

汇编语言与逆向技术实验报告

Lab1-HelloWorld

学号：2112060 姓名：孙蓓 专业：信息安全

一、实验内容

本实验提供一个在命令行输出“HelloWorld”字符串的汇编程序，和一个在 Windows MessageBox 中输出“HelloWorld”的汇编程序。

二、实验目的

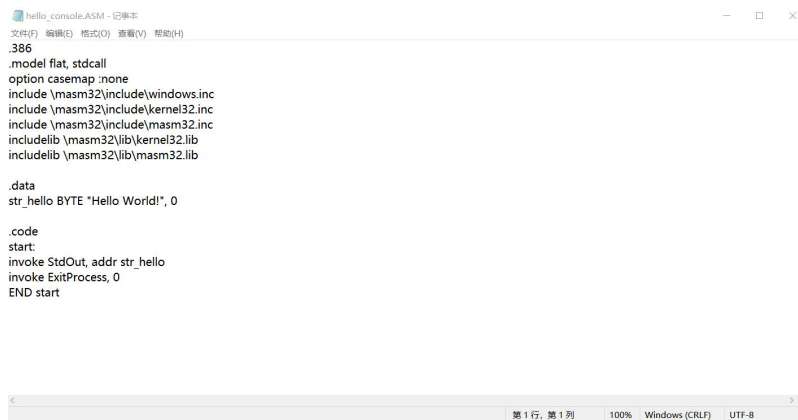
1. 熟悉 Win32 汇编 MASM32 的编译环境；
2. 命令行输出“HelloWorld”
3. 窗口输出“HelloWorld”

三、实验环境

Windows 操作系统，MASM32 编译环境。

四、实验步骤：命令行输出“HelloWorld”

1. 源文件：用文本编辑器编写的 asm 文本文件



```
hello_console.asm - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
.386
.model flat, stdcall
option casemap:none
include \masm32\include\windows.inc
include \masm32\include\kernel32.inc
include \masm32\include\masm32.inc
include \masm32\lib\kernel32.lib
include \masm32\lib\masm32.lib

.data
str_hello BYTE "Hello World!", 0

.code
start:
invoke StdOut, addr str_hello
invoke ExitProcess, 0
END start
```

2. 汇编：用汇编程序（\masm32\bin\ml.exe）对源程序进行汇编，形成目标文件（.obj），格式如下：

“\masm32\bin\ml /c /Zd /coff hello_console.asm”

hello_console.ASM	2022/9/30 18:17	ASM 文件	1 KB
hello_console.exe	2022/9/30 18:17	应用程序	3 KB
hello_console.obj	2022/9/30 18:17	3D Object	1 KB

```
Microsoft Windows [版本 10.0.19044.2006]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\LENOVO>d:

D:\>cd 第一次实验
'cd 第一次实验' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

D:\>cd A 汇编

D:\A 汇编>cd 第一次实验

D:\A 汇编\第一次实验>\masm32\bin\ml /c /Zd /coff hello_console.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

    Assembling: hello_console.asm

*****
ASCII build
*****

D:\A 汇编\第一次实验>
```

3. 连接：用连接程序（\masm32\bin\link.exe）对目标程序进行连接，形成可执行文件（.exe），格式如下

“\masm32\bin\Link /SUBSYSTEM:CONSOLE hello_console.obj”

```
Microsoft Windows [版本 10.0.19044.2006]
(c) Microsoft Corporation. 保留所有权利。

D:\A 汇编\第一次实验>\masm32\bin\ml /c /Zd /coff hello_console.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

    Assembling: hello_console.asm

*****
ASCII build
*****

D:\A 汇编\第一次实验>\masm32\bin\Link /SUBSYSTEM:CONSOLE hello_console.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

D:\A 汇编\第一次实验>\masm32\bin\Link /SUBSYSTEM:CONSOLE hello_console.obj*
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.
```

五、 实验命令行输出“HelloWorld”截图

输入.asm文件名

```
Microsoft Windows [版本 10.0.19044.2006]
(c) Microsoft Corporation. 保留所有权利。

D:\A 汇编\第一次实验>\masm32\bin\ml /c /Zd /coff hello_console.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

    Assembling: hello_console.asm

*****
ASCII build
*****

D:\A 汇编\第一次实验>\masm32\bin\Link /SUBSYSTEM:CONSOLE hello_console.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

D:\A 汇编\第一次实验>\masm32\bin\Link /SUBSYSTEM:CONSOLE hello_console.obj*
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

D:\A 汇编\第一次实验>
D:\A 汇编\第一次实验>
D:\A 汇编\第一次实验>
D:\A 汇编\第一次实验>
D:\A 汇编\第一次实验>hello_console
Hello World!
D:\A 汇编\第一次实验>
```

六、 实验步骤：窗口输出“HelloWorld”

1. 源文件：用文本编辑器编写的.asm文本文件

```
hello_window.asm - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)
.386
.model flat, stdcall
option casemap :none
include \masm32\include\windows.inc
include \masm32\include\kernel32.inc
include \masm32\include\user32.inc
includelib \masm32\lib\kernel32.lib
includelib \masm32\lib\user32.lib
.data
str_hello BYTE "Hello World!", 0
.code

start:
invoke MessageBox, NULL, addr str_hello, addr str_hello, MB_OK
invoke ExitProcess, 0
END start
```

2. 汇编：用汇编程序（\masm32\bin\ml.exe）对源程序进行汇编，形成目标文件（.obj），格式如下：

“\masm32\bin\ml /c /Zd /coff hello_window.asm”

```
命令提示符
Microsoft Windows [版本 10.0.19044.2006]
(c) Microsoft Corporation. 保留所有权利。




C:\Users\LENOVO>d:
D:\>cd A 汇编
D:\A 汇编>cd 第一次实验
D:\A 汇编\第一次实验>\masm32\bin\ml /c /Zd /coff hello_window.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

Assembling: hello_window.asm
*****
ASCII build
*****
D:\A 汇编\第一次实验>
```

 hello_window.asm	2022/9/30 18:12	ASM 文件	1 KB
 hello_window.obj	2022/9/30 18:56	3D Object	2 KB

3. 连接：用连接程序（\masm32\bin\link.exe）对目标程序进行连接，形成可执行文件（.exe），格式如下

“\masm32\bin\Link /SUBSYSTEM:WINDOWS hello_window.obj”

 hello_window.asm	2022/9/30 18:12	ASM 文件	1 KB
 hello_window.exe	2022/9/30 18:56	应用程序	3 KB
 hello_window.obj	2022/9/30 18:56	3D Object	2 KB

```
Microsoft Windows [版本 10.0.19044.2006]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\LENOVO>d:
D:\>cd A 汇编
D:\A 汇编>cd 第一次实验
D:\A 汇编\第一次实验>\masm32\bin\ml /c /Zd /coff hello_window.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

Assembling: hello_window.asm

*****
ASCII build
*****

D:\A 汇编\第一次实验>\masm32\bin\Link /SUBSYSTEM:WINDOWS hello_window.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

D:\A 汇编\第一次实验>
```

七、 实验窗口输出“HelloWorld”截图

输入.asm 文件名

```
Microsoft Windows [版本 10.0.19044.2006]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\LENOVO>d:
D:\>cd A 汇编
D:\A 汇编>cd 第一次实验
D:\A 汇编\第一次实验>\masm32\bin\ml /c /Zd /coff hello_window.asm
Microsoft (R) Macro Assembler Version 6.14.8444
Copyright (C) Microsoft Corp 1981-1997. All rights reserved.

Assembling: hello_window.asm

*****
ASCII build
*****

D:\A 汇编\第一次实验>\masm32\bin\Link /SUBSYSTEM:WINDOWS hello_window.obj
Microsoft (R) Incremental Linker Version 5.12.8078
Copyright (C) Microsoft Corp 1992-1998. All rights reserved.

D:\A 汇编\第一次实验>hello_window
D:\A 汇编\第一次实验>
```



八、 汇编命令与参数的解析

1. “\masm32\bin\ml /c /Zd /coff hello_console.asm”

- (1) \masm32\bin\ml /告诉要调用什么
- (2) ml 程序可以用来汇编并链接一个或多个汇编语言源文件
- (3) ml /c /Zd /coff

/c 是告诉 MASM 只编译不连接。

/coff 告诉 MASM 生成 Microsoft 公共目标文件格式的文件

/Zd--Add line number debug info 加上行号调试信息。

- (4) hello_console.asm 告诉执行文件在信息

2. “\masm32\bin\link /SUBSYSTEM:CONSOLE hello_console.obj”

- (1) 告诉要使用连接，连接使用 link 命令 (masm32\bin\link.exe)
- (2) /SUBSYSTEM:选择运行环境 (console 命令行或 WindowsGUI)
- (3) SUBSYSTEM:CONSOLE 生成命令程序
- (4) hello_console.obj 告诉执行文件信息

九、汇编程序解析

1.

.386 (允许汇编 80386 处理器的非特权指令, 禁用其后处理器引入的汇编指令, .386 兼容性相对最好)

.model flat, stdcall (flat: 平坦模式, 4GB 内存空间, stdcall: 调用约定, stdcall 是 Win32 API 函数的调用约定)

option casemap :none (不区分大小写)

include \masm32\include\windows.inc (include ...inc 函数的常量和声明)

include \masm32\include\kernel32.inc (windows 一些函数在 kernel 库里)

include \masm32\include\masm32.inc (masm32 也提供了些函数)

includelib \masm32\lib\kernel32.lib

includelib \masm32\lib\masm32.lib (includelib ...lib 链接库)

.data (定义已初始化数据段的开始)

str_hello BYTE "Hello World!", 0 (0 告诉字符串 Hello World! 已经结束到末尾了)

.code (定义代码段的开始)

start: (指令标号, 标记指令地址)

invoke StdOut, addr str_hello (StdOut, masm32.inc 中定义的函数, 将内存数据输出到命令行窗口上)

invoke ExitProcess, 0 (Kernel32.inc 中定义的函数, 退出程序执行)

END start (标记模块的结束, 指定程序的入口点, 告诉 CPU 从 start 开始执行, 并把 start 写到寄存器里)

2.

.386 (允许汇编 80386 处理器的非特权指令, 禁用其后处理器引入的汇编指令, .386 兼容性相对最好)

.model flat, stdcall (flat: 平坦模式, 4GB 内存空间, stdcall: 调用约定, stdcall 是 Win32 API 函数的调用约定)

```
option casemap :none (不区分大小写)

include \masm32\include\windows.inc (include ...inc 函数的常量和声明)

include \masm32\include\kernel32.inc (windows 一些函数在 kernel 库里)

include \masm32\include\user32.inc
includelib \masm32\lib\kernel32.lib
includelib \masm32\lib\user32.lib (includelib ...lib 链接库)

.data (定义已初始化数据段的开始)
str_hello BYTE "Hello World!", 0 (0 告诉字符串 Hello World! 已经结束到末尾了)

.code (定义代码段的开始)

start: (指令标号, 标记指令地址)
    invoke MessageBox, NULL, addr str_hello, addr str_hello, MB_OK (窗口输出 Hello World!)
    invoke ExitProcess, 0 (Kernel32.inc 中定义的函数, 退出程序执行)
END start (标记模块的结束, 指定程序的入口点, 告诉 CPU 从 start 开始执行, 并把 start 写到寄存器里)
```