

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

- A. Một máy thực thi mã độc, một máy giả lập IDS server
- B. Một máy thực thi mã độc, một IDS server
- C. Một máy thực thi mã độc, một DNS Server
- D. Một máy thực thi mã độc một máy giả lập DNS sever

2. Runtime Linking thường được sử dụng trong:

- A. Các worms
- B. Các mã độc hại bị nén hoặc làm rối
- C. Các virus
- D. Các mã độc có khả năng tự sao chép

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

- A. Applnit\_DLLs
- B. Winlogn Notify
- C. ScvHost DLLs
- D. Cả 3 đáp án trên

4. Kỹ thuật phân tích tĩnh là:

- A. Kỹ thuật phân tích mã độc dựa vào các thư viện liên kết của mã độc
- B. Kỹ thuật phân tích mã độc bằng cách nghiên cứu mã dịch ngược của mã độc
- C. Kỹ thuật phân tích mã độc mà không cần phải thực thi mã độc
- D. Kỹ thuật phân tích mã độc bằng cách nghiên cứu nguồn của mã độc

5. Kernel mode còn được gọi là

- A. Ring 0
- B. Ring 2
- C. Ring 3
- D. Ring 1

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

- A. Kernel32.dll
- B. Memory32.dll
- C. Memory.ll
- D. Kernel dll

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

- A. BKAIV, Kaspersky, Ollydbg
- B. BKAIV, Kaspersky
- C. BKAIV, Kasper, Virus total
- D. AVG, BKAIV, Windbg

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

	pFile	Data	Description	Value
TEST.exe				
IMAGE_DOS_HEADER	00000250	2E 74 65 78	Name	.text
MS-DOS Stub Program	00000254	74 00 00 00		
IMAGE_NT_HEADERS	00000258	0001B000	Virtual Size	
IMAGE_SECTION_HEADER UPX0	0000025C	00007000	RVA	
IMAGE_SECTION_HEADER UPX1	00000260	0001B000	Size of Raw Data	
IMAGE_SECTION_HEADER UPX2	00000264	00000C00	Pointer to Raw Data	
IMAGE_SECTION_HEADER .text	00000268	00000000	Pointer to Relocations	
SECTION UPX0	0000026C	00000000	Pointer to Line Numbers	
SECTION UPX1	00000270	0000	Number of Relocations	
SECTION UPX2	00000272	0000	Number of Line Numbers	
SECTION .text	00000274	E0000020	Characteristics	
		00000020	IMAGE_SCN_CNT_CODE	
		20000000	IMAGE_SCN_MEM_EXECUTE	
		40000000	IMAGE_SCN_MEM_READ	
		80000000	IMAGE_SCN_MEM_WRITE	

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 đúng.

(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,$SizeOf1image,...);  
  
WriteProcessMemory( . . . ,headers , . . . );  
  
for (i=0; i < NumberOfSections; i++) {  
    WriteProcessMemory(...,section,...);  
}  
  
SetThreadContext();  
  
.....  
  
ResumeThread();
```

(A) Tiêm vào trên 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 Resgistry lưu trữ cài đặt cấu hình của hệ điều hành và ứng dụng
- B Repstry có thể tạo kết nối mạng
- C không đáp án nàp đúng
- D Repstry chỉ có một kiểu dữ liệu

Câu 20: ZwUnmapViewO'Section là hàm mã độc sử dụng để

- A Ghi lên vùng nhớ
- B Giải phóng vùng nhớ
- C Huỷ 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 nà trong Olydbg

minh sau đây trình diện cửa sổ nào trên Olydbg

Address	Hex dump	ASCII
01007000	00 00 00 00 04 70 00 01	....'p.0
01007000	00 00 00 00 00 00 00 00	.....
01007010	00 00 00 00 00 00 00 00	.....
01007018	78 00 00 00 01 00 00 00	N...0...
01007020	4E 00 6F 00 74 00 65 00	N..t.e...
01007028	70 00 61 00 64 00 00 00	D..a.d...
01007030	FF FF FF FF 01 00 00 00	0...
01007038	02 00 00 00 03 00 00 00	0...0...
01007040	04 00 00 00 05 00 00 00	0...0...
01007048	06 00 00 00 07 00 00 00	0...0...
01007050	08 00 00 00 09 00 00 00	0...0...
01007058	0A 00 00 00 0B 00 00 00	0...0...
01007060	0C 00 00 00 0D 00 00 00	0...0...
01007068	0E 00 00 00 0F 00 00 00	0...0...
01007070	10 00 00 00 11 00 00 00	0...0...
01007078	12 00 00 00 13 00 00 00	0...0...
01007080	14 00 00 00 15 00 00 00	0...0...
01007088	16 00 00 00 17 00 00 00	0...0...
01007090	18 00 00 00 19 00 00 00	0...0...

- A String window
- (B) Data window
- (C) Memory dump window
- (D) Address window

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

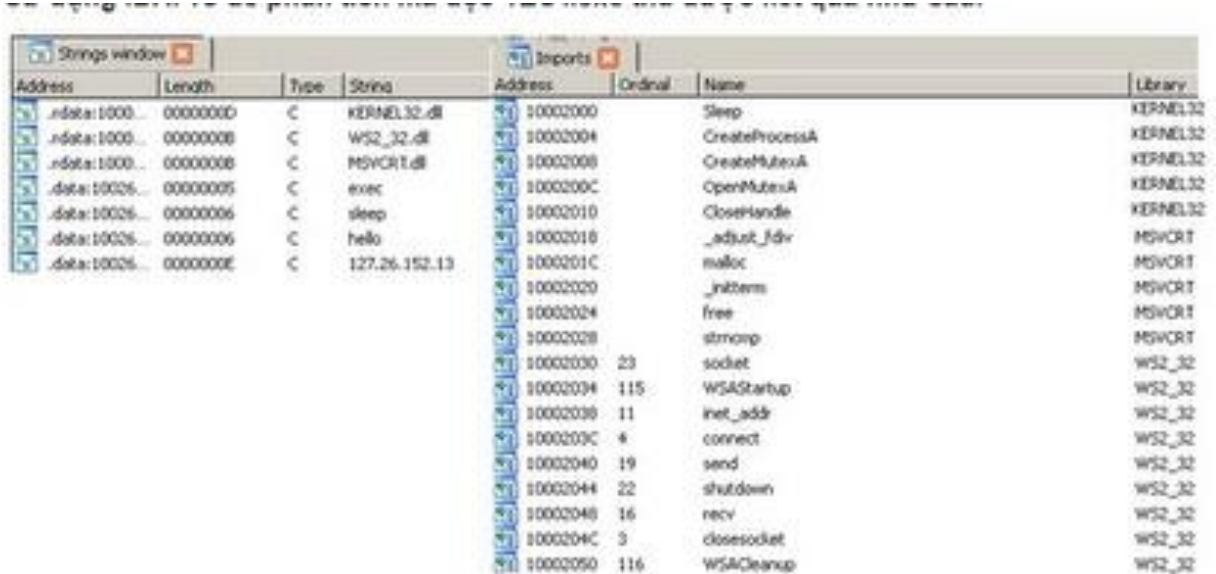
(A)O Spam

(B) Frame

(C) Payload

(D) Exploit

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



Address	Length	Type	String	Address	Ordinal	Name	Library
.idata:1000...	00000000	C	kernel32.dll	10002000		Sleep	kernel32
.idata:1000...	00000000	C	WS2_32.dll	10002004		CreateProcessA	kernel32
.idata:1000...	00000000	C	MSVCRT.dll	10002008		CreateMutexA	kernel32
.data:10026...	00000005	C	exec	1000200C		OpenMutexA	kernel32
.data:10026...	00000006	C	sleep	10002010		CloseHandle	kernel32
.data:10026...	00000006	C	hello	10002018		_adjust_fdiv	MSVCRT
.data:10026...	0000000E	C	127.26.152.13	1000201C		malloc	MSVCRT
				10002020		_initterm	MSVCRT
				10002024		free	MSVCRT
				10002028		strcmp	MSVCRT
				10002030	23	socket	WS2_32
				10002034	115	WSAStartup	WS2_32
				10002038	11	inet_addr	WS2_32
				1000203C	4	connect	WS2_32
				10002040	19	send	WS2_32
				10002044	22	shutdown	WS2_32
				10002048	16	recv	WS2_32
				1000204C	3	closesocket	WS2_32
				10002050	116	WSACleanup	WS2_32

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

(A) Sử dụng thư viện WININET để kết nối tới địa chỉ 127.26.152.13

(B) Thực hiện mã hóa các tập tin trên máy nạn nhân.

(C) sử dụng thư viện Winsock để kết nối tới địa chỉ 127.26.152.13,

(D) . 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 mã độc

(C) Phục hồi sau sự cố

(D) A, B, C

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

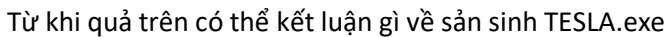
A) Giảm thiểu tác động của phần mềm độc hại

- D) Cả A,B,C

### (A)LoadWindowsHookEx

(C)WindowsHookEx

Câu 28. Phân tích tần trình TESTex thu được kết quả như sau.



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

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

(A) IsDebuggerPresent

(B) CheckRemoteDebuggerPresent

(C) `OutputDebugString`.

Câu 30. Địa chỉ IP 127.0.0.1 được 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 mã 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 tới 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 báo của các hệ thống phòng chống mã độc.

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

(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\Windows NT\CurrentVersion\WinlogonWSGin

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

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

(D) HKLM\SOFTWARE\Microsoft Windows NT\CurrentVersion\Winlogon GinaD

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

A) . Chỉ chạy một tiến trình duy nhất

(B) ít bị mà độc lợi dụng



(C) . Chạy được trong chế độ nhân

(D) Dừng 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 IDApro để phân tích mã đọc test.exe thu được kết quả như sau:

```
00401152 6A 00      push     0           ; dwFlags
00401154 6A 00      push     0           ; lpszProxyBypass
00401156 6A 00      push     0           ; lpszProxy
00401158 6A 01      push     1           ; dwAccessType
0040115A 68 54 30 40 00 push     offset szAgent ; "Internet Explorer 8.0"
0040115F FF 15 74 20 40 00 call     ds:InternetOpen
00401165 8B 3D 70 20 40 00 mov     edi, ds:InternetOpenUrl
0040116B 8B F0      mov     esi, eax
0040116D      loc_40116D:
0040116D      ; CODE XREF: StartAddress+30,j
0040116D 6A 00      push     0           ; dwContext
0040116F 68 00 00 00 00 push     00000000h    ; dwFlags
00401174 6A 00      push     0           ; dwHeadersLength
00401176 6A 00      push     0           ; lpszHeaders
00401178 68 30 30 40 00 push     offset szUrl  ; "http://www.malwareanalysisbook.com"
0040117D 56        push     esi          ; hInternet
0040117E FF 07      call     edi          ; InternetOpenUrl
```

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

- A. 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>
- B. kiểm tra có kết nối Internet hay không gọi tiến trình internet Explorer 8.0 tiến hành kết nối đến địa chỉ <http://www.malwareanalysisbook.com>
- C. kiểm tra có kết nối Internet hay không gọi tiến trình internet Explorer 8.0 tiến hành kết nối đến địa chỉ <http://www.malwareanalysisbook.com>, lặp lại quá trình kết nối
- D. 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 đọc trên môi trường máy ảo cần:

- A Kết nối mạng từ máy ảo đến DNS sever
- B Tạo snapshots cho máy ảo
- C không cần làm gì
- D khởi chạy mã đọc trên máy ảo

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

(A) Broken

**(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, gán 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.

9:53:1...	TEST.exe	2676	CreateFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	QueryNameInformationFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	QueryInformationVolume	C:\	SUCCESS
9:53:1...	TEST.exe	2676	QueryStandardInfo...	C:\Documents and Settings\SNAKECON\Desktop\TEST.exe	SUCCESS
9:53:1...	TEST.exe	2676	ReadFile	C:\Documents and Settings\SNAKECON\Desktop\TEST.exe	SUCCESS
9:53:1...	TEST.exe	2676	CloseFile	C:\Documents and Settings\SNAKECON\Desktop\TEST.exe	SUCCESS
9:53:1...	TEST.exe	2676	CreateFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	QueryNameInformationFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	QueryInformationVolume	C:\	SUCCESS
9:53:1...	TEST.exe	2676	CloseFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	Thread Create		SUCCESS
9:53:1...	TEST.exe	2676	Thread Exit		SUCCESS
9:53:1...	TEST.exe	2676	CreateFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS
9:53:1...	TEST.exe	2676	QueryAttributeTagFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS
9:53:1...	TEST.exe	2676	SetDispositionInfo...	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS
9:53:1...	TEST.exe	2676	CloseFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	CreateFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	QueryNameInformationFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	QueryInformationVolume	C:\	SUCCESS
9:53:1...	TEST.exe	2676	CloseFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS
9:53:1...	TEST.exe	2676	CreateFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS
9:53:1...	TEST.exe	2676	CloseFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	CreateFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	QueryNameInformationFile	C:\	SUCCESS
9:53:1...	TEST.exe	2676	WriteFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS
9:53:1...	TEST.exe	2676	CloseFile	C:\WINDOWS\system32\vmx32to64.exe	SUCCESS
9:53:1...	TEST.exe	2676	RegOpenKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS
9:53:1...	TEST.exe	2676	RegSetValue	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver	SUCCESS
9:53:1...	TEST.exe	2676	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	SUCCESS

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

- A. Sao chép file thực thi của hình 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. Ollydbg, Process Explorer**
- D. ollydbg, PEView

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

- A. F6
- B. F5
- C. F7**
- D. F8

