Khoa Khoa học & Kỹ thuật máy tính
Trường ĐH Bách Khoa TP.HCM

Cryptography and Network Security
Lab 4

Hieu Nguyen

Ngày 17 tháng 4 năm 2017

1 Mục tiêu

- Hiểu biết cề các lệnh cơ bản trong Linux.
- Hiểu biết về SSL (Secure Sockets Layer) và HTTPS (HTTP + SSL).
- Cài đặt SSL cho Apache trên máy chủ Ubuntu.

Chuẩn bị

Cài đặt hệ điều hành Ubuntu 14.04 hoặc mới hơn (có thể dùng VMWare nếu máy đang sử dụng hệ điều hành Windows).

PHẦN 1.

Tìm hiểu các lệnh cơ bản trong Linux va2 các thao tác cơ bản trên trình soạn thảo vi. (file basic_linux_commands.pdf và basic_vi_commands.pdf)

Bài tập: Làm các bài tập được cho trong file exercise_1.docx

PHẦN 2. Cấu hình xác thực dùng SSH key cho máy chủ Ubuntu.

Để đăng nhập từ xa vào một server dùng SSH chúng ta có thể dùng một trong hai cách để xác thực:

- Password based
- Key based

- Với Password based, chúng ta cần phải nhập password cho mỗi lần đăng nhập vào server thông qua SSH.

- Với Key based, cơ chế xác thực không cần password, chúng ta sẽ dùng một cặp public và private key để truyền thông giữa client và server. Client sẽ giữ private key và mã hóa thông điệp còn public key sẽ nằm trên server dùng để giải mã thông điệp.

Việc sử dụng password có thể bị kẻ gian đánh cắp sử dụng tấn công Brute Force. Thay vào đó, bằng việc sử dụng SSH key, chúng ta có thể tăng độ bảo mật hơn nữa bằng việc bảo vệ private key cùng với một passphrase.

Tham khảo: SSH_keys.pdf

Bài tập: Mô tả các bước cấu hình xác thực dùng SSH key cho máy chủ Ubuntu, chụp ảnh màn hình kết quả cho mỗi bước. Lưu vào file exercise_2.docx

PHẦN 3.

- Cài đặt SSL cho Apache trên máy chủ Ubuntu.
- SSL là viết tắt của từ Secure Sockets Layer. Đây là một tiêu chuẩn an ninh công nghệ toàn cầu tạo ra một liên kết được mã hóa giữa máy chủ web và trình duyệt. Liên kết này đảm bảo tất cả các dữ liệu trao đổi giữa máy chủ web và trình duyệt luôn được bảo mật và an toàn.
- SSL đảm bảo rằng tất cả các dữ liệu được truyền giữa các máy chủ web và các trình duyệt được mang tính riêng tư, tách rời. SSL là một chuẩn công nghiệp được sử dụng bởi hàng triệu trang web trong việc bảo vệ các giao dịch trực tuyến với khách hàng của họ. *(Nguồn: matbao.net)*
- *Tham khảo:* SSl_Apache_Ubuntu.pdf

Bài tập: Mô tả các bước cài đặt SSL cho Apache trên máy chủ Web Ubuntu

Yêu cầu:

- Chụp ảnh màn hình demo kết quả cho mỗi bước.
- Giải thích kết quả đạt được cho mỗi bước. . Lưu vào file **exercise_3.docx**

QUY ĐỊNH NỘP BÀI

- **Báo cáo**: Sinh viên thực hiện bài tập cho phần 1 và phần 2. Kết quả lưu trong 2 file **exercise_1.docx** và **exercise_2.docx** tương ứng.
  - File **exercise_1.docx**: Điền vào chỗ trống các lệnh nhập vào terminal để cho kết quả đúng yêu cầu.
  - File **exercise_2.docx**: Mô tả các bước thực hiện, chụp ảnh màn hình kết quả cho mỗi bước.

Cách tính điểm cho Lab 4:

- Sinh viên không nộp bài đúng hạn hoặc bài làm sai quá nửa sẽ nhận điểm 0 cho cột điểm bài tập.