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

BÁO CÁO THỰC HÀNH

ĐỀ TÀI: dct-dwt-steganography-sniff-lab

Mã sinh viên: B21DCAT104

Họ và tên: Tô Quang Huy

Nhóm môn học: 03

Giảng viên hướng dẫn: Đinh T. Duy

HÀ NỘI 2025

1. Mục đích

   - Giúp sinh viên hiểu rõ cơ chế và sử dụng thành thạo công cụ dct-dwt-steganography để giấu và tách tin

2. Yêu cầu đối với sinh viên

   - Có kiến thức về kĩ thuật giấu tin trong hình ảnh bằng dct và dwt.
   - Tìm hiểu về dct và dwt.

3. Nội dung thực hành

3.1. Khởi động bài lab

Vào terminal gõ:

labtainer stego-sniff-lab -r

Ba terminal ảo sẽ hiện lên, terminal server, terminal client và teminal attacker. Trước tiên hãy kiểm tra kết nối giữa ba máy bằng cách ping.

3.2. Giấu tin vào ảnh

Trên terminal server, khởi động server để chạy tool dùng:

cd dct-dwt-steganography

python3 -m http.server 8000

Trên terminal client, truy cập vào tool dùng:

firefox http://192.168.10.3:8000

Chọn tệp ảnh vừa tải và phần text to encode điền secret và ấn encode để giấu tin. Tải ảnh ở phần output về và đặt tên là output.png

3.3. Bắt tin

Client và server giao tiếp trực tiếp với nhau qua mạng bridge.

Đầu tiên dùng arpspoof để ép lưu lượng đi qua attacker. Trên terminal attacker, bạn có thể dùng: sudo arpspoof -i eth0 -t 192.168.10.2 192.168.10.3 > arpspoof.stdout 2>&1

Câu lệnh trên sẽ nói với client rằng attacker là server.

Ở một terminal khác của attacker dùng:

sudo arpspoof -i eth0 -t 192.168.10.3 192.168.10.2

Câu lệnh trên sẽ nói với server rằng attacker là client.

Ở một terminal khác của attacker bật IP forwarding dùng:

sudo sysctl -w net.ipv4.ip_forward=1

Nếu không bật, gói tin sẽ bị attacker giữ lại chứ không forward tiếp, làm ngắt kết nối giữa 2 máy.

3.4. Bắt gói tin

Trên attacker dùng tcpdump để bắt các gói tin và lưu vào file capture,pcap:

tcpdump -i eth0 -w capture.pcap

Trên terminal client setup một http server để server tải file output.png về:

python3 -m http.server 8000

Trên terminal server tải file về dùng wget:

wget http://192.168.10.2:8000/output.png

Trên terminal attacker dừng bắt gói tin và dùng wireshark để mở file capture.pcap:

wireshark capture.pcap

Trong thanh menu, chọn: File → Export Objects → HTTP. Cửa sổ hiện ra sẽ liệt kê tất cả các tệp HTTP được truyền trong gói tin. Tìm đến tệp output.png → chọn nó → bấm Save để lưu lại.

Truy cập vào tool giấu tin được chạy trên server: firefox http://192.168.10.3:8000

Chọn lại ảnh là output.png vừa tải và ấn decode. Tạo 1 file decode.txt chứa thông tin mật ở phần output và cat ra màn hình.

3.5. Kết quả đặt được

Kết quả cần đạt được

Chạy được tất cả các bước như yêu cầu.

Yêu cầu nộp file kết quả

Cần nộp 1 file: trong thư mục: /home/student/labtainer_xfer/TÊN_BÀI_LAB (tên tài khoản.TÊN_BÀI_LAB.lab)

Kết thúc bài lab:

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

stoplab stego-sniff-lab

Khi bài lab kết thúc, một tệp lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.

Sinh viên cần nộp file .lab để chấm điểm.

Để kiểm tra kết quả khi trong khi làm bài thực hành sử dụng lệnh: checkwork <tên bài thực hành>

Khởi động lại bài lab: Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

labtainer stego-sniff-lab -r