Hướng Dẫn Lab Echo Brute-Force

Giới Thiệu

Lab Echo Brute-Force là một bài tập kết hợp kỹ thuật giấu tin (steganography) và tấn công brute-force trong an ninh mạng. Trong lab này, bạn sẽ học cách nhúng một thông điệp bí mật vào file âm thanh bằng công cụ Steghide, sau đó thực hiện tấn công brute-force bằng Stegseek để tìm mật khẩu và trích xuất thông điệp. Lab được thực hiện trong môi trường Labtainer, sử dụng hai container: Attacker (máy tấn công) và Victim (máy chứa file âm thanh).

Hướng dẫn này cung cấp các bước chi tiết để khởi động lab, giấu tin, kiểm tra IP, tải file âm thanh, tấn công brute-force, trích xuất thông điệp, và xác minh kết quả.

Điều Kiện Tiên Quyết

- **Môi Trường Labtainer**: Cần cài đặt Labtainer trên hệ thống (Linux, macOS, hoặc Windows với Docker). Xem hướng dẫn cài đặt tại [Labtainers GitHub](https://github.com/mfthomps secondly/Labtainers) nếu chưa cài.
- **Lệnh Linux Cơ Bản**: Hiểu cách sử dụng các lệnh như `echo`, `steghide`, `wget`, `cat`, và `python3`.
- **Công Cụ Steghide**: Công cụ giấu tin trong file âm thanh hoặc hình ảnh. Đảm bảo Steghide có sẵn trong môi trường Labtainer (kiểm tra bằng `steghide --version`).
- **Công Cụ Stegseek**: Công cụ tấn công brute-force để tìm mật khẩu file giấu tin. Đảm bảo Stegseek có sẵn (kiểm tra bằng `stegseek --version`).
- **Danh Sách Mật Khẩu**: File `rockyou.txt` (danh sách mật khẩu phổ biến) cần có sẵn để tấn công brute-force.
- **Truy Cập Terminal**: Sử dụng terminal để tương tác với môi trường Labtainer, bao gồm cả container Attacker và Victim.

Hướng Dẫn Từng Bước

Bước 1: Khởi Động Lab

1. **Chạy Môi Trường Labtainer**:
   - Mở terminal và chạy lệnh sau để khởi động lab Echo Brute-Force:
   - `labtainer echo-brute-force`
   - Lệnh này tạo hai container Docker: Attacker (máy tấn công) và Victim (máy chứa file âm thanh). Bạn sẽ được đưa vào terminal của container Attacker.
2. **Kiểm Tra Thiết Lập Lab**:
   - Kiểm tra thư mục hiện tại trong container Attacker bằng lệnh `pwd`. Bạn nên ở trong thư mục chứa các công cụ và file cần thiết.
   - Liệt kê file bằng `ls` để xác nhận có các file như `rockyou.txt` (danh sách mật khẩu) và các công cụ (`steghide`, `stegseek`).

Bước 2: Giấu Tin Vào File Âm Thanh

1. **Tạo File Thông Điệp**:
   - Trong container Victim (nếu cần chuyển sang container Victim, sử dụng lệnh hoặc giao diện Labtainer), tạo file văn bản `secret.txt` chứa thông điệp cần giấu:
   - `echo "secret" > secret.txt`
   - Lệnh này ghi nội dung "secret" vào file `secret.txt`. Kiểm tra nội dung file bằng:
   - `cat secret.txt`
2. **Giấu Tin Bằng Steghide**:
   - Sử dụng công cụ Steghide để nhúng nội dung `secret.txt` vào file âm thanh `input.wav`:
   - `steghide embed -cf input.wav -ef secret.txt -sf secret_enc.wav -p password123`
   - Giải thích lệnh:
     - `-cf input.wav`: File âm thanh đầu vào (cover file).
     - `-ef secret.txt`: File chứa thông điệp cần giấu (embedded file).
     - `-sf secret_enc.wav`: File âm thanh đầu ra chứa thông điệp ẩn (stego file).
     - `-p password123`: Mật khẩu bảo vệ thông điệp.
   - Lệnh này tạo file `secret_enc.wav` chứa thông điệp ẩn.
3. **Kiểm Tra Kết Quả Giấu Tin**:
   - Kiểm tra thông tin file `secret_enc.wav` để xác nhận thông điệp đã được giấu thành công:
   - `steghide info secret_enc.wav`
   - Lệnh này hiển thị thông tin về file, như kích thước dữ liệu ẩn và yêu cầu mật khẩu. Nhập `password123` khi được yêu cầu để xem chi tiết.

Bước 3: Kiểm Tra Địa Chỉ IP Của Container Victim

1. **Khởi Động Máy Chủ HTTP**:
   - Trong container Victim, khởi động một máy chủ HTTP để chia sẻ file `secret_enc.wav`:
   - `python3 -m http.server 8080 --bind 0.0.0.0`
   - Lệnh này chạy máy chủ HTTP trên cổng 8080, cho phép truy cập file từ container Attacker.
   - Ghi lại địa chỉ IP của container Victim (ví dụ: `192.168.12.11`). Bạn có thể kiểm tra IP bằng lệnh `ifconfig` hoặc `ip addr` trong container Victim.
2. **Xác Minh Máy Chủ**:
   - Trong container Attacker, kiểm tra xem máy chủ Victim có hoạt động không bằng cách sử dụng `curl` hoặc trình duyệt (nếu Labtainer hỗ trợ):
   - `curl http://192.168.12.11:8080`
   - Nếu thành công, bạn sẽ thấy danh sách file, bao gồm `secret_enc.wav`.

Bước 4: Truy Cập Và Tải File Âm Thanh

1. **Tải File Âm Thanh**:

- Trong container Attacker, sử dụng `wget` để tải file `secret_enc.wav` từ máy chủ Victim:
- `wget http://192.168.12.11:8080/secret_enc.wav`
- Lệnh này tải file `secret_enc.wav` về thư mục hiện tại trong container Attacker.
- Kiểm tra file đã tải bằng:
- `ls secret_enc.wav`

Bước 5: Tấn Công Brute-Force Để Tìm Mật Khẩu

1. **Chạy Tấn Công Brute-Force**:
   - Sử dụng công cụ Stegseek để thực hiện tấn công brute-force nhằm tìm mật khẩu của file `secret_enc.wav`:
   - `stegseek secret_enc.wav rockyou.txt`
   - Giải thích lệnh:
     - `secret_enc.wav`: File âm thanh chứa thông điệp ẩn.
     - `rockyou.txt`: Danh sách mật khẩu phổ biến để thử.
   - Stegseek sẽ thử từng mật khẩu trong `rockyou.txt` cho đến khi tìm được mật khẩu đúng (ví dụ: `password123`). Khi tìm thấy, Stegseek sẽ hiển thị mật khẩu và trích xuất thông điệp vào file (ví dụ: `secret_enc.wav.out`).
2. **Trích Xuất Thông Điệp**:
   - Nếu Stegseek tìm được mật khẩu, sử dụng Steghide để trích xuất thông điệp từ `secret_enc.wav`:
   - `steghide extract -sf secret_enc.wav -p password123`
   - Lệnh này trích xuất thông điệp vào file `secret.txt` (hoặc tên file khác, tùy cấu hình).
   - Nếu Stegseek đã tự động trích xuất, bạn có thể bỏ qua bước này.
3. **Xem Nội Dung Thông Điệp**:
   - Hiển thị nội dung file thông điệp đã trích xuất:
   - `cat secret.txt`
   - Nội dung nên hiển thị thông điệp gốc (ví dụ: "secret").

Bước 6: Kiểm Tra Kết Quả

1. **Xác Minh Công Việc**:
   - Chạy lệnh kiểm tra của Labtainer để đánh giá kết quả:
   - `checkwork echo-brute-force`
   - Lệnh này kiểm tra tiến độ lab, xác nhận xem bạn đã trích xuất được thông điệp đúng hay không.
   - Xem kết quả để biết phản~~ phản hồi (ví dụ: “Lab hoàn thành thành công” hoặc lỗi chỉ ra vấn đề).

Bước 7: Khởi Động Lại Lab (Tùy Chọn)

1. **Đặt Lại Môi Trường Lab**:
   - Nếu cần khởi động lại lab (ví dụ: để thử lại hoặc xóa công việc trước), sử dụng:
   - `labtainer -r echo-brute-force`
   - Lệnh này đặt lại các container lab về trạng thái ban đầu, xóa mọi thay đổi.

    - Bắt đầu lại từ Bước 1 để lặp lại lab.

Giải Thích

- **Kỹ Thuật Giấu Tin (Steganography)**: Steghide nhúng dữ liệu (ví dụ: nội dung `secret.txt`) vào file âm thanh hoặc hình ảnh mà không làm thay đổi đáng kể nội dung gốc. Mật khẩu bảo vệ dữ liệu ẩn, yêu cầu nhập đúng mật khẩu để trích xuất.
- **Tấn Công Brute-Force**: Stegseek thử lần lượt các mật khẩu từ danh sách (như `rockyou.txt`) để tìm mật khẩu đúng, tận dụng sức mạnh tính toán để phá mã.
- **Labtainer**: Một nền tảng cho các bài tập an ninh mạng, cung cấp môi trường cách ly với hai container (Attacker và Victim) để mô phỏng kịch bản tấn công thực tế.
- **Công Cụ**:
    - `steghide`: Công cụ giấu tin và trích xuất dữ liệu từ file âm thanh/hình ảnh.
    - `stegseek`: Công cụ tấn công brute-force chuyên dụng cho file giấu tin.
    - `wget`: Công cụ tải file qua HTTP.
    - `rockyou.txt`: Danh sách mật khẩu phổ biến, thường được sử dụng trong tấn công brute-force.