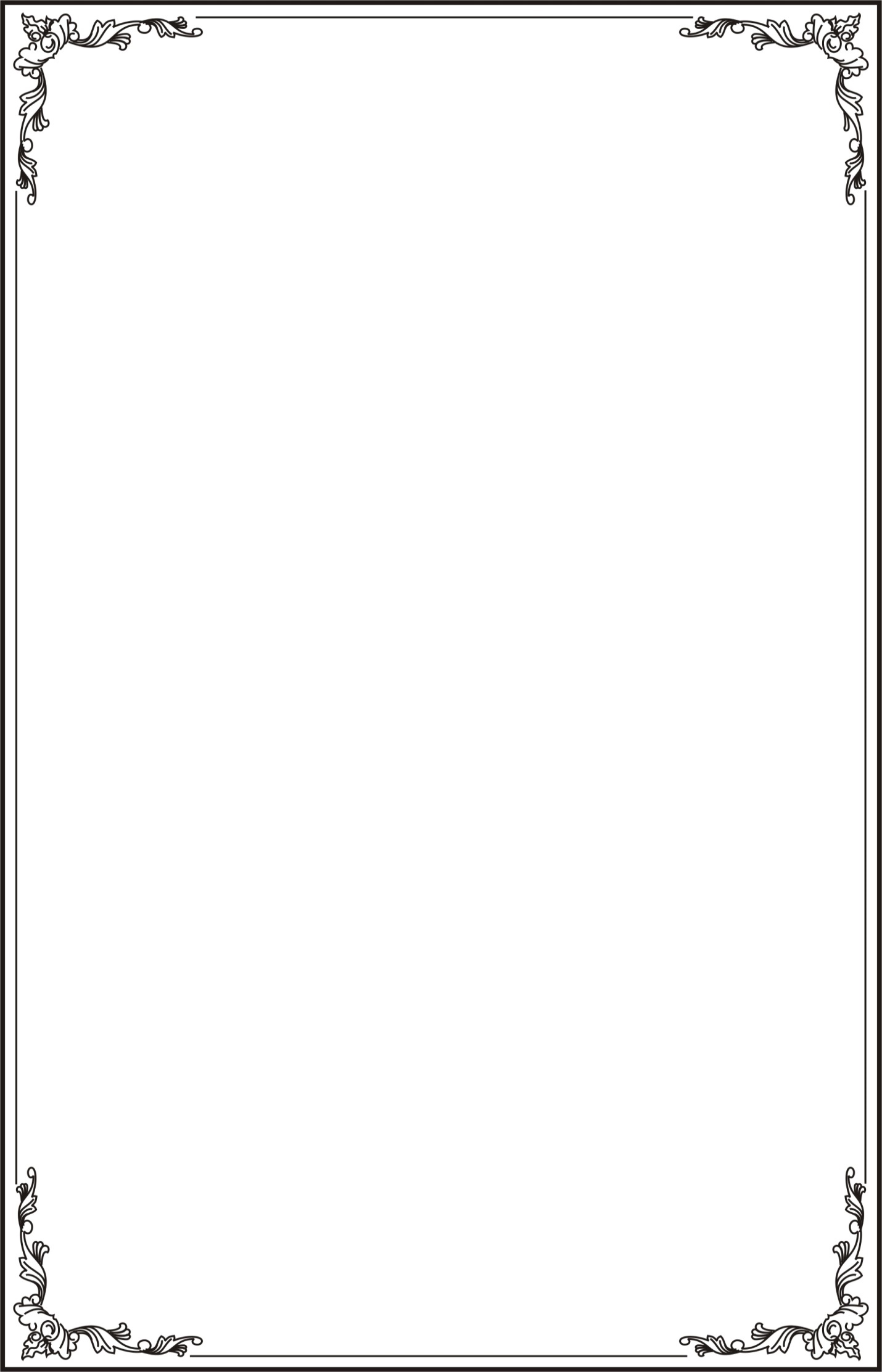
**BAN CƠ YẾU CHÍNH PHỦ**

**HỌC VIỆN KỸ THUẬT MẬT MÃ**

**🙡 Khoa An Toàn Thông Tin 🙣**

**-----🙞🙜🕮🙞🙜-----**

****

**BÁO CÁO MÔN HỌC**

**MÔN HỌC: AN TOÀN MẠNG MÁY TÍNH**

**ĐỀ TÀI: TÌM HIỂU VỀ GIẢI PHÁP PHÁT HIỆN**

**XÂM NHẬP MẠNG KHÔNG DÂY KISMET**

Giảng viên hướng dẫn : GV: Phạm Minh Thuấn

GV: Trần Thế Anh

Sinh viên thực hiện : Phan Duy Anh (AT170651)

Trần Đức thắng (AT170646)

Vương Xuân Chiến (AT170706)

Vũ Từ Khánh Linh (AT170728 )

Lê Văn Song (AT170741 )

*Hà nội, tháng 05 năm 2023*

**LỜI NÓI ĐẦU**

Giờ đây, công việc quan trọng nhất của một ngày được thực hiện trên máy tính, chẳng hạn như ngân hàng trực tuyến, giao dịch trực tuyến, học tập trực tuyến v.v., vì vậy chúng ta cần nhiều loại công cụ bảo mật khác nhau để bảo vệ thông tin chi tiết và dữ liệu quan trọng của chúng ta. Có rất nhiều hệ điều hành và công cụ bảo mật mạng. Có các công cụ bảo mật khác nhau cho các hệ điều hành khác nhau. Trong thập kỷ trước, mạng không dây là một phần cực kỳ quan trọng trong hầu hết các mạng kinh doanh. Bây giờ, mọi người sử dụng mạng không dây cho máy tính xách tay, điện thoại di động và máy tính bảng. Khi tầm quan trọng trong văn phòng của các thiết bị này tăng lên, vai trò của mạng không dây càng trở nên rõ rệt. Packet sniffing trên mạng không dây có một số khó khăn với các bộ điều hợp được hỗ trợ và đó là lúc Kismet tỏa sáng.

Vì vậy, chúng em đã tìm hiểu và hoàn thiện báo cáo về “Tìm hiểu về giải pháp phát hiện xâm nhập mạng không dây Kismet”.

Chúng em xin gửi lời cảm ơn đến các thầy đã giúp đỡ chúng em trong quá trình học tập và giảng dạy trên lớp!

**Mục Lục**

**DANH MỤC HÌNH ẢNH**

**DANH SÁCH MỤC VIẾT TẮT**

|  |  |  |
| --- | --- | --- |
| **Từ viết tắt** | **Thuật ngữ tiếng Anh/Giải thích** | **Thuật ngữ tiếng Việt/Giải thích** |
| **AP** | Access Point | Điểm truy cập |
| **AES** | Advanced Encryption Standad | Chuẩn mã hóa tiên tiến |
| **ASCII** | American Standard Code for Information Interchange | Chuẩn mã trao đổi thông tin Hoa Kỳ |
| **BSSID** | Basic service set identifier | Địa chỉ MAC của điểm truy cập |
| **DoS** | Denial of Service | Tấn công từ chối dịch vụ |
| **DS** | Distribution system | Hệ thống phân phối |
| **DSSS** | Direct sequence spread spectrum | Trải phổ trực tiếp |
| **ESSID** | Extended service set identifier | Mở rộng của SSID |
| **IDS** | Intrusion Detection System | Hệ thống phát hiện xâm nhập |
| **IoT** | Internet of Things | Internet vạn vật |
| **ISM** | Industrial, scientific and medical | Băng tầng dành cho công nghiệp, khoa học và y học |
| **ISP** | Internet service provider | Nhà cung cấp dịch vụ Internet |
| **LAN** | Local Area Network | Mạng cục bộ |
| **MAC** | Medium Access Control | Điều khiển truy cập môi trường |
| **MITM** | Man In The Middle | Tấn công người đứng giữa |
| **MIC** | Message integrity check | Phương thức kiểm tra tính toàn vẹn của thông điệp |
| **N/A** | Not Applicable | Chưa sử dụng |
| **NIC** | Network Interface Controller | Bộ điều khiển giao diện mạng |
| **PMK** | Pairwise Master Key | Khóa chính theo cặp |
| **PN** | Packet Number | Số gói |
| **PSK** | Pre-Shared Keys | Khóa chia sẻ |
| **RC4** | Rivest Cipher 4 | Thuật toán mã hóa được phát triển bởi Ron Rivest |
| **SSID** | Service set identifier | Bộ nhận dạng dịch vụ, hay còn được gọi là tên của mạng không dây |
| **TCP** | Transmission Control Protocol | Giao thức điều khiển truyền dẫn |
| **TK** | Temporal Key | Khóa tạm thời |
| **TSC** | TKIP Sequence Couter | Bộ đếm trình tự TKIP |
| **TIM** | Traffic Indication Map | Bản đồ chỉ dẫn luồng |
| **TKIP** | Temporal Key Integrity Protocol | Giao thức toàn vẹn khóa tạm thời |
| **TLS** | Transport Layer Security | Bảo mật tầng giao vận |
| **TU** | Time Unit | Đơn vị thời gian |
| **UDP** | User Datagram Protocol | Là một giao thức truyền tải |
| **VLAN** | Virtual Local Area Network | Mạng LAN ảo |
| **VPN** | Virtual Private Network | Mạng riêng ảo |
| **WI-FI** | Wireless Fidelity | Hệ thống mạng không dây sử dụng sóng vô tuyến |
| **WLAN** | Wireless Local Area Network | Mạng cục bộ không dây |

**PHẦN I. TỔNG QUAN HỆ THỐNG PHÁT HIỆN GIÁM SÁT MẠNG KHÔNG DÂY**

**1. Tổng quan về mạng không dây.**

*1.1. Mạng không dây là gì?*

- Wireless hay mạng không dây là mạng kết nối các thiết bị có khả năng thu phát sóng lại với nhau không sử dụng dây dẫn mà sử dụng song vô tuyến được truyền dẫn trong không gian thông qua các trạm thu/phát sóng.

- Ngày nay chúng đã trở thành một phần không thể thiếu trong cuộc sống khi bạn thấy chúng xuất hiện ở khắp mọi nơi trong đời sống. Nhờ sự tiện lợi của mình, mạng không dây đã dần thay thế kết nối truyền thống bằng cáp truyền thống.

- Đây là mạng dựa trên chuẩn IEEE 802.11 nên đôi khi nó còn được gọi là mạng 802.11 network Ethernet để nhấn mạnh rằng mạng này dựa trên mạng Ethernet truyền thống.

*1.2 Lịch sử ra đời của mạng không dây*

- Do “*Guglielmo Marconi”* sáng lập ra (ông là nhà phát minh vô tuyến điện, Nobel Vật lý 1909).

- Năm 1894, Marconi bắt đầu các cuộc thử nghiệm và năm 1899 đã gửi một bức điện báo băng qua kênh đào Anh mà không cần sử dụng bất kì loại dây nào.

- 3 năm sau đó, thiết bị vô tuyến của Marconi đã có thể chuyển và nhận điện báo qua Đại Tây Dương. Trong chiến tranh thế giới I, lần đầu tiên nó được sử dụng ở cuộc chiến Boer năm 1899 và năm 1912, một thiết bị vô tuyến đã được sử dụng trong con tàu Titanic.

- Trước thập niên 1920, điện báo vô tuyến đã trở thành một phương tiện truyền thông hữu hiệu bởi nó cho phép gửi các tin nhắn cá nhân băng qua các lục địa. Cùng với sự ra đời của radio (máy phát thanh), công nghệ không dây đã có thể tồn tại một cách thương mại hóa.

- Thập niên 1980, công nghệ vô tuyến là những tín hiệu analogue.

- Thập niên 1990, chuyển sang tín hiệu kỹ thuật số ngày càng có chất lượng tốt hơn, nhanh chóng hơn và ngày nay công nghệ phát triển đột phá với tín hiệu 4G.

- Năm 1994, công ty viễn thông Ericsson đã bắt đầu sáng chế và phát triển một công nghệ kết nối các thiết bị di động thay thế các dây cáp. Họ đặt tên thiết bị này là “Bluetooth”.

*1.3. Phân loại mạng không dây*

* **WPAN** là mạng vô tuyến cá nhân. Nhóm này bao gồm các công nghệ vô tuyến có vùng phủ nhỏ tầm vài mét đến hàng chục mét tối đa.

- Mục đích nối kết các thiết bị ngoại vi như máy in, bàn phím, chuột, đĩa cứng, khóa USB, đồng hồ,… với điện thoại di động, máy tính. Các công nghệ trong nhóm này bao gồm: Bluetooth, Wibree, ZigBee, UWB, Wireless USB, EnOcean…

- Đa phần các công nghệ này được chuẩn hóa bởi IEEE, cụ thể là nhóm làm việc (Working Group) 802.15. Do vậy các chuẩn còn được biết đến với tên như **IEEE 802.15.4** hay **IEEE 802.15.3…**

* **WLAN** là mạng vô tuyến cục bộ. Nhóm này bao gồm các công nghệ có vùng phủ tầm vài trăm mét. Nổi bật là công nghệ Wifi với nhiều chuẩn mở rộng khác nhau thuộc gia đình 802.11 a/b/g/h/i/…
* **WMAN** là mạng vô tuyến đô thị. Đại diện tiêu biểu của nhóm này chính là WiMAX ( Worldwide Interoperability for Microwave Access) hệ thống truy cập không dây băng rộng. Vùng phủ sóng của nó sẽ tằm vài km (tầm 4-5 km tối đa).
* **WWAN** là mạng vô tuyến diện rộng. Nhóm này bao gồm các công nghệ mạng thông tin di động như:

- UMTS (Universal Mobile Telecommunications Systems)

- GSM (Global System for Mobile Communication)

- CDMA2000 (là một tiêu chuẩn công nghệ di động họ 3G) …

- Vùng phủ của nó cũng tầm vài km đến tầm chục km.

* **WRAN** là mạng vô tuyến khu vực. Nhóm này đại diện là công nghệ 802.22 đang được nghiên cứu và phát triển bởi IEEE. Vùng phủ có nó sẽ lên tầm 40-100km. Mục đích là mang công nghệ truyền thông đến các vùng xa xôi hẻo lánh, khó triển khai các công nghệ khác.

*1.4 Các chuẩn trong mạng không dây*

Năm 1997, IEEE (Institute of Electrical and Electronics Engineers) đã giới thiệu một chuẩn đầu tiên cho Wireless LAN là 11.

* **802.11** chỉ hỗ trợ cho tốc độ cực đại lên đến 2 Mbps, sử dụng tần số 2,4 Ghz của sóng radio hoặc hồng ngoại.

○ Quá chậm đối với hầu hết các ứng dụng

○ Cần mở rộng IEEE 802.11 để có được băng tần lớn hơn.

* **802.11a** ra đời cùng thời gian với chuẩn b:
* Tần số: 5.0 Ghz
* Tốc độ: 54 Mbps
* Độ rộng băng thông: 20 Mhz
* Tầm hoạt động: 60-200m
* Điều chế: OFDM (Orthogonal Frequency-Division Multiplexing – 1 công nghệ đặc biệt trong điều chế đa sóng mang).
* Ưu điểm: do sử dụng ở tần số cao nên tránh được các cản nhiễu của thiết dân dụng, tốc độ truyền nhanh
* Nhược điểm: giá thành cao tầm phủ sóng ngắn hớn và dễ bị che khuất
* **802.11b** ra đời 10/1999:
* Tần số: 2,4 Ghz ○ Tốc độ: 11 Mbps ○ Độ rộng băng thông: 20 Mhz
* Tầm hoạt động: 300-500m ○ Điều chế: DSSS (Direct Sequence Spread Spectrum), CCK (Complementary Code Keying)
* Ưu điểm: giá thành thấp, tầm phủ sóng tốt và không dễ che khuất
* Nhược điểm: tốc độ thấp, có thể bị nhiễu bởi các thiết bị gia dụng như gương, bức tường, các thiết bị…
* **802.11g** ra đời vào tháng 6/2003:
* Tần số: 2,4 Ghz
* Tốc độ: 54 mbps-108 Mbps
* Độ rộng băng thông: 20 Mhz
* Tầm hoạt động: 300-500m ○ Điều chế: DSSS, CCK, OFDM
* Ưu điểm: tốc độ cao, phạm vi tín hiệu tốt ít bị che khuất.
* Nhược điểm: giá thành hơi đắt hơn so với 802.11b các thiết bị có thể bị xuyên nhiễu từ nhiều thiết bị khác sử dụng cùng băng tần.
* **802.11n** ra đời vào năm 2009:
* Tần số: 2,4 hoặc 5 Ghz
* Tốc độ: 54 Mbps-600 Mbps (trên lý thuyết)
* Độ rộng băng thông: 20 hoặc 40 Mhz
* Tầm hoạt động: 300-500m
* Điều chế: DSSS, CCK, OFDM
* Ưu điểm: tốc độ nhanh phạm vi tín hiệu tốt, khả năng chịu đựng tốt hơn từ việc xuyên nhiễu các nguồn bên ngoài.
* Nhược điểm: chuẩn này vẫn chưa được sử dụng rộng rãi, do giá thành đắt hơn so với chuẩn 802.11g sử dụng nhiều tín hiệu có thể gây nhiễu với mạng 802.11b/g ở gần.
* Ngoài ra còn có một số chuẩn wireless khác:
* **IEEE 802.11h**: Chuẩn này được sử dụng ở châu âu, dãy tầng 5 Ghz, nó cung cấp tính năng lựa chọn kênh động nhằm tránh nhiễu
* **IEEE 802.11d**: tính năng bổ sung
* **IEEE 802.11c**: các thủ tục quy định cách thức bắt cầu giữa các mạng Wi-Fi. Tiêu chuẩn này thường đi cặp với 802.11d.
* **IEEE 802.11e**: đưa QoS (Quality of Service) vào Wi-Fi, qua đó sắp đặt thứ tự ưu tiên cho các gói tin, đặc biệt quan trọng trong trường hợp băng thông bị giới hạn hoặc quá tải…

**2. Giới thiệu Kismet**

Kismet là một công cụ tuyệt vời được sử dụng để tìm kiếm mạng kết nối, gói sniffer cho các lớp 802.11a, 802.11b, 802.11g và 802.11n. Phần mềm này hỗ trợ các nền tảng Linux, OSX, Windows và BSD. Nó tìm kiếm mạng bằng cách thu thập các gói tin để tìm các mạng có tên chuẩn và các mạng ẩn.

Với tính năng Network Detector, Sniffer, và hoạt đông như một thiết bị giám sát IDS. Nó tự động phát hiện những gói tin thuộc các Protocol nào như TCP, UDP, ARP, và các gói tin DHCP, được ghi lại bằng Wireshark/TCPDump. Tools này còn được sử đụng để Wardriving, Warwalking, và wareflying.

Một trong những lợi thế lớn nhất của việc sử dụng Kismet là khả năng sử dụng màn hình hoặc chế độ rfmon. Điều này cho phép xác định các mạng không dây không phát Mã định danh nhóm dịch vụ (SSID) trong khung báo hiệu và đặt Kismet khác biệt với đối tác Windows NetStumbler.

Kismet cũng là một công cụ tuyệt vời cho người kiểm tra thâm nhập cần thực hiện khám phá mạng WLAN để xác định mạng mục tiêu. Mặc dù không phải lúc nào cũng chính xác 100%, Kismet có thể được sử dụng để xác định loại mã hóa được sử dụng trên mạng. Khi mục tiêu và mức mã hóa đã được xác định, một số công cụ nguồn mở có sẵn để tiếp tục thử nghiệm thâm nhập.

*2.1. Ưu điểm và nhược điểm của Kismet*

* Mất nhiều thời gian để tìm kiếm mạng.
* Nó chỉ có thể xác định được mạng không dây (Wi-Fi) trong một phạm vi nhỏ, nếu phạm vi nhiều hơn thì nó không thể hoạt động bình thường.
* Kết quả rất tốt cho phạm vi nhỏ.

*2.2. Các tính năng hiện tại:*

* Hỗ trợ tính năng sniffing 802.11
* Cung cấp tính năng ghi nhật ký PCAP tương thích với các công cụ packet sniffing khác như Wireshark và TCPDump.
* Tuân theo mô hình cấu trúc máy khách/máy chủ.
* Có cấu trúc plug in, vì vậy bạn có thể mở rộng chức năng của những tính năng cốt lõi.
* Cung cấp tùy chọn để xuất các gói sang nhiều công cụ khác thông qua giao diện trực quan. Tính năng xuất các gói này có thể được thực hiện trong thời gian thực.
* Cung cấp hỗ trợ cho các giao thức mạng khác như 802.11a, 802.11b, 802.11g và 802.11n.
* Kismet khác với các máy dò mạng không dây khác ở chỗ làm việc thụ động. Cụ thể, mà không cần gửi bất kỳ gói tin có thể đăng nhập nào, nó có thể phát hiện sự hiện diện của cả điểm truy cập không dây và máy khách không dây, đồng thời liên kết chúng với nhau
* Kismet cũng bao gồm các tính năng IDS không dây cơ bản như phát hiện các chương trình đánh hơi không dây đang hoạt động bao gồm NetStumbler, cũng như một số cuộc tấn công mạng không dây.
* Kismet cũng có khả năng phát hiện các mạng mặc định hoặc "chưa được định cấu hình", các yêu cầu thăm dò và xác định mức độ mã hóa không dây được sử dụng trên một điểm truy cập nhất định.
* Để tìm được nhiều mạng nhất có thể, Kismet hỗ trợ tính năng nhảy kênh. Điều này có nghĩa là nó liên tục thay đổi từ kênh này sang kênh khác không theo trình tự do người dùng xác định với giá trị mặc định để lại lỗ hổng lớn giữa các kênh (ví dụ: 1-6-11-2-7-12-3-8- 13-4-9-14-5-10). Ưu điểm của phương pháp này là nó sẽ bắt được nhiều gói hơn vì các kênh liền kề chồng lên nhau.
* Kismet cũng hỗ trợ ghi lại các tọa độ địa lý của mạng nếu đầu vào từ bộ thu GPS có sẵn.

*2.3. Kismet và ánh xạ*

* Các định dạng dữ liệu của Kismet rất phù hợp để cho phép tích hợp dữ liệu này vào các công cụ và chương trình liên quan đến lập bản đồ. Công cụ bản đồ gốc của Kismet được gọi là GPSMap. GPSMap được thiết kế để tải xuống bản đồ từ các kho lưu trữ trực tuyến và phủ các mạng Kismet lên chúng
* WiGLE (Wireless Geographic Logging Engine) là một cơ sở dữ liệu trực tuyến bao gồm hơn 15 triệu mạng không dây được ghi lại, hầu hết đều có tọa độ địa lý.
* WiGLE cấp quyền truy cập vào Mã định danh nhóm dịch vụ (SSID) và số liệu thống kê của nhà sản xuất, số liệu thống kê sử dụng bộ tám và kênhvà một bản đồ Web có thể duyệt qua về thế giới. WiGLE Google Map là một công cụ dựa trên Web hiển thị dữ liệu WiGLE trên Google Maps. GpsDrive là hệ thống định vị được thiết kế để hiển thị vị trí GPS của một người trên bản đồ có thể thu phóng. Mặc dù nó có thể được sử dụng hoàn toàn độc lập với Kismet như một chương trình ánh xạ độc lập, nó tích hợp độc đáo với Kismet (và MySQL) để hiển thị dữ liệu mạng Kismet trên bản đồ. GpsDrive yêu cầu hỗ trợ Ngôn ngữ truy vấn có cấu trúc (SQL) để giao tiếp với Kismet. Các lựa chọn thay thế khác để lập bản đồ với dữ liệu Kismet bao gồm Kismet Earth và OpenStreetMap.

*2.4. Kismet Drone*

Kismet đã phát triển khả năng chạy Drone: các thiết bị có thẻ không dây chỉ đơn thuần gửi dữ liệu của chúng trở lại máy chủ Kismet. Nếu bạn chạy Kismet Drone trên hộp DD-WRT của mình, bạn sẽ cần chạy máy khách và máy chủ ở nơi khác. Cả hai đều có thể nằm trên máy tính để bàn của bạn hoặc bạn có thể có một máy ở nơi khác chỉ chạy máy chủ. Chạy Drone Kismet trên WRT của bạn và Máy khách / Máy chủ trên (các) máy tính để bàn dường như là cách cài đặt phổ biến nhất đối với người dùng windows. Mặc dù Drone yêu cầu nhiều công việc hơn một chút để cài đặt, nhưng chúng cung cấp 3 lợi ích so với việc chạy các máy chủ đầy đủ trên WRT:

- Sẽ dễ dàng hơn để lưu các gói đã bắt để sử dụng sau này, chẳng hạn như để giải mã WEP.

- Việc lắp đặt Drone nhỏ hơn, yêu cầu ít không gian hơn trên WRT

- Việc cài đặt Drone có thể yêu cầu ít tài nguyên xử lý hơn cho phép bạn chạy nhiều chương trình bổ sung hơn trên WRT của mình.

**PHẦN II. CÀI ĐẶT CƠ BẢN, CẤU HÌNH VÀ VẬN HÀNH**

**1. Cài đặt**

Để bắt đầu cài đặt, một người cần đăng nhập vào máy tính xách tay của mình với tư cách là người dùng gốc và tải xuống mã nguồn mới nhất từ “*www.kismetwireless.net”*. Để sử dụng Kismet, người ta cần có một số thông tin không dây được gửi đến phần máy chủ của chương trình, sau đó sẽ chuyển nó cho máy khách. Thông thường, điều này được thực hiện bởi một thẻ không dây nói chuyện với máy chủ.

Trình điều khiển thẻ không dây được chọn, tải xuống làm mã nguồn, sau đó được biên dịch và cài đặt. Kismet phải được cho biết hai phần thông tin: phần thông tin đầu tiên là tên của người dùng sẽ chạy Kismet, và phần thứ hai là thẻ không dây nào sẽ nhận dữ liệu không dây và chuyển thông tin đó cho chính Kismet. Để thực hiện điều này, kismet.conflic điều khiển cấu hình Kismet, nên được chỉnh sửa để cho nó biết thẻ không dây nào đang chạy và để gửi dữ liệu không dây đến Kismet.

Sau khi cài đặt, Kismet đã sẵn sàng để chạy. Từ giao diện dòng lệnh của Linux , người ta có thể gõ “sudo kismet” và chương trình sẽ bắt đầu.

**2. Vận hành**

Kismet có một số tệp cấu hình kiểm soát các chức năng của nó, đáng chú ý nhất là tệp “*kismet\_ui.conf”* và “*kismet.conf”* có trong thư mục “*/ etc / kismet”*, có thể được chỉnh sửa để Kismet chạy theo thói quen sử dụng. Tệp “*kismet\_ui.conf”* kiểm soát cách giao diện người dùng tự trình bày với người dùng. Giao diện người dùng là phần khách hàng của Kismet mà người dùng nhìn thấy khi chạy ứng dụng. Tệp “*kismet\_ui.conf”* là một tệp văn bản đơn giản có thể được chỉnh sửa bằng bất kỳ trình soạn thảo văn bản nào. Hai trình soạn thảo văn bản phổ biến trong Linux là vi và nano, được sử dụng trên giao diện dòng lệnh (CLI). Nhiều người dùng mong đợi rằng họ có thể sử dụng Kismet ngay lập tức chỉ với một chiếc máy tính xách tay và card mạng không dây.

**3. Cấu hình máy chủ**

Tệp cấu hình kismet.conf có thể được chỉnh sửa trực tiếp bằng trình soạn thảo văn bản UNIX yêu thích của một người (chẳng hạn như vi, pico, emacs). Tệp cấu hình được máy chủ phân tích cú pháp trong thời gian chạy và mong đợi một tệp văn bản UNIX. Nói chung, nếu một người đang chỉnh sửa tệp kismet.conf, thì nên sử dụng trình chỉnh sửa UNIX. Nhận xét trong tệp *“kismet.conf”* là các dòng bắt đầu bằng ký hiệu *“#”.* Đây thường là các nhận xét hoặc cấu hình ví dụ và thường có thể hướng dẫn các tùy chọn cần thiết để được thiết lập. Các dòng không bắt đầu bằng chú thích là các biến tham số thực do máy chủ tác động.

Tham số tên máy chủ cho phép một người đặt tên cho máy chủ cho mục đích tổ chức của một người. Kismet yêu cầu quyền truy cập root để đặt chế độ giám sát và các tùy chọn khác, sau đó nó giảm các đặc quyền trên các quy trình Kismet cho người dùng được chỉ định trong tham số này. Tên người dùng của người dùng không có đặc quyền (nonroot) phải được chỉ định trên hệ thống; vị trí hợp lý cho điều này là thư mục chính của người dùng không có đặc quyền. Dòng nguồn cho Kismet biết những gì nó cần biết để đưa dữ liệu vào chương trình để người ta có thể bắt đầu quét. Mỗi nguồn có ba tham số: tên nguồn Kismet cho loại thẻ cụ thể, tên giao diện và tên lôgic được tìm thấy trong ứng dụng khách Kismet.

Kismet README có danh sách các nguồn tương thích và tên giao diện thích hợp của chúng. Chương này giải thích một số tham số khác của tệp cấu hình Kismet . Máy chủ Kismet, ngoài tệp cấu hình, có thể được điều khiển ngay từ đầu bằng các công tắc dòng lệnh.

**4. Cấu hình nâng cao tệp *“Server.conf”***

Kismet được sử dụng trên khắp mọi nơi, từ các hệ thống truy lùng giả mạo di động, khảo sát địa điểm, đến các thiết lập IDS đầy đủ để giám sát sóng không dây xung quanh các thiết bị không dây của một người. Asus eeePC subnotebook chạy đi kèm với xandros Linux được cài đặt và với một chipset không dây Atheros, làm cho nó trở thành một giàn Kismet nhẹ và di động.

EeePC có thể được sử dụng như một thiết bị tìm kiếm và dò tìm di động nhanh chóng và nhẹ nhàng. Theo mặc định, eeePC không đi kèm với trình biên dịch và hầu hết các công cụ phát triển cơ bản. Tuy nhiên, chúng có thể được thêm vào, nhưng không phải từ nguồn asus.

Kismet chủ yếu được phát triển trên và cho các hệ thống Linux, do sự phong phú của các trình điều khiển không dây mã nguồn mở cho phép chế độ giám sát. Kismet có thể chạy trên Windows, nhưng với một số hạn chế bộ chuyển đổi Universal Serial Bus (USB) của Cacetech.

**PHẦN III. Thực Nghiệm**

**1 Chuẩn bị**

\*\* Môi trường: Hacker - kali linux, Kismet,

\*\* Công cụ sử dụng: airgeddon, Kismet, wifite

1.1. Airgeddon

-- Khái niệm: Airgeddon là một công cụ tấn công mạng Wi-Fi mạnh mẽ và phổ biến được sử dụng trong Kali Linux. Nó được thiết kế để cung cấp một giao diện dễ sử dụng và tự động hóa các tác vụ liên quan đến tấn công mạng Wi-Fi, bao gồm thu thập thông tin, tấn công phổ biến, bẻ khóa mật khẩu và nhiều tính năng khác.



-- Cài đặt : Mở terminal trên Kali Linux.

+ Cập nhật danh sách gói phần mềm bằng lệnh: **sudo apt update**.

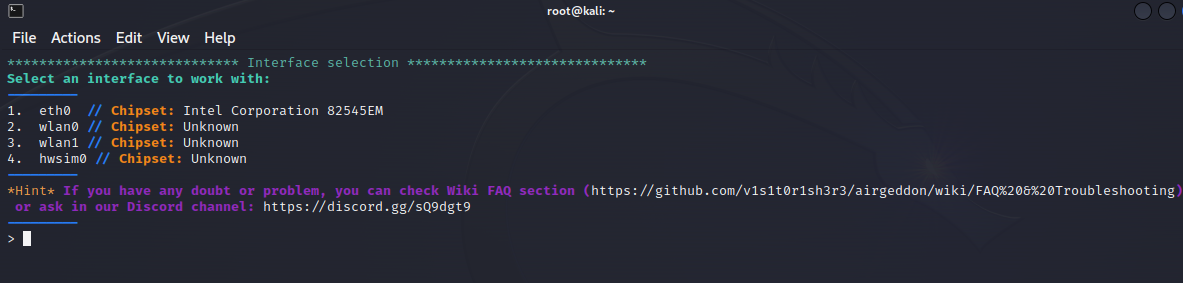
+ Cài đặt các phụ thuộc cần thiết bằng lệnh: **sudo apt install git curl iw wireless-tools**.

+ Tải mã nguồn Airgeddon từ kho lưu trữ Git bằng lệnh: **git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git.**

+ Di chuyển vào thư mục Airgeddon bằng lệnh: **cd airgeddon**.

+ Chạy tệp cài đặt bằng lệnh: **sudo bash airgeddon.sh**.

+Sau khi hoàn tất các bước trên, Airgeddon sẽ được cài đặt trên Kali Linux của bạn. Bạn có thể chạy nó bằng cách nhập lệnh **sudo airgeddon** trong terminal.



2.2.Wifite

-- Khái niệm : Wifite là một công cụ mã nguồn mở được sử dụng trong Kali Linux để thực hiện tấn công vào mạng Wi-Fi. Nó được thiết kế để giúp người dùng thực hiện các tấn công bằng cách tự động hóa quá trình thu thập thông tin, tìm kiếm điểm truy cập Wi-Fi và thực hiện tấn công vào mật khẩu Wi-Fi.

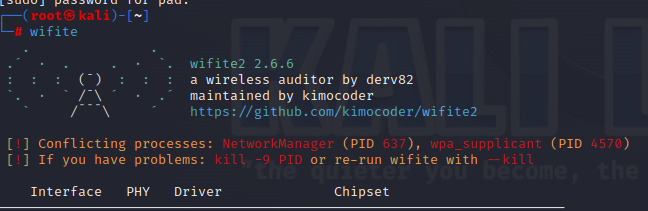
--- Cấu hình : Để cài đặt Wifite trên Kali Linux, bạn có thể thực hiện các bước sau:

+ Mở terminal trên Kali Linux.

+ Cập nhật danh sách gói phần mềm bằng lệnh: **sudo apt update.**

+ Cài đặt Wifite bằng lệnh: **sudo apt install wifite.**

+ Sau khi cài đặt hoàn tất, bạn có thể chạy Wifite bằng cách nhập lệnh **wifite** trong terminal.

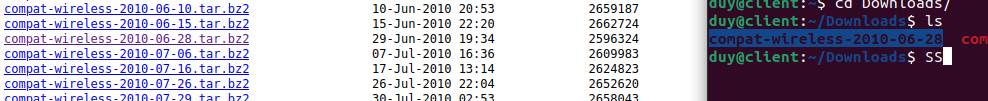


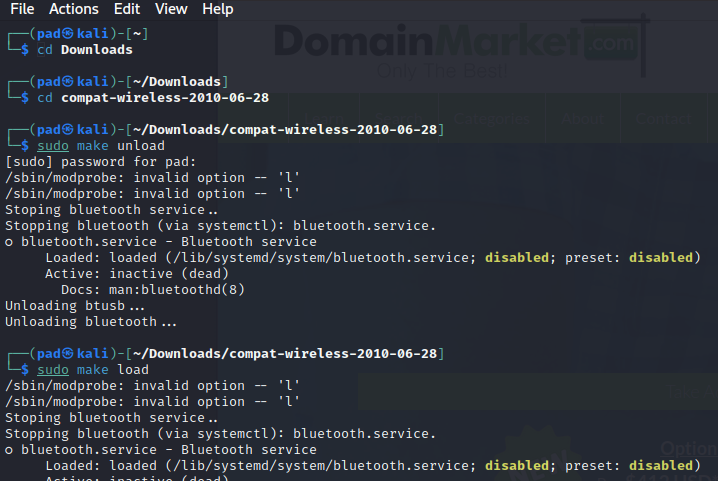
**2.Quét mạng không dây.**

\*\* Đầu tiên tạo 2 card mạng ảo wlan0 , và wlan1 :

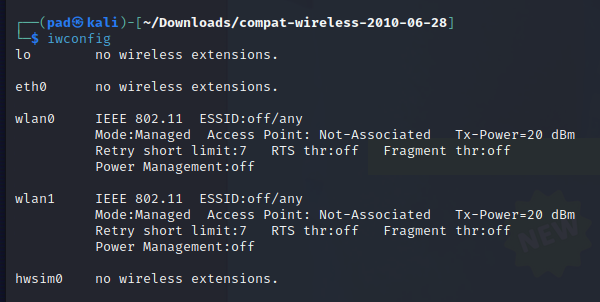
+ Vào trình duyệt web truy cập: dowload compat-wireless kali linux để tải file : compat-wireless-2010-06-28

+ Giải nén file và thực hiện cấu hình file



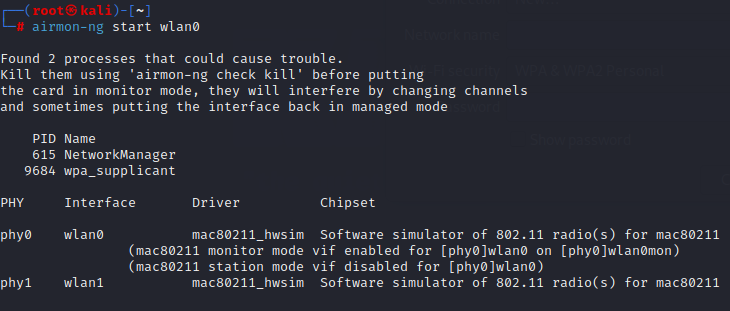


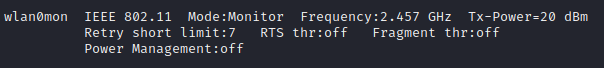
+ Kiểm tra card mạng wlan0 và wlan1:



\*\* Lúc này ta sẽ sử dụng wlan0 để giám sát mạng hay còn để thực hiện quét các mạng không dây còn wlan1 thì sẽ được sử dụng để tạo mạng không dây

+ Nâng cấp wlan0 lên wlan0mon ( chuyển sang chế độ monitor )

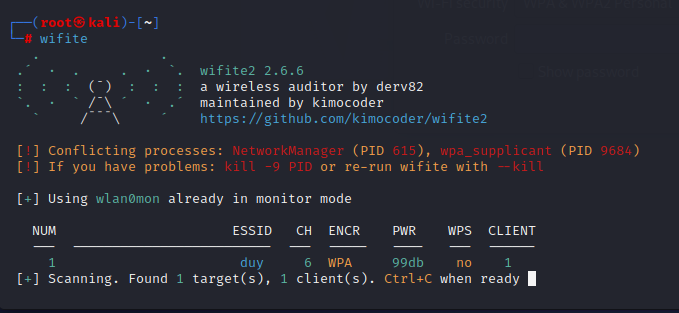




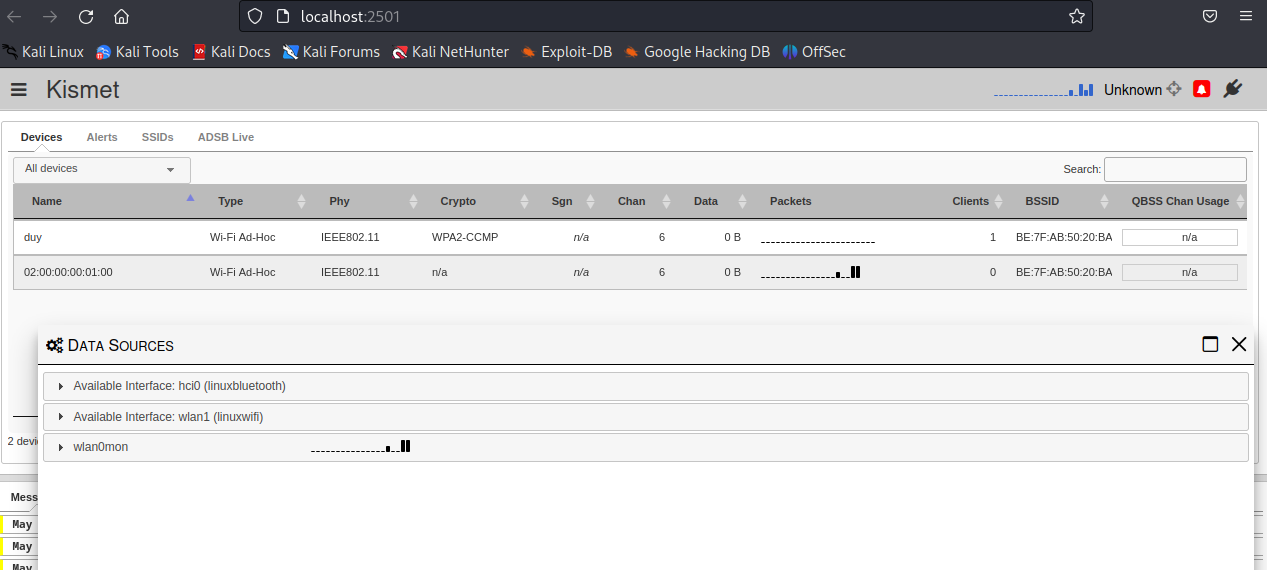
+ Tạo mạng không dây wlan1

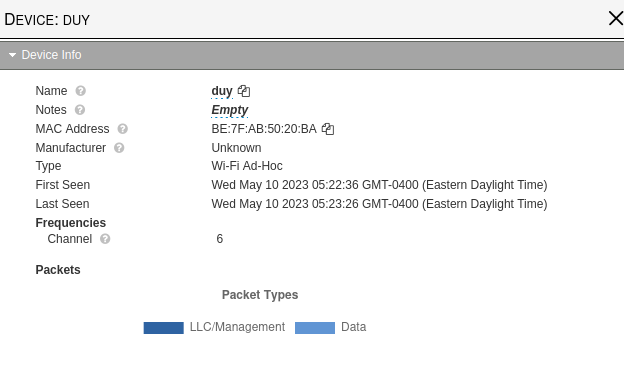


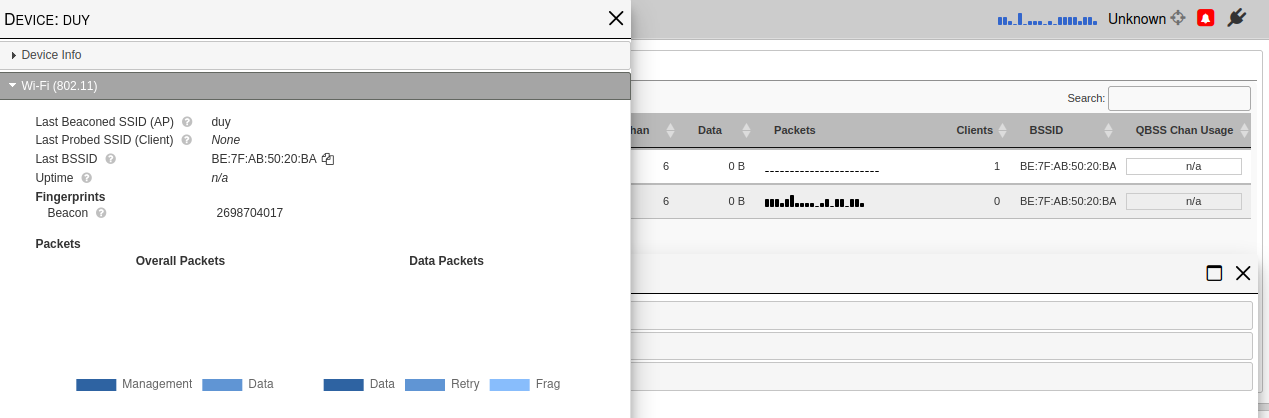
\*\* Sử dụng công cụ wifite để quét các mạng lúc này sẽ bắt được mạng wlan1 “duy’



\*\* Tiếp theo sử dụng công cụ Kismet để giám sát mạng



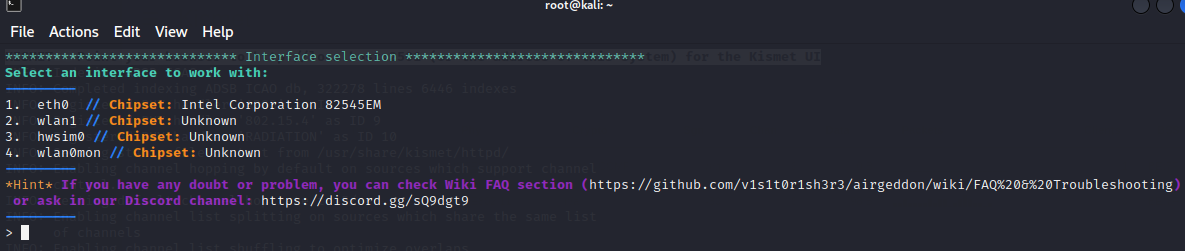




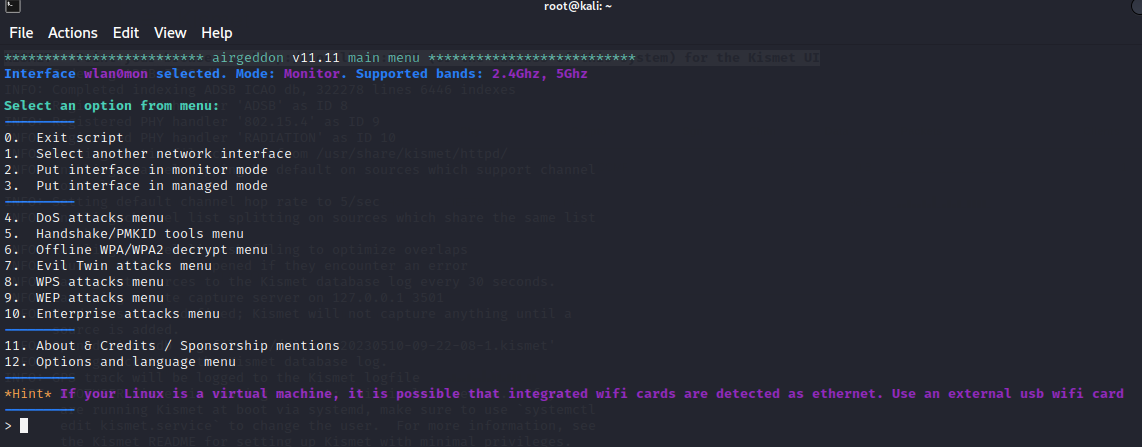
3.DoS with airgeddon

Tấn công DOS (Denial of Service) là một hình thức tấn công mạng nhằm làm cho một dịch vụ, hệ thống hoặc máy chủ trở nên không khả dụng cho người dùng hợp lệ bằng cách quá tải tài nguyên hệ thống hoặc làm cho tài nguyên không thể sử dụng được

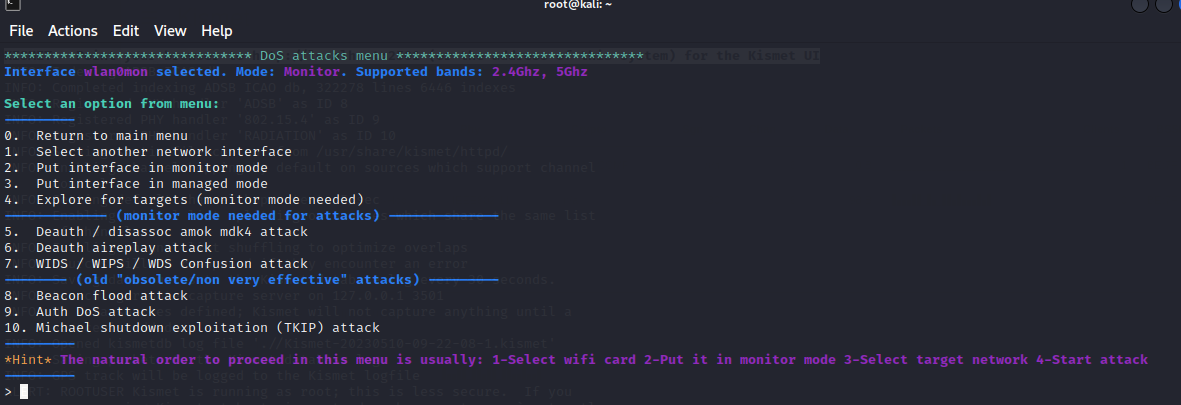
\*\* Khởi động airgeddon

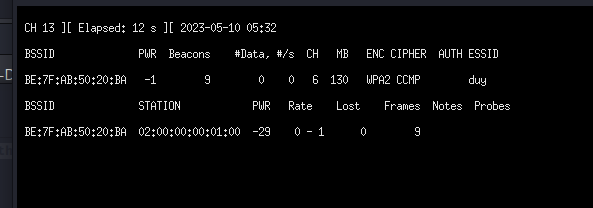


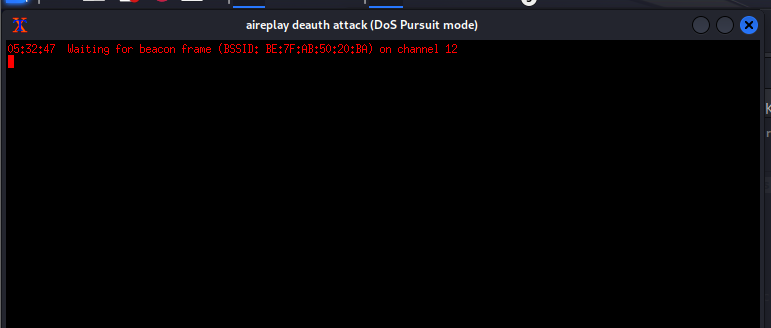
+ Chọn card mạng wlan0 bằng cách nhập số “4”



**+** Chọn “DoS attacks menu” để tấn công





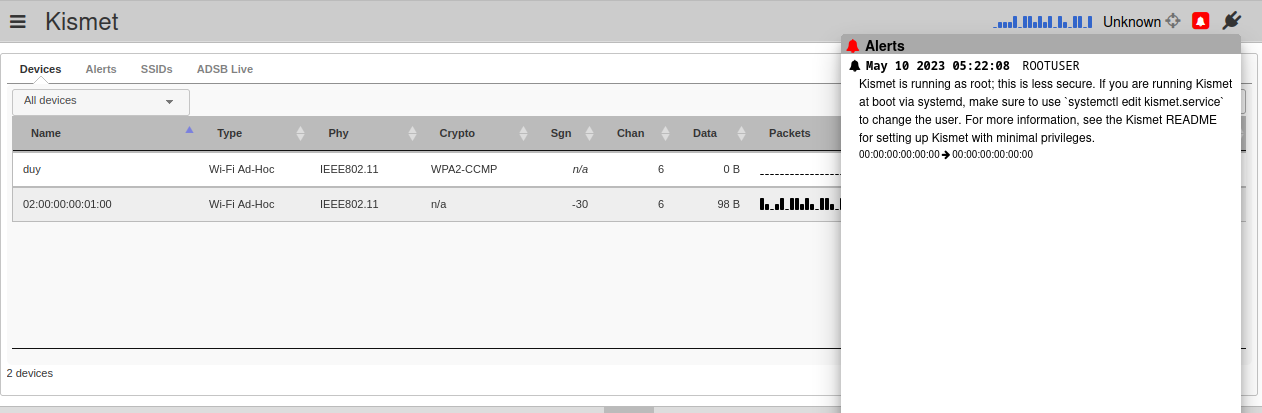


**+** Sử dụng Kismet

Lúc này Kismet sẽ hiển thị thông báo có bất thường về mạng



Nó thông báo về thời gian tấn công và cảnh báo về sự xâm nhập



Lúc này muốn truy cập vào mạng wlan1 “duy” sẽ bị văng ra không thế nào truy cập cho đến khi kẻ tấn công dừng tấn công



**3. Kết luận**

Trong bối cảnh an ninh mạng, các hành vi trộm cắp hoặc chặn dữ liệu bằng cách bắt lưu lượng truy cập mạng bằng sniffer (một ứng dụng nhằm mục đích bắt các gói tin mạng). Khi dữ liệu được truyền qua các mạng, nếu các gói dữ liệu không được mã hóa, dữ liệu trong gói mạng có thể được đọc bằng trình thám thính. Sử dụng ứng dụng sniffer, kẻ tấn công có thể phân tích mạng và lấy thông tin để cuối cùng khiến mạng bị sập hoặc bị hỏng hoặc đọc thông tin liên lạc xảy ra trên mạng.

Cũng trong bối cảnh mạng không dây phổ biến và an ninh trên môi trường mạng hiện nay rất nhiều rủi ro, bên cạnh tấn công sniffing thì còn có tấn công spoofing. Nếu như tấn công sniffing là việc chặn và bắt các gói tin thì tấn công spoofing là một cuộc tấn công giả mạo, là tình huống mà một người hoặc một chương trình làm sai lệch dữ liệu để đạt được lợi ích bất hợp pháp.

Chúng ta nên có những biện pháp phòng chống, cẩn trọng, bảo vệ thông tin dữ liệu một cách an toàn trước mối đe dọa của nó.

Áp dụng các cơ chế bảo mật cũng như ý thức, kiến thức an toàn được nâng cao là cách phòng vệ tốt nhất trên không gian mạng.

**Phụ Lục**

**TÀI LIỆU THAM KHẢO**

[1] CEH v10 Complete Training Guide With Labs, IPSpecialist LTD., 2018.

[2] [New Kismet version - Ethical hacking and penetration testing (miloserdov.org)](https://miloserdov.org/?p=2541)

[3] [Packet Sniffer là gì? - Chuẩn đoán phát hiện lỗi hệ thống mạng (quantrimang.com)](https://quantrimang.com/cong-nghe/packet-sniffer-la-gi-118706#mcetoc_1cudovq9s5)

[4] [https://www.sciencedirect.com/science/article/pii/B978159749117400009 5](https://www.sciencedirect.com/science/article/pii/B978159749117400009%205)

[5] EC-Council, Ethical Hacking and Countermeasures V11, 2020.

[6] D.T.Hanh,"Evil Twin," 20 3 2020. [Online]. Available: <https://viblo.asia/p/evil-twin-gDVK26GAKLj>.

[7] [Kismet Hacking | ScienceDirect](https://www.sciencedirect.com/book/9781597491174/kismet-hacking)

[8] V. mentor, "Cách duy trì bảo mật trước lỗ hổng wifi KRACK năm 2021," 2021. [Online]. Available: [Cách duy trì bảo mật trước lỗ hổng wifi KRACK năm 2023 (vpnmentor.com)](https://vi.vpnmentor.com/blog/cach-duy-tri-bao-mat-truoc-lo-hong-wifi-krack/)

[9] [Page not found | Uni Assignment Centre](https://www.uniassignment.com/essay-samples/information-technology/advantages-and-disadvantages-of-kismet-information-technology-essay.php)

[10] <https://khs247.com/mang-khong-day/>

[11] [Kismet - Wi-Fi, Bluetooth, RF, and more (kismetwireless.net)](https://www.kismetwireless.net/)