Hướng dẫn Hack Facebook, Twitter- Hacker Anonymous Việt Nam

***Bài tập mang tính chất học tập và nghiên cứu, không sử dụng bài tập này để thực hiện các hành vi vi phạm pháp luật.***

Vào một ngày đẹp trời, bạn login tài khoản [facebook](http://facebook.com/) của mình và bất ngờ khi trên tường của mình xuất hiện một dòng status do bạn viết mà không phải do bạn viết. Tá hỏa và bối rối không biết đang có chuyện gì xảy ra, bạn nhanh chóng đưa ra một phương án đó là change password tài khoản facebook của mình. Ok, mọi việc dường như đã khá hơn. Nhưng bất ngờ, một lát sau, bạn login vào tài khoản và thấy một dòng status khủng bố: “ Đổi pass cũng không ăn thua đâu  …”

*Vậy chuyện rắc rối gì đã xảy ra vậy? Vâng, rất có thể bạn đã là nạn nhân của một cuộc tấn công Session Sidejacking, hack facebook.*

Trong bài viết này sẽ hướng dẫn cách hack facebook, Twitter,… bằng kỹ thuật HTTP Session Sidejacking qua mạng LAN hoặc mạng WIFI .

**Các công cụ cần thiết:**

**1.**Wireshark ([tải về tại đây](http://www.filehippo.com/download_wireshark_32/))

**2.**Cain and Abel ([tải về tại đây](http://www.oxid.it/downloads/ca_setup.exe))

**3.**Trình duyệt Mozilla Firefox (Bắt buộc) và Mozilla Addons (Grease Monkey) ([tải về tại đây](https://addons.mozilla.org/firefox/downloads/latest/748/addon-748-latest.xpi?src=search))

**4.**Cookie Injector ([tải về tại đây](http://dustint.com/code/cookieinjector.user.js))

**Thực hiện hack facebook:**

Kết nối vào mạng LAN hoặc Wifi

**Bước 1:** Cài đặt Wireshark, Cain and Abel, Grease Monkey, Cookie Injector để hack facebook.

Bước này bạn thực hiện cài đặt bình thường như những phần mềm khác, với chú ý yêu cầu chạy dưới quyền administrator và cho phép cài đặt Winpcap.

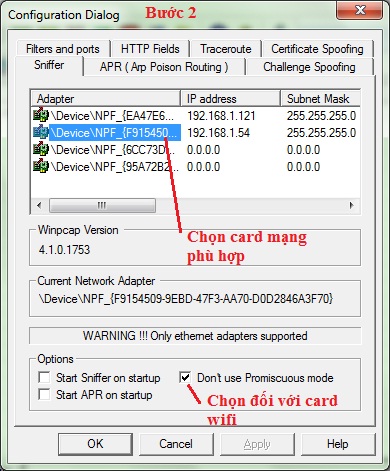
Cài đặt Cookie Injection, bạn chỉ cần kéo thả file **Cookieinjector.user.js** vào giao diện của Firefox, file sẽ tự động được cài đặt nha

**Bước 2:**Bật **Wireshark** vào menu **Capture / Interfaces (Ctrl + I).** Chọn card mạng của bạn và nhấn **Start** để bắt đầu quá trình chụp gói tin (capture packets) qua mạng.

Bạn sẽ thấy các gói tin hiện ra ào ào, trong đó bạn chú ý:

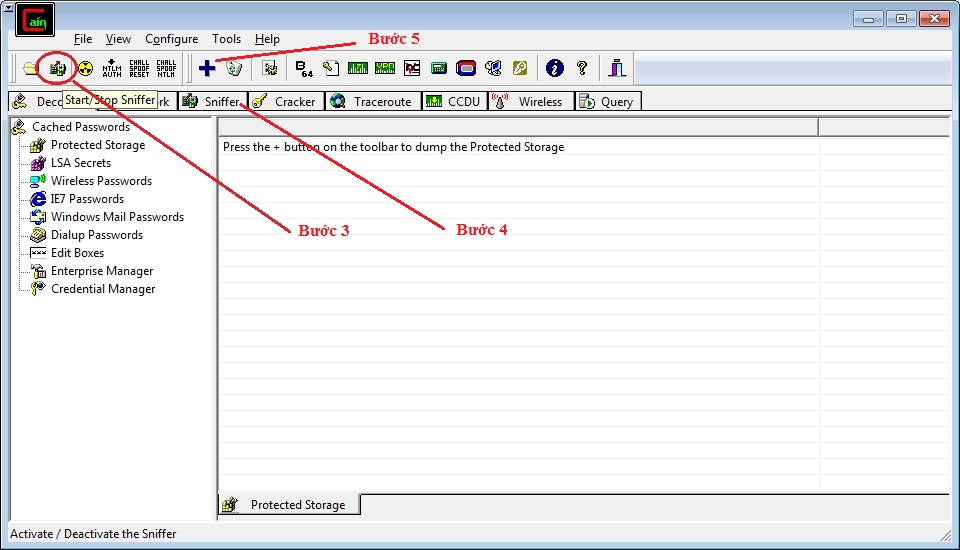
* **Source:** Địa chỉ nguồn, nơi chứa tất cả các địa chỉ mà gói tin xuất phát, bao gồm cả địa chỉ của nạn nhân bị tấn công
* **Destination:** Địa chỉ đích, nơi chứa địa chỉ mà gói tin sẽ tới

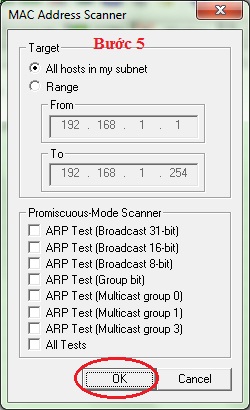
**Bước 3:**Chạy **Cain&Abel**, vào menu configure chọn card mạng (chọn cái nào hiện tại có địa chỉ IP) và cấu hình như hình dưới.

[](https://tranminhtuyen.files.wordpress.com/2013/06/huong-dan-su-dung-cain-and-abel-2.jpg)

Chuyển đến tab **Sniffer** ( trong dãy các tab nằm phía trên ). Click bật biểu tượng **Sniffer** ( hình card mạng)

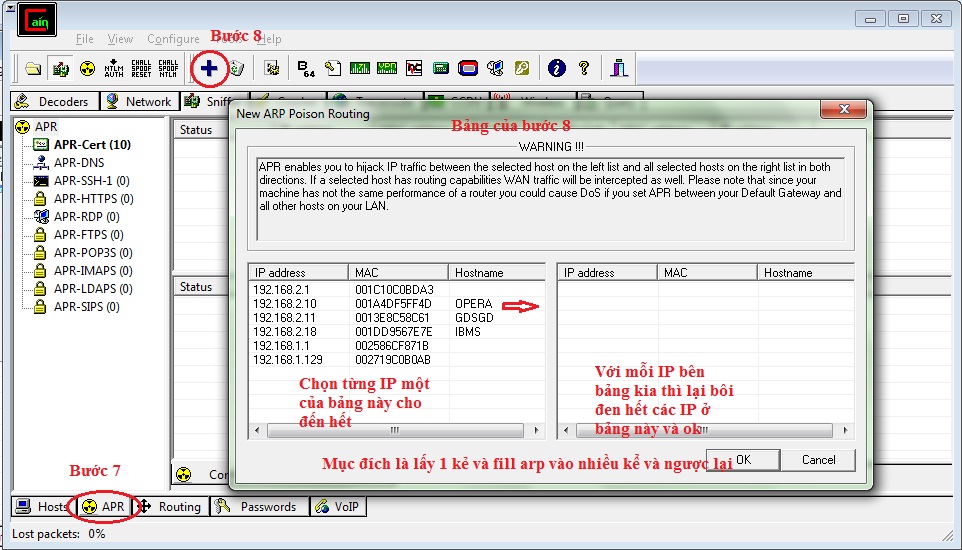
Nhấp vào biểu tượng hình dấu**+**màu xanh, chọn OK để thực hiện quá trình scan địa chỉ MAC và Ip trong mạng.

[](https://tranminhtuyen.files.wordpress.com/2013/06/huong-dan-su-dung-cain-and-abel-3.jpg)

[](https://tranminhtuyen.files.wordpress.com/2013/06/huong-dan-su-dung-cain-and-abel-4.jpg)

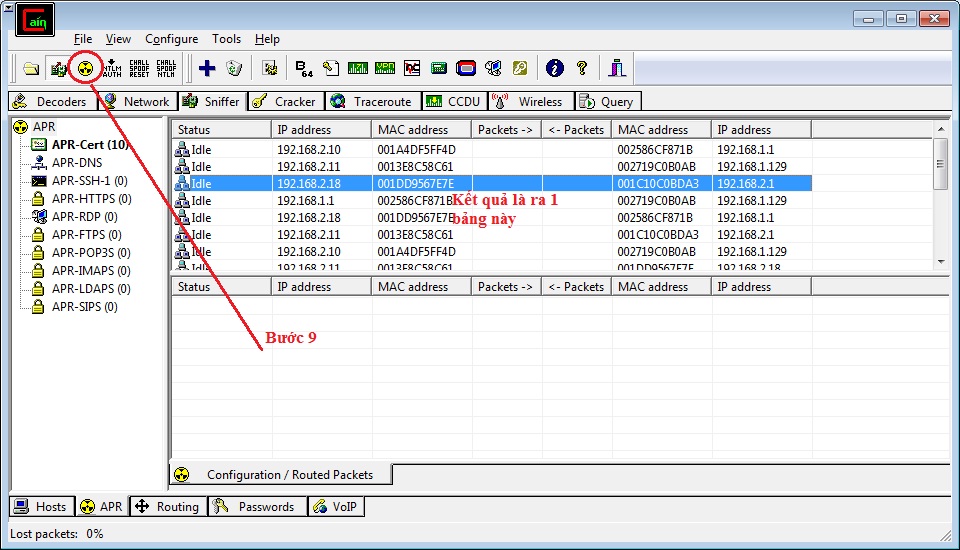
**Bước 4:** Sau khi có danh sách các máy tính hiện đang kết nối trong mạng wifi, ta tiến tới thực hiện ARP Poison Routing.

Bạn chuyển qua tab **APR** ( nằm ở dãy tab phía dưới màn hình – biểu tượng màu vàng và đen ). Click vào dấu cộng “+” ( chỗ khoanh tròn trong hình ) để mở hộp cấu hình ARP Poison Routing như sau:

[](https://tranminhtuyen.files.wordpress.com/2013/06/huong-dan-su-dung-cain-and-abel-6.jpg)

Việc ARP Poison Routing sẽ được thực hiện giữa máy tính bên trái và “các” máy tính bên phải. Bên trái có thể là router như trường hợp địa chỉ 192.168.1.1 trong hình ( các router thường có địa chỉ là x.x.x.1) và bên phải là tất cả các máy tính có trong mạng ở phía bên. Xong xuôi, click OK.

**Bước 5:**  Click chọn biểu tượng Start/Stop APR ( màu vàng và đen ) nằm ở trên bên trái của cửa sổ Cain&Abel

[](https://tranminhtuyen.files.wordpress.com/2013/06/huong-dan-su-dung-cain-and-abel-7.jpg)

Sau khi click sẽ thấy các dòng idle trước các địa chỉ IP sẽ đổi thành Poisoning. Bây giờ ta đã có đầy đủ điều kiện để sniff toàn bộ gói tin trong mạng này.

**Bước 6:** Chuyển sang tab Passwords, ta sẽ thấy một vài điều thú vị ở đây.

Bạn chú ý tiếp tới cột URL, danh sách này sẽ liên tục được cập nhật, mỗi khi người dùng trong mạng wifi truy cập một website nào đó, Cain&Abel sẽ ghi lại chi tiết: người dùng có IP nào truy cập website nào, URL là gì, địa chỉ IP của website, username & password (nếu có).

Bạn cứ liên tục theo dõi danh sách này, đến khi nào xuất hiện địa chỉ web bạn mong muốn. Ví dụ: http://www.facebook.com/\*\*\*\*\*  và chú ý tới một số thông tin sau:

* **IP của HTTP Server**: đây chính là IP của [facebook](http://facebook.com/Hackeranonymousvietnam)
* **IP của client**: đây chính là IP của người dùng đang truy cập facebook

Ngay lập tức bạn hãy chuyển trở lại **Wireshark**, click nút stop trên thanh công cụ.

Trong ô Filter bạn gõ: ***http.cookie contains datr***

Sau đó thực hiện việc lấy Cookie bằng cách, chọn địa chỉ IP trong mục Source trùng với IP của client mà bạn đã ghi nhớ bên Cain&Abel (trong hình là 192.168.1.6)

Chuột phải vào đó, chọn Copy / Bytes / Printable Text Only.

Lúc này Cookies của nạn nhân mà bạn lấy được đã được lưu vào bộ nhớ đệm của máy tính.

**Bước 7:** Phục dựng Session – Cookie injection

Trước hết, bạn mở Firefox và truy cập vào địa chỉ [http://www.facebook.com](http://www.facebook.com/)

*Chú ý: Ban phải logout ra khỏi tài khoản facebook hiện tại.*

Bây giờ thì bấm tổ hợp phím**Alt+C**( phím Alt và phím C đồng thời ), nó sẽ hiện ra cái khung nhỏ nhỏ (Wireshark Cookie Dump). Bạn paste cái chuỗi cookies đã copy ở bước trên vào ô textbox của cái khung nhỏ nhỏ này rồi bấm Ok. (Với chú ý add-on Grease Monkey đã được Enable)

Sau khi nhấn OK, hộp thoại thông báo quá trình ghi nhớ Cookies thành công

Click vào thanh address và nhấn Enter để trang được load lại. Và xem lại thành quả nha 😀

**Các phương thức bảo mật**

Khởi nguồn của vấn đề ARP Poisoning Routing ( APR), là việc các thiết bị trong mạng LAN không biết địa chỉ IP nào hiện đang được gán cho thiết bị có địa chỉ MAC nào. Như ta đã biết, địa chỉ MAC là duy nhất đối với mỗi thiết bị mạng.

Các thiết bị trong mạng LAN khi cần biết địa chỉ IP của nhau thì chúng cần kiểm tra trong bộ nhớ của chúng (bảng ARP) nếu không thấy chúng sẽ gửi đi một gói tin broadcast ARP Request. Khi này thiết bị nào hiện có IP là 192.168.1.1 phản hồi trở lại với cái thiết bị vừa hỏi kia rằng nó hiện đang sở hữu IP 192.168.1.1 và địa chỉ MAC của nó.

Vấn đề rắc rối phát sinh từ chỗ các client con không có cách nào để kiểm tra xem địa chỉ IP 192.168.1.1 của thiết bị kia có phải là thật không. Nên lúc này nếu có một thiết bị giả mạo nào đó, đưa ra nhiều gói tin chứng tỏ nó có địa chỉ 192.168.1.1 hơn thì client sẽ nghe theo và gửi gói tin qua cho nó ( ARP Reply flood ).

Vậy trong trường hợp này, chúng tôi đưa ra cho bạn 2 giải pháp:

1. **Sử dụng giao thức HTTPS để truy cập các trang web tránh hack facebook qua phising nữa:**Việc này sẽ giúp gói tin của bạn được mã hóa trước khi gửi đi, nhằm tránh việc nghe lén trong mạng. Nếu chưa biết phising là gỉ có thể đọc qua bài này : <https://anonymousvn.org/desktop-phising.hav>
2. **Gán địa chỉ IP tĩnh và áp dụng Static ARP**

Điều này giống như bạn ghi tên mình vào sổ danh bạ của router, tức là bạn sẽ luôn luôn biết được địa chỉ 192.168.1.1 ở đâu, và gửi thẳng dữ liệu tới đó, tránh được việc gửi nhầm gói tin tới các địa chỉ mạo danh.

Trước hết bạn đặt địa chỉ IP tĩnh cho máy tính của mình, sau đó vào Command Dos và thực hiện câu lệnh sau:

**arp –s X.X.X.X Y.Y.Y.Y**

Trong đó:

* X.X.X.X là địa chỉ IP tĩnh mà bạn vừa gán cho máy tính của mình
* Y.Y.Y.Y là địa chỉ MAC của máy tính của bạn.

Trích nguồn: https://anonymousvn.org/