NAME

ndiff − Utility to compare the results of Nmap scans

SYNOPSIS

ndiff [*options*] {*a.xml*} {*b.xml*}

DESCRIPTION

Ndiff is a tool to aid in the comparison of Nmap scans. It takes two Nmap XML output files and prints the differences between them. The differences observed are:

- Host states (e.g. up to down)
- Port states (e.g. open to closed)
- Service versions (from **−sV**)
- OS matches (from **−O**)
- Script output

Ndiff, like the standard **diff** utility, compares two scans at a time.

OPTIONS SUMMARY

−h, **−−help**
Show a help message and exit.

−v, **−−verbose**
Include all hosts and ports in the output, not only those that have changed.

−−text
Write output in human−readable text format.

−−xml
Write output in machine−readable XML format. The document structure is defined in the file ndiff.dtd included in the distribution.

Any other arguments are taken to be the names of Nmap XML output files. There must be exactly two.

EXAMPLE

Let's use Ndiff to compare the output of two Nmap scans that use different options. In the first, we'll do a fast scan (**−F**), which scans fewer ports for speed. In the second, we'll scan the larger default set of ports, and run an NSE script.

```
# nmap −F scanme.nmap.org −oX scanme−1.xml
# nmap −−script=html−title scanme.nmap.org −oX scanme−2.xml
$ ndiff −v scanme−1.xml scanme−2.xml
−Nmap 5.35DC1 at 2010−07−16 12:09
+Nmap 5.35DC1 at 2010−07−16 12:13

 scanme.nmap.org (64.13.134.52):
 Host is up.
−Not shown: 95 filtered ports
+Not shown: 993 filtered ports
 PORT      STATE  SERVICE VERSION
 22/tcp    open   ssh
 25/tcp    closed smtp
 53/tcp    open   domain
+70/tcp    closed gopher
 80/tcp    open   http
+|_ html−title: Go ahead and ScanMe!
 113/tcp   closed auth
+31337/tcp closed Elite
```

Changes are marked by a − or + at the beginning of a line. We can see from the output that the scan without the **−F** fast scan option found two additional ports: 70 and 31337. The html−title script produced some additional output for port 80. From the port counts, we may infer that the fast scan scanned 100 ports (95 filtered, 3 open, and 2 closed), while the normal scan scanned 1000 (993 filtered, 3 open, and 4 closed).

The **−v** (or **−−verbose**) option to Ndiff made it show even the ports that didn't change, like 22 and 25. Without **−v**, they would not have been shown.

OUTPUT

There are two output modes: text and XML. Text output is the default, and can also be selected with the **−−text** option. Text output resembles a unified diff of Nmap's normal terminal output. Each line is preceded by a character indicating whether and how it changed. − means that the line was in the first scan but not in the second; + means it was in the second but not the first. A line that changed is represented by a − line followed by a + line. Lines that did not change are preceded by a blank space.

Example 1 is an example of text output. Here, port 80 on the host photos−cache−snc1.facebook.com gained a service version (lighttpd 1.5.0). The host at 69.63.179.25 changed its reverse DNS name. The host at 69.63.184.145 was completely absent in the first scan but came up in the second.

Example 1. Ndiff text output

```
−Nmap 4.85BETA3 at 2009−03−15 11:00
+Nmap 4.85BETA4 at 2009−03−18 11:00

 photos−cache−snc1.facebook.com (69.63.178.41):
 Host is up.
 Not shown: 99 filtered ports
 PORT   STATE SERVICE VERSION
−80/tcp open  http
+80/tcp open  http    lighttpd 1.5.0

−cm.out.snc1.tfbnw.net (69.63.179.25):
+mailout−snc1.facebook.com (69.63.179.25):
 Host is up.
 Not shown: 100 filtered ports

+69.63.184.145:
+Host is up.
+Not shown: 98 filtered ports
+PORT    STATE SERVICE  VERSION
+80/tcp  open  http     Apache httpd 1.3.41.fb1
+443/tcp open  ssl/http Apache httpd 1.3.41.fb1
```

XML output, intended to be processed by other programs, is selected with the **−−xml** option. It is based on Nmap's XML output, with a few additional elements to indicate differences. The XML document is enclosed in *nmapdiff* and *scandiff* elements. Host differences are enclosed in *hostdiff* tags and port differences are enclosed in *portdiff* tags. Inside a *hostdiff* or *portdiff*, *a* and *b* tags show the state of the host or port in the first scan (*a*) or the second scan (*b*).

Example 2 shows the XML diff of the same scans shown above in Example 1. Notice how port 80 of photos−cache−snc1.facebook.com is enclosed in *portdiff* tags. For 69.63.179.25, the old hostname is in *a* tags and the new is in *b*. For the new host 69.63.184.145, there is a *b* in the *hostdiff* without a corresponding *a*, indicating that there was no information for the host in the first scan.

Example 2. Ndiff XML output

```
<?xml version="1.0" encoding="UTF−8"?>
<nmapdiff version="1">
  <scandiff>
```

```
<hostdiff>
  <host>
    <status state="up"/>
    <address addr="69.63.178.41" addrtype="ipv4"/>
    <hostnames>
      <hostname name="photos−cache−snc1.facebook.com"/>
    </hostnames>
    <ports>
      <extraports count="99" state="filtered"/>
      <portdiff>
        <port portid="80" protocol="tcp">
          <state state="open"/>
          <a>
            <service name="http"/>
          </a>
          <b>
            <service name="http" product="lighttpd" version="1.5.0"/>
          </b>
        </port>
      </portdiff>
    </ports>
  </host>
</hostdiff>
<hostdiff>
  <host>
    <status state="up"/>
    <address addr="69.63.179.25" addrtype="ipv4"/>
    <hostnames>
      <a>
        <hostname name="cm.out.snc1.tfbnw.net"/>
      </a>
      <b>
        <hostname name="mailout−snc1.facebook.com"/>
      </b>
    </hostnames>
    <ports>
      <extraports count="100" state="filtered"/>
    </ports>
  </host>
</hostdiff>
<hostdiff>
  <b>
    <host>
      <status state="up"/>
      <address addr="69.63.184.145" addrtype="ipv4"/>
      <ports>
        <extraports count="98" state="filtered"/>
        <port portid="80" protocol="tcp">
          <state state="open"/>
          <service name="http" product="Apache httpd"
                   version="1.3.41.fb1"/>
        </port>
        <port portid="443" protocol="tcp">
          <state state="open"/>
```

```
            <service name="http" product="Apache httpd" tunnel="ssl"
                  version="1.3.41.fb1"/>
           </port>
          </ports>
         </host>
        </b>
       </hostdiff>
      </scandiff>
    </nmapdiff>
```

PERIODIC DIFFS

Using Nmap, Ndiff, cron, and a shell script, it's possible to scan a network daily and get email reports of the state of the network and changes since the previous scan. Example 3 shows the script that ties it together.

Example 3. Scanning a network periodically with Ndiff and cron

```
#!/bin/sh
TARGETS="targets"
OPTIONS="−v −T4 −F −sV"
date=‘date +%F‘
cd /root/scans
nmap $OPTIONS $TARGETS −oA scan−$date > /dev/null
if [ −e scan−prev.xml ]; then
      ndiff scan−prev.xml scan−$date.xml > diff−$date
      echo "*** NDIFF RESULTS ***"
      cat diff−$date
      echo
fi
echo "*** NMAP RESULTS ***"
cat scan−$date.nmap
ln −sf scan−$date.xml scan−prev.xml
```

If the script is saved as /root/scan−ndiff.sh, add the following line to root's crontab:

```
0 12 * * * /root/scan−ndiff.sh
```

EXIT CODE

The exit code indicates whether the scans are equal.

- 0 means that the scans are the same in all the aspects Ndiff knows about.
- 1 means that the scans differ.
- 2 indicates a runtime error, such as the failure to open a file.

BUGS

Report bugs to the nmap−dev mailing list at <dev@nmap.org>.

HISTORY

Ndiff started as a project by Michael Pattrick during the 2008 Google Summer of Code. Michael designed the program and led the discussion of its output formats. He wrote versions of the program in Perl and C++, but the summer ended shortly after it was decided to rewrite the program in Python for the sake of Windows (and Zenmap) compatibility. This Python version was written by David Fifield. James Levine **released**[1] a Perl script named Ndiff with similar functionality in 2000.

AUTHORS

David Fifield <david@bamsoftware.com>

Michael Pattrick <mpattrick@rhinovirus.org>

WEB SITE

https://nmap.org/ndiff/

NOTES

1. released
   http://seclists.org/nmap-hackers/2000/315