|  |
| --- |
| BAN CƠ YẾU CHÍNH PHỦ  **HỌC VIỆN KỸ THUẬT MẬT MÃ**  Vector Logo] Học Viện Kỹ Thuật Mật Mã - ACTVN - Download Định Dạng EPS, SVG  Cho AI, Corel » Hải Triều  BÀI TẬP LỚN MÔN HỌC  **Kiểm thử và đánh giá An toàn hệ thống thông tin**  **ĐỀ TÀI: TÌM HIỂU VỀ WIRELESS PENTEST**  Ngành: An toàn thông tin  Sinh viên thực hiện:  **Nguyễn Công Thắng AT160252**  **Nguyễn Minh Đức AT160218**  **Bàn Văn Cường AT160210**  **Vũ Hồng Phúc AT160245**  Giảng viên hướng dẫn:  **ThS. Phạm Tiến Mạnh**  Khoa An toàn thông tin – Học viện Kỹ thuật mật mã    Hà Nội, 02-2023 |

MỤC LỤC

[MỤC LỤC 1](#_Toc127652208)

[LỜI CẢM ƠN 3](#_Toc127652209)

[LỜI NÓI ĐẦU 4](#_Toc127652210)

[CHƯƠNG 1. TỔNG QUAN LÝ THUYẾT 5](#_Toc127652211)

[1.1 Kiểm thử thâm nhập mạng không dây 5](#_Toc127652212)

[1.2 Kiểm thử thâm nhập mạng cục bộ không dây ( WLAN) 5](#_Toc127652213)

[1.3 Khám phá mạng không dây 6](#_Toc127652214)

[1.4 Kiểm tra bảo mật vật lý của các điểm truy cập ( AP) 7](#_Toc127652215)

[1.4.1 Phát hiện kết nối không dây 8](#_Toc127652216)

[1.5 Nghe lén lưu lượng giữa AP và các thiết bị được liên kết 9](#_Toc127652217)

[1.6 Tạo một điểm truy cập giả mạo 10](#_Toc127652218)

[1.7 Honeypot không dây 11](#_Toc127652219)

[1.8 Thực hiện tấn công từ chối dịch vụ DoS 12](#_Toc127652220)

[1.9 Tạo lưu lượng truy cập nhanh 13](#_Toc127652221)

[1.10 Giải mã gói tin 14](#_Toc127652222)

[1.11 Đầu độc ARP 14](#_Toc127652223)

[1.12 Tiêm một gói được mã hóa 16](#_Toc127652224)

[1.13 Lọc MAC 16](#_Toc127652225)

[1.14 Giả mạo MAC 17](#_Toc127652226)

[CHƯƠNG 2. TÌM HIỂU CÁC CÔNG CỤ 19](#_Toc127652227)

[2.1 Aircrack-ng 19](#_Toc127652228)

[2.1.1 Khái niệm về công cụ Aircrack-ng 19](#_Toc127652229)

[2.1.2 Những đặc điểm chính 19](#_Toc127652230)

[2.1.3 Đánh giá Aircrack-ng 19](#_Toc127652231)

[2.2 Crunch Kali Linux 20](#_Toc127652232)

[2.2.1 Khái niệm về công cụ Crunch 20](#_Toc127652233)

[2.2.2 Các tính năng của Crunch 21](#_Toc127652234)

[2.2.3 Tầm quan trọng của Crunch 21](#_Toc127652235)

[2.3 Wireshark 22](#_Toc127652236)

[2.3.1 Khái niệm Wireshark 22](#_Toc127652237)

[2.3.2 Các chức năng của Wireshark 22](#_Toc127652238)

[2.3.3 Tính năng 23](#_Toc127652239)

[2.3.4 Đánh giá Wireshark 23](#_Toc127652240)

[2.4 Nmap 24](#_Toc127652241)

[2.4.1 Khái niệm Nmap 24](#_Toc127652242)

[2.4.2 Tính năng Nmap 24](#_Toc127652243)

[2.4.3 Các kỹ thuật quét Nmap 24](#_Toc127652244)

[2.4.4 Ưu điểm Nmap 25](#_Toc127652245)

[2.5 Ettercap 25](#_Toc127652246)

[2.5.1 Khái niệm Ettercap 25](#_Toc127652247)

[2.5.2 Chức năng Ettercap 25](#_Toc127652248)

[2.5.3 Tính năng Ettercap 26](#_Toc127652249)

[CHƯƠNG 3. TRIỂN KHAI THỰC NGHIỆM 28](#_Toc127652250)

[3.1 Tấn công bẻ khoá mật khẩu WiFi 28](#_Toc127652251)

[3.1.1 Mô hình 28](#_Toc127652252)

[3.1.2 Kịch bản 28](#_Toc127652253)

[3.1.3 Thực nghiệm 28](#_Toc127652254)

[3.1.4 Đánh giá, kết luận 31](#_Toc127652255)

[3.2 Tấn công Man in the midle 31](#_Toc127652256)

[3.2.1 Mô hình 31](#_Toc127652257)

[3.2.2 Kịch bản 31](#_Toc127652258)

[3.2.3 Thực nghiệm 31](#_Toc127652259)

[3.2.4 Đánh giá, kết luận 31](#_Toc127652260)

[KẾT LUẬN 32](#_Toc127652261)

[TÀI LIỆU THAM KHẢO 33](#_Toc127652262)

LỜI CẢM ƠN

Trong quá trình thực hiện đồ án tốt nghiệp này, chúng tôi đã nhận được sự giúp đỡ tận tình của cán bộ hướng dẫn là TS. Phạm Tiến Mạnh – Giảng viên Khoa An toàn thông tin Học viện Kỹ thuật Mật mã.

Xin cảm ơn tất cả mọi người đã tạo những điều kiện tốt nhất để chúng tôi hoàn thành đồ án tốt nghiệp này!

|  |  |
| --- | --- |
|  | **SINH VIÊN THỰC HIỆN ĐỒ ÁN**  Nguyễn Công Thắng  Nguyễn Minh Đức  Bàn Văn Cường  Vũ Hồng Phúc |

LỜI NÓI ĐẦU

Trong thời đại công nghệ thông tin hiện nay, mạng không dây (Wireless Network) đã trở thành một phần không thể thiếu trong cuộc sống hàng ngày của chúng ta. Cùng với sự phát triển của công nghệ mạng, mạng không dây ngày càng trở nên phổ biến và đóng vai trò quan trọng trong việc kết nối các thiết bị với nhau.

Tuy nhiên, sự phát triển nhanh chóng của công nghệ không dây cũng đồng nghĩa với việc những mối đe dọa về bảo mật đang gia tăng. Trong khi đó, việc bảo vệ hệ thống mạng không dây trở nên ngày càng phức tạp hơn do sự phức tạp của các giao thức mạng.

Do đó, trong bài tập này, nhóm em sẽ tiến hành tấn công bẻ khoá mật khẩu wifi và từ đó xâm nhập vào hệ thống mạng. Sau đó tiến hành tấn công Man in the middle.

Hy vọng rằng đề tài của chúng em sẽ đem lại những giá trị thực tiễn và hữu ích cho cộng đồng trong việc tăng cường bảo mật mạng không dây.

# TỔNG QUAN LÝ THUYẾT

## Kiểm thử thâm nhập mạng không dây

Định nghĩa: Quá trình kiểm tra tính bảo mật của mạng không dây và thiết bị bằng cách mô phỏng các cuộc tấn công và xác định các lỗ hổng.

Mục tiêu: Để đánh giá hiệu quả của các biện pháp bảo mật mạng không dây và xác định các điểm yếu tiềm ẩn có thể bị khai thác bởi những kẻ tấn công.

Phạm vi: Bao gồm nhiều loại công nghệ không dây, bao gồm Wi-Fi, Bluetooth, di động và liên lạc vệ tinh.

Các bước chính:

* + Trinh sát: Thu thập thông tin về mạng mục tiêu, bao gồm SSID, địa chỉ MAC và cường độ tín hiệu.
  + Liệt kê: Xác định loại bảo mật không dây được sử dụng (WEP, WPA, WPA2, v.v.), khóa mã hóa và bất kỳ biện pháp bảo mật nào khác được áp dụng.
  + Khai thác: Cố gắng khai thác bất kỳ lỗ hổng nào được tìm thấy trong mạng hoặc thiết bị, chẳng hạn như mật khẩu yếu, điểm truy cập được định cấu hình sai hoặc phần mềm chưa được vá.
  + Báo cáo: Ghi lại các phát hiện và đưa ra các khuyến nghị để cải thiện tính bảo mật của mạng và thiết bị.

Công cụ: Các công cụ phổ biến được sử dụng để thử nghiệm thâm nhập mạng không dây bao gồm Aircrack-ng, Wireshark, Metasploit và Kali Linux.

Tầm quan trọng: Mạng không dây ngày càng phổ biến và dễ bị tấn công, điều quan trọng là các tổ chức phải kiểm tra và cải thiện các biện pháp bảo mật của họ để ngăn chặn vi phạm dữ liệu và các sự cố bảo mật khác.

## Kiểm thử thâm nhập mạng cục bộ không dây ( WLAN)

Định nghĩa: Quá trình kiểm thử tính bảo mật của mạng cục bộ không dây (WLAN) bằng cách mô phỏng các cuộc tấn công và xác định các lỗ hổng trong mạng và các thiết bị của mạng.

Mục tiêu: Để xác định các điểm yếu tiềm ẩn và lỗ hổng bảo mật trong mạng WLAN và đưa ra các khuyến nghị để cải thiện tính bảo mật của mạng.

Phạm vi: Bao gồm kiểm tra tính bảo mật của mạng WLAN, có thể bao gồm các điểm truy cập, bộ định tuyến không dây, máy khách không dây và chính giao thức truyền thông không dây.

Các bước chính:

* + Do thám: Thu thập thông tin về mạng WLAN, bao gồm SSID, địa chỉ MAC và cường độ tín hiệu.
  + Liệt kê: Xác định loại bảo mật không dây được sử dụng (WEP, WPA, WPA2, v.v.), khóa mã hóa và bất kỳ biện pháp bảo mật nào khác được áp dụng.
  + Khai thác: Cố gắng khai thác bất kỳ lỗ hổng nào được tìm thấy trong mạng WLAN, chẳng hạn như mật khẩu yếu, điểm truy cập được định cấu hình sai hoặc phần mềm chưa được vá.
  + Báo cáo: Ghi lại các phát hiện và đưa ra các đề xuất để cải thiện tính bảo mật của mạng WLAN và các thiết bị của nó.

Công cụ: Các công cụ phổ biến được sử dụng để kiểm tra thâm nhập mạng WLAN bao gồm Aircrack-ng, Wireshark, Metasploit và Kali Linux.

Tầm quan trọng: Mạng WLAN ngày càng phổ biến trong cả môi trường gia đình và doanh nghiệp và dễ bị tấn công, điều quan trọng là các tổ chức phải kiểm tra và cải thiện các biện pháp bảo mật của họ để ngăn chặn vi phạm dữ liệu và các sự cố bảo mật khác. Thử nghiệm thâm nhập mạng WLAN có thể giúp xác định các lỗ hổng bảo mật tiềm ẩn trong mạng và đưa ra các đề xuất để cải thiện tính bảo mật của mạng WLAN và các thiết bị của nó.

## Khám phá mạng không dây

Khám phá các mạng không dây là một bước quan trọng trong thử nghiệm xâm nhập không dây, vì nó giúp xác định các mục tiêu tấn công tiềm năng. Có một số công cụ và kỹ thuật có thể được sử dụng để khám phá các mạng không dây, bao gồm:

* Quét các điểm truy cập Wi-Fi: Các điểm truy cập Wi-Fi thường được định cấu hình để phát SSID (Mã định danh bộ dịch vụ) của chúng và có thể dễ dàng phát hiện bằng cách sử dụng các trình quét Wi-Fi, chẳng hạn như inSSIDer hoặc NetStumbler. Những công cụ này cho phép người kiểm tra thâm nhập xác định sự hiện diện, vị trí và độ mạnh của các điểm truy cập Wi-Fi.
* Sử dụng bộ dò tìm không dây: Có thể sử dụng bộ dò tìm không dây, chẳng hạn như Wireshark, để nắm bắt lưu lượng truy cập không dây và phân tích lưu lượng truy cập không dây đó để lấy thông tin về mạng không dây, bao gồm SSID, loại mã hóa và bất kỳ điểm truy cập mở hoặc dễ bị tấn công nào.
* Sử dụng máy phân tích phổ không dây: Máy phân tích phổ không dây, chẳng hạn như AirMagnet hoặc Wi-Spy, có thể được sử dụng để phân tích phổ tần số được sử dụng bởi các mạng không dây, cung cấp thông tin về loại và cường độ của tín hiệu không dây trong một khu vực nhất định.

Khám phá các mạng không dây là một bước quan trọng trong thử nghiệm thâm nhập không dây vì nó cung cấp thông tin cần thiết để xác định các mục tiêu tấn công tiềm năng. Bằng cách xác định các mạng không dây trong một khu vực nhất định, người kiểm tra thâm nhập có thể đánh giá tính bảo mật của các mạng và thiết bị này và đưa ra các khuyến nghị để cải thiện các biện pháp bảo mật của họ.

## Kiểm tra bảo mật vật lý của các điểm truy cập ( AP)

Bảo mật vật lý là một khía cạnh quan trọng của thử nghiệm thâm nhập mạng không dây, vì kẻ tấn công có thể cố gắng giành quyền truy cập vào mạng của tổ chức bằng cách giả mạo vật lý hoặc đánh cắp Điểm truy cập (AP). Dưới đây là một số bước có thể thực hiện để kiểm tra tính bảo mật vật lý của các AP:

* Xác minh vị trí AP: Xác minh rằng các AP được đặt ở những vị trí an toàn, chẳng hạn như tủ khóa hoặc phòng máy chủ, để ngăn truy cập trái phép.
* Kiểm tra các kết nối cáp: Kiểm tra các kết nối cáp của AP để đảm bảo rằng chúng được buộc chặt an toàn và người dùng trái phép không thể truy cập được.
* Kiểm tra các dấu hiệu giả mạo: Kiểm tra các dấu hiệu giả mạo hoặc hư hỏng vật lý đối với AP, chẳng hạn như con dấu bị hỏng, vít hoặc tấm che, điều này có thể cho thấy rằng ai đó đã cố gắng truy cập trái phép vào AP.
* Xác minh địa chỉ MAC: Xác minh rằng địa chỉ MAC của các AP khớp với địa chỉ MAC của các thiết bị được ủy quyền trên mạng, để đảm bảo rằng các AP giả mạo không được thêm vào mạng.
* Xác minh phiên bản chương trình cơ sở: Kiểm tra phiên bản chương trình cơ sở của các AP để đảm bảo rằng chúng được cập nhật và không có các lỗ hổng đã biết có thể bị kẻ tấn công khai thác.
* Tiến hành thử nghiệm thâm nhập vật lý: Tiến hành thử nghiệm thâm nhập vật lý để mô phỏng một cuộc tấn công vào bảo mật vật lý của các AP, để xác định bất kỳ điểm yếu hoặc lỗ hổng nào có thể bị kẻ tấn công khai thác.

Kiểm tra bảo mật vật lý của các AP là một bước quan trọng trong thử nghiệm xâm nhập không dây, vì nó giúp đảm bảo rằng mạng được bảo vệ khỏi các cuộc tấn công vật lý. Bằng cách thực hiện các bước để xác minh tính bảo mật vật lý của các AP, các tổ chức có thể giúp ngăn chặn truy cập trái phép vào mạng và bảo vệ khỏi các vi phạm bảo mật tiềm ẩn.

### Phát hiện kết nối không dây

Phát hiện các kết nối không dây là một khía cạnh quan trọng của thử nghiệm xâm nhập không dây, vì nó giúp xác định các mục tiêu tấn công tiềm năng. Có một số công cụ và kỹ thuật có thể được sử dụng để phát hiện các kết nối không dây, bao gồm:

* Máy quét không dây: Máy quét không dây, chẳng hạn như inSSIDer hoặc NetStumbler, có thể được sử dụng để phát hiện mạng không dây và cung cấp thông tin về tên mạng (SSID), loại mã hóa, cường độ tín hiệu và các chi tiết khác.
* Trình nghe lén gói không dây: Trình nghe lén gói không dây, chẳng hạn như Wireshark, có thể được sử dụng để nắm bắt và phân tích lưu lượng không dây, cung cấp thông tin về mạng không dây, các thiết bị được kết nối với mạng và lưu lượng truy cập qua mạng.
* Hệ thống phát hiện xâm nhập không dây (WIDS): Các hệ thống WIDS, chẳng hạn như Cisco Meraki hoặc Aruba Networks, được thiết kế để phát hiện và cảnh báo quản trị viên về truy cập không dây trái phép vào mạng.
* Bộ điều khiển điểm truy cập không dây: Bộ điều khiển điểm truy cập không dây, chẳng hạn như Aruba ClearPass hoặc Cisco Identity Services Engine (ISE), có thể được sử dụng để giám sát và kiểm soát quyền truy cập vào mạng bằng cách xác định các thiết bị trái phép và chặn quyền truy cập.

Bằng cách sử dụng các công cụ và kỹ thuật này để phát hiện các kết nối không dây, những người kiểm tra thâm nhập có thể hiểu rõ hơn về các mạng không dây trong môi trường mục tiêu và xác định các mục tiêu tấn công tiềm năng. Bằng cách xác định các mạng không dây trong một khu vực nhất định, người kiểm tra thâm nhập có thể đánh giá tính bảo mật của các mạng và thiết bị này và đưa ra các khuyến nghị để cải thiện các biện pháp bảo mật của họ.

Điều quan trọng cần lưu ý là việc phát hiện các kết nối không dây phải được thực hiện theo cách được kiểm soát và cho phép, đồng thời tuân thủ mọi cân nhắc về pháp lý và đạo đức. Người kiểm tra thâm nhập phải có được sự cho phép và đồng ý thích hợp trước khi tiến hành bất kỳ hoạt động kiểm tra thâm nhập không dây nào và phải tuân theo tất cả các luật, quy định và nguyên tắc đạo đức hiện hành.

## Nghe lén lưu lượng giữa AP và các thiết bị được liên kết

Nghe lén lưu lượng mạng là một bước quan trọng trong thử nghiệm xâm nhập không dây, vì nó cho phép người kiểm tra thâm nhập nắm bắt và phân tích lưu lượng mạng giữa các điểm truy cập không dây (AP) và các thiết bị được liên kết. Dưới đây là một số bước có thể được thực hiện để đánh hơi lưu lượng giữa AP và các thiết bị được liên kết:

* Chọn công cụ thích hợp: Chọn một công cụ để theo dõi lưu lượng truy cập tương thích với giao thức không dây đang được sử dụng bởi AP và các thiết bị được liên kết, chẳng hạn như Wireshark hoặc Aircrack-ng.
* Thiết lập bộ dò tìm: Định cấu hình bộ dò tìm để nắm bắt lưu lượng trên mạng không dây, chọn kênh và băng tần thích hợp.
* Nắm bắt lưu lượng: Nắm bắt lưu lượng giữa AP và các thiết bị được liên kết để phân tích lưu lượng mạng để tìm các dấu hiệu của lỗ hổng hoặc điểm yếu.
* Phân tích lưu lượng bị bắt: Phân tích lưu lượng bị bắt để xác định các lỗ hổng tiềm ẩn, chẳng hạn như mã hóa yếu, lưu lượng không được mã hóa hoặc thiết bị mạng được định cấu hình không đúng.
* Sử dụng lưu lượng truy cập bị bắt cho các cuộc tấn công tiếp theo: Sử dụng lưu lượng truy cập bị bắt để khởi chạy các cuộc tấn công tiếp theo, chẳng hạn như tấn công phát lại, liên quan đến việc phát lại lưu lượng truy cập bị bắt để giành quyền truy cập trái phép vào mạng.

Nghe lén lưu lượng giữa AP và các thiết bị được liên kết là một bước quan trọng trong thử nghiệm thâm nhập mạng không dây, vì nó cho phép người thử nghiệm thâm nhập xác định các lỗ hổng và điểm yếu tiềm ẩn trong mạng. Bằng cách nắm bắt và phân tích lưu lượng mạng, người kiểm tra thâm nhập có thể xác định các lỗ hổng và đề xuất các biện pháp bảo mật để ngăn chặn vi phạm bảo mật và các sự cố bảo mật khác.

## Tạo một điểm truy cập giả mạo

Điểm truy cập giả mạo là điểm truy cập không dây trái phép được kết nối với mạng mà quản trị viên mạng không biết hoặc không cho phép. Tạo điểm truy cập giả mạo là một kỹ thuật phổ biến được sử dụng trong thử nghiệm xâm nhập không dây để kiểm tra tính bảo mật của mạng không dây. Dưới đây là một số bước có thể được thực hiện để tạo một điểm truy cập giả mạo:

* Lấy điểm truy cập không dây: Lấy điểm truy cập không dây không thuộc mạng đang được kiểm tra. Đây có thể là một thiết bị độc lập hoặc thiết bị đã được định cấu hình để hoạt động ở chế độ giả mạo.
* Định cấu hình điểm truy cập: Định cấu hình điểm truy cập bằng SSID tương tự với SSID của mạng hợp pháp đang được thử nghiệm. Điều này có thể giúp đánh lừa các máy khách không dây kết nối với điểm truy cập lừa đảo.
* Kết nối với mạng: Kết nối điểm truy cập giả mạo với mạng đang được kiểm tra, bằng cách cắm điểm truy cập đó vào cổng có dây hoặc kết nối không dây.
* Giám sát lưu lượng mạng: Giám sát lưu lượng mạng để xác định bất kỳ thiết bị nào kết nối với điểm truy cập giả mạo. Điều này có thể giúp xác định các mục tiêu tiềm năng để tấn công.

Tạo một điểm truy cập giả mạo có thể là một kỹ thuật hữu ích trong thử nghiệm thâm nhập mạng không dây, vì nó có thể giúp xác định các lỗ hổng bảo mật tiềm ẩn trong mạng.

## Honeypot không dây

Honeypot không dây là một cơ chế bảo mật được sử dụng để thu hút và phát hiện các nỗ lực xâm phạm mạng không dây. Nó bắt chước một điểm truy cập không dây hợp pháp, nhưng thay vì cung cấp quyền truy cập vào mạng thực, nó cung cấp một mạng giả được sử dụng để thu thập thông tin về những kẻ tấn công hoặc lỗ hổng.

Dưới đây là các bước chung để sử dụng một honeypot không dây để khám phá các máy khách không dây dễ bị tấn công:

1. Thiết lập honeypot không dây: Để tạo honeypot không dây, bạn cần một thiết bị có thể bắt chước điểm truy cập không dây. Bạn có thể sử dụng phần mềm chuyên dụng như Kismet, Wireshark hoặc OpenWRT để thiết lập một điểm truy cập không dây giả có thể nắm bắt và phân tích lưu lượng. Bạn cũng sẽ cần tạo một tên mạng giả (SSID) và mật khẩu.
2. Thu hút khách hàng đến với honeypot: Sau khi thiết lập xong honeypot, bạn cần thu hút các khách hàng không dây dễ bị tổn thương kết nối với nó. Một cách để thực hiện điều này là làm cho tên mạng (SSID) và mật khẩu giả trông hợp pháp, chẳng hạn như sử dụng các tên mạng phổ biến như "Starbucks" hoặc "Wi-Fi miễn phí". Bạn cũng có thể thử phát SSID để xem có thiết bị nào tự động kết nối với nó không.
3. Nắm bắt lưu lượng và phân tích nó: Khi một máy khách dễ bị tổn thương kết nối với honeypot, thì honeypot sẽ nắm bắt lưu lượng và phân tích nó. Bạn có thể sử dụng các công cụ như Wireshark để phân tích lưu lượng truy cập và tìm kiếm bất kỳ dấu hiệu dễ bị tổn thương hoặc tấn công nào. Ví dụ: bạn có thể thấy lưu lượng truy cập không được mã hóa, mật khẩu yếu hoặc dấu hiệu của một cuộc tấn công vũ phu.
4. Bảo mật mạng: Khi bạn đã xác định được các máy khách dễ bị tấn công, bạn có thể sử dụng thông tin này để bảo mật mạng. Điều này có thể liên quan đến việc vá các lỗ hổng, thay đổi mật khẩu hoặc triển khai mã hóa mạnh hơn.
5. Giám sát mạng: Để tiếp tục bảo vệ mạng, bạn nên giám sát mạng thường xuyên và đảm bảo rằng không có lỗ hổng hoặc cuộc tấn công mới nào được phát hiện. Bạn có thể sử dụng honeypot không dây để tiếp tục thu hút những kẻ tấn công tiềm năng và xác định các lỗ hổng mới.

## Thực hiện tấn công từ chối dịch vụ DoS

Thực hiện tấn công từ chối dịch vụ (DoS), cụ thể là tấn công hủy xác thực, liên quan đến việc gửi các gói hủy xác thực giả mạo đến một điểm truy cập không dây hoặc thiết bị khách. Kiểu tấn công này có thể ngăn người dùng hợp pháp truy cập mạng không dây hoặc có thể khiến thiết bị ngắt kết nối khỏi mạng và cố gắng kết nối lại nhiều lần, do đó gây ra tình trạng từ chối dịch vụ.

Dưới đây là các bước chung liên quan đến việc thực hiện một cuộc tấn công hủy xác thực:

1. Lấy bộ điều hợp không dây: Để thực hiện tấn công hủy xác thực, bạn sẽ cần một bộ điều hợp không dây có khả năng chèn gói. Điều này cho phép bạn gửi các gói hủy xác thực giả mạo đến thiết bị hoặc mạng đích.
2. Chọn mục tiêu: Mục tiêu có thể là một thiết bị cụ thể được kết nối với mạng không dây hoặc toàn bộ mạng. Bạn có thể sử dụng các công cụ như Kismet, Airodump-ng hoặc Wireshark để xác định mạng không dây và các thiết bị được kết nối với mạng đó.
3. Sử dụng công cụ hủy xác thực: Hiện có nhiều công cụ hủy xác thực khác nhau, chẳng hạn như Aireplay-ng hoặc MDK3, có thể tự động hóa quá trình gửi các gói hủy xác thực. Các công cụ này sẽ gửi các gói hủy xác thực đến thiết bị hoặc mạng đích, khiến thiết bị hoặc mạng đó bị ngắt kết nối khỏi mạng không dây.
4. Theo dõi cuộc tấn công: Trong cuộc tấn công, bạn có thể sử dụng các công cụ như Wireshark hoặc tcpdump để theo dõi lưu lượng và xác nhận rằng các gói hủy xác thực đang được gửi và nhận.
5. Dừng cuộc tấn công: Để dừng cuộc tấn công, bạn chỉ cần ngừng gửi các gói xác thực.

Điều quan trọng cần lưu ý là thực hiện tấn công hủy xác thực mà không được phép là bất hợp pháp và có thể dẫn đến hậu quả nghiêm trọng. Kiểu tấn công này có thể làm gián đoạn người dùng hợp pháp truy cập mạng không dây và có thể gây hư hỏng cho thiết bị hoặc mạng. Ngoài ra, điều quan trọng là phải thận trọng khi thử nghiệm hoặc thực hành các kiểu tấn công này vì chúng có thể vô tình gây hại.

## Tạo lưu lượng truy cập nhanh

"Tạo lưu lượng truy cập nhanh" là một kỹ thuật được sử dụng trong thử nghiệm xâm nhập không dây để đánh giá hiệu suất và tính bảo mật của mạng không dây. Kỹ thuật này liên quan đến việc tạo ra một lưu lượng truy cập lớn trong một khoảng thời gian ngắn để kiểm tra khả năng xử lý và phản hồi lưu lượng của mạng.

Trong quá trình thử nghiệm thâm nhập không dây, việc tạo lưu lượng truy cập nhanh có thể được sử dụng để kiểm tra hiệu suất tổng thể của mạng không dây, xác định các tắc nghẽn hiệu suất tiềm ẩn và kiểm tra cách mạng phản ứng với các loại lưu lượng khác nhau. Kỹ thuật này cũng có thể được sử dụng để xác định các lỗ hổng bảo mật, chẳng hạn như các cuộc tấn công từ chối dịch vụ (DoS), bằng cách làm mạng quá tải lưu lượng và quan sát cách mạng phản hồi.

Tuy nhiên, điều quan trọng cần lưu ý là việc tạo lưu lượng truy cập nhanh có thể làm gián đoạn hoạt động bình thường của mạng không dây và do đó chỉ nên được thực hiện bởi các chuyên gia bảo mật có trình độ trong môi trường được kiểm soát. Việc sử dụng trái phép các kỹ thuật tạo lưu lượng truy cập nhanh có thể gây gián đoạn dịch vụ, vi phạm chính sách mạng và thậm chí dẫn đến hậu quả pháp lý.

## Giải mã gói tin

Giải mã gói tin là một kỹ thuật được sử dụng trong thử nghiệm thâm nhập không dây để bẻ khóa lưu lượng mạng không dây được mã hóa. Trong các mạng không dây, dữ liệu thường được truyền qua mạng ở dạng mã hóa để ngăn chặn việc nghe lén và truy cập trái phép. Để giải mã dữ liệu này, kẻ tấn công cần nắm bắt các gói được mã hóa, sau đó sử dụng các công cụ và kỹ thuật để phá vỡ mã hóa.

Giải mã gói đơn là phương pháp liên quan đến việc nắm bắt một gói lưu lượng truy cập mạng và sau đó cố gắng bẻ khóa mã hóa của nó. Kỹ thuật này rất hữu ích trong các tình huống mà kẻ tấn công có thời gian hoặc tài nguyên hạn chế, vì nó không yêu cầu bắt một số lượng lớn các gói hoặc một phiên hoàn chỉnh.

Có một số công cụ và kỹ thuật có sẵn để thực hiện giải mã gói đơn, bao gồm các công cụ như Aircrack-ng, Wireshark và Cain and Abel. Các công cụ này sử dụng nhiều phương pháp khác nhau để bẻ khóa mã hóa, bao gồm tấn công từ điển, tấn công vũ phu và tấn công bảng cầu vồng. Mỗi phương pháp đều có điểm mạnh và điểm yếu riêng và có thể ít nhiều hiệu quả tùy thuộc vào loại mã hóa được sử dụng.

Cần lưu ý rằng việc cố gắng giải mã một gói không phải lúc nào cũng hợp pháp và nó chỉ nên được thực hiện trong môi trường được kiểm soát với sự cho phép hợp pháp thích hợp. Thử nghiệm thâm nhập và hack đạo đức chỉ nên được thực hiện với sự cho phép rõ ràng của tổ chức mục tiêu và dưới sự hướng dẫn của một chuyên gia có kinh nghiệm.

## Đầu độc ARP

Đầu độc ARP (còn được gọi là giả mạo ARP) là một kỹ thuật được sử dụng để chặn lưu lượng mạng. Trong cuộc tấn công này, kẻ tấn công gửi thông báo Giao thức phân giải địa chỉ (ARP) giả mạo tới mạng, liên kết địa chỉ MAC của kẻ tấn công với địa chỉ IP của thiết bị hợp pháp trên mạng. Do đó, tất cả lưu lượng truy cập mạng dành cho thiết bị hợp pháp thay vào đó được gửi đến kẻ tấn công.

Thực hiện một cuộc tấn công đầu độc ARP thường bao gồm các bước sau:

1. Xác định thiết bị đích: Xác định địa chỉ IP của thiết bị mà bạn muốn chặn lưu lượng truy cập.
2. Bật chuyển tiếp IP: Trên máy tấn công của bạn, hãy bật chuyển tiếp IP để nó có thể hoạt động như một bộ định tuyến và chuyển tiếp lưu lượng truy cập từ thiết bị đích đến đích dự kiến. Trong Linux, bạn có thể sử dụng lệnh sau để bật chuyển tiếp IP:
3. tiếng vang 1 > /proc/sys/net/ipv4/ip\_forward
4. Thực hiện giả mạo ARP: Sử dụng công cụ giả mạo ARP như Ettercap hoặc arpspoof để gửi thông báo ARP giả mạo đến mạng. Những thông báo này sẽ liên kết địa chỉ MAC của bạn với địa chỉ IP của thiết bị đích. Ví dụ: để thực hiện đầu độc ARP bằng Ettercap, bạn có thể sử dụng lệnh sau:
5. ettercap -T -M arp:remote /targetIP// /gatewayIP//
6. Trong lệnh này, **/targetIP/** là địa chỉ IP của thiết bị đích và **/gatewayIP/** là địa chỉ IP của cổng mặc định của mạng.
7. Chặn lưu lượng: Sau khi bạn đã đầu độc thành công bộ đệm ARP của thiết bị đích, bạn có thể chặn lưu lượng của nó bằng cách sử dụng trình thám thính mạng như Wireshark. Trình thám thính sẽ nắm bắt tất cả lưu lượng mạng dành cho thiết bị đích, có thể bao gồm thông tin xác thực đăng nhập, dữ liệu nhạy cảm hoặc thông tin có giá trị khác.

Điều quan trọng cần lưu ý là việc thực hiện một cuộc tấn công đầu độc ARP mà không được phép là bất hợp pháp và phi đạo đức. Nó chỉ nên được thực hiện trong một môi trường được kiểm soát với sự cho phép của chủ sở hữu mạng như một phần của đánh giá bảo mật hoặc thử nghiệm thâm nhập.

## Tiêm một gói được mã hóa

Tiêm một gói được mã hóa yêu cầu kiến thức về thuật toán mã hóa và khóa được sử dụng để mã hóa gói. Không có thông tin này, không thể tiêm một gói được mã hóa hợp lệ.

Giả sử bạn có khóa và thuật toán mã hóa, bạn có thể thực hiện các bước sau để cố gắng đưa vào một gói tin được mã hóa:

1. Chụp gói mã hóa hợp lệ: Sử dụng trình nghe trộm mạng như Wireshark để chụp gói mã hóa hợp lệ được gửi giữa hai thiết bị trên mạng.
2. Giải mã gói bị bắt: Sử dụng khóa mã hóa và thuật toán để giải mã gói bị bắt. Điều này sẽ cho phép bạn xem nội dung của gói tin.
3. Sửa đổi gói đã giải mã: Sau khi gói được giải mã, hãy sửa đổi nội dung của gói để bao gồm tải trọng hoặc dữ liệu mong muốn.
4. Mã hóa gói tin đã sửa đổi: Sử dụng khóa mã hóa và thuật toán để mã hóa gói tin đã sửa đổi.
5. Tiêm gói đã mã hóa: Sử dụng một công cụ như Scapy để đưa gói đã sửa đổi và mã hóa vào mạng.

## Lọc MAC

Lọc MAC là một tính năng bảo mật được sử dụng trong các mạng không dây để hạn chế truy cập mạng bằng cách cho phép hoặc từ chối các thiết bị dựa trên địa chỉ MAC của chúng. Để kiểm tra lọc MAC, hãy làm theo các bước sau:

1. Xác định địa chỉ MAC của thiết bị: Bạn có thể thực hiện việc này bằng cách sử dụng lệnh "ipconfig /all" trên Windows hoặc "ifconfig" trên Linux hoặc macOS.
2. Truy cập cài đặt bộ định tuyến không dây: Nhập địa chỉ IP của bộ định tuyến vào trình duyệt web của bạn và đăng nhập bằng thông tin xác thực quản trị viên của bộ định tuyến.
3. Điều hướng đến cài đặt lọc MAC: Tùy thuộc vào bộ định tuyến, cài đặt này có thể nằm trong phần Không dây, Bảo mật hoặc Kiểm soát truy cập.
4. Kiểm tra cài đặt lọc MAC: Tìm các tùy chọn như "Lọc MAC", "Bộ lọc MAC không dây" hoặc "Kiểm soát truy cập". Nếu tính năng lọc MAC được bật, bạn có thể thấy danh sách các địa chỉ MAC được phép hoặc bị từ chối.

Xác định xem thiết bị của bạn có được phép hay không: Nếu địa chỉ MAC của bạn không được liệt kê hoặc được liệt kê là bị từ chối, bạn có thể bị lọc MAC

## Giả mạo MAC

Giả mạo MAC là một kỹ thuật được sử dụng để thay đổi địa chỉ Điều khiển truy cập phương tiện (MAC) của giao diện mạng. Điều này có thể hữu ích trong một số tình huống chẳng hạn như bỏ qua bộ lọc MAC hoặc để tiến hành một cuộc tấn công trung gian (MitM). Dưới đây là các bước để giả mạo địa chỉ MAC của bạn:

1. Xác định giao diện mạng: Trước tiên, bạn cần xác định giao diện mạng có địa chỉ MAC mà bạn muốn giả mạo. Bạn có thể sử dụng lệnh **ifconfig** trên Linux hoặc **ipconfig /all** trên Windows để xác định giao diện mạng.
2. Tắt giao diện mạng: Tiếp theo, bạn cần tắt giao diện mạng để thay đổi địa chỉ MAC. Bạn có thể dùng lệnh **ifconfig <interface> down** trên Linux hoặc **netsh interface set interface "<interface>" admin=disable** trên Windows để tắt giao diện.
3. Thay đổi địa chỉ MAC: Sau khi tắt giao diện, bạn có thể thay đổi địa chỉ MAC. Bạn có thể sử dụng lệnh **macchanger -m <new\_mac\_address> <interface>** trên Linux hoặc **getmac /v /fo list** trên Windows để thay đổi địa chỉ MAC.

Bật giao diện mạng: Sau khi thay đổi địa chỉ MAC, bạn cần bật lại giao diện mạng. Bạn có thể dùng lệnh **ifconfig <interface> up** trên Linux hoặc **netsh interface set interface "<interface>" admin=enable** trên Windows để bật giao diện.

Để tạo kết nối trực tiếp đến điểm truy cập không dây, bạn có thể làm theo các bước sau:

1. Xác định SSID và loại bảo mật của điểm truy cập không dây mà bạn muốn kết nối.
2. Đảm bảo rằng bộ điều hợp mạng không dây của bạn được bật và hoạt động bình thường.
3. Quét các mạng không dây khả dụng và tìm điểm truy cập bạn muốn kết nối.
4. Nếu điểm truy cập đang sử dụng bảo mật, bạn sẽ cần cung cấp thông tin đăng nhập phù hợp để kết nối. Điều này có thể bao gồm khóa bảo mật mạng hoặc tên người dùng và mật khẩu cho chế độ Doanh nghiệp WPA/WPA2.
5. Khi bạn đã kết nối thành công với điểm truy cập không dây, bạn sẽ có thể truy cập internet và các tài nguyên mạng khác.

Cần lưu ý rằng một số điểm truy cập không dây có thể có các biện pháp bảo mật bổ sung, chẳng hạn như lọc MAC hoặc cách ly máy khách, điều này có thể ngăn bạn kết nối trực tiếp. Trong những trường hợp như vậy, bạn có thể cần sử dụng các kỹ thuật bổ sung như giả mạo địa chỉ MAC hoặc giả mạo ARP để có quyền truy cập.

# TÌM HIỂU CÁC CÔNG CỤ

## Aircrack-ng

### Khái niệm về công cụ Aircrack-ng

**Aircrack-ng** nổi tiếng là một trong những truy cập bảo mật mạng WiFi tốt nhất. Nó có thể tập trung vào nhiều vùng bảo mật WiFi. Chẳng hạn như giám sát, kiểm tra và tấn công mạng WiFi. Aircrack-ng rất phong phú với các thành phần khác nhau và nó sở hữu 20 tiện ích riêng lẻ để tổng hợp lại. Mỗi thành phần này đều cần thiết và có vai trò trong việc thực hiện công việc của chúng ta một cách hiệu quả.

### Những đặc điểm chính

Aircrack-ng cũng nổi tiếng là một công cụ linh hoạt mà chúng tôi sử dụng để sửa đổi và quan sát chi tiết mạng WiFi của mình. Nó bao gồm những điều dưới đây

* Giám sát mạng WiFi
* Tấn công điểm truy cập sai
* Sửa đổi và kiểm tra trình điều khiển Internet
* Bẻ khóa nhiều loại mã hoá
* Dòng lệnh
* Tính khả dụng của các thành phần

### Đánh giá Aircrack-ng

**Giao diện**

Giao diện của Aircrack-ng không sử dụng các yếu tố đồ họa. Nó chỉ bao gồm giao diện màu đen và phông chữ kiểu mã hóa. Tuy nhiên, giao diện của phần mềm này giúp ích rất nhiều trong việc đưa ra một quy trình hiệu quả nhất cho những người dùng cần một công cụ hữu hiệu cho mạng WiFi của họ. Thiết kế phẳng và đơn giản của giao diện mang lại quá trình mượt mà nhất cho tất cả chúng ta.

**Giám sát mạng WiFi**

Tính năng này là một gói tin giúp ích rất nhiều trong việc người dùng nắm bắt và xuất dữ liệu thành các tệp văn bản. Nó sẽ giúp người dùng xử lý nhiều hơn bởi phần mềm của bên thứ ba.

**Tấn công quyền truy cập giả mạo**

Nhiều người dùng gặp sự cố với các cuộc tấn công phát lại, điểm truy cập giả mạo, không có xác thực và các vấn đề khác liên quan đến việc đưa gói vào mạng WiFi của họ. Đó là lý do tại sao, Aircrack-ng đã trở thành một trợ giúp đắc lực với rất nhiều người dùng theo thời gian, bởi vì nó có một tính năng giúp bạn giảm bớt tất cả các cuộc tấn công và các điểm sai trên Mạng của mình.

**Kiểm tra trình điều khiển mạng**

Một tính năng hữu ích khác của Aircrack-ng là khả năng kiểm tra trình điều khiển Mạng của bạn. Chúng ta phải nhớ rằng việc thử các thành phần, trình điều khiển và các thẻ khác nhau của mạng WiFi là điều cần thiết. Hành động này sẽ duy trì hiệu suất tuyệt vời của kết nối internet của bạn. May mắn thay, Aircrack-ng sẽ giúp bạn thực hiện điều đó.

**Bẻ khóa mạng WiFi**

Một lý do khác mà chúng ta có thể xem xét tại sao Aircrack-ng là một trong những phần mềm tốt nhất là vì nó bẻ khóa các mạng WiFi không dây khác nhau. Nó bao gồm nhiều mạng khác nhau, chẳng hạn như WEP, WPA PSK, WPA 1 và WPA 2. Dù bạn có Mạng nào, bạn đều có thể sử dụng công cụ này để bẻ khóa nó.

## Crunch Kali Linux

### Khái niệm về công cụ Crunch

Crunch là một wordlist generator, nơi chúng ta có thể chỉ định một bộ ký tự tiêu chuẩn hoặc một bộ ký tự mà chúng tôi chỉ định. Crunch có thể tạo ra tất cả các tổ hợp và hoán vị khả thi dựa trên các tiêu chí đã cho. Dữ liệu được tạo bởi crunch có thể được hiển thị trên màn hình, được lưu vào một tệp hoặc được chuyển đến một chương trình khác

Nó là công cụ rất quan trọng để tạo ra một wordlist generator có thể có của bất kỳ mật khẩu nào. Trong Kali Linux, công cụ bẻ khóa được cung cấp miễn phí. Chương trình này hỗ trợ số và ký hiệu, ký tự chữ hoa và chữ thường Unicode riêng biệt.

### Các tính năng của Crunch

Sau đây là các tính năng của Crunch:

* Crunch tạo wordlist generator theo cả hai cách kết hợp và hoán vị.
* Crunch có thể chia đầu ra theo một số dòng hoặc kích thước tệp.
* Crunch hiện đã có hỗ trợ tiếp tục.
* Giờ đây, mẫu hỗ trợ số và biểu tượng
* Hiện tại, mẫu hỗ trợ các ký tự chữ hoa và chữ thường riêng biệt
* Thêm báo cáo trạng thái khi tạo nhiều tệp.
* Tùy chọn -d mới để hạn chế các ký tự trùng lặp; xem tập tin người đàn ông để biết chi tiết.

Bây giờ đã có hỗ trợ Unicode.

### Tầm quan trọng của Crunch

Một tệp từ điển được yêu cầu trong quá trình tấn công mật khẩu; Tệp từ điển là tệp văn bản chứa nhiều mật khẩu thường được sử dụng. Những mật khẩu này thường được sử dụng với các công cụ bẻ khóa mật khẩu. Tuy nhiên, đôi khi người dùng rất thông minh. Họ sử dụng mật khẩu thông minh như javatpoint @ 123 và số điện thoại di động. Tệp từ điển không bao gồm các loại mật khẩu này. Bây giờ chúng ta cần một công cụ bẻ khóa, mà tin tặc thường sử dụng để tạo mật khẩu.

**crunch <min> <max> [options]**

Crunch có thể tạo ra một wordlist generator tùy thuộc vào các thông số của chúng tôi. Đầu ra của Crunch có thể được truyền tới màn hình, một tệp hoặc một chương trình khác.

Các thông số sau là bắt buộc:

1. **min-len**

Min-len là chuỗi độ dài tối thiểu mà chúng ta muốn crunch bắt đầu. Tùy chọn này là cần thiết ngay cả đối với các tham số sẽ không sử dụng giá trị.

1. **max-len**

Nó là chuỗi độ dài tối đa mà chúng ta cần crunch để kết thúc. Mặc dù giá trị sẽ không được sử dụng, tùy chọn này là cần thiết.

1. **charset string**

Chúng ta có thể chỉ định các bộ ký tự cho crunch để sử dụng trên dòng lệnh và nếu chúng tôi để trống, crunch sẽ sử dụng các bộ ký tự mặc định. Thứ tự phải là ký tự viết thường, ký tự viết hoa, số và sau đó là ký hiệu. Nếu chúng ta không tuân theo thứ tự này thì chúng ta sẽ không nhận được đầu ra mong muốn. Chúng ta phải chỉ định các giá trị cho kiểu ký tự hoặc một dấu cộng.

Lưu ý: Nếu chúng ta cần bao gồm ký tự khoảng trắng trong bộ ký tự của mình, chúng tôi phải thoát khỏi nó bằng cách sử dụng ký tự \ hoặc đặt bộ ký tự của chúng tôi trong dấu ngoặc kép có nghĩa là “abc”.

## Wireshark

### Khái niệm Wireshark

Wireshark là phần mềm phân tích gói mạng (tiếng Anh gọi là network packet analyzer). Nhiệm vụ của nó là nắm bắt tất cả các network packets rồi hiển thị dữ liệu của gói đó một cách chi tiết nhất

### Các chức năng của Wireshark

Sử dụng Wireshark nhằm các mục đích sau:

* Network administrators sử dụng Wireshark để khắc phục sự cố mạng.
* Các kỹ sư Network security sử dụng Wireshark để kiểm tra các vấn đề bảo mật.
* Các kỹ sư QA sử dụng Wireshark để xác minh các network applications.
* Các developers sử dụng Wireshark để gỡ lỗi triển khai giao thức.
* Mọi người sử dụng Wireshark để học internals giao thức mạng.
* Không chỉ các tình huống trên, Wireshark cũng có thể hữu ích trong nhiều tình huống khác nữa.

### Tính năng

* Có sẵn cho UNIX và Windows.
* Chụp dữ liệu gói trực tiếp từ giao diện mạng.
* Mở các tệp có chứa dữ liệu gói được bắt bằng tcpdump/ WinDump, Wireshark và một số chương trình packet capture khác.
* Nhập các gói từ các tệp văn bản có chứa các hex dumps của packet data.
* Hiển thị các gói với thông tin giao thức rất chi tiết.
* Lưu dữ liệu gói bị bắt.
* Xuất một số hoặc tất cả các gói trong một số định dạng capture file.
* Lọc các gói tin trên nhiều tiêu chí.
* Tìm kiếm các gói trên nhiều tiêu chí.
* Colorize gói hiển thị dựa trên bộ lọc.
* Tạo các số liệu thống kê khác nhau.

### Đánh giá Wireshark

**Trình phân tích giao thức mạng WiFi**

Wireshark sẽ cho phép chúng ta xem các lần xuất hiện trên mạng của mình. Khả năng của máy phân tích đi kèm với khả năng ở cấp độ hiển vi. Đây là một chức năng tuyệt vời sẽ giúp chúng ta truy cập thông tin trong mạng internet

**Thu thập tín hiệu và dữ liệu**

Nhiều người dùng đang sử dụng Wireshark để nắm bắt các mạng dữ liệu mà chúng ta có thể duyệt qua GUI hoặc thông qua tiện ích TShark ở chế độ TTY. Mặt khác, phần mềm này nắm bắt dữ liệu và tín hiệu và có thể đọc và đọc nhiều định dạng tệp. Mặt khác, điều này cũng có thể được nén bằng GZIP và giải nén nó trong quá trình này.

**Gói mạng Wireshark**

Cũng có thể phân tích các gói mạng bằng Wireshark. Điều tuyệt vời về nó là bạn có thể khám phá ngay cả với các tệp hiện có. Bên cạnh đó, thu thập dữ liệu gói từ một mạng trực tiếp và lưu trữ chúng trong một kho lưu trữ tập trung cũng có sẵn. Tính năng này có thể bắt các gói tin trong một khu vực.

## Nmap

### Khái niệm Nmap

**Nmap (Network mapper)** là một tiện ích mã nguồn mở và miễn phí dùng để khai thác thông tin mạng và kiểm tra bảo mật. Nhiều quản trị viên hệ thống và quản trị viên network đã chứng minh sự hữu dụng của Nmap trong các tác vụ như kiểm tra mạng, quản lý dịch vụ và theo dõi thời gian hoạt động của máy chủ và dịch vụ.

### Tính năng Nmap

**Khám phá máy chủ** – xác định máy chủ trên mạng. ví dụ, liệt kê các máy chủ phản hồi request TCP hoặc ICMP hoặc mở một port cụ thể.

**Version Detection** – kiểm tra các dịch vụ mạng và xác định tên ứng dụng cũng như phiên bản.

**Thực hiện tương tác với đối tượng**– sử dụng Nmap scripting Engine (NSE) và ngôn ngữ Lua để tương tác dịch vụ với đối tượng máy chủ.  
Nmap có thể cung cấp thêm thông tin trên đối tượng, bao gồm DNS phân giải ngược, loại thiết bị và địa chỉ MAC

### Các kỹ thuật quét Nmap

* TCP SYN (half open) scanning
* TCP FIN
* Xmas hay NULL (stealth) scanning
* TCP ftp proxy (bounce attack) scanning,
* SYN/FIN scanning thông qua IP  (bypass một số bộ loc)
* TCP ACK và Window scanning
* UDP raw ICMP port unreachable scanning
* ICMP scanning (ping-sweep),
* TCP Ping scanning
* Direct (non portmapper) RPC scanning
* Nhận diện hệ điều hành bằng TCP/IP Fingerprinting
* Reverse-ident scanning
* Vanilla TCP connect() scanning

### Ưu điểm Nmap

**Miễn phí:** Mục tiêu chính của dự án Nmap là giúp internet trở nên an toàn hơn và cung cấp cho quản trị viên (hoặc hacker) một công cụ để khai thác mạng. Nmap hoàn toàn miễn phí đi kèm mã nguồn đầy đủ, bạn có thể tải về.

**Tài liệu đầy đủ:**bạn có thể tìm được cả ebook, các bài hướng dẫn về Nmap dễ dàng.

**Hỗ trợ:**Nmap là tiện ích mã nguồn mở, vì vậy nó được cộng đồng các nhà phát triển và người dùng hỗ trợ rất tốt. Hầu hết các tương tác được gửi về mail Nmap.

**Sự công nhận:**Nmap nhận được nhiều giải thưởng bao gồm “sản phẩm bảo mật thông tin của năm” được trao bởi Linux Jonrnal, Info World và Codetalker Digest. Nó được giới thiệu trong hàng trăm bài báo, các bộ phim, sách và truyện tranh.

**Phổ biến:**Hàng ngàn người download Nmap mỗi ngày và được sử dụng trong nhiều hệ điều hành như Redhat Linux, Debian Linux, Gentoo, FreeBSD…Nó nằm trong top 10 chương trình hàng đầu (trong số 30000 chương trình) tại kho lưu trữ Freshmeat.net

## Ettercap

### Khái niệm Ettercap

Ettercap là một công cụ chuyên nghiệp có thể giúp bạn giả mạo các kết nối, giả mạo DNS,..Ettercap giúp bạn trung gian giữa các cuộc tấn công trong mạng LAN. Nó có tính năng đánh hơi các các kết nối trực tiếp, lọc nội dung chuyển trên mạng và nhiều thủ thuật thú vị khác. . sự tìm tòi, nghiên cứu và thử nghiệm một số công cụ phần mềm hỗ trợ

### Chức năng Ettercap

Ettercap hoạt động bằng cách đặt giao diện mạng ở chế độ hỗn tạp và bằng ARP đầu độc các máy mục tiêu. Qua đó, nó có thể hoạt động như một 'người đứng giữa' và thực hiện nhiều cuộc tấn công khác nhau vào các nạn nhân. Ettercap có hỗ trợ plugin để các tính năng có thể được mở rộng bằng cách thêm các plugin mới.

### Tính năng Ettercap

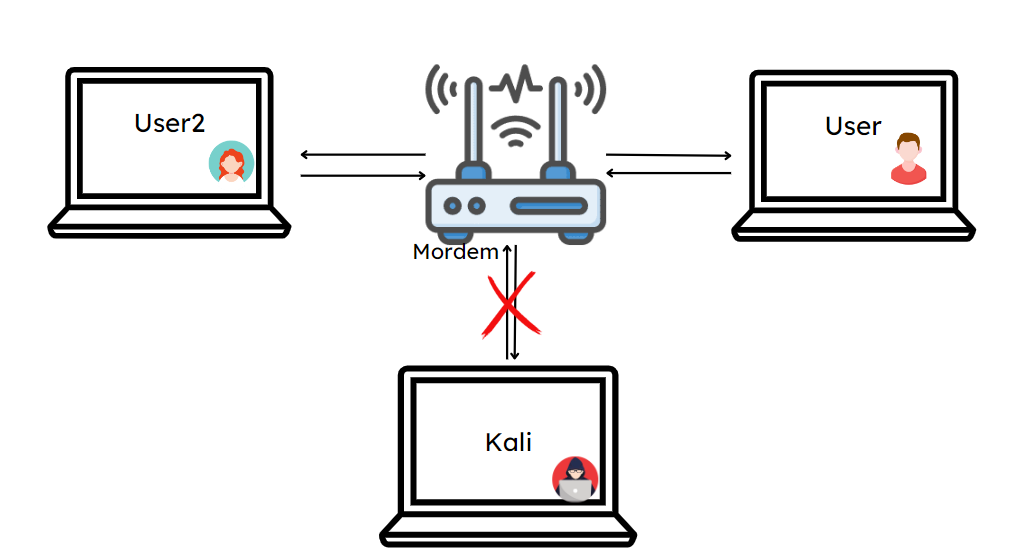
Ettercap hỗ trợ phân tích chủ động và thụ động nhiều giao thức (bao gồm cả giao thức được mã hóa) và cung cấp nhiều tính năng để phân tích mạng và máy chủ. Ettercap cung cấp bốn chế độ hoạt động:

* Dựa trên IP: các gói được lọc dựa trên nguồn và đích IP.
* Dựa trên MAC: các gói được lọc dựa trên địa chỉ MAC , hữu ích cho việc đánh hơi các kết nối thông qua một cổng.
* Dựa trên ARP : sử dụng đầu độc ARP để đánh hơi mạng LAN được chuyển đổi giữa hai máy chủ (song công hoàn toàn).
* Dựa trên PublicARP: sử dụng đầu độc ARP để đánh hơi mạng LAN đã chuyển đổi từ máy chủ nạn nhân sang tất cả các máy chủ khác (bán song công).
* Ngoài ra, phần mềm còn cung cấp các tính năng sau:
* Chèn ký tự vào một kết nối đã thiết lập: các ký tự có thể được đưa vào máy chủ (mô phỏng lệnh) hoặc máy khách (mô phỏng trả lời) trong khi duy trì kết nối trực tiếp.
* Hỗ trợ SSH1: đánh hơi tên người dùng và mật khẩu và thậm chí cả dữ liệu của kết nối SSH1. Ettercap là phần mềm đầu tiên có khả năng đánh hơi kết nối SSH ở chế độ song công hoàn toàn.
* Hỗ trợ HTTPS: đánh hơi dữ liệu được bảo mật HTTP SSL —ngay cả khi kết nối được thực hiện thông qua proxy .
* Lưu lượng truy cập từ xa qua đường hầm GRE : đánh hơi lưu lượng truy cập từ xa thông qua đường hầm GRE từ bộ định tuyến Cisco từ xa và thực hiện một cuộc tấn công trung gian vào nó.
* Hỗ trợ trình cắm: tạo các trình cắm tùy chỉnh bằng cách sử dụng API của Ettercap .
* Lọc/xóa gói: thiết lập bộ lọc tìm kiếm một chuỗi cụ thể (hoặc chuỗi thập lục phân) trong tải trọng TCP hoặc UDP và thay thế nó bằng một chuỗi/chuỗi tùy chỉnh do lựa chọn hoặc loại bỏ toàn bộ gói.
* Dấu vân tay ngăn xếp TCP/IP : xác định hệ điều hành của máy chủ nạn nhân và bộ điều hợp mạng của nó.
* Hủy kết nối: hủy kết nối được chọn từ danh sách kết nối.
* Chiếm đoạt các yêu cầu DNS .

# TRIỂN KHAI THỰC NGHIỆM

## Tấn công bẻ khoá mật khẩu WiFi

### Mô hình



Hình 3. Mô hình tấn công bẻ khoá mật khẩu

**Access point**:

* BSSID: 52:A1:95:F8:92:6B
* Channel: 2
* Encryption: WPA2
* ESSID: GTNeoHii

**Attacker**:

* OS: Kali Linux 2022.4

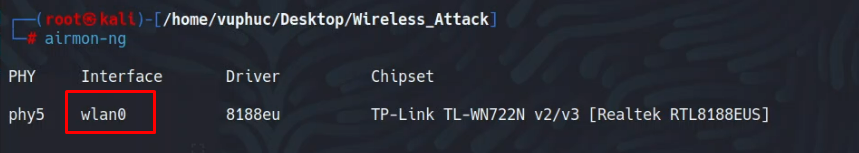
### Kịch bản

Máy attacker dò tìm Wifi và phát hiện sóng wifi của access point cần truy cập, attacker tiến hành tấn công bẻ khoá mật khẩu access point.

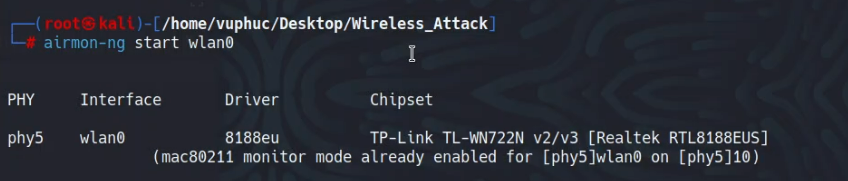
### Thực nghiệm

Tất cả các bước sau đều tiến hành dưới quyền superuser.

Trên máy Kali mở terminal và nhập lệnh: **arimon-ng** để kiểm tra adapter



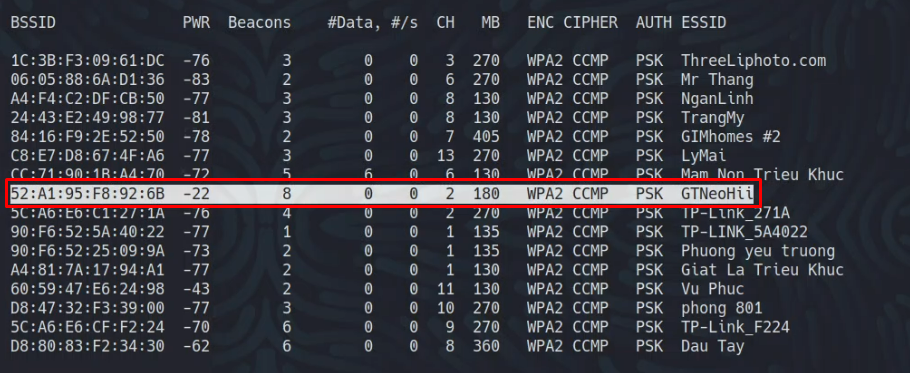
Tiến hành bật monitor mode bằng câu lệnh: **airmon-ng check kill** và **airmon-ng start wlan0.**



Tìm kiếm các thông tin access point bằng câu lệnh: **airodump-ng wlan0**



Kết quả trả về có dạng sau:

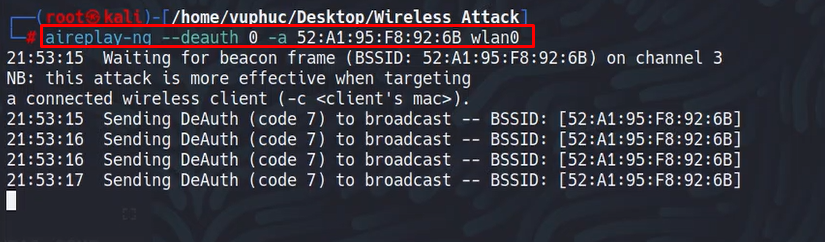


Tiến hành theo dõi AP bằng câu lệnh: **airodump-ng --bssid 52:A1:95:F8:92:6B -c 2 -w handshake.txt wlan0**

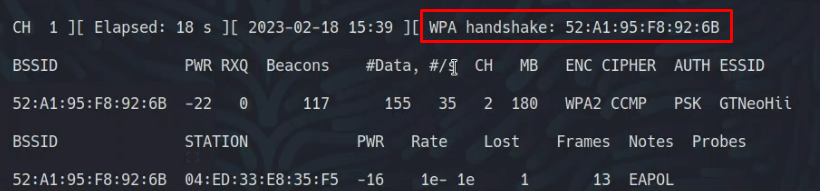
Câu lệnh trên: -c 2 là channel bằng 2, -w handshake.txt là ghi vào file handshake.txt



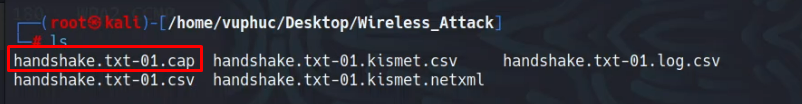
Mở terminal mới và chạy với câu lệnh sau để client kết nối với AP: **aireplay-ng --deauth 0 -a 52:A1:95:F8:92:6B wlan0** (--deauth 0 là số khung bỏ xác thực, bằng 0 là liên tục**)**



Vậy là thành công, quay lại terminal theo dõi khi nào hiện dòng WPA handshake: 52:A1:95:F8:92:6B là đã thành công, nhấn ctrl+c để dừng chặn AP.



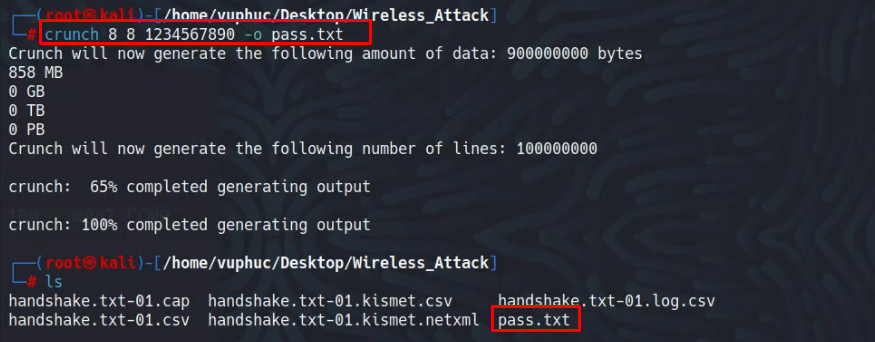
Sử dụng lệnh **ls** để kiểm tra file vừa ghi.



Tiến hành tạo file word list để bruteforce password bằng crunch:

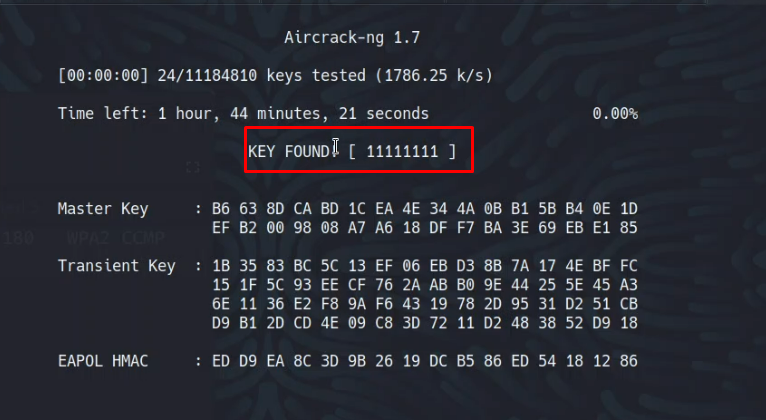
**crunch [độ dài min] [dộ dài max] [liệt kê kí tự] [tùy chọn thêm]**

Trong bài này sẽ là **crunch 8 8 1234567890 -o pass.txt**



Sau khi đã có wordlist tiến hành decode file vừa ghi bằng lệnh **aircrack-ng -w pass.txt -b 52:A1:95:F8:92:6B handshake.txt-01.cap**

Khi nào hiện kết quả dưới thì đã tìm được key thành công:



### Đánh giá, kết luận

Đã thành công bẻ khoá mật khẩu Wifi sử dụng phương thức mã hoá WPA2 bằng các sử dụng công cụ aircrack-ng và crunch.

## Tấn công Man in the middle

### Mô hình



Hình 3. Mô hình tấn công MITM

**Victim1:**

* OS: Windows 10 HOME
* IP: 192.168.248.39
* MAC:08:6A:C5:64:80:0C

**Victim2:**

* OS:Windows 10 Home
* IP: 192.168.248.106
* MAC:4C:03:4F:E8:97:4D

**Attacker:**

* OS: Kali linux 2022.4
* IP: 192.168.248.69
* MAC: 28:87:BA:1F:7F:56

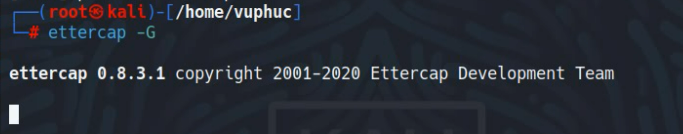
### Kịch bản

Khi kẻ tấn công xâm nhập thành công vào mạng nội bộ, kẻ tấn công hoàn toàn có thể tấn công MITM bất kì 2 máy nào trong mạng nội bộ.

### Thực nghiệm

Các câu lệnh sau chạy dưới quyền superuser:

Trên máy attacker chạy lệnh sau để khởi động ettercap dạng GUI: **ettercap -G**

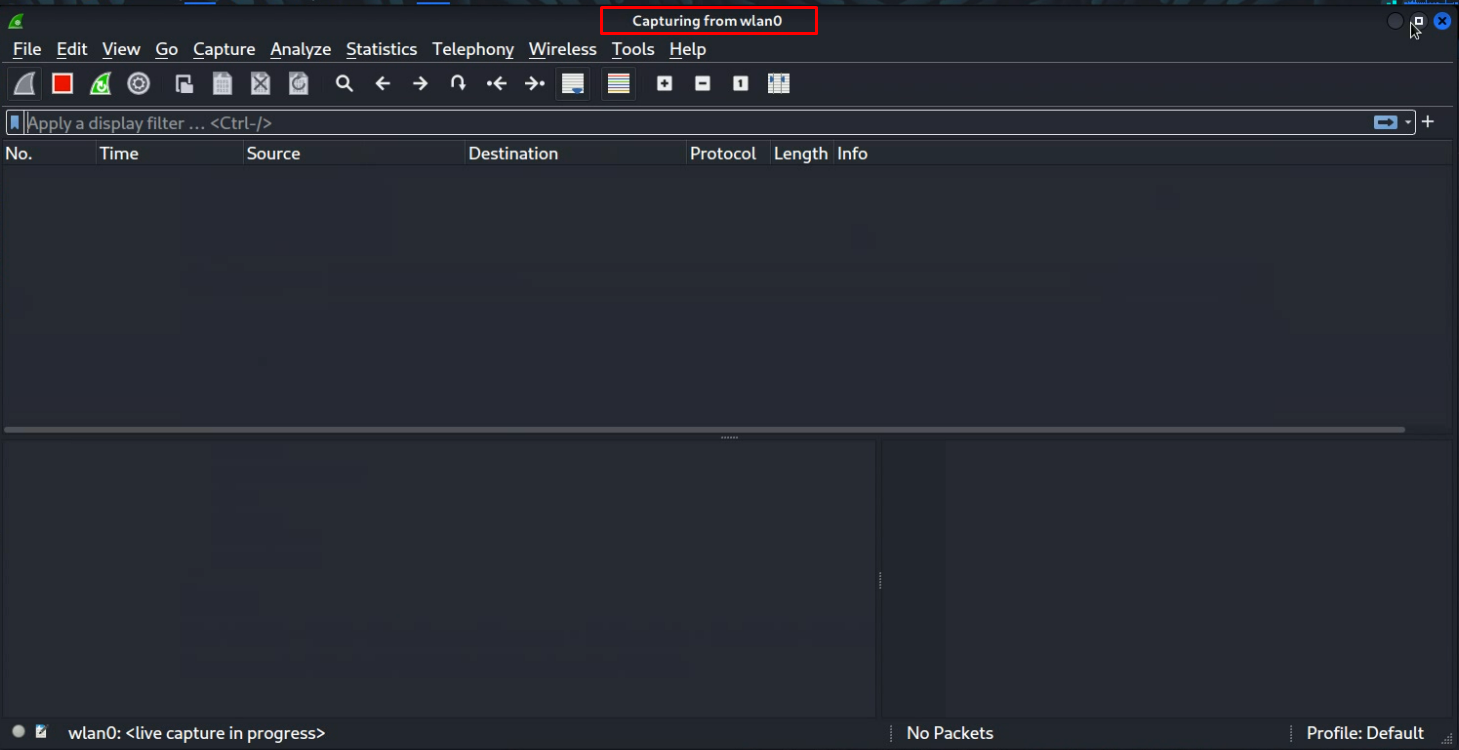


Giao diện ettercap dạng GUI:

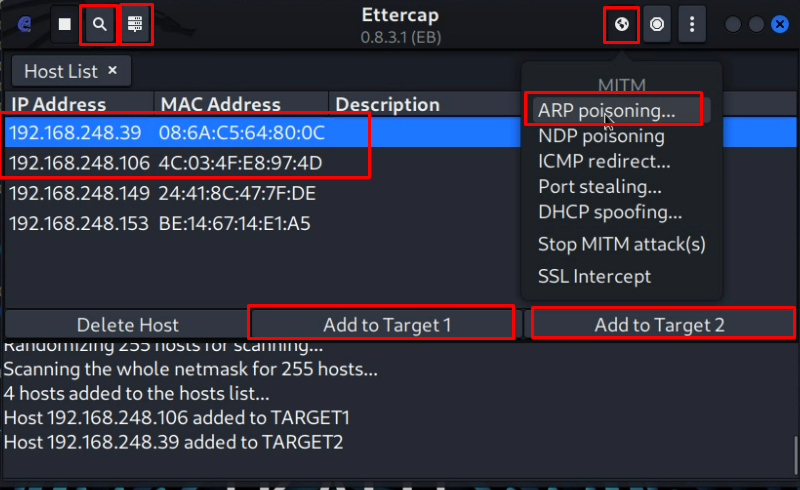


Chọn primary interface là wlan0 sau đó nhấn nút tich trên góc phải để bắt đầu.

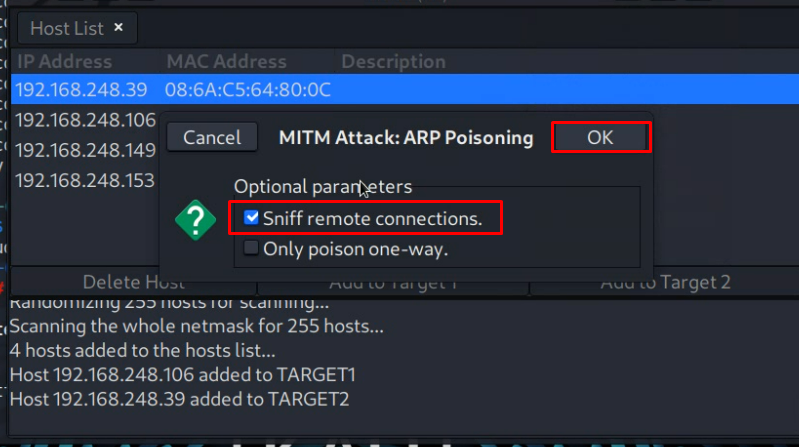
Đồng thời bật sẵn Wireshark và bắt các gói tin trên interface Wlan0



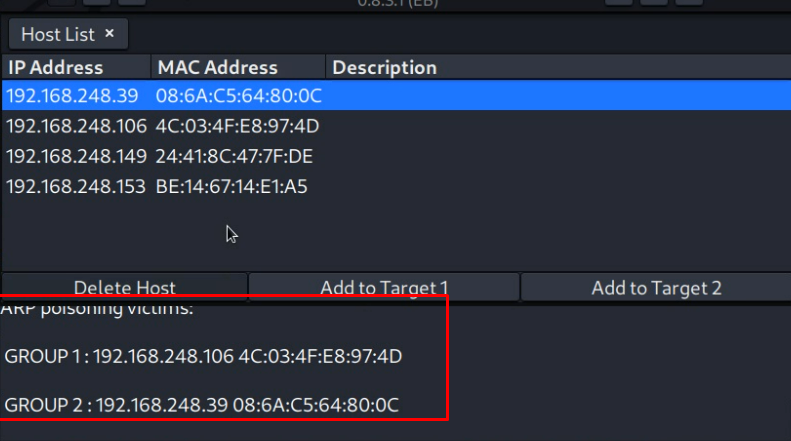
Trên giao diện GUI của ettercap bấm vào nút kính lúp để tìm các host trong mạng, sau đó bấm nút hình biểu tượng csdl để xem danh sách, bấm chọn từng mục tiêu và nhấn lần lượt vào ô Add to target 1 và Add to target 2, sau đó bấm vào nút biểu tượng địa cầu và chọn ARP poisoning… để tấn công.



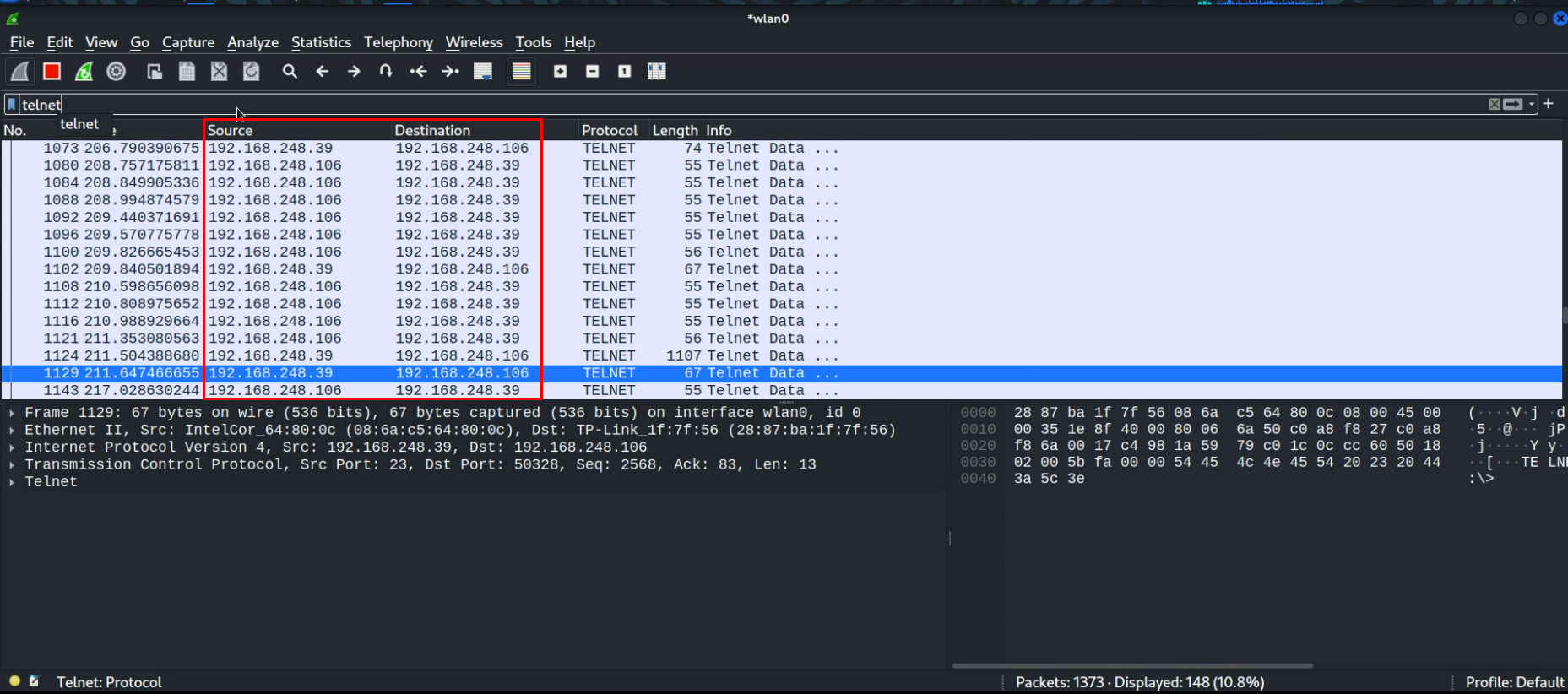
Chọn sniff remote connections sau đó nhấn OK

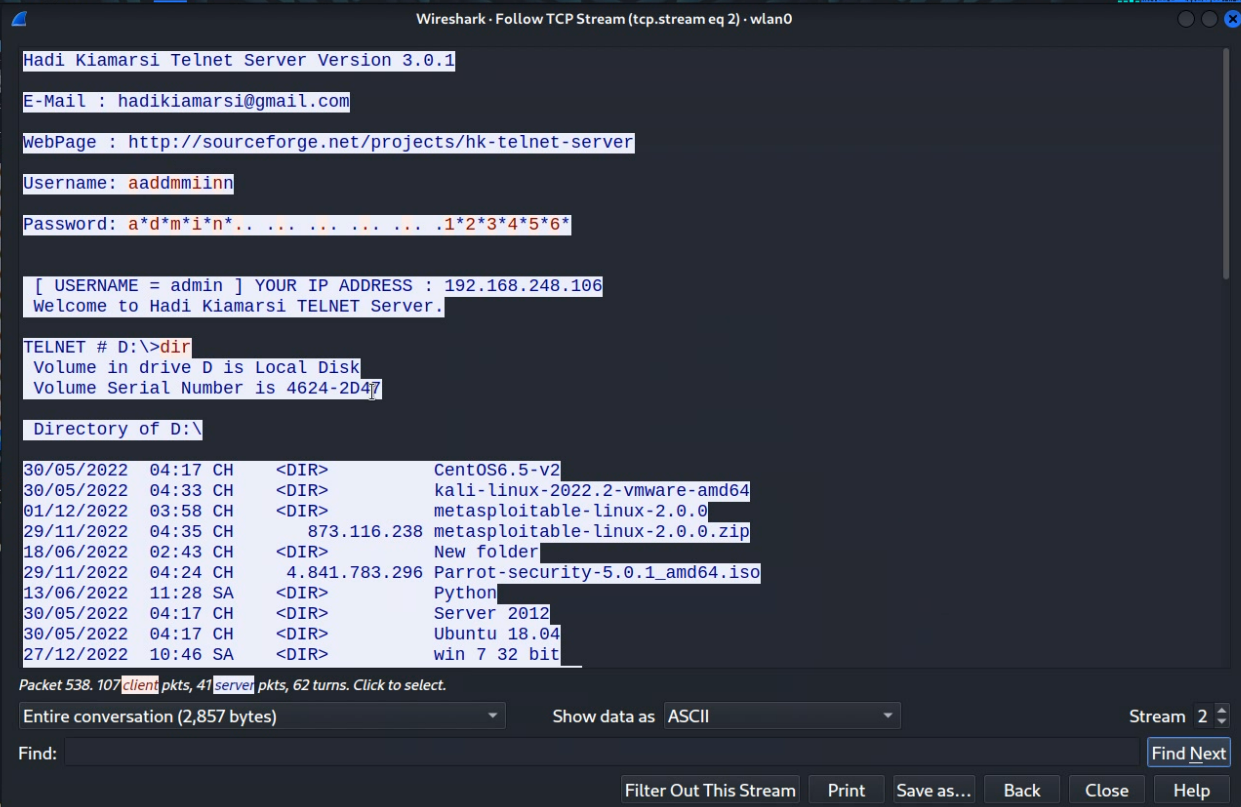


Màn hình hiện ra như vậy là thành công



Trên máy victim tiến hành telnet với nhau và quay lại phần record trong wireshark của máy attacker để xem các gói tin





### Đánh giá, kết luận

Tiến hành tấn công man in the middle thành công và đọc được các gói tin không được mã hoá trao đổi giữa 2 máy.

KẾT LUẬN

Ba chương của bài tập đã thể hiện được rằng những mục tiêu đặt ra khi thực hiện bài tập đều đã đạt được. Cụ thể:

Chương 1 đã hệ thống lại kiến thức tổng quan kiểm thử thâm nhập , các kĩ thuật tấn công mạng.

Chương 2 đã giới thiệu từng công cụ thực hiện . Khái niệm , ưu điểm , nhược điểm của từng công cụ , đem đến cho người đọc những cái nhìn khách quan của từng công cụ.

Trong chương 3 chỉ ra rõ các bước để triển khai dịch vụ kiểm thử cũng như thâm nhập mạng nội bộ wifi . Từ đó khai thác các thông tin cần thiết của hệ thống.

Trong khi thực hiện bài tập này, do hạn chế về thời gian và trình độ nên không tránh khỏi những thiếu sót và hạn chế nhất định, chúng em rất mong có sự đóng góp ý kiến và bổ sung của thầy để nhóm có thêm kinh nghiệm hoàn thành tốt hơn trong những đề tài tiếp theo.

Chúng em xin chân thành cảm ơn!

TÀI LIỆU THAM KHẢO