BỘ GIÁO DỤC VÀ ĐÀO TẠO

TRƯỜNG ĐẠI HỌC CÔNG NGHỆ TP. HCM

BÁO CÁO ĐỒ ÁN

HACKING MOBILE

Ngành: **Công nghệ thông tin**

Môn học: Bảo mật thông tin

Giảng viên hướng dẫn: ThS. Tống Thanh Văn

Sinh viên thực hiện:

Họ tên:	MSSV:
Bùi Minh Quang	1911060531
Lương Văn Xưởng	1911060329
Phạm Vũ Phi Long	1911066192
Lớp:	19DTHD1

TP. Hồ Chí Minh, 2022

LỜI NHẬN XÉT

.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....
.....

LỜI CẢM ƠN

Lời đầu tiên em xin gửi lời cảm ơn đến ThS. Tống Thanh Văn giáo viên hướng dẫn môn “Bảo mật thông tin”. Trong suốt thời gian thực hiện đồ án “Hacking mobile”, mặc dù rất bận rộn trong công việc nhưng thầy vẫn giành thời gian và tâm quyết trong việc hướng dẫn nhóm em. Luôn định hướng, góp ý và sửa chữa chỗ sai, thiếu sót giúp em hoàn thành tốt đề tài lần này.

Em cũng xin chân thành cảm ơn các thầy trong trường đã giảng dạy, và giúp đỡ em, thầy đã xây dựng cho chúng em những kiến thức nền tảng và kiến thức chuyên môn để em có thể hoàn thành đồ án này cũng như những thầy việc của mình sau này.

Em xin trân trọng cảm ơn!

LỜI CAM KẾT

Em xin cam đoan rằng đồ án môn học về đề tài "Hacking mobile" là đề tài nguyên cứu độc lập của nhóm em. Đồng thời những số liệu được tham khảo liên quan tới đồ án đa phần được ghi rõ nguồn gốc.

Nhóm em xin chịu hoàn toàn trách nhiệm trước nhà trường nếu bị phát hiện ra bất cứ sai phạm hay vấn đề sao chép nào trong đồ án.

MỤC LỤC

LỜI MỞ ĐẦU

Ngày nay, xu thế của xã hội đang chuyển dần sang lĩnh vực công nghệ di động nói chung và điện thoại di động nói riêng. Minh chứng có thể thấy rõ đó chính là sự ra đời của hai hệ điều hành điện thoại phổ biến ngày nay là Android và iOS. Tuy nhiên, hiện nay các điện thoại thông minh sử dụng hệ điều hành Android của Google vẫn có sức hút và gây sự chú ý hơn hẳn so với thế giới điện thoại thông minh còn lại. Android cung cấp một bộ đầy đủ các phần mềm cho các thiết bị di động.

Vì thế việc sử dụng một chiếc điện thoại thông minh để quản lý các công việc là vô cùng quan trọng, chúng có thể đồng bộ hóa nội dung từ thiết đến thiết bị khác một cách nhanh chóng và tiện lợi trong khi thiết kế chỉ nhỏ nhắn trong lòng bàn tay.

Tuy nhiên, sự tiện lợi đó cũng mang lại rất nhiều mặt trái, trong khi các thiết bị điện tử khác như máy tính có nhiều lớp bảo mật như tường lửa và thêm một vài ứng dụng bảo vệ và quét virus cài thêm trên máy. Giúp phát hiện các mã độc trong phần mềm hay ứng dụng thứ ba khi được cài vào máy, ngăn chặn một số thành phần đánh cắp thông tin trên máy. Tuy nhiên, các ứng dụng bảo vệ được làm riêng cho điện thoại hiện nay chưa được quá phổ biến, vì thế đây là môi trường còn đầy cơ hội để cho các hacker dùng các cách thức khác nhau như thông qua wifi, phần mềm thứ ba, tin nhắn,... để xâm nhập vào thiết bị của người dùng và đánh cắp thông tin hay thậm trí truy được vị trí của người dùng.

Nhóm em nhằm để biết được cách thức mà các bên thứ ba này dùng để biến các ứng dụng an toàn trở thành một phần mềm có thể theo dõi và đọc thông tin của người dùng, nên đã quyết định chọn đề tài “Hacking mobile”. Ngoài việc, chúng em có thể học hỏi được cách thức để truy cập vào một thiết bị mobi thông qua bên thứ ba, nó còn giúp tụi em biết cách hạn chế được việc cài các phần mềm độc hại này vào máy hay tìm ra các phần mềm đó có bị gắn mã độc hại nào vào không.

DANH MỤC HÌNH ẢNH

CHƯƠNG 1: TỔNG QUAN ĐỀ TÀI

1.1. Giới thiệu đề tài:

1.1.1. Khái niệm hacking mobile:

- Là hoạt động xác định các điểm yếu trong hệ thống điện thoại nhắm khai thác bảo mật để đạt được quyền truy cập vào dữ liệu cá nhân hoặc dữ liệu kinh doanh.

Ví dụ: sử dụng thuật toán để "bẻ khóa mật" của điện thoại từ đó xâm nhập để tìm thông tin cá nhân.

1.1.2. Thực trạng:

- Hiện nay việc tải các trò chơi lậu hay các bảng ứng dụng đã được crack trên mạng được xem là hành động đáng lên án ở các nước phát triển. Tuy nhiên ở các nước đang phát triển như Việt Nam thì việc này được nhìn qua một lăng kính khác, khi mà việc tải các bản lậu giúp người dùng có thể tiếp cận được với nhiều phiên bản khác nhau của ứng dụng hơn, hoặc các ứng dụng bị hạn chế truy cập ở khu vực của người dùng và tiết kiệm được một khoản cho ví tiền của họ.
- Về mặt lý thuyết thì việc crack một ứng dụng là việc thay đổi code bên trong ứng dụng đó, khiến nó bị thay đổi quyền, giới hạn truy cập các chức năng. Việc này dẫn tới một thực trạng là các đối tượng xấu có thể thêm các đoạn mã độc hoặc các tệp tin gián điệp giúp theo dõi vị trí và đọc thông tin của người dùng, khi người dùng tải các tệp tin này về máy.

1.1.3. Cách thức tấn công

- Sử dụng Kali Linux tạo ra một ứng dụng có chứa mã độc, chứa port và local host của máy làm hack, gửi ứng dụng có chứa mã độc và gửi cho các máy android khác. Thông qua ứng dụng được cài vào máy android, trong ứng dụng đó có mã độc bên thứ ba có thể dùng mã đó để xâm nhập vào hệ thống của người dùng qua đó đánh cắp các thông tin trong máy.

1.1.4. Tác hại:

- Hacker có thể đánh cắp dữ liệu từ máy của người dùng.

- Theo dõi người dùng thông qua việc truy cập vào định vị và camera trên máy của người dùng.
- Người dùng có thể bị các hacker dùng các thông tin cá nhân để tống tiền, hoặc gây khủng hoảng cho nạn nhân.
- Điện thoại có cài đặt phần mềm độc sẽ chạy chậm hẳn do tiêu hao năng lượng.

1.2. Mục tiêu đề tài:

- Cách sử dụng VMware.
- Cách sử dụng và vận hành Kali Linux.
- Cách thao tác các chức năng trên máy ảo của Android Studio.
- Cách tạo ra một ứng dụng có chứa mã độc bằng Kali Linux.
- Cách thức xâm nhập vào thiết bị của người dùng thông qua một ứng dụng khác.
- Cách lấy được thông tin của người dùng bằng ứng dụng đó.
- Cách tìm ra các phần mềm không an toàn trên máy và cách phòng bị trước các thành phần có ý đồ xấu.

1.3. Đối tượng nghiên cứu:

- Các máy điện thoại di động có hệ điều hành Android có Android 5.0 trở xuống.
- Tool sử dụng trong Kali Linux có thể xâm nhập vào điện thoại

1.4. Phạm vi nghiên cứu:

- Các loại điện thoại di động thuộc hệ điều hành Android.
- Các tool có thể tạo ra tệp độc xâm nhập vào máy điện thoại di động có hệ điều hành Android 1.0 - hiện nay.

CHƯƠNG 2: CƠ SỞ LÝ THUYẾT

2.1. Phần mềm ảo hóa VMware Workstation Player 16

- VMware Player hay tên đầy đủ là VMware Workstation Player là một phần mềm ảo hóa cho máy tính chạy trên kiến trúc 64-bit sử dụng hệ điều hành Windows hoặc Linux.
- VMware Player có thể chạy các máy ảo tạo sẵn cũng như tự tạo các máy ảo của riêng nó (yêu cầu cài đặt hệ điều hành để hoạt động). Nó sử dụng cùng một lõi ảo hóa như VMware Workstation Pro, nhưng là phiên bản rút gọn tính năng và tuyệt vời hơn là hoàn toàn miễn phí.
- Ưu và nhược điểm:
  + Ưu điểm:
    - Cung cấp giao diện trực quan để chạy các máy ảo có cấu hình sẵn được tạo bởi GSX Server, VMware Workstation…
    - Đối với máy chủ Windows, ứng dụng cũng có thể hoạt động đồng thời máy ảo Microsoft Virtual PC và Virtual Server.
    - Hỗ trợ người dùng truy cập mạng lưới công việc riêng mà không cần sử dụng sản phẩm của VMware. Như vậy, chỉ cần vài thao tác đơn giản như tải xuống và cài đặt, bất cứ ai cũng có thể khởi tạo cũng như chạy hệ thống máy ảo tương thích.
    - Đặc biệt, ứng dụng hiện nay đã có sẵn phiên bản tải sẵn miễn phí dành cho PC chạy hệ điều hành Windows và Linux. Tuy nhiên, trong quá trình sử dụng, người dùng cần tuân thủ áp dụng quy định của VMware đồng thời tận dụng tài liệu hướng dẫn để phát huy tối đa công năng của ứng dụng.
  + Nhược điểm:
    - Kết hợp bộ xử lý và bộ xử lý khách của máy ảo được bảo vệ bằng FT phải được hỗ trợ bởi Fault Tolerance. Vui lòng tham khảo trang web VMware cho sự kết hợp CPU và hệ điều hành khách được hỗ trợ
    - Phiên bản phần cứng máy ảo phải từ 7 trở lên

2.2. Nhà phân phối Linux (Kali Linux):

- Kali Linux là một bản phân phối Linux dựa trên Debian. Mục tiêu của nó đơn giản là: tập hợp nhiều công cụ kiểm tra bảo mật và thâm nhập tốt nhất có thể trong một môi trường hệ điều hành. Kali Linux được sinh ra với mục đích như vậy nên bạn có thể tìm thấy nhanh gọn nhiều công cụ mã nguồn mở để thực hiện các quy trình kiểm thử (pentest), tấn công, hacking,...tiết kiệm thời gian.

- Kali Linux là một bản phân phối Linux được phát triển và duy trì bởi Offensive Security khi được tổ chức này phát hành vào tháng 3 năm 2013. Là sự thay thế phát triển cho hệ điều hành BackTrack. Offensive Security là một tổ chức nổi tiếng và đáng tin cậy trong thế giới bảo mật, thậm chí chứng nhận các chuyên gia bảo mật với một số chứng chỉ được xem trọng nhất hiện có như: OCSP, OSCE, OSWP, OSEE. Kali Linux là một hệ điều hành được sử dụng nhiều trong lĩnh vực bảo mật, bởi cả những hacker tìm cách xâm nhập hệ thống và những chuyên gia về bảo mật muốn bảo vệ các tài nguyên thông tin. Kali Linux cung cấp rất nhiều công cụ cho những tác vụ liên quan đến bảo mật.

- Ưu và nhược điểm

  + Ưu điểm:

    - Có hơn 600 công cụ kiểm tra thâm nhập được cài đặt sẵn.
    - Mã nguồn mở, hoàn toàn miễn phí sử dụng.
    - Hỗ trợ nhiều ngôn ngữ.
    - Khả năng tùy chỉnh 100%

  + Nhược điểm:

    - Kali Linux dễ bị sử dụng sai mục đích
    - Định hướng của Kali Linux là dành cho các chuyên gia, Không phải những người làm quen với Linux có định hướng sai.
    - Không có sẵn các cấu hình bảo mật và các cấu hình khác cho người dùng bình thường.
    - Một số phần mềm bên trong có thể hoạt động sai cách, bị chậm.

2.3. Máy ảo giả lập điện thoại Android (Android Studio)

- Là một công cụ tích hợp (IDE) của Google dùng để phát triển các ứng dụng chạy trên các thiết bị sử dụng hệ điều hành Android. Được xây dựng dựa trên

mã nguồn của IntelliJ, sử dụng ngôn ngữ lập trình Kotlin của JetBrains thay thế cho Java, tuy nhiên Java và C++ vẫn được hỗ trợ để phát triển ứng dụng Android. Cài đặt được trên các hệ thống máy tính Windows, mac OS và Linux. Android Studio được Google tích hợp tất cả các công cụ hỗ trợ như SDK (Software Development Kit), máy ảo giả lập thiết bị di động ngay trên máy tính, UX/UI Android,...

- Ưu và nhược điểm:
  + Ưu điểm:
    - Được phát triển bởi chính Google, cũng là chủ sở hữu hệ điều hành Android.
    - Các gói công cụ hỗ trợ được cập nhật đầy đủ và mới nhất.
    - Giao diện và tính năng dễ làm quen và sử dụng của nó là một điểm cộng lớn.
    - Tài liệu tham khảo và hướng dẫn rõ ràng và đầy đủ trên trang chủ, cũng như và có vô số diễn đàn dành cho các lập trình viên Android.
  + Nhược điểm:
    - Vì nó là bộ công cụ tích hợp tất cả, nên nó buộc phải tải toàn bộ những dữ liệu hỗ trợ cho việc phát triển ứng dụng tối ưu nhất. Đó là lượng dữ liệu lớn chiếm dụng không ít không gian bộ nhớ lưu trữ máy tính của bạn.
    - Android Studio là một phần mềm phát triển ứng dụng mà ở đó bạn có thể kiểm tra cách hoạt động của app ngay trên máy tính thông qua trình giả lập của Android Studio. Và nó chính là nguyên nhân gây đơ máy lag, nóng hay hao pin trên laptop.

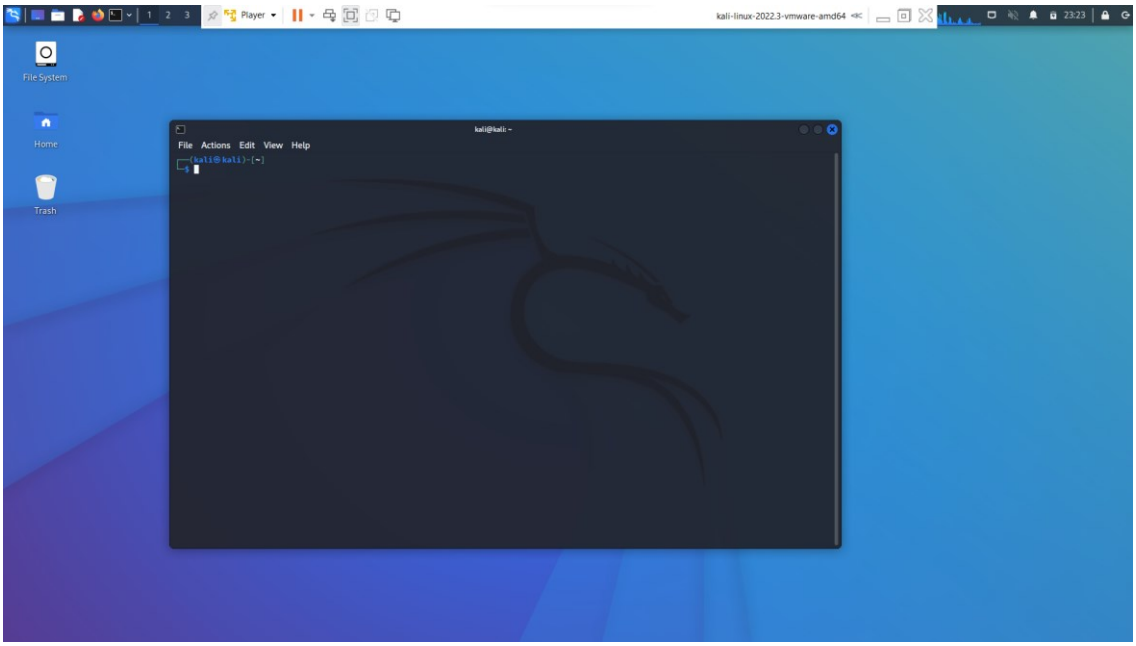
CHƯƠNG 3: CƠ SỞ THỰC NGHIỆM

3.1. Cách thức thực nghiệm

3.1.1. Các bước chuẩn bị cho thực nghiệm:

- Thao tác chuẩn bị bên Kali Linux.

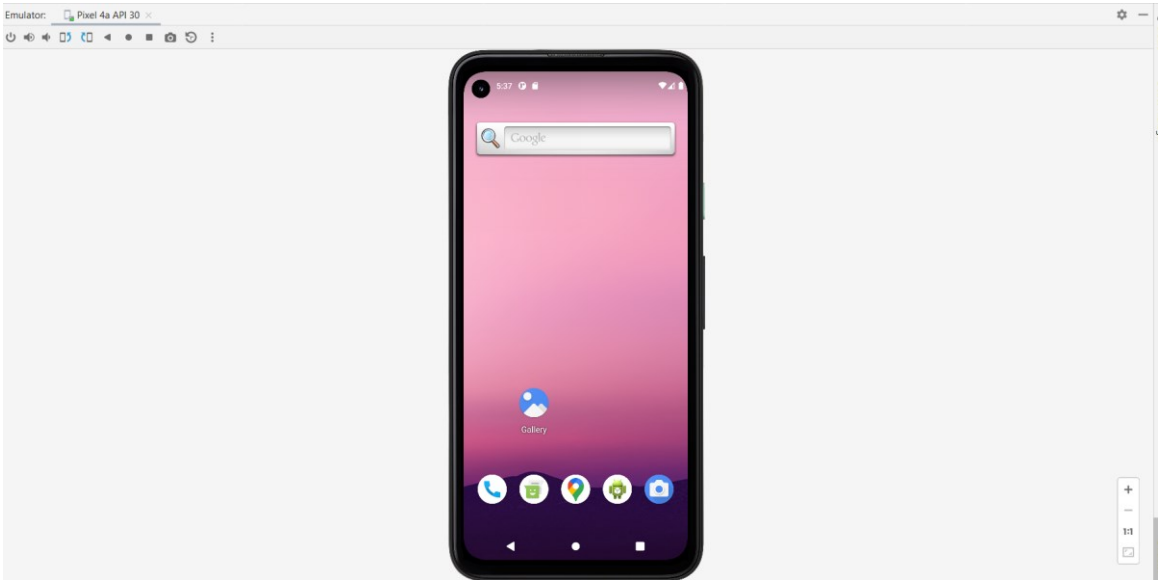
  + Máy ảo Kali Linux thuộc bản 2022.3 chạy trên VMware.



Hình 1: Giao diện của phần mềm Kali Linux chạy trên Vmware

- Thao tác chuẩn bị máy ảo trên Android Studio:

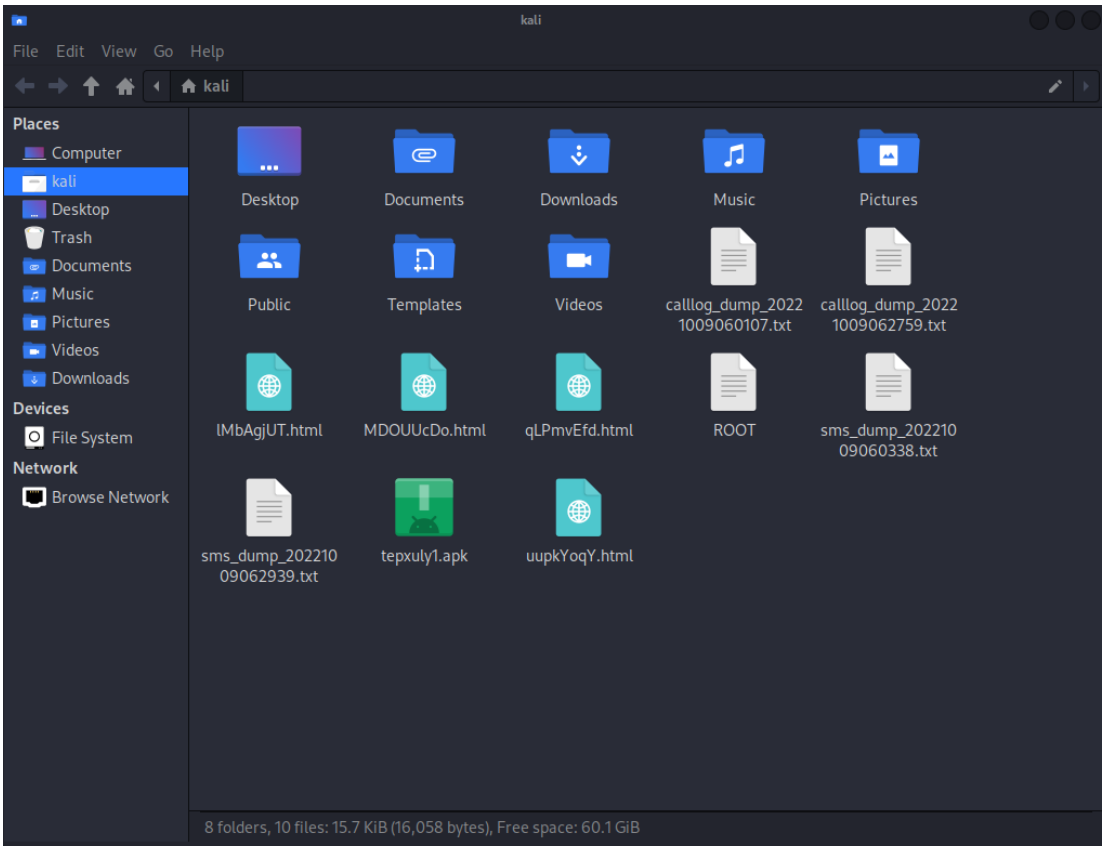
Hệ điều hành	Android 4.0
Ram	1536 MB
VM heap	256 MB
Internal Storage	6144 MB
SD card	512 MB



Hình 2: Giao diện điện thoại giả lập Android Studio

3.1.2. Các bước thực hiện:

Bước 1: Tạo phần mềm có chứa tệp độc bằng Kali Linux.



Hình 3: Giao diện trên Kali Linux tạo ra tepxuly1.apk

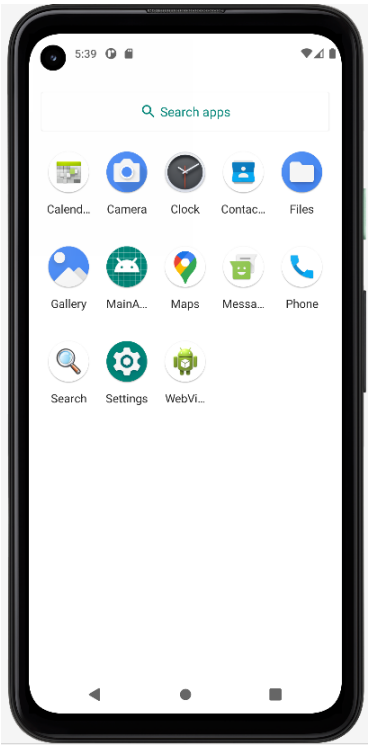
- Dùng Kali Linux tạo ra phần mềm có chứa tệp độc có tên là tepxuly1.apk có:

+ Localhost là địa chỉ ip của máy ảo: 192.168.81.128.

+ Port: 4444 .

+ Nơi lưu trữ tệp trên máy là ở màn hình chính.

Bước 2: Cài tệp độc vào máy ảo Android được chuẩn bị:



Hình 4: Giao diện trên điện thoại Android có chứa tepxuly1.apk.

- Bạn làm nhiều cách khác nhau để có thể đưa phần mềm chứa tệp độc vào điện thoại android và khi đã được cài thì ứng dụng chứa tệp độc có tên là MainActivity.

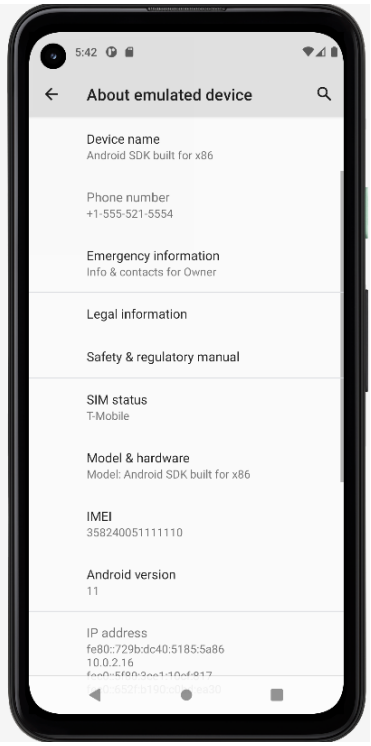
Bước 3: Sử dụng giao diện Kali Linux để xâm nhập vào máy ảo qua bên ứng dụng mới cài đặt.

Sau khi đã có máy android cài đặt ứng dụng đó thì bạn vào Command Line của Kali để bắt đầu connect vào máy android có phần mềm chứa tệp độc.

Bước 4: Lấy thông tin của người dùng:

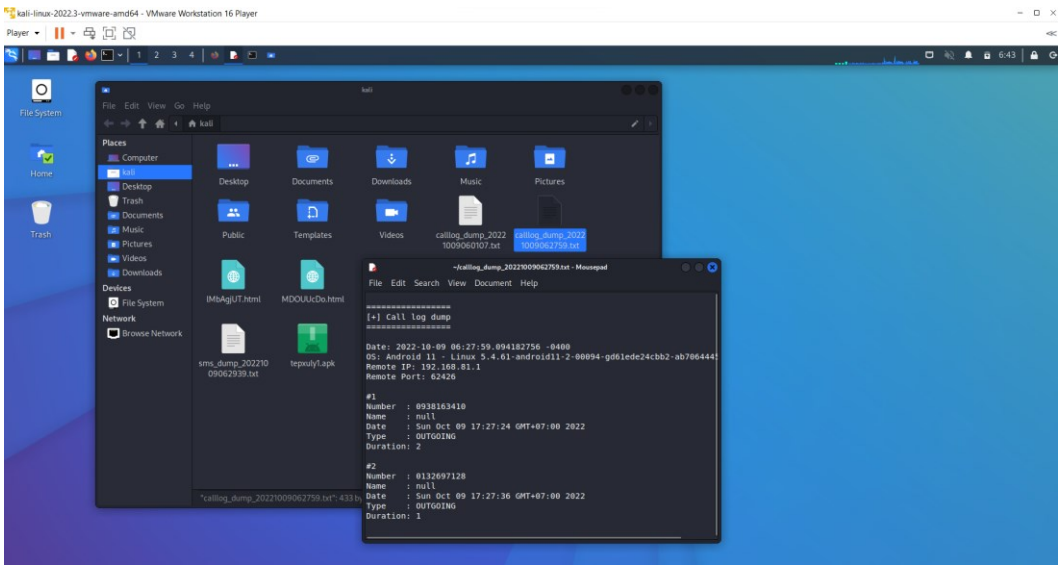
- Lấy thông tin thiết bị:

+ Xem thông tin dòng máy.
+ Kích thước RAM.
+ Hệ điều hành.
+ Số điện thoại của máy.



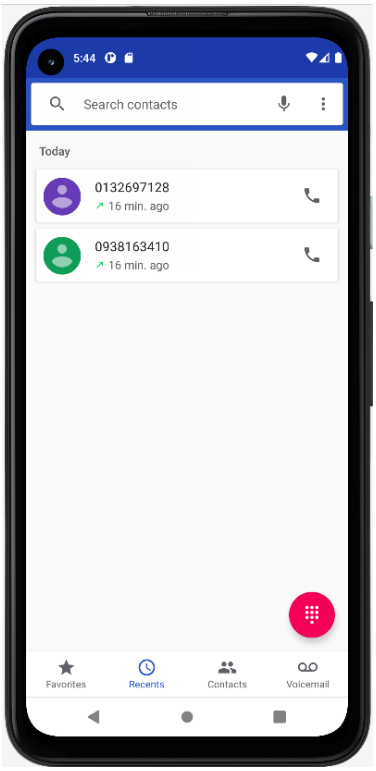
Hình 5: Giao diện thông số thiết bị của Android

- Kiểm tra root: Ta có thể xem điện thoại android đó đã root hay chưa.
- Kiểm tra cuộc gọi thoại:



Hình 6: Danh sách các cuộc gọi trên Android mà Kali khai thác.

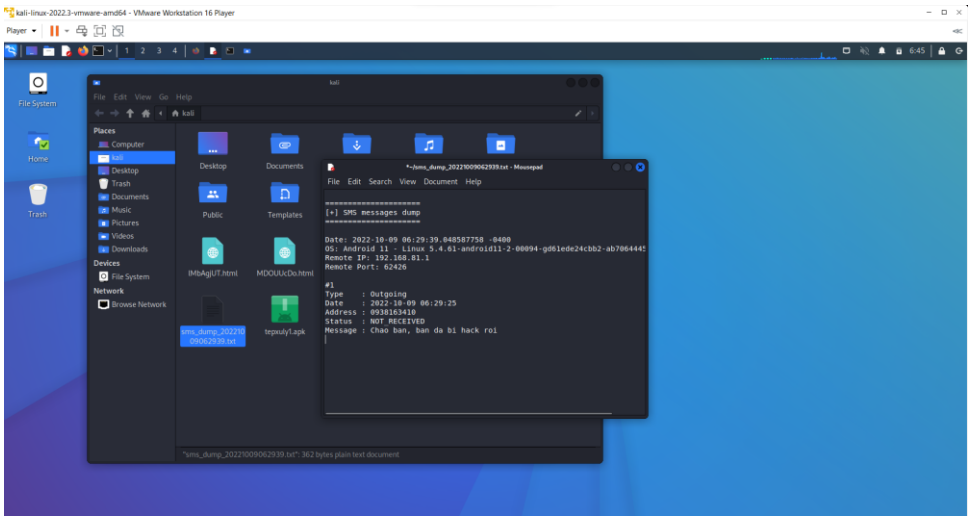
+ Tại máy chủ Kali ta dùng câu lệnh trong Command Line để có thể tạo ra danh sách những cuộc gọi mà điện thoại chứa mã độc đã gọi trước đó. Như trên hình có 2 số điện thoại sau khi dùng command line để xem.



Hình 7: Danh sách cuộc gọi trên Android

+ Đây là 2 số điện thoại mà chủ của máy android đã gọi trước đó mà máy Kali có thể khai thác và xem thông tin.

- Kiểm tra tin nhắn:



Hình 8: Danh sách và nội dung tin nhắn bị khai thác bởi Kali.

+ Sau khi đã khai thác được cuộc gọi trước đó, ta có thể tiếp tục khai thác thêm tin nhắn của chủ điện thoại di động để có thể thuận lợi cho mục đích khác. Khi dùng lệnh trong Command Line thì sẽ xuất hiện danh sách các tin nhắn đã gửi đi trong thời gian trước đó của chủ điện thoại Android. Như trên hình người sử dụng điện thoại trước đó có 1 dòng tin nhắn tới 1 số điện thoại có nội dung: "Chao ban, ban da bi hack".

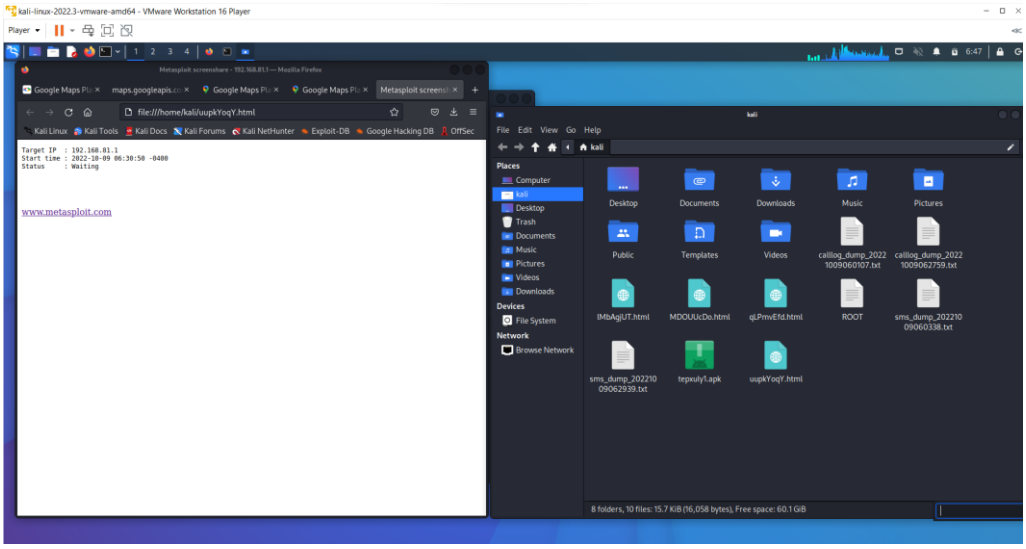
Hình 9: Danh sách tin nhắn và nội dung của máy Android

+ Đây là danh sách và nội dung mà người sử dụng điện thoại Android trước đó đã nhắn.

- Kiểm tra danh sách webcam

+ Ta có thể kiểm tra danh sách webcam bằng Command Line.

+ Điều khiển webcam stream trực tiếp.



Hình 10: Giao diện máy Android bị máy Kali điều khiển LiveStream

+ Ta có thể điều khiển máy điện thoại livestream trực tiếp trên mạng xã hội mà người chủ điện thoại không hay biết. Và sẽ xuất hiện 1 tệp web có link stream.

3.2. Cách thức phòng chống:

- Luôn cập nhật các phiên bản mới của hệ điều hành kể cả cập nhật ứng dụng: mỗi lần phiên bản mới hay bản vá lỗi được làm ra không phải để làm máy bạn ngày càng yếu với hư hỏng mà là để nâng cấp bảo mật, sửa các lỗ hỏng của hệ điều hành cũ để tránh các hacker xâm nhập.

- Cẩn thận với những gì bản thân cài đặt: Mỗi lần tải một ứng dụng nào đó thì thường có thông báo cho ứng dụng đó truy cập vào máy ảnh, danh bạ… đối với một số phần mềm có bảo mật tốt, đối với các phần mềm bản thân không rành có thể bị lạm dụng.

- Thường xuyên xem lại các ứng dụng có trên điện thoại: phải luôn xem kỹ các phần mềm đã cài trên máy kể cả bản cập nhật, phần mềm theo dõi thứ ba

có thể xuất hiện trong máy mà bạn không biết dựa vào việc cập nhật phần mềm có sẵn trên điện thoại.

- Làm kẻ gian khó xâm nhập: Hãy cảnh giác các tính năng mở khóa thông minh, nó thường hay tự động sử dụng mở khóa điện thoại khi bạn ở gần.
- Cảnh giác với wifi miễn phí: hiện trạng hiện nay wifi rất phổ biến và đặc biệt nơi công cộng lại không có mật khẩu hãy cẩn thận nếu bạn truy cập wifi công cộng vì tại đây hacker có thể xâm nhập vào wifi và tiến vào xâm nhập máy tính bạn.
- Sử dụng bảo mật từng ứng dụng: nếu có thể hãy khóa mật khẩu từng ứng dụng quan trọng trên điện thoại để có thể bảo mật 2 lớp.
- Nhận một cảnh báo khi điện thoại mất kết nối Bluetooth: nếu bạn đang ở hàng rào về đầu tư vào một smartwatch, đây là một tính năng ít được biết đến có thể xoay nó: Các thiết bị Apple Watch và Android Wear có thể cảnh báo bạn ngay lập tức nếu mất liên lạc Bluetooth với điện thoại của bạn. Nếu bạn nhận được thông báo này khi đang ở nơi công cộng, có một cơ hội tốt để ai đó chỉ cần nhặt túi của bạn và hiện đang đánh cắp điện thoại của bạn.

CHƯƠNG 4: TỔNG QUAN VÀ ĐÁNH GIÁ

4.1. Nhiệm vụ đạt được:

- Hiểu được giao thức tạo mã độc bằng Kali Linux.
- Chạy và cài đặt thành công phần mềm độc trên điện thoại Android
- Sử dụng mã độc để xâm nhập vào điện thoại.
- Tìm kiếm thông tin của người dùng.

4.2. Cách khắc phục lỗi hiện tại:

- Khắc phục các cách đưa file xâm nhập.
- Có thể coi được nhiều chức năng hơn.
- Chạy một lúc nhiều máy.

4.3. Hướng phát triển:

- Phát triển trên điện thoại thật.
- Tự động sao chép mật khẩu, tất cả thông tin của người dùng khi sửa đổi.

TÀI LIỆU THAM KHẢO

[1]. Blog Tiền Điện Tử.Cách hack điện thoại di động bằng Kali Linux, 17/06/2022. https://blogtiendientu.vn/hack-dien-thoai-qua-kali-linux/

[2]. Bizfly Cloud. VMware WorkStation Player 16 là gì ?, 06/08/2021. https://bizflycloud.vn/tin-tuc/vmware-player-la-gi-20210806032051561.htm.

[3]. Quách Chí Cường. Kali Linux là gì ? Giới thiệu Hệ Điều Hành Kali Linux, https://cuongquach.com/kali-linux-la-gi-gioi-thieu-he-dieu-hanh-kali-linux.html

[4]. Chang Nguyen, Android Studio là gì ?, 29/01/2021. https://ghiencongnghe.info/android-studio-la-gi.html

[5]. Những cách phòng chống hack cho điện thoại thông minh của bạn ?, 28/11/2017. https://24hstore.vn/cong-nghe/12-cach-de-chong-hack-cho-dien-thoai-thong-minh-cua-ban-n254