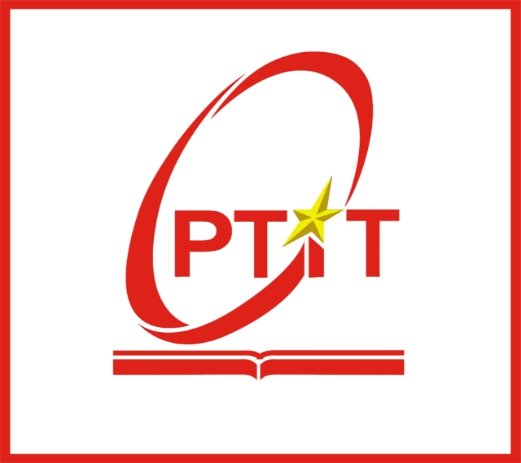


**HỌC VIỆN CÔNG NGHỆ BƯU CHÍNH VIỄN THÔNG**

**KHOA AN TOÀN THÔNG TIN**



**ptit-debugging**

Giảng viên: Đinh Trường Duy

1. **Bài thực hành ptit-debugging trên Windows**
   1. **Nội dung và hướng dẫn bài thực hành**
      1. ***Mục đích***

* Giúp sinh viên tìm hiểu về cách debug mã độc từ đó giúp sinh viên hiểu rõ hơn về logic, dữ liệu và hành động của phần mềm độc hại cũng như khả năng sửa đổi chúng một cách nhanh chóng.
* Giúp sinh viên nắm được cách sử dụng các công cụ cho việc loại bỏ các cơ chế phát hiện sandbox của mã độc.
  + 1. ***Yêu cầu với sinh viên***
* Có kiến thức cơ bản về phân tích mã độc, nắm vững kiến thức về hệ điều hành, lệnh hợp ngữ, kỹ năng debug chương trình mã độc.
  + 1. ***Nội dung thực hành***
* Khởi động bài lab
* Vào terminal gõ:

*labtainer -r ptit-debugging*

(Chú ý : sinh viên sử dụng mã sinh viên của mình để nhập thông tin email người thực hiện bài lab khi có yêu cầu để sử dụng khi chấm điểm)

* Trước khi khởi động bài lab nếu máy Windows 7 và máy Ubuntu chưa được cấu hình mạng NAT, sinh viên cần cấu hình môi trường thực hành bằng cách mở máy Windows 7, cài đặt máy Windows 7 và máy Ubuntu cùng một Network Adapter là NAT bằng cách chọn:

*VM => Settings… => Network Adapter => NAT*

* Sau đó sinh viên đăng nhập vào máy Windows 7 với tài khoản (*user1:user1*), thực hiện kiểm tra địa chỉ IP của máy Windows 7 => Giả sử tìm được địa chỉ IP là *192.168.1.128*
* Khi khởi động bài lab, một cửa sổ ubuntu hiện lên, sinh viên thực hiện kết nối đến máy windows bằng lệnh

*./connect\_windows.sh.x < địa chỉ IP của máy Windows >*

* Sau khi kết nối thành công, cửa sổ Windows 7 sẽ hiện lên. Sinh viên cần mở một cửa sổ Windows powershell để thực hành và kiểm tra kết quả thực hành trên Windows, sinh viên thực hiện các lệnh trên cửa sổ powershell này trong suốt quá trình làm bài thực hành.
* Sau đó sinh viên xem phần mềm độc hại có tên shell.exe tại đường dẫn C:\Users\user1\Downloads\.

(Chú ý: Sau mỗi lần thực hiện một lệnh theo nhiệm vụ của bài thực hành cần chạy chương trình [*\\tsclient\C\_\check\_lab.ps1*](file:///\\tsclient\C_\check_lab.ps1) để ghi lại tiến độ làm bài thực hành)

* ***Nhiệm vụ 1:*** Cài đặt và cấu hình InetSim trên máy ubuntu và cấu hình DNS cho máy Windows để phục vụ chặn yêu cầu DNS, HTTP hoặc các yêu cầu khác phát sinh từ phần mềm độc hại chạy trên máy Windows.
* Để hoàn thành được nhiệm vụ này sinh viên cần cài đặt và cấu hình thành công dịch vụ Inetsim cho máy Ubuntu và DNS cho máy Windows. Sau khi cài đặt và cấu hình thành công Inetsim, sinh viên có thể kiểm tra dịch vụ Inetsim đã hoạt động hay chưa bằng lệnh: *curl <IP máy cài Inetsim>* trên Ubuntu container của bài thực hành.

Tại máy ubuntu chạy labtainer sinh viên thực hiện cài đặt Inetsim:

Lưu ý: Cài Inetsim trên máy Ubuntu chạy labtainer, không phải trong container thực hành.

*sudo apt-get update*

*sudo apt-get install inetsim*

Sau khi cài đặt thành công sinh viên cần thực hiện chỉnh sửa file cấu hình inetsim.conf được đặt tại */etc/inetsim/inetsim.conf*  để điều hướng lưu lượng truy cập của mã độc từ đó bắt được các yêu cầu DNS, HTTP hoặc các yêu cầu khác phát ra từ mẫu phần mềm độc hại ( shell.exe), từ đó cung cấp cho mã độc các phản hồi tổng hợp, có kiểm soát.

Để có thể cấu hình, trước tiên sinh viên cần thực hiện trích xuất strings để tìm được domain mà mã độc truy cập tới.Tại file cấu hình sinh viên thực hiện cấu hình địa chỉ IP dịch vụ sẽ liên kết, cài đặt máy chủ tên miền

service\_bind\_address <IP máy Ubuntu labtainer cài Inetsim>   
dns\_default\_ip <IP máy Ubuntu labtainer cài Inetsim>   
dns\_default\_hostname www   
dns\_default\_domainname <domain mà mã độc truy cập tới>

Sau khi cấu hình thành công, sinh viên chạy inetsim bằng lệnh:

*sudo inetsim*

Để kiểm tra Inetsim đã chạy chưa, từ Ubuntu container của bài thực hành sinh viên sử dụng lệnh:

*curl <IP máy Ubuntu labtainer cài Inetsim >*

Tiếp theo tại máy Window sinh viên chọn *Open Sharing and Internet Setting*. Tại mục *NetWork Connection* sinh viên thực hiện chọn cấu hình Ipv4 . Tại mục *General* chọn *Use the following DNS server addresss* và điền DNS Server là địa chỉ IP máy đang chạy dịch vụ Inetsim.

Lúc này, DNS của máy Window được sinh ra sẽ được trỏ tới máy ubuntu labtainer đang chạy Inetsim. Tại máy Windows lúc này khi truy cập vào địa chỉ IP ubuntu labtainer hoặc bất kì tên miền nào ví dụ google.com, youtube.com,… đều sẽ được được điều hướng đến máy chủ chạy Inetsim với nội dung hiển thị

(This is the default HTML page for InetSim HTTP server fake mode.

This file is an HTML document)

* ***Nhiệm vụ 2:*** Thực hiện ngăn chặn phát hiện sandbox của mã độc với chương trình x64dbg bằng cách loại bỏ các cơ chế phát hiện sandbox của mã độc shell.exe. Khi chạy mã độc chưa được loại bỏ hoàn toàn các cơ chế phát hiện sandbox, nó sẽ thông báo “Sandbox detected”.
* Để hoàn thành được nhiệm vụ này sinh viên cần loại bỏ các cơ chế phát hiện sandbox của mã độc shell.exe.

Để thực hiện nhiệm vụ này sinh viên thực hiện chạy shell.exe với x64dbg. Sau đó sinh viên chọn Run trên tab công cụ và tìm các chuỗi Sanbox Detected trong String references (Tại mục Seach for -> Current Module -> String references)

Lúc này sinh viên sẽ tìm được 3 chuỗi Sanbox detected.

Sau đó sinh viên thực hiện đặt breakpoint, để khi chúng ta nhấn chạy, quá trình thực thi sẽ tạm dừng tại thời điểm này.

Trước tiên sinh viên thực hiện thêm điểm dừng với chuỗi Sanbox detected thứ 3 .Sinh viên nhấn đúp vào chuỗi này để được trỏ đến địa chỉ của nó (00000000004032EC)

Theo quan sát, một lệnh:

cmp dword ptr ss:[rsp+0x30], 0x01

hiện diện phía trên MessageBox này để so sánh giá trị với 1 sau khi thực hiện so sánh đường dẫn đăng ký. Thay vào đó, hãy sửa đổi giá trị so sánh này để khớp với 0 bằng cách nhấn space tại vị trí lệnh đó. Chúng ta có thể thay đổi giá trị so sánh từ 0x01 thành 0x00 . Việc thay đổi so sánh thành 0 có thể chuyển luồng điều khiển của mã và nó sẽ không chuyển đến địa chỉ nơi MessageBox được hiển thị. Sau khi chỉnh sửa mã sẽ có dạng:

cmp dword ptr ss:[rsp+0x30],0x00

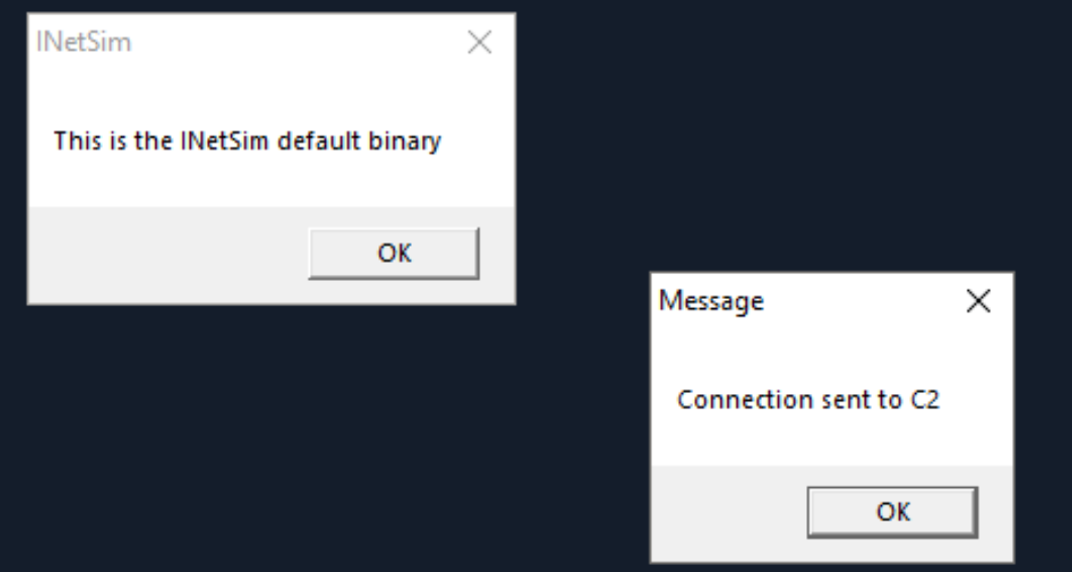
Khi nhấp vào Run trong x64dbg hoặc nhấn F9, nó sẽ không đạt điểm dừng (breakpoint) cho mã thông báo “Sandbox detected” đầu tiên. Điều này có nghĩa là chúng ta đã vá lỗi thành công.

Theo cách tương tự, chúng ta có thể thêm điểm dừng (breakpoint) trên chức năng phát hiện hộp cát tiếp theo trước khi nó in MessageBox. Để làm điều đó, điểm ngắt phải được đặt ở chuỗi Sanbox detected thứ 2 được đặt ở (00000000000402F13). Nếu bấm đúp vào chuỗi này, chúng ta sẽ nhận thấy có một lệnh jump mà chúng ta có thể bỏ qua, chuyển luồng thực thi sang lệnh tiếp theo gọi hàm khác.Có thể để thực thi được thay vì hiển thị MessageBox Sandbox Detected mã độc chuyển sang một chức năng khác.

Sinh viên cần thực hiện thay đổi từ *je shell.402F09* thành *jne shell.402F09*.

Bên cạnh đó, shell.exe thực hiện phát hiện hộp cát bằng cách kiểm tra kết nối internet. Mục tiêu của phần này không có kết nối internet. Vì lý do này, sinh viên cần thực hiện vá phương pháp phát hiện hộp cát này. Chúng ta có thể làm điều đó bằng cách nhấp vào chuỗi Sandbox detected đầu tiên (0000000000402CBD) . Tại đây sinh viên sẽ nhận thấy có lệnh jne có thể bỏ qua, sinh viên thực hiện chỉnh sửa thành lệnh jmp để chuyển luồng thực thi của mã độc

Bây giờ,mọi chức năng phát hiện sanbox của mã độc đã được vá, khi chúng ta nhấn Run, shell.exe đã vá sẽ tiếp tục tiến hành. Truy cập trỏ đến tên miền của mã độc lúc này sẽ được điều hướng đến máy chủ đang chạy inetsim, và tải xuống tệp thực thi mặc định từ INetSim và thực thi nó. Khi sinh viên vá thành công màn hình sẽ hiển thị



* Sau khi loại bỏ thành công, mã độc sẽ hiện ra 2 cửa sổ thông báo (sinh viên chạy chương trình [*\\tsclient\C\_\check\_lab.ps1*](file:///\\tsclient\C_\check_lab.ps1) để ghi lại tiến độ làm bài thực hành)
* ***Nhiệm vụ 3***: Sử dụng Wireshark kiểm tra lưu lượng mạng, kiểm tra phản hồi HTTP và nhận về tệp nhị phân trả về bởi InetSim.
* Để hoàn thành nhiệm vụ này sinh viên cần sử dụng Wireshark để nắm bắt và kiểm tra lưu lượng truy cập mạng do phần mềm độc hại tạo ra. Sinh viên cần chú ý đến lưu lượng được mã hóa màu: màu đỏ tương ứng với lưu lượng từ máy khách đến máy chủ, trong khi màu xanh lam biểu thị sự trao đổi giữa máy chủ với máy khách.

Sinh viên thực hiện kiểm tra yêu cầu HTTP cho thấy mẫu phần mềm độc hại có yêu cầu “*GET /svhost.exe”* đồng thời thêm tên máy chủ của máy tính vào trường tác nhân người dùng.

Có thể thấy rõ rằng nó InetSim đã trả về tệp nhị phân mặc định dưới dạng phản hồi đối với phần mềm độc hại với nội dung “This program cannot be run in DOS mode”.

Yêu cầu của phần mềm độc hại này của mã độc tới svchost.exe để lấy tệp nhị phân mặc định từ InetSim. Hệ nhị phân này phản hồi bằng một MessageBox thông báo “This is the INetSim default binary”.

Ngoài ra, sinh viên cần thực hiện kiểm tra yêu cầu DNS của mã độc cho một miền và địa chỉ ngẫu nhiên ms-windows-update[.]com đã được mã độc gửi đi và INetSimphản hồi bằng các phản hồi giả mạo

(sinh viên chạy chương trình [*\\tsclient\C\_\check\_lab.ps1*](file:///\\tsclient\C_\check_lab.ps1) để ghi lại tiến độ làm bài thực hành)

* Để thúc bài lab :
* Trên terminal đầu tiên sử dụng lệnh sau để kết thúc bài lab:

*stoplab ptit-debugging*

* Khi bài lab kết thúc, một tệp zip lưu kết quả được tạo và lưu vào một vị trí được hiển thị bên dưới stoplab.
* Khởi động lại bài lab:
* Trong quá trình làm bài sinh viên cần thực hiện lại bài lab, dùng câu lệnh:

*labtainer –r ptit-debugging*