Câu 1: Names Window trong IPA Pro hiển thị…

* Tên các hàm, dữ liệu, chuỗi đi kèm với địa chỉ của chúng

Câu 2: Cờ ZF bật nếu kết quả của phép toán:

1. Bằng 0
2. Là số dương
3. Là số âm

Câu 3: … chứa mã nguồn đã được biên dịch của chương trình

* Code Segment

Câu 4: Lệnh NOP là lệnh:

1. Kết thúc đoạn chương trình
2. Không làm gì
3. Bắt đầu đoạn chương trình

Câu 5: Dịch ngược là quá trình tái tạo và chuyển đổi phần mềm độc hại ở dạng nhị phân về dạng:

1. Mã python
2. Hợp ngữ
3. Opcode

Câu 6: MOV ECX, 0X40 là lệnh:

1. Truyền giá trị 64 vào thanh ghi ECX
2. Lấy giá trị 40 từ thanh ghi ECX
3. Truyền giá trị 40 vào thanh ghi ECX
4. Lấy giá trị 64 từ thanh ghi ECX

Câu 7: Trong chế độ graph mode của IDA Pro, mũi tên hướng lên biểu thị gì?

1. Rẽ nhánh theo điều kiện sai
2. Rẽ nhánh theo điều kiện đúng
3. Vòng lặp

Câu 8: Loại mã độc nào sau đây kích hoạt nhằm mục đích phá hoại máy tính người dùng?

1. Keylog
2. Logic Boom
3. Backdoor

Câu 9: Loại mã độc nào sau đây có khả năng thực thi độc lập như một chương trình bình thường?

1. Worm
2. Virus
3. Trojan Horse

Câu 10: Mã độc lây nhiễm vào máy tính người dùng…

1. Khi trên máy người dùng không cài đặt AV
2. Khi người dùng truy cập vào Internet
3. Mà không có sự cho phép của người dùng

Câu 11: Hiện nay, mục đích phổ biến của mã độc là

1. Phá hoại hệ thống thông tin
2. Chiếm quyền điều khiển máy tính
3. Lừa đảo, quảng cáo

Câu 12: .rdata section trong PE file format chứa

1. Các hàm, thư viện liên kết dùng trong chương trình
2. Các biến trong chương trình
3. Các icon, menu, media… dùng trong chương trình

Câu 13: Công cụ nào sau đây là công cụ phân tích động cơ bản?

1. String
2. Wireshark
3. PE View

Câu 14: PE format là

1. Định dạng của mã độc trên Windows
2. Định dạng tệp tin thực thi trên Windows

Câu 15: Khi phân tích mã độc người phân tích nên

1. Sử dụng nhiều công cụ phân tích
2. Sử dụng một phương pháp phân tích
3. Phân tích chi tiết tất cả các phần của mã độc

Câu 16: Trước khi phân tích mã độc cần…

1. Ngắt kết nối mạng máy tính dùng để phân tích mã độc
2. Xây dựng môi trường phân tích an toàn
3. Cài đặt và triển khai các công cụ phân tích mã độc

Câu 17: Phân tích tĩnh là…

1. Phân tích các string trong mã độc
2. Cho mã độc thực thi và theo dõi các hành động của mã độc
3. Phân tích mà không thực thi mã độc

Câu 18: .text section trong PE file format chứa

1. Các icon, button, media trong chương trình
2. Mã thực thi của chương trình
3. Các biến trong chương trình

Câu 19: Dựa vào các … trong mã độc, người phân tích có thể dự đoán các hành động của mã độc.

1. Tham số
2. DLL
3. String

Câu 20: Mã độc có thể sử dụng các thư viện mạng nào?

1. network32.dll, Wininet.dll
2. ws2\_32.dll, Wininet.dll
3. system32.dll, Wininet.dll

Câu 21: Hàm ReleaseMutex được gọi:

1. Khi một thread khai báo một mutex
2. Khi một thread hoàn tất sử dụng mutex
3. Để một thread tương tác với mutex đã khai báo

Câu 22: Hàm CreateFileMapping thường được sử dụng…

1. Trong chương trình bình thường, để tải tệp vào RAM
2. Trong mã độc, để tạo file
3. Trong mã độc, để tải tệp vào RAM

Câu 23: Hàm CreateWindowEx trả về…

1. Một cửa sổ
2. Một handle cho một cửa sổ
3. Nhiều cửa sổ

Câu 24: Rootkit thường chạy ở

1. User Mode
2. Kernel Mode

Câu 25: Hầu hết các Native API làm hàm của thư viện nào sau đây?

1. system32.dll
2. ntdll.dll
3. kernel32.dll

Câu 26: Tiến trình nào sau đây thường là mục tiêu lây nhiễm của mã độc

1. Task Manager
2. Svchost
3. Autorun

Câu 27: Để duy trì hiện diện mã độc có thể đăng ký vào Registry nào sau đây?

1. HKLM\SOFTWARE\MicrosoftNT\CurrentV ersion\Winlogon\GinaDLL
2. HKEY\_LOCAL\_MACHINE\SOFTWARE\Windows\Run
3. HKEY\_LOCAL\_MACHINE\SOFTWARE\Windows\Windows

Câu 28: Mã thực thi của mã độc khác có thể được lưu ở phần nào của Loader?

1. header
2. .text
3. .rsrc

Câu 29: Mã độc tạo regestry key tại HKLM\SOFTWARE\Microsoft\CurrentVersion\Run để làm gì?

1. Để Windows hiểu mã độc là một chương trình
2. Để tránh sự phát hiện của AV
3. Để khởi chạy cùng Windows

Câu 30: Mutex được mã độc sử dụng nhằm mục đích gì?

1. Để cập nhật phiên bản mới nhất của mã độc tè máy chủ của hacker
2. Để kiểm tra đã có phiên bản nào thực thi trên máy chưa
3. Để kiểm tra đã có phiên bản cập nhật nào của mã độc trên máy chủ của hacker không

Câu 31: Mật khẩu của các user trên Windows được lưu tại …

1. File GINA
2. File LSASS
3. File SAM

Câu 32: Quá trình Login vào Windows sử dụng cơ chế và thư viện nào sau đây?

1. GINA, gina.dll
2. GINA, msgina.dll
3. GINA, fsgina.dll

Câu 33: Hooking keylog sử dụng hàm API nào sau đây?

1. GetAsyncKeyState
2. WlxLoggedOutSAS
3. SetWindowsHookEx

Câu 34: Loader là mã độc…

1. Chuẩn bị và thực thi một phần mềm độc hại khác
2. Lây nhiễm phần mềm độc hại khác trong mạng LAN
3. Tải một phần mềm độc hại khác vào máy tính nạn nhân

Câu 35: Mật khẩu của các User trên Windows được lưu dưới dạng hàm băm nào sau đây?

1. SHA-256 hash
2. MD5 hash
3. NTLM hash

Câu 36: Polling keylog sử dụng hàm API nào sau đây

1. WlxLoggedOutSAS
2. SetWindowsHookEx
3. GetAsyncKeyState

Câu 37: Botnet là …

1. Một tập hợp các hacker thực hiện một cuộc tấn công mạng
2. Một tập hợp các máy bị nhiễm mã độc
3. Một tập hợp các máy chủ của hacker

Câu 38: Để xóa một vùng nhớ của một section mã độc có thể sử dụng hàm API nào sau đây?

1. ZwDeleteOfSectionSAS
2. ZwUnmapViewOfSection

Câu 39: Khi mã độc lưu mã thực thi vào phần .rsrc, để thuực thi đoạn mã đó cần phải làm gì?

1. Tải đoạn mã lên RAM và thực thi
2. Mã hóa hoặc giải nén đoạn mã, say đó tải lên RAM
3. Ghi đoạn mã trở lại vào phần .text và thực thi

Câu 40: Mục tiêu của APC injection thường là…

1. cmd.exe
2. WinLogon.exe
3. Svchost.exe

Câu 41: User-Mode Rootkit sử dụng kỹ thuật nào sau đây để thực hiện hành vi độc hại?

1. DAT Hooking
2. IAT Hooking
3. OAT Hooking

Câu 42: Local Hook

1. Chặn bắt và sửa đổi các thông điệp bên trong một tiến trình cục bộ
2. Chặn bắt và sửa đổi các thông điệp được trao đổi giữa các tiến trình khác nhau

Câu 43: Detour là cơ chế mà mã độc có thể lợi dụng để…

1. Thêm các DLL mới vào máy nạn nhân
2. Tải một tệp mã độc mới vào máy nạn nhân
3. Khởi chạy cùng Windows

Câu 44: Để cấp phát vùng nhớ khi tiêm vào tiến trình, mã độc có thể sử dụng hàm API nào sau đây?

1. WriteProcessMemory
2. CreateProcessMemory
3. VirtualAllocEx

Câu 45: Khi leo thang đặc quyền, mã độc có thể sử dụng hàm API nào sau đây?

1. SetWindowsHook
2. SizeofPrivilege
3. SeDebugPrivilege

Câu 46: Để tiến hành thay thế tiến trình mã độc cần làm gì?

1. Trực tiếp thay thế tiến trình
2. Tắt tiến trình mục tiêu và khởi chạy lại tiến trình đó
3. Đưa tiến trình mục tiêu về trạng thái suspended

Câu 47: Các phần mềm độc hại tồn tại trên ổ cứng ở dạng nào?

1. Hợp ngữ
2. Machine code
3. Mã python
4. Mã C

Câu 48: Đoạn mã sau in ra màn hình kết quả gì?



1. Hello! 3, 2, 1.
2. Hello! 1, 2, 3.
3. 3, 2, 1. Hello!

Câu 49: Lệnh JZ thực hiện phụ thuộc vào cờ nào sau đây?

1. TF
2. ZF
3. CF

Câu 50: 0X90 là opcode của lệnh nào?

1. MOV
2. NOP
3. MUL
4. ADD

Câu 51: Trong IDA Pro để chuyển qua lại giữa hai chế độ hiển thị cần sử dụng phím nào?

1. Cách
2. Ctrl
3. Shift

Câu 52: Nếu step-into một lệnh gọi hàm,lệnh tiếp theo ta thấy trên debugger là lệnh nào?

1. Lệnh cuối cùng trong hàm được gọi
2. Lệnh đầu tiên trong hàm được gọi

Câu 53: Các… được dùng để làm điểm dừng thực thi và cho phép ta quan sát trạng thái của chương trình

1. Breaker
2. Breakpoint
3. Broken

Câu 54: Hardware Breakpoint sử dụng … để dừng chương trình

1. Thanh ghi DR10
2. Thanh ghi DR7
3. Thanh ghi DR9

Câu 55: Ollybg là trình gỡ rối

1. Mức người dùng
2. Cả mức người dùng và mức nhân
3. Mức nhân

Câu 56: Gỡ rối là việc … một chương trình khác

1. Dịch ngược và kiểm tra
2. Thực thi
3. Kiểm tra hoạt động
4. Kiểm tra và thực thi

Câu 57: Loại breakpoint nào thường là breakpoint mặc định trên các trình gỡ rối?

1. Hardware breakpoint
2. Software breakpoint
3. Memory breakpoint

x Câu 58: Khi dùng Software Breakpoint trình gỡ rối sẽ:

1. Ghi đè lệnh 0xCC lên vị trí đặt breakpoint
2. Ghi đè lệnh 0x00 lên vị trí đặt breakpoint
3. Ghi đè lệnh 0x0C lên vị trí đặt breakpoint

Câu 59: Trên ollydbg để đặt software breakpoint cần:

1. Sử dụng phím F2
2. Sử dụng Crtl +B
3. Thao tác trên thanh menu

Câu 60: Phần mềm nào sau đây giúp phòng chống mã độc:

1. IDS
2. Firewall
3. Tất cả các đáp án đều đúng
4. Anti virus

Câu 61: Khi nhận được một email từ địa chỉ lạ người dùng nên:

1. Bỏ qua email đó
2. Xem nội dung email đó
3. Xem nội dung email và các tệp đính kèm

Câu 62: Trong mạng nội bộ cần hạn chế sử dụng:

1. Các tệp tin nén
2. Thiết bị lưu trữ di động
3. Các chương trình soạn thảo văn bản

Câu 63: Để phòng tránh mã độc, khi người dùng muốn có quyền truy cập Internet cần:

1. Đăng ký và được công ty cho phép
2. Có thể sử dụng mạng Internet bất cứ lúc nào

Câu 64: Mã nhận dạng mã độc là gì?

1. Là một đoạn mã đặc biệt nằm trong mã độc mà dựa vào đó có thể phân biệt được nó và các tệp tin khác
2. Là mã hàm băm của mã độc

Câu 65: Phương pháp phát hiện dựa trên dấu hiệu giúp phát hiện:

1. Các mẫu mã độc đã biết
2. Các mẫu mã độc chưa biết
3. Các mẫu mã độc đã hoặc chưa biết

Câu 66: Để phục hồi hệ thống từ sự cố mã độc nhanh chóng cần

1. Xây dựng bản sao lưu sạch
2. Xây dựng bộ phần mềm cần thiết
3. Cài đặt các bản vá hệ thống

Câu 67: Sau sự cố mã độc công ty cần:

1. Thay đổi mật khẩu các tài khoản quản trị, tài khoản người dùng
2. Triển khai lại chính sách an toàn đã xây dựng
3. Cài đặt lại hệ thống về trạng thái như trước khi xảy ra

Câu 68: Tài nguyên dùng để phân tích sự cố là …

1. Hàm băm của các tệp tin văn bản trong hệ thống
2. Tệp tin cấu hình máy tính người dùng
3. Sơ đồ mạng

Câu 69: Dấu hiệu sự cố mã độc có thể là …

1. Hệ thống IDS phát cảnh báo tấn công mạng
2. Máy tính người dùng đột ngột chạy chậm
3. Tất cả đáp án đều đúng
4. VNCert gửi đến các cảnh báo về mã độc

Câu 70: Giai đoạn ban đầu của phản ứng sự cố mã độc cần chuẩn bị…

1. Quy trình xử lý sự cố mã độc
2. Các mẫu mã độc
3. Các bản ghi chép, báo cáo sự cố

**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 mã 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**

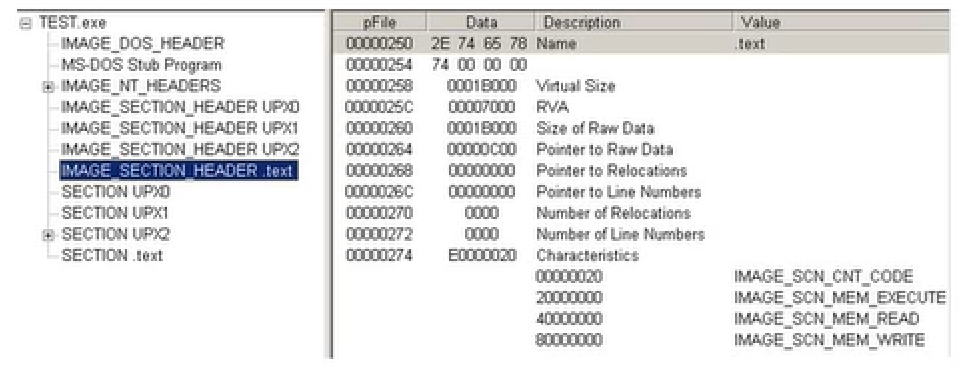
1. Ring 0
2. Ring 2
3. Ring 3
4. Ring 1

**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 thống 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 bí mật, tính toàn vẹn hoặc tính sẵn sàng của dữ liệu và ứng dụng thực thi trên hệ thống.

(D) Các chương trình máy tính được tạo ra với mục đích 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.

**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 động, 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 thể 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**

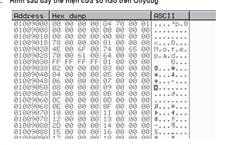
A. File LSASS

B. File NTLM

C. File LSA

D. File SAM

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

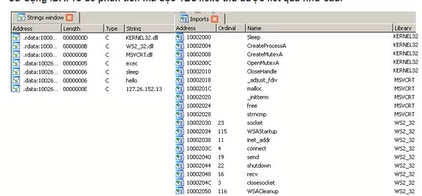


1. String window
2. Data window
3. Memory dump window
4. Address window

**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 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 nhấn phím của người dùng:**

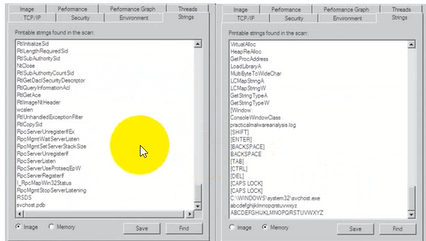
(A)LoadWindowsHookEx

(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 tại:

(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 mã độc 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:**

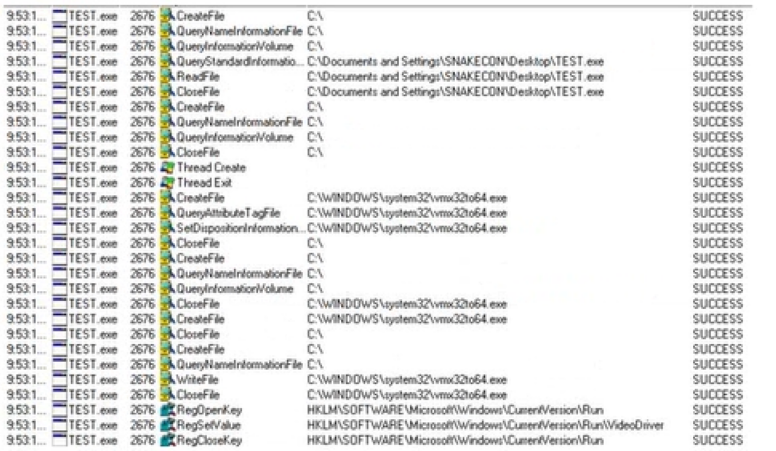
A Ntdll.dll

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 chính nó vào thư mục C:\\WINDOWS\System32 với tên vmx32to64.exe

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

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