BÁO CÁO THỰC HÀNH

**Môn học: Nhập môn mạng máy tính**

**Buổi báo cáo: Lab 06**

**Tên chủ đề: Bắt gói tin & dò tìm mật khẩu WPA/WPA2**

**Scanning WPA/WPA2 Passwords**

*GVHD: Phan Trung Phát*

*Ngày thực hiện: 03/12/2022*

*Ngày nộp báo cáo: 17/12/2022*

1. **THÔNG TIN CHUNG:**

*(Liệt kê tất cả các thành viên trong nhóm)*

Lớp: IT005.N19.1

|  |  |  |  |
| --- | --- | --- | --- |
| **STT** | **Họ và tên** | **MSSV** | **Email** |
| 1 | Nguyễn Thị Thanh Mai | 21521112 | 21521112@gm.uit.edu.vn |
| 2 | Lê Đoàn Trà My | 21521149 | 21521149@gm.uit.edu.vn |

1. **ĐÁNH GIÁ KHÁC:**

|  |  |
| --- | --- |
| **Nội dung** | **Kết quả** |
| Tổng thời gian thực hiện bài thực hành trung bình | 10 tiếng |
| Link Video thực hiện  *(nếu có)* | Link drive chứa 2 video thực hiện: <https://drive.google.com/drive/folders/1M7jccWGdM29WS98M8msHRl0prO9qJpWq?usp=sharing> |
| Ý kiến *(nếu có)*  + Khó khăn  + Đề xuất … |  |
| Điểm tự đánh giá | 9-9.5 |

BÁO CÁO CHI TIẾT

---

1. **Kịch bản quay và chi tiết các bước thực hành**

(kịch bản mang tính chất dự kiến, bao quát)

**\*Ghi chú về màu chữ trong kịch bản :**

**- Màu xanh:**  thay đổi tên cho thích hợp với thực tế khi làm.

**- Màu đất:** yêu cầu thêm khi tiến hành quay.

**- Màu đen:** chữ để phụ đề.

**1.1.Phương pháp Wordlist (danh sách các từ có sẵn)**

- Video thực hiện bắt gói tin và dò tìm mật khẩu WPA/WPA2 với phương pháp Wordlist (danh sách các từ có sẵn) cho wifi ***\*Tên wifi\****.

Biết mật khẩu được chọn từ một trong các mật khẩu thông dụng thuộc wordlist rockyou.txt tại thư mục /usr/share/wordlist.

(Chờ không làm gì mấy giây đầu).

- Nhóm sinh viên thực hiện Nguyễn Thị Thanh Mai 21521112 - Lê Đoàn Trà My 21521149 .

- Đầu tiên, sử dụng lệnh “**sudo su**” để chuyển thành chế độ root user (lệnh được thực thi ở chế độ “người dùng cấp cao”).

- Sau khi vào chế độ root user, kiểm tra card Wireless đang sử dụng bằng lệnh **“iwconfig”.**

- Chuyển card mạng Wifi sang chế độ monitor (chế độ theo dõi toàn bộ

các tín hiệu trong mạng), bằng câu lệnh **“airmon-ng start wlan0” .**

- Kiểm tra lại card mạng đã ở chế độ monitor hay chưa với lệnh “**iwconfig**”.

- Sử dụng lệnh **“airodump-ng wlan0mon”** để theo dõi hoạt động của mạng wifi hiện tại.

- Màn hình sẽ hiển thị một danh sách các mục tiêu wifi được phát hiện.

Sau khi tìm thấy wifi ***\*Tên wifi***\* cần crack, nhấn Ctrl+C để dừng xem danh sách wifi hiện tại.

- Tiến hành xác định mục tiêu, quan sát trường dữ liệu: BSSID, CH (chanel) (các trường cần để tiến hành crack wifi).

(Dùng chuột di chuyển tại dòng wifi mục tiêu).

- Chuyển sang theo dõi duy nhất mạng mục tiêu ***\*Tên wifi***\*, với câu lệnh **“airodump-ng -c [channel] -w [tập tin] --bssid [BSSID của mạng] wlan0mon”.**

Với[CH] = **CH**, [bssid của mạng] = **BSSID,** -w[tập tin]: đường dẫn lưu tập tin bắt được.

Cụ thể: **“airodump-ng -c [CH] -w wifi-sniff —bssid [bssid địa chỉ] wlan0mon”.**

- Thu thập gói tin bắt tay WPA handshake trong quá trình đăng nhập có 2 cách: Chờ người dùng nào đó đăng nhập **hoặc** Sử dụng aireplay để tạo tín hiệu deauth (kích các người dùng đang sử dụng mạng thoát ra và đăng nhập lại liên tục) với cú pháp:

aireplay-ng --deauth [số lệnh deauth] -a [BSSID của mạng] wlan0mon

- Trong lần này, nhóm tiến hành thông qua việc thiết bị khác truy cập mạng mục tiêu ***\*Tên wifi***\* để bắt gói tin.

- Khi nhận được gói tin WPA handshake của mạng mục tiêu tương ứng, ta dừng quá trình bắt gói tin (Ctrl+C) và tiến hành dò tìm mật khẩu dựa vào file .cap đã bắt được.

(Di chuyển chuột vào địa chỉ WPA…..).

-Sử dụng Wordlist rockyou.txt có sẵn, thực hiện lệnh:

**“cp /usr/share/wordlists/rockyou.txt.gz .”,** để copy file nén rockyou.txt tới folder đang làm việc trên terminalvà tiến hành giải nén file với lệnh**“ gzip -d rockyou.txt.gz”.**

- Sau khi đã có file rockyou.txt đã giải nén, sử dụng lệnh để dò tìm password: **aircrack-ng -w [đường dẫn file Wordlist] [đường dẫn file .cap]**

Cụ thể: **“aircrack-ng -w rockyou.txt wifi-sniff-01.cap”.**

- Chờ đợi…..

(Màn hình đang chạy để dò tìm mật khẩu).

- Đã tìm thấy mật khẩu wifi ***\*Tên wifi\****, là **\*mật khẩu\***

(Kéo chuột bôi/ di chuyển chuột bao quanh mật khẩu).

- Tắt chế độ monitor của card wlan0 để có thể sử dụng lại Wifi bằng lệnh **“airmon-ng stop wlan0mon”**

- Dùng mật khẩu **\*mật khẩu\*** để truy cập vào ***\*Tên wifi\*****,* thấy đã có thể kết nối được.

Vậy, mật khẩu đã tìm là chính xác.

**1.2. Phương pháp kết hợp tool Crunch để Brute-force (dò tìm vét cạn)**

- Video thực hiện bắt gói tin và dò tìm mật khẩu WPA/WPA2 với phương pháp kết hợp tool Crunch để Brute-force (dò tìm vét cạn) cho wifi ***\*Tên wifi\****.

Biết **mật khẩu** gồm **8 ký tự: 6 ký tự đầu tiên là ký tự số và 2 ký tự cuối là ký tự chữ**, với **ký tự đầu: 2**, **ký tự cuối: m.**

(Chờ không làm gì mấy giây đầu).

- Nhóm sinh viên thực hiện Nguyễn Thị Thanh Mai 21521112 - Lê Đoàn Trà My 21521149.

- Đầu tiên, sử dụng lệnh “**sudo su**” để chuyển thành chế độ root user (lệnh được thực thi chế độ “người dùng cấp cao”).

- Sau khi vào chế độ root user, kiểm tra card Wireless đang sử dụng bằng lệnh **“iwconfig’’.**

- Chuyển card mạng Wifi sang chế độ monitor (chế độ theo dõi toàn bộ

các tín hiệu trong mạng), bằng câu lệnh **“airmon-ng start wlan0”.**

- Kiểm tra lại card mạng đã ở chế độ monitor hay chưa với lệnh “**iwconfig**”.

- Sử dụng lệnh **“airodump-ng wlan0mon”** để theo dõi hoạt động của mạng wifi hiện tại.

- Màn hình sẽ hiển thị một danh sách các mục tiêu wifi được phát hiện.

Sau khi tìm thấy wifi ***\*Tên wifi***\* cần crack, nhấn Ctrl+C để dừng xem danh sách wifi hiện tại.

- Tiến hành xác định mục tiêu, quan sát trường dữ liệu: BSSID, CH (chanel) (các trường cần để tiến hành crack wifi).

(Dùng chuột di chuyển tại dòng wifi mục tiêu).

- Chuyển sang theo dõi duy nhất mạng mục tiêu ***\*Tên wifi***\*, với câu lệnh **“airodump-ng -c [channel] -w [tập tin] --bssid [BSSID của mạng] wlan0mon”.** Với[CH] = **CH**, [bssid của mạng] = **BSSID,** -w[tập tin]: đường dẫn lưu tập tin bắt được.

Cụ thể: **“airodump-ng -c [CH] -w wifi-sniff —bssid [bssid địa chỉ] wlan0mon”.**

- Thu thập gói tin bắt tay WPA handshake trong quá trình đăng nhập có 2 cách: Chờ người dùng nào đó đăng nhập **hoặc** Sử dụng aireplay để tạo tín hiệu deauth (kích các người dùng đang sử dụng mạng thoát ra và đăng nhập lại liên tục) với cú pháp:

aireplay-ng --deauth [số lệnh deauth] -a [BSSID của mạng] wlan0mon

- Trong lần này, nhóm tiến hành thông qua việc thiết bị khác truy cập mạng mục tiêu ***\*Tên wifi***\* để bắt gói tin.

- Khi nhận được gói tin WPA handshake **\*địa chỉ\*** của mạng mục tiêu tương ứng, ta dừng quá trình bắt gói tin (Ctrl+C) và tiến hành dò tìm mật khẩu dựa vào file .cap đã bắt được.

(Di chuyển chuột vào địa chỉ WPA…..).

- Sử dụng Crunch để dò tìm mật khẩu với cú pháp:

**crunch [số ký tự min] [số ký tự max] [danh sách các ký tự có có trong chuỗi] -t [mẫu định dạng mật khẩu] | aircrack-ng -w- [tập tin đã capture.cap] --bssid [địa chỉ MAC của mục tiêu]**

- Kết hợp với gợi ý mật khẩu đã cho: mật khẩu gồm 8 ký tự, 6 ký tự đầu tiên là ký tự số và 2 ký tự cuối là ký tự chữ, với **ký tự đầu: 2**, **ký tự cuối: m** (định dạng pass: **2%%%%%@m**).

(ký tự số chưa biết ký hiệu %, ký tự chữ chưa biết ký hiệu @).

Cụ thể: **“crunch 8 8 -t 2%%%%%@m | aircrack-ng -w- wifi-sniff-02.cap —bssid [bssid địa chỉ]”.**

- Chờ đợi…..

(Màn hình đang chạy để dò tìm mật khẩu).

- Đã tìm thấy mật khẩu wifi ***\*Tên wifi\****, là **\*mật khẩu\*.**

(Kéo chuột bôi/ di chuyển chuột bao quanh mật khẩu)

- Tắt chế độ monitor của card wlan0 để có thể sử dụng lại Wifi bằng lệnh **“airmon-ng stop wlan0mon”.**

- Dùng mật khẩu **\*mật khẩu\*** để truy cập vào ***\*Tên wifi\*****,* thấy đã có thể kết nối được.

Vậy, mật khẩu đã tìm là chính xác.

1. **Sản phẩm thực hành**

**2.1. Link video báo cáo thực hành:**

- Video báo cáo dò tìm mật khẩu wifi theo phương pháp **Wordlists:** <https://drive.google.com/file/d/1EbUlWrNsg_Bm7L3Dpqh_sDzX70WF8CJJ/view>

- Video báo cáo dò tìm mật khẩu wifi theo phương pháp **Brute-force:**

<https://drive.google.com/file/d/15Vkjh3ZIxiqXyTjDTJSUyYSBHQuIPrfT/view>

**2.2. Phần mở rộng - các nội dung tìm hiểu thêm về công cụ:**

- Công cụ **Aircrack-ng :** Là một bộ công cụ hoàn chỉnh để đánh giá an ninh mạng WiFi.

+ ***Tính năng:*** Bẻ khóa các giao thức bảo mật wifi (ví dụ: WEP, PSK, WPA, WPA2); giám sát, bắt gói tin; phát lại các cuộc tấn công, hủy xác thực, giả mạo điểm truy cập,…; phân tích - kiểm tra mạng LAN/wifi,…

+ ***Một số công cụ/tập lệnh khác được hỗ trợ***trong bộ Phần mềm Aircrack-ng:

++ airbase-ng: Công cụ tấn công đa mục tiêu máy khách thay vì chính Điểm truy cập (AP).

++ aircrack-ng: Chương trình bẻ khoá mật khẩu không dây.

++ airdecap-ng: Giải mã các gói tin WEP/WPA/WPA2.

++ airdrop-ng: Công cụ hủy cấp phép không dây dựa trên quy tắc nhất định.

++ airgraph-ng: Biểu đồ mạng không dây.

++ airmon-ng: Bật và tắt chế độ màn hình trên giao diện không dây.

++ airodump-ng: Bắt các gói tin trong mạng wifi.

++ airolib-ng: Tính toán trước cụm mật khẩu WPA/WPA2 trong cơ sở dữ liệu để sử dụng sau này với aircrack-ng,….

- Công cụ **Crunch**: một công cụ tạo danh sách từ được cài đặt sẵn với Kali Linux.

+ ***Tính năng:*** tạo các từ khóa tùy chỉnh dựa trên danh sách từ (wordlist). Nó tạo ra một wordlist với tổ hợp và hoán vị khả thi dựa trên các tiêu chí đã cho.

+ Crunch hỗ trợ số và ký hiệu, ký tự chữ hoa và chữ thường Unicode riêng biệt.

Có 4 ký tự đại diện cho một số nhóm ký tự như sau: **,** (chữ in hoa) ; **@** (chữ thường); **%** (ký tự số) ; **^** (ký tự đặc biệt).

+Crunch có thể kết hợp CUPP (common user password profile) để tạo ra 1 wordlist liên quan đến mật khẩu.

- Công cụ **CUPP** (common user password profile): một tập lệnh Python, có khả năng tạo wordlist dò mật khẩu sát với thông tin cá nhân của mục tiêu bằng cách thu thập dữ liệu cơ bản về mục tiêu.

+ Không được cài đặt sẵn trên Kali Linux, cần cài đặt từ GitHub (bản sao git: <https://github.com/mebus/cupp.git> ).

- Trong quá trình bắt các gói tin, nhận thấy hiện nay phần lớn các mạng sử dụng giao thức bảo mật WPA/WPA2,…

Với mạng wifi được phát từ Iphone, nhận thấy nó sử dụng giao thức bảo mật WPA3, vì vậy có thể dò tìm thấy tên mạng nhưng không thể bắt gói tin .cap.

1. **Phân chia công việc trong nhóm**

|  |  |  |
| --- | --- | --- |
| **Công việc** | **Thanh Mai** | **Trà My** |
| Chung | - Thực hiện quay video thực hành báo cáo.  - Tìm hiểu thêm về các công cụ | |
| Riêng | - Edit 2 video thực hành: Wordlist, Brute-force. | - Viết kịch bản chữ edit, hoàn thiện báo cáo. |

**\* Tài liệu tham khảo**

1. Aircrack-ng, <https://www.aircrack-ng.org/>, ngày truy cập: 16/12/2022.
2. Kali Linux – Crunch Utility, <https://www.geeksforgeeks.org/kali-linux-crunch-utility/> , ngày truy cập: 16/12/2022.
3. Crunch Kali Linux – tạo wordlist trong kali linux, <https://websitehcm.com/crunch-kali-linux-tao-wordlist-trong-kali-linux/>, ngày truy cập: 16/12/2022.
4. Make a Strong Wordlist By Crunch and Cupp, <https://auntoracharja.medium.com/make-a-strong-wordlist-by-crunch-and-cupp-78735820a02c> , ngày truy cập: 16/12/2022.
5. Tạo wordlist dựa trên thông tin cá nhân bằng CUPP, <https://www.thekalitools.com/2017/08/tao-wordlist-dua-tren-thong-tin-ca-nhan.html> , ngày truy cập: 16/12/2022.