HƯỚNG DẪN LAB: img-stego-att2-tool

1. Mục đích

Bài lab này hướng dẫn sinh viên thực hiện mô phỏng một cuộc tấn công Man-in-the-Middle (MITM) trong mạng nội bộ nhằm chặn, phân tích và ngăn cản quá trình truyền ảnh có chứa thông tin được giấu giữa hai container. Qua bài lab, sinh viên sẽ:

- Thực hành giấu tin vào ảnh bằng công cụ Steghide.
- Thực hành bắt gói tin và ngăn chặn truyền dữ liệu bằng arpspoof và iptables.
- Phân tích kết quả khi dữ liệu bị chặn và thử lại quá trình giải mã sau khi bỏ chặn.
- Hiểu rõ tác động của tấn công MITM trong việc bảo vệ thông tin.

2. Yêu cầu đối với sinh viên

Trước khi thực hiện bài lab này, sinh viên cần:

- Có kiến thức cơ bản về dòng lệnh Linux.
- Hiểu khái niệm về Steganography, MITM và vai trò của iptables.
- Biết cách sử dụng Labtainer để chạy lab nhiều container song song.

3. Nội dung lý thuyết

3.1. Steganography và Steghide

Steganography là kỹ thuật giấu dữ liệu vào trong các file đa phương tiện như ảnh hoặc âm thanh mà không gây nghi ngờ. Steghide là công cụ phổ biến cho việc giấu và trích xuất dữ liệu với hỗ trợ mã hóa bằng mật khẩu.

3.2. IP Forwarding, arpspoof và iptables

Tấn công MITM thường dựa vào việc giả mạo địa chỉ MAC giữa các thiết bị mạng, điều này có thể thực hiện qua công cụ arpspoof. Để kiểm soát luồng gói tin sau khi giả mạo thành công, attacker dùng iptables để chặn hoặc chuyển hướng gói tin tùy ý. Tắt IP forwarding sẽ khiến gói tin không được định tuyến tiếp, kết hợp với iptables để chủ động chặn hoàn toàn việc truyền dữ liệu.

---

4. Nội dung thực hành

4.1. Khởi động Lab

Khởi động bài lab bằng lệnh:

labtainer img-stego-att2-tool

5. Các nhiệm vụ thực hành

Nhiệm vụ 1: Tạo ảnh chứa tin

Trong container sender, tạo file chứa thông điệp:

wget https://icdn.dantri.com.vn/a3HWDOlTcvMNT73KRccc/Image/2013/12/A1-0fe0d.jpg -O input.jpg

echo "Đây là thông điệp bí mật" > secret.txt

Sau đó giấu tin vào ảnh:

steghide embed -cf input.jpg -ef secret.txt

Ghi nhớ mật khẩu để phục vụ cho việc giải mã.

Nhiệm vụ 2: Tắt IP forwarding và bật arpspoof

Trong container attacker, sử dụng tmux để chạy 3 phiên :

tmux

Sử dụng Ctrl+b +% để tạo phiên mới. Ctrl + ↑ → ↓ ← để di chuyển giữa các phiên

Hai phiên đầu chạy arpspoof để định tuyến lưu lượng qua attacker

sudo arpspoof -i eth0 -t [ip sender] [ip receiver]
sudo arpspoof -i eth0 -t [ip receiver] [ip sender]

Sau đó ở phiên thứ 3 tắt ipforward để không cho chuyển tiếp gói tin

sudo sysctl -w net.ipv4.ip_forward=0

Nhiệm vụ 3: Chặn gói tin giữa sender và receiver bằng iptables

Ở phiên thứ 3 của Attacker chặn gói tin giữa hai máy bằng các lệnh:

sudo iptables -A FORWARD -s [ip sender] [ip receiver] -j DROP
sudo iptables -A FORWARD -s [ip receiver] [ip sender] -j DROP

Kiểm tra rule đã thêm:

sudo iptables -L FORWARD -v -n

Ghi chú: -A để chặn, -D để bỏ chặn.

Nhiệm vụ 4: Giải mã thử thông điệp từ ảnh bị bắt (không thành công)

Gửi thông tin giữa sender và reiceiver với netcat

Lắng nghe trên reiceiver : nc -l -p 4444 > anh.jpg

Gửi trên sender : nc [ip reiceiver] 4444 < input.jpg

Sau đó thử giải mã thông điệp với mật khẩu :

steghide extract -sf anh.jpg -p matkhau

Không thể giải mã thông điệp

Nhiệm vụ 5: Tắt iptables (bỏ chặn gói tin)

Bỏ chặn kết nối giữa sender và receiver:

sudo iptables -D FORWARD -s [ip sender] [ip receiver] -j DROP
sudo iptables -D FORWARD -s [ip receiver] [ip sender] -j DROP

Kiểm tra lại:

sudo iptables -L FORWARD -v -n

Lúc này chain FORWARD sẽ không còn rule chặn nữa.

Nhiệm vụ 6: Gửi lại ảnh và giải mã thành công

Bỏ chặn và gửi lại thông điệp và giải mã.Sẽ giải mã thành công được thông điệp.

6. Kết thúc bài lab

Sau khi hoàn tất các nhiệm vụ, sử dụng lệnh:

checkwork

Để dừng bài lab:

Stoplab

Để khởi động lại lab:

labtainer -r img-stego-att2-tool