HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN

HỌC PHẦN: KĨ THUẬT GIẤU TIN
MÃ HỌC PHẦN: INT14102

LAB : lss-lab-1

Sinh viên thực hiện: Phạm Anh Tuấn

Mã sinh viên: B21DCAT212

Tên lớp: 04

Giảng viên hướng dẫn: Đỗ Xuân Chợ

HÀ NỘI 2025

LAB : lss-lab-1

1. Mục đích

Giúp sinh viên hiểu được thuật toán giấu tin sử dụng phương pháp dịch chuyển vị trí dòng (Line-Shift Stegnography), và cách ứng dụng trong việc truyền file qua ssh bằng scp.

2. Yêu cầu đối với sinh viên

Sử dụng thuần thục hệ điều hành Linux và có kiến thức về kĩ thuật giấu tin.

3. Nội dung lý thuyết

Thuật toán giấu tin sử dụng phương pháp dịch chuyển vị trí dòng:
Trong phương pháp này, các dòng của văn bản sẽ được dịch chuyển theo chiều dọc với một độ dài nhất định, ví dụ mỗi dòng sẽ được dịch chuyển một khoảng rất nhỏ khoảng 1/300 inch lên hoặc xuống (inch là một đơn vị chiều dài trong hệ thống đo lường) và thông tin sẽ được ẩn giấu bằng việc tạo ra các hình dạng của khoảng dịch chuyển của văn bản. Thông điệp sẽ được giấu vào khoảng dịch chuyển đó bằng cách chèn vào các bit 0 hoặc 1 tùy theo quy ước. Điều này rất khó có thể phát hiện bằng mắt thường vì khoảng cách thay đổi khá nhỏ.
Thuật toán giấu tin:
Đầu vào:
- Thông điệp bí mật
- Văn bản phủ
Các bước thực hiện:
- Bước 1: Chuyển thông tin bí mật thành dạng nhị phân
- Bước 2: Đọc dạng nhị phân của thông điệp bí mật và dịch chuyển vị trí các dòng theo quy ước dòng được dịch giảm đi tương ứng bit 0 được giấu, dòng được dịch tăng lên tương ứng bit 1 được giấu.
Đầu ra:
- Văn bản chứa thông điệp.

4. Nội dung thực hành

Khởi động bài lab:

Vào terminal, gõ :

labtainer -r lss-lab-1

(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)

Nhiệm vụ 1: Thực hiện giấu tin

- Để bắt đầu thực hiện giấu tin ta cần thực hiện việc chuyển thông điệp sang dạng nhị phân sau đó mới giấu vào trong văn bản phủ. Để thực hiện điều đó trong terminal của user1 có thể tìm thấy file encrypt.py giúp thực hiện việc này, tiến hành chạy file encrypt.py:

python3 encrypt.py

Sau khi chạy file python sẽ yêu cầu nhập nội dung để giấu. Nhập i_am_ptiter và xem kết quả : thông điệp nhị phân, quá trình giấu từng bit, nơi lưu trữ file đầu ra.

Nhiệm vụ 2: Quan sát thử file đầu ra

- Sau khi hoàn thành bước trên, bạn nhận được một file pdf có tên là output.pdf. Thực hiện việc đọc file PDF này với firefox bằng lệnh:

  firefox output.pdf
- Quan sát nội dung file PDF khoảng cách giữa các dòng xem có thấy được sự chênh lệch nào giữa chúng không (khoảng cách chênh lệch rất nhỏ nên rất khó để nhìn được bằng mắt thường)

Nhiệm vụ 3: Thực hiện truyền file qua SSH bằng SCP

- Sau khi đọc xong file trên user1, ta sẽ thực hiện truyền file cho user2. Tại terminal của user2 và user1 ta thực hiện kiểm tra trạng thái của ssh:

  sudo systemctl status ssh
- Sau khi xác nhận cả 2 đều đã chạy ssh thì ta sẽ thực hiện truyền file từ user1 sang cho user2 bằng lệnh scp :

  scp output.pdf ubuntu@10.10.0.20:~/
- Mật khẩu là 123 cho cả 2 user

Nhiệm vụ 4: Giải mã

- Sau khi truyền file xong, tại terminal của user2 thực hiện kiểm tra xem có file output.pdf chưa bằng lệnh *ls.* Khi thực hiện list danh sách file ta có thể thấy được là còn có một file giúp chúng ta giải mã thông điệp đó là file decrypt.py. Thực hiện giải mã file output.pdf để lấy thông điệp bằng cách chạy file decrypt.py :

  python3 decrypt.py
- Kết quả mong đợi là thông điệp khớp với thông điệp giấu bên user1

Kết thúc bài lab:

o Kiểm tra checkwork:

checkwork

o Trên terminal đầu tiên sử dụng câu lệnh sau để kết thúc bài lab:

Stoplab

Khởi động lại bài lab:

labtainer -r lss-lab-1