PROJ 6: IDA Pro

Prof. Alberto LaCava

CY -640

MALWARE ANALYSIS & DEFENSE

Nikhil Patel

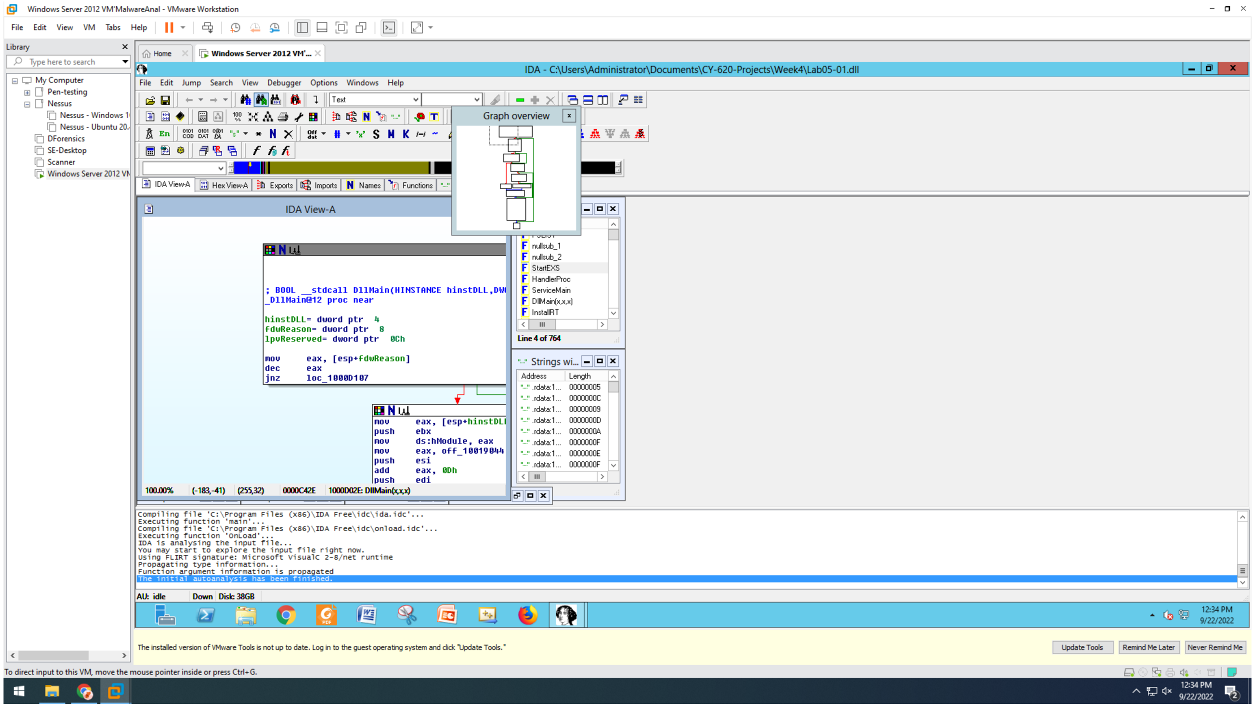
10/04/2022

Introduction: In this lab, we are going to perform the practical malware analysis using IDA Pro.

Procedure :

Getting Started with IDA Pro

- Go to Start and Type IDA Pro to open the application.
- Once the program is launched then click Ok and then the New / PE Dynamic Library icon and Ok.



```
; BOOL __stdcall DllMain(HINSTANCE hinstDLL,DW
_DllMain@12 proc near

hinstDLL= dword ptr  4
fdwReason= dword ptr  8
lpvReserved= dword ptr  0Ch

mov     eax, [esp+fdwReason]
dec     eax
jnz     loc_1000D107
```

```
mov     eax, [esp+hinstDLL
push    ebx
mov     ds:hModule, eax
mov     eax, off_10019044
push    esi
add     eax, 0Dh
push    edi
```

100.00% (-183,-41) (255,32) 0000C42E 1000D02E: DllMain(x,x,x)

Address	Length
.rdata:1...	00000005
.rdata:1...	0000000C
.rdata:1...	00000009
.rdata:1...	0000000D
.rdata:1...	0000000A
.rdata:1...	0000000F
.rdata:1...	0000000E
.rdata:1...	0000000F

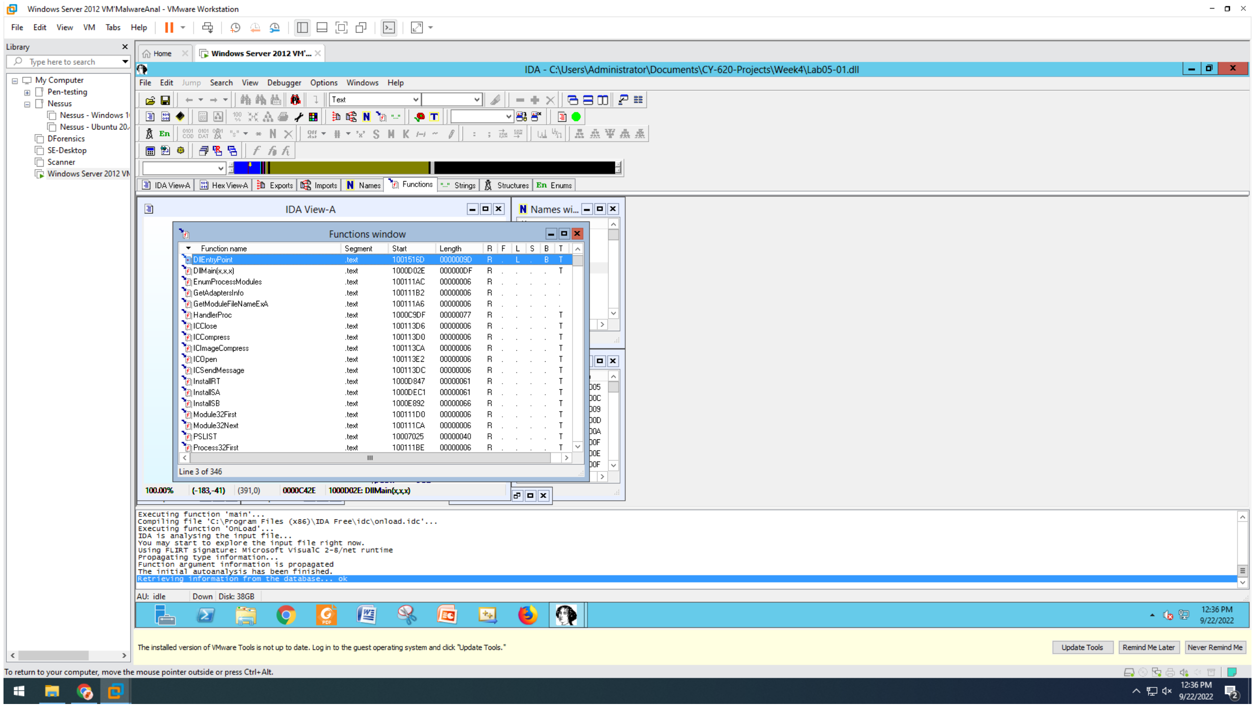
```
Compiling file 'C:\Program Files (x86)\IDA Free\idc\ida.idc'...
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
```

AU: idle Down Disk: 38GB

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

Finding the Address of DLLMain

- In IDA Pro, click Windows/ Function Window and click Function name.
- Take a screenshot and capture the DLLMain window.



Windows Server 2012 VM'MalwareAnal - VMware Workstation

IDA - C:\Users\Administrator\Documents\CY-620-Projects\Week4\Lab05-01.dll

Functions window

Function name	Segment	Start	Length	R	F	L	S	B	T
DllEntryPoint	.text	1001516D	0000009D	R	.	L	.	B	T
DllMain(x,x,x)	.text	1000D02E	000000DF	R	.	.	.	.	T
EnumProcessModules	.text	100111AC	00000006	R	.	.	.	.	.
GetAdaptersInfo	.text	100111B2	00000006	R	.	.	.	.	.
GetModuleFileNameExA	.text	100111A6	00000006	R	.	.	.	.	.
HandlerProc	.text	1000C9DF	00000077	R	.	.	.	.	T
ICClose	.text	100113D6	00000006	R	.	.	.	.	T
ICCompress	.text	100113D0	00000006	R	.	.	.	.	T
ICImageCompress	.text	100113CA	00000006	R	.	.	.	.	T
ICOpen	.text	100113E2	00000006	R	.	.	.	.	T
ICSendMessage	.text	100113DC	00000006	R	.	.	.	.	T
InstallRT	.text	1000D847	00000061	R	.	.	.	.	T
InstallSA	.text	1000DEC1	00000061	R	.	.	.	.	T
InstallSB	.text	1000E892	00000066	R	.	.	.	.	T
Module32First	.text	100111D0	00000006	R	.	.	.	.	T
Module32Next	.text	100111CA	00000006	R	.	.	.	.	T
PSLIST	.text	10007025	00000040	R	.	.	.	.	T
Process32First	.text	100111BE	00000006	R	.	.	.	.	T

Line 3 of 346

100.00% (-183,-41) (391,0) 0000C42E 1000D02E: DllMain(x,x,x)

```
Executing function 'main'...
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
Retrieving information from the database... ok
```

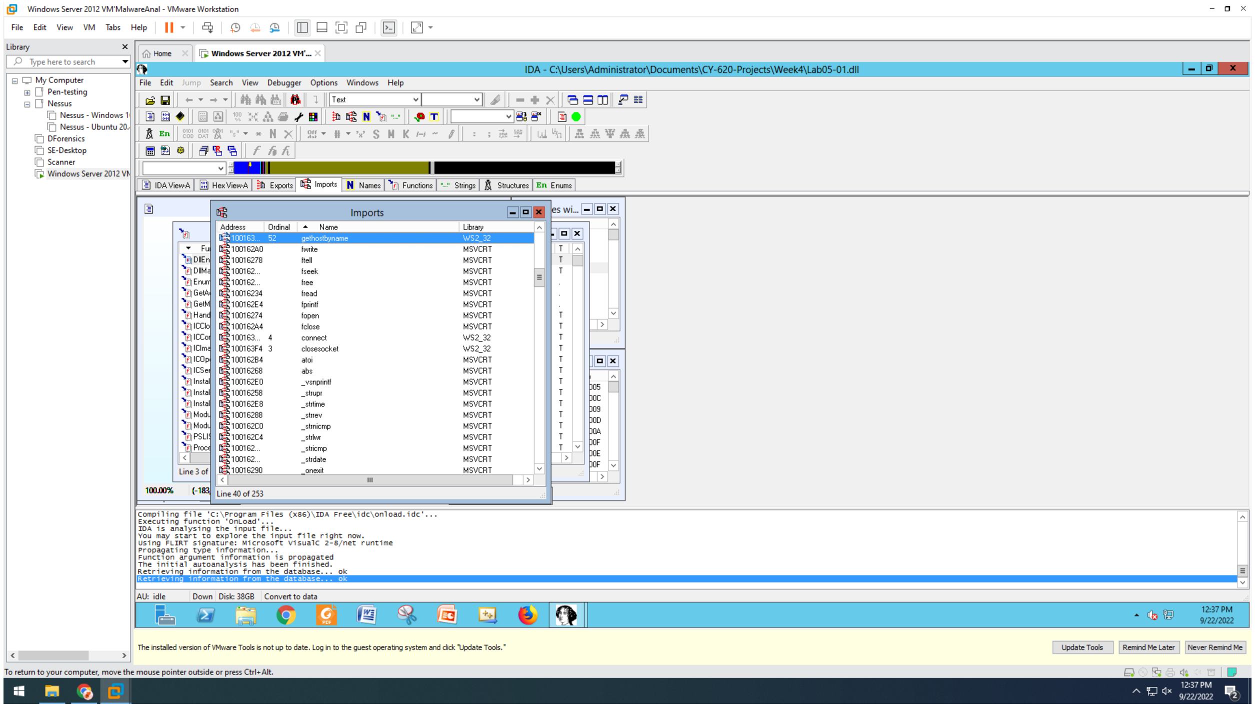
AU: idle Down Disk: 38GB

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Find the import for the gethostbyname

- In IDA Pro, click Windows/ Imports. Click the Name header to sort by name. Find "gethostbyname" and widen the Address column to make the entire address visible.
- Take a fullscreen screenshot of the desktop.



Windows Server 2012 VM'MalwareAnal - VMware Workstation

IDA - C:\Users\Administrator\Documents\CY-620-Projects\Week4\Lab05-01.dll

Imports

Address	Ordinal	Name	Library
100163...	52	gethostbyname	WS2_32
100162A0		fwrite	MSVCRT
10016278		ftell	MSVCRT
100162...		fseek	MSVCRT
100162...		free	MSVCRT
10016234		fread	MSVCRT
100162E4		fprintf	MSVCRT
10016274		fopen	MSVCRT
100162A4		fclose	MSVCRT
100163...	4	connect	WS2_32
100163F4	3	closesocket	WS2_32
100162B4		atoi	MSVCRT
10016268		abs	MSVCRT
100162E0		_vsnprintf	MSVCRT
10016258		_strupr	MSVCRT
100162E8		_strtime	MSVCRT
10016288		_strrev	MSVCRT
100162C0		_strnicmp	MSVCRT
100162C4		_strlwr	MSVCRT
100162...		_stricmp	MSVCRT
100162...		_strdate	MSVCRT
10016290		_onexit	MSVCRT

Line 40 of 253

```
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
Retrieving information from the database... ok
Retrieving information from the database... ok
```

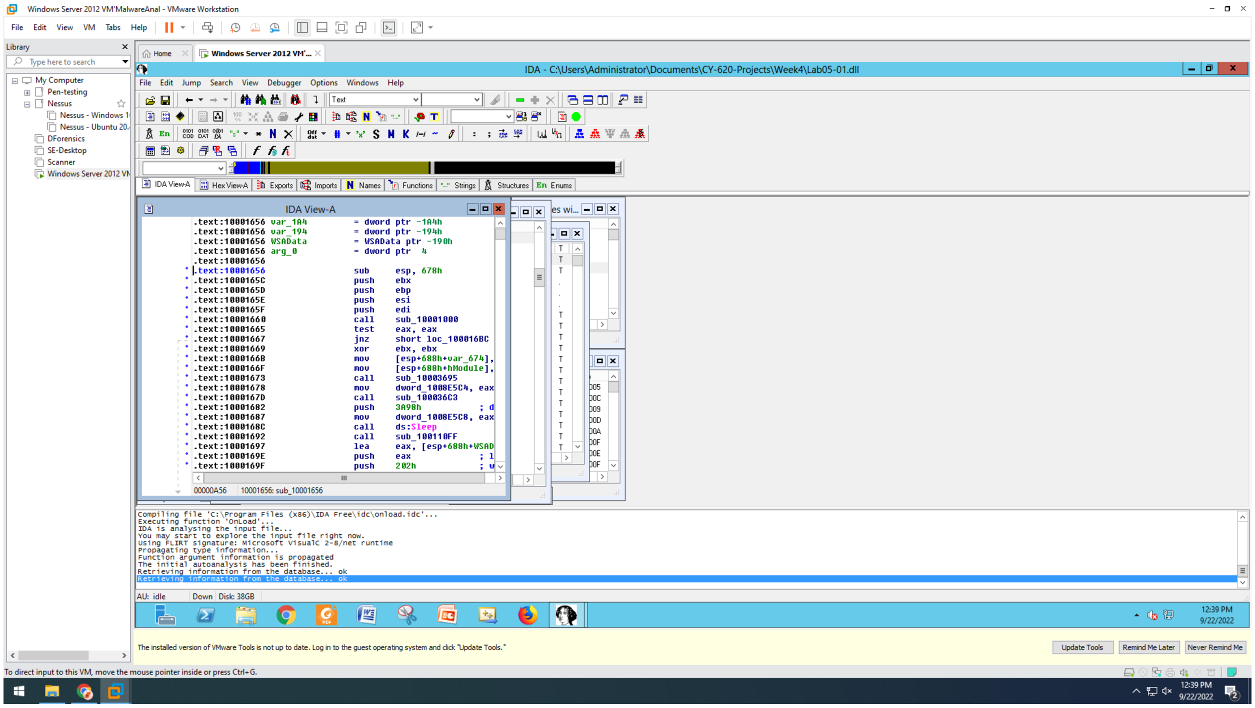
AU: idle Down Disk: 38GB Convert to data

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Count Local Variables for the Subroutine at 0x10001656

- In IDA Pro, click Windows/ IDA View-A and press SPACEBAR to get the text view.
- Now press g to go and enter address 0x10001656 and click OK.



```
.text:10001656 var_1A4         = dword ptr -1A4h
.text:10001656 var_194         = dword ptr -194h
.text:10001656 WSAData         = WSAData ptr -190h
.text:10001656 arg_0           = dword ptr  4
.text:10001656
.text:10001656                 sub     esp, 678h
.text:1000165C                 push    ebx
.text:1000165D                 push    ebp
.text:1000165E                 push    esi
.text:1000165F                 push    edi
.text:10001660                 call    sub_10001000
.text:10001665                 test    eax, eax
.text:10001667                 jnz     short loc_100016BC
.text:10001669                 xor     ebx, ebx
.text:1000166B                 mov     [esp+688h+var_674],
.text:1000166F                 mov     [esp+688h+hModule],
.text:10001673                 call    sub_10003695
.text:10001678                 mov     dword_1008E5C4, eax
.text:1000167D                 call    sub_100036C3
.text:10001682                 push    3A98h           ; d
.text:10001687                 mov     dword_1008E5C8, eax
.text:1000168C                 call    ds:Sleep
.text:10001692                 call    sub_100110FF
.text:10001697                 lea     eax, [esp+688h+WSAD
.text:1000169E                 push    eax             ; l
.text:1000169F                 push    202h            ; w
```

00000A56 10001656: sub_10001656

```
Compiling file 'C:\Program Files (x86)\IDA Free\idc\onload.idc'...
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
Retrieving information from the database... ok
Retrieving information from the database... ok
```

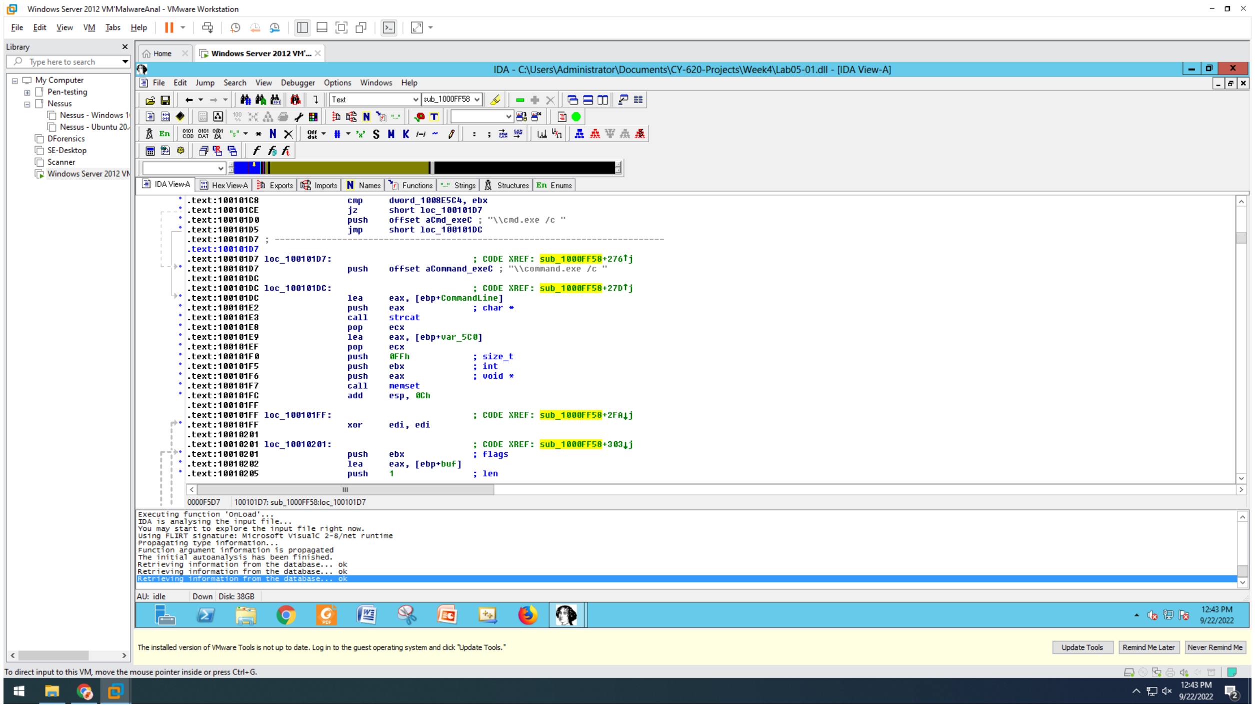
AU: idle Down Disk: 38GB

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.

Finding the Purpose of the code that References \cmd.exe /c

- In IDA Pro, click on strings and sort by string find the string “\\cmd.exe/c” and double click it.
- You will see the “XREF” double click the address and Press SPACEBAR to the graph view.
- Take a full Screenshot of the desktop.
- Now drag the graph view to subroutines and Double click “aHiMasterDDDD” to find the whole message.


Windows Server 2012 VM'MalwareAnal - VMware Workstation
IDA - C:\Users\Administrator\Documents\CY-620-Projects\Week4\Lab05-01.dll - [IDA View-A]
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums

```
.text:100101C8                 cmp     dword_1008E5C4, ebx
.text:100101CE                 jz      short loc_100101D7
.text:100101D0                 push    offset aCmd_exeC ; "\\cmd.exe /c "
.text:100101D5                 jmp     short loc_100101DC
.text:100101D7 ; ---------------------------------------------------------------------------
.text:100101D7
.text:100101D7 loc_100101D7:                           ; CODE XREF: sub_1000FF58+276↑j
.text:100101D7                 push    offset aCommand_exeC ; "\\command.exe /c "
.text:100101DC
.text:100101DC loc_100101DC:                           ; CODE XREF: sub_1000FF58+27D↑j
.text:100101DC                 lea     eax, [ebp+CommandLine]
.text:100101E2                 push    eax             ; char *
.text:100101E3                 call    strcat
.text:100101E8                 pop     ecx
.text:100101E9                 lea     eax, [ebp+var_5C0]
.text:100101EF                 pop     ecx
.text:100101F0                 push    0FFh            ; size_t
.text:100101F5                 push    ebx             ; int
.text:100101F6                 push    eax             ; void *
.text:100101F7                 call    memset
.text:100101FC                 add     esp, 0Ch
.text:100101FF
.text:100101FF loc_100101FF:                           ; CODE XREF: sub_1000FF58+2FA↓j
.text:100101FF                 xor     edi, edi
.text:10010201
.text:10010201 loc_10010201:                           ; CODE XREF: sub_1000FF58+303↓j
.text:10010201                 push    ebx             ; flags
.text:10010202                 lea     eax, [ebp+buf]
.text:10010205                 push    1               ; len
```

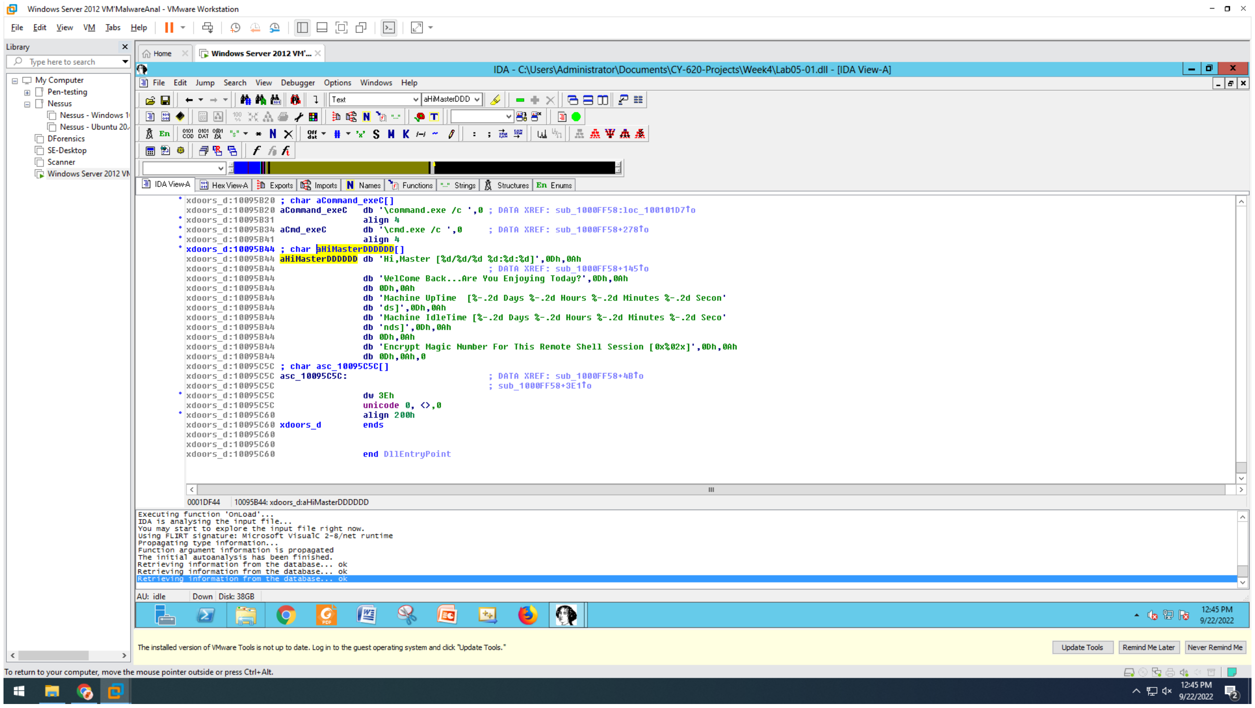
```
0000F5D7       100101D7: sub_1000FF58:loc_100101D7
```

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
```

AU: idle   Down   Disk: 38GB

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To direct input to this VM, move the mouse pointer inside or press Ctrl+G.


Windows Server 2012 VM'MalwareAnal - VMware Workstation
IDA - C:\Users\Administrator\Documents\CY-620-Projects\Week4\Lab05-01.dll - [IDA View-A]
IDA View-A
Hex View-A
Exports
Imports
Names
Functions
Strings
Structures
Enums

```
xdoors_d:10095B20 ; char aCommand_exeC[]
xdoors_d:10095B20 aCommand_exeC   db '\command.exe /c ',0 ; DATA XREF: sub_1000FF58:loc_100101D7↑o
xdoors_d:10095B31                 align 4
xdoors_d:10095B34 aCmd_exeC       db '\cmd.exe /c ',0     ; DATA XREF: sub_1000FF58+278↑o
xdoors_d:10095B41                 align 4
xdoors_d:10095B44 ; char aHiMasterDDDDDD[]
xdoors_d:10095B44 aHiMasterDDDDDD db 'Hi,Master [%d/%d/%d %d:%d:%d]',0Dh,0Ah
xdoors_d:10095B44                                         ; DATA XREF: sub_1000FF58+145↑o
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 0Dh,0Ah
xdoors_d:10095B44                 db 'Encrypt Magic Number For This Remote Shell Session [0x%02x]',0Dh,0Ah
xdoors_d:10095B44                 db 0Dh,0Ah,0
xdoors_d:10095C5C ; char asc_10095C5C[]
xdoors_d:10095C5C asc_10095C5C:                           ; DATA XREF: sub_1000FF58+4B↑o
xdoors_d:10095C5C                                         ; sub_1000FF58+3E1↑o
xdoors_d:10095C5C                 dw 3Eh
xdoors_d:10095C5C                 unicode 0, <>,0
xdoors_d:10095C60                 align 200h
xdoors_d:10095C60 xdoors_d        ends
xdoors_d:10095C60
xdoors_d:10095C60
xdoors_d:10095C60                 end DllEntryPoint
```

```
0001DF44       10095B44: xdoors_d:aHiMasterDDDDDD
```

```
Executing function 'OnLoad'...
IDA is analysing the input file...
You may start to explore the input file right now.
Using FLIRT signature: Microsoft VisualC 2-8/net runtime
Propagating type information...
Function argument information is propagated
The initial autoanalysis has been finished.
Retrieving information from the database... ok
Retrieving information from the database... ok
Retrieving information from the database... ok
```

AU: idle   Down   Disk: 38GB

The installed version of VMware Tools is not up to date. Log in to the guest operating system and click "Update Tools."

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

Conclusion: To conclude with the lab we get to know about the basics of how to use the IDA-Pro and also we try out different tasks to get hands-on with IDA-Pro for Other Projects.