SSL/TLS Project

1. Server
2. Tạo cert.pem, key.pem

* Cd đến folder server, nhập lệnh: openssl req -new -x509 -days 365 -nodes -out cert.pem -keyout key.pem, sau đó sẽ hiện ra:

Giải thích lệnh:

-new -x509: Tạo chứng chỉ định dạng X.509 (chuẩn SSL).

-days 365: Có hiệu lực 1 năm.

-nodes: Không mã hóa private key bằng mật khẩu (để server dễ dùng).

-out cert.pem: File chứng chỉ public.

-keyout key.pem: File private key.

Sau đó, bạn sẽ phải điền những thông tin:

Country Name (2 letter code) [AU]:VN

State or Province Name (full name) [Some-State]:Hanoi

Locality Name (eg, city) []:Hanoi

Organization Name (eg, company) [Internet Widgits Pty Ltd]:SSL/TLS Project

Organizational Unit Name (eg, section) []:BKHN

Common Name (e.g. server FQDN or YOUR name) []:localhost (đây là phần quan trọng, cần nhập đúng)

Email Address []:0 nhập

* Tạo ra 2 file cert.pam và key.pam có nội dung như trong file.

1. Viết file code server.py