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

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

LAB: stclab-1

Sinh viên thực hiện: Nguyễn Quốc Việt

Mã sinh viên: B21DCAT220

Tên lớp: 04

Giảng viên hướng dẫn: Đỗ Xuân Chợ

HÀ NỘI 2025

LAB: stclab-1

1. Mục đích

Giúp sinh viên hiểu được thuật toán giấu tin sử dụng phương pháp dựa trên tính phản xạ đối xứng của ký tự 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

Trong hầu hết các thuật toán giấu tin, thông điệp bí mật được ẩn giấu bằng cách thay đổi cấu trúc của văn bản chứa do đó khả năng bị nghi ngờ hay mất mát dữ liệu khi gõ lại văn bản theo cấu trúc chính xác là có thể xảy ra. Để tránh xảy ra khả năng này cũng như tăng cường tính bảo mật, thay vì giấu các bit bí mật bằng cách thay đổi cấu trúc của văn bản chứa, phương pháp này sẽ giấu các thông điệp bí mật bằng cách tạo ra một văn bản tóm tắt thu thập từ các bài báo hay bất kỳ một phương tiện văn bản thông tin đại chúng. Quá trình tạo ra văn bản tóm tắt phụ thuộc vào tính phản xạ đối xứng của bảng chữ cái tiếng Anh. Dựa vào tính chất này, bảng chữ cái được chia thành các bộ khác nhau, mỗi bộ đại diện cho một cặp bit. Để thực hiện điều này cần phân tích tính phản xạ đối xứng của bảng chữ cái tiếng Anh và phân loại chúng để thể hiện các bit.

Thuật toán giấu tin

Đầu vào:

Thông điệp bí mật

Bất kỳ văn bản bằng ngôn ngữ tiếng Anh

Các bước thực hiện:

Bước 1: Biến đổi thông điệp bí mật thành chuỗi bit nhị phân

Bước 2: Kiểm tra xem tổng độ dài của chuỗi bit là chẵn hay lẻ. Nếu lẻ, phải thêm 1 bit ‘0’ vào cuối chuỗi bit nhị phân. Bây giờ có thể chia chuỗi bit tổng thành các cặp bit liên tiếp.

Bước 3: Chuyển đổi toàn bộ các ký tự của văn bản đầu vào thành các chữ cái viết hoa.

Bước 4: Với từng cặp bit, xem xét chữ cái đầu tiên của từ đầu tiên trong câu:

✓ Nếu chữ cái đó nằm trong nhóm đại diện cho cặp bit đang xem xét, chọn câu này và đưa vào văn bản chứa.

✓ Nếu chữ cái đó không nằm trong nhóm đại điện cho cặp bit đang xem xét, bỏ qua câu này và chọn câu tiếp theo

Bước 5: Quá trình tiếp diễn cho đến khi toàn bộ chuỗi bit của thông điệp bí mật được thực thi hết

Bước 6: Văn bản mã hóa thu được là bản tóm tắt của văn bản đầu vào và được gửi đến người nhận

Đầu ra:

Văn bản chứa thông điệp bí mật, hay chính là văn bản tóm lược của văn bản đầu vào

Thuật toán tách tin:

Đầu vào:

Văn bản chứa thông điệp bí mật (đầu ra của thuật toán giấu tin) Các bước thực hiện:

Bước 1: Lấy các chữ cái đầu tiên của các từ đầu tiên trong từng câu.

Bước 2: Dựa vào bảng để lấy ra các cặp bit từ những chữ cái thu được và đưa ra một file.

Bước 3: Chuyển đổi chuỗi bit nhị phân thành dạng chữ cái tương ứng.

Bước 4: Toàn bộ thông điệp dưới dạng chữ cái thu được chính là thông điệp ẩn giấu Đầu ra:

Thông điệp bí mật

4. Nội dung thực hành

Add module file lab:

imodule https://github.com/kokushibouz/Labtainer-Lab/raw/refs/heads/main/stclab-1.tar

Khởi động bài lab:

Vào terminal, gõ :

labtainer -r stclab-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 xuất hiện file message.txt.

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 message.txt

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 message.txt

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 bằng lệnh:

Ls

- Quan sát thử nội dung file:

cat message.txt

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 mức độ tương đồng của các câu cũng như đếm số lượng các từ nối trong câu để xác định xem có giấu tin không và xâu chuỗi lại để giải mã thành thông điệp. Kết quả đúng sẽ ra dòng chữ :

ptit

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 stclab-1