

HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO BÀI TẬP LỚN

**AN TOÀN MẠNG KHÔNG DÂY VÀ DI DỘNG**

**Đề tài:**

**TÌM HIỂU HACKING IOS**

***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

Đặng Xuân Đức AT170612

Hoàng Hữu Ánh AT170604

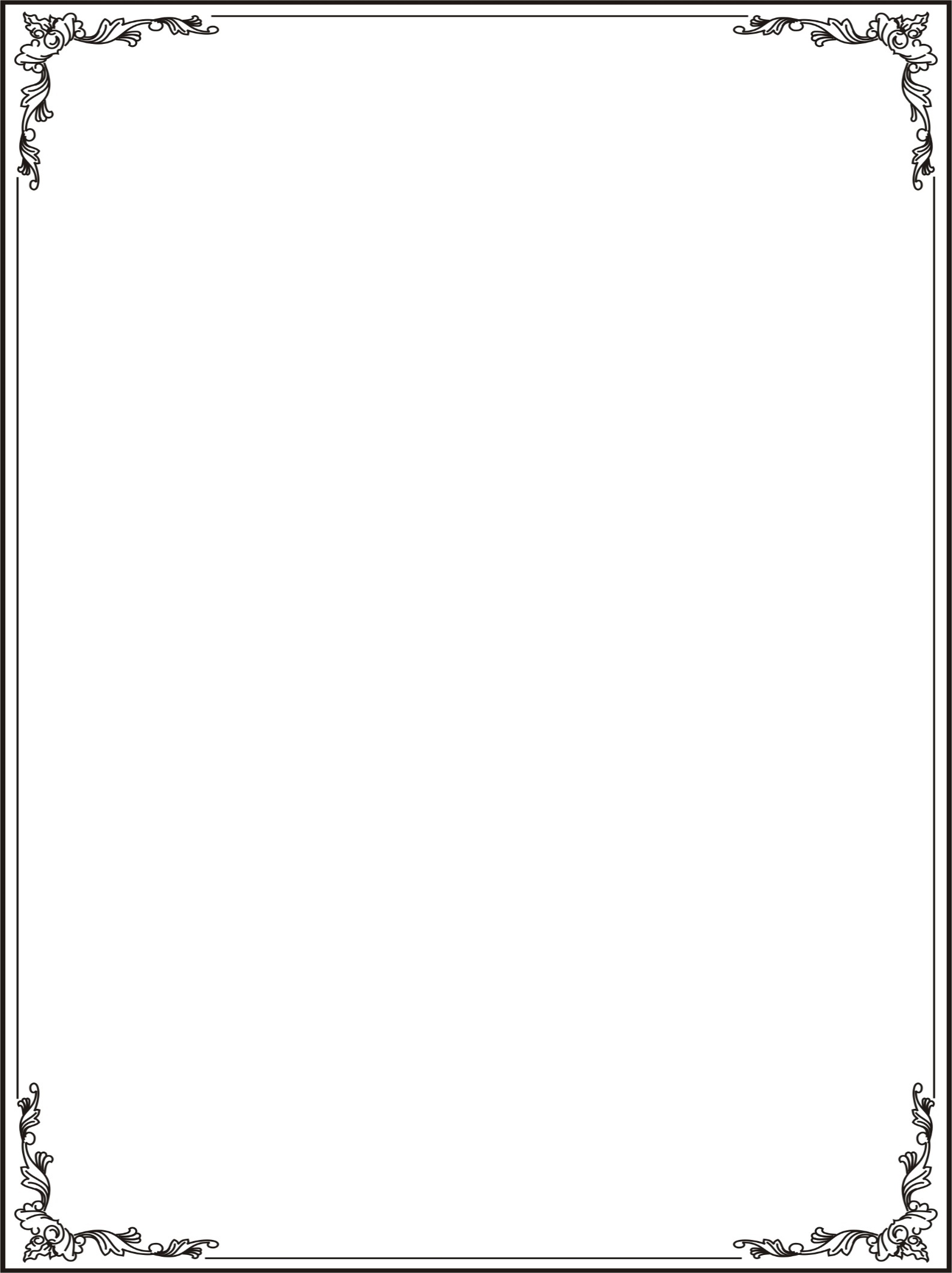
Tạ Quang Chiến AT170607

Phan Văn Hoàng AT170622

Nhóm 12

***Giảng viên hướng dẫn****:* ThS.

Hà Nội, -2023



HỌC VIỆN KỸ THUẬT MẬT MÃ

**KHOA AN TOÀN THÔNG TIN**



BÁO CÁO BÀI TẬP LỚN

**AN TOÀN MẠNG KHÔNG DÂY VÀ DI DỘNG**

**Đề tài:**

**TÌM HIỂU HACKING IOS**

***Nhóm sinh viên thực hiện:*** Vũ Tiến Đạt AT170609

Đặng Xuân Đức AT170612

Hoàng Hữu Ánh AT170604

Tạ Quang Chiến AT170607

Phan Văn Hoàng AT170622

Nhóm 12

***Giảng viên hướng dẫn****:* ThS.

Hà Nội, 2023

# MỤC LỤC

# LỜI CẢM ƠN

Nhóm chúng em xin gửi lời cảm ơn chân thành tới cô giáo trong Khoa Công nghệ thông tin đã tạo điều kiện thuận lợi cho nhóm em trong quá trình thực hiện đề tài.

Chúng em xin gửi lời cảm ơn đặc biệt đến Thạc sĩ thầy: đã nhiệt tình hướng dẫn và chỉ bảo nhóm trong suốt thời gian thực hiện để tài, giúp chúng em có thể hoàn thành tốt đề tài chuyên đề cơ sở lần này.

|  |  |
| --- | --- |
| **GIẢNG VIÊN HƯỚNG DẪN** | **NHÓM SINH VIÊN THỰC HIỆN** |
|  | Vũ Tiến Đạt |
|  | Đặng Xuân Đức |
|  | Hoàng Hữu Ánh |
|  | Tạ Quang Chiến |
|  | Phan Văn Hoàng |

# LỜI MỞ ĐẦU

**1. Tính cấp thiết của đề tài.**

**2. Mục tiêu nghiên cứu của đề tài**

Nghiên cứu hacking iOS.

**3. Đối tượng và phạm vi nghiên cứu**

Đối tượng: điện thoại di động

Phạm vi: Nghiên cứu các phương pháp, công cụ và kỹ thuật để thiết kế, triển khai và thực thi các kịch bản hacking iOS.

**4. Các nhiệm vụ chính cần thực hiện**

Nội dung nghiên cứu được tập trung vào các nội dung chính như sau:

- Khảo sát, tổng hợp kiến thức nền tảng về iOS

- Thiết kế và triển khai các kịch bản

- Thực thi các kịch bản

- Đánh giá và báo cáo kết quả

- Cài đặt, thử nghiệm, đánh giá

**5. Kết quả dự kiến**

**Lý thuyết:**

**Thực nghiệm:**

# TỔNG QUAN VỀ IOS

## Tổng quan về Apple IOS

### Khái niệm

### Cấu trúc

### Vai trò

## Tổng quan về Hacking mobile

### Mobile Platform attack vector

### Owasp top 10 mobile risk

### Cấu trúc một cuộc tấn công thiết bị di động

# KỸ THUẬT KHAI THÁC IOS

## Ios Jailbreaking

### Jailbreaking iOS

### Phân loại Jailbreaking

### Công cụ Jailbreaking checkra1n

## Tấn công thiết bị iOS

### Kỹ thuật SSL pinning bypass

### Insecure Local data Storage

### Fingerprint Bypass

## Tool pentest Objection

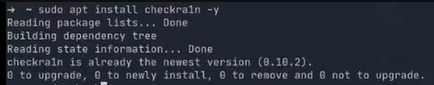
# THỰC NGHIỆM

### Chuẩn bị

Cài đặt xcode

Cài đặt DVIA

Máy kali cài đặt checkta1n

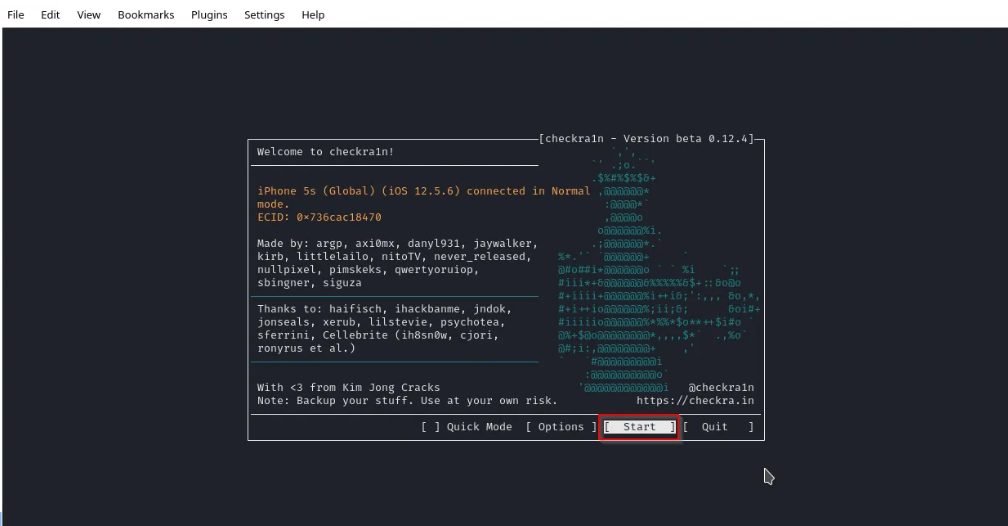


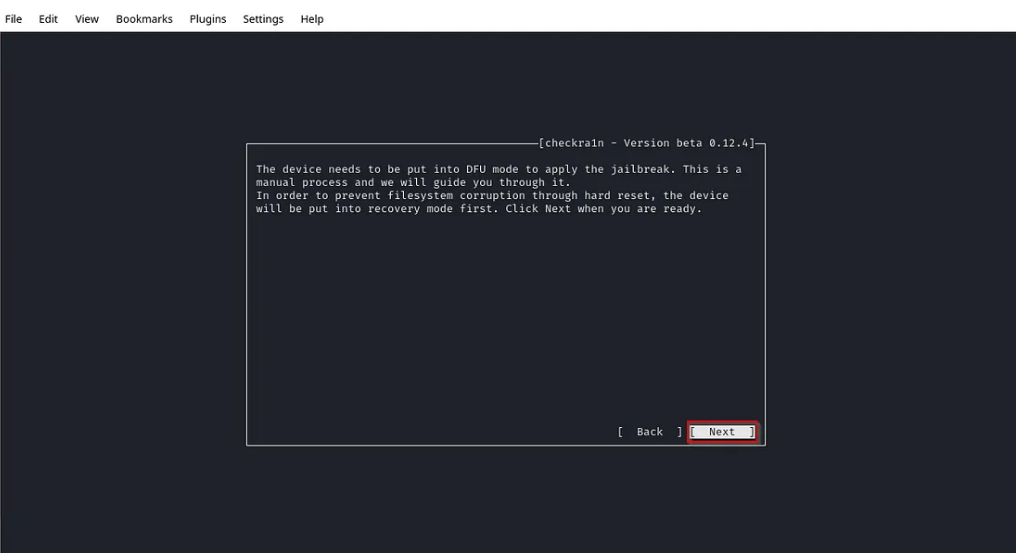
## Kịch bản Ios Jailbreaking

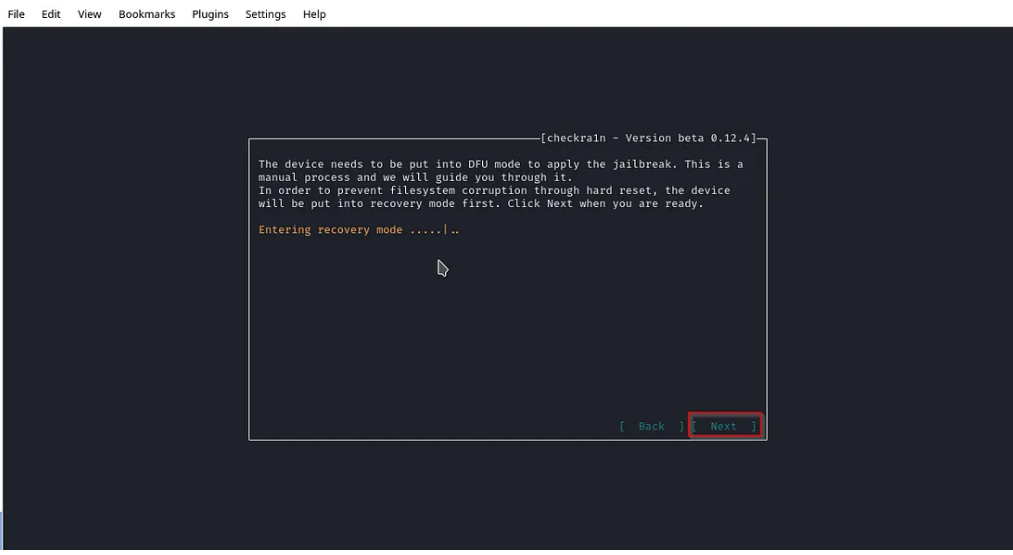
Kết nối thiết bị iOS với máy kali thông qua ssh: ssh root@ mật khẩu là Alpine

Mở terminal trên máy kali chạy lệnh *sudo checkra1n* để khởi động công cụ checkra1n

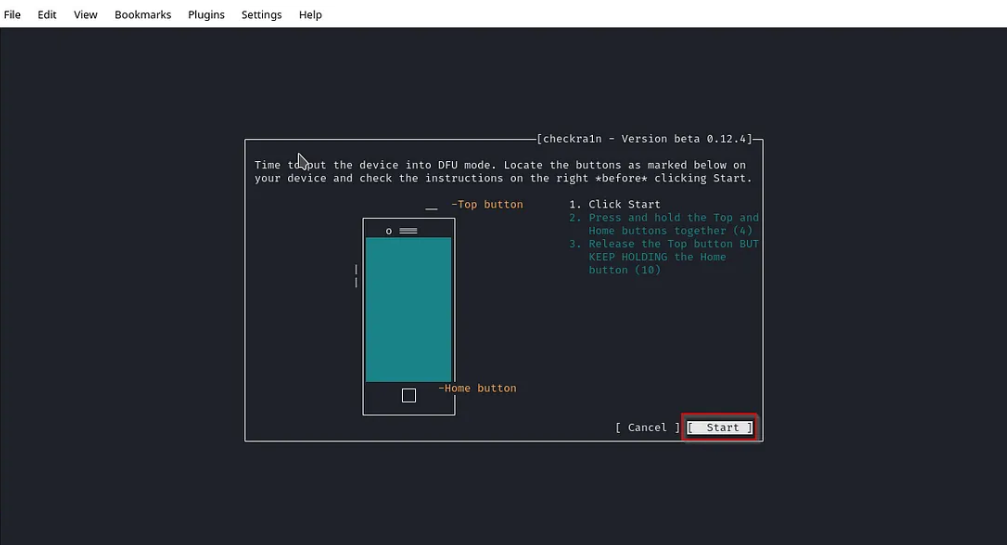
Nhấp vào nút “Bắt đầu” trong giao diện checkra1n. Điều này sẽ đưa thiết bị của bạn vào chế độ phục hồi.

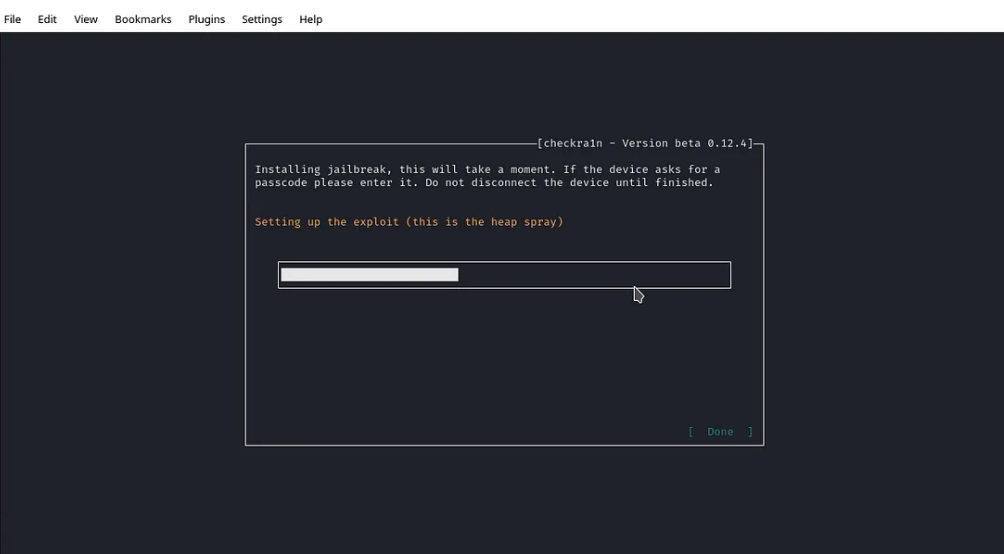




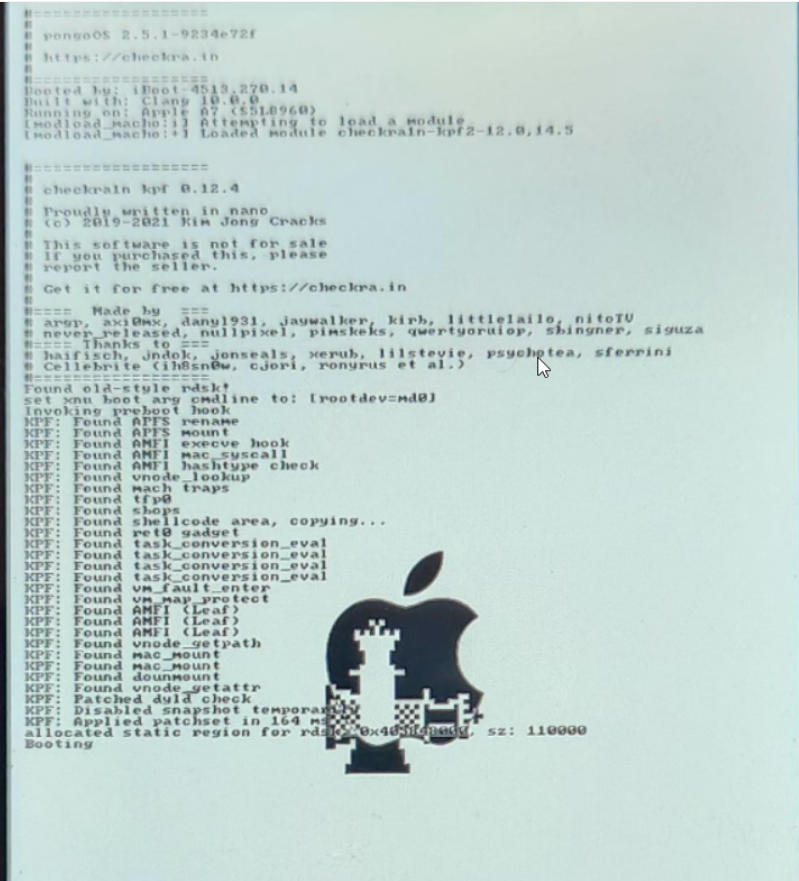


Làm theo hướng dẫn trên màn hình để đưa thiết bị của bạn vào chế độ DFU (Cập nhật chương trình cơ sở thiết bị).

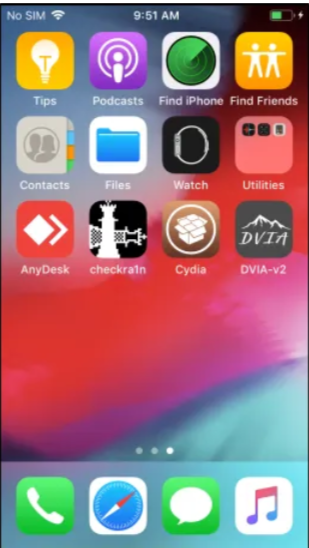




Quá trình bẻ khóa sẽ bắt đầu và thiết bị sẽ được khởi động lại sau khi hoàn tất.



Sau khi thiết bị của bạn khởi động lại sau khi bẻ khóa, bạn sẽ thấy biểu tượng ứng dụng checkra1n trên màn hình chính.



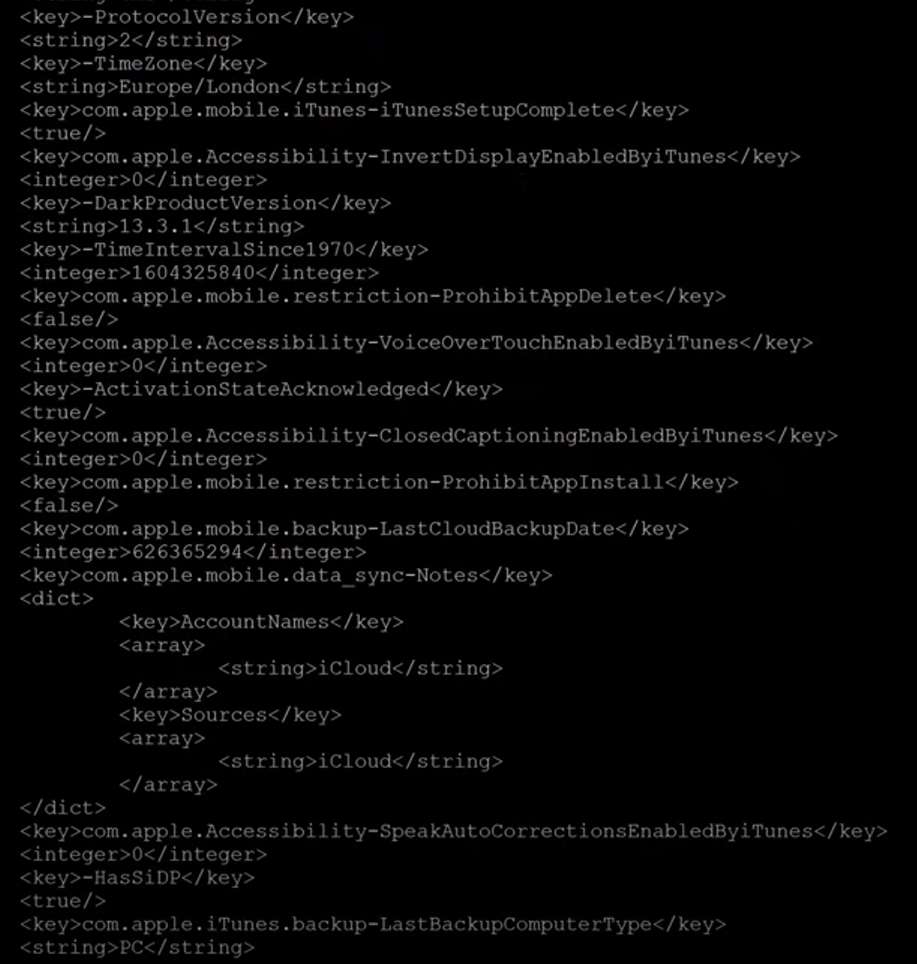
## Kịch bản hacking ios

### Insecure Local data Storage

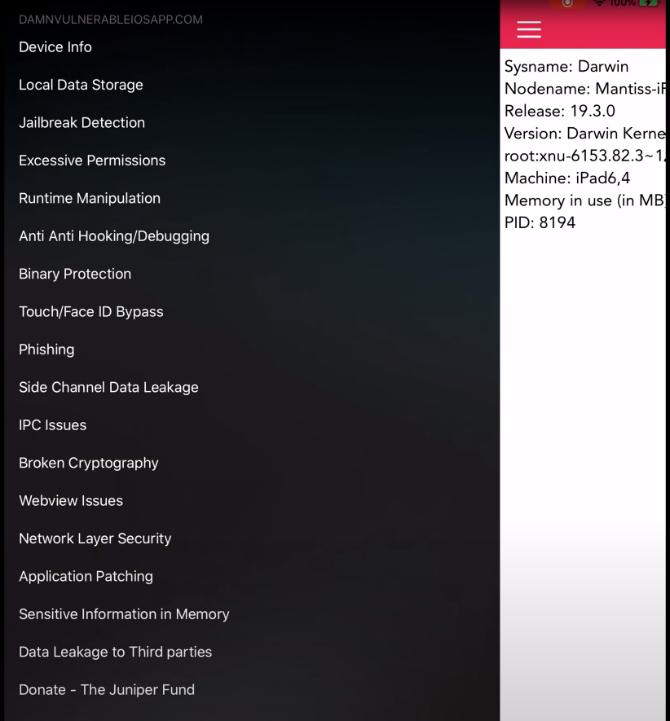
1. Khai thác tệp Plist trong App Directory

Plist (Property List) là định dạng linh hoạt và tiện lợi để lưu trữ dữ liệu cấu hình ứng dụng. Chúng ta có thể gọi nó là bảng kê khai cho một ứng dụng iOS. Đó là một tập tin danh sách tài sản từ Apple. Nó quyết định nên sử dụng biểu tượng nào cho một gói, loại tài liệu nào mà ứng dụng có thể hỗ trợ và nhiều hành vi khác có tác động bên ngoài gói đó. Các tệp này có thể chứa dữ liệu nhạy cảm như khóa API Gmaps, v.v.

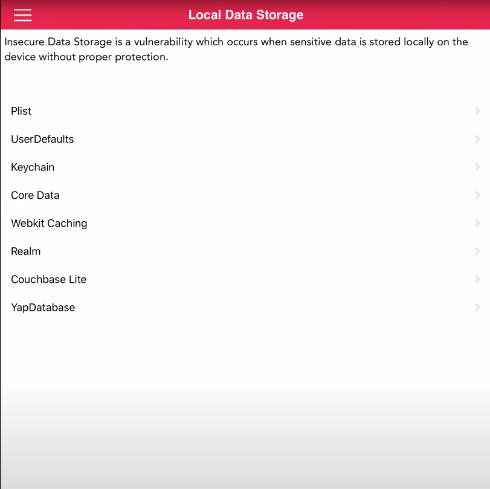
B1: Đọc file Plist trên máy giả lập bằng lệnh *plistutil -i info.plist*



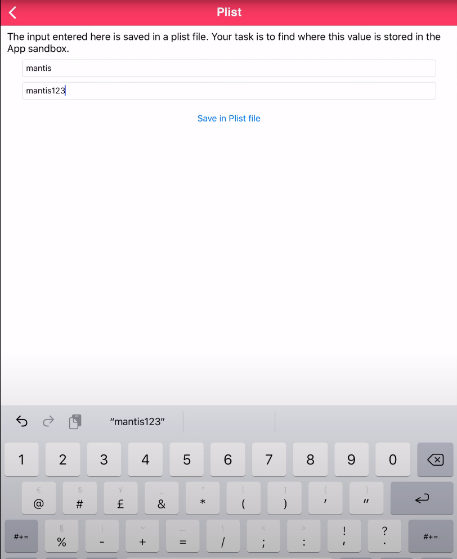
B2 vào máy giả lập chọn DVIA-v2 sau đó chọn Local Data Storage



Chọn Plist



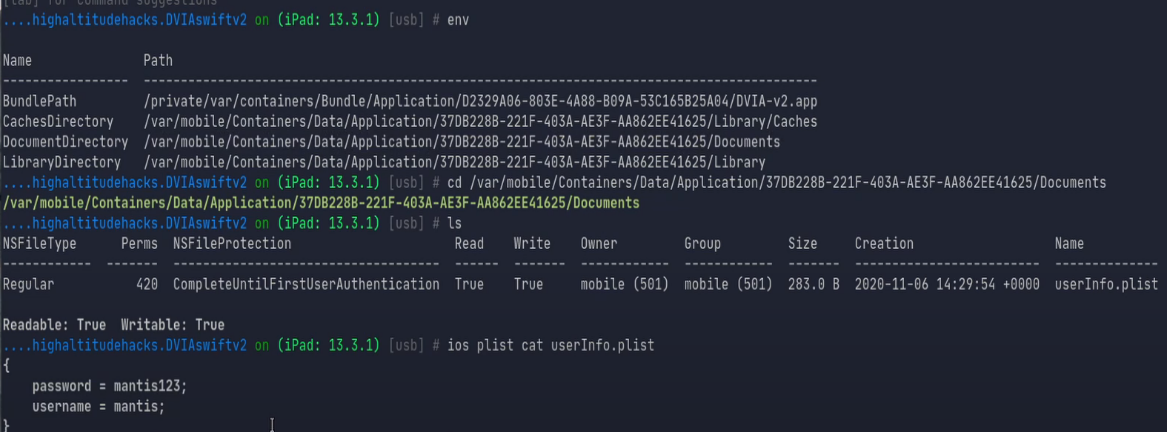
Nhập 1 username, password bất kỳ lưu vào file plist



B3: Chạy objection



Sau khi khai thác thành công kiểm tra file

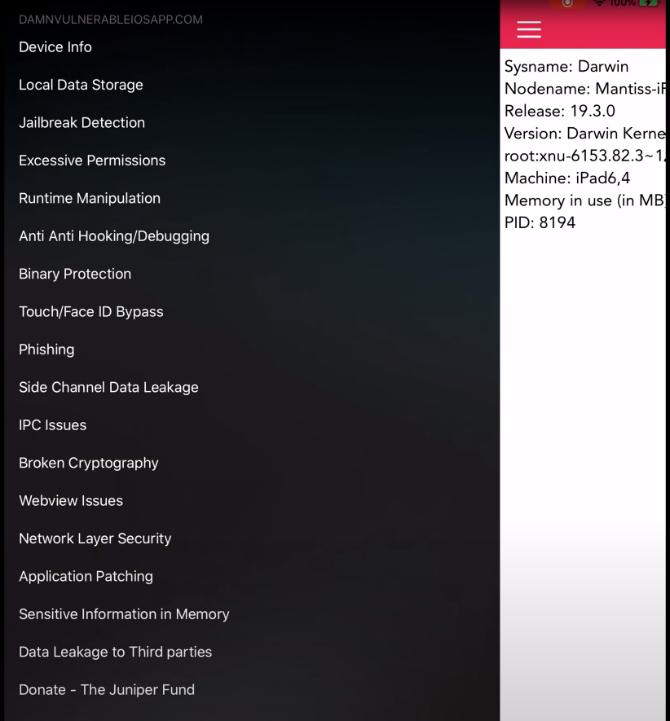


Thấy được username, password vừa lưu

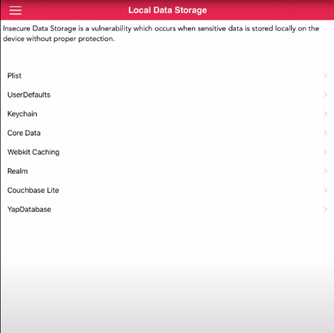
1. Khai thác NSUserDefaults

NSUserDefault là một class cung cấp một giải pháp để lưu trữ dữ liệu một cách đơn giản. Dữ liệu sau khi được lưu thì kể cả reset thiết bị nó cũng vẫn được lưu lại. Có thể sử dụng NSUserDefaults để lưu trữ các kiểu dữ liệu cơ bản như: Bool, Float, Double, Int, String hoặc NSURL, arrays, dictionaries, NSData, NSData

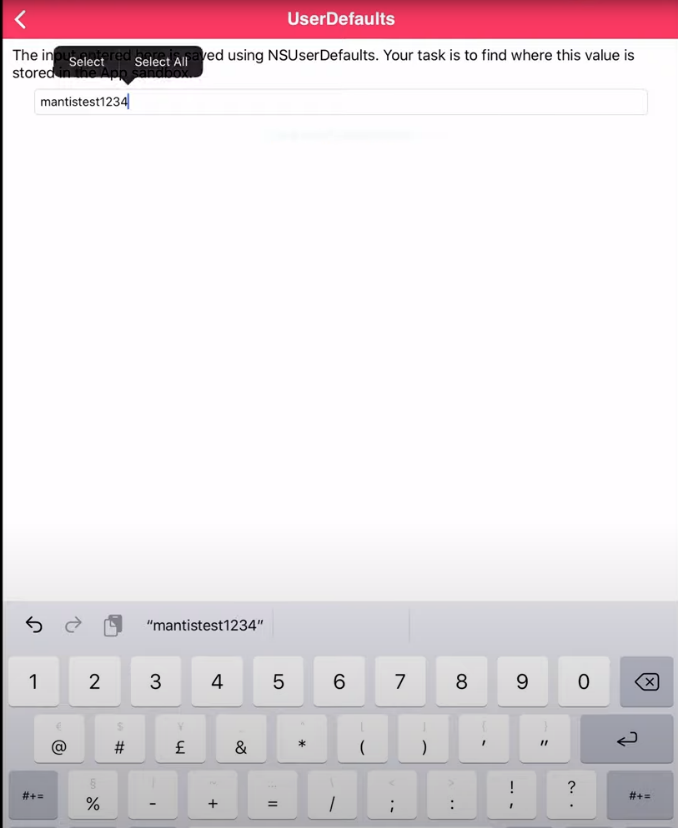
B1: vào thiết bị ios giả lập chọn ứng dụng DVIA-v2



Chọn NSUserDefaults



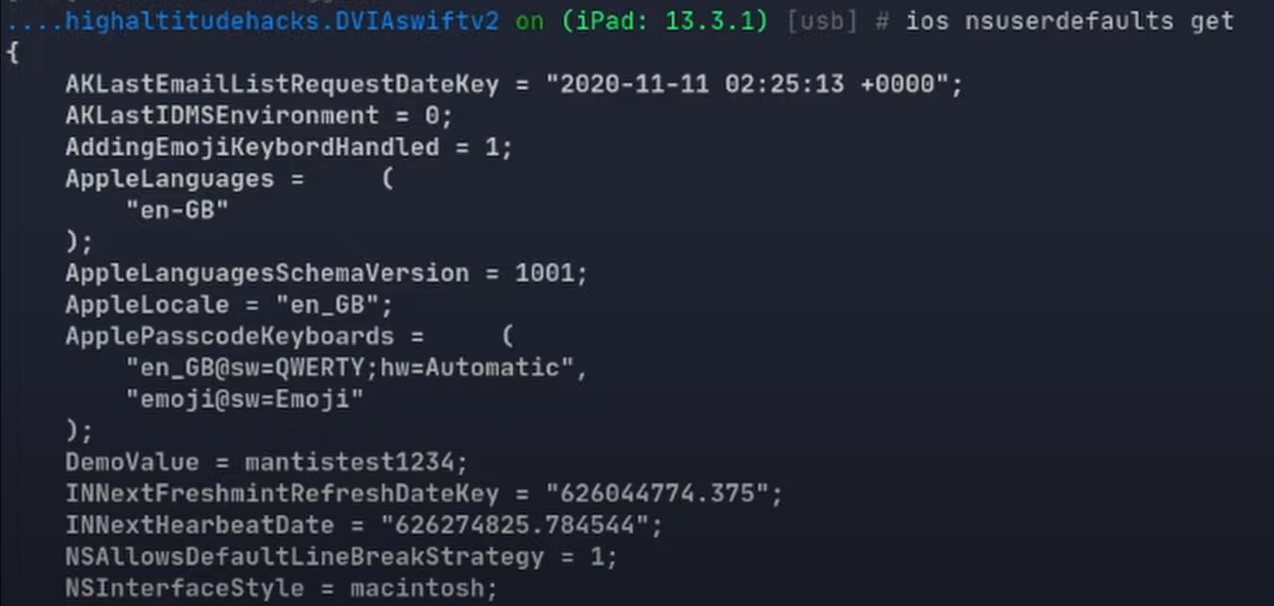
B2 nhập nội dung và lưu vào NSUserDefaults



B3: chạy Objection



Kiểm tra nsuserdefaults khai thác được thấy được giá trị đã nhập ở *DemoValue*

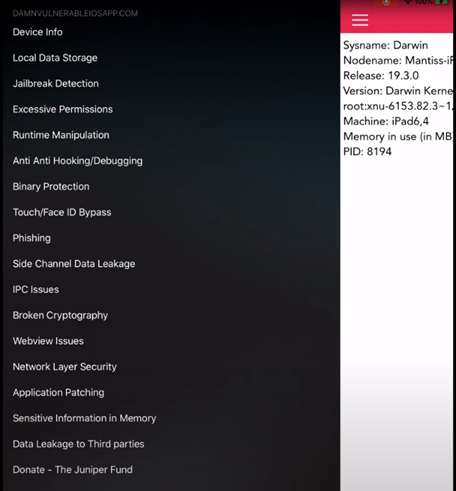


### Fingerprint Bypass

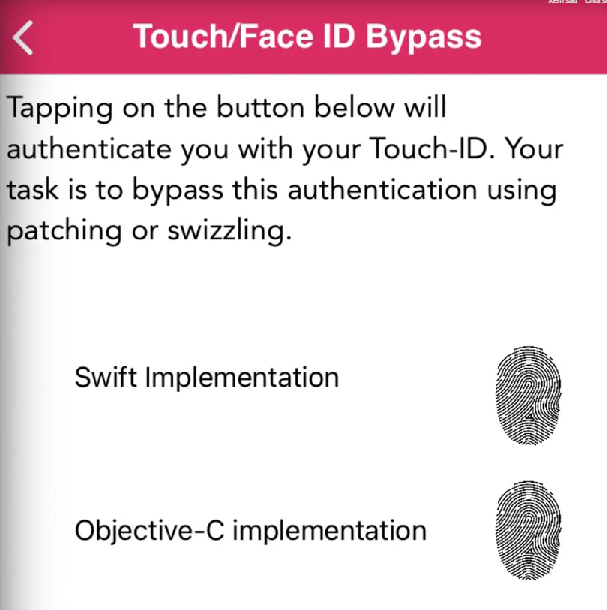
 Để vượt qua sinh trắc học, bạn không cần phải có cùng dấu vân tay/khuôn mặt với mục tiêu. Thay vào đó, chúng ta có thể đi thẳng vào cơ chế kiểm tra dấu vân tay. Nếu nó được triển khai không an toàn thì chúng ta có thể bỏ qua việc kiểm tra

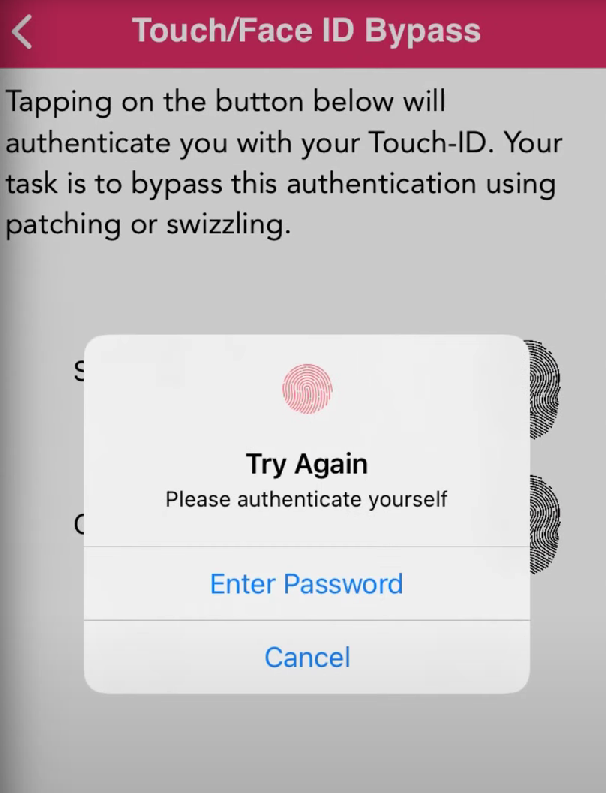
Bạn nên cài đặt dấu vân tay trên điện thoại trước khi thực hiện việc này

B1: vào thiết bị giả lập chọn DVIA-v2 sau đó chọn Touch/Face ID Bybass



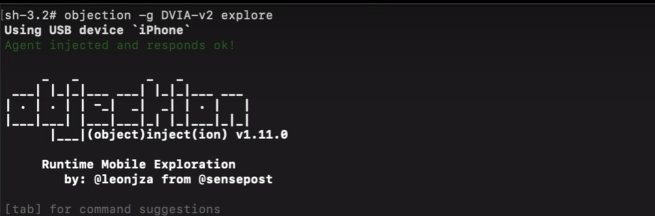
Chọn Objective-C sau đó sử dụng vân tay không chính xác, kích hoạt phản hồi cho biết thông tin nhập của bạn sai



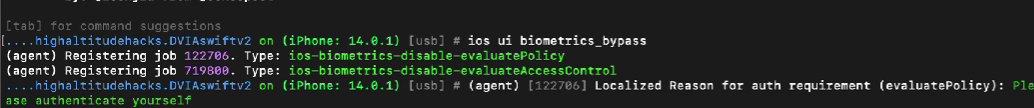


B3: chạy objection

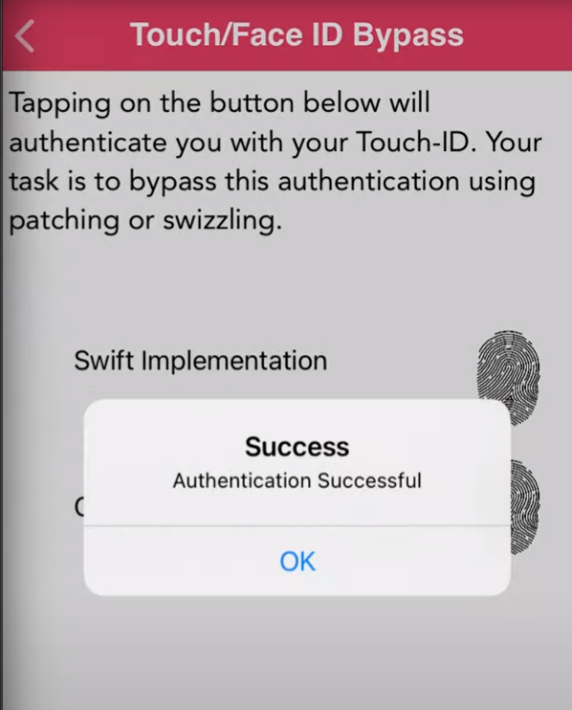
*objection — gadget DVIA-v2 explore*

**

chạy lệnh *ios ui bimetrucs\_bybass* kích hoạt khai thác

**

Thử lại vân tay thì bybass thành công

**

