

HỌC VIỆN KỸ THUẬT MẬT MÃ
KHOA AN TOÀN THÔNG TIN

MODULE THỰC HÀNH
MÃ ĐỘC

BÀI THỰC HÀNH SỐ 07

Phân tích một số kỹ thuật khởi chạy của mã độc

Người thực hiện bài thực hành:

TS. Đặng Xuân Bảo

Hà Nội, 2020

MỤC LỤC

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH.....	3
CHUẨN BỊ BÀI THỰC HÀNH.....	4
Phân tích một số kỹ thuật khởi chạy mã độc	5
1.1. Mô tả	5
1.2. Chuẩn bị	5
1.3. Phân tích Lab12-01	5

THÔNG TIN CHUNG VỀ BÀI THỰC HÀNH

Tên bài thực hành: Phân tích một số kỹ thuật khởi chạy của mã độc

Học phần: Mã độc

Số lượng sinh viên cùng thực hiện:

Địa điểm thực hành: Phòng máy

Yêu cầu:

- Yêu cầu phần cứng:
 - + Máy tính với cấu hình tối thiểu: CPU 2.0 GHz, RAM 4GB, HDD 500GB
- Yêu cầu phần mềm trên máy:
 - + Hệ điều hành Windows 10
 - + VMware Workstation 15.0
- Yêu cầu kết nối mạng LAN: có
- Yêu cầu kết nối mạng Internet: có

CHUẨN BỊ BÀI THỰC HÀNH

Đối với giảng viên

Trước buổi học, giảng viên (người hướng dẫn thực hành) cần kiểm tra sự phù hợp của điều kiện thực tế của phòng thực hành với các yêu cầu của bài thực hành.

Ngoài ra không đòi hỏi gì thêm.

Đối với sinh viên

Trước khi bắt đầu thực hành, cần tạo các bản sao của máy ảo để sử dụng. Đồng thời xác định vị trí lưu trữ các công cụ đã chỉ ra trong phần yêu cầu.

Phân tích một số kỹ thuật khởi chạy mã độc

1.1. Mô tả

Bài thực hành hướng dẫn sinh viên sử dụng một số công cụ trong việc phân tích động một số mẫu mã độc đơn giản..

1.2. Chuẩn bị

- Môi trường phân tích mã độc đã xây dựng trong Lab 1.

1.3. Phân tích Lab12-01

Trong bài thực hành này, chúng ta sẽ thực hành file Lab12-1.exe.

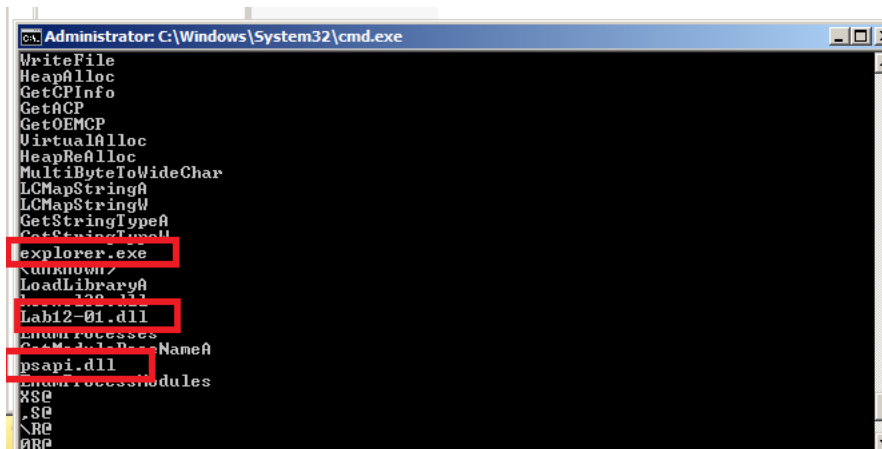
CÔNG CỤ PEVIEW

- Cần chú ý đến những dòng sau, chúng được sử dụng trong quá trình inject mã độc.
 - CreateRemoteThread
 - WriteProcessMemory
 - VirtualAllocEx

pFile	Data	Description	Value
00005000	0000552C	Hint/Name RVA	001B CloseHandle
00005004	0000553A	Hint/Name RVA	01EF OpenProcess
00005008	00005548	Hint/Name RVA	0046 CreateRemoteThread
0000500C	0000555E	Hint/Name RVA	0126 GetModuleHandleA
00005010	00005572	Hint/Name RVA	02E9 WriteProcessMemory
00005014	00005588	Hint/Name RVA	02BC VirtualAllocEx
00005018	0000559A	Hint/Name RVA	02F9 IsntCapiA
0000501C	000055A6	Hint/Name RVA	00F5 GetCurrentDirectoryA
00005020	000055BE	Hint/Name RVA	013E GetProcAddress
00005024	000055D0	Hint/Name RVA	01C2 LoadLibraryA
00005028	000055EE	Hint/Name RVA	00CA GetCommandLineA
0000502C	00005600	Hint/Name RVA	0174 GetVersion
00005030	0000560E	Hint/Name RVA	007D ExitProcess
00005034	0000561C	Hint/Name RVA	029E TerminateProcess
00005038	00005630	Hint/Name RVA	00F7 GetCurrentProcess
0000503C	00005644	Hint/Name RVA	02AD UnhandledExceptionFilter
00005040	00005660	Hint/Name RVA	0124 GetModuleFileNameA
00005044	00005676	Hint/Name RVA	00B2 FreeEnvironmentStringsA
00005048	00005690	Hint/Name RVA	00B3 FreeEnvironmentStringsW
0000504C	000056AA	Hint/Name RVA	02D2 WideCharToMultiByte
00005050	000056C0	Hint/Name RVA	0106 GetEnvironmentStrings
00005054	000056D8	Hint/Name RVA	0108 GetEnvironmentStringsW
00005058	000056F2	Hint/Name RVA	026D SetHandleCount
0000505C	00005704	Hint/Name RVA	0152 GetStdHandle
00005060	00005714	Hint/Name RVA	0115 GetFileType
00005064	00005722	Hint/Name RVA	0150 GetStartupInfoA
00005068	00005734	Hint/Name RVA	0109 GetEnvironmentVariableA
0000506C	0000574E	Hint/Name RVA	0175 GetVersionExA
00005070	0000575E	Hint/Name RVA	019D HeapDestroy
00005074	0000576C	Hint/Name RVA	019B HeapCreate
00005078	0000577A	Hint/Name RVA	01BE VirtualFree

CÔNG CỤ STRING

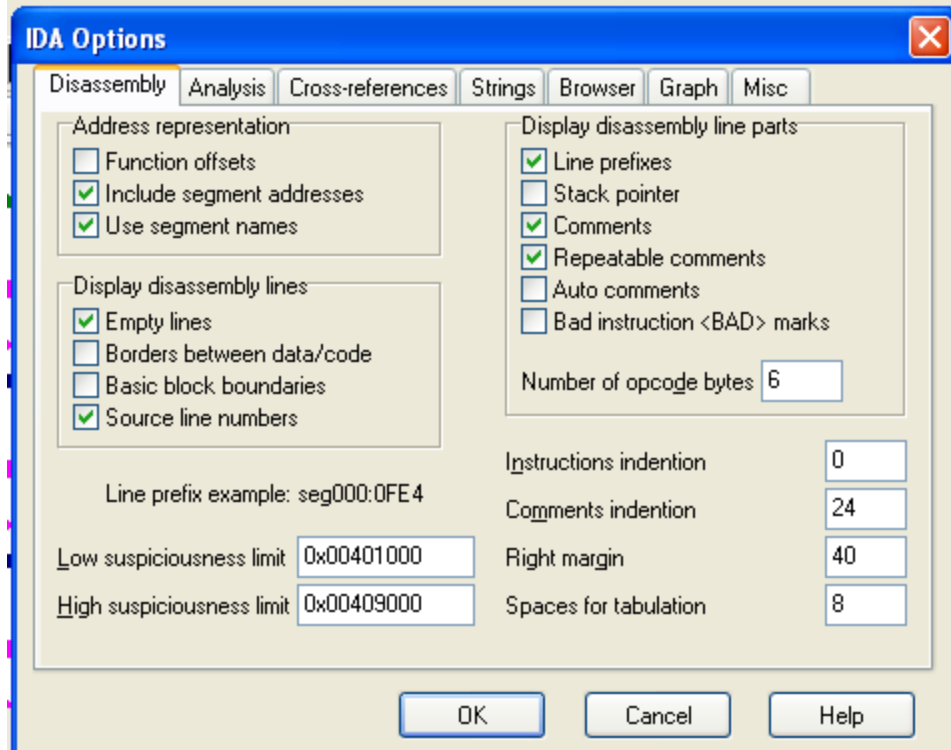
- Sử dụng string để kiểm tra các chuỗi trong file Lab12-1.
- Tìm ba chuỗi sau đây, cho thấy quá trình tiêm các chuỗi này, tệp DLL và psapi được sử dụng để liệt kê quy trình.
 - Explorer.exe
 - Lab12-01.dll
 - Psapi.dll



```
Administrator: C:\Windows\System32\cmd.exe
WriteFile
HeapAlloc
GetCPInfo
GetACP
GetOEMCP
VirtualAlloc
HeapReAlloc
MultiByteToWideChar
LCMapStringA
LCMapStringW
GetStringTypeA
GetStringTypeW
explorer.exe
LoadLibraryA
Lab12-01.dll
psapi.dll
NameA
ProcessModules
x32
x64
x86
x86_64
```

CÔNG CỤ IDA PRO

- Mở file Lab12-01 trong IDA Pro, chọn Option, General, tích Line Prefixes và chỉnh Number of opcode bytes thành 6.



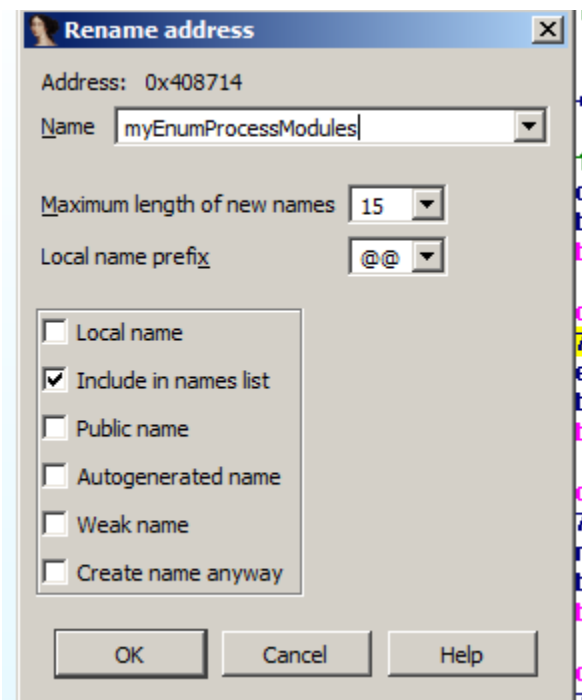
- Tìm những đoạn code sau, chúng ở gần hàm main()

```

004010E8 mov     eax, eax
004010EA mov     [ebp+var_110], eax
004010F0 mov     [ebp+var_10C], eax
004010F6 mov     [ebp+var_108], eax
004010FC mov     [ebp+var_1178], 44h
00401106 mov     ecx, 10h
00401108 xor     eax, eax
0040110D lea     edi, [ebp+var_1174]
00401113 rep stosd
00401115 mov     [ebp+var_118], 0
0040111F push    offset ProcName ; "EnumProcessModules"
00401124 push    offset LibFileName ; "psapi.dll"
00401129 call    ds:LoadLibraryA
0040112F push    eax ; hModule
00401130 call    ds:GetProcAddress
00401136 mov     dword_408714, eax
0040113B push    offset aGetmodulebasen ; "GetModuleBaseNameA"
00401140 push    offset LibFileName ; "psapi.dll"
00401145 call    ds:LoadLibraryA
00401148 push    eax ; hModule
0040114C call    ds:GetProcAddress
00401152 mov     dword_40870C, eax
00401157 push    offset aEnumprocesses ; "EnumProcesses"
0040115C push    offset LibFileName ; "psapi.dll"
00401161 call    ds:LoadLibraryA
00401167 push    eax ; hModule
00401168 call    ds:GetProcAddress
0040116E mov     dword_408710, eax
00401173 lea     ecx, [ebp+Buffer]
00401179 push    ecx ; lpBuffer
0040117A push    104h ; nBufferLength
0040117F call    ds:GetCurrentDirectoryA
00401185 push    offset String2 ; ""
0040118A lea     edx, [ebp+Buffer]
00401190 push    edx ; lpString1
00401191 call    ds:lstrcatA

```

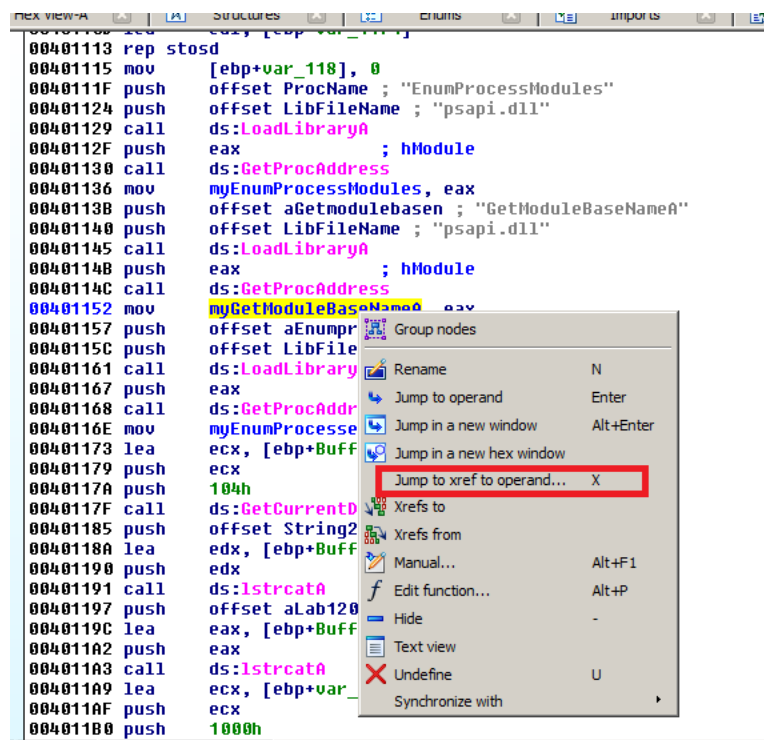
- Mã này sử dụng psapi ba lần để định vị hàm Windows API và lưu địa chỉ của trong một địa chỉ số. Điều này làm xáo trộn mã, vì vậy những lệnh gọi sau này đến các chức năng này sẽ khó nhận ra.
- Bạn cần gán nhãn cho các địa chỉ bộ nhớ này trong IDA Pro để giúp sau này phân tích dễ dàng hơn.
- Phần đầu tiên của mã gán một con trỏ cho hàm EnumProcessModules.
 - Ở dòng có địa chỉ 00401136, nhấp chuột phải vào dword_408714 và nhấp rename.
 - Nhập vào Name một tên mới là myEnumProcessModules, rồi nhấp Ok



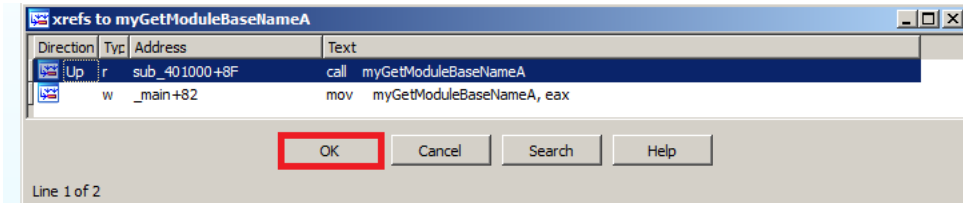
- Làm tương tự với dword_40870C đổi thành myGetModulesBaseA
- Làm tương tự với dword_408710 đổi thành myEnumProcess


```
00401113 rep stosd
00401115 mov [ebp+var_118], 0
0040111F push offset ProcName ; "EnumProcessModules"
00401124 push offset LibFileName ; "psapi.dll"
00401129 call ds:LoadLibraryA
0040112F push eax ; hModule
00401130 call ds:GetProcAddress
00401136 mov myEnumProcessModules, eax
00401138 push offset aGetModulebasen ; "GetModuleBaseNameA"
00401140 push offset LibFileName ; "psapi.dll"
00401145 call ds:LoadLibraryA
00401148 push eax ; hModule
0040114C call ds:GetProcAddress
00401152 mov myGetModuleBaseNameA, eax
00401157 push offset aEnumProcesses ; "EnumProcesses"
0040115C push offset LibFileName ; "psapi.dll"
00401161 call ds:LoadLibraryA
00401167 push eax ; hModule
00401168 call ds:GetProcAddress
0040116E mov myEnumProcesses, eax
00401173 lea ecx, [ebp+Buffer]
00401179 push ecx ; lpBuffer
0040117A push 104h ; nBufferLength
0040117F call ds:GetCurrentDirectoryA
00401185 push offset String2 ; "\\\"
0040118A lea edx, [ebp+Buffer]
00401190 push edx ; lpString1
00401191 call ds:lstrcatA
00401197 push offset aLab1201_dll ; "Lab12-01.dll"
0040119C lea eax, [ebp+Buffer]
004011A2 push eax ; lpString1
004011A3 call ds:lstrcatA
004011A9 lea ecx, [ebp+var_1120]
004011AF push ecx
004011B0 push 1000h
```

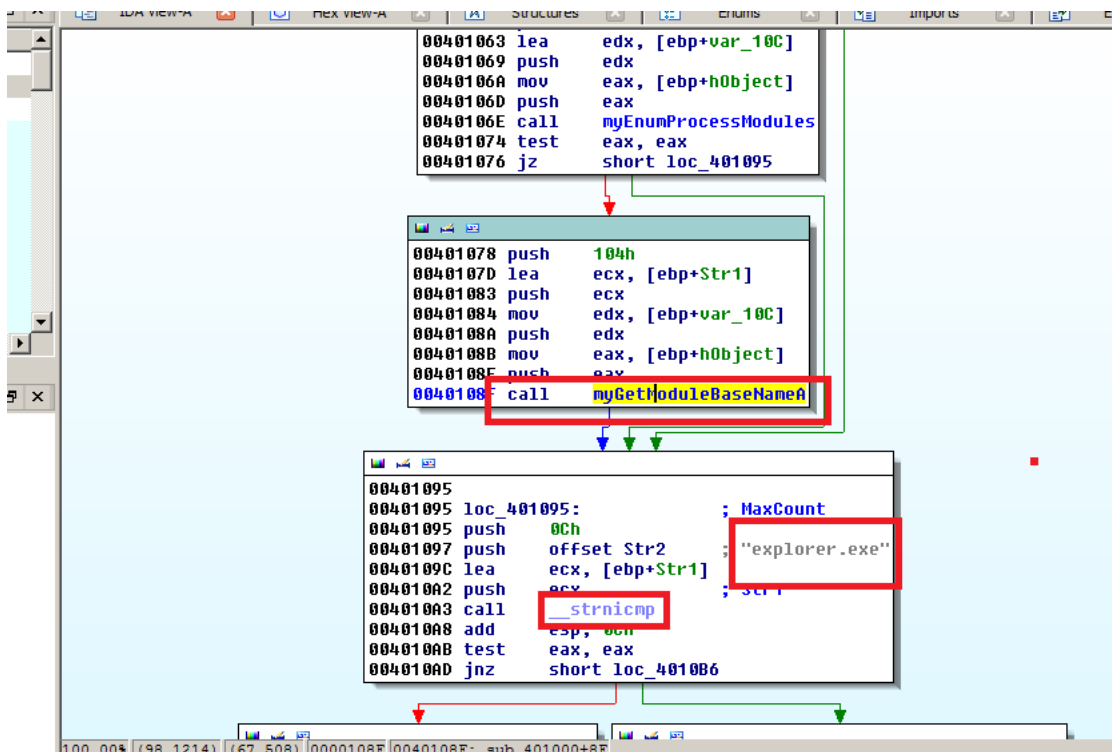
- Nhấp chuột phải vào myGetModulesBaseNameA, chọn Jump tp xrefs of operand.



- Xrefs hiện lên, có hình như bên dưới, cho thấy địa chỉ này chỉ được sử dụng một lần, ở sub_401000. Sau đó chọn OK



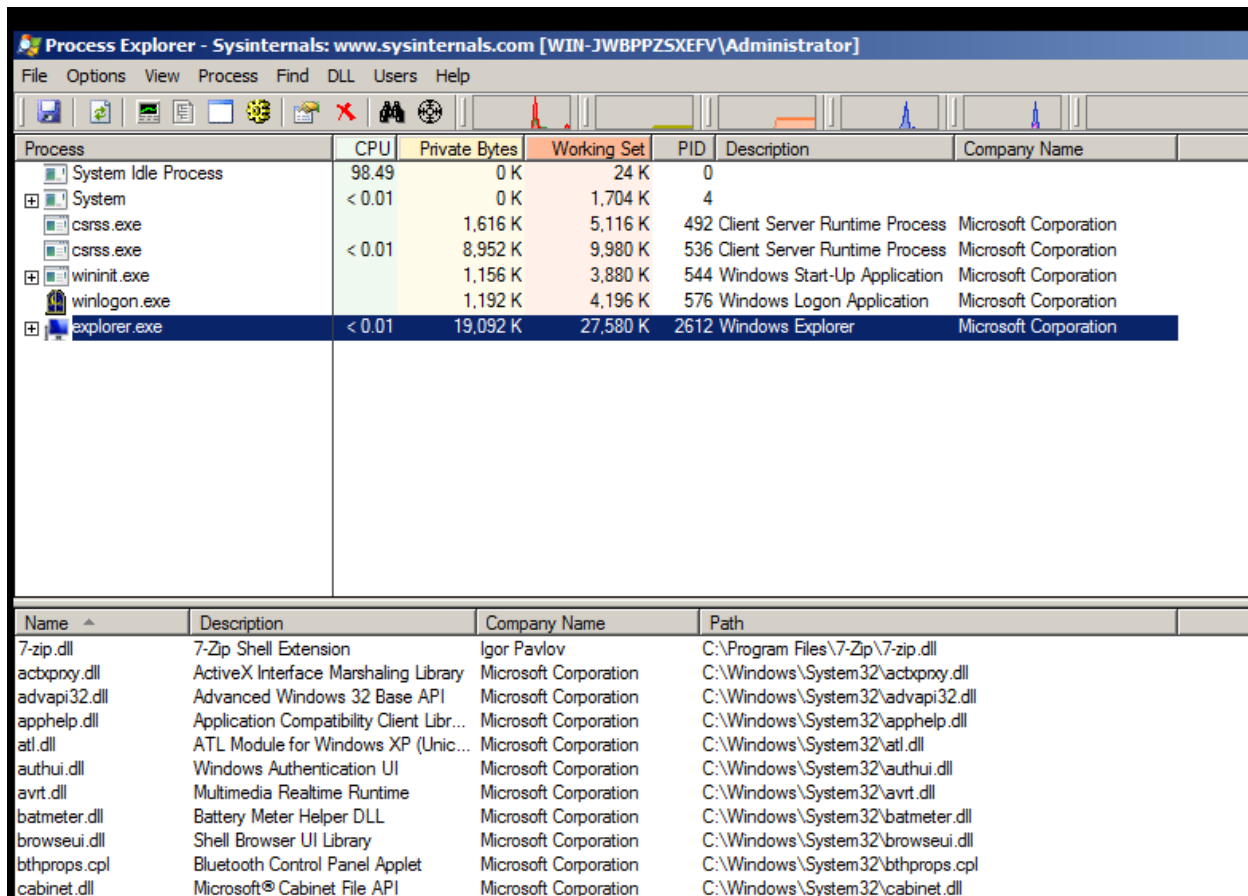
- Ở đây liệt kê các modules và so sánh từng tên modules với explorer.exe, để tìm được modules đã tiêm.
- Chắc chắn rằng bạn thấy ba mục sau:
 - call myGetModuleBaseA
 - “explorer.exe”
 - call __strnicmp



CÔNG CỤ PROCESS EXPLORER

- Giới thiệu công cụ Process Explorer:

- Process Explorer có chức năng quản lý các tiến trình chạy trên Windows. Kết quả của tiến trình quét sẽ hiển thị ngay trên giao diện của phần mềm.
- Giao diện của Process Explorer:

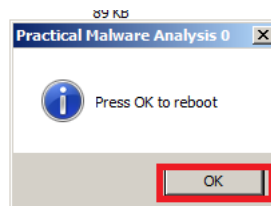


The screenshot shows the Process Explorer application window. The top menu bar includes File, Options, View, Process, Find, DLL, Users, and Help. The main window is divided into two panes. The top pane displays a list of running processes with columns for Process, CPU, Private Bytes, Working Set, PID, Description, and Company Name. The bottom pane displays a list of loaded DLLs with columns for Name, Description, Company Name, and Path.

Process	CPU	Private Bytes	Working Set	PID	Description	Company Name
System Idle Process	98.49	0 K	24 K	0		
System	< 0.01	0 K	1,704 K	4		
csrss.exe		1,616 K	5,116 K	492	Client Server Runtime Process	Microsoft Corporation
csrss.exe	< 0.01	8,952 K	9,980 K	536	Client Server Runtime Process	Microsoft Corporation
wininit.exe		1,156 K	3,880 K	544	Windows Start-Up Application	Microsoft Corporation
winlogon.exe		1,192 K	4,196 K	576	Windows Logon Application	Microsoft Corporation
explorer.exe	< 0.01	19,092 K	27,580 K	2612	Windows Explorer	Microsoft Corporation

Name	Description	Company Name	Path
7-zip.dll	7-Zip Shell Extension	Igor Pavlov	C:\Program Files\7-Zip\7-zip.dll
actxproxy.dll	ActiveX Interface Marshaling Library	Microsoft Corporation	C:\Windows\System32\actxproxy.dll
advapi32.dll	Advanced Windows 32 Base API	Microsoft Corporation	C:\Windows\System32\advapi32.dll
apphelp.dll	Application Compatibility Client Libr...	Microsoft Corporation	C:\Windows\System32\apphelp.dll
atl.dll	ATL Module for Windows XP (Unic...	Microsoft Corporation	C:\Windows\System32\atl.dll
authui.dll	Windows Authentication UI	Microsoft Corporation	C:\Windows\System32\authui.dll
avrt.dll	Multimedia Realtime Runtime	Microsoft Corporation	C:\Windows\System32\avrt.dll
batmeter.dll	Battery Meter Helper DLL	Microsoft Corporation	C:\Windows\System32\batmeter.dll
browseui.dll	Shell Browser UI Library	Microsoft Corporation	C:\Windows\System32\browseui.dll
bthprops.cpl	Bluetooth Control Panel Applet	Microsoft Corporation	C:\Windows\System32\bthprops.cpl
cabinet.dll	Microsoft® Cabinet File API	Microsoft Corporation	C:\Windows\System32\cabinet.dll

- Đóng IDA Pro, nhấp đúp Lab12-01 để chạy Malware.
- Một hộp hiện lên, nhấn OK để khởi động lại.



- Mở Process Explorer.

- Trong khung phía trên, cuộn xuống cuối danh sách, nhấp vào explorer để chọn.
- Từ thanh menu, chọn “View”, và đảm bảo “Show Lower Pane” đã được check.
- Trên thanh menu, chọn “View”, chọn “Lower Pane View”, chọn DLLs.
- Trong khung bên dưới, tìm Lab12-01.dll đã được đưa vào explorer.exe, như hình dưới đây.

lsn.exe	1.496 K	3.752 K	644 Local Session Manager Serv...	Microsoft Corporation	
winlogon.exe	1.196 K	4.184 K	576 Windows Logon Application	Microsoft Corporation	
explorer.exe	< 0.01	21.548 K	31.708 K	2644 Windows Explorer	Microsoft Corporation
usched.exe		912 K	2.960 K	2728 Java(TM) Update Scheduler	Oracle Corporation
vmtoolsd.exe	< 0.01	18.368 K	27.628 K	2736 VMware Tools Core Service	VMware, Inc.
PEView.exe		6.068 K	13.836 K	3104 PE/COFF File Viewer	Wayne J. Radburn
cmd.exe		1.564 K	1.960 K	2168 Windows Command Processor	Microsoft Corporation
procexp.exe	1.52	16.564 K	23.980 K	3060 Sysinternals Process Explorer	Sysinternals - www.sysinter...

Name	Description	Company Name	Path
index.dat			C:\Users\Administrator\AppData\Local\Microsoft\Windows...
index.dat			C:\Users\Administrator\AppData\Local\Microsoft\Windows...
IPHLPAPI.DLL	IP Helper API	Microsoft Corporation	C:\Windows\System32\IPHLPAPI.DLL
kernel32.dll	Windows NT BASE API Client DLL	Microsoft Corporation	C:\Windows\System32\kernel32.dll
ksuser.dll	User CSA Library	Microsoft Corporation	C:\Windows\System32\ksuser.dll
Lab12-01.dll			C:\Users\Administrator\Desktop\Practical Malware Analysis ...
loc2008.nls			C:\Windows\System32\loc2008.nls
loc2008.nls			C:\Windows\System32\loc2008.nls
lpk.dll	Language Pack	Microsoft Corporation	C:\Windows\System32\lpk.dll
mlang.dll	Multi Language Support DLL	Microsoft Corporation	C:\Windows\System32\mlang.dll
MMDevAPI.dll	MMDevice API	Microsoft Corporation	C:\Windows\System32\MMDevAPI.dll
mpr.dll	Multiple Provider Router DLL	Microsoft Corporation	C:\Windows\System32\mpr.dll
msasn1.dll	ASN.1 Runtime APIs	Microsoft Corporation	C:\Windows\System32\msasn1.dll
msctf.dll	MSCTF Server DLL	Microsoft Corporation	C:\Windows\System32\msctf.dll
msimg32.dll	GDIEXT Client DLL	Microsoft Corporation	C:\Windows\System32\msimg32.dll
msshqs.dll	Structured Query	Microsoft Corporation	C:\Windows\System32\msshqs.dll
msvcoi.dll	Windows NT CRT DLL	Microsoft Corporation	C:\Windows\System32\msvcoi.dll
NaturalLanguage6.dll	Natural Language Development PI...	Microsoft Corporation	C:\Windows\System32\NaturalLanguage6.dll
netapi32.dll	Net Win32 API DLL	Microsoft Corporation	C:\Windows\System32\netapi32.dll
netapi32.dll	Net Win32 API DLL	Microsoft Corporation	C:\Windows\System32\netapi32.dll