Đại học Quốc gia thành phố Hồ Chí Minh
Trường Đại học Công nghệ Thông tin
Khoa mạng máy tính và truyền thông
Bộ môn An toàn thông tin

2

Lab

PHỤC VỤ MỤC ĐÍCH GIÁO DỤC
FOR EDUCATIONAL PURPOSE ONLY

VPN

Thực hành môn An toàn mạng

Tháng 9/2024

Lưu hành nội bộ

<Nghiêm cấm đăng tải trên internet dưới mọi hình thức>

A. TỔNG QUAN

1. Mục tiêu

- Hiểu được cách VPN hoạt động
- Cấu hình VPN tunnel đơn giản trên Linux

2. Thời gian thực hành

- Thực hành tại lớp: 5 tiết tại phòng thực hành.
- Hoàn thành báo cáo kết quả thực hành: tối đa 13 ngày.

B. CHUẨN BỊ MÔI TRƯỜNG

- Cài đặt 3 máy ảo Ubuntu (có thể sử dụng Seed Ubuntu 20.04 (https://seedsecuritylabs.org/labsetup.html hoặc các máy ảo đã có sẵn từ các bài thực hành trước) trên Virtual Box
- Tải xuống các tập tin được đính kèm theo bài lab
- Cài đặt Phần mềm Wireshark trên các máy ảo

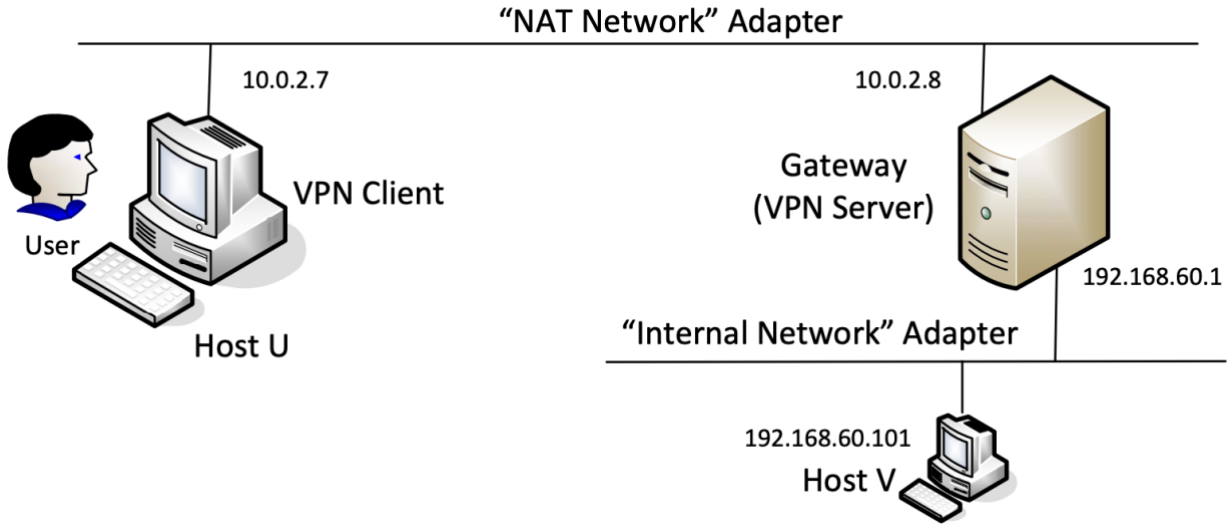
C. THỰC HÀNH

1. Tạo VPN đơn giản trên Linux

Ở phần này, chúng ta sẽ tạo một VPN đơn giản trên Linux bằng phần mềm được viết trên ngôn ngữ C.

a. Chuẩn bị môi trường

Chúng ta sẽ thiết lập một VPN tunnel giữa một máy tính client và một gateway, cho phép máy tính có thể truy cập an toàn vào mạng riêng thông qua gateway.
Mô hình của chúng ta sẽ gồm ít nhất là 3 máy ảo: VPN client (Host U), VPN Server (gateway) và một host V trong mạng riêng ảo.



Chúng ta có thể tận dụng máy ảo seedlab ở bài lab 1 làm Gateway và tạo thêm 2 máy ảo khác để làm Host U và Host V.

b. Tạo VPN tunnel sử dụng TUN/TAP

Ở phần này, bài lab sẽ cung cấp cho chúng ta một chương trình VPN đơn giản sử dụng TUN/TAP. Sử dụng chương trình này để tạo VPN tunnel. Sử dụng đoạn code trong thư mục "vpn" để thực hiện các task ở phần b.

Bước 1: Khởi chạy VPN Server.

Đầu tiên, chúng ta sẽ chạy chương trình VPN server vpnserver trên máy ảo VPN Server (gateway). Sau khi chương trình được chạy, một giao diện mạng ảo (virtual interface) TUN sẽ được xuất hiện trong hệ thống. Sử dụng lệnh "ifconfig -a" để quan sát, chúng ta sẽ thấy một giao diện mạng với tên tun0 xuất hiện. Interface này chưa được cấu hình, nên chúng ta sẽ tiến hành cấu hình địa chỉ IP cho interface này.

```
$ make

$ sudo ./vpnserver

Run the following command in another window:

$ sudo ifconfig tun0 192.168.53.1/24 up
```

Thông thường, một máy tính sẽ hoạt động như một host thay vì một gateway. VPN Server cần forward gói tin giữa mạng riêng ảo và tunnel, do đó chúng ta cần enable IP forwarding. Lưu ý: nếu máy ảo có sử dụng firewall, hãy thêm rule trên firewall cho phép forward gói tin giữa các interface.

```
$ sudo sysctl net.ipv4.ip_forward=1
```

Bước 2: Khởi chạy VPN Client

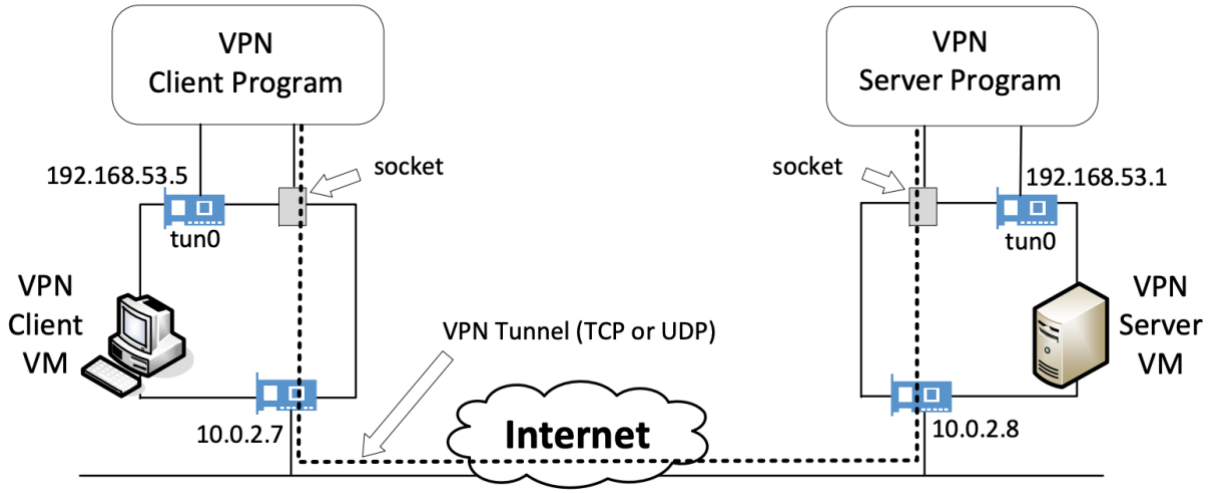
Bây giờ chúng ta sẽ khởi chạy chương trình VPN client trên máy ảo VPN Client.
Mở file vpnclient.c trên máy ảo Host U. Thay địa chỉ IP 127.0.01 của dòng code SERVER_IP "127.0.0.1" bằng địa chỉ IP Server cho phù hợp. Ví dụ:

```
#define BUFF_SIZE 2000

#define PORT_NUMBER 55555

#define SERVER_IP "10.0.2.8"

struct sockaddr_in peerAddr;
```

Sau khi đã sửa code. Tiến hành complie vài chạy chương trình

```
On VPN Client VM:

$ make

$ sudo ./vpnclient

Run the following command in a different window

$ sudo ifconfig tun0 192.168.53.5/24 up
```

Bước 3: Cấu hình route trên Host U (VPN client) và VPN Gateway



Sau hai bước trên, tunnel của chúng ta đã được tạo, chúng ta cần cấu hình route ở cả client và server để định hướng lưu lượng mạng thông qua tunnel. Trên máy client, chúng ta cần định

hướng tất cả các gói tin đi đến mạng riêng (192.168.60.0/24) qua interface tun0, từ đó các gói tin có thể được chuyển tiếp qua VPN tunnel.

Trên cả client và server, chúng ta cũng cần thiết lập một route cho tất cả lưu lượng truy cập đến mạng 192.168.53.0/24 được chuyển hướng tự động đến interface tun0.

Câu lệnh dưới đây để route traffic đi tới mạng 192.168.60.0/24 qua interface tun0. Hãy tham khảo để thực hiện tương tự trên VPN client và VPN server.

```
$ sudo route add -net 192.168.60.0/24 tun0
```

Bước 4: Cấu hình Route trên host V

Chúng ta cần thực hiện route traffic từ host V sang mạng riêng. Khi Host V nhận được một gói tin từ Host U, chúng ta cần biết IP nguồn trong gói tin là gì để có thể trả lời. Do đó, để thực hiện lệnh route này, cần tìm ra IP nguồn của các gói tin từ Host U đến Host V.

Task 1: Hãy thực hiện cấu hình route trên các máy ảo Gateway, Host U và Host V cho phép traffic VPN được điều hướng thông qua VPN tunnel.

Bước 5: Test tunnel

Sau khi đã hoàn thành các bước cấu hình, chúng ta có thể truy cập vào mạng riêng ảo từ VPN Client.

Task 2: Hãy thực hiện các lệnh ping, telnet và sử dụng Wireshark để bắt gói tin và chứng minh rằng hệ thống VPN đã hoạt động chính xác.

Task 3: Trên Host U, telnet đến Host V. Trong khi vẫn duy trì kết nối telnet, hãy ngắt VPN tunnel. Sau đó, gõ ký tự bất kỳ vào cửa sổ telnet và báo cáo những gì bạn quan sát được. Sau đó, kết nối lại VPN tunnel. Điều gì sẽ xảy ra với kết nối telnet? Nó sẽ bị ngắt hay được tiếp tục? Vui lòng mô tả và giải thích những quan sát của bạn.

c. Bảo mật tunnel

Tại thời điểm này, tunnel của chúng ta đã được tạo. Tuy nhiên, các gói tin gửi đi vẫn chưa được bảo mật. Chúng ta sẽ thực hiện mã hoá nội dung các gói tin này bằng TLS.

Sử dụng các tập tin trong tls.zip, thực hiện theo hướng dẫn trong file README để khởi chạy tls server và client.

Task 4: Chạy thực thi đoạn code mã hoá TLS. Dùng Wireshark bắt gói tin, để chứng minh nội dung gói tin gửi đi giữa client và server đã được mã hoá thành công.

D. YÊU CẦU & ĐÁNH GIÁ

- Sinh viên tìm hiểu và thực hành theo hướng dẫn, thực hiện theo nhóm đã đăng ký.

- Nộp báo cáo kết quả gồm chi tiết những việc (Report) mà nhóm đã thực hiện, quan sát thấy và kèm ảnh chụp màn hình kết quả (nếu có); giải thích cho quan sát (nếu có).
- Báo cáo:
  - File .PDF. Tập trung vào nội dung, không mô tả lý thuyết.
  - Đặt tên theo định dạng: [Mã lớp]-LabX_MSSV1_MSSV2.
  - Ví dụ: [NT140.P12.ANTT.1]-Lab1_2252xxxx_2252yyyy.
  - Nếu báo cáo có nhiều file, nén tất cả file vào file .ZIP với cùng tên file báo cáo.
  - Nộp file báo cáo trên theo thời gian đã thống nhất tại courses.uit.edu.vn.

Bài sao chép, trễ, … sẽ được xử lý tùy mức độ vi phạm.

HẾT

Chúc các bạn hoàn thành tốt!