

# New developments in Nmap

David Fifield <david@bamssoftware.com> October 12, 2007

Nmap (<http://insecure.org/nmap/>) is known for being the preeminent port scanner, however it is capable of much more than just port scanning. Recent development work, some of it done as part of the Google Summer of Code, has given Nmap powerful new capabilities. These are present only in recent releases. To get a recent Nmap, go to <http://insecure.org/nmap/download.html>. As of today, the latest release is 4.22SOC7.

Try these commands to see what the latest Nmap has to offer.

**nmap -sC scanme.nmap.org**

**nmap --script=safe,intrusive scanme.nmap.org**

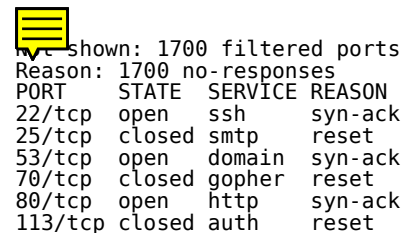
**nmap --script=HTTPAuth.nse scanme.nmap.org**

The `-sC` option activates NSE, the Nmap Scripting Engine. This powerful new feature of Nmap allows you to use custom scripts to extend Nmap in many ways. Scripts are just small programs, written in the Lua programming language, that have access to Nmap's knowledge of ports and its parallel socket engine. NSE allows the detection of services that were unidentifiable before, as well as other advanced features like the detection of open proxies and the extraction of web page titles.

Nmap comes with dozens of scripts, however not all of them are run by default. Scripts are placed in the following categories: backdoor, demo, discovery, intrusive, malware, safe, version, and vulnerability. By default scripts in the "safe" and "intrusive" categories are run with `-sC`, and scripts in the "version" category are run as part of standard version detection (`-sV`). To run others, use the `--script` option as shown above. To get a list of scripts, look in `/usr/share/nmap/scripts` on Unix or `C:\Program Files\Nmap\scripts` on Windows. Complete documentation for NSE is at <http://insecure.org/nmap/nse/>.

**nmap --reason scanme.nmap.org**

Did you ever wonder why a particular port was marked filtered? It might have been because the target didn't respond, or perhaps you received an ICMP Destination Unreachable. Nmap's new reason reporting causes it to display why it said what it did about a port.



```
Host: scanme.nmap.org (205.217.153.62)
Nmap scan report for scanme.nmap.org
Host is up (0.0000s).
Interesting ports on scanme.nmap.org:
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3 (protocol 2.0)
25/tcp    closed smtp
53/tcp    open  domain
70/tcp    closed gopher
80/tcp    open  http     Apache httpd 2.2.2 ((Fedora))
113/tcp   closed auth

Reason: 1700 filtered ports
Reason: 1700 no-responses
```

**nmap -p 'ssh,http\*,nntp' scanme.nmap.org**

**nmap -p '[1-1024],oracle,3306' scanme.nmap.org**

Quick, what's the port number for NNTP? What are the ports with known service names between 1 and 1024? Nmap's new, more powerful port selection answers these questions for you. It is now possible to specify ports using common port names rather than numbers. `*` and `?` wildcards are supported. The square bracket syntax scans only named ports. It's possible to mix and match any of these mechanisms in one command line. Remember to quote your strings because the port selection syntax uses shell metacharacters.

**nmap --traceroute scanme.nmap.org**

Nmap now has a traceroute function built in, and it offers some advantages over the standard traceroute program. Nmap's traceroute uses the results of a port scan, so the traceroute probes can be aimed at a known responsive port. Also, performing a parallel traceroute on many hosts at once will send fewer probes than tracing all the hosts individually.

## umit

Umit is Nmap's new graphical frontend. Start it up by typing `umit` or by clicking on the Umit icon. Umit can run any Nmap scan and show the results with syntax highlighting. Umit stores your scan results in a searchable database. You can graphically compare two saved scans to see what has changed ("What new machines have been added to my network?"). You can save your favorite scan parameters as a profile so it's easy to run the same scan against many targets.

Umit began as a project for the Google Summer of Code in 2005. After further development in 2006 and 2007 it is now distributed with Nmap.

