

**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG
KHOA AN TOÀN THÔNG TIN**



**HỌC PHẦN: MẬT MÃ HỌC CƠ SỞ
MÃ HỌC PHẦN: INT1344**

LAB : firefox_decrypt

Sinh viên thực hiện: Lê Ngọc Đức

Mã sinh viên: B22DCAT092

Tên lớp: 04

Giảng viên hướng dẫn: Đỗ Xuân Chợt

HÀ NỘI 2025

LAB : Firefox_decrypt

1. Mục đích

Giúp sinh viên hiểu và thực hành cách Firefox lưu trữ, mã hóa và giải mã thông tin đăng nhập.

2. Yêu cầu đối với sinh viên

Sử dụng thuần thục hệ điều hành Linux và có kiến thức về mật mã học

3. Nội dung lý thuyết

Cơ chế mã hóa trong Firefox:

- Firefox sử dụng thư viện NSS (Network Security Services).
- Khóa mã hóa được lưu trong file key4.db (trước đây là key3.db).
- Các dữ liệu (username/password) được mã hóa bằng một key đối xứng (symmetric encryption) – AES-CBC.
- Khóa chính (master key) được mã hóa bằng một "khóa bọc" (wrapping key) lưu trong key4.db.
- Nếu người dùng thiết lập master password, thì quá trình truy xuất sẽ cần mật khẩu này để giải mã khóa chính.
- logins.json Chứa username/password đã được mã hóa
- key4.db Chứa khóa mã hóa, được mã hóa bằng master password (nếu có)
- cert9.db Chứa chứng chỉ được NSS sử dụng

4. Nội dung thực hành

Add module file lab:

```
imodule https://github.com/ptit-wibu/labtainer/raw/refs/heads/main/firefox_decrypt.tar
```

Khởi động bài lab:

Vào terminal, gõ :

```
labtainer -r firefox_decrypt
```


(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)

Nhiệm vụ 1: Lưu tài khoản/mật khẩu trong Firefox

Thực hiện mở Firefox bằng cách nhập lệnh:

firefox

Ấn vào  rồi chọn Password, thêm tài khoản và mật khẩu theo ý muốn của bản thân (không giới hạn số lượng tài khoản và mật khẩu)

Sau khi thêm tài khoản và mật khẩu xong, cd tới thư mục `.mozilla/firefox/....default-release` và thực hiện lệnh

`ls -l`


Nhiệm vụ 2: Thực hiện giải mã

- Sau khi hoàn thành bước trên, thoát firefox và thực hiện kiểm tra xem đã có tool giải mã chưa bằng cách:

`ls`

- Tiến hành mở lại tool bằng lệnh `python3 decrypt_firefox`, sau đó lựa chọn có quan sát file logins gốc hay không. Quan sát tài khoản với mật khẩu sau khi được giải mã có trùng với tài khoản và mật khẩu đã tạo hay không

Nhiệm vụ 3: Thực hiện thêm master key

- Ấn vào  rồi chọn Settings, sau đó chọn Privacy & Security, kéo xuống tới phần Passwords, chọn Primary Password.
- Sau khi cài Primary Password, chạy lại tool và nhập Primary Password vào để giải mã:

`python3 decrypt_firefox`

Nhiệm vụ 4: Đọc nội dung file

- Sau khi đã chạy tool sẽ có 1 file `results.txt`, chứa các tài khoản và mật khẩu đã giải mã. Xem file để kiểm tra có trùng với các tài khoản đã lưu không:

`cat results.txt`

Kết thúc bài lab:

o Kiểm tra checkwork:

`checkwork`

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

`stoptlab`

Khởi động lại bài lab:

`labtainer -r firefox_decrypt`