HỌC VIỆN KTMM
PHÒNG KT&ĐBCLĐT

ĐỀ THI CHÍNH THỨC
(Đề thi có 11 trang)

ĐỀ THI MẪU ĐỂ CÔNG BỐ
Môn thi: MÃ ĐỘC
Thời gian làm bài: 60 phút, không kể thời gian phát đề

Họ, tên thí sinh: .....
Số báo danh: .....

Mã đề thi 461

Câu 1. Người quản trị hệ thống nhận thấy rằng trên hệ thống máy chủ Web của công ty tồn tại một loại mã độc cho phép vượt qua các cơ chế kiểm tra an toàn của hệ thống nhằm tạo điều kiện đăng nhập trái phép vào một chương trình hoặc hệ thống. Mã độc đó thuộc loại mã độc nào sau đây?

A. Worm.
B. Virus.
C. Backdoor.
D. Adware.

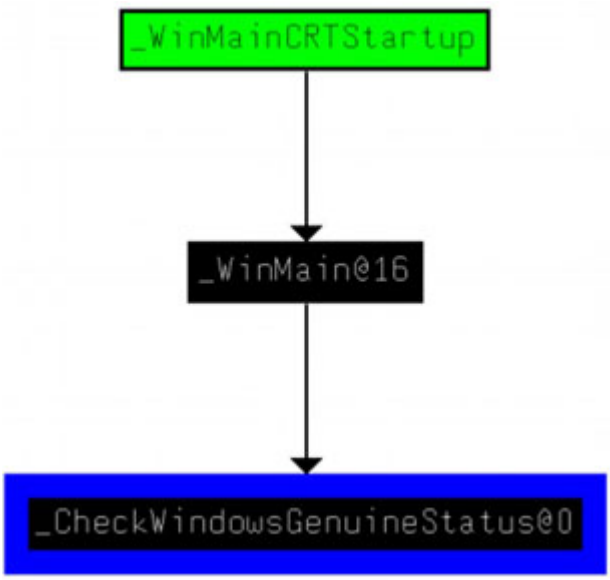
Câu 2. Phân tích mã độc TEST.exe thu được đoạn mã dịch ngược sau:

```
cmp     bl, 80h
jg      short loc_402B1D
```

Mã độc thực hiện nhảy đến hàm loc_402B1D khi _____

A. Giá trị lưu tại thanh ghi bl < 80h.
B. Giá trị lưu tại thanh ghi bl > 80h.
C. Giá trị lưu tại thanh ghi bl = 80h.
D. Giá trị lưu tại thanh ghi bl ≤ 80h.

Câu 3. Trong quá trình phân tích mã độc TEST.exe bằng IDA Pro thu được kết quả như sau.:



Chức năng nào sau đây được người phân tích sử dụng?

A. Xref from _CheckWindowsGenuiseStatus@0.
B. Xref from _WinMain@16.
C. Xref to _CheckWindowsGenuiseStatus@0.
D. Xref to _WinMain@16.

Câu 4. Trong OllyDbg, để thực hiện debug một tiến trình đang chạy cần sử dụng tính năng nào sau đây?

A. Attach Process.
B. Revers Process.
C. Deman Process.
D. Open Process.

Câu 5. Một mã độc bị pack sẽ có đặc điểm nào sau đây?

A. Kích thước của Virtual Size của mã độc lớn hơn nhiều lần so với kích thước của Size of Raw Data.
B. Kích thước của Virtual Size của mã độc bằng kích thước của Size of Raw Data.
C. Kích thước của Virtual Size của mã độc nhỏ hơn nhiều lần so với kích thước của Size of Raw Data.
D. Kích thước của Virtual Size của mã độc gần bằng với kích thước của Size of Raw Data.

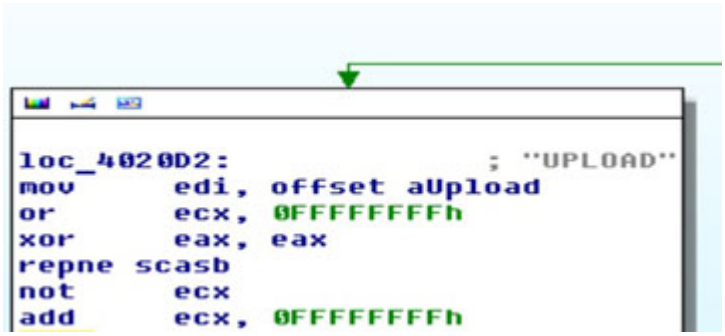
Câu 6. Tại sao trong một số trường hợp nên phân tích mã độc trên máy vật lý?

A. Một số mã độc chỉ thực thi trên máy vật lý.
B. Giúp quá trình phân tích đơn giản hơn.
C. Có thể phân tích các đoạn code bị mã hóa.
D. Có thể theo dõi các thay đổi trên regestry.

Câu 7. Thứ tự gọi các hàm trong quá trình kết nối mạng của server botnet là:

A. socket, listen, bind, accept.
B. socket, accept, bind, listen.
C. socket, bind, listen, accept.
D. listen, accept, bind, socket.

Câu 8. Mũi tên màu xanh lá cây trong chế độ graph mode của IDA Pro biểu diễn _____



A. Hướng thực thi khi điều kiện nhảy là đúng.
B. Lệnh nhảy không điều kiện.
C. Vòng lặp.
D. Hướng thực thi khi điều kiện nhảy là sai.

Câu 9. Trong OllyDbg, để sửa đổi dữ liệu trong cửa sổ Registers người phân tích cần _____

A. Nhấn chuột trái vào giá trị của thanh ghi tương ứng, sau đó nhấn phím Del.
B. Nhấn đúp chuột trái vào giá trị của thanh ghi tương ứng.
C. Nhấn đúp chuột phải vào giá trị của thanh ghi tương ứng.
D. Nhấn chuột trái vào giá trị của thanh ghi tương ứng, sau đó nhấn phím Insert.

Câu 10. _____ là phương pháp phổ biến được sử dụng để xác định định danh (uniquely identify) mã độc

A. Caching.
B. Networking.
C. Dumping.
D. Hashing.

Câu 11. Khi người dùng trong công ty A sử dụng các máy tính của họ để truy cập vào các trang web thì xuất hiện hiện tượng các quảng cáo bật lên liên tục xuất hiện. Sau khi tiến hành điều tra, thấy rằng một trong những trang web mà một người trong công ty đã truy cập vào đã bị nhiễm mã độc và lây nhiễm ra toàn bộ các máy trong phòng. Loại mã độc mà người đó đã bị nhiễm là mã độc nào sau đây?

A. Worm.
B. Adware.
C. Macro virus.
D. Worm mang Adware.

Câu 12. Người phân tích mã độc cần hiểu biết sâu về ngôn ngữ assembly vì _____

A. Họ không có khả năng tiếp cận mã nguồn của mã độc
B. Mã độc khi thực thi được dịch ra mã máy.
C. Mã độc thường được viết bằng ngôn ngữ assembly
D. Các máy tính chạy hệ điều hành Windows là phổ biến nhất

Câu 13. Nâng cao nhận thức người dùng là việc_____

A. 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.
B. Cấp quyền cho người dùng dựa trên nguyên tắc đặc quyền tối thiểu.
C. Đào tạo về các nguy cơ, cách thức phần mềm độc hại xâm nhập vào hệ thống cho người dùng.
D. Hướng dẫn người dùng sử dụng phần mềm Antivirus.

Câu 14. Tính chất nào của Hàm băm được ứng dụng trong phân tích mã độc?

A. Tính nén.
B. Tính kháng va chạm.
C. Tính kháng tiền ảnh.
D. Tính kháng tiền ảnh thứ hai.

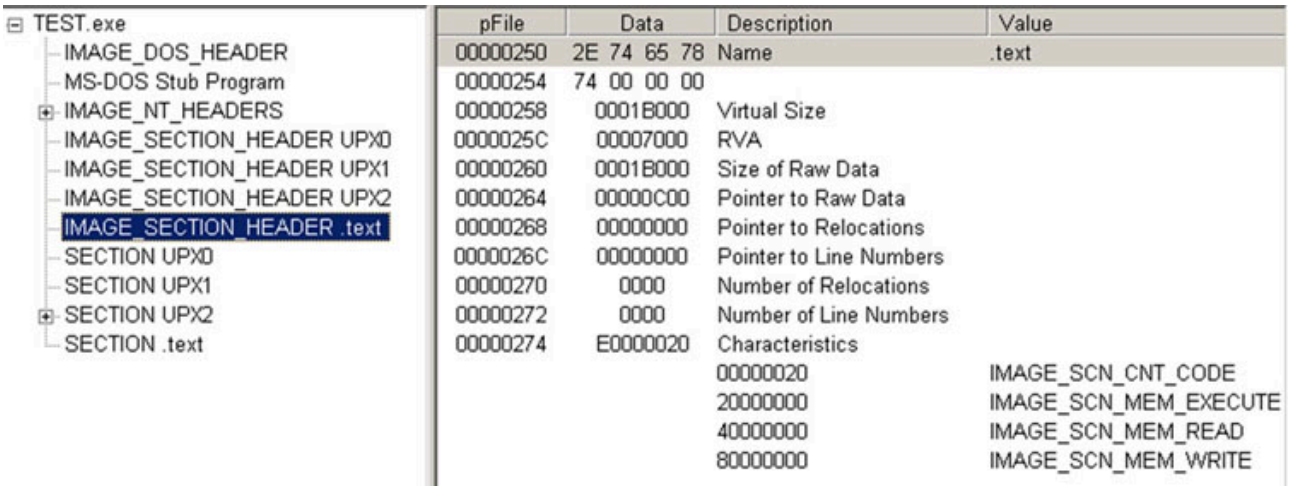
Câu 15. (Những) Biện pháp nào sau đây giúp giảm thiểu nguy cơ lây nhiễm mã độc?

A. Vô hiệu hóa, gỡ bỏ những phần mềm soạn thảo văn bản.
B. Vô hiệu hoá cơ chế tự động thực thi các tệp tin nhị phân và các tệp tin scripts.
C. Loại bỏ những tập tin chia sẻ.
D. Cả A, B, C.

Câu 16. Trong PE Header trường VirtualSize trong thông tin về một section cho biết điều gì?

A. Kích thước của section đó khi lưu trên ổ đĩa cứng.
B. Kích thước của section đó khi tải lên bộ nhớ.
C. Kích thước của section đó khi truyền qua mạng.
D. Kích thước của section đó khi lưu trên đĩa CD.

Câu 17. Dùng PEView đọc thông tin của một tệp tin cho ra kết quả như hình sau.



Chọn phát biểu đúng nhất về kết quả phân tích?

A. Là một tệp tin thực thi được pack bằng UPX nhưng không nén.

B. Là một tệp tin thực thi được pack bằng UPX ba lần.

C. Là một tệp tin thực thi được pack bằng UPX 2.0.

D. Là một tệp tin thực thi được pack bằng UPX.

Câu 18. Kỹ thuật phân tích động là:

A. Kỹ thuật phân tích mã độc bằng trình gỡ rối.

B. Kỹ thuật phân tích mã độc thông qua các hành vi của mã độc.

C. Kỹ thuật phân tích mã độc bằng cách thực thi mã độc và theo dõi hoạt động của chúng.

D. Kỹ thuật phân tích mã độc bằng thực thi mã độc trong sandbox.

Câu 19. Phân tích một mã độc thu được đoạn mã sau đây. Từ đoạn mã nãy có thể dự đoán mã độc thực hiện hành động gì?

```
00401100        push    esi
00401101        push    edi
00401102        push    offset LibFileName ; "hook.dll"
00401107        call    LoadLibraryA
0040110D        mov     esi, eax
0040110F        push    offset ProcName ; "MalwareProc"
00401114        push    esi             ; hModule
00401115        call    GetProcAddress
0040111B        mov     edi, eax
0040111D        call    GetNotepadThreadId
00401122        push    eax             ; dwThreadId
00401123        push    esi             ; hmod
00401124        push    edi             ; lpfn
00401125        push    WH_CBT   ; idHook
00401127        call    SetWindowsHookExA
```

A. Khởi động tiến trình hook.dll.

B. Ghi mã thực thi vào vùng nhớ của tiến trình Notepad.

C. Ghi mã thực thi vào thư viện hook.dll.

D. Tiêm vào hook.

Câu 20. Phân tích một mã độc thu được đoạn mã sau đây. Từ đoạn mã nãy có thể phỏng đoán mã độc đã thực hiện cơ chế gì sau đây?

```
00403594        mov     eax, large fs:30h
0040359A        db      3Eh
0040359A        mov     eax, [eax+68h]
0040359E        sub     eax, 70h
004035A1        mov     [ebp+var_1828], eax
004035A7        cmp     [ebp+var_1828], 0
004035AE        jnz     short loc_4035B5
004035B0        call    sub_401000
```

A. Checksum checks.

B. Anti-Debugging.

C. Timing checks.

D. Anti-VM.

Câu 21. Những phát biểu nào sau đây đúng về Backdoor?

A. B và D đúng.

B. Tạo một cửa hậu cho phép kẻ tấn công kết nối tới máy tính nạn nhân.

C. Xóa các tệp tin hệ thống trên máy tính nạn nhân.

D. Cho phép kẻ tấn công sao chép dữ liệu từ máy tính nạn nhân.

Câu 22. Wannacry là mã độc thuộc loại nào sau đây?

A. Backdoor. **B**. Virus. **C**. Ransomware. **D**. Botnet.

Câu 23. Một nhân viên phát triển phần mềm đã viết một chương trình có khả năng kết nối với phòng chat và chờ nhận lệnh thu thập thông tin người dùng cá nhân. Anh ta nhúng chương trình này vào bộ cài của phần mềm office và chia sẻ tệp này trên mạng chia sẻ tệp P2P. Chương trình này được gọi là:

A. Logic Bomb.
B. Trojan.
C. Worm.
D. Bot.

Câu 24. Macro virus là loại mã độc thường lây nhiễm vào tệp tin nào sau đây?

A. Tệp .exe
B. Tệp .doc
C. Tệp .cap
D. Tệp .bat

Câu 25. Phân tích mã độc thu được kết quả như sau:

```
40CB08: found const array Rijndael_Te0 (used in Rijndael)
40CF08: found const array Rijndael_Te1 (used in Rijndael)
40D308: found const array Rijndael_Te2 (used in Rijndael)
40D708: found const array Rijndael_Te3 (used in Rijndael)
40DB08: found const array Rijndael_Td0 (used in Rijndael)
40DF08: found const array Rijndael_Td1 (used in Rijndael)
40E308: found const array Rijndael_Td2 (used in Rijndael)
40E708: found const array Rijndael_Td3 (used in Rijndael)
Found 8 known constant arrays in total.
```

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

A. Mã độc có sử dụng mã hóa AES.
B. Mã độc có sử dụng mã hóa XOR.
C. Mã độc có sử dụng mã hóa RC4.
D. Mã độc có sử dụng mã hóa RSA.

Câu 26. Mã độc có thể sử dụng hàm InternetOpen để làm công việc nào sau đây?

A. Kết nối đến một trang web.
B. Khởi tạo cấu trúc dữ liệu chuẩn bị cho kết nối.
C. Mở một kết nối HTTPS.
D. Mở một tệp tin trên Internet.

Câu 27. Phân tích mã độc TEST.exe thu được đoạn mã dịch ngược sau:

```
00401004        mov         [ebp+var_4], 0
0040100B        jmp         short loc_401016
0040100D  loc_40100D:
0040100D        mov         eax, [ebp+var_4]
00401010        add             eax, 1
00401013        mov         [ebp+var_4], eax
00401016  loc_401016:
00401016        cmp         [ebp+var_4], 64h
0040101A        jge         short loc_40102F
0040101C        mov           ecx, [ebp+var_4]
0040101F        push            ecx
00401020        push      offset aID  ; "i equals %d\n"
00401025        call            printf
0040102A        add             esp, 8
0040102D        jmp         short loc_40100D
```

Đoạn mã trên thể hiện mã độc thực hiện công việc nào sau đây?

A. Mã độc thực hiện vòng lặp for.

B. Mã độc thực hiện vòng lặp do-white.

C. Mã độc thực hiện lệnh switch case.

D. Mã độc thực hiện vòng lặp vô hạn.

Câu 28. Các công cụ phân tích mã độc có tính năng gỡ rối là công cụ _____

A. Phân tích tĩnh nâng cao

B. Phân tích động cơ bản

C. Phân tích động nâng cao

D. Phân tích tĩnh cơ bản

Câu 29. Phân tích mã độc TEST.exe thu được đoạn mã dịch ngược sau:

```
mov esp, ebp
pop ebp
ret
```

Phát biểu nào sau đây là đúng?

A. Đây là kết thúc vòng lặp.

B. Đây là bắt đầu vòng lặp.

C. Đây là phần bắt đầu của một hàm

D. Đây là phần kết thúc của một hàm.

Câu 30. Để trích xuất phần .rsrc mã độc cần sử dụng (các) hàm nào sau đây?

A. FindResource. **B**. LoadResource. **C**. SizeofResource. **D**. Cả A, B, C.

Câu 31. Vì sao mã độc thường lây nhiễm vào explorer.exe?

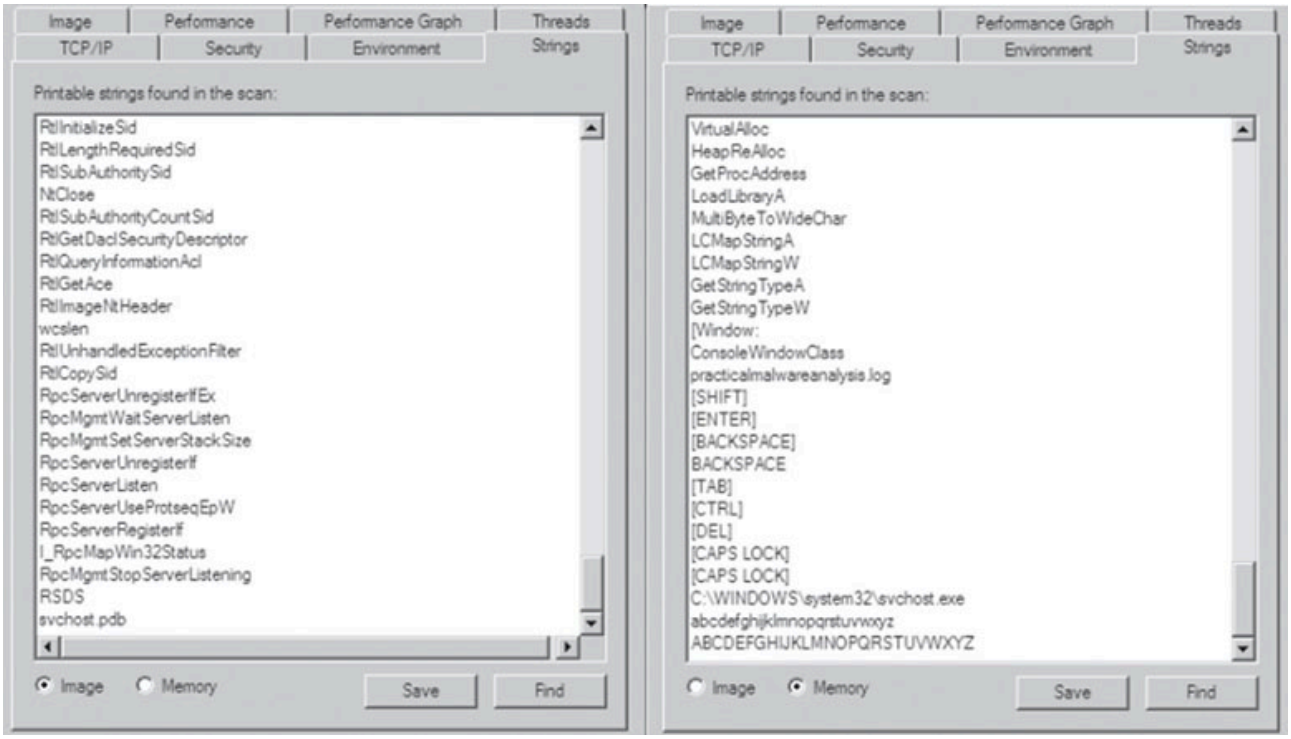
A. Vì explorer.exe rất cần thiết để đảm bảo cho hệ điều hành Windows hoạt động bình thường.

B. Vì nếu khai được explorer.exe hacker sẽ chiếm được quyền điều khiển máy tính nạn nhân.

C. Vì explorer.exe ít không bị hệ điều hành kiểm tra bảo mật.

D. Vì explorer.exe sử dụng cổng 80 để truyền nhận dữ liệu.

Câu 32. Phân tích tiến trình TEST.exe thu được kết quả như sau.



Từ kết quả trên có thể kết luận gì?

A. Tệp tin TEST.exe là một tệp tin lành tính.

B. Tiến trình TEST.exe đã bị thay thế bởi một đoạn mã độc.

C. Tệp tin TEST.exe là một mã độc, cố gắng kết nối đến địa chỉ practicalmalwareanalysis.log.

D. Tệp tin TEST.exe là một mã độc dạng keylog.

Câu 33. Mã độc thường sử dụng cổng nào để kết nối tới máy chủ C&C?

A. Cổng 23.

B. Cổng 43.

C. Cổng 80.

D. Cổng 21.

Câu 34. Sử dụng IDAPro để phân tích mã độc TEST.exe thu được kết quả như sau.

```
void __cdecl sub_401130(char a1, LPCSTR lpExistingFileName)
{
  HKEY phkResult; // [esp+4h] [ebp-4h]

  switch ( a1 )
  {
    case 'a':
      CreateDirectoryA(PathName, 0);            // "C:\\Temp"
      break;
    case 'b':
      CopyFileA(lpExistingFileName, (LPCSTR)Data, 1);// "C:\\Temp\\cc.exe"
      break;
    case 'c':
      DeleteFileA((LPCSTR)Data);
      break;
    case 'd':
      RegOpenKeyExA(HKEY_LOCAL_MACHINE, SubKey, 0, 0xF003Fu, &phkResult);// "Software\\Microsoft\\Windows\\CurrentVersion\\Run"
      if ( RegSetValueExA(phkResult, ValueName, 0, 1u, Data, 0xFu) )// "Malware", "C:\\Temp\\cc.exe"
        printf(aError31CouldNo);                // "Error 3.1: Could not set Registry value"
      break;
    case 'e':
      Sleep(100000u);
      break;
    default:
      printf(aError32NotAVal);
      break;
  }
}
```

Hàm sub_401130 của mã độc TEST.exe thực hiện những hành động gì sau đây?

A. Một trong các hành động: Tạo thư mục C:\Temp, Tạo file C:\Temp\cc.exe, Xóa các tệp tin dữ liệu trên máy, Mở subkey tại Software\Microsoft\Windows\CurrentVersion\Run, thêm một value mới là "Malware" và đặt giá trị cho key đó là "C:\Temp\cc.exe", Sleep 10 giây, Báo lỗi Error 3.2

B. Một trong các hành động: Tạo thư mục C:\Temp, Tạo file C:\Temp\cc.exe, Xóa file C:\Temp\cc.exe, Mở subkey tại Software\Microsoft\Windows\CurrentVersion\Run, thêm một value mới là "Malware" và đặt giá trị cho key đó là "C:\Temp\cc.exe", Sleep 10 giây, Báo lỗi Error 3.2.

C. Một trong các hành động: Tạo thư mục C:\Temp, Tạo file C:\Temp\cc.exe, Xóa các tệp tin dữ liệu trên máy, Mở subkey tại Software\Microsoft\Windows\CurrentVersion\Run, thêm một value mới là "Malware" và đặt giá trị cho key đó là "C:\Temp\cc.exe", Sleep 100 giây, Báo lỗi Error 3.2.

D. Một trong các hành động: Tạo thư mục C:\Temp, Tạo file C:\Temp\cc.exe, Xóa file C:\Temp\cc.exe, Mở subkey tại Software\Microsoft\Windows\CurrentVersion\Run, thêm một value mới là "Malware" và đặt giá trị cho key đó là "C:\Temp\cc.exe", Sleep 100 giây, Báo lỗi Error 3.2.

Câu 35. Sử dụng các naitive api giúp mã độc _____

A. Tương tác với thiết bị ngoại vi.

B. Tắt tiến trình AV.

C. Ẩn tiến trình mã độc.

D. Vượt qua các cơ chế kiểm tra an toàn của hệ thống.

Câu 36. Để phòng chống mã độc cần thực hiện biện pháp nào sau đây?

A. Cung cấp quyền quản trị cho người dùng.

B. Hạn chế hoặc cấm việc sử dụng phần mềm không cần thiết

C. Cấm sử sụng các thiết bị di động.

D. Cả A, B, C.

Câu 37. Công cụ nào sau đây KHÔNG có khả năng xem các chuỗi ký tự trong mã độc?

A. IDA pro
B. Process monitor
C. Process explorer
D. Bintext

Câu 38. Tại sao các trình dịch ngược thường dịch ngược mã độc về dạng hợp ngữ?

A. Vì hợp ngữ là ngôn ngữ gần với ngôn ngữ mà máy tính có thể hiểu được để thực thi.
B. Vì hợp ngữ là ngôn ngữ lập trình phổ biến nhất.
C. Vì kết quả của quá trình dịch ngược là chính xác nhất mà con người vẫn có thể đọc được.
D. Vì mã độc thường được viết bằng hợp ngữ.

Câu 39. Một mã độc bị pack có đặc điểm nào sau đây?

A. Chứa rất ít string.
B. Có kích thước rất nhỏ.
C. Có kích thước rất lớn.
D. Chứa rất nhiều string.

Câu 40. Worms là loại mã độc _____

A. có khả năng tự nhân bản, cần vật chủ để lây nhiễm.
B. không có khả năng tự nhân bản, không cần vật chủ để lây nhiễm.
C. không có khả năng tự nhân bản, cần vật chủ để lây nhiễm.
D. có khả năng tự nhân bản, không cần vật chủ để lây nhiễm.

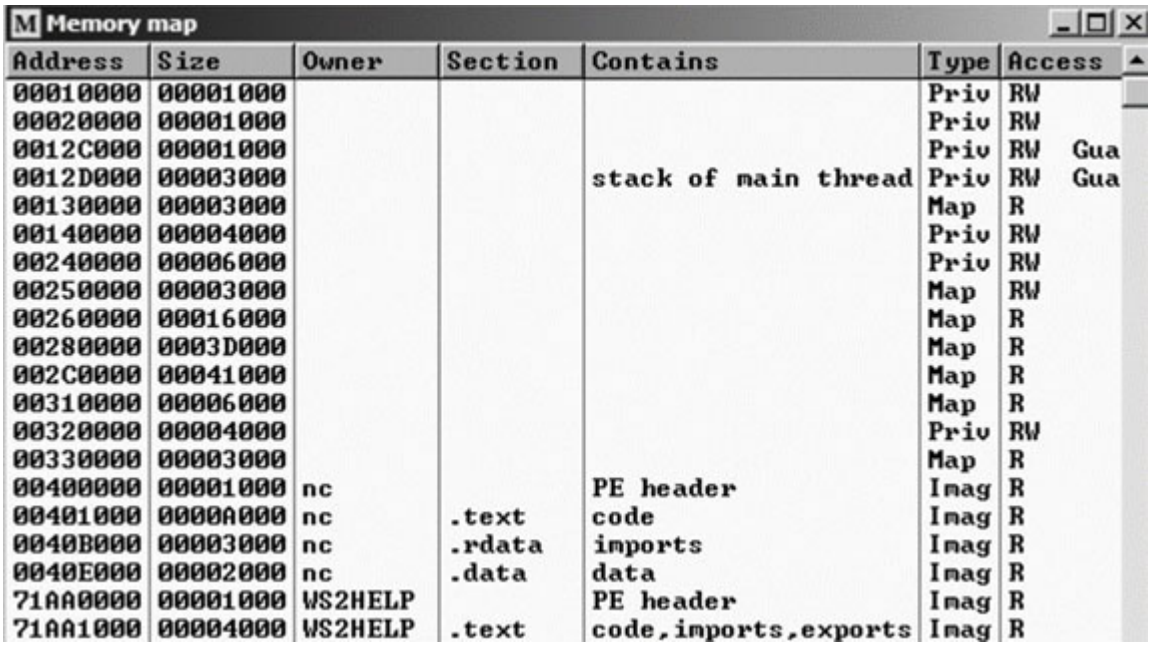
Câu 41. Công cụ nào sau đây cho phép theo dõi hành vi của các tiến trình đang chạy trong thời gian thực?

A. Process explorer.
B. OllyDbg.
C. Process monitor.
D. Regshot.

Câu 42. Vì sao mã độc đăng ký registry key tại mục HKLM\SOFTWARE\MicrosoftWindowsNT\CurrentVersion\Winlogon\Notify?

A. Vì Winlogon service được gọi khi Windows khởi động.
B. Vì Winlogon service không thể khởi chạy trong chế độ Safe mode của Windows.
C. Vì mã độc dễ thực hiện lây nhiễm vào Winlogon service.
D. Vì Winlogon Notify không bị kiểm tra an toàn.

Câu 43. Cửa sổ Memory map trên OllyDbg _____



Memory map

Address	Size	Owner	Section	Contains	Type	Access
00010000	00001000				Priv	RW
00020000	00001000				Priv	RW
0012C000	00001000				Priv	RW Gua
0012D000	00003000			stack of main thread	Priv	RW Gua
00130000	00003000				Map	R
00140000	00004000				Priv	RW
00240000	00006000				Priv	RW
00250000	00003000				Map	RW
00260000	00016000				Map	R
00280000	0003D000				Map	R
002C0000	00041000				Map	R
00310000	00006000				Map	R
00320000	00004000				Priv	RW
00330000	00003000				Map	R
00400000	00001000	nc		PE header	Imag	R
00401000	0000A000	nc	.text	code	Imag	R
0040B000	00003000	nc	.rdata	imports	Imag	R
0040E000	00002000	nc	.data	data	Imag	R
71AA0000	00001000	WS2HELP		PE header	Imag	R
71AA1000	00004000	WS2HELP	.text	code,imports,exports	Imag	R

A. Hiển thị mọi memory block cấp phát cho chương trình được debug.

B. Hiển thị các biến toàn cục và cục bộ của chương trình được debug.

C. Hiển thị các biến cục bộ của chương trình được debug

D. Giúp ta quan sát giá trị các thanh ghi và cờ ở thời điểm hiện tại.

Câu 44. Ứng dụng nào sau đây thực hiện bảo vệ hệ thống trước mã độc trong thời gian thực?

A. Pop-up blocker, Virus total

B. Anti-spyware, Virus total

C. Pop-up blocker, Anti-spyware

D. Pop-up blocker, Anti-spyware, Virus total

Câu 45. TimeDateStamp trong PE Header chỉ ra điều gì?

A. Thời gian tệp tin được viết.

B. Thời gian tệp tin bắt đầu khởi chạy.

C. Tổng thời gian tệp tin đã thực thi.

D. Thời gian tệp tin được biên dịch.

---------- *Hết* ----------