WORK AND PLAY WITH NMAP AND FRIENDS

David Fifield <david@bamsoftware.com> June 26, 2009

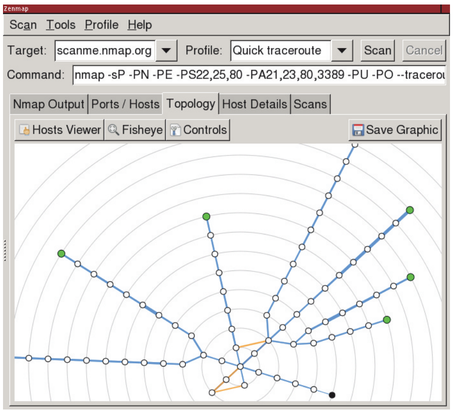
Nmap is a free network security scanner. It is best known as a port scanner, but it also has a variety of related abilities that complement this basic function. These include OS detection, service version identification, and custom script scanning. It comes with some companion tools, Nmap's "little brothers," that complement it in its purpose of network exploration and security auditing.

(Get Nmap from http://nmap.org/.)

Zenmap http://nmap.org/zenmap/

Zenmap is a graphical frontend for Nmap. It aims to make network scanning easy for beginners and to give additional power to expert Nmap users.

The program in its default view has a command line and a window where output is shown. Experts who know what they are doing can type in the command they want and go. But Zenmap also ships with a collection of common scans saved as scan profiles, having names like "Quick scan," "Ping scan," and "Intense scan." Selecting one of these fills in the command line with the appropriate options. We hope that this will eventually turn beginners into experts as they see the options that control their scans. Of course expert users can create their own custom scan profiles, like "Malware scan" or "DMZ audit."



Target: scanme.nmap.org
Profile: Quick traceroute
Command: nmap -sP -PN -PE -PS22,25,80 -PA21,23,80,3389 -PU -PO --tracerou

The results of several scans can be combined together in a process known as scan aggregation. The results of all scans run in the same window are combined as if they came from one big scan. You can take scan results from a week ago and update them with fresh information without losing the earlier results. Or you can do a quick scan of many hosts and augment it with an intensive scan of just a few of them. You can even have several scans running at the same time; as each one finishes, its results are added into the aggregation.

Zenmap can draw an interactive map of the network, called the "Topology." This function works best with scans that include route information; use Nmap's `--traceroute` option (included in the "Quick traceroute" scan profile). Scan aggregation causes the topology to be updated whenever a new scan is added.

Ndiff http://nmap.org/ndiff/

Ndiff is a tool for comparing Nmap scans. Given two Nmap scan logs, it shows how they differ: what hosts came up or went down, which ports became open or closed, DNS name changes, changes to server software (when available with Nmap's `-sV` option), and changes in operating system (when available with `-O`). It is designed to work just like the diff utility that compares text files.

Try this script in a crontab to get automated daily diffs.

```
#!/bin/sh
date=`date +%F`
cd /root/scans
nmap -v -T4 -F -sV -oA scan-$date targets > /dev/null
if [ -f scan-prev.xml ]; then
        ndiff scan-prev.xml scan-$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
```

Sample Ndiff output.

```
$ ndiff -v scan-1.xml scan-2.xml
-Nmap 4.85BETA4 at 2009-03-24 17:34
+Nmap 4.85BETA4 at 2009-03-25 16:35

+10.181.218.66:
+Host is up.
+Not shown: 998 closed ports
+PORT     STATE    SERVICE    VERSION
+222/tcp  open     rsh-spx
+8080/tcp filtered http-proxy

-utkjlegbx-701.example.com (10.196.172.89):
+cdgzhwik-216.example.com (10.196.172.89):
 Host is up.
```

Ncat http://nmap.org/ncat/

Ncat is a general-purpose network connection and troubleshooting tool inspired by the Netcat program and its many derivatives. Its most basic function is to operate as a raw client or server, relaying data between a socket and its own standard input and output. It is suitable for interactive use, for example in debugging a mail server, or as a backend network connector for non-network-aware programs. Ncat supports all the features of traditional Netcat programs and adds some innovations. Connections may be made over TCP, UDP, or SSL; over IPv4 or IPv6.

The best way to learn Ncat is by example. Try these sample commands and see many more at http://nmap.org/ncat/guide/.

Retrieve a web page.

```
ncat -C server 80
GET / HTTP/1.0
```

Connect through a proxy.

```
ncat --proxy proxy host port
```

Transfer a single file.

```
host2$ ncat -l > outputfile
host1$ ncat --send-only host2 < inputfile
```

Transfer many files.

```
host2$ ncat -l | tar xzv
host1$ tar czv files | ncat --send-only host2
```

Transfer a file through an intermediate broker (useful for getting around firewall restrictions).

```
host3$ ncat -l --broker
host2$ ncat host3 > outputfile
host1$ ncat --send-only host3 < inputfile
```

Run a chat server (small extension to brokering).

```
ncat -l --chat
```

Run an echo server on port 7.

```
ncat -l 7 --exec "/bin/cat"
```

Run a remote shell (be careful!).

```
ncat -l --exec "/bin/bash"
```

Connect to an SSL service.

```
ncat -v -C --ssl-verify pop.example.com 995
```

Unwrap an SSL service.

```
ncat -l localhost 143 --sh-exec \
  "ncat --ssl imap.example.com 993"
```

Make an IPv4-to-IPv6 gateway.

```
ncat -4 -l port --sh-exec \
  "ncat -6 host port"
```

Silly Perl tricks.

```
ncat -l --sh-exec 'perl -e "$| = 1; \
  while (<>) { print uc; }"'
```

NSE, the Nmap Scripting Engine http://nmap.org/book/nse.html

The Nmap Scripting Engine, or NSE, while not exactly new, is still not as well known as some other Nmap features. NSE is an embedded Lua interpreter and a set of network-specific libraries. With NSE you can get SSH host keys, date settings, and lists of Windows shares; do vulnerability assessment by checking for weak passwords, open proxies, and malware infections; and more.

To activate NSE, use the `-sC` option to run just the default scripts, or use `--script` with a list of the scripts or categories you want to run.

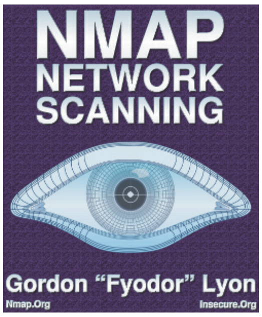
```
# nmap -sC target
# nmap --script=safe,vuln,whois target
```

Everybody wants to know how to scan for Conficker with Nmap. Here's how. (Also see `p2p-conficker.nse` for an alternative method of detection.)

```
# nmap -PN -T4 -p139,445 -n -v --script=smb-check-vulns --script-args safe=1 networks
```

A list of all the scripts that come with Nmap is online at http://nmap.org/nsedoc/.

More information



The Nmap book, *Nmap Network Scanning*, was published in January 2009. About half of the chapters are available free online, including those covering OS detection, the scripting engine, and Zenmap. A German translation is available since May 2009.

http://nmap.org/book/

Most project discussion and user support occurs on the development mailing list, nmap-dev@insecure.org. The list receives around 200–300 messages per month. The nmap-hackers@insecure.org list is used for major announcements; it receives less than one message per month. Subscribe to the lists or read the archives at http://seclists.org/.