**Nội dung và hướng dẫn bài thực hành**

***Mục đích***

Mục đích của bài lab này là giúp sinh viên hiểu và thực hành kỹ thuật Credential Dumping, nhằm thu thập thông tin đăng nhập từ các hệ thống hoặc cơ sở dữ liệu. Sinh viên sẽ học cách tìm kiếm và phân tích các tệp cơ sở dữ liệu chứa thông tin người dùng, dump dữ liệu, giải mã mật khẩu, và thử đăng nhập vào hệ thống. Bài lab cũng giúp sinh viên nhận thức về các rủi ro bảo mật, đồng thời nghiên cứu các biện pháp phòng ngừa như mã hóa mật khẩu và xác thực đa yếu tố để bảo vệ hệ thống khỏi các cuộc tấn công.

***Yêu cầu đối với sinh viên***

Sinh viên cần có kiến thức cơ bản về bảo mật mạng, kỹ năng sử dụng công cụ bảo mật như sqlite3 và curl, hiểu về cơ sở dữ liệu SQLite, tuân thủ đạo đức trong bảo mật, phân tích rủi ro bảo mật và áp dụng biện pháp phòng ngừa như mã hóa mật khẩu và xác thực đa yếu tố (MFA).

***Nội dung thực hành***

*imodule https://github.com/ParadoxParadise/labattt-2025/raw/refs/heads/main/pen-bsic-credentialdump/imodule.tar*

Khởi động bài lab:

Vào terminal, gõ:

*labtanier pen\_bsic\_credentialdump*

*(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, một terminal ảo sẽ xuất hiện. Sinh viên sẽ thực hiện khai thác lỗ hổng Credential Dumping bằng cách sử dụng các công cụ như curl hoặc Postman để gửi các yêu cầu HTTP và truy xuất thông tin đăng nhập từ hệ thống mục tiêu. Cụ thể, sinh viên sẽ tìm kiếm và phân tích các tệp cơ sở dữ liệu chứa thông tin đăng nhập, sau đó sử dụng các lệnh SQL để trích xuất dữ liệu từ các bảng đăng nhập. Sinh viên cần giải mã mật khẩu đã mã hóa trong cơ sở dữ liệu và thử đăng nhập vào ứng dụng web để kiểm tra quyền truy cập với thông tin thu thập được. Nếu thành công, sinh viên cần ghi nhận kết quả và phân tích các nguy cơ bảo mật có thể xảy ra, ví dụ như lộ thông tin đăng nhập nhạy cảm. Ngoài ra, sinh viên cũng sẽ nghiên cứu các biện pháp bảo mật phòng chống, như mã hóa mật khẩu mạnh hơn, sử dụng các cơ chế xác thực bổ sung và thực hiện kiểm tra quyền truy cập tài nguyên để bảo vệ dữ liệu người dùng khỏi bị xâm phạm.

**Kết thúc bài lab:**

Khi hoàn thành bài lab, sinh viên sẽ sử dụng câu lệnh sau để kết thúc:

*stoplab pen\_bsic\_credentialdump*

Khi bài lab kết thúc, một tệp lưu kết quả sẽ được tạo và lưu vào một vị trí được hiển thị dưới câu lệnh **stoplab**

**Khởi động lại bài lab:**

Trong trường hợp sinh viên cần thực hiện lại bài lab, sử dụng câu lệnh:

*labtainer –r pen\_bsic\_credentialdump*