Bài thực hành: Phát hiện giấu tin trong trường định danh IPv4

1. Khái quát chung

1.1. Tổng quan

Bài lab này hướng dẫn sinh viên cách phát hiện và trích xuất thông điệp bí mật được giấu trong trường Identification (ID) của gói tin IPv4. Đây là một kỹ thuật giấu tin trong header giao thức, tận dụng trường IP ID để nhúng thông điệp mà không làm thay đổi nội dung gói tin, khiến việc phát hiện trở nên khó khăn hơn.

1.2. Mô tả

- Gửi 100 gói tin, trong đó một số gói tin chứa thông điệp ẩn (đọc từ file .txt).
- Mỗi gói tin chứa thông điệp có IP Identification với 8 bit cao là ASCII của ký tự, 8 bit thấp dùng để đánh dấu vị trí.
- Các gói tin chứa thông điệp được gửi ở vị trí ngẫu nhiên, giữ thứ tự trước sau.
- Các gói tin còn lại là nhiễu.

1.3. Mục tiêu của bài lab

- Hiểu được cách giấu tin trong header gói tin IPv4 bằng cách kiểm soát trường Identification.
- Sử dụng Scapy để trích xuất IP ID và giải mã thông điệp.

1.4. Yêu cầu đối với sinh viên

- Sinh viên đã có kiến thức về giấu tin trong mạng, hiểu về cấu trúc gói tin IP và trường ID của tiêu đề IP.
- Có kiến thức cơ bản về hệ điều hành Linux.

2. Chuẩn bị môi trường thực hành

Mở terminal, trong thư mục labtainer-student, bắt đầu bài thực hành bằng lệnh:

labtainer -r stego-detect-identification_ipv4

*(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)*

Kiểm tra các bài tập phải làm trong bài thực hành

Checkwork

3. Nội dung thực hành

3.1. Gửi gói tin chứa thông điệp bí mật

Kiểm tra các file có sẵn trên máy sender: *ls*

Thực hiện tạo thông điệp bí mật chứa trong file *message.txt*. Ví dụ:

echo "PTIT" > message.txt

hoặc có thể thể dụng **nano, vim** để mở trình soạn thảo văn bản rồi nhập thông điệp bí mật vào đó.

3.2. Thiết lập cảnh báo phát hiện giấu tin

Trên máy receiver, chạy lệnh:

sudo python3 alert_detect.py

Quay trở lại bước **3.1**, tại máy **sender**, thực hiện gửi 100 gói tin có chứa các gói tin mà trong đó có thông điệp được giấu trong đó.

sudo python3 sender.py

Lúc này trên máy receiver sẽ xuất hiện các cảnh báo về các gói tin chứa thông điệp ẩn trong đó.

3.3. Giải mã thông điệp bí mật được giấu

Bên máy receiver, chạy lệnh:

python3 decrypt.py

Quan sát nội dung của cảnh báo bên trên, sẽ thấy có các giá trị IP ID kèm theo từng cảnh báo. Sau đó, nhập các giá trị IP ID, **cách nhau bằng dấu phẩy** (***chú ý**: nhập theo đúng thứ tự từ trên xuống dưới*), rồi nhấn Enter để giải mã thông điệp.

- Kết quả mong đợi: Tìm ra được hide message.

4. Kết thúc bài lab

- **Kết thúc bài lab:**
    - Kiểm tra checkwork:

      checkwork

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

      stoplab

    - Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.
- **Khởi động lại bài lab:**
    - Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

      labtainer -r stego-detect-identification_ipv4