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-3

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-3

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 thay đổi file truyền đi qua ftp làm cho bên nhận tách tin ra sai thông điệp.

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-3.tar

Khởi động bài lab:

Vào terminal, gõ :

labtainer -r stclab-3

(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: Mở ftp server

- Để thực hiện mở ftp server, trên máy user2 có sẵn file ftp_server.py giúp thực hiện việc đó, chạy lệnh :

python3 ftp_server.py

Sau khi chạy file python dịch vụ ftp sẽ chạy trên máy user2 với ip là 172.22.2.2.

Nhiệm vụ 2: Bắt log về thông tin của ftp

- Sau khi hoàn thành bước trên, tiến hành bật arp spoofing trên máy attack để bắt lưu lượng từ user1 đến user2 :

sudo arpspoof -i eth0 -t 172.22.2.10 172.22.2.2

- Thực hiện chạy file log.py để bắt log :

sudo python3 log.py

- Sau đó tiến hành ftp từ user1 đến user2, trên user1 chạy lệnh :

ftp 172.22.2.2

- Thực hiện đăng nhập với tài khoản là user, mật khẩu là 123456, quan sát log trên máy attack xem có bắt được thông tin về username và password không, nếu chưa bắt được đầy đủ thông tin lặp lại các bước trong nhiệm vụ 2.

Nhiệm vụ 3: Thực hiện giấu tin

- Tại máy user1 thực hiện giấu tin để gửi thông điệp lên phía server bằng file encrypt.py:

python3 encrypt.py

- Sau khi chạy xong sẽ xuất hiện file encrypt.txt với thông điệp được giấu là "ptit"

Nhiệm vụ 4: Chuẩn bị file giả mạo để thay thế

- Để thực hiện thay đổi file khi truyền đi, ta cần chuẩn bị một file với thông điệp khác được ẩn giấu khi đã biết được thuật toán giấu tin từ bài thực hành trước. Từ máy attacker ta thực hiện tạo file txt được giấu tin bằng file encrypt.py:

Python3 encrypt.py

- Sau khi chạy xong sẽ xuất hiện file encrypt1.txt với thông điệp được giấu là "pt" , đây sẽ là file mà ta muốn thay đổi khi user1 chuyển file encrypt.txt sang cho user2 bằng ftp làm cho user2 không nhận được thông điệp mà user1 muốn gửi

Nhiệm vụ 5: Chỉnh sửa file tấn công

- Sau khi đã chuẩn bị xong file txt, ta cần thực hiện thay đổi 1 số tham số trong file attack.py ở các dòng:

FTP_SERVER = <ip ftp_server>
FTP_USER = <username>
FTP_PASS = <password>
FAKE_FILE = <tên file giả mạo>

- Sau khi sửa đổi xong lưu lại thực hiện đọc lại file để kiểm tra và chạy file bằng lệnh:

cat attack.py
sudo python3 attack.py

Nhiệm vụ 6: Thực hiện tấn công

- Thực hiện ftp đến user2 từ user1:

ftp 172.22.2.2

- Sau khi đăng nhập thành công thực hiện chuyển file encrypt.txt qua cho user2:

put encrypt.txt

- Quan sát trên máy attacker xem đã thực hiện thay đổi file encrypt.txt thành encrypt1.txt thành công hay chưa.

Nhiệm vụ 7: Giải mã

- Bây giờ ta sẽ tiến hành kiểm tra xem file đã được gửi qua chưa bằng lệnh:

ls

- Ta có thể thấy xuất hiện file encrypt.txt giống tên file mà user1 gửi qua với thông điệp là "ptit", thực hiện giải mã bằng file decrypt.py:

python3 decrypt.py

- Sau khi giải mã có thể thấy thông điệp lại là "pt" của file encrypt1.txt, thực hiện tấn công thành công.

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-3