Labtainer : Giấu tin trong văn bản- phương pháp ngữ nghĩa-từ đồng nghĩa(trung bình)

1. **Mục đích**
   - Bài thực hành này giúp sinh viên nắm bắt được phương pháp giấu tin trong văn bản bằng cách sử dụng từ đồng nghĩa
     - Sử dụng **python1.py** để giấu thông điệp vào văn bản
     - Sử dụng **python2.py** để giải mã thông điệp mà bên gửi gửi cho bên nhận
     - Sử dụng **python3.py** để phát hiện văn bản có giấu tin hay không trên máy attacker.
2. **Nội dung lý thuyết**
   - Tìm hiểu về phương pháp giấu tin trong văn bản sử dụng từ đồng nghĩa
   - Tìm hiểu về cấu trúc code python.
3. **Các bước thực hiện**

3.1. Khởi động bài lab

3.1.1. Các bước cần thực hiện

Thực hiện cài đặt lab tại**: https://github.com/B21DCAT076/KTGT**

Sinh viên thực hiện tải file steganography-semantic-medium.rar và giải nén ra

-Sau đó thực hiện copy file giải nén vào thư mục**: labtainer/trunk/labs/**

Tại Terminal của labtainer gõ lệnh

```
`labtainer -r steganography-semantic-medium `
```

(chú ý: sinh viên sử dụng <TÊN_TÀI_KHOẢN_HỆ_THỐNG> của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Tại **Terminal** của máy sẽ hiện ra 3 máy , 1 là Client, 2 là Server, 3 là Attacker, chúng có chung 1 mạng con, tiến hành kiểm tra địa chỉ IP của 3 máy bằng **ifconfig**

Trên máy client có: file python1.py: đây là code mã hóa, text1.txt(văn bản phủ), text2.txt (văn bản mã hóa)

Trên Server: file python2.py: code giải mã, text3.txt(nhận dc từ text2.txt bằng nc), text4.txt(chứa nội dung thông điệp)

Trên Attacker: file python3.py: code phát hiện giấu tin hay không, text5.txt (chứa nội dung file text2.txt mà client gửi server)

Task 1: Thực hiện Giau Tin

-Trên Client ta quan sát bằng lệnh ls có 1 file python1.py(đây là file code mã hóa) và 2 file văn bản là text1.txt(file văn bản phủ) và text2.txt(file văn bản mã hóa sau khi chạy code python1.py)

Trên client tiến hành chạy file python1.py bằng lệnh:

python3 python1.py

Khi được hỏi nhập thông điệp cần giấu, bạn hãy nhập :PTIT

Quan sát kết quả đầu ra với file text2.txt và so sánh text1.txt để xem sự khác biệt

Task 2 : Thực hiện truyền file sang Server:

-Trên Server ta thực hiện lệnh :

nc –l –p 1234 > text3.txt

- Trên Attacker:

Ta thực hiện lệnh: Sudo nmap <ip máy server> để biết cổng nào đang mở trên Server.

sau đó ta thự hiện lệnh : nc –lvp 1234 >> text5.txt

<mục đích: ghi lại file.txt mà Client gửi cho Server rồi gán vào text5.txt >

-Trên Client ta thực hiện lệnh:

nc <ip máy server> 1234 < text2.txt

<text3.txt chính là file text2.txt mà client gửi cho server>

Task3: Thực hiện giải mã thông điệp trên Server

-Ta thực hiện lệnh:

cat text3.txt

Lệnh này kiểm tra xem văn bản client đã gửi cho server được chưa

- Ta tiến hành giải mã:

python3 python2.py

Sau đó ta tiến hành mở file text4.txt để nhận dc thông điệp giải mã

Task4: Kiểm tra Attacker có bắt đc file Client gửi cho server:

Dùng lệnh: Cat text5.txt

<Trước đó đã dùng lệnh nc –lvp 1234 >> text5.txt >

Task 5: Phát hiện giấu tin

-Trên **Attacker** tiến hành chạy file python3.py bằng lệnh:

python3 python3.py

-PP phát hiện giấu tin trong văn bản bằng từ đồng nghĩa chủ yếu dựa trên ngữ nghĩa, cấu trúc ngữ pháp, lỗi logic câu, lỗi nghĩa diễn đạt câu

3.2 Kết thúc bài lab:

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

stoplab

- Khi bài lab kết thúc, một tệp lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.
- Sinh viên cần nộp file *.lab* để chấm điểm.
- Để kiểm tra kết quả khi trong khi làm bài thực hành sử dụng lệnh: *checkwork <tên bài thực hành>*
- Khởi động lại bài lab: Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer –r steganography-semantic-medium