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-2

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-2

1. Mục đích

Giúp sinh viên hiểu được thuật toán giấu tin sử dụng phương pháp dịch chuyển vị trí dòng (Line-Shift Stegnography), biết cách thực hiện tấn công MITM để thực hiện bắt log ftp và phát hiện thuật toán giấu tin để tách tin.

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

Add module file lab:

imodule https://github.com/Snut5923/Labtainer/raw/refs/heads/main/lss-lab-2.tar

Khởi động bài lab:

Vào terminal, gõ :

labtainer -r lss-lab-2

(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 xuất hiện file ouput.pdf.

Nhiệm vụ 2: Chuẩn bị tấn công

- Sau khi hoàn thành bước trên, tiến hành bật ftp server trên user2 thông qua file ftp_server.py:

  python3 ftp_server.py

- Để có thể bắt được thông điệp truyền từ user1 đến user2 qua ftp ta cần thực hiện bật arp spoofing trên máy attacker :

  sudo arpspoof -i eth0 -t 192.168.0.10 192.168.0.20

- Sau đó tiến hành chạy file attack.py trên attacker để bắt log:

  sudo python3 attack.py

Nhiệm vụ 3: Gửi file qua ftp

- Sau khi chuẩn bị xong, từ user1 tiến hành ftp đến user2 để gửi file output.pdf qua (tài khoản là user, mật khẩu là 123456) :

  ftp 192.168.0.20

- Sau khi đăng nhập thành công tiến hành gửi file qua ftp bằng lệnh put:

  put output.pdf

Nhiệm vụ 4: Bắt log

- Sau khi truyền file xong, tại terminal của attacker quan sát xem có thấy được thông tin về username và password của ftp server cũng như thông tin về tên file được gửi qua lệnh put hay không (trên log là STOR), nếu không bắt được đầy đủ thông tin thực hiến chạy lại nhiệm vụ 3

Nhiệm vụ 5: FTP đến server từ attacker

- Sau khi bắt được log , tiến hành ftp đến user2 từ các thông tin chúng ta có :

  ftp 192.168.0.20

- Sau khi đăng nhập thành công tiến hành lấy file về bằng lệnh get:

  get output.pdf

Nhiệm vụ 6: Kiểm tra file

- Sau khi get được file về gõ *bye* để thoát ftp sau đó thực hiện list các file xem có file output.pdf chưa :

  ls

- Quan sát file bằng firefox :

  firefox output.pdf

Nhiệm vụ 7: Phát hiện và giải mã

- Bây giờ ta sẽ tiến hành phát hiện thuật toán giấu tin dịch chuyển dòng trong file pdf trên bằng file detect.py có trong attacker :

python3 detect.py

- Sau khi chạy nó sẽ tiến hành tính toán khoảng cách dòng và dựa vào đó để lấy ra các bit 01 và xâu chuỗi lại để giải mã thành thông điệp. Kết quả đúng sẽ ra dòng chữ : i_am_ptiter

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-2