BÀI THỰC HÀNH: OPENVPN

1. **Mục đích**

   Giúp sinh viên hiểu được ứng dụng của mật mã và tạo được đường hầm VPN .

2. **Yêu cầu đối với sinh viên**

   Sử dụng thuần thục hệ điều hành Linux cũng như công cụ OpenVPN

3. **Nội dung thực hành**

- Tải bài lab:

imodule

https://github.com/congtoan123/labtainer-ptit-openvpn/raw/main/imodule.tar

- Khởi động bài lab:

  Vào terminal, gõ :

  labtainer -r ptit-openvpn

  (chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

  Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy chủ : server, một cái là đại diện cho máy khách: openvpn. Biết rằng 2 máy nằm cùng mạng LAN.

- Ta sẽ tiến hành thực hiện trong thư mục /etc/openvpn/ nên sẻ tiến hành di chuyển file cấu hình và x509- extension vào thư mục client và server tương ứng .
- Đầu tiên ta sẽ tiến hành cấu hình cho VPN **server**
- Chỉnh sửa cấu hình các tham số cho VPNServer trong file: *server.conf*
- Tạo chứng chỉ và khóa của cơ quan cung cấp chứng chỉ gốc:

  openssl req -x509 -newkey rsa:4096 -keyout ca.key -sha256 -days 3650 -set_serial 00 -out ca.crt -subj "/C=VN/ST=HN/L=HD/O=PTIT/CN=<MSV>" -addext nsComment="ROOT CA"

- Kiểm tra thông tin chứng chỉ gốc đã tạo:

  openssl x509 -in ca.crt -text -noout

- Chỉnh sửa cấu hình mở rộng cho chứng chỉ số x509 trong file: *x509-extensions.cnf*
- Tạo yêu cầu chứng chỉ (CSR) và cặp khóa cho máy chủ và kí bởi trung tâm cung cấp chứng chỉ CA :

  openssl req -new -newkey rsa:2048 -nodes -keyout server.key -out server.csr -subj "/C=VN/ST=HN/L=HD/O=PTIT/CN=SERVER

- Kí bằng khóa và chữ kí của CA:

  openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -set_serial 01 -sha256 -days 730 -text -out server.crt -extensions v3_vpn_server -extfile ./x509-extensions.cnf

- Sau đó kiểm tra thông tin

  openssl x509 -in server.crt -text -noout

- Bước tiếp theo tạo chứng chỉ và cặp khóa cho máy khách và kí bởi trung tâm cung cấp chứng chỉ CA:

openssl req -new -newkey rsa:2048 -nodes -keyout client.key -out client.csr -subj "/C=VN/ST=HN/L=HD/O=PTIT/CN=CLIENT

- Kí với khóa và chữ kí của CA:
  openssl x509 -req -in client.csr -CA ca.crt -CAkey ca.key -set_serial 02 -sha256 -days 365 -text -out client.crt -extensions v3_vpn_client -extfile ./x509-extensions.cnf
- Kiểm tra thông tin
  openssl x509 -in client.crt -text -noout
- Tạo khóa chia sẻ giữa client và server:
  openvpn --genkey --secret tc.key
- Trên máy **client** (openvpn) truy cập thư mục /etc/openvpn/client với quyền root : Chỉnh sửa file câu hình máy khách: client.conf
- Tiếp theo khởi động dịch vụ ssh và trên máy **server** sử dụng scp để truyền file tới client:
  sudo scp ca.crt client.crt client.key tc.key <Username>@<IP>:<Destination>/
- Trên **client** chuyển file vừa nhận được vào thư mục /etc/openvpn/client/ và chỉnh sửa lại quyền thực thi :
  sudo mv -f ca.crt client.crt client.key tc.key /etc/openvpn/client/
  cd /etc/openvpn/client/
  *sudo chown root: **
  *sudo chmod 0600 *.key*
- Khởi động VPNserver và VPN client:
- Trên **server** :
  sudo openvpn --config server.conf
- Trên **client:**
  sudo openvpn --config client.conf
- Tiến hành kiểm tra kết nối:
  ifconfig tun0
  ping 10.8.0.1
- Kết thúc bài lab:
  - Kiểm tra checkwork:
    checkwork
  - Trên terminal đầu tiên sử dụng câu lệnh sau để kết thục bài lab:
    Stoplab
  - Khi bài lab kết thúc, một tệp zip lưu kết quả được tạp và lưu vào một vị trí hiển thị dưới stoplab
- Khởi động lại bài lab:

labtainer -r ptit-openvpn