Lab: Tấn công Brute-force bằng giấu tin

Khởi động bài lab:

Labtainer echo-brute-force

1. Giấu tin vào tệp ảnh hoặc âm thanh

- Tạo tệp tin chứa thông tin mô tả: Lệnh này tạo một tệp tin tên secret.txt và ghi nội dung "secret" vào tệp:

```
echo "secret" > secret.txt
```

- .Chọn tệp âm thanh dùng để giấu tin:

```
steghide embed -cf input.wav -ef secret.txt -sf secret_enc.wav -p password123
```

- Mô tả: Lệnh này sử dụng công cụ steghide để giấu nội dung của secret.txt vào tệp âm thanh input.wav, tạo ra tệp secret_enc.wav với mật khẩu password123.
- Kiểm tra kết quả:

```
steghide info secret_enc.wav
```

- Mô tả: Lệnh này kiểm tra thông tin về tệp secret_enc.wav để xác nhận rằng nội dung đã được giấu thành công.

2. Kiểm tra địa chỉ IP của container Victim

- Chạy lệnh để kiểm tra địa chỉ IP từ máy Attacker:

```
python3 -m http.server 8080 --bind 0.0.0.0
```

- Mô tả: Lệnh này khởi động một máy chủ HTTP trên cổng 8080, lắng nghe trên tất cả các địa chỉ IP.

3. Thử truy cập bằng địa chỉ IP trực tiếp

- Sử dụng IP trực tiếp để truy cập tệp:

```
wget http://192.168.12.11/secret_enc.wav
```

- Mô tả: Lệnh này sử dụng công cụ wget để tải tệp secret_enc.wav từ địa chỉ IP 192.168.12.11.

4. Tấn công brute-force để tìm mật khẩu

- Tấn công brute-force vào tệp âm thanh:

stegseek audio.wav rockyou.txt

Mô tả: Lệnh này sử dụng công cụ stegseek để thực hiện tấn công brute-force vào tệp audio.wav bằng cách sử dụng danh sách mật khẩu rockyou.txt.

- Giải nén thông tin từ âm thanh nếu tìm được mật khẩu:

steghide extract -sf audio.wav -p [mật khẩu tìm được]

Mô tả: Lệnh này sử dụng công cụ steghide để giải nén thông tin từ tệp audio.wav bằng mật khẩu tìm được.

Xem nội dung file giải mã

cat secret.txt

5. kiểm kết quả

- Checkwork echo-brute-force

Khởi động lại bài lab:

Labtainer -r echo-brute-force