|  |
| --- |
| HỌC VIỆN KỸ THUẬT MẬT MÃ  **KHOA AN TOÀN THÔNG TIN**  Logo HvKTMM  BÀI TẬP MÔN HỌC  **AN TOÀN MẠNG KHÔNG DÂY**  **Đề tài:**  **TÌM HIỂU VỀ**  **WIRELESS HACKING COUNTERMEASURES**  **AND SECURITY TOOLS**  Sinh viên thực hiện: ĐỖ XUÂN BẢNG AT160206  PHẠM CÔNG HƯỞNG AT160230  VŨ HỒNG PHÚC AT160240  **Nhóm 07**  Giảng viên hướng dẫn: Thầy NGUYỄN NGỌC TOÀN    Hà Nội, 11-2022 |

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

KHOA AN TOÀN THÔNG TIN

BÁO CÁO MÔN HỌC

ĐỀ TÀI:

**WIRELESS HACKING COUNTERMEASURES**

**AND SECURITY TOOLS**

Bảng Phân Công Công Việc

|  |  |
| --- | --- |
| Phạm Công Hưởng |  |
| Đỗ Xuân Bảng |  |
| Vũ Hồng Phúc |  |

**MỤC LỤC**

**LỜI MỞ ĐẦU**

**Chương I. Các biện pháp phòng chống tấn công mạng không dây**

*1.1. Lớp bảo mật không dây*

*1.2. Phòng thủ chống bẻ khóa WPA / WPA2 / WPA3*

*1.3. Phòng thủ chống lại các cuộc tấn công KRACK*

*1.4. Phòng thủ chống lại các cuộc tấn công aLTEr*

*1.5. Phát hiện và chặn các AP giả mạo*

*1.6. Phòng thủ chống lại các cuộc tấn công mạng không dây*

*1.7. Phòng thủ chống lại tấn công Bluetooth*

**Chương II. Wireless Security Tools**

*2.1. Hệ thống ngăn chặn xâm nhập mạng không dây WIPS*

*2.2. Công cụ kiểm tra bảo mật Wi-Fi*

*2.3. Công cụ lập kế hoạch dự đoán Wi-Fi*

*2.4. Công cụ dò quét lỗ hổng Wi-Fi*

*2.5. Công cụ bảo mật Bluetooth*

*2.6. Công cụ bảo mật Wi-Fi cho di động*

**Chương III. Thực nghiệm dò quét lỗ hổng bằng công cụ Zenmap**

**LỜI MỞ ĐẦU**

**Chương I. Các biện pháp phòng chống tấn công mạng không dây**

**Wireless Security Layers**

Graphical user interface, application

Description automatically generated

*1.1. Lớp bảo mật không dây*

Một cơ chế bảo mật không dây có sáu lớp. Cách tiếp cận phân lớp này làm tăng phạm vi ngăn chặn kẻ tấn công xâm phạm mạng và tăng khả năng bắt kẻ tấn công. Hình dưới đây cho thấy cấu trúc của các lớp bảo mật không dây.

Diagram

Description automatically generated

* Bảo mật tín hiệu không dây: Trong mạng không dây, mạng và phổ tần RF trong môi trường phải được giám sát và quản lý liên tục để xác định các mối đe dọa và khả năng nhận biết. Hệ thống phát hiện xâm nhập không dây (WIDS) phân tích và giám sát phổ RF. Tạo cảnh báo giúp phát hiện các thiết bị không dây trái phép vi phạm chính sách bảo mật của mạng. Các hoạt động như sử dụng băng thông tăng, nhiễu sóng RF và các AP không dây giả mạo không xác định có thể cho thấy có kẻ xâm nhập độc hại trên mạng. Giám sát liên tục mạng là biện pháp duy nhất có thể ngăn chặn các cuộc tấn công như vậy và bảo mật mạng
* Bảo mật kết nối: Xác thực từng khung / gói cung cấp khả năng bảo vệ chống lại các cuộc tấn công MITM. Nó ngăn kẻ tấn công đánh cắp dữ liệu khi hai người dùng thực giao tiếp với nhau, do đó đảm bảo kết nối.
* Bảo mật thiết bị: Cả quản lý lỗ hổng và bản vá đều là những thành phần quan trọng của cơ sở hạ tầng bảo mật.
* Bảo vệ dữ liệu: Các thuật toán mã hóa như WPA3, WPA2 và AES có thể bảo vệ dữ liệu.
* Bảo vệ mạng: Xác thực mạnh đảm bảo rằng chỉ những người dùng được ủy quyền mới có quyền truy cập vào mạng.
* Bảo vệ người dùng cuối: Ngay cả khi kẻ tấn công đã liên kết với các AP, tường lửa cá nhân được cài đặt trên hệ thống người dùng cuối trên mạng WLAN sẽ ngăn kẻ tấn công truy cập tệp.

*1.2. Phòng thủ chống bẻ khóa WPA / WPA2 / WPA3*

* Cụm mật khẩu

Cách duy nhất để bẻ khóa WPA là dò tìm mật khẩu [PMK](https://www.igi-global.com/dictionary/pairwise-master-key-pmk/21784) được liên kết với quá trình xác thực "bắt tay". Nếu mật khẩu này cực kỳ phức tạp thì hầu như không thể bẻ khóa được. Các biện pháp sau đây có thể được áp dụng để bảo mật mật khẩu.

* + Chọn một cụm mật khẩu ngẫu nhiên không được tạo thành từ các từ trong từ điển.
  + Chọn một cụm mật khẩu phức tạp có độ dài tối thiểu 20 ký tự và thay đổi nó thường xuyên.
  + Sử dụng các từ tạo từ phương pháp Diceware hoặc trình quản lý mật khẩu để bảo mật mật khẩu.
* Cài đặt máy khách
  + Chỉ sử dụng WPA2 với mã hóa AES / CCMP.
  + Đặt cài đặt máy khách thích hợp (ví dụ: xác thực máy chủ, chỉ định địa chỉ máy chủ và không nhắc máy chủ mới).
  + Tạo lại khóa cho mọi kết nối mới.
* Kiểm soát bổ sung
  + Đảm bảo cập nhật định kỳ phần lõi của các thiết bị không dây.
  + Sử dụng các công nghệ mạng riêng-ảo (VPN) như VPN truy cập từ xa, VPN extranet và VPN mạng nội bộ.
  + Triển khai các giao thức như IPSec và SSL / TLS để liên lạc an toàn
  + Triển khai giải pháp kiểm soát truy cập mạng (NAC) hoặc bảo vệ truy cập mạng (NAP) để kiểm soát bổ sung kết nối của người dùng cuối

*1.3. Phòng thủ chống lại các cuộc tấn công KRACK*

Sau đây là một số biện pháp đối phó để ngăn chặn các cuộc tấn công KRACK.

* Cập nhật tất cả các bộ định tuyến và thiết bị Wi-Fi với các bản vá bảo mật mới nhất.
* Bật cập nhật tự động cho tất cả các thiết bị không dây và vá chương trình cơ sở của thiết bị.
* Tránh sử dụng mạng Wi-Fi công cộng.
* Chỉ duyệt các trang web được bảo vệ và không truy cập các tài nguyên nhạy cảm khi thiết bị được kết nối với mạng không được bảo vệ.
* Nếu có thiết bị loT, hãy kiểm tra các thiết bị và không kết nối với bộ định tuyến Wi-Fi không an toàn.
* Luôn bật tiện ích mở rộng HTTPS Everywhere.
* Bật xác thực hai yếu tố.
* Sử dụng VPN để bảo mật thông tin khi truyền.

*1.4. Phòng thủ chống lại các cuộc tấn công aLTEr*

Phương pháp quan trọng nhất được đề xuất để bảo vệ mạng khỏi các cuộc tấn công aLTEr là mã hóa các truy vấn DNS với các tiêu chuẩn bảo mật phù hợp. Để thực hiện biện pháp này, Cisco, phối hợp với Apple, đã phát triển một ứng dụng có tên "Cisco Security Connectors" để ngăn chặn khách hàng truy cập các trang web không mong muốn. Ứng dụng này mã hóa các truy vấn DNS và tải chúng vào Cisco Umbrella (khối thông minh) để xác thực thêm. Nó bảo vệ mạng khỏi bị tấn công ở cấp IP cũng như cấp DNS. Các biện pháp đối phó sau đây có thể được áp dụng để bảo vệ chống lại các cuộc tấn công aLTEr.

* Mã hóa các truy vấn DNS và chỉ sử dụng các trình phân giải DNS đáng tin cậy.
* Giải quyết các truy vấn DNS bằng giao thức HTTPS.
* Chỉ truy cập các trang web có kết nối HTTPS.
* Sử dụng DNS qua Bảo mật tầng truyền tải (TLS) hoặc DNS qua TLS datagram (DTLS) để mã hóa lưu lượng DNS và bảo vệ tính toàn vẹn.
* Triển khai RFC 7858 / RFC 8310 để ngăn chặn các cuộc tấn công giả mạo DNS. Nó cũng có thể tăng mã hóa và các chính sách thông minh để phân giải tên.
* Thêm mã xác thực tin nhắn (MAC) vào các gói tin trên mặt phẳng người dùng.
* Sử dụng giao thức DNSCrypt để xác thực giao tiếp giữa máy khách DNS và trình phân giải DNS.
* Sử dụng các công cụ dành cho thiết bị di động như Zimperium để phát hiện lừa đảo và các cuộc tấn công khác từ các trang web độc hại.

*1.5. Phát hiện và chặn các AP giả mạo*

* Phát hiện các AP giả mạo
  + Quét RF: Các AP tái sử dụng chỉ thực hiện thu thập và phân tích gói tin (cảm biến RF) được cắm trên toàn bộ mạng có dây để phát hiện và cảnh báo cho quản trị viên mạng WLAN về bất kỳ thiết bị không dây nào hoạt động trong khu vực.
  + Quét AP: Các AP có chức năng phát hiện các AP lân cận sẽ hiển thị dữ liệu thông qua MIBS (Management Information Base - Cơ sở thông tin quản lý) và giao diện web của nó.
  + Đầu vào phía có dây: Phần mềm quản lý mạng sử dụng kỹ thuật này để phát hiện các AP giả mạo. Phần mềm này phát hiện các thiết bị được kết nối trong mạng LAN, bao gồm Telnet, SNMP và Cisco Discovery Protocol (CDP), sử dụng nhiều giao thức.
* Chặn các AP giả mạo
  + Từ chối dịch vụ không dây cho các máy khách mới bằng cách khởi chạy một cuộc tấn công từ chối dịch vụ (DoS) vào AP giả mạo.
  + Chặn cổng chuyển đổi mà AP được kết nối hoặc xác định vị trí AP theo cách thủ công và xóa vật lý khỏi mạng LAN.

Diagram

Description automatically generated

*1.6. Phòng thủ chống lại các cuộc tấn công không dây*

* Các phương pháp tốt nhất cho cấu hình
  + Thay đổi SSID mặc định sau khi cấu hình WLAN.
  + Đặt mật khẩu truy cập bộ định tuyến và bật tính năng bảo vệ bằng tường lửa.
  + Tắt chương trình phát sóng SSID.
  + Tắt đăng nhập bộ định tuyến từ xa và quản trị không dây.
  + Bật tính năng lọc địa chỉ MAC trên AP hoặc bộ định tuyến.
  + Bật mã hóa trên AP và thường xuyên thay đổi mật khẩu.
  + Đóng tất cả các cổng không sử dụng để ngăn chặn các cuộc tấn công vào Aps.
* Các phương pháp tốt nhất cho cài đặt SSID
  + Sử dụng kỹ thuật che giấu SSID để giữ cho một số thông báo không dây mặc định không phát SSID cho mọi người.
  + Không sử dụng SSID, tên công ty, tên mạng hoặc bất kỳ chuỗi dễ đoán nào trong cụm mật khẩu.
  + Đặt tường lửa hoặc bộ lọc gói giữa AP và Intranet của công ty.
  + Hạn chế sức mạnh của mạng không dây để nó không thể bị phát hiện bên ngoài giới hạn của tổ chức.
  + Thường xuyên kiểm tra các thiết bị không dây để biết các vấn đề về cấu hình hoặc thiết lập.
  + Thực hiện một kỹ thuật bổ sung để mã hóa lưu lượng, chẳng hạn như IPSec qua mạng không dây.
* Các phương pháp tốt nhất để xác thực
  + Chọn WPA2-Enterprise với xác thực 802.lx thay vì WPA hoặc WEP.
  + Triển khai WPA2 / WPA3-Enterprise bất cứ khi nào có thể.
  + Tắt mạng khi không được cần thiết.
  + Đặt các AP không dây ở một vị trí an toàn.
  + Luôn cập nhật trình điều khiển trên tất cả các thiết bị không dây.
  + Sử dụng máy chủ tập trung để xác thực.
  + Kích hoạt xác minh máy chủ ở phía máy khách sử dụng xác thực 802.lX để ngăn chặn các cuộc tấn công MITM.
  + Bật xác thực hai yếu tố như một tuyến phòng thủ bổ sung.
  + Triển khai các hệ thống phát hiện / ngăn chặn xâm nhập / xâm nhập không dây rogue-AP để ngăn chặn các cuộc tấn công không dây.

Diagram

Description automatically generated

*1.7. Phòng thủ chống tấn công Bluetooth*

Bluetooth hoạt động ở một trong bốn chế độ bảo mật. Các thiết bị Bluetooth áp dụng chế độ bảo mật 1 có rất ít khả năng bảo mật, khiến bản thân và mạng dễ bị tấn công. Tonaf bộ chương trình bảo mật được cải thiện khi số lượng chế độ bảo mật tăng lên. Để thiết lập ghép nối Bluetooth giữa người xác nhận quyền sở hữu (người gửi) và người xác minh (người nhận), chế độ bảo mật 2 và 3 triển khai kỹ thuật ghép nối số nhận dạng cá nhân (PIN), trong khi chế độ bảo mật 4 thực hiện kỹ thuật phân tích cú pháp bảo mật (SSP) đơn giản. Các thiết bị Bluetooth sử dụng chế độ bảo mật 4 ngăn không cho tin tặc truy cập vào thiết bị hoặc mạng Bluetooth. Sau đây là một số biện pháp đối phó để chống lại hack Bluetooth.

* Sử dụng các mẫu không thông thường làm mã PIN trong khi ghép nối thiết bị. Các tổ hợp phím không được tuần tự trên bàn phím.
* Giữ Bluetooth ở trạng thái tắt và chỉ bật khi cần. Tắt Bluetooth ngay sau khi hoàn thành tác vụ dự định.
* Giữ thiết bị ở chế độ không thể phát hiện (ẩn).
* Không chấp nhận bất kỳ yêu cầu ghép nối không xác định hoặc không mong muốn nào.
* Thường xuyên kiểm tra tất cả các thiết bị đã ghép nối trước đây và xóa mọi thiết bị đã ghép nối đáng ngờ.
* Luôn bật mã hóa khi thiết lập kết nối Bluetooth.
* Đặt phạm vi mạng của thiết bị hỗ trợ Bluetooth ở mức thấp nhất và chỉ thực hiện ghép nối trong một khu vực an toàn.
* Cài đặt phần mềm chống vi-rút hỗ trợ phần mềm bảo mật dựa trên máy chủ trên các thiết bị hỗ trợ Bluetooth.
* Thay đổi cài đặt mặc định của thiết bị hỗ trợ Bluetooth thành tiêu chuẩn bảo mật tốt nhất.
* Sử dụng mã hóa liên kết cho tất cả các kết nối Bluetooth.
* Nếu nhiều liên lạc không dây đang được sử dụng, hãy đảm bảo rằng mã hóa được cấp quyền cho mỗi liên kết trong chuỗi liên lạc.
* Tránh chia sẻ thông tin nhạy cảm qua các thiết bị hỗ trợ Bluetooth.
* Tắt kết nối tự động với mạng Wi-Fi công cộng để bảo vệ thiết bị Bluetooth khỏi các nguồn không an toàn.
* Cập nhật phần mềm và trình điều khiển của thiết bị Bluetooth và thường xuyên thay đổi mật khẩu.
* Sử dụng VPN để kết nối an toàn giữa các thiết bị Bluetooth.

**Chương II. Wireless Security Tools**

*2.1. Hệ thống ngăn chặn xâm nhập không dây (WIPS)*

Hệ thống ngăn chặn xâm nhập không dây (WIPS) là một thiết bị mạng giám sát phổ vô tuyến để phát hiện các AP (phát hiện xâm nhập) mà không có sự cho phép của máy chủ ở các vị trí gần đó. Nó cũng có thể thực hiện các biện pháp đối phó một cách tự động. WIPS bảo vệ mạng khỏi các mối đe dọa không dây và cung cấp cho quản trị viên khả năng phát hiện và ngăn chặn các cuộc tấn công mạng khác nhau.

Chart, line chart

Description automatically generated

*Triển khai WIPS*

WIPS bao gồm một số thành phần hoạt động cùng nhau để cung cấp một giải pháp giám sát an ninh thống nhất. Việc triển khai WIPS của Cisco bao gồm các chức năng thành phần sau:

* AP ở chế độ giám sát: Chế độ này cung cấp khả năng quét kênh liên tục với khả năng phát hiện tấn công và bắt gói tin.
* Công cụ dịch vụ di động (chạy dịch vụ IPS không dây): Đây là điểm trung tâm của việc tổng hợp cảnh báo từ tất cả các bộ điều khiển và các AP chế độ màn hình IPS không dây tương ứng của chúng. Thông tin báo động và hồ sơ pháp y được lưu trữ trên hệ thống để lưu trữ.
* (Các) AP chế độ cục bộ: Chế độ này cung cấp dịch vụ không dây cho các máy khách ngoài chức năng quét định vị và giả mạo theo thời gian.
* (Các) bộ điều khiển mạng LAN không dây: Các bộ điều khiển này chuyển tiếp thông tin tấn công từ các AP chế độ màn hình IPS không dây tới MSE và phân phối các thông số cấu hình cho các AP.
* Hệ thống điều khiển không dây: Cung cấp phương tiện để định cấu hình dịch vụ IPS không dây trên MSE, đẩy các cấu hình IPS không dây đến bộ điều khiển và đặt các AP ở chế độ màn hình IPS không dây. Nó cũng được sử dụng để xem cảnh báo IPS không dây, pháp y, báo cáo và truy cập bách khoa toàn thư về mối đe dọa.

Diagram

Description automatically generated

*2.2. Công cụ kiểm tra bảo mật Wi-Fi*

* IPS không dây thích ứng của Cisco

Nguồn: <https://www.cisco.com>

Hệ thống Ngăn chặn Xâm nhập Không dây Thích ứng của Cisco (IPS) cung cấp bảo mật mạng tiên tiến để giám sát và phát hiện chuyên biệt các bất thường của mạng không dây, truy cập trái phép và các cuộc tấn công RF. Được tích hợp hoàn toàn với Mạng không dây hợp nhất của Cisco, giải pháp này mang lại khả năng hiển thị và kiểm soát tích hợp trên toàn mạng mà không cần giải pháp lớp phủ. WIPS thích ứng cung cấp khả năng phát hiện và giảm thiểu mối đe dọa mạng không dây chống lại các cuộc tấn công nguy hiểm và lỗ hổng bảo mật. Nó cũng cung cấp cho các chuyên gia bảo mật khả năng phát hiện, phân tích và xác định các mối đe dọa không dây.

Graphical user interface, email

Description automatically generated

Sau đây là một số công cụ kiểm tra bảo mật Wi-Fi bổ sung:

* AirMagnet WiFi Analyzer PRO (<https://www.netally.com>)
* RFProtect (<https://www.orubanetworks.com>)
* Fern Wifi Cracker (<https://github.com>)
* OSWA-Assistant (<http://securitystortshere.org>)
* BoopSuite (https://github.com)

*2.3. Wi-Fi IPS*

Wi-Fi IPS ngăn chặn các mối đe dọa không dây bằng cách tự động quét, phát hiện và phân loại truy cập không dây trái phép và lưu lượng truy cập giả mạo vào mạng, do đó ngăn người dùng lân cận hoặc tin tặc lành nghề truy cập trái phép vào tài nguyên mạng Wi-Fi.

* WatchGuard WIPS

Nguồn: https: //www.watchguard.com

WatchGuard WIPS bảo vệ chống lại các thiết bị trái phép và Aps giả mạo, ngăn chặn các [evil twin](https://viblo.asia/p/evil-twin-gDVK26GAKLj) và ngăn chặn các cuộc tấn công độc hại như các cuộc tấn công DoS với gần như 0 lần nhận diện sai trong khi đảm bảo kết nối không dây hiệu suất cao.

Diagram

Description automatically generated

Diagram

Description automatically generated

Sau đây là một số công cụ ngăn chặn xâm nhập không dây bổ sung:

* Extreme AirDefense (<https://www.extremenetworks.com>)
* AirMagnet Enterprise (<https://www.netscout.com>)
* SonicWall SonicPoint N2 (<https://www.dell.com>)
* Dòng điểm truy cập bảo mật không dây SonicPoint (<https://www.sonicwall.com>)
* Hộp mạng IDP (<https://www.network-box.com>)

*2.4. Công cụ lập kế hoạch dự đoán Wi-Fi*

Các công cụ lập kế hoạch dự đoán Wi-Fi được sử dụng để lập kế hoạch, triển khai, giám sát, khắc phục sự cố và báo cáo về mạng không dây từ một vị trí tập trung.

* Công cụ lập kế hoạch AirMagne

Nguồn: <https://www.netally.com>

AirMagnet Planner là một công cụ lập kế hoạch mạng không dây tính đến vật liệu xây dựng, vật cản, cấu hình AP, mẫu ăng-ten và một số biến số khác để cung cấp bản đồ dự đoán đáng tin cậy về hiệu suất và tín hiệu Wi-Fi.

Graphical user interface, application

Description automatically generated

Sau đây là một số công cụ lập kế hoạch dự đoán Wi-Fi bổ sung:

* Cơ sở hạ tầng Prime của Cisco (<https://www.cisco.com>)
* Công cụ lập kế hoạch AirTight (<http://www.moupiri.co.nz>)
* Ekahau Pro (<https://www.ekahau.com>)
* Khảo sát trang web TamoGraph (<https://www.tomos.com>)
* NetSpot (<https://www.netspotapp.com>)

*2.5. Công cụ quét lỗ hổng Wi-Fi*

Các chuyên gia bảo mật sử dụng các công cụ quét lỗ hổng Wi-Fi để xác định điểm yếu trong mạng không dây và bảo mật chúng trước khi các cuộc tấn công xảy ra.

* Zenmap

Nguồn: <https://nmap.org>

Zenmap là GUI đa nền tảng cho Nmap Security Scanner, hữu ích để quét các lỗ hổng trên mạng không dây. Công cụ này lưu các bản quét lỗ hổng bảo mật dưới dạng hồ sơ để làm cho chúng chạy nhiều lần. Kết quả của các lần quét gần đây được lưu trữ trong cơ sở dữ liệu có thể tìm kiếm được.

Graphical user interface, text, application, email

Description automatically generated

Sau đây là một số công cụ quét lỗ hổng Wi-Fi bổ sung:

* Nessus Pro (<https://www.tenable.com>)
* Network Security Toolkit (<https://networksecuritytoolkit.org>)
* Nexpose (https: j / [www.rapid7.com](http://www.rapid7.com))
* Penetrator Vulnerability Scanner (<https://www.secpoint.com>)
* SILICA (<http://www.immunityinc.com>)

**Công cụ bảo mật Bluetooth**

* Bluetooth Firewall
* Nguồn: <http://www.fruitmobile.com>
* FruitMobile Bluetooth Firewall bảo vệ thiết bị Android chống lại tất cả các loại tấn công Bluetooth. Nó hiển thị cảnh báo khi các hoạt động Bluetooth xảy ra. Nó cũng cho phép người dùng quét thiết bị và phát hiện các ứng dụng có khả năng Bluetooth.

**Graphical user interface, text, application, chat or text message

Description automatically generated**

Sau đây là một số công cụ bảo mật Bluetooth bổ sung:

* Arduino Bluetooth Security Lock (<https://play.google.com>)
* Bluelog (<http://www.digifail.com>)
* BlueMaho (<https://github.cam>)
* Btscanner (<https://package.debian.org>)
* SecureTether (<https://play.google.com>)

*2.6. Công cụ bảo mật Wi-Fi cho di động*

* Wifi Protector

Nguồn: https: //www.wifiprotector.com

Wifi Protector phát hiện và bảo vệ điện thoại thông minh khỏi các kiểu tấn công ARP khác nhau, chẳng hạn như tấn công DoS và MITM. Ứng dụng này bảo vệ điện thoại khỏi các công cụ vi phạm quyền riêng tư như FaceNiff, Ettercap và DroidSheep cố gắng chiếm quyền điều khiển các phiên thông qua các cuộc tấn công MITM thông qua giả mạo ARP hoặc nhiễm độc ARP. Nó cũng cho phép sử dụng an toàn các nền tảng như Facebook, Twitter, Linkedln và eBay.

**Graphical user interface, application, Teams

Description automatically generated**

* WiFiGuard

Nguồn: <https://play.goog/e.com>

WiFiGuard, hoạt động trên cả thiết bị đã root và chưa root, có thể ngăn chặn các cuộc tấn công giả mạo ARP như các cuộc tấn công MITM, được khởi chạy bằng các ứng dụng như WifiKill, dSploit và trình đánh hơi.

* Wi-Fi Inspector

Nguồn: <https://play.goog/e.com>

Wi-Fi Inspector tìm tất cả các thiết bị được kết nối với mạng (cả có dây và Wi-Fi, bao gồm bảng điều khiển, TV, PC, máy tính bảng và điện thoại), cung cấp dữ liệu liên quan như địa chỉ IP, tên nhà sản xuất, tên thiết bị và địa chỉ MAC. Công cụ này có thể các thiết bị truy cập dữ liệu. Nó cũng cho phép lưu danh sách các thiết bị đã biết với tên tùy chỉnh và tìm ra kẻ xâm nhập một cách nhanh chóng.

Sau đây là một số công cụ bảo mật Wi-Fi bổ sung cho điện thoại di động:

* ARP Guard (<https://play.google.com>)
* Secure WiFi (https://play.google.com)
* Hotspot Shield (https://play.google.com)
* Fing - Network Tools (<https://play.google.com>)
* Net Master (https://play.google.com)

**Chương III. Thực nghiệm một số công cụ tấn công và phòng chống tấn công mạng không dây**

*3.1* Kịch bản tấn công mạng không dây

a. Sử dụng công cụ Fern WIFI Cracker

- Mô hình

Địa chỉ mạng: 192.168.0.0/24

Attacker (Kali Linux): 192.168.56.128/24

Victim (Android): 192.168.0.102/24

Gateway: 192.168.0.1/24

- Kịch bản tấn công deauth nạn nhân sử dụng wifi với mức bảo mật WPA

Bước 1: Kẻ tấn công sử dụng Fern để dò quét các điểm truy cập lân cận và phát hiện được 1 điểm truy cập sử dụng mức bảo mật WPA

Bước 2: Kẻ tấn công sẽ huỷ xác thực người dùng và chờ đợi nạn nhân kết nối lại và bắt gói tin handshake

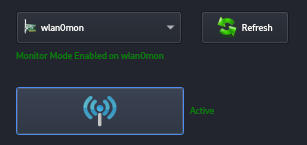
Bước 3: Nếu may mắn với từ điển mật khẩu hiện có, kẻ tấn công sẽ có được mật khẩu điểm truy cập

- Yêu cầu: Card wifi [TP-Link TL-WN722N] với chế độ Monitor

Đầu tiên, khởi động công cụ Fern WIFI Cracker



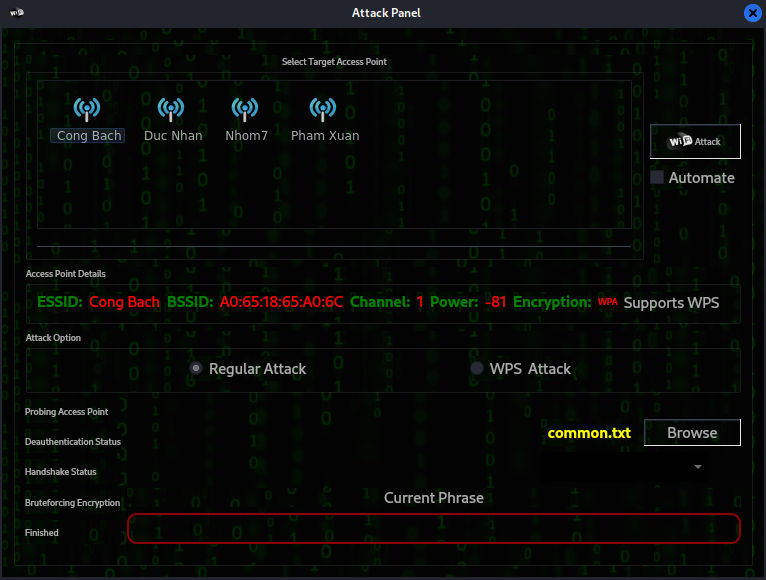
Sau đó, chọn interface và click vào biểu tượng thu phát sóng



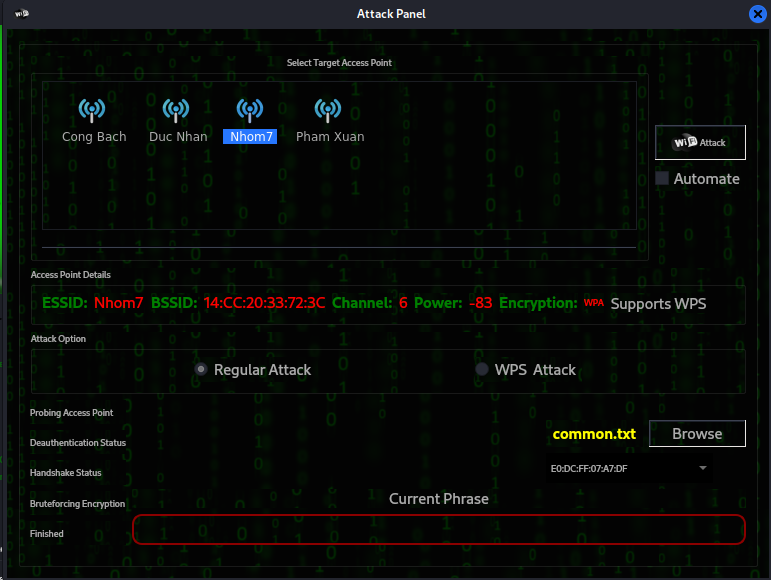
Sau một vài phút sẽ được một vài điểm truy cập sử dụng mức bảo mật WPA



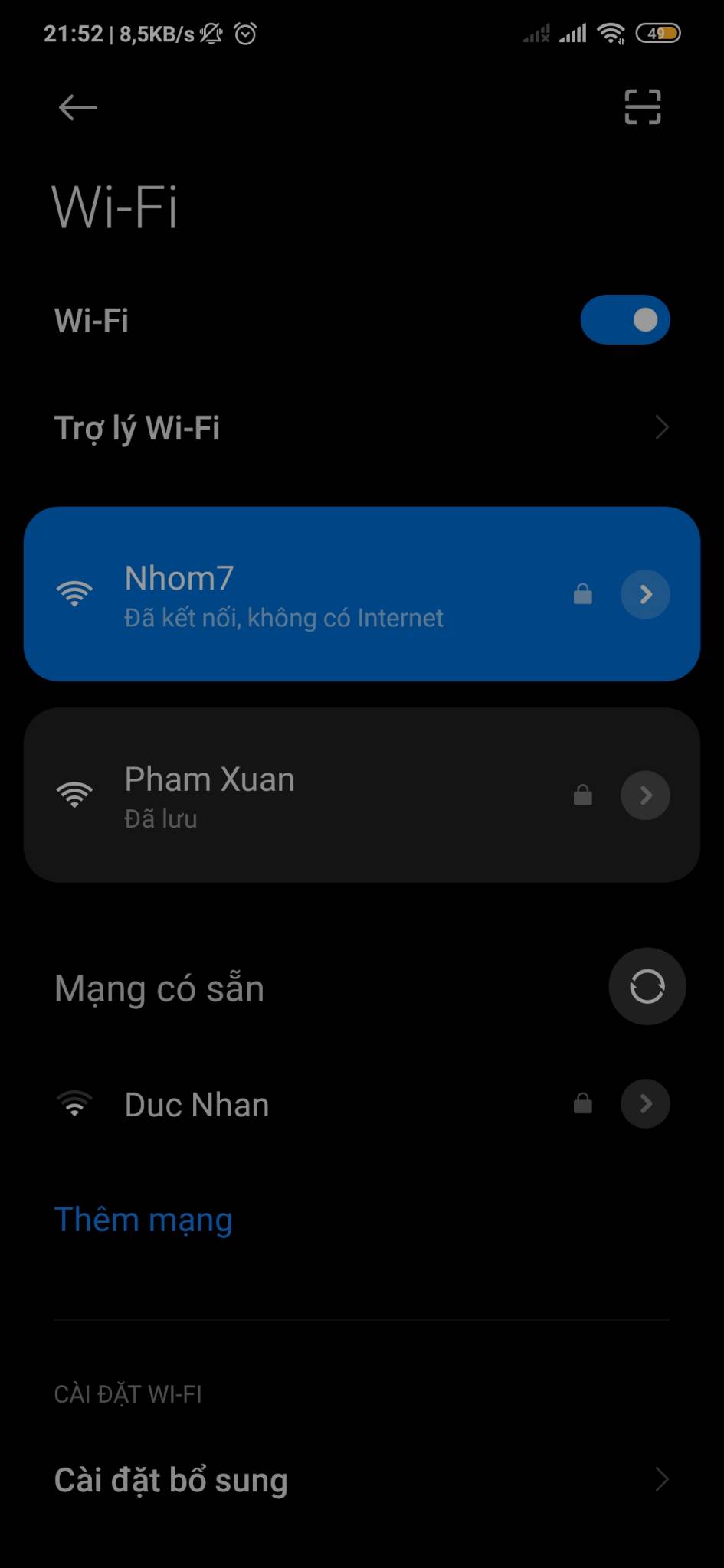
Giao diện khi nhấn vào Wifi WPA:



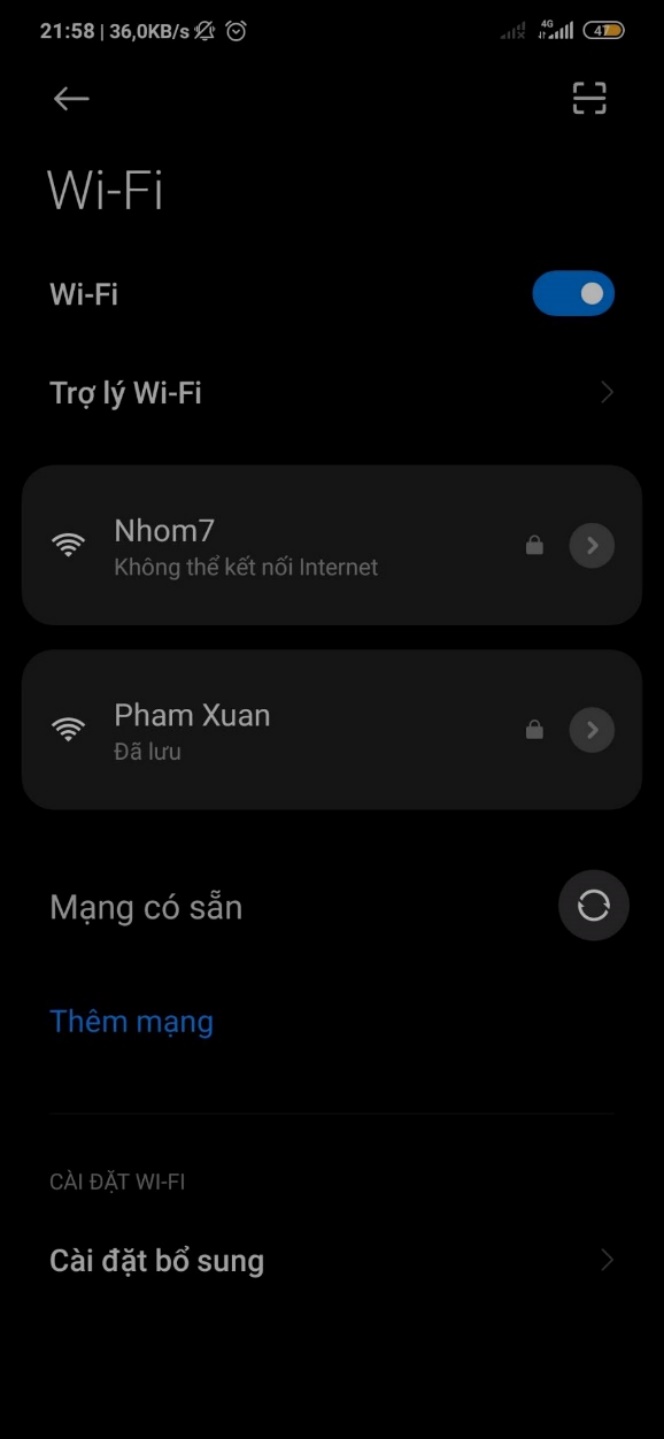
Chọn wifi muốn tấn công, ở đây là Nhom7, chờ một lúc để máy tự nhập một địa chỉ MAC của máy nạn nhân vào. Chọn wordlists và ấn Attack để tấn công



Trước khi bị DeAuth



Sau khi bị DeAuth, và sẽ tự động kết nối lại.



Quá trình hoàn tất với mật khẩu là Administrator123456



Sau khi lấy được mật khẩu của điểm truy cập, kẻ tấn công có thể truy cập vào điểm truy cập và quét tất cả các thiết bị có trong mạng và tấn công các thiết bị này tuỳ thuộc vào mục đích của kẻ tấn công.

*3.2 Phòng chống tấn công mạng không dây*

a. Phòng chống tấn công huỷ xác thực DeAuth

- Đưa modem về mức bảo mật cao nhất WPA2, thay đổi mật khẩu với mức bảo mật cao hơn.