HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

HỌC PHẦN: KĨ THUẬT GIẤU TIN

MÃ HỌC PHẦN: INT14102

Lab: stego-whitespace-endtext

Sinh viên thực hiện: Phạm Thùy Trang

Mã sinh viên: B21DCAT184

Hà Nội 2025

BÀI THỰC HÀNH: STEGO-WHITESPACE-ENDTEXT

1. **Mục đích:**
   - Giúp sinh viên hiểu được cách sử dụng khoảng trắng cuối dòng để giấu tin.
2. **Yêu cầu đối với sinh viên:**
   - Có kiến thức về giấu tin trong khoảng trắng.
3. **Nội dung lý thuyết:**

Nguyên tắc giấu tin vào cuối mỗi dòng dựa trên việc tận dụng các khoảng trắng thêm vào sau mỗi dòng có thể lưu trữ được một lượng lớn các bit. Các khoảng trắng ở cuối mỗi dòng có thể bị bỏ qua và không hiện lên các bởi các ứng dụng đọc văn bản. Trong toàn bộ văn bản, nếu giấu tin vào cuối mỗi dòng thì lượng bit thu được là rất lớn, có thể có đủ không gian để lưu trữ chuỗi bí mật.

Thuật toán giấu tin:

Đầu vào:

- Thông điệp bí mật

- Văn bản phủ

Các bước thực hiện:

Bước 1: Chuyển thông điệp bí mật thành dạng nhị phân

Bước 2: Đọc dạng nhị phân của thông tin bí mật và thêm khoảng trắng vào cuối mỗi dòng theo quy ước: 0 dấu cách sẽ tìm đến câu tiếp theo và tương đương không có bit thông tin nào được giấu trong đó; 1 dấu cách sẽ mã hóa 0; 2 dấu cách sẽ mã hóa 1.

Đầu ra:

- Văn bản phủ có chứa thông điệp

4. **Nội dung bài lab:**
   - Khởi động bài lab:

labtainer -r stego-whitespace-endtext

   - Sau khi khởi động xong, hai terminal ảo sẽ xuất hiện, hai máy đều là máy student nằm trong cùng một mạng LAN.

Task 1: Sử dụng code để mã hóa giấu thông điệp bí mật vào một tệp văn bản

- Tại máy student1, tạo một văn bản phủ để giấu tin vào văn bản:

echo "This is a normal message." > cover.txt

- Nhập lệnh chạy code python để giấu thông điệp bí mật vào tệp văn bản phủ:

python3 encoder.py "This is a secret message." cover.txt message.txt

Task 2: Gửi tệp chứa thông điệp bí mật sang máy khác qua SSH

- Sử dụng scp để gửi tệp qua máy khác (đảm bảo máy đích đã bật SSH và địa chỉ đúng), tên và mật khẩu máy đích đều là ubuntu

scp message.txt <tên máy đích>@<địa chỉ máy đích>:/home/ubuntu

Lưu ý: Khi chạy scp, nếu hiện lỗi "kex_exchange_identification: read: Connection reset by peer/ lost connection" thì chạy các lệnh sau trên cả 2 máy student:

- Bật dịch vụ ssh: *sudo systemctl enable ssh*
- Dừng hoàn toàn dịch vụ xinetid: *sudo systemctl stop xinetd*
- Khởi động dịch vụ ssh: *sudo systemctl start ssh*
- Sau khi chạy xong trên cả 2 máy thì thực hiện lại lệnh scp

Task 3: Giải mã thông điệp bí mật

- Tại máy student2, nhập lệnh chạy code python để giải mã thông điệp bí mật được giấu trong tệp văn bản:

python3 decoder.py message.txt

⇨ Nhận được thông điệp bí mật mà student1 gửi.

- Kết thúc bài lab:
  - Kiểm tra checkwork:

checkwork

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

stoplab

  - Khởi động lại bài lab:

labtainer -r stego-whitespace-endtext