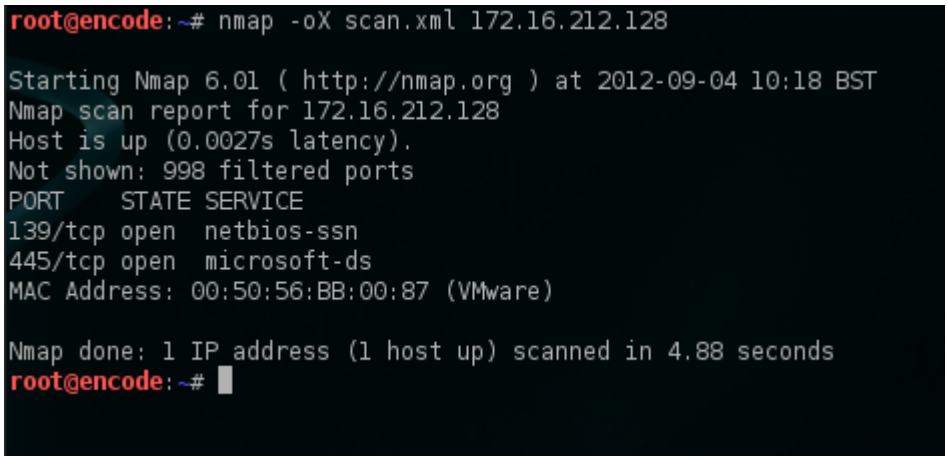
# Ndiff

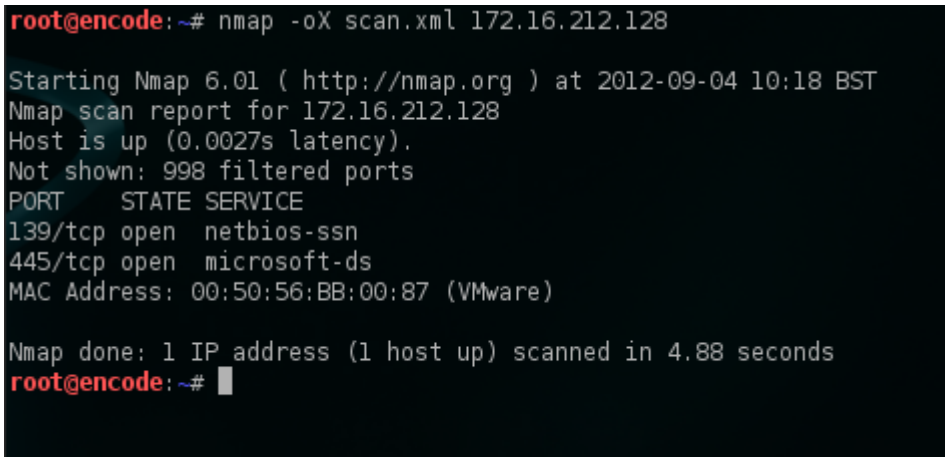


September 4, 2012




Ndiff is a tool that it can be used to compare two nmap scan files and highlights any changes between them.In order to compare the scans,the files in nmap must be saved in text or xml format.Ndiff will point out the differences between them for easy comparison by using plus and minus signs.

Lets say that we want to compare two scans of a single host.We will use the option **-oX** and a **filename.xml** which will save the nmap outputs in a xml file.




Save the results on an XML file – 1st Scan

```
root@encode:~# nmap -oX scan2.xml 172.16.212.128

Starting Nmap 6.01 ( http://nmap.org ) at 2012-09-04 11:23 BST
Nmap scan report for 172.16.212.128
Host is up (0.00086s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1111/tcp open  lmsocialserver
3389/tcp open  ms-wbt-server
MAC Address: 00:50:56:BB:00:87 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 4.85 seconds
```

Save the results on an XML file – 2nd Scan

As we can see from the first scan the host has only two ports open while in the second has 5.Now lets try to compare these two results with the Ndiff.The comparison can be done very easily just by using the command **ndiff [filename.xml filename2.xml]**

```
root@encode:~# ndiff scan.xml scan2.xml
-Nmap 6.01 scan initiated Tue Sep 04 10:18:02 2012 as: nmap -oX scan.xml 172.16.212.128
+Nmap 6.01 scan initiated Tue Sep 04 11:23:07 2012 as: nmap -oX scan2.xml 172.16.212.128

 172.16.212.128, 00:50:56:BB:00:87:
-Not shown: 998 filtered ports
+Not shown: 995 filtered ports
 PORT     STATE SERVICE       VERSION
+135/tcp  open  msrpc
+1111/tcp open  lmsocialserver
+3389/tcp open  ms-wbt-server
```

ndiff – Comparison of two nmap scans

The above image illustrates the differences between these two scans that we have conducted on the same host.The **plus** sign (+) highlights the differences of the second file in relation with the first while the **minus** (-) sign indicates the differences of the first file in comparison with the second.Specifically in the example above we can see that the port 135,1111 and 3389 have the  plus sign which means that in the second scan these ports were found open while in the first scan these ports were closed.

Alternatively we can use the **-v** option (verbose mode) which it will display all the output of these two xml files and it will highlight the differences with the plus and minus signs as before.

```
root@encode:~# ndiff -v scan.xml scan2.xml
-Nmap 6.01 scan initiated Tue Sep 04 10:18:02 2012 as: nmap -oX scan.xml 172.16.212.128
+Nmap 6.01 scan initiated Tue Sep 04 11:23:07 2012 as: nmap -oX scan2.xml 172.16.212.128

 172.16.212.128, 00:50:56:BB:00:87:
 Host is up.
-Not shown: 998 filtered ports
+Not shown: 995 filtered ports
 PORT     STATE SERVICE        VERSION
+135/tcp  open  msrpc
 139/tcp  open  netbios-ssn
 445/tcp  open  microsoft-ds
+1111/tcp open  lmsocialserver
+3389/tcp open  ms-wbt-server
```

ndiff verbose mode

Ndiff also provides the ability to produce the results in XML output with the **–xml** option.This option is useful in cases where we want to import the information from Ndiff into a third party tool that uses this format.

```
root@encode:~# ndiff --xml scan.xml scan2.xml
<?xml version="1.0" encoding="utf-8"?>
<nmapdiff version="1"><scandiff><a><nmaprun args="nmap -oX scan.xml 172.16.212.128" scanner=
"nmap" start="1346750282" startstr="Tue Sep 04 10:18:02 2012" version="6.01"/>
</a><b><nmaprun args="nmap -oX scan2.xml 172.16.212.128" scanner="nmap" start="1346754187" s
tartstr="Tue Sep 04 11:23:07 2012" version="6.01"/>
</b><hostdiff>
<host>
<address addr="172.16.212.128" addrtype="ipv4"/>
<address addr="00:50:56:BB:00:87" addrtype="mac"/>
<ports>
<a>
<extraports count="998" state="filtered"/>
</a>
<b>
<extraports count="995" state="filtered"/>
</b>
<portdiff>
<a>
<port portid="135" protocol="tcp"/>
</a>
<b>
<port portid="135" protocol="tcp">
<state state="open"/>
<service name="msrpc"/>
</port>
```

ndiff – xml output