操作系统

实

验

报

告

**实验名称：\_\_\_\_\_\_\_\_\_实验六\_\_\_ \_\_\_\_\_\_\_**

**小组成员姓名：\_\_\_\_\_\_\_刘俊武\_\_\_\_\_\_\_\_\_\_\_\_\_**

**小组成员学号：\_\_\_SZ160110120\_\_\_\_\_\_\_\_\_\_\_\_**

**学院：\_\_\_\_计算机科学与技术\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**专业：\_\_\_\_\_\_\_\_计算机专业\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

一、实验目的

此次实验的主要目的有如下几点:

1.掌握对程序进行fuzzingd的使用方法，致使程序发生段错误

2.实现缓冲区溢出攻击

二、实验内容

本实验的内容是通过fuzzing对程序实施缓冲区溢出漏洞判断，并实现可远程执行的缓冲区溢出攻击。

我们利用Metasploit渗透测试框架，编写攻击程序，来攻击含有漏洞的FTPServer.exe的程序。并通过Ollydbg程序观察现象。

三、实验过程

1.运行FTPServer.exe



2.虚拟机上面的windowsxp的ip地址

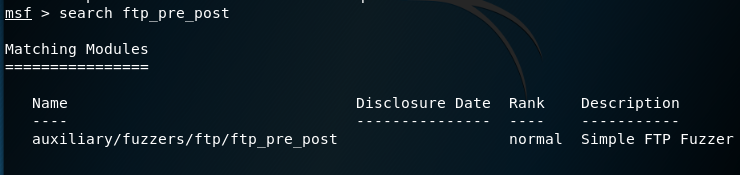
3.在kali 中启动metasploit

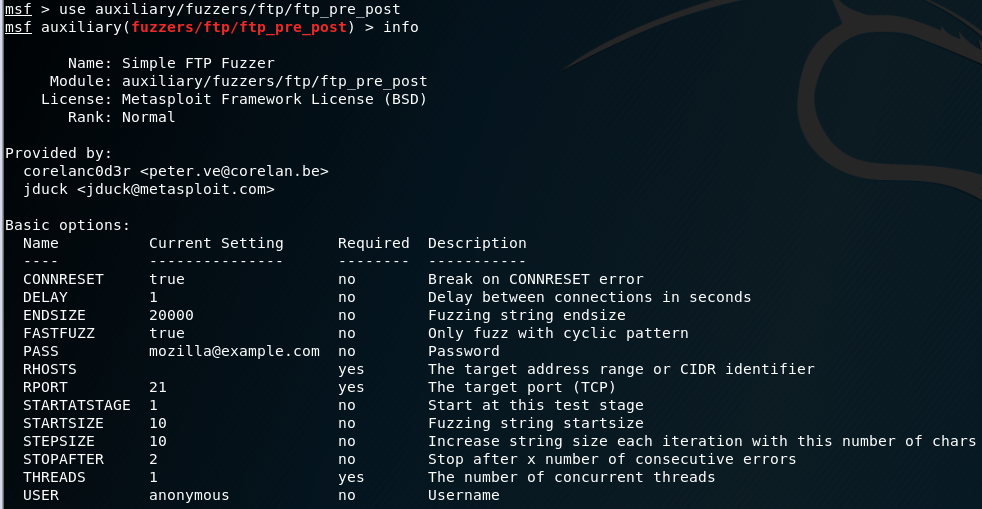




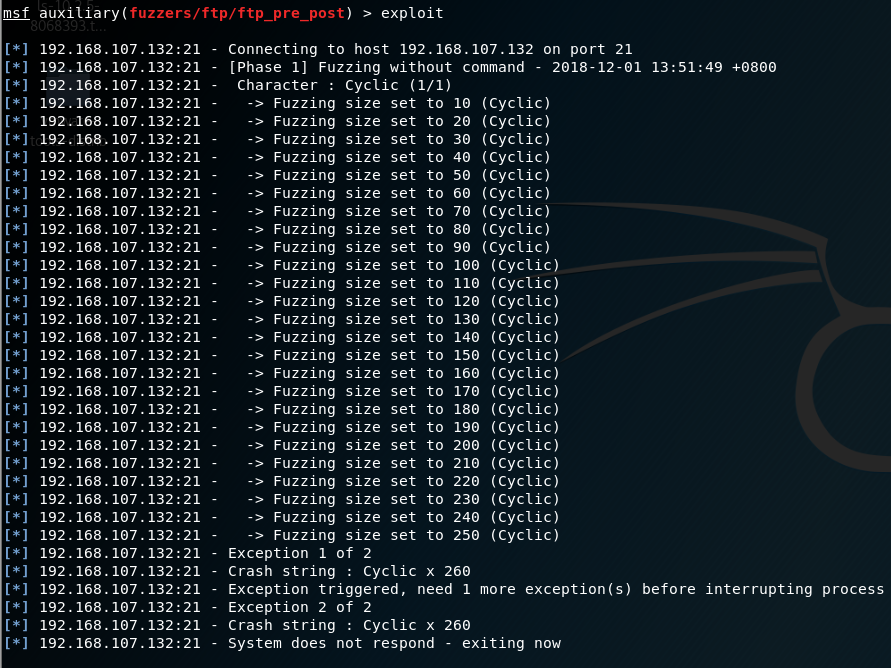
4.使用ping 测试下ip 是否可以访问：

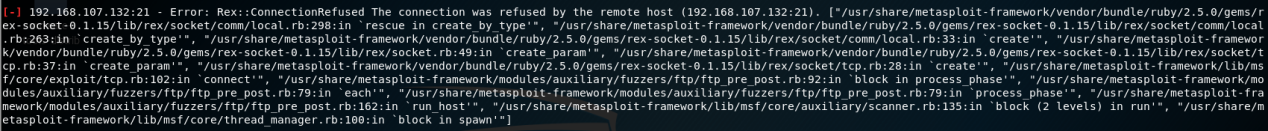
5.搜索需要的工具，使用search ftp\_pre\_post

6.使用此工具，输入行use auxiliary/fuzzers/ftp/ftp\_pre\_post，并输入info来查看运行此工具所需要配置的参数。

7.设置参数，只用设置RHOSTS的参数

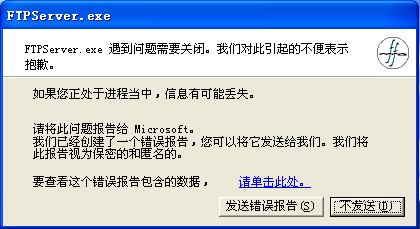
8.攻击结果：



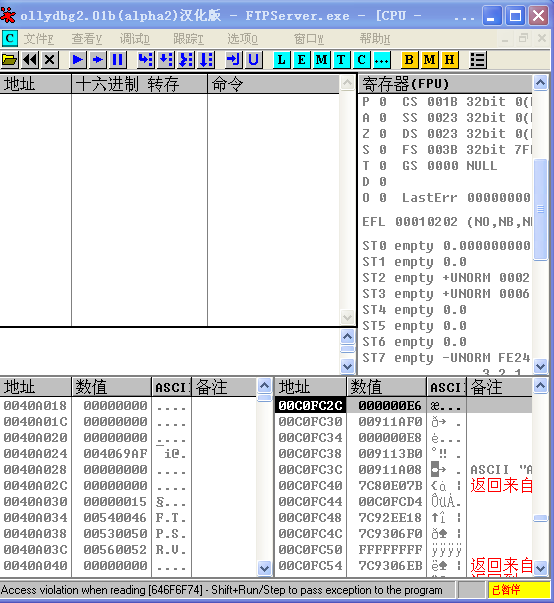


9.ERROR报错：当输入260 Bytes的数据时会报错。

Windowsxp 中会显示：

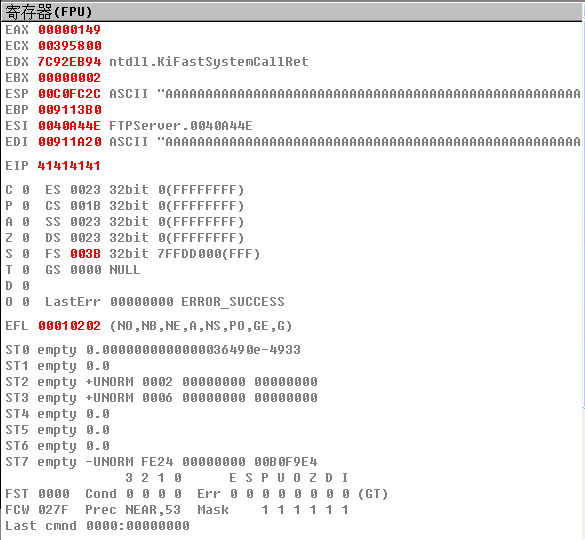


9.使用ollydbg 工具，对缓冲区内部进行观测，来辅助测试：



10.创建一个bomb.py的文件，用它进行攻击的结果，通过ollydgb查看，可以看到

ESP、EDI、EIP三个寄存器都被填为AAAA…。

11.创建一个新的终端，进入到指导书给出的文件夹内

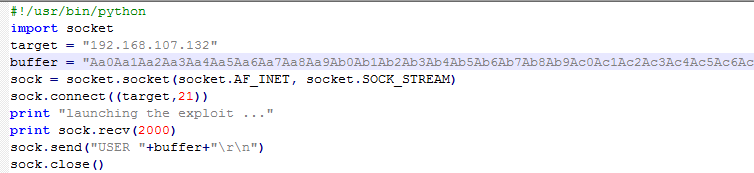
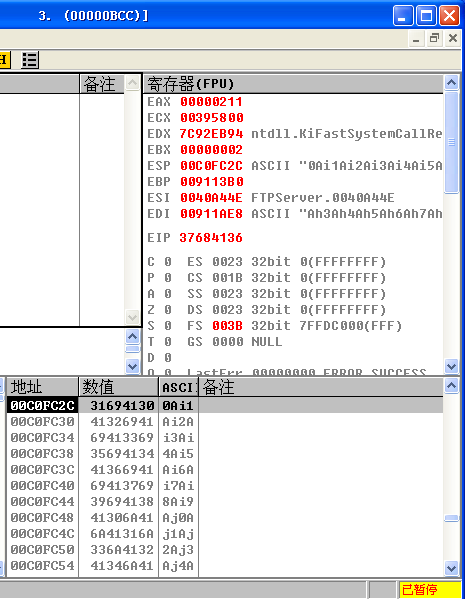
/usr/share/metasploit-framework/tools/exploit

再用 Msf 提供的模式创建工具pattern\_create.rb，创建一个长度为500的字符串：

（由于不小心删除了终端口直接复制了字符串）

Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6Ab7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7Ad8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8Af9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9Ai0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0Ak1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1Am2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2Ao3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3Aq4Aq5Aq

12.在bomb.文件中修改

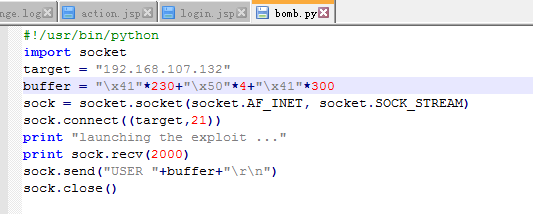
结果如下：

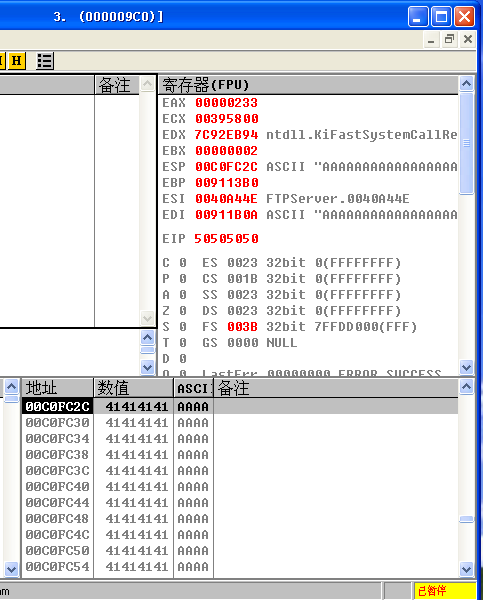
13.可以看到EIP中的值变为了37684136，这个值自己创建出来的长度为500的字符串中的一部分。

14.再利用 /usr/share/metasploit-framework/tools/exploit 目录下的另一工具 pattern\_offset.rb 定位EIP，发现EIP的偏移位置为230：



15.继续修改buffer的值

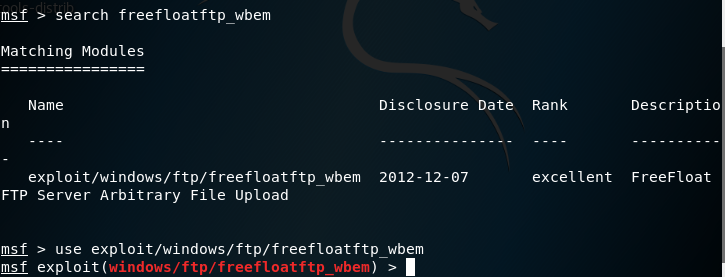


16攻击结果如下：

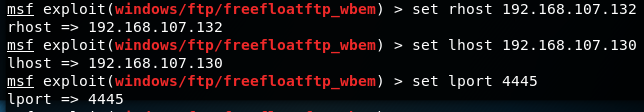
EIP寄存器中的值变为了50505050，右下角的内存区也被修改为了41414141。

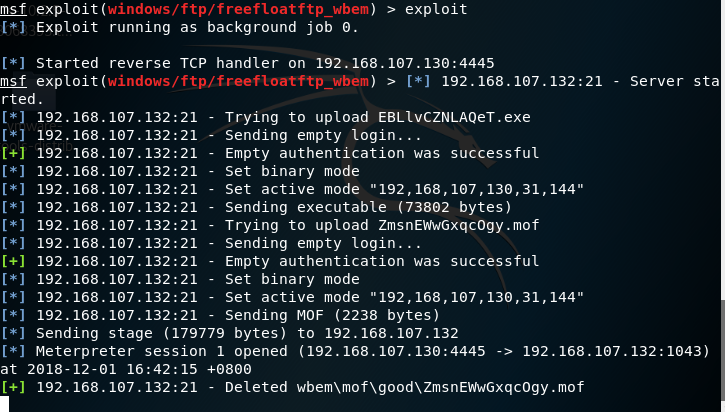
四、实验结果与分析

在msf 中搜索freefloatftp\_wbem，并使用



设置参数



结果

五、实验课收获与总结

本次实验，最大的感觉就是自己仿佛也当了一次黑客，在kali虚拟机上对Windows XP虚拟机攻击成功的同时，让我明白了缓冲区溢出的恐怖性，不仅仅是会将系统弄得崩溃，更有可能使得系统被修改，利用，使得自己的权益受损、隐私泄露等。

同时自己也学会对一些指令和软件的使用，收获也挺多的。