# **Proj 6: IDA Pro (Lab 5-1) (20 pts., 4 images)**

What you need:

- A Windows machine, real or virtual, such as the Windows 2008 Server VM we've been using
- The textbook: "Practical Malware Analysis"

#### **Purpose**

You will practice using IDA Pro.

You should already have the lab files, but if you don't, do this:

### **Downloading the Lab Files**

In a Web browser, go here:

http://practicalmalwareanalysis.com/labs/

Download and unzip the lab files.

#### **Downloading and Installing IDA Pro**

In your Windows machine, open a Web browser and go to

https://www.hex-rays.com/products/ida/support/download\_freeware.shtml

Download "IDA Freeware" and install it.

If that link is down, use this alternate download link:

https://samsclass.info/126/proj/idafree50.exe

#### **Follow the Textbook**

Follow the instructions for **Lab 5-1** in the textbook, questions 1-8, to analyze Lab05-01.dll using only IDA Pro. There are more detailed solutions in the back of the book.

### Opening Lab05-01.dll in IDA Pro

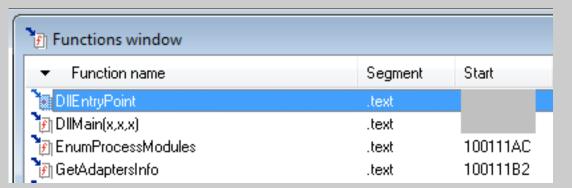
Launch IDA Pro. Click OK. Click New. Click the "PE Dynamic Library" icon and click OK. Navigate to Lab05-01.dll and open it.

#### Q 1: Finding the Address of DLLMain

In IDA Pro, click Windows, "Functions window".

Click the "Function name" header to sort by name and scroll to the top.

Your image should show the location of DLLMain, as shown below:



Press the **PrntScrn** key to capture an image of the whole desktop.

Open Paint and paste the image in with **Ctrl+V**.

Save this image with the filename "Proj 6a from YOUR NAME".

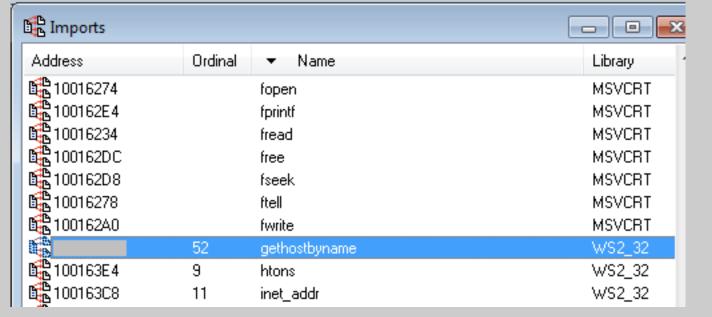
#### YOU MUST SUBMIT WHOLE-DESKTOP IMAGES TO GET FULL CREDIT!

# **Q 2:** Find the import for gethostbyname

In IDA Pro, click **Windows**, **Imports**. Click the **Name** header to sort by name. Find "gethostbyname" -- note that capital letters and lowercase letters sort into separate groups.

Widen the **Address** column to make the entire address visible.

Your image should show the location of gethostbyname, as shown below:



Save a full-desktop image with the filename "Proj 6b from YOUR NAME".

# Q 5: Count Local Variables for the Subroutine at 0x10001656

In IDA Pro, click Windows, "IDA View-A". Press the SPACEBAR to get to text view.

Press  $\mathbf{g}$  to Go. Enter the address  $0\mathbf{x}10001656$  and click  $\mathbf{OK}$ .

Scroll up to show the comments IDA added to the start of the function, listing its local variables, as shown below:

```
.text:10
.text:10
            .text:10
.text:10
.text:10
                    _stdcall sub_10001656(LPV0ID)
            ; DWORD
            sub_10001656
.text:10
                         proc near
                                              ; DATA XREF: DllMain(x,x,x)+C810
.text:10
.text:10
            var 675
                         = byte ptr -675h
                         = dword ptr 4
.text:100
            arg_0
text:100
```

Save a full-desktop image with the filename "Proj 6c from YOUR NAME".

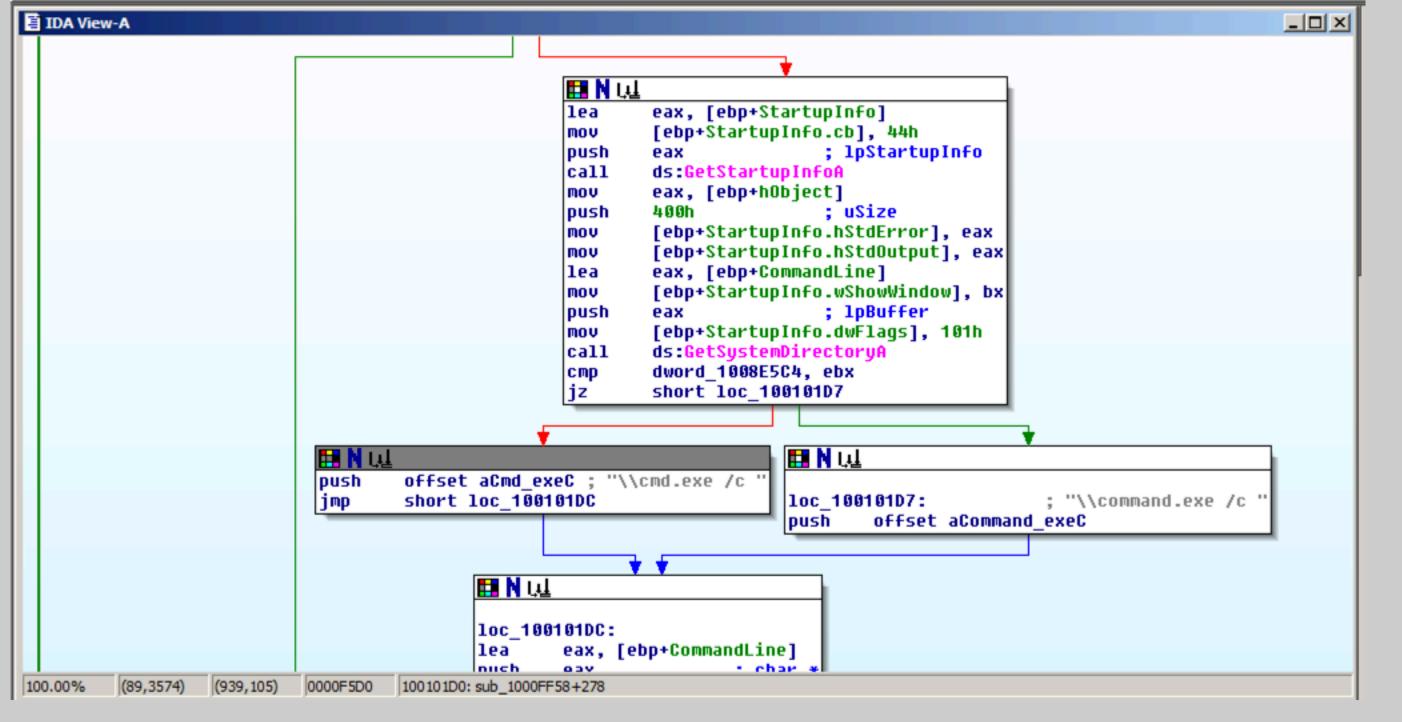
## Q 8: Finding the Purpose of the Code that References \cmd.exe /c

In IDA Pro, click **Windows**, **Strings**. Make the window larger. Sort by **String**. Find the String "\cmd.exe/c" and double-click it. The function opens in text view, as shown below.

In the line containing "\cmd.exe /c", double-click the address to the right of "XREF", as indicated by the red outline in the image below.

```
IDA View-A
                                                                                                                        db 'quit',0
         xdoors d:10095B18 aQuit
                                                                    ; DATA XREF: sub_1000FF58+36FTo
                                            align 10h
         xdoors d:10095B1D
         xdoors d:10095B20 ; char aCommand exeC[]
                                            db '\command.exe /c ',0 ; DATA XREF: sub_1000FF58:loc_100101D7fo
         xdoors d:10095B20 aCommand exeC
         xdoors d:10095B31
                                                                      DATA XREF: sub_1000FF58+278†o
         xdoors d:10095B34 aCmd exeC
                                            db '\cmd.exe /c ',0
         xdoors d:10095B41
                                            align 4
         xdoors_d:10095B44 ; char aHiMasterDDDDDD[]
         xdoors_d:10095B44 aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',ODh,OAh
         xdoors d:10095B44
                                                                    ; DATA XREF: sub 1000FF58+145To
         xdoors_d:10095B44
                                            db 'WelCome Back...Are You Enjoying Today?',0Dh,0Ah
         xdoors_d:10095B44
                                            db 0Dh,0Ah
         xdoors_d:10095B44
                                            db 'Machine UpTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Secon'
         xdoors_d:10095B44
                                            db 'ds]',0Dh,0Ah
         xdoors_d:10095B44
                                            db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Seco'
         xdoors_d:10095B44
                                            db 'nds]',0Dh,0Ah
         xdoors_d:10095B44
                                            db ODh,OAh
         xdoors_d:10095B44
                                            db 'Encrypt Magic Number For This Remote Shell Session [0x%02x]',0Dh,0Ah
         xdoors_d:10095B44
                                            db ODh,OAh,O
         xdoors_d:10095C5C ; char asc_10095C5C[]
         xdoors_d:10095C5C asc_10095C5C:
                                                                     ; DATA XREF: sub_1000FF58+4BTo
                                                                     ; sub 1000FF58+3E1†o
         xdoors_d:10095C5C
         0001DF34
                  10095B34: xdoors_d:aCmd_exeC
```

Press the **SPACEBAR** to get to graph view, as shown below. "\cmd.exe /c" is used in the little routine on the left.



Drag the graph view down to see the subroutines before it. About three boxes up you should find text beginning with "Hi, Master", as shown below.

```
push
        eax
        eax, [ebp+SystemTime.wHour]
MOVZX
push
        eax
MOVZX
        eax, [ebp+SystemTime.wDay]
push
        eax
MOVZX
        eax, [ebp+SystemTime.wMonth]
push
        eax
        eax, [ebp+SystemTime.wYear]
MOVZX
push
        eax
lea
        eax, [ebp+var_EC0]
        offset aHiMasterDDDDDD ; "Hi, Master [%d/%d/%d %d:%d:%d]\r\nWelCome "..
push
                         ; char *
push
        eax
call
        ds:sprintf
        esp, 44h
add
xor
        ebx, ebx
        eax, [ebp+var_EC0]
lea
push
        ebx
                         ; char *
push
        eax
call
        strlen
```

Double-click aHiMasterDDDD to find the complete message. The purpose of the malware is clearly stated.

Your image should show what the code is doing, as shown below. The purpose is behind the red rectangle in the image below.

```
IDA View-A
        xdoors_d:
                            ; char aCommand_exeC[]
                                            db '\command.exe /c ',0 ; DATA XREF: sub 1000FF58:loc 100101D7To
         xdoors_d:
                           aCommand_exeC
        xdoors_d:
                                            align 4
                                            db '\cmd.exe /c '.0
       xdoors_d:
                                                                     ; DATA XREF: sub_1000FF58+2781o
                            aCmd_exeC
        xdoors_d:
                                            align 4
        xdoors_d:
                            ; char aHiMasterDDDDDD[]
        xdoors d:
                           aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
                                                                     ; DATA XREF: sub 1000FF58+145To
         xdoors_d:
                                            db 'WelCome Back...Are You Enjoying Today?',0Dh,0Ah
         xdoors d:
         xdoors_d:
                                            db 0Dh,0Ah
        xdoors d:
                                            db 'Machine UpTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Secon'
        xdoors_d:
                                            db 'ds]',0Dh,0Ah
         xdoors_d:
                                            db 'Machine IdleTime [%-.2d Days %-.2d Hours %-.2d Minutes %-.2d Seco'
         xdoors_d:
                                            db 'nds]',0Dh,0Ah
         xdoors_d:
                                            db 0Dh,0Ah
                                            db 'Encrypt Magic Number For This
                                                                                                     [0x%02x]',0Dh,0Ah
         xdoors_d:
         xdoors d:
                                            db 0Dh,0Ah,0
         xdoors_d:
                            ; char asc_10095C5C[]
         xdoors_d:
                           asc_10095C5C:
                                                                     ; DATA XREF: sub_1000FF58+4BTo
                                                                     ; sub_1000FF58+3E1To
         xdoors d:
        xdoors d:
                                            dw 3Eh
         xdoors_d:
                                            unicode 0, \langle \rangle,0
```

Save a full-desktop image with the filename "Proj 6d from YOUR NAME".

#### **Turning in your Project**

Email the images showing to cnit.126sam@gmail.com with the subject line: Proj 6 from YOUR NAME