedKeysFile không có trong config thì sao

- Nếu `/etc/ssh/sshd_config` không có dòng `AuthorizedKeysFile`, OpenSSH dùng mặc định: `.ssh/authorized_keys .ssh/authorized_keys2`.
- Kiểm tra cấu hình daemon hiện tại:

```
sudo sshd -T | grep authorizedkeysfile
```

- Nếu bạn muốn chắc chắn, có thể **thêm**: `AuthorizedKeysFile .ssh/authorized_keys` vào `sshd_config` rồi restart.

## 7) Đổi port / chặn root / giới hạn user

- Thay Port 22 bằng Port 2222 trong `sshd_config` → restart.
- Chặn root: `PermitRootLogin no`.
- Giới hạn user: `AllowUsers user1 user2`.

**Lưu ý quan trọng:** nếu đổi port mà quên cấu hình firewall, bạn có thể bị khóa ngoài. Luôn test 1 terminal session trước khi đóng session hiện tại.

## 8) Firewall (ufw) và fail2ban

**ufw:**

```
sudo apt install -y ufw
sudo ufw allow 22/tcp          # hoặc sudo ufw allow 2222/tcp
sudo ufw enable
sudo ufw status
```

**fail2ban:** chặn brute-force tự động

```
sudo apt install -y fail2ban
# tạo /etc/fail2ban/jail.local
# ví dụ simple:
# [sshd]
# enabled = true
# port = ssh
# maxretry = 5
```

Khởi động: `sudo systemctl enable --now fail2ban`.

## 9) Kiểm tra & debug (logs, sshd -T, journalctl) 📖

Xem cấu hình đang dùng:

```
sudo sshd -T  
sudo sshd -T | grep pubkeyauthentication  
sudo sshd -T | grep authorizedkeysfile
```

Xem log thời gian thực:

```
sudo journalctl -u ssh -f  
# hoặc  
sudo tail -f /var/log/auth.log
```

Một vài lỗi phổ biến trong log: - `Permission denied (publickey)` → lỗi key/permission -  
`Authentication refused: bad ownership or modes` → quyền file/folder sai

## 10) Các lệnh scp thường dùng (2 chiều) 📁

Client → Server:

```
scp -P 2222 ~/file.txt user@server_ip:/home/user/
```

Server → Client:

```
scp -P 2222 user@server_ip:/etc/ssh/sshd_config ~/Downloads/
```

Copy thư mục:



```
scp -r ~/project user@server_ip:/home/user/
```

Dùng key cụ thể:

```
scp -i ~/.ssh/id_rsa ~/file.txt user@server_ip:/home/user/
```






## 11) Sơ đồ minh họa (ASCII) 📖

```
[Client] --(SSH over TCP port 22/2222)---> [Kali Server]  
      |                                   |  
      |-- scp / ssh-copy-id ---> .ssh/authorized_keys
```

Gợi ý hình ảnh: -  = public/private key pair -  = cấu hình trong `/etc/ssh/sshd_config`

---

## 12) Checklist nhanh trước khi tắt PasswordAuthentication

1. Bạn đã **vào được** server bằng key (từ client) không? 
  2. `~/.ssh` có quyền `700` và `authorized_keys` có `600`? 
  3. `sshd -T` cho thấy `pubkeyauthentication yes`? 
  4. Bạn có 1 session SSH mở (để rollback) trước khi tắt password? 
  5. Firewall đã mở port bạn dùng? 
- 

## 13) FAQ & lỗi thường gặp

- **Vẫn bị** `Permission denied (publickey)` → check quyền `~/.ssh` & `authorized_keys`, check owner, kiểm tra `sshd -T`.
  - **Không thấy** `PubkeyAuthentication` **trong config** → mặc định là yes; kiểm tra `sshd -T`.
  - **AuthorizedKeysFile không tồn tại** → OpenSSH dùng mặc định `.ssh/authorized_keys`.
  - **Bị khoá khi đổi port** → có thể firewall chưa mở port mới.
- 

## 14) Tóm tắt & tài nguyên nhanh

- Bước nhanh: `apt install openssh-server` → cấu hình `~/.ssh/authorized_keys` → `chmod` quyền → test → tắt password.
  - Các lệnh debugging: `sshd -T`, `journalctl -u ssh -f`, `tail -f /var/log/auth.log`.
- 

**Muốn mình xuất file PDF/Doc/Markdown để bạn up lên Git hoặc in không?** Mình có thể xuất sẵn định dạng Markdown (có sẵn code blocks) hoặc tạo PDF đẹp (có hình minh hoạ) — nói loại file bạn muốn mình sẽ tạo ngay.