

BÀI THỰC HÀNH SỐ 6

Môn: MẬT MÃ VÀ AN NINH MẠNG

-o0o-

I. MỤC TIÊU

Mục tiêu của bài thực hành này cung cấp kỹ năng an ninh hệ thống E-mail cá nhân, an ninh hệ thống Web.

Các nội dung chính trong bài thực hành gồm 2 phần:

- An ninh hệ thống E-mail cá nhân với Thunderbird và OpenPGP.
- An ninh hệ thống Web với Apache Web Server và SSL.

II. TÀI LIỆU THAM KHẢO

- [1]. <https://wiki.mozilla.org/Thunderbird:OpenPGP:2020>
- [2]. <https://httpd.apache.org/>
- [3]. <https://windowsreport.com/create-self-signed-certificate/>
- [4]. <https://www.sslshopper.com/article-how-to-create-and-install-an-apache-self-signed-certificate.html>

III. CHUẨN BỊ TRƯỚC KHI THỰC HIỆN BÀI THỰC HÀNH

Các trang thiết bị và phiên bản phần mềm sử dụng trong bài thực hành:

- 01 máy tính truy cập đến Internet.
- Trình gửi và nhận thư: Mozilla Thunderbird phiên bản 78.10.0.
- Apache Web Server và OpenSSL.

IV. CÁCH THỨC VÀ HẠN CHÓT NỘP BÀI

- Sinh viên cần trả lời thông tin (văn bản, hình ảnh) vào các phần yêu cầu trong bài thực hành vào lưu lại thành tập tin lab6.doc
- Thời gian làm bài là 14 ngày.

V. NỘI DUNG THỰC HIỆN

1. An ninh hệ thống E-mail cá nhân

a. Cài đặt Mozilla Thunderbird

Mozilla Thunderbird là chương trình miễn phí, nguồn mở hoạt động trên mọi nền tảng hệ điều hành giúp quản lý việc nhận, gửi và lưu trữ thư điện tử. Một phần mềm quản lý thư điện tử từ phía người dùng là một chương trình giúp bạn tải về và quản lý thư điện tử mà không cần sử dụng trình duyệt Internet. Bạn có thể quản lý nhiều tài khoản thư điện tử khác nhau sử dụng chương trình này. Tài khoản của bạn phải được tạo ra trước khi dùng với **Thunderbird**.

Download Thunderbird từ <http://www.mozilla.org/en-US/thunderbird/>

Các bước ngắn gọn để cài đặt Thunderbird:

.....
.....
.....



.....
.....
.....
.....
b. Đăng ký một tài khoản thư điện tử vào Thunderbird

Các bước ngắn gọn để đăng ký một tài khoản thư điện tử của bạn vào thunderbird:

.....
.....
.....
.....
.....
.....
c. Tạo cặp khóa từ OpenPGP Key Manager

Từ **Tools-> OpenPGP Key Manager**, cửa sổ hiện ra là:

.....
.....
.....
.....
.....
.....
Chọn **Generate -> New Key Pair**, cửa sổ hiện ra là:

.....
.....
.....
Thực hiện các bước tiếp theo để tạo cho tài khoản của mình một cặp khóa.

d. Tạo thư và gửi đính kèm khóa công khai

Nhấp vào “Write” để tạo một bức thư.gửi đến cho người bên cạnh có đính kèm khóa công khai của mình (chọn **Security -> Attach My Public Key**).

e. Thêm khóa công khai của các người dùng khác

Mở thư có chứa khóa công khai của bạn bên cạnh. Các bước tiếp theo là:

.....
.....
.....
f. Tạo thư, mã hóa và gửi đi

Các bước thực hiện là:

.....
.....
.....
g. Nhận thư. giải mã, đọc thư

Các bước thực hiện là:



Mở trình duyệt và đọc thư nói trên, cho biết nội dung thể hiện:

.....

.....

.....

h. Tạo thư, tạo chữ ký số, mã hóa và gửi đi

Các bước thực hiện là:

.....

.....

.....

i. Nhận thư, giải mã, xác minh chữ ký số, đọc thư

Các bước thực hiện là:

.....

.....

.....

Mở trình duyệt và đọc thư nói trên, cho biết nội dung thể hiện:

.....

.....

.....

2. An ninh hệ thống Web

a. Cài đặt và cấu hình Apache Web Server

Apache là phần mềm web server miễn phí mã nguồn mở. Tên chính thức của Apache là Apache HTTP Server được điều hành và phát triển bởi Apache Software Foundation.

Download Apache Web Server từ <https://httpd.apache.org/download.cgi>

Các bước ngắn gọn để cài đặt và cấu hình Apache Web Server:

.....

.....

.....

Lưu ý: [Cần disable IIS đối với các hệ điều hành MS Windows.](#)

b. Tạo chứng chỉ SSL tự ký bằng OpenSSL

Các bước thực hiện là:

.....

.....

.....

.....

.....

.....

c. Cài đặt Apache Web Server với chứng chỉ SSL đã tạo

Các bước thực hiện là:



.....
.....
.....
.....
.....

d. Tìm hiểu và cho biết khác biệt các loại chứng chỉ SSL (DV, OV, EV)

.....
.....
.....

e. Cho biết cách tạo và duy trì chứng chỉ SSL miễn phí từ Let's Encrypt

.....
.....
.....

-HẾT-