****

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

VÀ TRUYỀN THÔNG VIỆT - HÀN

**KHOA KĨ THUẬT MÁY TÍNH VÀ ĐIỆN TỬ**

**BÁO CÁO**

**THỰC TẬP DOANH NGHIỆP**

**BÁO CÁO THỰC TẬP DOANH NGHIỆP TẠI VNNIC**

**Sinh viên thực hiện: Nguyễn An Phúc -** 21IT639

**Trần Vũ Lập Thi -** 21IT448

**Giảng viên hướng dẫn:**  **HOÀNG HỮU ĐỨC**

***Đà Nẵng, tháng 8 năm 2024***

**** TRƯỜNG ĐẠI HỌC CÔNG NGHỆ THÔNG TIN

VÀ TRUYỀN THÔNG VIỆT - HÀN

**KHOA KĨ THUẬT MÁY TÍNH**

**BÁO CÁO**

**THỰC TẬP DOANH NGHIỆP**

**BÁO CÁO THỰC TẬP DOANH NGHIỆP TẠI VNNIC**

**Sinh viên thực hiện: Nguyễn An Phúc -** 21IT639

**Trần Vũ Lập Thi -** 21IT448

**Giảng viên hướng dẫn:**  **TS. Hoàng Hữu Đức**

***Đà Nẵng, tháng 8 năm 2024***

LỜI CẢM ƠN

Để đề tài này đạt kết quả tốt đẹp, chúng em đã nhận được sự hỗ trợ, giúp đỡ của nhiều cơ quan, tổ chức, cá nhân. Với tình cảm sâu sắc, chân thành, cho phép chúng em được bày tỏ lòng biết ơn sâu sắc đến tất cả các cá nhân và cơ quan đã tạo điều kiện giúp đỡ trong quá trình học tập và nghiên cứu đề tài.

Trước hết em xin gửi tới các thầy cô khoa Kĩ thuật máy tính và điện tử Trường Đại học Công nghệ thông tin và Truyền thông Việt - Hàn lời chào trân trọng, lời chúc sức khỏe và lời cảm ơn sâu sắc. Với sự quan tâm, dạy dỗ, chỉ bảo tận tình chu đáo của thầy cô, đến nay chúng em đã có thể hoàn thành đề tài.

Đặc biệt em xin gửi lời cảm ơn chân thành nhất tới cô giáo – **ThS. Trần Thu Thủy** đã quan tâm giúp đỡ, hướng dẫn chúng em hoàn thành tốt đồ án này trong thời gian qua.

Với điều kiện thời gian cũng như kinh nghiệm còn hạn chế của một học viên, đồ án này không thể tránh được những thiếu sót. Chúng em rất mong nhận được sự chỉ bảo, đóng góp ý kiến của các thầy cô để em có điều kiện bổ sung, nâng cao ý thức của mình, phục vụ tốt hơn công tác thực tế sau này.

Em xin chân thành cảm ơn!

**Sinh viên chịu trách nhiệm chính**

(Ký và ghi rõ họ tên)

NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN

…………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………………

Đà Nẵng, ngày….tháng….năm 2024

Giảng viên hướng dẫn

MỤC LỤC

[LỜI CẢM ƠN 1](#_Toc30824)

[NHẬN XÉT CỦA GIẢNG VIÊN HƯỚNG DẪN 2](#_Toc3172)

[MỤC LỤC 1](#_Toc6888)

[DANH MỤC HÌNH ẢNH 3](#_Toc29347)

[DANH MỤC CÁC TỪ VIẾT TẮT 4](#_Toc31121)

[DANH MỤC BẢNG BIỂU 5](#_Toc12951)

[MỞ ĐẦU 6](#_Toc30087)

[1. Giới thiệu đề tài 6](#_Toc7264)

[2. Mục tiêu của đề tài 6](#_Toc27595)

[3. Phương pháp nghiên cứu 6](#_Toc14546)

[4. Phạm vi nghiên cứu 6](#_Toc19031)

[5. Nội dung và kế hoạch thực hiện 6](#_Toc27823)

[6. Bố cục báo cáo 6](#_Toc32481)

[CHƯƠNG 1 CƠ SỞ LÝ THUYẾT 7](#_Toc8904)

[1.1 Giới thiệu về mạng máy tính không dây 7](#_Toc7167)

[1.1.1 Mạng máy tính không dây là gì 7](#_Toc18133)

[1.1.2 Các thành phần cơ bản của mạng máy tính không dây 7](#_Toc15489)

[1.1.3 Hoạt động của mạng máy tính không dây 7](#_Toc6499)

[1.1.4 Ưu, nhược điểm của của mạng không dây 7](#_Toc10166)

[1.2 Các chuẩn của mạng máy tính không dây 8](#_Toc12743)

[1.2.1 Chuẩn 802.11 WLAN 8](#_Toc18606)

[1.2.2 Chuẩn 802.16 Broadband Wireless 9](#_Toc10265)

[1.2.3 Chuẩn 802.15 Bluetooth 9](#_Toc4898)

[1.3 Khái niệm an ninh an toàn thông tin 9](#_Toc5399)

[1.4 Các loại hình tấn công mạng máy tính không dây 10](#_Toc26938)

[1.4.1 Tấn công bị động - Passive Attacks 10](#_Toc13626)

[1.4.2 Tấn công chủ động - Active Attacks 10](#_Toc13490)

[1.4.3 Tấn công kiểu chèn ép - Jamming Attacks 10](#_Toc5582)

[1.4.4 Tấn công theo kiểu thu hút - Man in the Middle Attacks 10](#_Toc30241)

[1.4.5 Tấn công vào các yếu tố con người 11](#_Toc9121)

[1.4.6 Một số kiểu tấn công khác 11](#_Toc25446)

[1.5 Giải pháp đảm bảo an ninh an toàn mạng máy tính không dây 11](#_Toc28730)

[1.5.1 Bảo mật bằng WEP (Wired Equivalent Privacy) 11](#_Toc13957)

[1.5.2 Bảo mật bằng WPA (Wifi Protected Access) 11](#_Toc27067)

[1.5.3 Bảo mật bằng WPA2 12](#_Toc6276)

[CHƯƠNG 2 XÂY DỰNG ĐỀ TÀI 13](#_Toc25305)

[2.1 Aircrack là gì? 13](#_Toc12287)

[2.2 Ưu và nhược điểm của Aircrack-ng 13](#_Toc29583)

[2.3 Cách sử dụng Aircrack-ng 13](#_Toc22925)

[2.4 Kali Linux là gì? 17](#_Toc16505)

[2.5 Các Đặc Điểm Chính của Kali Linux: 17](#_Toc51)

[2.6 Cách sử dụng Kali Linux 17](#_Toc26107)

[CHƯƠNG 3 CÁC ĐOẠN CODE CÓ TRONG DEMO 18](#_Toc32367)

[CHƯƠNG 4 CHƯƠNG TRÌNH DEMO 19](#_Toc28060)

[KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN 25](#_Toc29863)

[1. Kết quả đạt được 25](#_Toc10048)

[2. Hạn chế và hướng phát triển 25](#_Toc10236)

[TÀI LIỆU THAM KHẢO 26](#_Toc19745)

DANH MỤC HÌNH ẢNH

[Hình 1 : Kiểm tra card mạng 19](#_Toc515)

[Hình 2 : Chuyển card mạng sang chế độ monitor 19](#_Toc22197)

[Hình 3 : Xác nhận card mạng đã chuyển sang chế đọ monitor 20](#_Toc26439)

[Hình 4 : Theo dõi các hoạt động các mạng wifi hiện tại qua card wlan0 20](#_Toc7562)

[Hình 5 : Xác định mạng cần tấn công 21](#_Toc19645)

[Hình 6 : Bắt gói tin và theo dõi duy nhất một mạng cần tấn công 21](#_Toc29571)

[Hình 7 : Kick người dùng thoát ra và đăng nhập lại mạng 22](#_Toc17060)

[Hình 8 : Bắt WPA handshake key 22](#_Toc14050)

[Hình 9 : Key WPA handshake đã được lưu vào file 23](#_Toc18021)

[Hình 10 : Dùng lệnh để tìm password trong wordlist 23](#_Toc26247)

[Hình 11 : Kết quả 24](#_Toc5389)

DANH MỤC CÁC TỪ VIẾT TẮT

|  |  |  |
| --- | --- | --- |
| **STT** | **VIẾT TẮT** | **NỘI DUNG** |
| 1 | WLAN | Wireless Local Area Network |
| 2 | NIC | Network Interface Card |
| 3 | AAA | Authentication, Authorization, Accounting |
| 4 | LAN | Local Area Network |
| 5 | IEEE | Institute of Electrical and Electronic Engineers |
| 6 | MBPS | Megabit per second |
| 7 | ISM | Industrial, Scientific and Medical |
| 8 | GHZ | Gigahertz |
| 9 | FHSS | Frequency-hopping spread spectrum |
| 10 | DSSS | Direct-Sequence Spread Spectrum |
| 11 | OFDM | Orthogonal Frequency Division Multiplexing |
| 12 | MIMO | Multiple In, Multiple Out |
| 13 | MAC | Media Access Control |
| 14 | WEP | Wired Equivalent Privacy |
| 15 | STA | Standard Template Attack |
| 16 | AP | Access point |
| 17 | WPA | Wifi Protected Access |

DANH MỤC BẢNG BIỂU

[Table 1 : Các chế độ cơ bản 14](#_Toc30244)

[Table 2 : Các chế độ phá khóa WEP tĩnh 14](#_Toc20286)

[Table 3 : Các chế độ phá khóa WEP và WPA-PSK 16](#_Toc16376)

[Table 4 : Các chế độ WPA-PSK 16](#_Toc21287)

[Table 5 : SIMD 16](#_Toc1083)

[Table 6 : Các chế độ khác 17](#_Toc14908)

MỞ ĐẦU

##### Giới thiệu đề tài

Mạng Wifi hiện nay rất phổ biến nhưng cũng chứa nhiều lỗ hổng bảo mật tiềm ẩn. Aircrack-ng là một công cụ miễn phí và mạnh mẽ để kiểm tra và phát hiện các lỗ hổng bảo mật trong mạng Wifi. Việc tìm hiểu và sử dụng Aircrack-ng sẽ giúp người quản trị mạng hiểu rõ hơn về các mối đe dọa bảo mật và có biện pháp khắc phục phù hợp.

##### Mục tiêu của đề tài

Tìm hiểu cấu trúc, nguyên lý hoạt động và khả năng của công cụ Aircrack-ng. Học cách sử dụng Aircrack-ng để thực hiện các bài kiểm tra bảo mật trên mạng Wifi. Đánh giá hiệu quả của Aircrack-ng trong việc phát hiện và khắc phục các lỗ hổng bảo mật trong mạng Wifi.

##### Phương pháp nghiên cứu

Tìm hiểu tài liệu, bài báo khoa học và hướng dẫn sử dụng về Aircrack-ng. Thực hành sử dụng Aircrack-ng trên các mạng Wifi ảo và thực tế. Đánh giá kết quả, so sánh hiệu quả của Aircrack-ng với các công cụ khác.

##### Phạm vi nghiên cứu

Tập trung vào việc sử dụng Aircrack-ng để kiểm tra bảo mật mạng Wifi. Nghiên cứu các tính năng chính của Aircrack-ng như capture gói tin, phát hiện mật khẩu, phát hiện lỗ hổng, v.v. Đánh giá hiệu quả của Aircrack-ng trong việc phát hiện và khắc phục các lỗ hổng bảo mật.

##### Nội dung và kế hoạch thực hiện

Tìm hiểu về cấu trúc và nguyên lý hoạt động của Aircrack-ng. Học cách sử dụng các tính năng chính của Aircrack-ng. Thực hành sử dụng Aircrack-ng trên các mạng Wifi ảo và thực tế. Đánh giá kết quả và hiệu quả của Aircrack-ng. Xây dựng báo cáo kết quả nghiên cứu.

##### Bố cục báo cáo

Sau phần *Mở đầu*, báo cáo được trình bày trong ba chương, cụ thể như sau:

Chương 1. *Cơ sở lý thuyết*

Chương 2. *Xây dựng đề tài*

Chương 3. *Chương trình Demo*

# CƠ SỞ LÝ THUYẾT

## Giới thiệu về mạng máy tính không dây

### Mạng máy tính không dây là gì

“Mạng máy tính không dây” hay còn gọi là mạng WLAN (Wireless Local Area Network) mạng cục bộ không dây, gồm hai hay nhiều máy tính giao tiếp với nhau bằng những giao thức mạng chuẩn nhưng không cần dây cáp mạng.

### Các thành phần cơ bản của mạng máy tính không dây

Kiến trúc WLAN cơ bản bao gồm:

* Access Point
* Card giao diện mạng NIC
* Anten
* Bridge và Workgroup Bridge
* Máy chủ AAA
* Switch và router “cảnh báo không dây”.

### Hoạt động của mạng máy tính không dây

Các mạng WLAN sử dụng các sóng điện từ không gian để truyền thông tin từ một điểm tới điểm khác. Các sóng vô tuyến thường được xem như các sóng mang vô tuyến do chúng chỉ thực hiện chức năng cung cấp năng lượng cho một máy thu ở xa. Dữ liệu đang được phát được điều chế trên sóng mang vô tuyến sao cho có thể được khôi phục chính xác tại máy thu.

Trong một cấu hình mạng WLAN tiêu chuẩn, một điểm truy cập nối với mạng hữu tuyến từ một vị trí cố định sử dụng cáp tiêu chuẩn. Chức năng tối thiểu của điểm truy cập là thu, làm đệm, phát dữ liệu giữa mạng WLAN và cơ sở hạ tầng mạng hữu tuyến.

### Ưu, nhược điểm của của mạng không dây

* + Ưu điểm
* Tính di động: Những người sử dụng mạng WLAN có thể truy nhập nguồn thông tin ở bất kỳ nơi nào trong phạm vi phủ sóng.
* Tính đơn giản: Việc lắp đặt, thiết lập, kết nối một mạng WLAN rất dễ dàng, đơn giản và có thể tránh được việc kéo cáp qua các bức tường và trần nhà.
* Tính linh hoạt: Có thể triển khai mạng WLAN ở những nơi mà mạng hữu tuyến không thể triển khai được hoặc khó triển khai.
* Tiết kiệm chi phí lâu dài: WLAN rất dễ dàng mở rộng và có thể đáp ứng tức thì khi gia tăng số lượng người dùng mà không cần phải cung cấp thêm cáp kết nối như mạng LAN truyền thống.
* Khả năng vô hướng: Các mạng WLAN có thể được cấu hình theo các topo khác nhau, dễ dàng thay đổi từ các mạng ngang hàng thích hợp cho một số lượng nhỏ người sử dụng đến các mạng có cơ sở hạ tầng đầy đủ dành cho hàng nghìn người sử dụng mà có khả năng di chuyển trên một vùng rộng.
  + Nhược điểm
* Về tính bảo mật: Do sử dụng sóng điện từ để thu/ phát dữ liệu nên tất cả mọi máy trạm nằm trong khu vực phủ sóng đều có thể thu được tín hiệu. Vì vậy, khả năng tấn công của người dùng là rất cao.
* Về phạm vi: Một mạng chuẩn 802.11g với các thiết bị chuẩn chỉ có thể hoạt động tốt trong phạm vi vài chục mét như trong phạm vi gia đình hoặc văn phòng.
* Về độ tin cậy: WLAN sử dụng sóng vô tuyến để truyền thông nên việc bị nhiễu, tín hiệu bị giảm do tác động của các thiết bị khác như lò vi sóng,… là điều không tránh khỏi.
* Về tốc độ: Tốc độ của mạng không dây chậm hơn so với mạng sử dụng cáp.

## Các chuẩn của mạng máy tính không dây

### Chuẩn 802.11 WLAN

* IEEE 802.11: Chuẩn không dây IEEE 802.11 cung cấp các giao tiếp không dây với tốc độ l Mbps hoặc 2 Mbps trong các dải ISM 2,4 GHz sử dụng FHSS hoặc DSSS.
* IEEE 802.11b: Chuẩn IEEE 802.11b cung cấp việc truyền dữ liệu cho các mạng WLAN trong dải tần số 2,4 GHZ với tốc độ 1 Mbps; 2 Mbps; 5,5 Mbps và có thể đạt tốc độ cao nhất là 11 Mbps.
* IEEE 802.11a: Chuẩn IEEE 802.11a hoạt động trong dải tần số từ 5 Ghz đến 6 GHZ, sử dụng phương pháp điều biến OFDM và có thể nâng tốc độ truyền dữ liệu tối đa lên tới 54 Mbps.
* IEEE 802.11g: Chuẩn IEEE 802.11g hỗ trợ việc truyền dữ liệu trong khoảng cách tương đối ngắn với tốc độ 20Mbps đến 54 Mbps. 802.11g là sự kết hợp tốt nhất giữa 802.11a và 802.11b.
* IEEE 802.11n: 802.11n là thế hệ hiện tại của mạng không dây tốc độ cao, khả năng hỗ trợ tốc độ, phạm vi phủ sóng lớn nhất hiện nay. Nó phù hợp với các ứng dụng cần băng thông lớn như các ứng dụng đa phương tiện. Wireless-N được xây dựng dựa trên cơ sở các chuẩn không dây trước đó kết hợp với công nghệ MIMO.

### Chuẩn 802.16 Broadband Wireless

Chuẩn IEEE 802.16 (WiMAX) là công nghệ không dây mang tính cách mạng trong ngành công nghiệp dịch vụ không dây băng rộng. Lớp MAC 802.16 hỗ trợ nền tảng point-to-multipoint trên băng tần 10-66 GHZ, tốc độ truyền tải dữ liệu từ 75 Mbps tới 120 Mbps. Nó sử dụng công nghệ OFDM, tương tự như 802.11a và 802.11g.

### Chuẩn 802.15 Bluetooth

Bluetooth hoạt động ở dải tần 2,4 Ghz, sử dụng phương thức trải phổ FHSS. Trong mạng Bluetooth, các phần tử kết nối với nhau theo kiểu ngang hàng hoặc theo kiểu tập trung, có 1 máy xử lý chính và có tối đa là 7 máy có thể kết nối vào.

## Khái niệm an ninh an toàn thông tin

An ninh an toàn thông tin (Information Security) là lĩnh vực liên quan đến việc bảo vệ thông tin và các hệ thống thông tin khỏi các mối đe dọa, đảm bảo tính bảo mật, toàn vẹn và sẵn sàng của thông tin. Dưới đây là một số khái niệm cơ bản trong an ninh an toàn thông tin

* Tính bảo mật (Confidentiality): Đảm bảo rằng thông tin chỉ được truy cập bởi những người hoặc hệ thống được phép. Điều này giúp bảo vệ thông tin khỏi việc tiết lộ trái phép.
* Tính toàn vẹn (Integrity): Đảm bảo rằng thông tin không bị thay đổi hoặc hỏng hóc bởi các hành động trái phép. Thông tin cần được bảo vệ khỏi việc bị chỉnh sửa hoặc xoá bỏ không đúng cách.
* Tính sẵn sàng (Availability): Đảm bảo rằng thông tin và các dịch vụ thông tin có sẵn để sử dụng khi cần thiết. Điều này bao gồm việc bảo vệ hệ thống khỏi các cuộc tấn công làm gián đoạn dịch vụ.
* Tính xác thực (Authentication): Xác định và xác minh danh tính của người dùng hoặc hệ thống truy cập vào thông tin. Điều này giúp đảm bảo rằng các thông tin truy cập và các hành động được thực hiện bởi những đối tượng hợp lệ.
* Tính không chối bỏ (Non-repudiation): Đảm bảo rằng một bên không thể phủ nhận việc đã thực hiện một hành động nào đó. Điều này thường liên quan đến việc sử dụng chữ ký số hoặc các biện pháp xác thực khác để ghi lại các giao dịch.
* Quản lý rủi ro (Risk Management: Quá trình xác định, đánh giá và ưu tiên các rủi ro bảo mật, từ đó thực hiện các biện pháp giảm thiểu để bảo vệ thông tin.
* Biện pháp kiểm soát bảo mật (Security Controls): Các công cụ, chính sách và quy trình được sử dụng để bảo vệ thông tin. Các biện pháp này có thể là kỹ thuật, quản lý hoặc vật lý.
* Tấn công mạng (Cyber Attacks): Các hành động cố ý gây hại đến thông tin và hệ thống thông tin, bao gồm tấn công từ chối dịch vụ (DDoS), phần mềm độc hại (malware), tấn công phishing, và nhiều loại tấn công khác.
* Mã hóa (Encryption): Phương pháp biến đổi thông tin thành dạng không thể đọc được nếu không có chìa khóa giải mã, nhằm bảo vệ tính bảo mật của thông tin khi truyền tải hoặc lưu trữ.
* Nhận diện và phản hồi (Incident Response): Quá trình phát hiện, phân tích và phản hồi lại các sự cố an ninh thông tin để giảm thiểu tác động và ngăn chặn sự cố tái diễn.

An ninh an toàn thông tin là một lĩnh vực liên tục phát triển, đặc biệt là trong bối cảnh các mối đe dọa ngày càng tinh vi và đa dạng. Việc áp dụng các biện pháp bảo mật toàn diện và linh hoạt là rất cần thiết để bảo vệ các tài sản thông tin quan trọng.

## Các loại hình tấn công mạng máy tính không dây

### Tấn công bị động - Passive Attacks

Tấn công bị động là một phương pháp tấn công WLAN đơn giản nhất nhưng vẫn rất hiệu quả. Passive attack không để lại một dấu vết nào chứng tỏ đã có sự hiện diện của hacker trong mạng vì hacker không thật kết nối với AP để lắng nghe các gói tin truyền trên đoạn mạng không dây.

### Tấn công chủ động - Active Attacks

Tấn công chủ động là tấn công trực tiếp vào một hoặc nhiều thiết bị trên mạng, ví dụ như vào AP, STA. Cuộc tấn công chủ động có thể được dùng để tìm cách truy nhập tới một Server để thăm dò, lấy những dữ liệu quan trọng, thậm chí thực hiện thay đổi cấu hình cơ sở hạ tầng mạng. Kiểu tấn công này dễ phát hiện nhưng khả năng phá hoại của nó rất nhanh và nhiều, khi phát hiện ra chúng ta chưa kịp có phương pháp đối phó thì nó đã thực hiện xong quá trình phá hoại.

### Tấn công kiểu chèn ép - Jamming Attacks

Phương thức Jamming là sử dụng máy phát có tần số phát giống tần số mà mạng sử dụng để áp đảo làm mạng bị nhiễu, bị ngừng làm việc. Tấn công bằng Jamming không phải là sự đe dọa nghiêm trọng, nó khó có thể được thực hiện phổ biến do vấn đề giá cả của thiết bị, nó quá đắt trong khi kẻ tấn công chỉ tạm thời vô hiệu hóa được mạng.

### Tấn công theo kiểu thu hút - Man in the Middle Attacks

Tấn công theo kiểu thu hút là dùng một khả năng mạnh hơn chen vào giữa hoạt động của các thiết bị và thu hút, giành lấy sự trao đổi thông tin của thiết bị về mình. Thiết bị chèn giữa đó phải có vị trí, khả năng thu phát trội hơn các thiết bị sẵn có của mạng.

### Tấn công vào các yếu tố con người

Đây là một hình thức tấn công nguy hiểm nhất nó có thể dẫn tới những tổn thất hết sức khó lường. Kẻ tấn công có thể liên lạc với người quản trị hệ thống thay đổi một số thông tin nhằm tạo điều kiện cho các phương thức tấn công khác.

### Một số kiểu tấn công khác

Ngoài các hình thức tấn công kể trên, kẻ tấn công còn sử dụng một số kiểu tấn công khác như tạo ra các virus đặt nằm tiềm ẩn trên các file khi người sử dụng do vô tình trao đổi thông tin qua mạng không dây mà người sử dụng đã tự cài đặt nó lên trên máy của mình.

## Giải pháp đảm bảo an ninh an toàn mạng máy tính không dây

### Bảo mật bằng WEP (Wired Equivalent Privacy)

WEP là một thuật toán bảo nhằm bảo vệ sự trao đổi thông tin chống lại sự nghe trộm, chống lại những kết nối mạng không được cho phép cũng như chống lại việc thay đổi hoặc làm nhiễu thông tin truyền. WEP sử dụng stream cipher RC4 cùng với một mã 40 bit và một số ngẫu nhiên 24 bit (initialization vector - IV) để mã hóa thông tin. Thông tin mã hóa được tạo ra bằng cách thực hiện phép toán XOR giữa keystream và plain text. Thông tin mã hóa và IV sẽ được gửi đến người nhận. Người nhận sẽ giải mã thông tin dựa vào IV và khóa WEP đã biết trước.

Những điểm yếu về bảo mật của WEP:

* WEP sử dụng khóa cố định được chia sẻ giữa một AP (Access) và nhiều người dùng cùng với một IV ngẫu nhiên 24 bit. Do đó, cùng một IV sẽ được sử dụng lại nhiều lần. Bằng cách thu thập thông tin truyền đi, kẻ tấn công có thể có đủ thông tin cần thiết để có thể bẻ khóa WEP đang dùng.
* Một khi WEP đã được biết, kẻ tấn công có thể giải mã thông tin truyền đi và có thể thay đổi nội dung của thông tin truyền.
* Việc sử dụng một khóa cố định được chọn bởi người sử dụng và ít khi được thay đổi (tức có nghĩa là khóa WEP không được tự động thay đổi) làm cho WEP rất dễ bị tấn công.
* WEP cho phép người dùng (supplicant) xác minh (authenticate) AP trong khi AP không thể xác minh tính xác thực của người dùng. Nói một cách khác, WEP không cung ứng mutual authentication.

### Bảo mật bằng WPA (Wifi Protected Access)

WPA là một giải pháp bảo mật được đề xuất bởi liên minh WiFi nhằm khắc phục những hạn chế của WEP. WPA được nâng cấp bằng việc cập nhật phần mềm SP2 của Microsoft.

WPA cải tiến 3 điểm yếu nổi bật của WEP :

* WPA cũng mã hóa thông tin bằng RC4 nhưng chiều dài của khóa là 128 bit và IV có chiều dài là 48 bit. Một cải tiến của WPA là WPA sử dụng giao thức TKIP nhằm thay đổi khóa dùng AP và user một cách tự động trong quá trình trao đổi thông tin.
* WPA sử dụng 802.1x/EAP để đảm bảo tính nhận thực lẫn nhau chống lại kiểu tấn công xen vào giữa. Quá trình nhận thực dựa trên một server nhận thực (Radius/Diameter).
* WPA sử dụng thuật toán kiểm tra tính toàn vẹn của bản tin MIC để tăng cường tính toàn vẹn của thông tin truyền. MIC là bản tin 64 bit được tính dựa trên thuật toán Michael. MIC được gửi trong gói TKIP, giúp người nhận kiểm tra xem thông tin nhận được có bị lỗi trên đường truyền hoặc bị thay đổi bởi kẻ phá hoại hay không.

Những điểm yếu của WPA :

* Điểm yếu đầu tiên của WPA là nó vẫn không giải quyết được kiểu tấn công từ chối dịch vụ. Kẻ phá hoại có thể làm nhiễu mạng WPA WiFi bằng cách gửi ít nhất hai gói thông tin với một khóa sai mỗi giây.
* Ngoài ra, WPA vẫn sử dụng thuật toán RC4 mà có thể dễ dàng bị bẻ vỡ bởi tấn công FMS đã được đề xuất bởi những nhà nghiên cứu ở trường đại học Berkeley. Hệ thống mã hóa RC4 chứa đựng những khóa yếu. Những khóa yếu này cho phép truy ra khóa mã. Để có thể tìm ra khóa yếu của RC4, chỉ cần thu thập một số lượng đủ thông tin truyền trên kênh truyền không dây

### Bảo mật bằng WPA2

Đến năm 2006, WPA chính thức bị thay thế bởi WPA2. Một trong những cải tiến đáng chú ý nhất của WPA2 so với WPA là sự có mặt bắt buộc của AES và CCMP nhằm thay thế cho TKIP. AES sử dụng thuật toán mã hóa đối xứng theo khối Rijndael, sử dụng khối mã hóa 128 bit và 192 bit hoặc 256 bit. Chuẩn mã hóa này được sử dụng cho các cơ quan chính phủ Mỹ để bảo vệ các thông tin nhạy cảm.

# XÂY DỰNG ĐỀ TÀI

## Aircrack là gì?

Aircrack-ng là một bộ phần mềm mạng bao gồm công cụ dò tìm, dò gói, bẻ khóa WEP và WPA / WPA2-PSK và công cụ phân tích cho các mạng LAN không dây 802.11. Nó hoạt động với bất kỳ bộ điều khiển giao diện mạng không dây nào có trình điều khiển hỗ trợ chế độ giám sát thô và có thể đánh hơi lưu lượng 802.11a, 802.11b và 802.11g. Chương trình chạy trên Linux, FreeBSD, mac OS, OpenBSD và Windows.

Vào tháng 4 năm 2007, một nhóm nghiên cứu tại Đại học Công nghệ Darmstadt ở Đức đã phát triển một phương pháp tấn công mới dựa trên một bài báo phát hành về mật mã RC4 của Adi Shamir. Cuộc tấn công mới này, được đặt tên là 'PTW', làm giảm số lượng vectơ khởi tạo hoặc IV cần thiết để giải mã khóa WEP và đã được đưa vào bộ aircrack-ng kể từ bản phát hành 0.9.

Aircrack-ng là một ngã ba của dự án Aircrack ban đầu. Nó có thể được tìm thấy như một công cụ được cài đặt sẵn trong nhiều bản phân phối Linux như Kali Linux hoặc Parrot, có chung các thuộc tính khi chúng được phát triển trong cùng một dự án (Debian).

Aircrack- ng là một bộ công cụ hoàn chỉnh để đánh giá an ninh mạng WiFi. Nó tập trung vào các lĩnh vực bảo mật WiFi khác nhau:

* Giám sát: Chụp gói và xuất dữ liệu sang tệp văn bản để xử lý thêm bằng các công cụ của bên thứ ba
* Tấn công: Phát lại các cuộc tấn công, hủy xác thực, điểm truy cập giả mạo và những thứ khác thông qua chèn gói
* Kiểm tra: Kiểm tra thẻ WiFi và khả năng của trình điều khiển (chụp và chèn)
* Bẻ khóa: WEP và WPA PSK (WPA 1 và 2)

Tất cả các công cụ đều là dòng lệnh cho phép tạo script nặng. Rất nhiều GUI đã tận dụng tính năng này. Nó hoạt động chủ yếu trên Linux nhưng cũng có Windows, OS X, FreeBSD, OpenBSD, NetBSD, cũng như Solaris và thậm chí cả eComStation 2.

## Ưu và nhược điểm của Aircrack-ng

Ưu điểm:

* Các nhà phát triển tiếp tục thực hiện các thay đổi và cập nhật rất thông minh
* Tất cả các công cụ là dòng lệnh cho phép kịch bản nặng

Nhược điểm:

* Bạn cần các kỹ năng lập trình để tạo các tệp DLL của riêng bạn
* Có thể được sử dụng cho nhiều mục đích bất chính

## Cách sử dụng Aircrack-ng

Câu lệnh sử dụng Aircrack – ng: aircrack-ng [các chế độ] <file bắt được>

Table : Các chế độ cơ bản

|  |  |  |
| --- | --- | --- |
| Chế độ | Tham số | Mô tả |
| -a | amode | Lựa chọn chế độ tấn công (1 = WEP tĩnh, 2 = WPA/WPA2-PSK) |
| -e | essid | Nếu được sử dụng, tất cả IV (Initialization Vector (Vector khởi tạo)) từ các mạng có cùng ESSID sẽ được sử dụng. Chế độ này cũng được sử dụng để phá khóa WPA/WPA2-PSK nếu ESSID không phát quảng bá (chế độ ẩn) |
| -b | bssid | Viết ngắn gọn của –bssid. Chọn một mạng chỉ định dựa vào địa chỉ MAC của điểm truy cập. |
| -p | nbcpu | Trên hệ thống SMP. Chế độ này không được sử dụng nếu không phải hệ thống SMP. |
| -q | none | Chế độ yên lặng (không hiển thị trạng thái kể cả khi tìm thấy khóa) |
| -C | MACs | Viết tắt của –combine. Kết hợp các điểm truy cập được cung cấp (ngăn cách bởi dấu phẩy) thành một điểm truy cập ảo. |
| -l | file name | (chữ L viết thường) Ghi khóa vào tệp được chỉ định. Ghi đè tệp nếu nó đã tồn tại. |

Table 2: Các chế độ phá khóa WEP tĩnh

|  |  |  |
| --- | --- | --- |
| Chế độ | Tham số | Mô tả |
| -c | none | Giới hạn không gian tìm kiếm chỉ trong các ký tự chữ và số (0x20 - 0x7F) |
| -t | none | Giới hạn không gian tìm kiếm trong các ký tự hex thập phân được mã hóa nhị phân |
| -h | none | Giới hạn không gian tìm kiếm ở các ký tự số (0x30-0x39) Các khóa này được sử dụng theo mặc định trong hầu hết Fritz!BOXes |
| -d | start | Viết ngắn gọn của –debug. Cài đặt vị trí bắt đầu của khóa WEP (bằng hex), cho mục debug. |
| -m | maddr | Địa chỉ MAC để lọc gói dữ liệu WEP. Ngoài ra, chỉ định -m ff: ff: ff: ff: ff: ff để sử dụng tất cả và mọi IVs, bất kể mạng nào |
| -n | nbits | Chỉ định độ dài của khóa: 64 cho WEP 40 bit, 128 cho WEP 104 bit, v.v. Giá trị mặc định là 128 |
| -i | index | Chỉ giữ lại các IV có key index này (1 đến 4). Chế độ mặc định bỏ qua key index |
| -f | fudge | Theo mặc định, tham số này được đặt thành 2 cho WEP 104 bit và thành 5 cho WEP 40 bit. Chỉ định giá trị cao hơn để tăng mức độ vét cạn: việc phá khóa sẽ mất nhiều thời gian hơn, nhưng khả năng thành công cao hơn |
| -k | korek | Có 17 cuộc tấn công thống kê Korek. Đôi khi một cuộc tấn công tạo ra một dương tính giả rất lớn khiến khóa không được tìm thấy, ngay cả với rất nhiều IV. Hãy thử -k 1, -k 2,… -k 17 để vô hiệu hóa từng đòn tấn công một cách chọn lọc |
| -x/-x0 | none | Tắt chế độ vét cạn keybytes cuối cùng |
| -x1 | none | Bật chế độ vét cạn keybytes cuối cùng (mặc định) |
| -x2 | none | Bật chế độ vét cạn hai keybytes cuối cùng |
| -X | none | Tắt chế độ vét cạn đa luồng (chỉ dành cho SMP) |
| -s | none | Hiện khóa ở dạng ASCII khi trong quá trình phá khóa |
| -y | none | Chế độ tấn công vét cạn đơn lẻ thử nghiệm chỉ nên được sử dụng khi chế độ tấn công tiêu chuẩn không thành công với hơn một triệu IVs |
| -z | none | Sử dụng phương pháp phá khóa PTW WEP (Mặc định ở v1.x) |
| -P | number | Viết ngắn gọn của --ptw-debug. Sử dụng chế độ debug PTW: 1 Tắt klein, 2 PTW. |
| -K | none | Sử dụng phương pháp phá khóa Korek WEP. (Mặc định ở v0.x) |
| -D | none | Viết ngắn gọn của –wep-decloak. Chạy ở chế độ WEP decloak. |
| -1 | none | Viết ngắn gọn của –oneshot. Chạy 1 lần thử duy nhất để phá khóa với PTW |
| -M | number | (Phá khóa WEP) cài đặt độ dài lớn nhất để dùng của IVs |
| -V | none | Viết ngắn gọn của –visual-inspection. Chạy ở chế độ kiểm tra trực quan (chỉ dùng với Korek) |

Table 3: Các chế độ phá khóa WEP và WPA-PSK

|  |  |  |
| --- | --- | --- |
| Chế độ | Tham số | Mô tả |
| -w | words | Đường dẫn đến từ điển hoặc “-” không có dấu ngoặc kép cho tiêu chuẩn trong (stdin). Phân tách nhiều danh sách từ bằng dấu phẩy |
| -N | file | Tạo một phiên phá khóa mới và lưu nó vào tệp được chỉ định |
| -R | file | Khôi phục phiên bẻ khóa từ tệp được chỉ định |

Table 4: Các chế độ WPA-PSK

|  |  |  |
| --- | --- | --- |
| Chế độ | Tham số | Mô tả |
| -E | file> | Tạo EWSA Project file v3 |
| -j | file | Tạo Hashcat v3.6+ Capture file (HCCAPX) |
| -J | file | Tạo Hashcat Capture file |
| -S | none | Kiểm nghiệm tốc độ phá khóa WPA |
| -Z | sec | Kiêm nghiệm tốc độ phá khóa WPA tính bằng giây |
| -r | database | Sử dụng cơ sở dữ liệu do airolib-ng tạo ra làm đầu vào để xác định khóa WPA. Xuất ra thông báo lỗi nếu aircrack-ng chưa được biên dịch với sự hỗ trợ của sqlite |

Table 5: SIMD

|  |  |  |
| --- | --- | --- |
| Chế độ | Tham số | Mô tả |
| --simd | optimization | Sử dụng tối ưu hóa SIMD do người dùng chỉ định thay vì tối ưu hóa nhanh nhất |
| --simd-list | none | Hiển thị danh sách các tối ưu hóa SIMD có sẵn |

Table 6: Các chế độ khác

|  |  |  |
| --- | --- | --- |
| Chế độ | Tham số | Mô tả |
| -H | none | Viết tắt của –help. Hiển thị thông tin trợ giúp. |
| -u | none | Dạng đầy đủ --cpu-detect. Cung cấp thông tin về số lượng CPU và các tính năng có sẵn như MMX, SSE2, AVX, AVX2, AVX512 |

## Kali Linux là gì?

Kali Linux là một hệ điều hành mã nguồn mở dựa trên Debian, được phát triển và duy trì bởi Offensive Security. Kali Linux được thiết kế đặc biệt cho việc kiểm tra bảo mật và nghiên cứu an ninh mạng, với một loạt các công cụ được tích hợp sẵn để thực hiện các nhiệm vụ như kiểm tra thâm nhập (penetration testing), phân tích pháp lý kỹ thuật số (digital forensics), và tấn công mật khẩu (password attacks).

## Các Đặc Điểm Chính của Kali Linux:

1. **Công Cụ Tích Hợp:** Kali Linux đi kèm với hơn 600 công cụ bảo mật đã được cài đặt sẵn, bao gồm nmap (máy quét mạng), Wireshark (phân tích giao thức mạng), Metasploit (khung công cụ kiểm tra thâm nhập), và nhiều công cụ khác.
2. **Bảo Mật và Cập Nhật:** Kali Linux thường xuyên được cập nhật để đảm bảo tính bảo mật và hiệu suất. Nó cũng hỗ trợ bảo mật tuyệt đối cho người dùng với các tính năng như mật mã hoá dữ liệu.
3. **Đa Nền Tảng:** Kali Linux có thể chạy trên nhiều nền tảng phần cứng khác nhau, từ máy tính để bàn, máy tính xách tay đến các thiết bị ARM như Raspberry Pi.
4. **Tùy Biến Cao:** Người dùng có thể tùy chỉnh Kali Linux theo nhu cầu riêng của mình. Có thể tạo ra các phiên bản tùy chỉnh với các công cụ và cấu hình riêng biệt.
5. **Hỗ Trợ Từ Cộng Đồng:** Kali Linux có một cộng đồng người dùng và nhà phát triển lớn, cung cấp tài liệu, hướng dẫn, và hỗ trợ kỹ thuật.

## Cách sử dụng Kali Linux

Kali Linux chủ yếu được sử dụng bởi các chuyên gia bảo mật, hacker mũ trắng, và các tổ chức an ninh mạng để:

\* **Kiểm Tra Thâm Nhập:** Đánh giá mức độ bảo mật của hệ thống bằng cách giả lập các cuộc tấn công để tìm ra các lỗ hổng.

\* **Phân Tích Pháp Lý Kỹ Thuật Số:** Khám phá và phục hồi dữ liệu từ các thiết bị số để sử dụng trong điều tra.

\* **Nghiên Cứu và Học Tập:** Đào tạo về an ninh mạng và phát triển kỹ năng bảo mật.

## Wireshark là gì?



Hình : Wireshark.

Wireshark là một ứng dụng dùng để bắt (capture), phân tích và xác định các vấn đề liên quan đến network như: rớt gói tin, kết nối chậm, hoặc các truy cập bất thường. Phần mềm này cho phép quản trị viên hiểu sâu hơn các Network Packets đang chạy trên hệ thống, qua đó dễ dàng xác định các nguyên nhân chính xác gây ra lỗi.

Sử dụng WireShark có thể capture các packet trong thời gian thực (real time), lưu trữ chúng lại và phân tích chúng offline. Ngoài ra, nó cũng bao gồm các filter, color coding và nhiều tính năng khác, cho phép người dùng tìm hiểu sâu hơn về lưu lượng mạng cũng như inspect (kiểm tra) các packets.

Dưới đây là một số chức năng chính của Wireshark:

+ **Phân tích Gói Tin:** Wireshark cho phép bạn theo dõi và phân tích từng gói tin dữ liệu trên mạng. Bạn có thể xem các thông tin chi tiết như nguồn, đích, loại gói tin, dữ liệu payload và nhiều thông tin khác.

+ **Đánh giá Hiệu suất Mạng:** Wireshark cung cấp thông tin về thời gian phản hồi (response time), độ trễ (latency), và các thống kê khác, giúp đánh giá hiệu suất của mạng.

+ **Phân tích Giao thức:** Wireshark hỗ trợ nhiều giao thức mạng khác nhau. Bạn có thể xem và phân tích giao thức HTTP, TCP, UDP, IP, DNS, và nhiều giao thức khác.

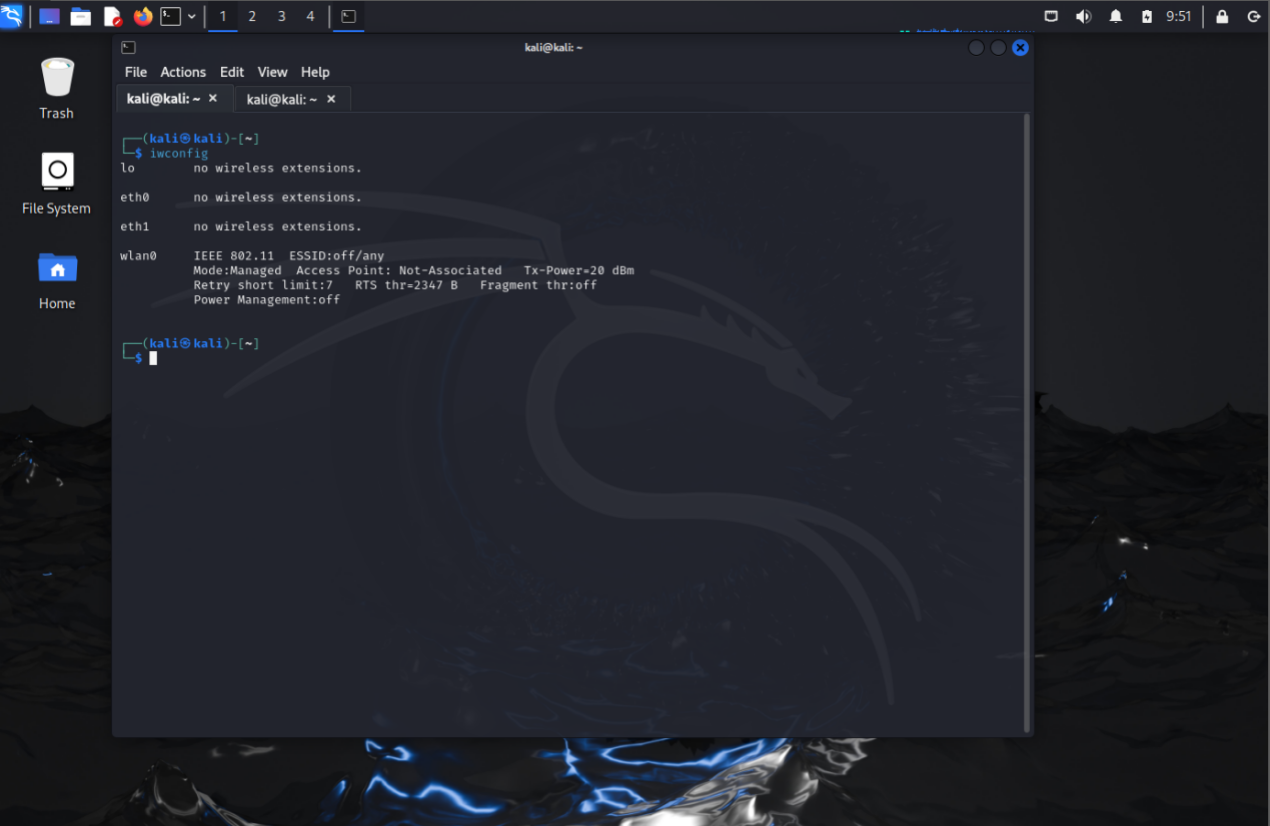
+ **Điều tra Vấn đề Mạng:** Khi xảy ra vấn đề mạng, Wireshark là một công cụ mạnh mẽ để phân tích và xác định nguyên nhân của sự cố.

+ **Bảo mật Mạng:** Wireshark có thể được sử dụng để phát hiện các hoạt động độc hại trên mạng. Nó cho phép bạn xem gói tin để phát hiện các tấn công mạng, như phishing hoặc kiểm soát truy cập không được ủy quyền.

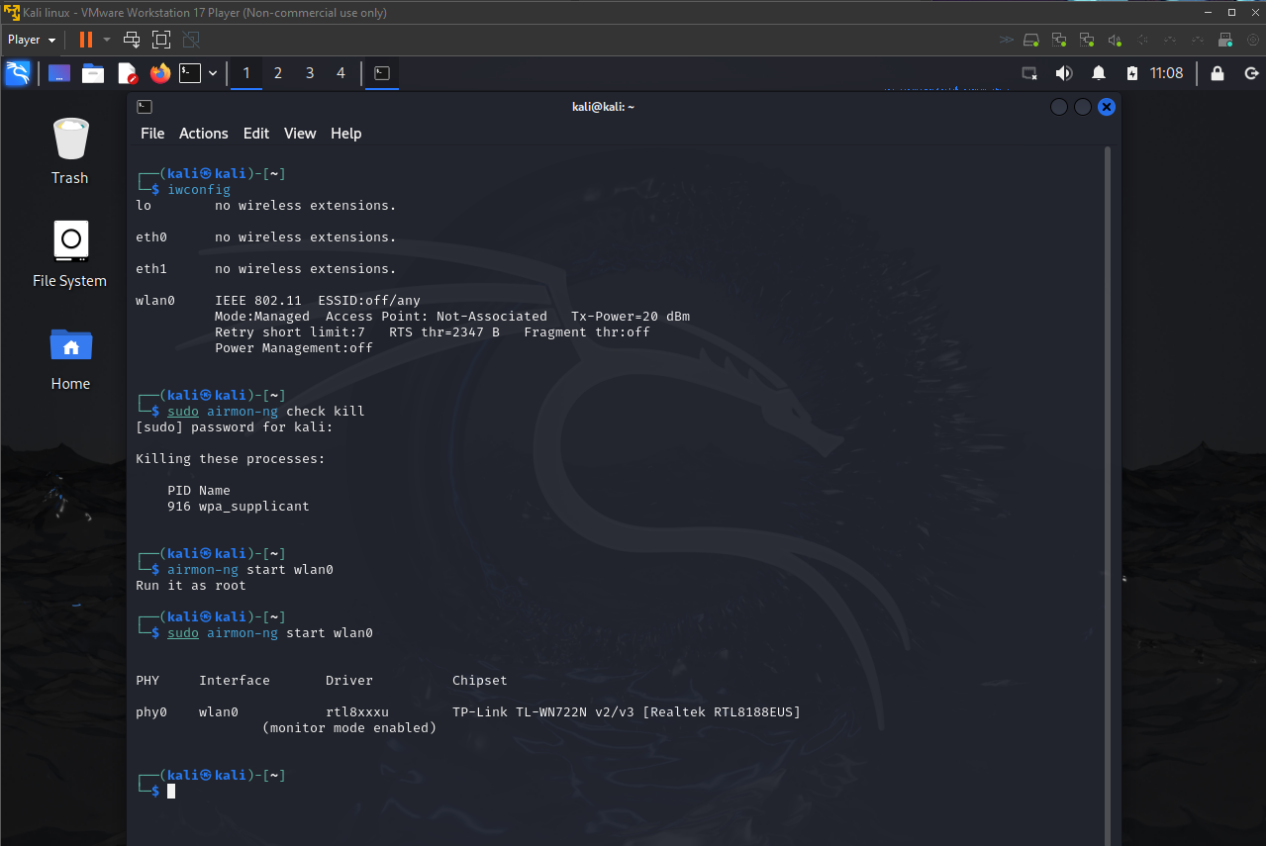
+ **Giáo dục và Học tập:** Wireshark là một công cụ hữu ích cho sinh viên, chuyên gia mạng, và người quan tâm đến việc hiểu rõ cách mạng hoạt động. Nó cung cấp một cách thức thực hành để nắm bắt và hiểu các khái niệm mạng.

# CHƯƠNG TRÌNH DEMO

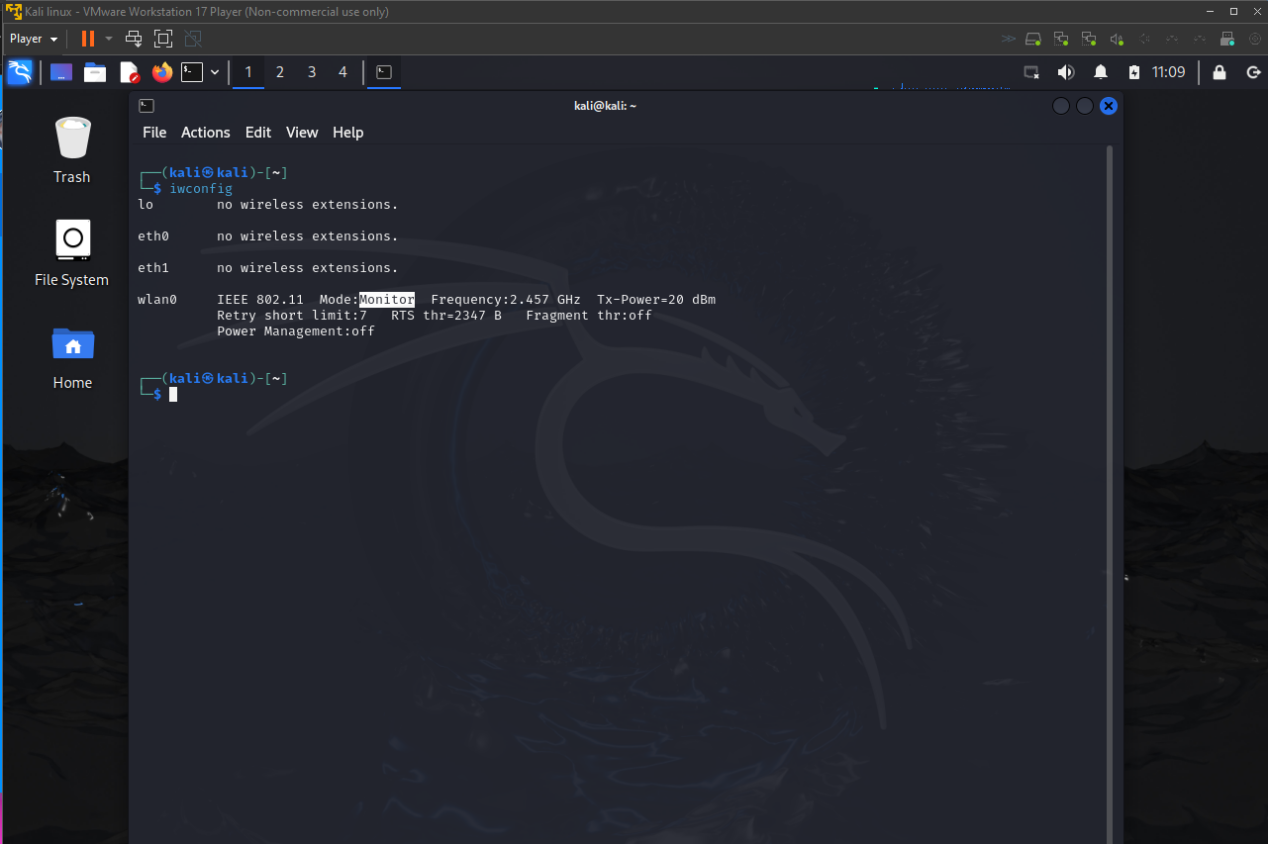
\* PHẦN 1: BẺ KHÓA MẬT KHẨU WIFI



Hình : Kiểm tra card mạng



Hình : Chuyển card mạng sang chế độ monitor



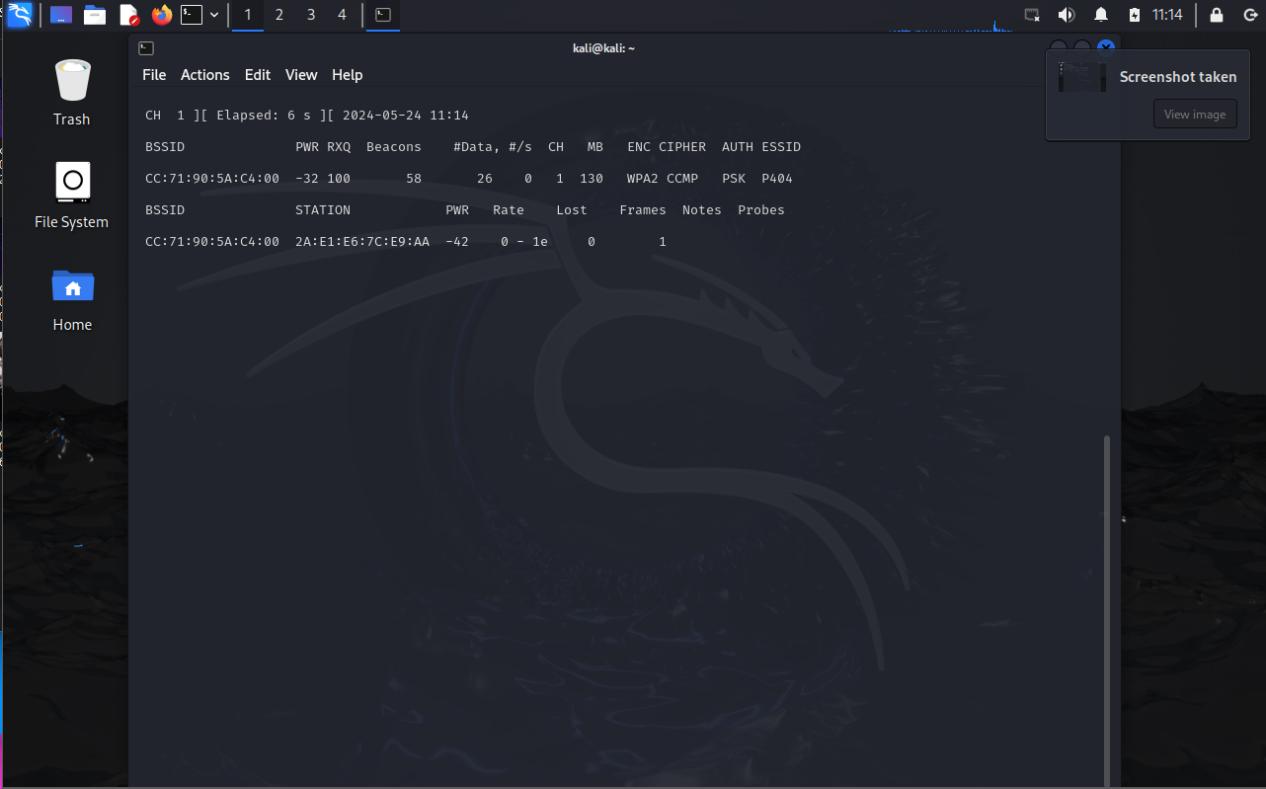
Hình : Xác nhận card mạng đã chuyển sang chế đọ monitor



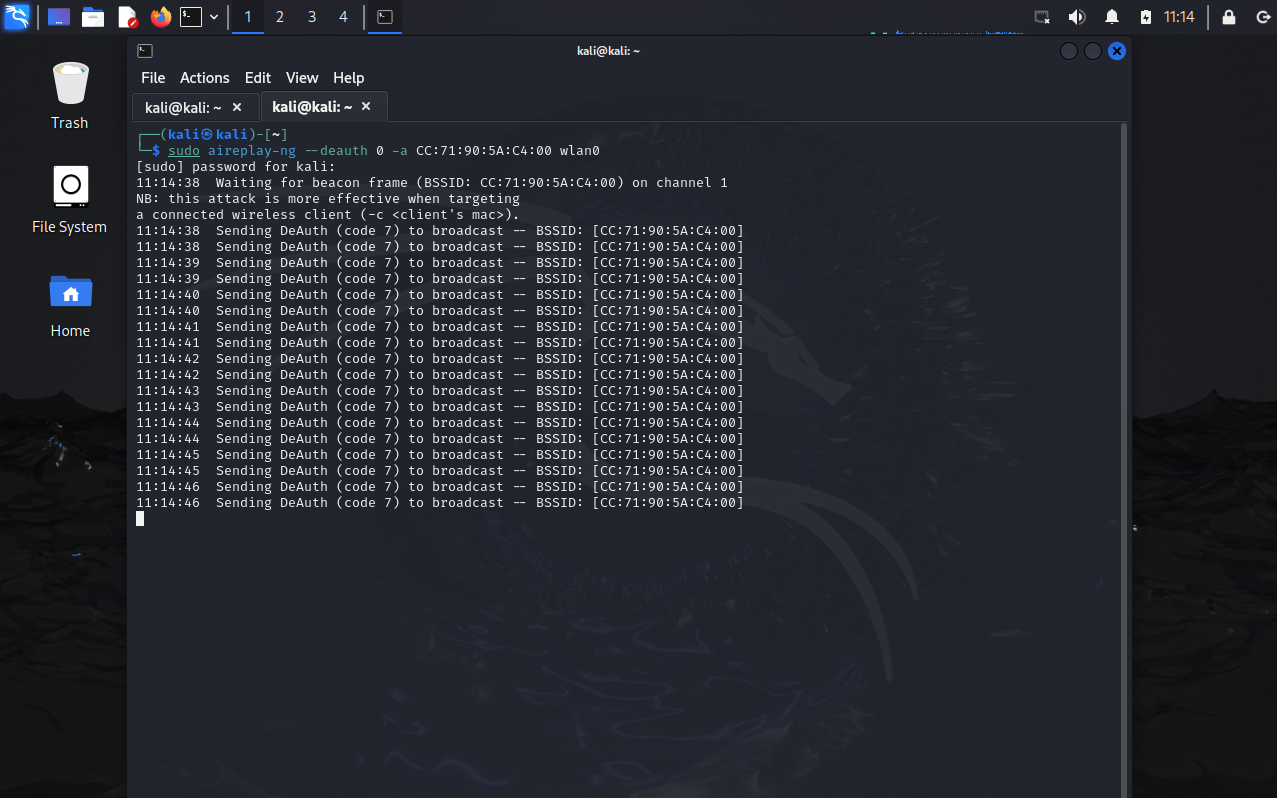
Hình : Theo dõi các hoạt động các mạng wifi hiện tại qua card wlan0



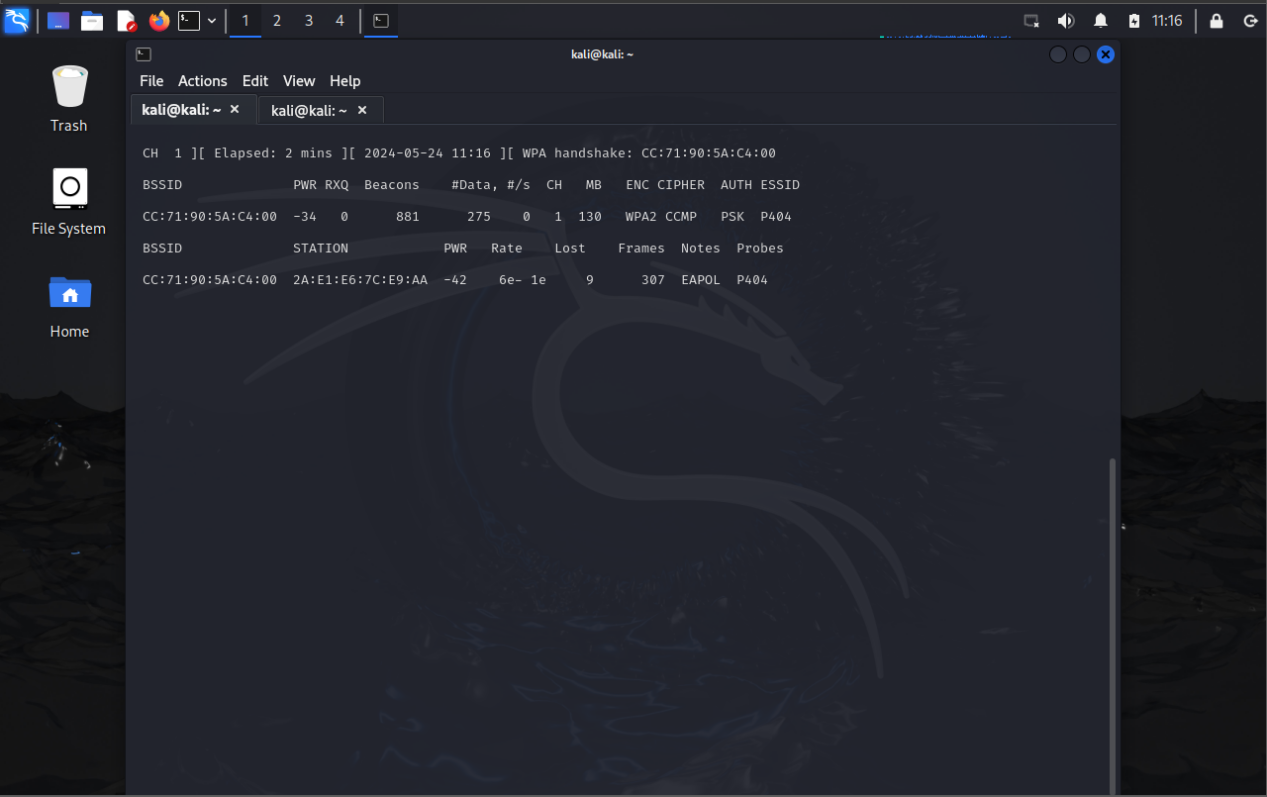
Hình : Xác định mạng cần tấn công



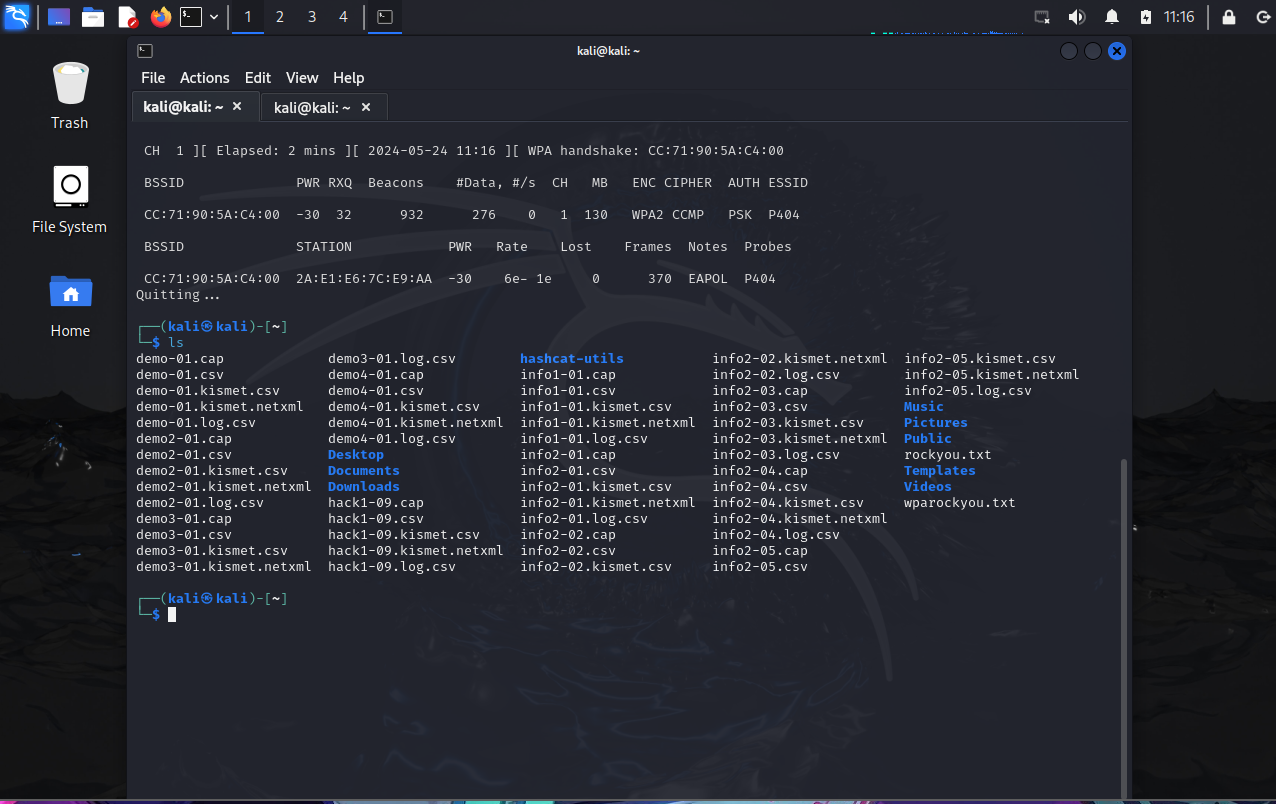
Hình : Bắt gói tin và theo dõi duy nhất một mạng cần tấn công



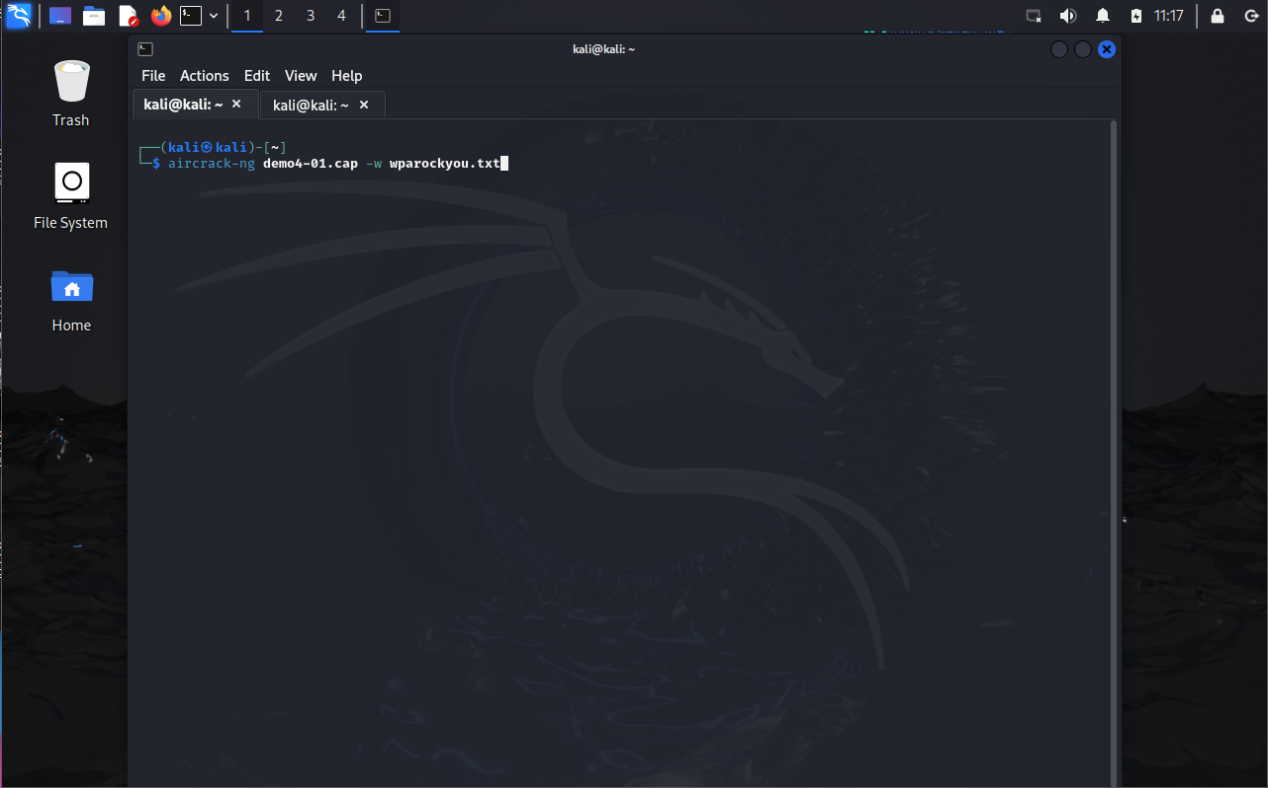
Hình : Kick người dùng thoát ra và đăng nhập lại mạng



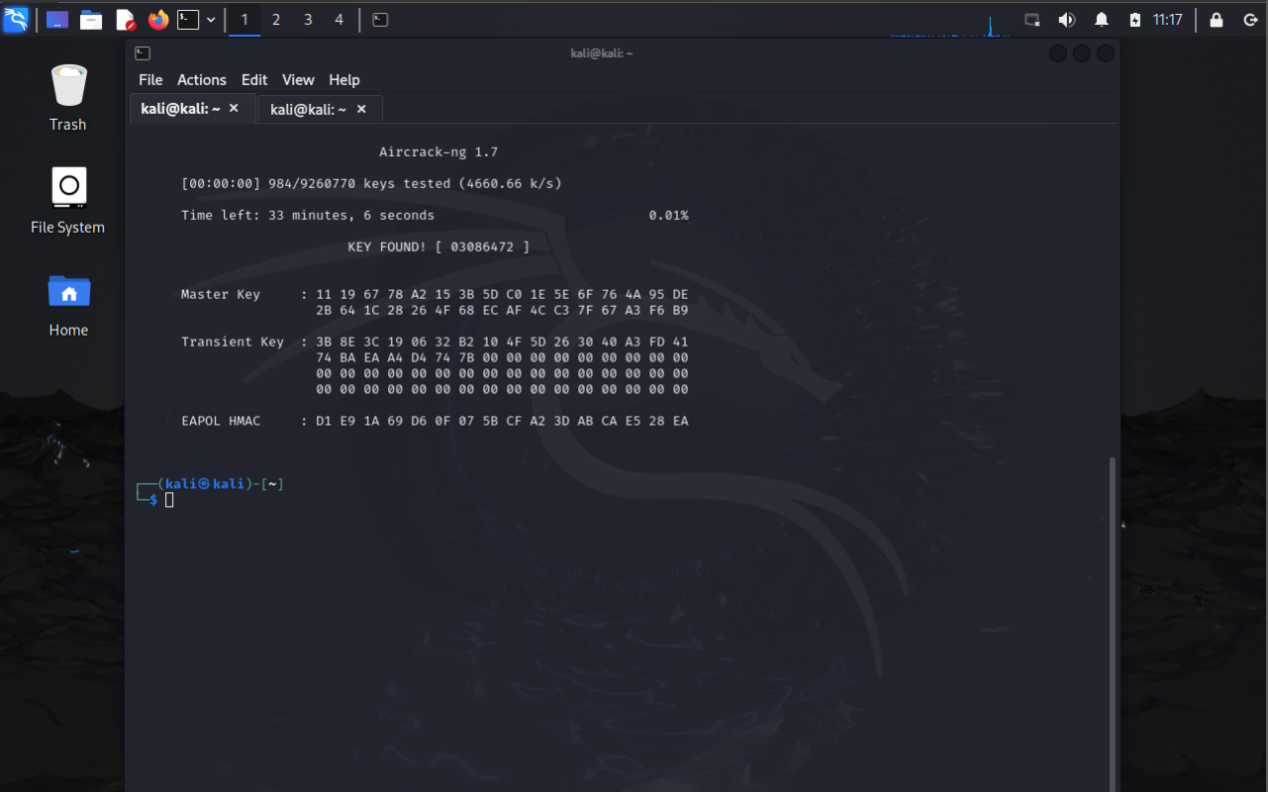
Hình : Bắt WPA handshake key



Hình : Key WPA handshake đã được lưu vào file

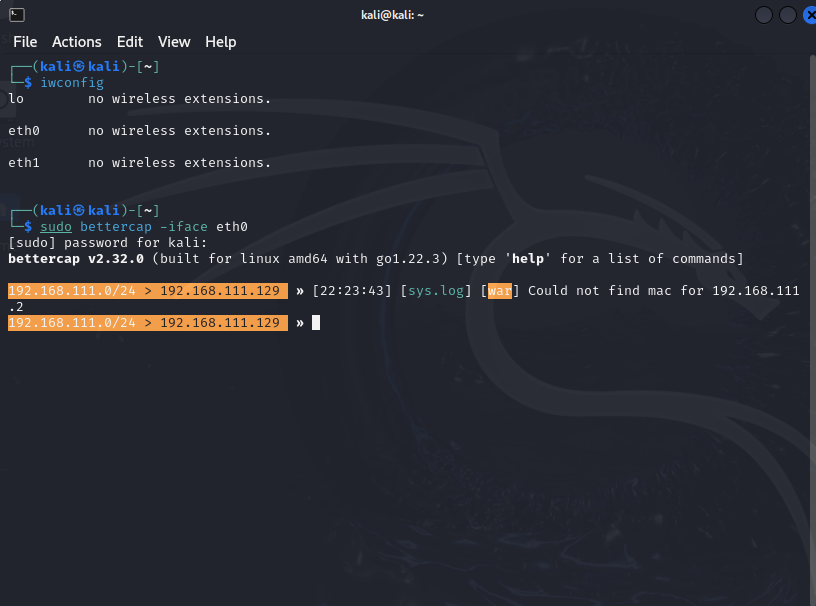


Hình : Dùng lệnh để tìm password trong wordlist

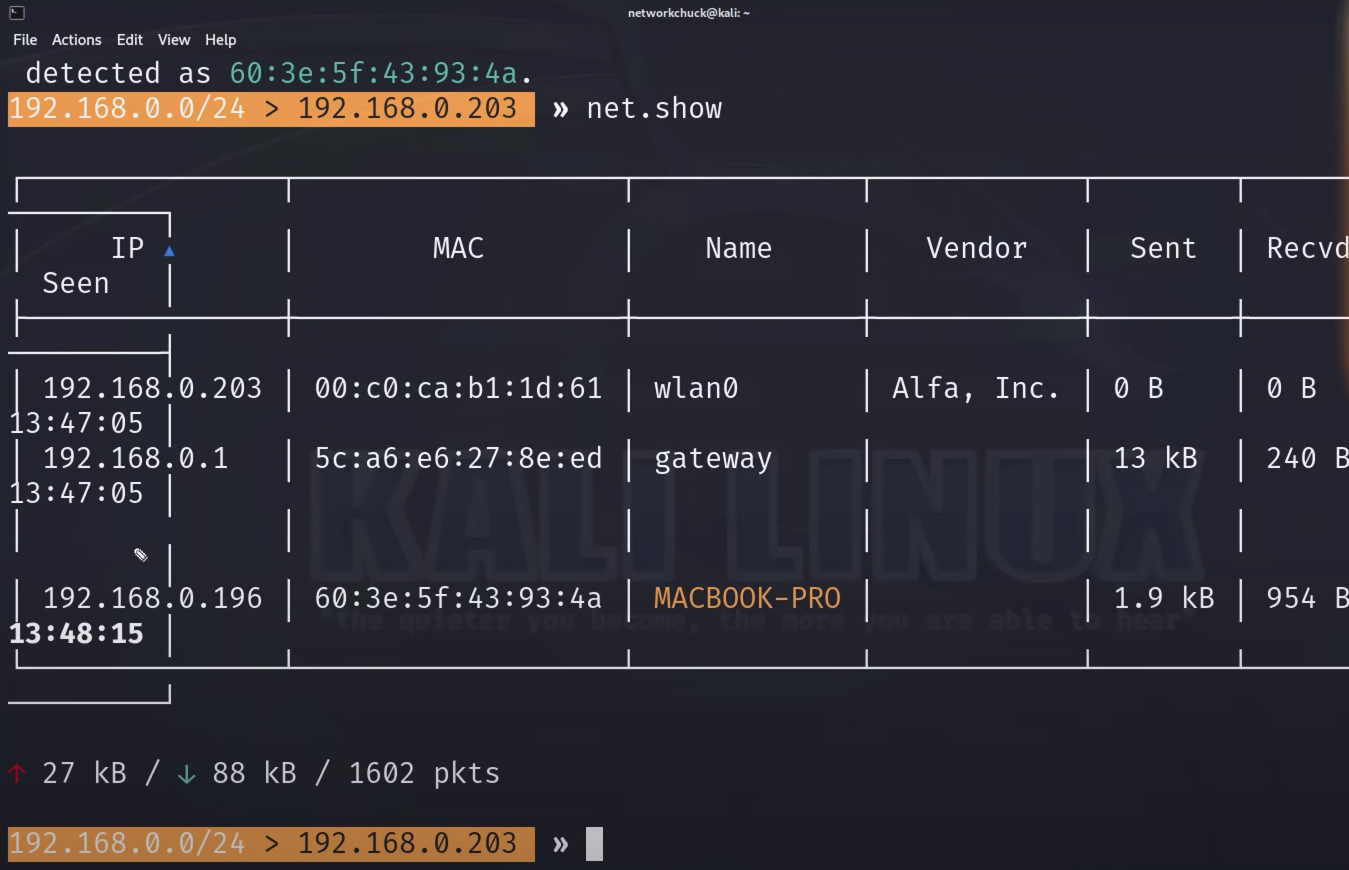


Hình : Kết quả

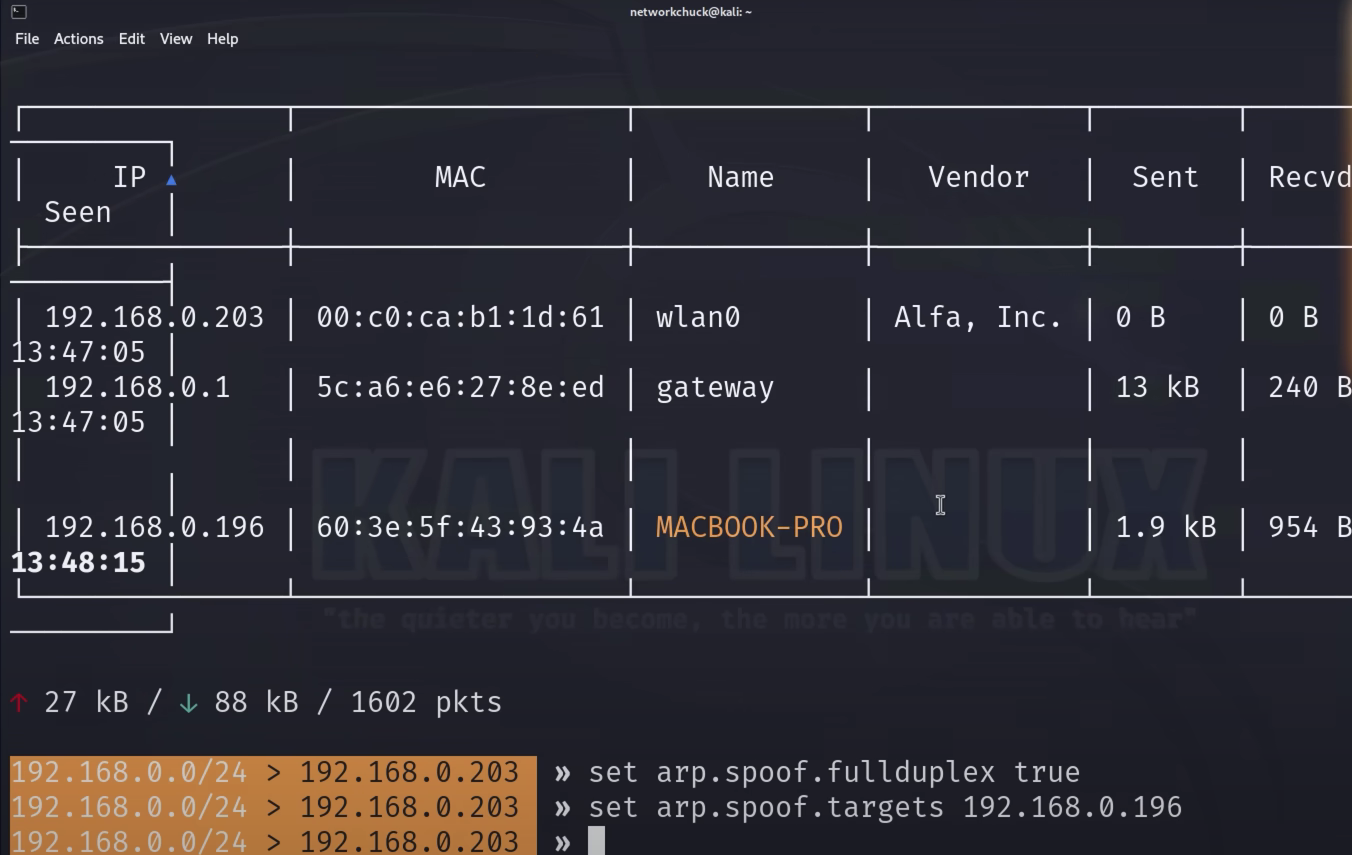
\* PHẦN 2: TẤN CÔNG



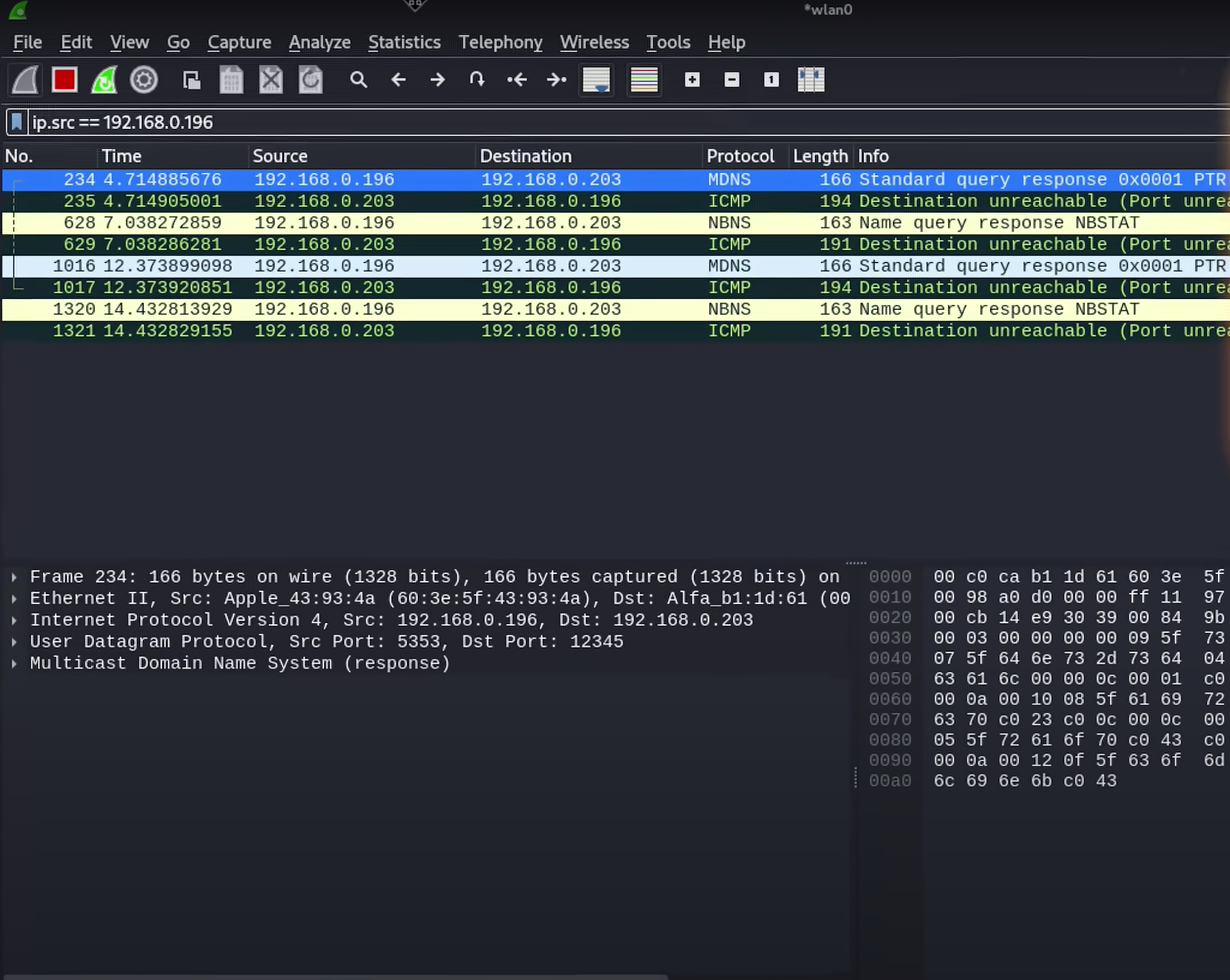
Hình : Chọn card mạng



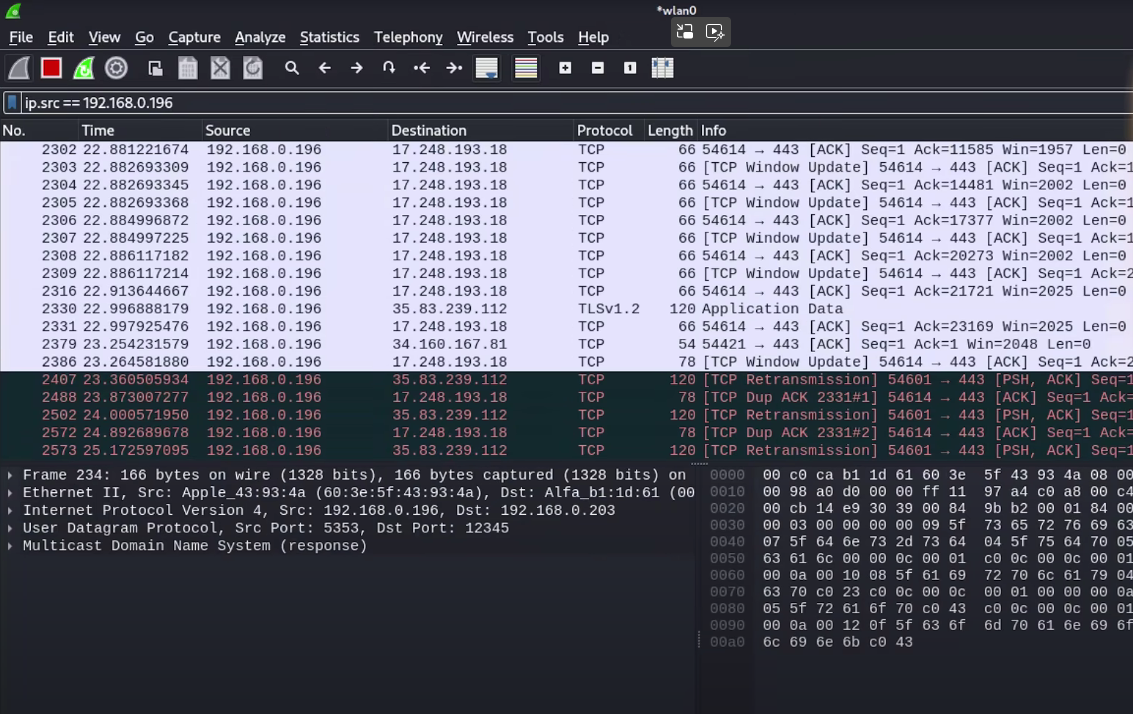
Hình : Hiển thị danh sách thiết bị truy cập



Hình : Đặt mục tiêu cần tấn công



Hình : Trước khi bật spoof on



Hình : Sau khi bật spoof on

KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Kết luận: Trong thời gian thực hiện đề tài:

##### Kết quả đạt được

* Về mặt lý thuyết: Đã tìm hiểu và phân tích được các chức năng, nguyên lý hoạt động của công cụ Aircrack-ng.
* Hiểu rõ các kỹ thuật tấn công và đánh giá bảo mật mạng WiFi bằng Aircrack-ng, như bắt gói tin, phân tích mã hóa, tấn công từ điển và tấn công từ từ.
* Về thực nghiệm: đã xây dựng được hệ thống thực hiện các chức năng cơ bản….

##### Hạn chế và hướng phát triển

* Hạn chế:

+ Vì thời gian có hạn nên chúng em nghiên chưa đầy đủ tất cả các tính năng của aircrack-ng.

+ Chưa bẻ khóa được bảo mật WPA3.

+ Chưa nghiên cứu được cách đọc gói tin để lấy thông tin.

* Hướng phát triển:

+ Nghiên cứu sâu hơn các tính năng khác.

+ Từ kết quả đạt được ở trên chúng em sẽ nghiên cứu các cách lấy cắp thông tin từ các gói tin đã bắt được.

TÀI LIỆU THAM KHẢO

|  |
| --- |
| https://www.aircrack-ng.org/doku.php |
| https://www.lifewire.com/what-is-wi-fi-2377430 |
| https://www.rapid7.com/fundamentals/man-in-the-middle-attacks/ |
| https://en.wikipedia.org/wiki/Wi-Fi\_Protected\_Access |