1. Môi trường phân tích mã độc tối thiểu bao gồm

1. Một máy thực thi mã độc, một máy giả lập IDS server
2. Một máy thực thi mã độc, một IDS server
3. Một máy thực thi mã độc, một DNS Server
4. Một máy thực thi mã độc một máy giả lập DNS sever

2. Runtime Linking thường được sử dụng trong:

1. Các worms
2. Các mã độc hại hại bị nén hoặc làm rối
3. Các virus
4. Các mã độc có khả năng tự sao chép

3. Những Registry entries mà mã độc thường thay đổi để duy trì hiện diện gồm:

1. AppInit\_DLLs
2. Winlogn Notify
3. ScvHost DLLs
4. Cả 3 đáp án trên

4. Kỹ thuật phân tích tĩnh là:

1. Kỹ thuật phân tích mã độc dựa vào các thư viện liên kết của mã độc
2. Kỹ thuật phân tích mã độc bằng cách nghiên cứu mã dịch ngược của mãc độc
3. Kỹ thuật phân tích mã độc mà không cần phải thực thi mã độc
4. Kỹ thuật phân tích mã độc bằng cách nghiên cứu nguồn của mã độc

5. Kernel mode còn được gọi là

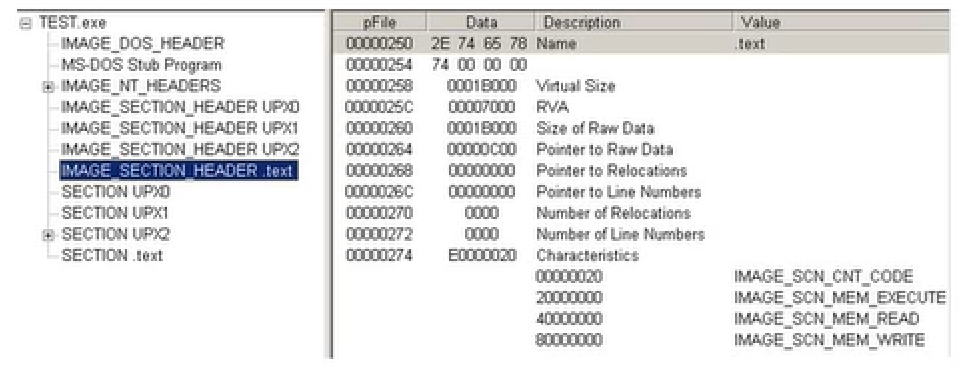
1. Ring 0
2. Ring 2
3. Ring 3
4. Ring 1

6.Thư viện nào sau đây giúp mã độc truy cập và thao tác lên bộ nhớ tập tin phần cứng

1. Kernel32.dll
2. Memory32.dll
3. Memory.ll
4. Kernel dll

7. Để diệt mã độc trên máy laptop cá nhân chạy HĐH windows có thể dùng:

1. BKAV, Kaspersky, Ollydbg
2. BKAV, Kaspersky
3. BKAV, Kasper, Virus total
4. AVG, BKAV, Windbg

8. Dùng PEID đọc thông tin của một tệp cho ra kết quả như hình: 

A. Là một mã độc được pack bằng thuật toán UPX

B. Là một tệp thực thi được pack bằng thuật toán UPX

C. Là một tệp tin thực thi.

D. Là một mã độc

Câu 9. Lệnh nào sau đây thường được mã độc sử dụng để phòng chống thực thi trong môi trường ảo hóa:

(A) sldt.

(B) sgot

(c) smsw.

(D) cả A B C

câu 10. Để chọn kiểu hiển thị các toán tử trong IDAPro ta cần:

(A) Nhấn chuột phải vào toán tử và chọn kiểu hiển thị.

(B) Sử dụng tính năng xref.

(c) Nhấn chuột trái vào toán tử và chọn kiểu hiển thị.

(D) Sử dụng tính năng subview.

Câu 11. Virtual Size là

(A) Kích thước của file trên đĩa CD.

(B) Kích thước của file trên USB.

(c) Kích thước của file trên bộ nhớ RAM.

(D) Kích thước của file trên Ổ đĩa cứng.

Câu 12. Nâng cao nhận thức người dùng là việc:

(A) Đào tạo về các nguy cơ, cách thức phần mềm độc hại xâm nhập vào hệ thông cho người dùng.

(B) Hướng dẫn người dùng sử dụng phần mềm Anti virus.

(C) Cấp quyền cho người dùng dựa trên đặc quyền tối thiểu.

(D) Hướng dẫn cho tất cả cán bộ, nhân viên cách phòng tránh sự cố liên quan đến mã độc hại, giảm thiểu mức độ nghiêm trọng của sự cố.

Câu 13. Time Date Stamp trong PE Header chỉ ra

(A) Không đáp án nào dùng.

(B) Thời gian chương trình được biên dịch.

(C) Thời gian chương trình bắt đầu khởi chạy.

(D) Tổng thời gian chương trình đã thực thi.

Câu 14: Mã độc là

(A) Các chương trình máy tính có khả năng tự sao chép và làm hại đến tính bí mật, tính toàn vẹn hoặc tính sẵn sàng của dữ liệu, Ứng dụng và hệ điều hành của hệ thống.

(B) Các chương trình máy tính có khả năng tự sao chép và lây nhiễm vào máy tính của người dùng.

(C) Các chương trình máy tính được tạo ra với mục đích làm hại đến tính bi mật, tính toàn vẹn hoặc tính sẵn sàng của dữ liệu và ứng dụng thực thi trên hệ thông.

(D) Các chương trình máy tính được tạo ra với mục đích làm hại đến tính bí mật, tính toàn vẹn hoặc tính sẳn sàng của dữ liệu, ứng dụng và hệ điều hành của hệ thống.

Câu 15. Mã độc có thể lây nhiễm qua

(A) Qua các thiết bị lưu trữ di động, qua thư điện tử, qua trình duyệt web và lây nhiễm từ smartphone sang máy tính.

(B) Qua các USB, qua thư điện tử, qua trình duyệt web và lây nhiễm từ smartphone sang máy tính.

(C) Qua các thiết bị lưu trữ di đông, qua thư điện tử, và lây nhiễm từ smartphone sang máy tính.

(D) Qua USB, qua thư điện tử, qua các trang web không an toàn và lây nhiễm từ smartphone sang máy tính.

Câu 16. Đoạn giải mã sau đây thế hiện cơ chế gì của mã độc.

CreateProcess(...,"svchost.exe",...,CREATE\_SUSPEND,...);

**ZwUnmapViewOfSection(...);**

**VirtualAllocEx(...,Image8ase,$ize0f1mage,...);**

**WriteProcessMemory( . . . ,tfheaders , . . . );**

for (i=0; i < NumberOfSections; i++) {

**WriteProcessMemory(...,section,...);**

}

**SetThreadContext();**

**…..**

**ResumeThread();**

(A) Tiêm vào tiến trình.

(B) APC.

(C) Detour.

(D) Thay thế tiến trình.

Câu 17. Sử dụng máy thật làm môi trường phân tích mã độc:

(A) Quá trình thực hiện phân tích đơn giản, tuy nhiên kết quả đôi khi không chính xác.

(B) Kết quả phân tích đôi khi không chính xác, quá trình thực hiện phân tích phức tạp.

(C) Cho kết quả phân tích chính xác, tuy nhiên quá trình thực hiện phân tích phức tạp.

(D) Cho kết quả phân tích chính xác, quá trình thực hiện phân tích đơn giản.

Câu 18. Trojan horse là

(A) Mã độc có khả năng nhân bản, không cần vật chủ để lây nhiễm.

(B) Mã độc không có khả năng nhân bản, không cần vật chủ để lây nhiễm.

(C) Mã độc không có khả năng nhân bản, cần vật chủ để lây nhiễm.

(D) Mã độc có khả năng nhân bản, cần vật chủ để lây nhiễm.

Câu 19: Mã độc thường nhằm đến Registry vì:

A. Registry lưu trữ cài đặt cấu hình của hệ điều hành và ứng dụng

B. Registry có thể tạo kết nối mạng

C. Không đáp án nào đúng

D. Registry chỉ có một kiểu dữ liệu

Câu 20: ZwUnmapViewOfSection là hàm mã độc sử dụng để

A Ghi lên vùng nhớ

B. Giải phóng vùng nhớ

C. Hủy vùng nhớ

D. Tạo Vùng Nhớ

Câu 21: Mật khẩu đăng nhập window được lưu tại

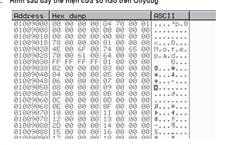
A. File LSASS

B. File NTLM

C. File LSA

D. File SAM

Câu 22: Hình sau đây sử dụng cửa sổ nào trong Olydbg

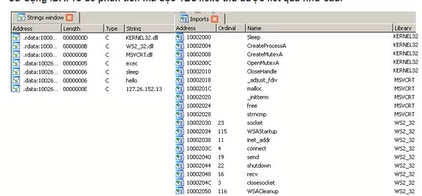


1. String window
2. Data window
3. Memory dump window
4. Address window

Câu 23: thành phần nào của mã độc chịu trách nhiệm những hành vi độc hại:

1. Spam
2. Frame
3. Payload
4. Exploit

24. Sử dụng IDA pro để phân tích mã độc TEST.exe thu được kết quả như sau



Từ kết quả trên có thể dự đoán gì và mã độc TEST.exe?

1. Sử dụng thư viện WININET để kết nối tới địa chỉ 127 26.152.13
2. Thực hiện mã hóa các tập tin trên máy nạn nhân.
3. Sử dụng thư viện Winsock để kết nối tới địa chỉ 127 26.152.13
4. Là một backdoor

Câu 25. (Những) công nghệ nào sau đây giúp giảm thiểu nguy cơ lây nhiễm mã độc trong hệ thống

A) Giảm thiểu tác động của phần mềm độc hại

(B)Tiêu diệt các tác hại của mà độc

(C) Phục hồi sau sự cố

(D) A, B, C

Câu 26. Giai đoạn ngăn chặn, loại bỏ và phục hồi nhằm

1. Giảm thiểu tác động của phần mềm độc hại
2. Tiêu diệt tác hại của mã độc
3. Phục hồi sau sự cố
4. Cả A,B,C

Câu 27. Hooking keylog sử dụng hàm nào để thu thập thao tác nhân phim của người dùng:

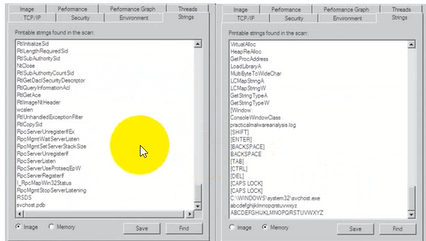
(A)LoadWindowsHookEx

(B) SetWindowsHookEx

(C)WindowsHookEx

(D) GetWindowsHookEx

Câu 28. Phân tích tiến trình TEST.exe thu được kết quả như sau.



Từ khi quả trên có thể kết luận gì về sản sinh TEST.exe

(A)Tiến trình đã bị thay thế bởi một đoạn mã độc.

(B) Tệp tin TEST.exe là một mã độc dạng keylog

(C) Tệp tin TEST exe là một mà độc, cố gắng kết nối đến địa chỉ practicalmalwareanlysis.com

(D) Tên tin TEST exe là một tập tin bình thường

Câu 29. Hàm nào sau đây được mã độc dùng để xác định trình debug:

1. IsDebuggerPresent
2. CheckRemoteDebuggerPresent
3. OutputDebugString.
4. Cả A, B, C

Câu 30. Địa chỉ IP 127.0.0.1 dược lưu trữ trong RAM dưới dạng:

(A) 0x0100007F

(B) 1.0.0.127.

(C) 127.0.0.1.

(D) 0x7F000001.

Câu 31. Nhược điểm của kỹ thuật phân tích động là

(A) Không cho kết quả phân tích chính xác với tất cả các loại mà độc

(B) Khó phân tích được những mẫu mã độc phức tạp.

(C) Chỉ phân tích được những mã độc chạy trên HĐH Window

(D) Không phân tích được những mã độc chạy trên HĐH Window

Câu 32. Handle có thể hiểu là:

A) Con trỏ tôi một tiến trình

(B) Con trỏ tới một đối tượng

(C) Con trỏ lại một vùng nhớ.

(D) Con trỏ tới một tiếp.

Câu 33.Sự cố mã độc có thể được phát hiện thông qua:

(A) Cảnh bảo của các hệ thống phòng chống mã độc.

(B) Báo cáo của người dùng về những bất thường trong hoạt động cửa

(C) Sự thay đổi của các tệp tin hệ thống

(D) Cả A, B, C.

Câu 34. GINA Registry Key lưu tai:

(A) HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\ MSGinaDLL

(B) HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion MSGinaDLL

(C) HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GinaDLL

(D) HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\ GinaDLL

Câu 35: Phát biểu nào sau đây đúng về svchost:

(A) Chỉ chạy một tiến trình duy nhất

(B) Ít bị mà đốc lợi dụng

(C) Chạy được trong chế độ nhân

(D) Dùng chung cho các service khác nhau

Câu 36. Ollydbg là công cụ:

(A) Phân tích tính cơ bản

(B) Phân tích động nâng cao

(C) Phân tích động cơ bản

(D) Phân tích tính năng cao

Câu 37. Sử dụng IDA pro để phân tích mã độc test.exe thu được kết quả như sau:



Mã độc test.exe thực hiện những hành động gì sau đây:

1. Gọi tiến trình internet Explorer 8.0, kiểm tra có kết nối internet không, tiến hành kết nối đến địa chỉ <http://www.malwareanalysisbook.com>
2. Kiểm tra có kết nối Internet hay không gọi tiến trình internet Explorer 8.0 tiến hành kết nối đến địa chỉ <http://ww.malwareanalysisbook.com>
3. Kiểm tra có kết nối Internet hay không gọi tiến trình internet Explorer 8.0 tiến hành kết nối đến địa chỉ <http://ww.malwareanalysisbook.com>, lặp lại quá trình kết nối
4. Gọi tiến trình internet Explorer 8.0, kiểm tra có kết nối internet không, tiến hành kết nối đến địa chỉ <http://www.malwareanalysisbook.com>,lặp lại tiến trình kết nối

Câu 38: Trước khi tiến hành phân tích mã độc trên môi trường máy ảo cần:

A Kết nối mạng từ máy ảo đến DNS server

B Tạo snapshots cho máy ảo

C không cần làm gì

D khởi chạy mã độc trên máy ảo

Câu 39: Một chương trình khi dừng tại breakpoint được gọi là

(A)Breaked

(B) Broken

(C)Breaker

D Paused

Câu 40. Backdoor thường sử dụng cổng nào có kết nối tới máy tính nạn nhân

A 21

B 80

C 43

D 23

Câu 41. Socket là lệnh mã độc sử dụng để

A Cho phép kết nối đến một cổng

B Tạo một socket

C Lắng nghe kết nối đến một cổng

D, Gần socket đến một cổng

Câu 42. Native API là các hàm của thư viện nào sau đây:

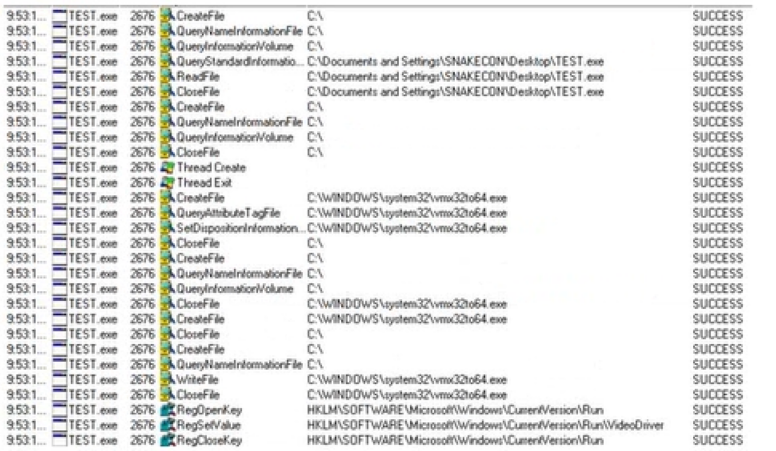
A Ntdll.dll

B User32.dll

C Kernel32.dll

D Kernel.dll

Câu 43. Sử dụng Process Monitor để phân tích mã độc TEST.exe thu được kết quả như sau.



Từ kết quả trên có thể kết luận gì về mã độc TEST.exe?

A. Sao chép file thực thi của hcính nó vào thư mục C:\\WINDOWS\System32 với tên vmx32to64.exe

B. Tạo một registry tại HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver.

C. Registry tạo ra giá trị trỏ tới C:\\WINDOWS\System32\vmx32to64.exe

D. Cả A, B, C

Câu 44. Sử dụng những công cụ nào sau đây có thể tiến hành phân tích động mã độc.

A. Ollydbg, Strings

B. Ollydbg, HashCal

C. Ollybdg, Process Explorer

D. Ollybdg, PEView

Câu 45. Để thực hiện chế độ single-step trên Ollydbg cần ấn phím

A. F6

B. F5

C. F7

D. F8