T1110: Brute Force

1. **Mục đích**

Giúp sinh viên tìm hiểu được thế nào là Brute Force, cách dung Hydra để thực hiện một cuộc tấn công đơn giản nhằm tìm được mật khẩu đúng nhằm truy cập tới máy mục tiêu.

2. **Yêu cầu đối với sinh viên**

Có kiến thức cơ bản về hệ điều hành Linux, biết sử dụng ssh cơ bản công cụ Hydra. Sinh viên cần thực hiện tìm hiểu thêm kiến thức về Hydra.

3. **Nội dung thực hành**

Khởi động bài lab:

Vào terminal, gõ:

labtainer pen_tool_mitre_t1110

(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 máy là **attacker**, một máy là **victim**. Trên terminal **attacker** đã được cung cấp sẵn một file password_list.txt có chứa danh sách mật khẩu phổ biến dễ bị tấn công, sinh viên sẽ sử dụng file này làm để brute force bằng Hydra.

- Bước 1: Trên máy Victim, sinh viên kiểm tra địa chỉ IP của máy bằng câu lệnh:

ifconfig

- Bước 2: Sinh viên sử dụng Hydra với password_list.txt để cố gắng ssh đến máy victim với cú pháp:

hydra -l <username> -P /path/to/passwords.txt ssh://<ip_victim>

- Bước 3: Sinh viên sử dụng password đúng sau khi tìm được ở trên để ssh đến

máy victim:

ssh <ip_victim>

Kiểm tra kết quả:

Tại terminal ban đầu, sử dụng câu lệnh sau để có thể kiểm tra kết quả bài làm:

checkwork

Kết thúc bài lab:

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

stoplab pen_tool_mitre_t1110

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 pen_tool_mitre_t1110