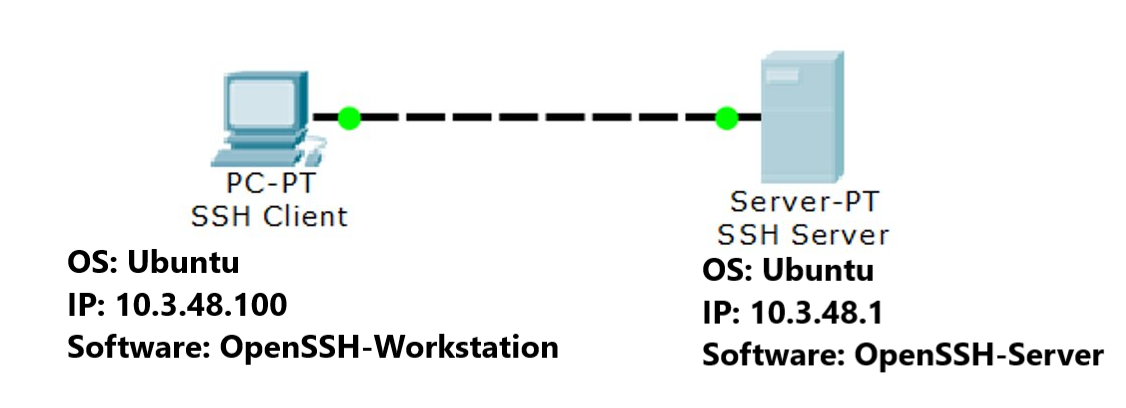
1. **Tự chấm điểm**
2. **Mô hình triển khai**
3. **Cấu hình Client**
4. **Cấu hình Server**
5. **Cấu hình dùng mật mã khóa công khai**

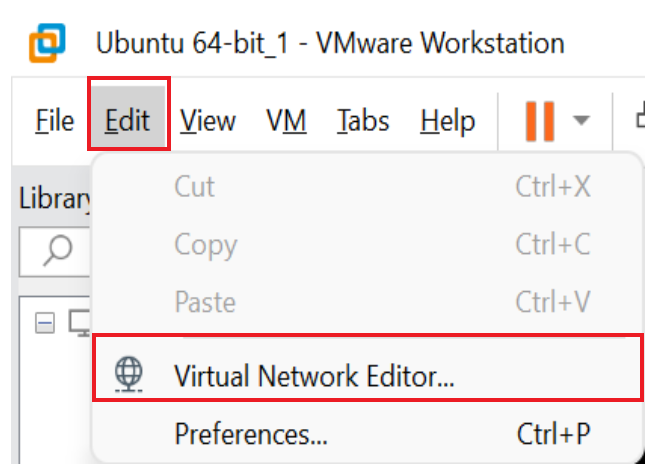
**I.Tự chấm điểm**

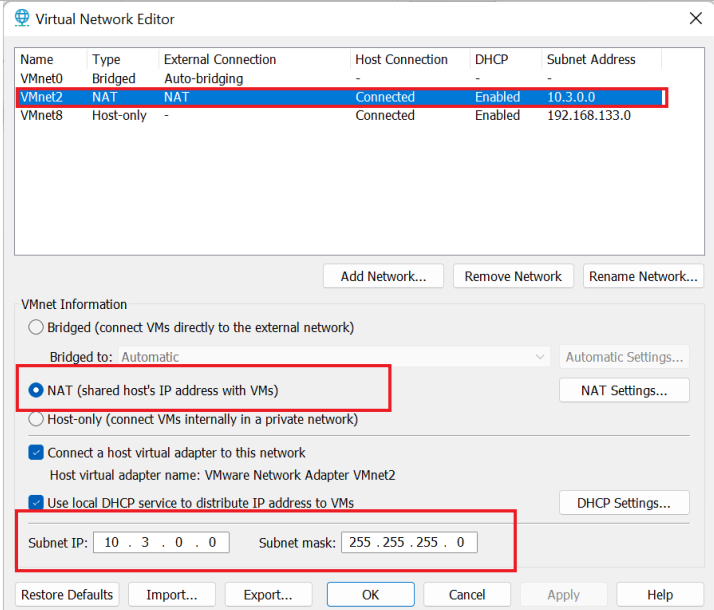
|  |  |  |
| --- | --- | --- |
| Yêu cầu | Điểm tối đa | Ghi chú |
| Triển khai được hệ thống SSH xác thực bằng mật khẩu | 2,0 | Bắt buộc |
| Sinh cặp khóa cho máy chủ SSH từ bên ngoài | +1,0 |  |
| Triển khai xác thực người dùng bằng mật mã khóa công khai | +1,0 |  |
| Tổng điểm | 4,0 |  |

**II. Mô hình triển khai**

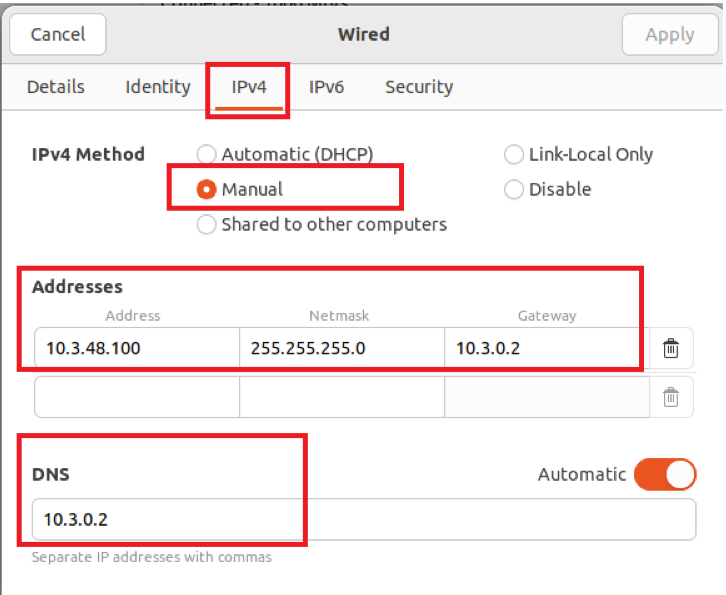
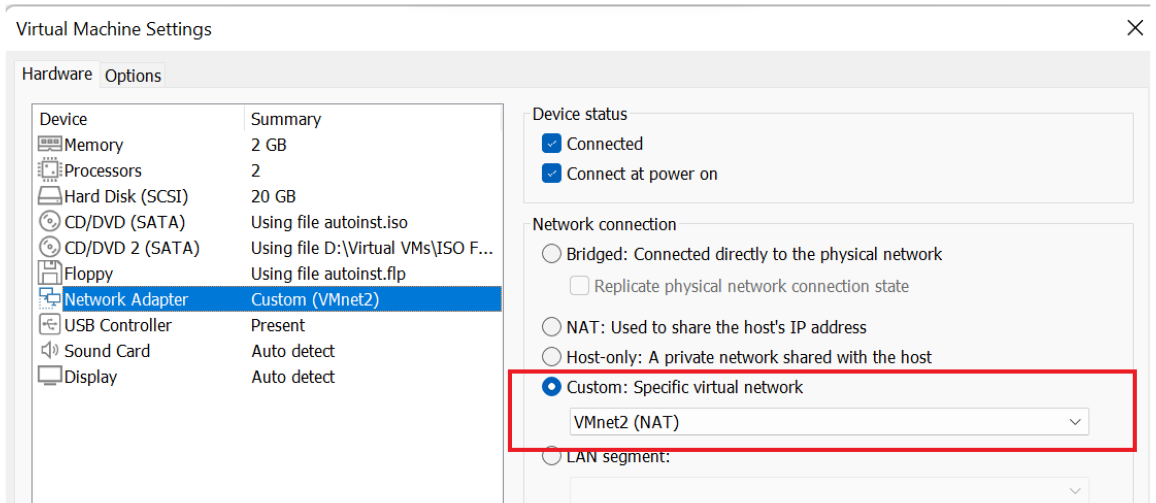
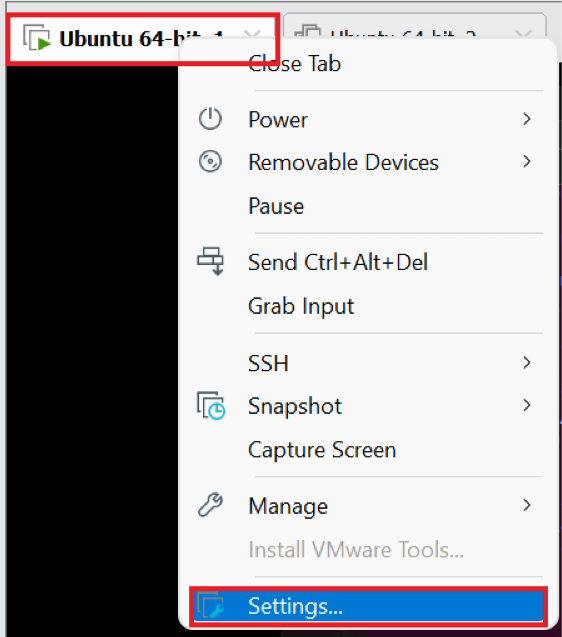


**III.Cấu hình VMWARE**



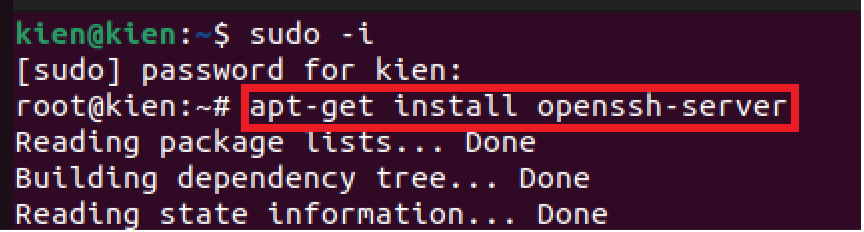


**III.Cấu hình Client**



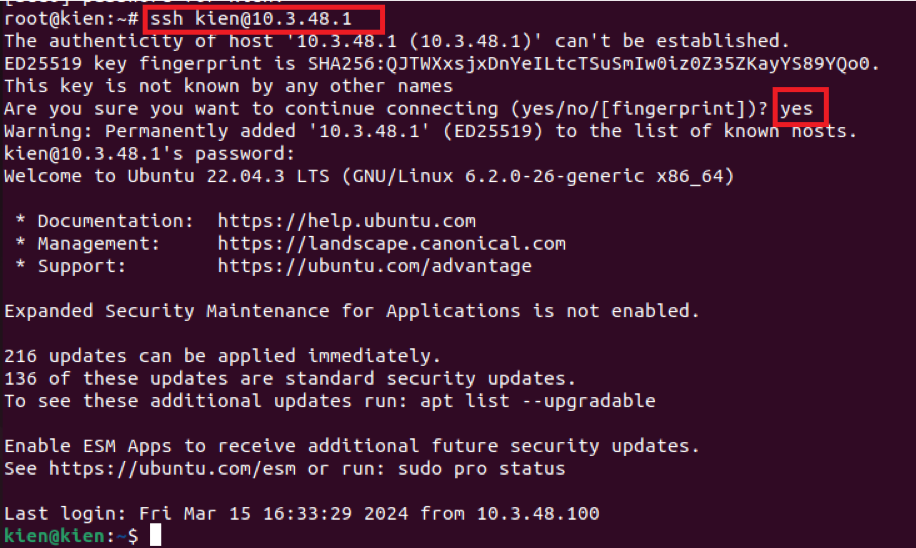
**IV.Cấu hình Server**

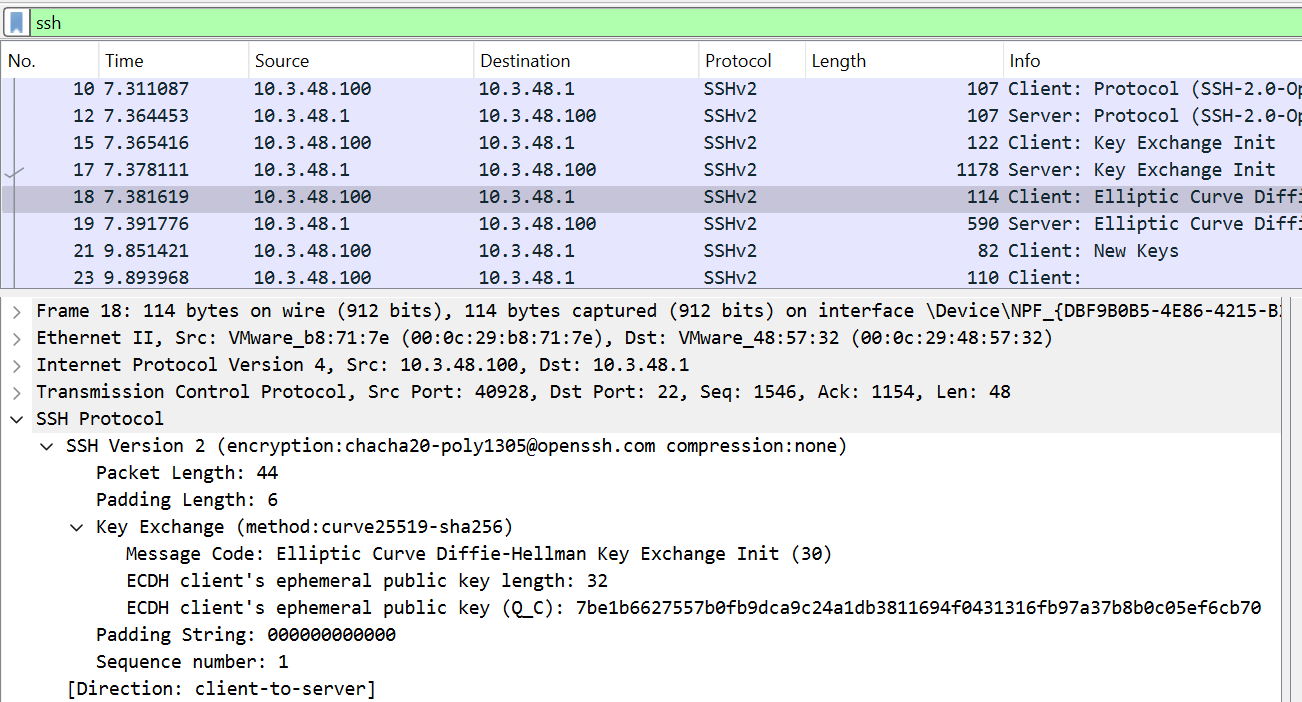
**Cấu hình tương tự như Client**



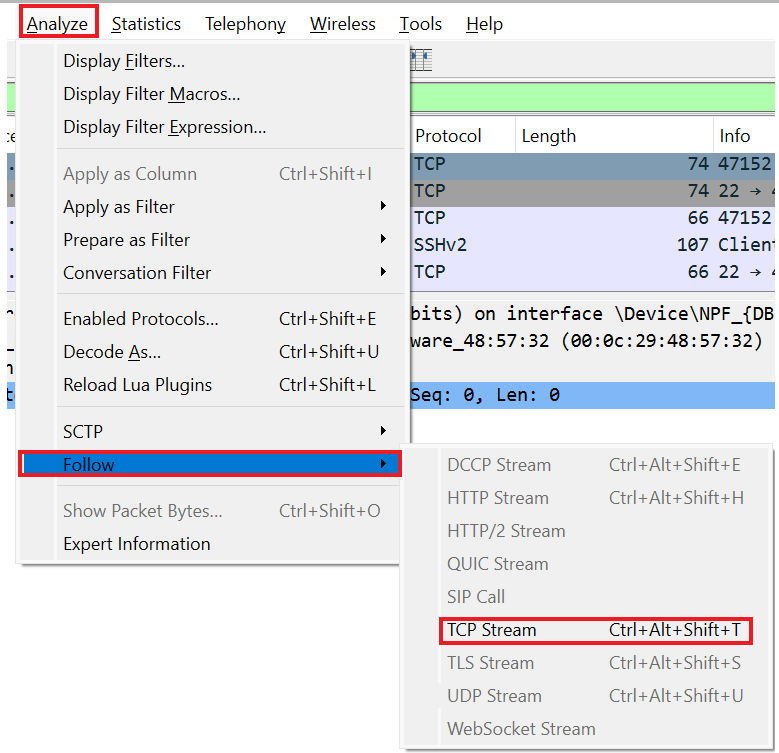
Cài đặt SSH

SSH lên Server bắt gói tin

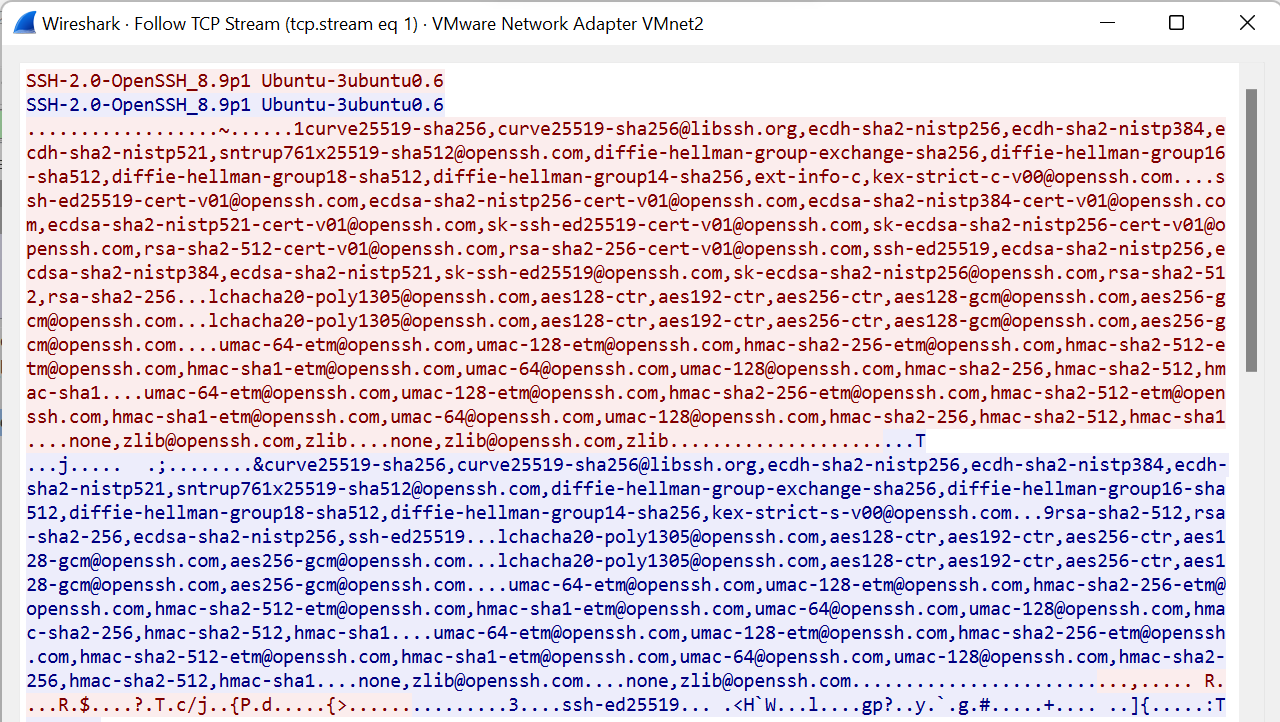




Khởi tạo trao đổi khóa Diffie-Hellman (DH) dựa trên đường cong elliptic curve (ECDH) giữa máy khách (client) và máy chủ (server)

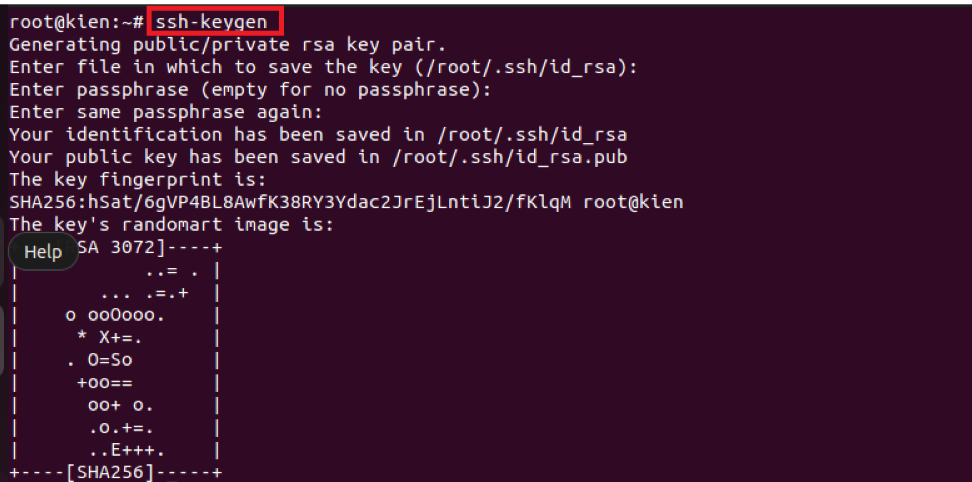


Xem quá trình trao đổi thông tin giữa 2 máy với nhau

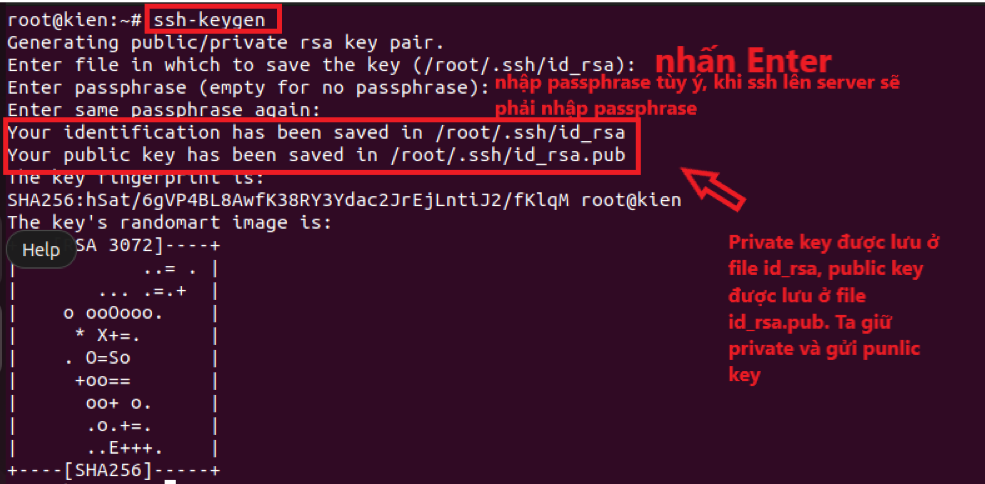


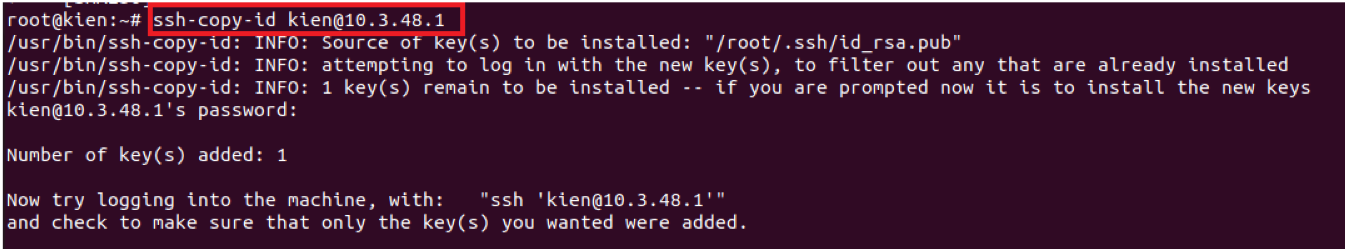
**V.Cấu hình dùng mật mã khóa công khai**

**Cấu hình Client**

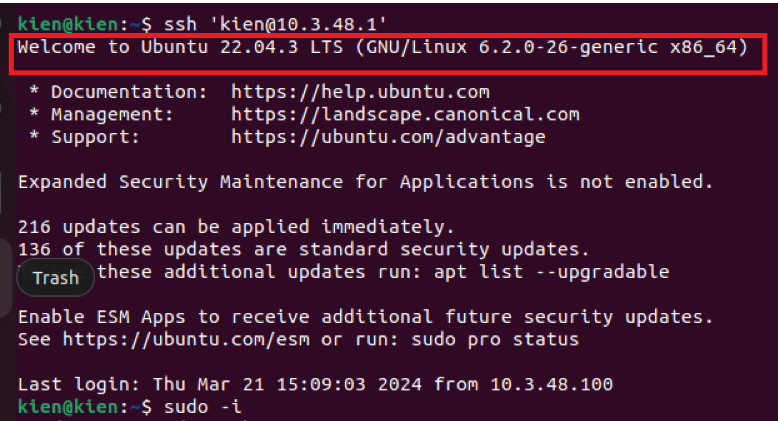


ssh-keygen một công cụ dùng để tạo cặp khóa SSH, bao gồm một khóa riêng (private key) và một khóa công khai (public key).





Gửi khóa công khai đến cho máy server



Quá trình xác thực sau khi gửi khóa không cần mật khẩu để đăng nhập