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-3

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-3

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 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

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-3.tar

Khởi động bài lab:

Vào terminal, gõ :

labtainer -r lss-lab-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

- Sau khi đã bắt được log từ user1 thực hiện giấu tin bằng file encrypt.py :

python3 encrypt.py

- Sau khi chạy xong sẽ xuất hiện file output.pdf với thông điệp được giấu là i_am_ptiter

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 pdf được giấu tin bằng file encrypt.py:

python3 encrypt.py

- Sau khi chạy xong sẽ xuất hiện file fake_output.pdf với thông điệp được giấu là you_are_hacked , đây sẽ là file mà ta muốn thay đổi khi user1 chuyển file output.pdf 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 pdf, 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 và chạy file bằng lệnh :

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 output.pdf qua cho user2 :

put output.pdf

- Quan sát trên máy attacker xem đã thực hiện thay đổi file output.pdf thành fake_output.pdf 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:

ls

- Ta có thể thấy xuất hiện file output.pdf giống tên file mà user1 gửi qua với thông điệp là i_am_ptiter, thực hiện giải mã bằng file decrypt.py:

python3 decrypt.py

- Sau khi giải mã có thể thấy thông điệp lại là you_are_hacked của file fake_output.pdf, 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 lss-lab-3