PHẦN 1: CHUẨN BỊ HOST VÀ CÀI ĐẶT PHẦN MỀM

Bước 1: Kiểm tra phần cứng và an toàn

- Đảm bảo máy tính (Host) có ít nhất 8GB RAM (nên 16GB nếu chạy nhiều máy ảo).
- Nếu có thể, sử dụng một máy chuyên cho nghiên cứu malware hoặc tạm thời ngắt kết nối Internet để bảo vệ an toàn.

Bước 2: Tải và cài đặt VMware Workstation

- Truy cập trang tải VMware Workstation Player (miễn phí cho học tập) tại: https://www.vmware.com/go/getplayer
- Tải về và tiến hành cài đặt theo hướng dẫn trên màn hình, chấp nhận các thiết lập mặc định nếu không có yêu cầu thay đổi.

Bước 3: Tải file ISO của Windows

- Tải Windows 10/11 Enterprise Evaluation từ website Microsoft (hoặc sử dụng file ISO Windows hợp lệ mà em đã có).
- Lưu file ISO vào một thư mục trên Host ví dụ: C:\ISOs

- Ví dụ file ISO: C:\ISOs\Windows10.iso

Lưu ý: File ISO nằm trên ổ C của máy Host. Máy ảo sau này sẽ "gắn" file này qua ổ đĩa ảo CD/DVD, không phải copy vào máy ảo.

PHẦN 2: TẠO MÁY ẢO TRÊN VMWARE VỚI MẠNG CÁCH LY (SỬ DỤNG VMnet1)

Bước 4: Tạo máy ảo Windows

1. Mở VMware Workstation Player.

2. Chọn "Create a New Virtual Machine".

3. Trong cửa sổ "New Virtual Machine Wizard":

– Chọn "Installer disc image file (iso)"

– Duyệt đến file ISO trên Host: nhập đường dẫn "C:\ISOs\Windows10.iso"

4. Chọn hệ điều hành: lựa chọn "Microsoft Windows" với phiên bản "Windows 10 x64".

5. Đặt tên máy ảo, ví dụ: "Win10-Malware-Analysis".

6. Chọn vị trí lưu file máy ảo, ví dụ: D:\VMs\Win10-Malware-Analysis.

7. Phân bổ tài nguyên:

– RAM: ít nhất 4096 MB (nên dùng 8192 MB nếu có đủ tài nguyên).

– Ổ cứng: ít nhất 40GB; chọn kiểu ổ cứng SCSI (để hiệu năng tối ưu).

8. Hoàn tất wizard và máy ảo sẽ được tạo.

Bước 5: Cấu hình Network Isolation sử dụng VMnet1

1. Nhấp phải chuột vào máy ảo "Win10-Malware-Analysis" trong VMware Workstation và chọn "Settings".

2. Trong cửa sổ "Virtual Machine Settings", chọn phần "Network Adapter" ở cột bên trái.

3. Phía bên phải, thay vì chọn "NAT" hay "Bridged", hãy chọn mục "Custom: Specific virtual network".

4. Nhấp vào menu thả xuống để chọn mạng ảo; chọn "VMnet1".

– Để kiểm tra: Từ menu "Edit" trong VMware Workstation, chọn "Virtual Network Editor".

– Xem danh sách các mạng ảo; đảm bảo rằng "VMnet1" được thiết lập ở chế độ "Host-only".

5. Nhấn "OK" để lưu cấu hình.

(Nếu em muốn đảm bảo không có kết nối Internet, em có thể bỏ tích "Connect at power on" trong phần "Network Adapter" của máy ảo.)

Bước 6: Khởi động máy ảo và cài đặt Windows

1. Trong VMware Workstation, chọn máy ảo "Win10-Malware-Analysis" và nhấn nút "Play virtual machine".

2. Khi máy ảo bật lên, nó sẽ dùng ổ đĩa CD/DVD ảo đã gán file ISO.

– File ISO được gán ở bước 4 là "C:\ISOs\Windows10.iso" trên Host. Máy ảo "thấy" file này qua ổ đĩa ảo CD/DVD.

3. Windows sẽ khởi động từ file ISO, sau đó em làm theo hướng dẫn cài đặt:

– Chọn ngôn ngữ, múi giờ, và định dạng phân vùng ổ cứng.

– Cài đặt hoàn tất và tạo tài khoản quản trị nội bộ.

PHẦN 3: CÀI ĐẶT CÔNG CỤ PHÂN TÍCH & TẠO SNAPSHOT

Bước 7: Cài đặt các công cụ phân tích

1. Sau khi Windows được cài đặt, mở trình duyệt trong máy ảo.

2. Tải các công cụ theo các đường link sau:

– Process Explorer và Process Monitor từ trang Sysinternals:

https://docs.microsoft.com/en-us/sysinternals/

– Wireshark tại:

https://www.wireshark.org

3. Cài đặt và lưu các công cụ vào thư mục (ví dụ: C:\Tools) trong máy ảo để tiện theo dõi khi chạy malware.

Bước 8: Tạo Snapshot Ban Đầu

1. Trong VMware Workstation, chọn máy ảo "Win10-Malware-Analysis".

2. Từ giao diện chính, chọn "Snapshot" hoặc tìm mục "Take Snapshot".

3. Đặt tên Snapshot là "Clean Windows + Tools".

4. Nhập mô tả nếu cần (ví dụ: "Hệ thống đã cài đặt Windows và các công cụ phân tích sẵn sàng").

5. Nhấn "OK" để tạo Snapshot – điểm phục hồi ban đầu của máy ảo.

PHẦN 4: CHUYỂN FILE SAMPLE MALWARE VÀ THIẾT LẬP THƯ MỤC CHIA SẺ (HOST → VM)

Bước 9: Lấy Sample Malware từ bài viết của Zeltser

1. Trên máy Host, mở trình duyệt và truy cập:

https://zeltser.com/vmware-network-isolation-for-malware-analysis/

2. Đọc kỹ bài viết. Zeltser hướng dẫn cách thiết lập môi trường cách ly; trong một số bài có link tải mẫu malware.

3. Nếu bài viết có link tải mẫu malware, em tải file (ví dụ: "sample_malware.exe") và lưu vào một thư mục trên Host, ví dụ "C:\SampleMalware".

Bước 10: Thiết lập Thư Mục Chia Sẻ chỉ Một Chiều (Read-only) từ Host sang VM

1. Trên Host, chắc chắn rằng thư mục "C:\SampleMalware" chứa file "sample_malware.exe".

2. Trong VMware Workstation, nhấp phải chuột vào máy ảo "Win10-Malware-Analysis" và chọn "Settings".

3. Chuyển đến tab "Options" (đối với VMware Workstation Pro có tính năng này) và chọn "Shared Folders".

4. Chọn "Always enabled".

5. Nhấn "Add…" để khởi tạo Shared Folder Wizard.

6. Trong hộp thoại:

– Chọn "Folder Path": duyệt đến "C:\SampleMalware".

– Đặt "Folder Name": ví dụ "SampleMalware".

– Tick chọn "Read-only" để đảm bảo máy ảo chỉ có quyền xem tập tin, không ghi thay đổi lại lên Host.

7. Hoàn tất wizard và nhấn "OK".

8. Khởi động lại máy ảo (nếu cần) để thư mục chia sẻ được gắn tự động.

9. Trong Windows VM, mở "File Explorer" và kiểm tra thư mục chia sẻ "SampleMalware" dưới "Network Locations" hoặc ổ đĩa được gắn.

PHẦN 5: CHẠY VÀ PHÂN TÍCH SAMPLE MALWARE

Bước 11: Tạo Snapshot Trước Khi Thử Nghiệm

1. Trong VMware Workstation, tạo một Snapshot mới từ máy ảo, đặt tên "Before Malware Execution".

2. Snapshot này giúp em phục hồi lại trạng thái ngay trước khi chạy malware.

Bước 12: Chuyển File và Chạy Sample Malware

1. Trong Windows VM, mở thư mục chia sẻ "SampleMalware".

2. Copy file "sample_malware.exe" từ thư mục chia sẻ sang một vị trí làm việc trên VM, ví dụ: Desktop hoặc C:\Temp.

3. (Tùy chọn) Để tăng an toàn, em có thể tạm thời vô hiệu hóa kết nối mạng ở VM:

– Vào "Control Panel → Network and Sharing Center" và vô hiệu hóa Network Adapter, hoặc

– Trong VMware, tắt kết nối "Connect at power on" cho Adapter.

4. Chạy file "sample_malware.exe" (chạy dưới tài khoản người dùng tiêu chuẩn, không dùng quyền Administrator nếu không cần).

5. Mở các công cụ phân tích như Process Explorer, Process Monitor, và sử dụng Wireshark (nếu cần) để theo dõi mọi hoạt động của malware:

– Quan sát tạo tiến trình, thay đổi Registry, hoạt động mạng, tạo/xoá file…

6. Ghi chép lại hành động của malware cho mục đích phân tích.

BƯỚC 13: SỬ DỤNG PROCESS EXPLORER VÀ PROCESS MONITOR

A. Sử dụng Process Explorer (procexp.exe)

1. Vào thư mục C:\Tools, tìm file "procexp.exe" và nhấp đôi để chạy ứng dụng.

2. Giao diện Process Explorer hiển thị danh sách các tiến trình đang chạy trên hệ thống với thông tin chi tiết như ID tiến trình (PID), tên tiến trình, mức CPU đang sử dụng, DLL được nạp,…

3. Quan sát trước khi chạy malware:

– Xem danh sách tiến trình hiện có.

– Em có thể sắp xếp theo tên, PID hay mức sử dụng CPU để có thể nhận ra sự thay đổi khi malware chạy.

4. Khi em chạy malware (sau khi chuyển file malware vào thư mục làm việc riêng của VM, ví dụ Desktop), Process Explorer sẽ cho biết tiến trình mới xuất hiện.

5. Em có thể nhấp phải vào tiến trình đó để xem "Properties" nhằm xem thông tin chi tiết như đường dẫn file, các kết nối mạng nếu có, danh sách DLL được tải, …

6. Ghi chép lại các tiến trình không bình thường hoặc bất thường được tạo ra sau khi malware chạy.

B. Sử dụng Process Monitor (procmon.exe)

1. Vào thư mục C:\Tools, tìm file "procmon.exe" và nhấp đôi để chạy nó.

2. Khi chạy Process Monitor, ứng dụng sẽ ngay lập tức bắt đầu ghi lại tất cả các hoạt động hệ thống:

– Các hoạt động truy cập tập tin (File System), thay đổi Registry, truy cập hệ thống mạng, …

3. Để giảm thiểu dữ liệu ghi lại từ quá trình khởi động ban đầu, em có thể nhấn biểu tượng "Capture" (nút Camera đỏ hoặc biểu tượng có hình quả dừng) để tạm dừng ghi dữ liệu trước khi chạy malware.

4. Sau đó, hãy xóa bộ lọc hiện có (nếu cần) hoặc thêm bộ lọc để chỉ theo dõi hoạt động liên quan đến file malware (ví dụ: đường dẫn chứa tên file malware hoặc đường dẫn tới Thư mục chứa file được copy vào thư mục làm việc của VM).

5. Khi sẵn sàng, nhấn vào nút "Capture" để bắt đầu ghi lại toàn bộ hoạt động.

6. Chạy malware và Process Monitor sẽ ghi lại các sự kiện:

– Các lần truy cập file (mở, đọc, ghi, xoá file).

– Thao tác trên Registry (mở, ghi, xoá key).

– Hoạt động mạng (nếu có).

7. Sau khi chạy xong, em có thể dừng ghi dữ liệu bằng cách nhấp nút "Capture" một lần nữa và lưu file log lại để phân tích chi tiết. Em có thể dùng chức năng "Find" (Ctrl+F) trong Process Monitor để tìm các từ khóa chẳng hạn "sample_malware.exe" để xem các hoạt động liên quan.

BƯỚC 14: SỬ DỤNG WIRESHARK ĐỂ THEO DÕI HOẠT ĐỘNG MẠNG

A. Vào thư mục nơi em đã cài đặt Wireshark (nếu trên máy ảo, có thể đã được cài đặt qua file cài đặt từ www.wireshark.org).

B. Mở Wireshark bằng cách nhấp đôi vào biểu tượng Wireshark trên desktop hoặc từ thư mục cài đặt.

C. Khi mở Wireshark, 1 cửa sổ hiện ra bao gồm danh sách các giao diện mạng đang có trên hệ thống (ví dụ: "Ethernet", "VMware Network Adapter for VMnet1", …)

1. Chọn giao diện mạng tương ứng của VM (thường là giao diện đang sử dụng VMnet1 – Host-only).

2. Nhấp vào "Start capturing packets" trên giao diện đó.

3. Wireshark sẽ bắt đầu ghi lại tất cả các gói tin đến và đi qua giao diện.

4. Để dễ dàng theo dõi, em có thể áp dụng bộ lọc (filter), ví dụ nếu malware gửi HTTP, em có thể gõ bộ lọc "http" hoặc sử dụng các bộ lọc liên quan đến IP, cổng cụ thể.

5. Sau khi chạy malware, dừng việc capture (bấm biểu tượng stop) và xem lại các gói tin bắt được để phân tích các kết nối mạng, các gói tin được gửi, phản hồi từ server, …

6. Ghi chép lại các địa chỉ IP, thông tin giao thức và các thông tin bất thường để phục vụ việc phân tích hành vi của malware.

BƯỚC 15: GHI CHÉP VÀ PHÂN TÍCH HOẠT ĐỘNG MALWARE

A. Khi malware được chạy, chú ý ghi chép các điểm sau đây:

1. Process Explorer:

– Các tiến trình mới xuất hiện, tên file, đường dẫn thực thi, mức sử dụng CPU, các DLL bất thường.

2. Process Monitor:

– Các thao tác trên file hệ thống, truy cập Registry, ghi đè.

– Các kết nối ra ngoài hoặc tạo file log.

3. Wireshark:

– Các gói tin bất thường, thông điệp giao tiếp ra ngoài nếu malware cố gắng liên lạc với server.

B. Em có thể chụp màn hình (screenshot) các bước quan trọng hoặc lưu log từ các ứng dụng (Process Monitor cho phép lưu log dưới định dạng PML).

C. Sau khi thu thập số liệu, em so sánh các hoạt động đã ghi với hành vi kỳ vọng của malware (theo tài liệu phân tích malware, các bài báo hay link tham khảo từ Zeltser) và ghi chú lại các điểm khác biệt cần phân tích sâu.

Các công cụ phân tích như Process Explorer và Process Monitor cung cấp thông tin chi tiết về tiến trình và hoạt động hệ thống, trong khi Wireshark giúp bắt gói tin mạng để xác định các kết nối bất thường.

Sự kết hợp của nó cho phép em theo dõi toàn diện hành vi của malware khi nó được chạy trong môi trường ảo cách ly, giúp em hiểu rõ hơn về tác động của malware lên hệ thống.

Đảm bảo bảo mật môi trường và lưu ý ghi chép lại tất cả các thông tin để phục vụ việc phân tích sau này.

Bước 16: Sau Khi Phân Tích

1. Nếu hệ thống bị ảnh hưởng hoặc malware hoạt động không mong muốn, tắt máy ảo.

2. Sử dụng Snapshot “Before Malware Execution” hoặc “Clean Windows + Tools” để khôi phục lại hệ thống trong VMware Workstation.

3. Xóa các tập tin malware không cần thiết trong VM nếu hoàn thành phân tích.

LƯU Ý AN TOÀN

- CHỈ THỰC HIỆN TRÊN MÁY ẢO: Không bao giờ chạy malware trên máy thật (Host).
- NETWORK ISOLATION: Việc cấu hình "Network Adapter" theo "Custom: Specific virtual network" với lựa chọn "VMnet1" (được cài đặt theo chế độ Host-only trong Virtual Network Editor) giúp cách ly VM hoàn toàn khỏi Internet.
- SNAPSHOT: Luôn tạo Snapshot trước khi chạy malware, nhằm có thể phục hồi nhanh nếu hệ thống bị ảnh hưởng.
- THƯ MỤC CHIA SẺ: Sử dụng Shared Folder dưới chế độ "Read-only" giúp chuyển file sample malware từ Host sang VM một cách an toàn, tránh ghi đè lên file trên Host.