KHOA KỸ THUẬT VÀ CÔNG NGHỆ
BỘ MÔN CÔNG NGHỆ THÔNG TIN

THỰC TẬP ĐỒ ÁN CHUYÊN NGÀNH
HỌC KỲ VII, NĂM HỌC 2023-2024

NGHIÊN CỨU VÀ ỨNG DỤNG HACKING MOBILE DEVICES

Giáo viên hướng dẫn:
Nguyễn Bá Nhiệm

Sinh viên thực hiện:
Họ tên: Lê Minh Hận
MSSV: 110120027
Lớp: DA20TTA

Trà Vinh, tháng 12 năm 2023

KHOA KỸ THUẬT VÀ CÔNG NGHỆ
BỘ MÔN CÔNG NGHỆ THÔNG TIN

THỰC TẬP ĐỒ ÁN CHUYÊN NGÀNH
HỌC KỲ VII, NĂM HỌC 2023-2024

NGHIÊN CỨU VÀ ỨNG DỤNG HACKING MOBILE DEVICES

Giáo viên hướng dẫn:
Nguyễn Bá Nhiệm

Sinh viên thực hiện:
Họ tên: Lê Minh Hận
MSSV: 110120027
Lớp: DA20TTA

Trà Vinh, tháng 12 năm 2023

NHẬN XÉT CỦA GIÁO VIÊN HƯỚNG DẪN

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

Trà Vinh, ngày ..... tháng …… năm ……

Giáo viên hướng dẫn

(Ký tên và ghi rõ họ tên)

NHẬN XÉT CỦA THÀNH VIÊN HỘI ĐỒNG

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

Trà Vinh, ngày ..... tháng …… năm ……

Thành viên hội đồng

(Ký tên và ghi rõ họ tên)

LỜI CẢM ƠN

Muốn đi nhanh thì đi một mình, muốn thành công thì cần có người đi trước giúp đỡ. Nhân đây, tôi xin chân thành cám ơn thầy **Nguyễn Bá Nhiệm** giúp đỡ tôi trong quá trình nghiên cứu tài liệu, giải đáp kịp thời những những khó khăn trong quá trình thực hiện đề tài. Đồng thời, tôi cũng xin cám ơn anh chị khóa trên, bạn đã hỗ trợ tôi.

Một lần nữa, tôi xin chân thành cảm ơn !

MỤC LỤC

Trang

DANH MỤC HÌNH ẢNH – BẢNG BIỂU

Trang

MỞ ĐẦU

1. Lý do chọn đề tài

Xã hội hiện nay là một xã hội rất hiện đại, và theo Statista – một nền tảng trực tuyến của Đức chuyên thu thập và trực quan hóa dữ liệu, thì tại Việt Nam có khoảng 61,3 triệu smartphone đang được sử dụng và nằm ở vị trí thứ 10 với trong top 10 quốc gia có số lượng smartphone cao nhất, cụ thể Việt Nam xếp sau Trung Quốc, Ấn Độ, Mỹ, In-do-ne-si-a, Brazil, Nga, Nhật Bản, Mê-xi-cô, Đức. Nói như vậy để thấy, thị trường smartphone ở Việt Nam không cũng nhộn nhịp không kém cạnh các quốc gia khác trên thế giới.

Smartphone hiện tại không còn chỉ dừng lại ở chức năng nghe gọi và nhắn tin nữa, mà ngày nay, điện thoại thông minh còn giúp người dùng lưu trữ những thông tin, tài liệu quan trọng. Bởi vì đặc trưng của smartpone là nhỏ gọn, thuận tiện cho việc mang đi nhiều nơi, đây là điểm tối ưu có smartphone so với việc lưu trữ tài liệu trên máy tính.

Nhưng việc lưu trữ thông tin trên smartphone cũng tồn tại nhiều rủi ro tiềm tàn, một trong số đó là việc những thông tin quan trọng được lưu trong smartphone có thể bị đánh cắp bởi những hacker vì họ có thể lợi dụng những lỗ hỏng của hệ điều hành để xâm nhập vài điện thoại của chúng ta. Đó là lí do tôi chọn đề tài "Nghiên cứu và ứng dụng hacking mobile devices" này.

2. Mục đích

Mục đích tôi viết bài báo cáo này là để mọi người có thể hiểu hơn về khái niệm lỗ hổng của hệ điều hành, những tác hại mà nó mang đến, cũng như là những biện pháp nhằm hạn chế nguy cơ thiết bị di động bị tấn công.

3. Đối tượng nghiên cứu

Đối tượng nghiên cứu của bài báo cáo này là các cuộc tấn công thiết bị di động. Đề tài này tập trung nghiên cứu các phương thức, kỹ thuật, và các biện pháp bảo vệ thiết bị di động khỏi nguy cơ bị tấn công.

4. Phạm vi nghiên cứu

Phạm vi nghiên cứu của tấn công thiết bị di động bao gồm các khía cạnh sau:

Các phương thức tấn công thiết bị di động: Phương thức tấn công thiết bị di động là các cách thức mà kẻ tấn công có thể xâm nhập vào thiết bị di động

của nạn nhân. Các phương thức tấn công này có thể được phân loại thành các nhóm chính sau:

+ Tấn công phần mềm độc hại

+ Tấn công mạng.

+ Tấn công vật lý.

Các kỹ thuật tấn công thiết bị di động: Kỹ thuật tấn công thiết bị di động là các phương pháp mà kẻ tấn công sử dụng để thực hiện các cuộc tấn công. Các kỹ thuật tấn công này có thể được phân loại thành các nhóm chính sau:

+ Khai thác lỗ hổng

+ Cài đặt phần mềm độc hại

+ Trộm cắp thông tin

+ Tấn công từ chối dịch vụ (DoS/DDoS)

Các biện pháp bảo vệ thiết bị di động: Để bảo vệ thiết bị di động khỏi các cuộc tấn công, người dùng cần thực hiện các biện pháp sau:

+ Cài đặt phần mềm bảo mật

+ Cập nhật hệ điều hành và ứng dụng

+ Cẩn thận khi tải xuống ứng dụng

+ Sử dụng mật khẩu mạnh

+ Kích hoạt xác thực hai yếu tố (2FA)

CHƯƠNG 1: TỔNG QUAN

Khi lưu trữ thông tin bằng điện thoại thông minh, thì một trong những vấn đề được quan tâm nhiều nhất đó là sự an toàn. Bởi vì hiện nay, có rất nhiều trường hợp hacker xâm nhập để lấy thông tin nhằm mục đích phi pháp mà nạn nhân thường là những người nổi tiếng, hoặc là người có ảnh hưởng trong và ngoài nước, điển hình là vụ điện thoại của nữ diễn viên Scarlett Johansson bị hacker tấn công và bị tung những tấm ảnh nhạy cảm của cô ấy lên mạng. Nếu như trước đây những kẻ xâm nhập lợi dụng việc truy cập vào những đường dẫn có chứa mã độc để tiến hành tấn công, thì giờ đây, thông qua các phần mềm chứa mã độc, thông qua những lỗ hổng bảo mật hoặc là thông qua các kết nối với mạng Wi-Fi hoặc Bluetooth không an toàn cũng có thể tạo cơ hội để hacker tấn công.

Vì thế, sau khi nghiên cứu đề tài này, tôi hi vọng bài báo cáo này có thể giúp mọi người nhận biết được cách thức hacker tấn công, tầm quan trọng của việc cập nhật phiên bản mới cho hệ điều hành cũng như biết được một cuộc tấn công của tin tặc vào thiết bị di động diễn ra như thế nào.

CHƯƠNG 2: NGHIÊN CỨU LÝ THUYẾT

2.1 Tổng quan về hệ điều hành

2.1.1 Khái niệm về hệ điều hành

Hệ điều hành (Operating System hay OS) là phần mềm hệ thống, được dùng để quản lý tài nguyên phần cứng và phần mềm và cung cấp các dịch vụ cho các chương trình máy tính.

Hệ điều hành đóng vai trò như trung gian giữ người dùng và phần cứng của máy tính, giúp người dùng tương tác thuận tiện và dễ dàng hơn.

Hiện tại có rất nhiều hệ điều hành được các công ty công nghệ cho ra mắt, nhưng chung quy thì có thể phân các hệ điều hành này thành ba loại là:

+ Hệ điều hành cho máy tính: Windows, macOS, Linux,…

+ Hệ điều hành cho di động: Android, IOS, Windows Phone,..

+ Hệ điều hành nhúng: Được sử dụng trong các thiết bị điện tử như TV, máy tính bảng, ….

2.1.2 Chức năng của hệ điều hành

Chức năng quản lý tài nguyên phần cứng: Hệ điều hành quản lý các tài nguyên phần cứng của máy tính, bao gồm: Bộ nhớ, CPU, thiết bị vào/ra,… Hệ điều hành giúp các tài nguyên hoạt động trơn tru với nhau mà không bị xung đột.

Chức năng cung cấp giao việc cho người dùng: Hệ điều hành cung cấp giao diện để người dùng có thể tương tác với máy tính. Giao diện người dùng có thể là giao diện dòng lệnh (CLI) hoặc là giao diện đồ họa người dùng (GUI).

Chức năng quản lý các chương trình ứng dụng: Hệ điều hành sẽ quản lý các ứng dụng đang chạy trên máy tính. Hệ điều hành có vai trò đảm bảo các chương trình được thực thi an toàn và hiệu quả.

Chức năng cung cấp dịch vụ chung: Hệ điều hành cung cấp các dịch vụ chung cú chương trình ứng dụng, chẳng hạn như quản lý tệp tin, quản lí in ấn,… [1] [2]

2.2 Tổng quan về hệ điều hành di động

2.2.1 *Khái niệm hệ điều hành di động*

Hệ điều hành di động là hệ điều hành dành cho các thiết bị di động như điện thoại, máy tính bảng, đồng hồ thông minh, … Hiện tại, khi nhắc đến hệ điều hành dành cho các thiết bị di động, không khó để nghĩ đến hai cái tên nổi bật hơn tất cả là Android và IOS, hai hệ điều hành này có những ưu nhược điểm và khả năng bảo mật khác nhau. [2]

2.2.2 Tổng quan về hệ điều hành Android, IOS

2.2.2.1 Giới thiệu về hệ điều hành Android

Hệ điều hành Android là một hệ điều hành được phát triện lấy hệ điều hành Linux làm nền tảng, Android được thiết kế dành cho các thiết bị di động có màn hình cảm ứng như điện thoại thông minh và máy tính bảng. Theo thống kê của StatCounter, Android hiện là hệ điều hành phổ biết nhất trên thế giới và vào tháng 8 năm 2023, Android chiếm 75,74% thị phần điện thoại thông minh toàn cầu.

Tính năng: Hệ điều hành Android có rất nhiều tính năng, dưới đây làm một số tính năng tiêu biểu:

+ Hệ điều hành Android là hệ điều hành nguồn mở, tức là cho phép các nhà sản xuất thiết bị và nhà phát triển ứng dụng tự do tùy chỉnh và phát triển các tính năng mới.

+ Giao diện người dùng trực quan, dễ sử dụng.

+ Hỗ trợ đa nhiệm, cho phép người dùng chạy nhiều ứng dụng cùng một lúc.

+ Kho ứng dụng khổng lồ với hàng triệu ứng dụng miễn phí và trả phí.

+ Hỗ trợ các tính năng tiên tiến như nhận dạng khuôn mặt, nhận dạng vân tay, thanh toán di động,...

Ưu điểm của Android:

+ Đa dạng thiết bị: Android được hỗ trợ trên nhiều loại thiết bị khác nhau, từ điện thoại thông minh giá rẻ đến máy tính bảng cao cấp.

+ Mở rộng: Android cho phép các nhà sản xuất thiết bị và nhà phát triển ứng dụng tùy chỉnh và phát triển các tính năng mới.

+ Miễn phí: Android là một hệ điều hành nguồn mở, miễn phí cho các nhà sản xuất thiết bị sử dụng.

Nhược điểm của Android:

+ Bảo mật: Android có thể dễ bị tấn công bảo mật hơn các hệ điều hành khác.

+ Tương thích: Android có thể không tương thích với tất cả các ứng dụng và dịch vụ.

Kết luận:

Nhìn chung, hệ điều hành Android là một hệ điều hành mạnh mẽ và tương đối linh hoạt vì có thể sử dụng trên nhiều loại thiết bị di động khác nhau. Android cũng có nhiều ưu điểm đáng chú ý như đa dạng thiết bị, mở rộng và miễn phí, tuy nhiên Android cũng nhược điểm lại là khả năng tương thích và vấn đề bảo mật. [3]

2.2.2.2 Giới thiệu về hệ điều hành IOS

Hệ điều hành IOS là một hệ điều hành được Apple Inc phát triển, được dùng cho các sản phẩm của Apple như: iPhone, iPad, Apple Watch,…. Hệ điều hành IOS dùng Unix làm nền tảng để phát triển và phát triển để chạy trên các thiệt bị có màn hình cảm ứng. Theo StatCounter, vào tháng 8 năm 2023 thì thị phần điện thoại thông minh sử dụng hệ điều hành IOS chiếm 20.26% toàn cầu.

Tính năng: Là một hệ điều hành được ưa chuộng thứ hai trên thế giới, IOS có rất nhiều tính năng nổi bật, chẳng hạn như:

+ IOS có giao diện người dùng trực quan, dễ sử dụng.

+ Có hỗ trợ đa nhiệm, cho phép người dùng chạy nhiều ứng dụng cùng một lúc.

+ Có một kho ứng dụng khổng lồ với hàng triệu ứng dụng miễn phí và trả phí.

+ Có hỗ trợ các tính năng như nhận dạng khuôn mặt, nhận dạng vân tay, thanh toán di động,...

Ưu điểm: Tuy chỉ đứng thứ hai về mức độ phổ biến, nhưng hệ điều hành IOS vẫn có những ưu điểm nổi trội hơn hệ điều hành Android, chẳng hạn chư:

+ Hiệu suất ổn định: IOS được tối ưu hóa cho các thiết bị của Apple, mang lại hiệu suất ổn định và mượt mà.

+ Bảo mật cao: Nếu so về mức độ bảo mật thì IOS hơn hẳn Android vì Apple rất chú trọng vấn đề bảo mật, với nhiều tính năng và biện pháp bảo vệ người dùng.

+ Tương thích: IOS tương thích với tất cả các ứng dụng và dịch vụ của Apple.

Nhược điểm: Tuy nhiên, IOS vẫn có hai nhược điểm dễ thấy, thứ nhất là giá thành vì nếu so về giá thành thì các thiết bị sử dụng Android sẽ phù hợp với túi tiền hơn là các thiết sử dụng IOS, thứ hai là tính linh hoạt vì không như Android, IOS rất hạn chế việc người dùng có thể tùy chỉnh tính năng của hệ điều hành.

Kết luận: Nói một cách công bằng thì cả IOS và Android đều có những ưu - nhược điểm riêng biệt, người dùng có thể cân nhắc các tính năng và nhu cầu sử dụng để chọn hệ điều hành cho phù hợp. [4]

2.3 Lỗ hổng trong hệ điều hành

2.3.1 Khái niệm lỗ hổng và nguyên nhân xuất hiện

Khái niệm: Lỗ hổng trong hệ điều hành được hiểu là những sai sót hoặc là những thiếu sót trong bộ mã nguồn của hệ điều hành.

Nguyên nhân:

Lỗ hổng trong hệ điều hành có thể xuất hiện do nhiều nguyên nhân, chẳng hạn như:

+ Do lỗi lập trình: Đây là nguyên nhân phổ biến nhất gây ra lỗ hổng trong hệ điều hành, lỗi lập trình có thể xuất phát từ việc các lập trình viên không cẩn thận, hoặc là do các tác nhân bên ngoài ảnh hưởng trực tiếp hoặc gián tiếp đến bộ mã nguồn, có thể là do virus, phần mềm độc hại,…

+ Do tính phức tạp của hệ điều hành: Hệ điều hành được phát triển với hàng triệu dòng mã nên việc kiểm tra và phát hiện tất cả lỗi sẽ gặp khó khăn. [1]

2.3.2 Các hành vi của tin tặc

Một số hành vi thường thấy của tin tặc khi hệ điều hành xuất hiện lỗ hổng:

+ Tin tặc có thể chiếm quyền điều khiển hệ thống thông qua lỗ hổng, từ đó có thể truy cập và kiểm soát tất cả các dữ liệu và tài nguyên trong hệ thống.

+ Tin tặc có thể tải mã độc vào thiết bị bằng lỗ hổng này, từ đó tin tặc có thể kiểm soát hệ thống hoặc đánh cắp dữ liệu.

+ Tin tặc có thể khiến hệ thống không thể truy cập được bằng cách sử dụng lỗ hổng để tấn công từ chối dịch vụ (DDoS).

2.3.3 Một số loại lỗ hổng

Lỗ hổng có rất nhiều loại, tôi sẽ trình bày một vài loại lỗ hổng thường gặp sau đây:

+ Lỗ hổng thực thi mã từ xa (RCE cho phép tin tặc có thể thực thi các mã độc trên hệ thống từ xa.

+ Lỗ hổng leo thang đặc quyền là lỗ hổng cho phép tin tặc chiếm quyền điều khiển hệ thống với các đặc quyền cao hơn.

+ Lỗ hổng vượt qua xác thực là kiểu lỗ hổng mà tin tặc có thể truy cập vào các tài nguyên hoặc thông tin mà họ không được phép truy cập.

+ Lỗ hổng tràn bộ đệm là lỗ hổng xảy ra khi dữ liệu được ghi vượt quá dung lượng của bộ đệm. Điều này có thể dẫn đến các vấn đề bảo mật, chẳng hạn như RCE hoặc leo thang đặc quyền. [4]

2.3.4 Biện pháp hạn chế sự xuất hiện của lỗ hổng

+ Cài đặt các bản cập nhật hệ điều hành mới nhất: Các bản cập nhật hệ điều hành thường bao gồm các bản vá bảo mật để khắc phục các lỗ hổng đã biết.

+ Sử dụng phần mềm diệt virus và phần mềm chống phần mềm độc hại: Phần mềm diệt virus và phần mềm chống phần mềm độc hại có thể giúp phát hiện và loại bỏ các tác nhân bên ngoài có thể gây ra lỗ hổng trong hệ điều hành.

+ Sử dụng các biện pháp bảo mật cơ bản: Các biện pháp bảo mật như sử dụng mật khẩu mạnh, thay đổi mật khẩu thường xuyên,... cũng có thể giúp bảo vệ hệ thống khỏi các lỗ hổng trong hệ điều hành.

2.4 Tổng quan về tấn công thiết bị di động

2.4.1 Khái niệm về tấn công thiết bị di động

Tấn công thiết bị di động được hiểu là các hành vi độc hại được các tin tặc thực hiện nhằm mục đích tấn công, xâm phạm, chiếm quyền kiểm soát các thiết bị di động hoặc là đánh cắp các dữ liệu quan trọng có trong thiết bị di động.

2.4.2 Phương pháp tấn công

Có nhiều phương pháp được các tin tặc sử dụng để xâm nhập một thiết bị di động, chẳng hạn như:

+ Thiết bị có thể dính mã độc hoặc phần mềm theo dõi nếu người dùng cài đặt những ứng dụng có nguồn gốc không rõ ràng, tin tặc có thể từ những mã độc này mà tiến hành tấn công thiết bị để đánh cắp dữ liệu, chiếm quyền điều khiển thiết bị, v.v.

+ Các lỗ hổng xuất hiện trong hệ điều hành cũng có thể bị tin tặc khai thác để chiếm quyền điều khiển thiết bị.

+ Các ứng dụng hệ thống là các ứng dụng quan trọng được cài đặt sẵn trên thiết bị di động. Các lỗ hổng trong các ứng dụng này có thể bị tin tặc khai thác để chiếm quyền điều khiển thiết bị.

+ Các cuộc tấn công mạng, chẳng hạn như tấn công từ chối dịch vụ (DDoS), tấn công lừa đảo (phishing), v.v. cũng có thể được sử dụng để tấn công thiết bị di động.

2.4.3 Hậu quả

Các cuộc tấn công thiết bị di động có thể gây ra nhiều hậu quả nghiêm trọng, chẳng hạn như:

Đánh cắp dữ liệu: Tin tặc có thể đánh cắp dữ liệu cá nhân, tài chính, v.v. từ thiết bị di động.

Chiếm quyền điều khiển thiết bị: Tin tặc có thể chiếm quyền điều khiển thiết bị và sử dụng thiết bị để thực hiện các hành vi độc hại, chẳng hạn như phát tán mã độc, tấn công mạng, v.v.

Tốn tiền: Các cuộc tấn công thiết bị di động có thể khiến người dùng phải tốn tiền để sửa chữa thiết bị hoặc khôi phục dữ liệu bị mất.

2.4.4 Cách phòng tránh

Ngoài những biện pháp đã nêu ở mục 2.1.4.5 Cách bảo vệ hệ thống khỏi các lỗ hổng của hệ điều hành, tôi muốn trình bày một vài biện pháp hữu ích khác:

+ Cài đặt các biện pháp bảo mật trên thiết bị di động: Các biện pháp bảo mật này có thể bao gồm sử dụng mật khẩu mạnh, bật xác thực hai yếu tố, v.v.

+ Cẩn thận khi cài đặt ứng dụng: Chỉ cài đặt các ứng dụng từ các nguồn đáng tin cậy.

+ Cẩn thận khi sử dụng Wi-Fi công cộng: Không thực hiện các hoạt động nhạy cảm trên Wi-Fi công cộng.

Một điều quan trọng nữa là người dùng cần phải nâng cao nhận thức về các cuộc tấn công thiệt bị di động, để từ đó có thể bảo vệ điện thoại của mình và người thân được tốt hơn.

2.4 Quy trình của một cuộc tấn công

Quy trình của một cuộc tấn công thiết bị di động thông thường bao gồm các bước sau:

2.4.1 Tấn công mục tiêu

Trước khi tấn công, tin tặc sẽ tiến hành thu thập một số thông tin của nạn nhân, chẳng hạn như tên nạn nhân, địa chỉ email, số điện thoại, v.v. Điều này sẽ giúp kẻ tấn công tăng khả năng thành công khi thực hiện hành vi.

2.4.2 Lợi dụng lỗ hổng

Tin tặc sẽ bắt đầu tìm kiếm các lỗ hổng bảo mật hoặc lỗ hổng trên ứng dụng để bắt đầu tấn công. Những lỗ hổng trong hệ điều hành giống như đường cao tốc để tin tặc tấn công hệ điều hành.

2.4.3 Truyền tải mã độc

Sao khi tìm thấy lỗ hổng, tin tặc sẽ tiến hành cài mã độc vào thiết bị của nạn nhân bằng cách, bằng cách lừa nạn nhân truy cập vào đường link hoặc cài đặt ứng dụng có chứ mã độc.

2.4.4 Thực thi hành vi độc hại

Sau khi đã tải mã độc vào thiết bị của nạn nhân, tin tặc có thể thực hiện các hành vi độc hại như tôi đã nêu ở **phần 2.3.2 Các hành vi của tin tặc.** Ngoài những

hành vi đã nêu, tin tặc còn có thể triển khai ransomware để mã hóa dữ liệu và yêu cầu tiền chuộc từ nạn nhân.

2.4.5 Ẩn dấu

Sau khi đã thực hiện hành vi độc hại, những kẻ tấn công sẽ cố gắng ẩn dấu để tránh bị phát hiện bao gồm cả việc tất xóa dấu vết của mã độc hoặc là sử dụng kĩ thuật ẩn danh.

2.5 Các công nghệ được sử dụng

Để mô phỏng một cuộc tấn công vào thiết bị di động, tôi sẽ sử dụng phần mềm **VirtualBox, Genymotion** để tạo một thiết bị di động sử dụng hệ điều hành Android, sau đây là quá trình cài đặt các phần mềm cần thiết.

2.5.1 Phần mềm VirtualBox

2.5.1.1 Giới thiệu về VirtualBox

Tổng quan

VirtualBox là một trình ảo hóa phần mềm mã nguồn mở và miễn phí dành cho ảo hóa x86 do Tập đoàn Oracle tạo ra. Nó là một trình ảo hóa loại 2, nghĩa là nó chạy trên hệ điều hành máy chủ và tạo ra các máy ảo (VM) hoạt động như hệ điều hành khách trên máy chủ.

Chức năng

VirtualBox là một công cụ mạnh mẽ có thể được sử dụng cho nhiều mục đích khác nhau, bao gồm:

- Phát triển và thử nghiệm: VirtualBox có thể được sử dụng để tạo môi trường thử nghiệm và phát triển riêng biệt. Điều này có thể hữu ích cho việc phát triển và thử nghiệm phần mềm trên các hệ điều hành khác nhau hoặc để thử nghiệm phần mềm ở các cấu hình khác nhau.
- Giáo dục và đào tạo: VirtualBox có thể được sử dụng để tạo ra các máy ảo mà sinh viên và học viên có thể sử dụng để tìm hiểu về các hệ điều hành và ứng dụng khác nhau.
- Hợp nhất máy chủ: VirtualBox có thể được sử dụng để hợp nhất nhiều máy chủ vào một máy vật lý. Điều này có thể giúp giảm chi phí và cải thiện việc sử dụng tài nguyên.

- Ảo hóa máy tính để bàn: VirtualBox có thể được sử dụng để tạo máy tính để bàn ảo có thể truy cập từ các thiết bị từ xa. Điều này có thể hữu ích khi cung cấp cho nhân viên quyền truy cập vào máy tính để bàn làm việc của họ ở nhà hoặc cung cấp cho khách hàng quyền truy cập vào các ứng dụng mà không cần phải cài đặt chúng trên thiết bị của riêng họ.

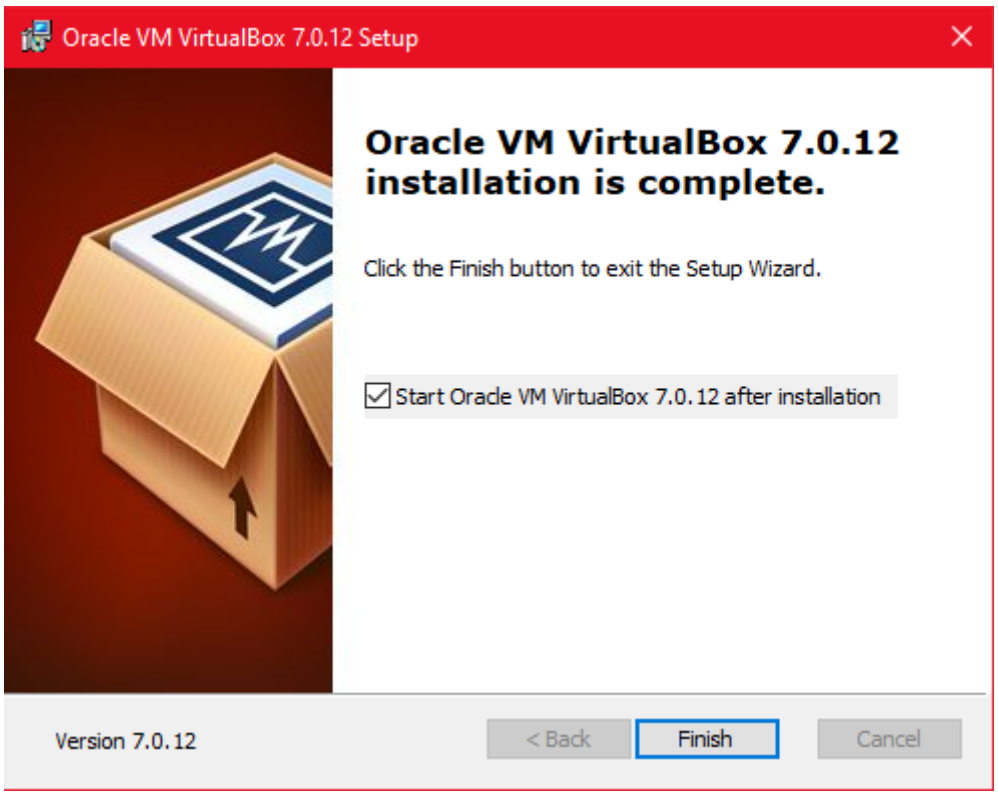
2.5.1.2 Quá trình cài đặt

Bước 1: Truy cập vào liên kết https://www.virtualbox.org/wiki/Downloads để chọn phiên bản VirtualBox phù hợp với hệ điều hành.

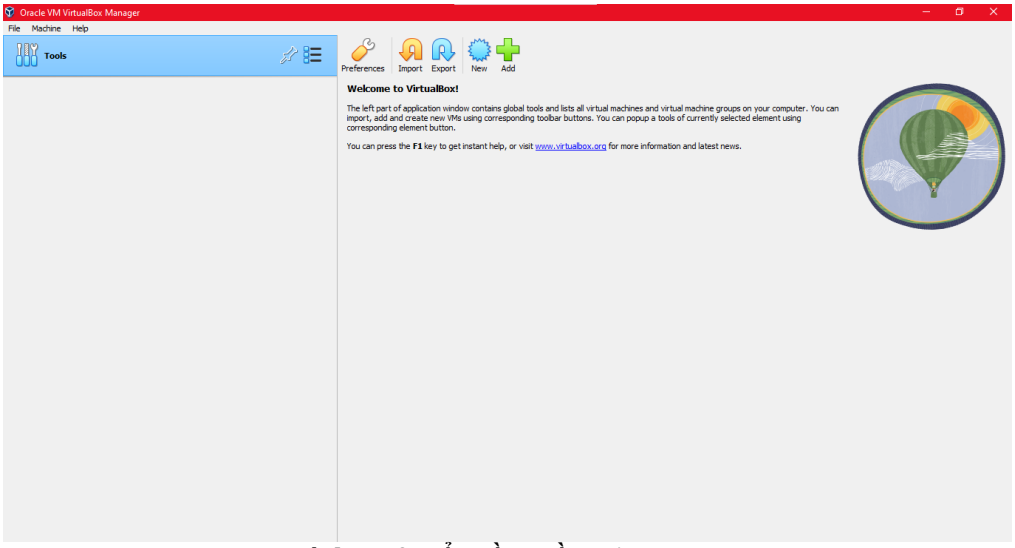
Hình 1 Trang web tải phầm mềm VirtualBox

Bước 2: Mở file **VirtualBox-7.0.12-159484-Win.exe** vừa tải xong, chọn **Next** -> chọn vị trí cài đặt bằng cách chọn **Browse**, sau đó chọn **Next -> Yes -> Yes -> Install.**

Sau khi quá trình cái đặt hoàn tất, chọn Start để khởi động phầm mềm VirtualBox



Hình 2 Hoàn tất cài đặt



Hình 3 Cửa sổ phầm mềm VirtualBox

2.5.2 Phần mềm Genymotion

2.5.2.1 Giới thiệu về Genymotion

Tổng quan

Genymoti là là một phần mềm giả lập Android được phát triển bởi Xamarin. Genymotion cho phép người sử dụng chạy các ứng dụng và trò chơi Android trên máy tính

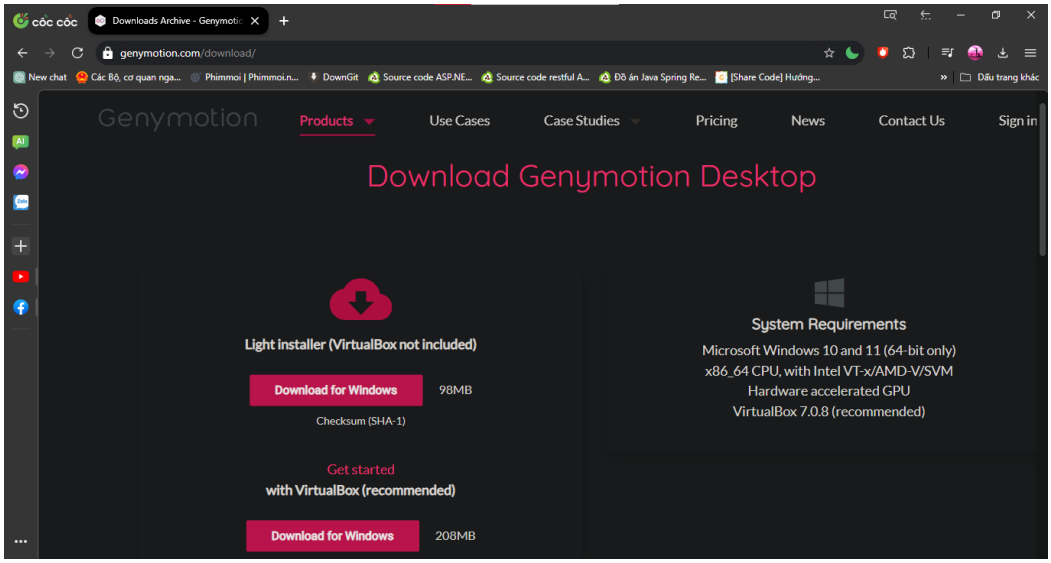
Tính năng

- Hỗ trợ nhiều phiên bản Android, từ Android 4.0.3 cho đến Android 13.
- Hỗ trợ nhiều thiết bị Android, bao gồm điện thoại, máy tính bảng, TV,…

- Hỗ trợ được nhiều tính năng của Android, bao gồm GPS, camera, microphone, ….

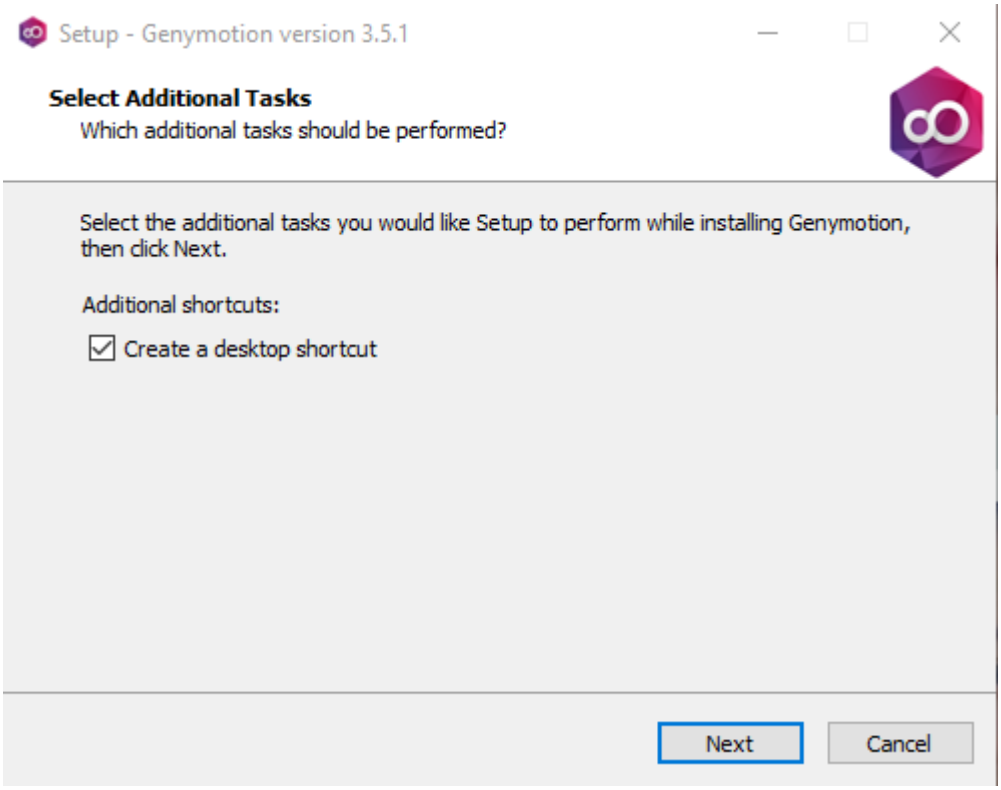
2.5.2.2 Quá trình cài đặt

Bước 1: Truy cập vào đường dẫn: **https://www.genymotion.com/download/** để đến trang tải xuống của Genymotion. Sau khi truy cập, hãy chọn phiên bản phù hợp là tải xuống. Ở đây tôi chọn phiên bản có hỗ trợ VirtualBox.

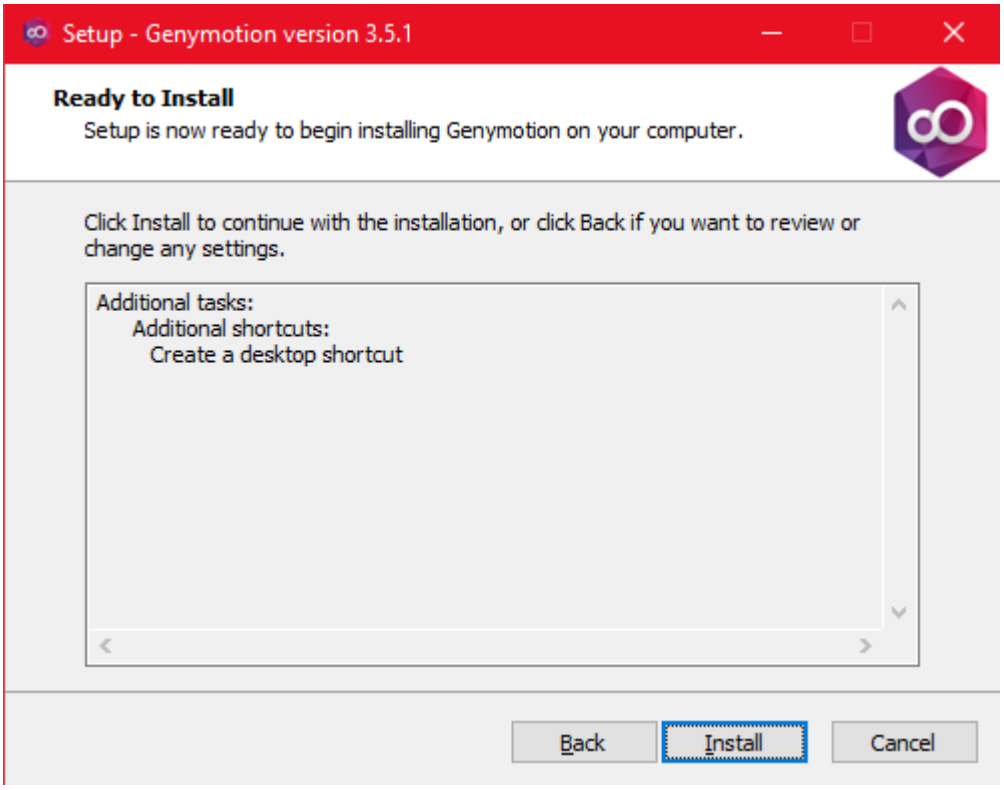


Hình 4 Website dowload Genymotion

Bước 2: Sau khi quá trình tải xuống hoàn tất, mở tập tin vừa tải về, một cửa sổ cài đặt sẽ hiện ra. Chọn **Next-> Install**.



Hình 5 Quá trình cài đặt Genymotion (1)

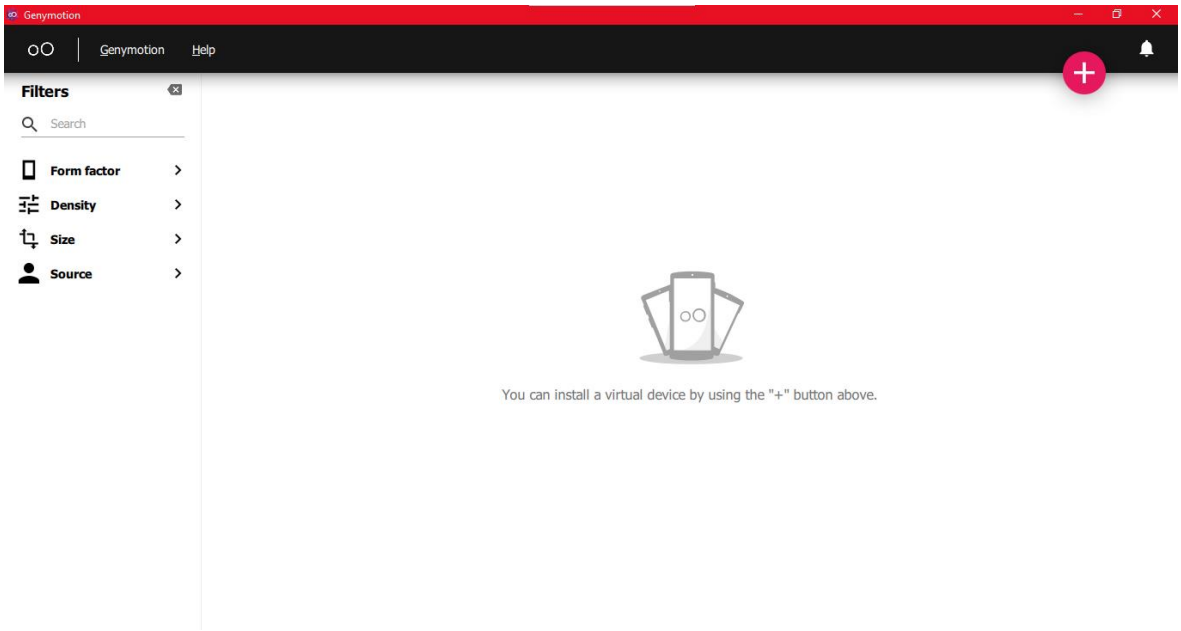


Hình 6 Quá trình cài đặt Genymotion (2)

Sau khi cài đặt xong, khởi động lại máy tính để sử dụng phần mềm.

Hình 7 Giao diện sao khi hoàn tất cài đặt

Sau khi khởi động lại máy tính, mở phầm mềm Genymotion vừa mới cái đặt, giao diện sau hi khởi động của Genymotion như hình bên dưới.



Hình 8 Giao diện sau khi khởi động

CHƯƠNG 4: KẾT QUẢ NGHIÊN CỨU

Sau qua trình thực hiện đồ án, các kết quả thu được là:

+ Xác định được mục tiêu, mục đích và phạm vi nghiên cứu của đề tài.

+ Trình bày được tổng quan, chức năng của các hệ điều hành Android, IOS.

+ Trình bày khái niệm, những rủi ro và cách phòng tránh một cuộc tấn công vào thiết bị Android.

CHƯƠNG 5: KẾT LUẬN VÀ HƯỚNG PHÁT TRIỂN

Kết luận

Bài nghiên cứu này nhằm mục đích giới thiệu cho mọi người hiểu hơn về những hiểm họa mà lỗ hổng hệ thống mang lại, từ đó rút ra được những biện pháp phòng tránh việc tin tặc lợi dụng cái lỗ hổng đó để tiến hành đánh cấp hoặc phá hoại thông tin có trong thiết bị di động.

Hướng phát triển

Bài nghiên cứu là mô phỏng một cuộc tấn công vào thiết bị di động sử dụng hệ điều hành Android, nên tôi đề xuất hướng phát triển tiếp theo sẽ là tìm hiểu và mô phỏng cuộc tấn công vào các hệ điều hành cho thiết bị di động khác, có thể là hệ điều hành IOS hoặc hệ điều hành Window Phone.

DANH MỤC TÀI LIỆU THAM KHẢO

[1] P. T. Minh, trong *Giáo tình Hệ điều hành*, Hà Nội, 2016, pp. 12-16.

[2] B. k. t. t. m. Wikipedia, "Hệ điều hành di động," [Trực tuyến]. Available: https://vi.wikipedia.org/wiki/H%E1%BB%87_%C4%91i%E1%BB%81u_h%C3%A0nh_di_%C4%91%E1%BB%99ng. [Đã truy cập 20 12 2023].

[3] "Android Open Source Project," [Trực tuyến]. Available: https://source.android.com/?hl=vi. [Đã truy cập 2 11 2023].

[4] B. k. t. t. m. Wikipedia, "IOS," [Trực tuyến]. Available: https://vi.wikipedia.org/wiki/IOS. [Đã truy cập 26 12 2023].

[5] Curt Franklin, Chris Pollette, "How Operating Systems Work," HowStuffWorks, [Trực tuyến]. Available: https://computer.howstuffworks.com/operating-system.htm. [Đã truy cập 15 12 2023].

[6] H. Vu, "Những lỗ hổng bảo mật trên di động và kiểm thử bảo mật di động," Viblo, 25 8 2016. [Trực tuyến]. Available: https://viblo.asia/p/nhung-lo-hong-bao-mat-tren-di-dong-va-kiem-thu-bao-mat-di-dong-PaLkDQDmvlX. [Đã truy cập 26 12 2023].