FUN WITH NMAP and FREE SOFTWARE DEVELOPMENT

David Fifield <david@bamsoftware.com> March 18, 2009

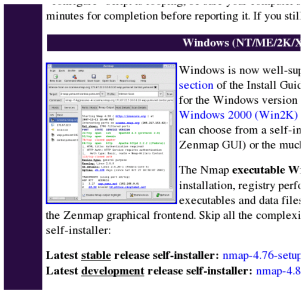
Nmap ("Network Mapper") is a powerful free tool for network exploration and security auditing. While its core function has always been port scanning, in its ten years of development it has grown into a general-purpose network security scanner. Today Nmap can identify the operating system of remote hosts, identify server software, and run custom scripts to gain even more information about a network.

HOWTO install Nmap with an executable installer (for noobs)

The Nmap home page is http://nmap.org/. Go to

http://nmap.org/download.html

and download the package appropriate for your system. There is an .exe for Windows, a .dmg for Mac OS X, and an .rpm for varieties of Unix. On a free Unix, use your package manager: `yum install nmap`, `apt-get install nmap`, or what have you. See http://nmap.org/book/install.html for full instructions.



minutes for completion before reporting it. If you stil

Windows (NT/ME/2K/X

Windows is now well-su
section of the Install Guid
for the Windows version
Windows 2000 (Win2K)
can choose from a self-in
Zenmap GUI) or the muc

The Nmap **executable W**
installation, registry perf
executables and data file
the Zenmap graphical frontend. Skip all the complexi
self-installer:

Latest stable release self-installer: nmap-4.76-setu
Latest development release self-installer: nmap-4.8

HOWTO install Nmap from source (for hackers)

At the download page you can download a .tgz for the Nmap source code. But if you're going to do that, you might as well go all the way and get a bleeding-edge copy from Subversion. The `svn` command is easily available on Unix (and installed by default on Mac OS X). On Windows the whole process is more difficult, but you knew that.

```
svn co --username guest --password "" svn://svn.insecure.org/nmap
cd nmap
./configure
make
```

You can then run `make install` to install the program, or just run it from within the distribution directory.

Your first scans

Always get permission before scanning a network. There is a host for which you already have permission: **scanme.nmap.org**. This server is set up specifically as a target for anyone testing Nmap. Let's start with the simplest possible scan. On Unix, make sure you're root, then run

```
nmap scanme.nmap.org
```

In a matter of seconds you'll get a list of open and closed ports on scanme. Try these other simple scans:

`nmap -O scanme.nmap.org` (operating system detection)
`nmap -sV scanme.nmap.org` (service detection)
`nmap -p 1-65535 scanme.nmap.org` (scan every port)
`nmap -A scanme.nmap.org` (the works: OS and service detection, script scanning, and traceroute)

HOT NEW NMAP FEATURES

Top ports

By default, Nmap doesn't scan every single port. (Use `–p 1–65535` if you want that.) Until recently, its selection of default ports was rather crude: all the ports in the range 1–1024, plus all other named ports. During the summer of 2008 Fyodor conducted scans of thousands of IPs on the Internet. We sorted the ports by how often they were found open. Now Nmap scans the most common 1,000 ports by default—fewer ports are scanned but the ones scanned are more likely to be open. With the –F (fast scan) option, only the top 100 ports are scanned. The effect of all this is better results in a shorter time. Try it:

```
  nmap scanme.nmap.org
  nmap –F scanme.nmap.org
  nmap ––top–ports 2000 scanme.nmap.org
```

Nmap Scripting Engine (NSE)

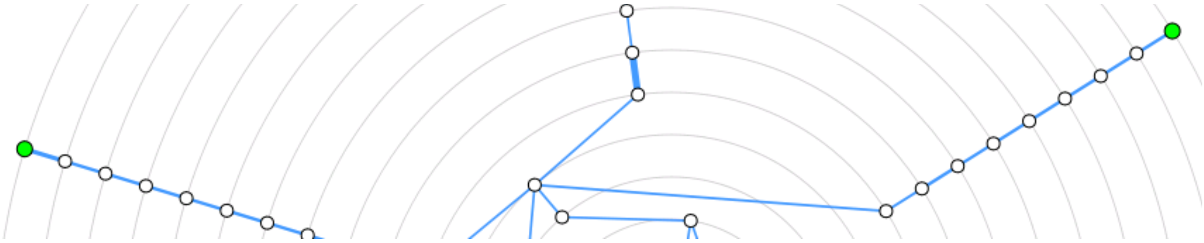
Some network detection operations are beyond the power of Nmap's general-purpose service and OS detection. As a simple example, to check if an FTP server allows anonymous logins, you have to connect to the service, send an anonymous user name, then parse the server's response. The Nmap Scripting Engine (NSE) handles this and much more.
NSE uses the embedded Lua programming language, the same language used in other popular applications like World of Warcraft. NSE extends Lua with libraries specialized for network scanning. Nmap already comes with dozens of scripts. Activate NSE by passing the `–sC` option to Nmap, or list just the scripts you want with `––script`.

```
  nmap –sC scanme.nmap.org
  nmap ––script=html–title,whois,ssh–hostkey scanme.nmap.org
```

http://nmap.org/book/nse.html   http://nmap.org/nsedoc/

Topology mapping with the Zenmap GUI

Nmap comes with a GUI called Zenmap that aims to make network scanning easy for beginners and more convenient for advanced users. Last summer Zenmap gained a fantastic new ability. Using traceroute information gained from an Nmap scan, it will draw you an interactive network graph to explore. You have to try it to see how neat it is. Run a few scans with the "Quick traceroute" scan profile then click the "Topology" tab.



Zenmap's topology mode was originally a separate project called RadialNet, which viewed results but could not run scans. Because both projects were free software, we were able to combine them into one application with the abilities of both.

Nmap is a rapidly developed project. For the latest, see

http://nmap.org/changelog.html

The top 100 TCP ports

80	http
23	telnet
443	https
21	ftp
22	ssh
25	smtp
3389	ms-term-serv
110	pop3
445	microsoft-ds
139	netbios-ssn
143	imap
53	domain
135	msrpc
3306	mysql
8080	http-proxy
1723	pptp
111	rpcbind
995	pop3s
993	imaps
5900	vnc
1025	NFS-or-IIS
587	submission
8888	sun-answerbook
199	smux
1720	H.323/Q.931
465	smtps
548	afp
113	auth
81	hosts2-ns
6001	X11:1
10000	snet-sensor-mgmt
514	shell
5060	sip
179	bgp
1026	LSA-or-nterm
2000	callbook
8443	https-alt
8000	http-alt
32768	unknown
554	rtsp
26	rsftp
1433	ms-sql-s
49152	unknown
2001	dc
515	printer
8008	http
49154	unknown
1027	IIS
5666	nrpe
646	ldp
5000	upnp
5631	pcanywheredata
631	ipp
49153	unknown
8081	blackice-icecap
2049	nfs
88	kerberos-sec
79	finger
5800	vnc-http
106	pop3pw
2121	ccproxy-ftp
1110	nfsd-status
49155	unknown
6000	X11
513	login
990	ftps
5357	unknown
427	svrloc
49156	unknown
543	klogin
544	kshell
5101	admdog
144	news
7	echo
389	ldap
8009	ajp13
3128	squid-http
444	snpp
9999	abyss
5009	airport-admin
7070	realserver
5190	aol
3000	ppp
5432	postgresql
1900	upnp
3986	mapper-ws_ethd
13	daytime
1029	ms-lsa
9	discard
5051	ida-agent
6646	unknown
49157	unknown
1028	unknown
873	rsync
1755	wms
2717	unknown
4899	radmin
9100	jetdirect
119	nntp
37	time

Companion tools

Nmap is much more than a port scanner, and the Nmap distribution is now more than just Nmap. These other applications are part of the standard installation package.

Zenmap is a graphical user interface for Nmap. Aside from the topology mapping already mentioned, it can combine the results of several scans and search through a database of saved scans.

Ncat is a modern replacement for the versatile Netcat tool. It is just what its name implies: the Unix utility `cat` for the network. Ncat comes with some neat features like proxying and SSL support.

Ndiff takes two Nmap results files and compares them, showing you what changed. It will, for example, show you what hosts have come up or gone down, and any ports that have changed state.

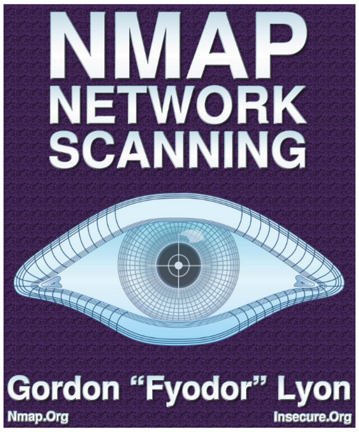
http://nmap.org/zenmap/ http://nmap.org/ncat/ http://nmap.org/ndiff/

NMAP RESOURCES

Nmap Network Scanning

Published in January 2009, *Nmap Network Scanning* is *the* book on the subject, written by the author of Nmap. Half the book is available free online. It describes every feature and option in detail and has lots of examples of how they apply to you, the intrepid network scanner. You'll find out how to get a list of addresses belonging to an organization, use unwitting laser printers to perform a stealthy scan, tune Nmap performance, and even how to defend yourself against Nmap. Not to be missed is the account of how Trinity used Nmap to save humanity in *The Matrix Reloaded.*

http://nmap.org/book/



Mailing Lists

There are three Nmap-related mailing lists to be aware of. nmap-hackers is very low-volume, suitable for the whole family. The others are for aficionados. Subscribe to any of these lists by going to

http://seclists.org/

nmap-hackers@insecure.org
<1 message per month

Anyone even casually interested in Nmap should be on this list. Only release announcements and other big news goes here.

Sample post

Nmap 4.50 released
Hi everyone. I'm proud to say that Nmap has reached its 10th anniversary since I released it in 1997, and it is still going strong!

nmap-dev@insecure.org
150–250 messages per month

Join this list if you want to follow up on a feature request or bug report, or if you want to get involved in Nmap development.

Sample post

[PATCH] timing.cc integer overflow
Please find attached an attempt to fix the integer overflow in the printStats method of ScanProgressMeter (timing.cc).

nmap-svn@insecure.org
>400 messages per month

For those who like pain. Every single Subversion commit, delivered to you within moments of it happening.

Sample post

r12301 2009-02-25 11:01:50
In nmap-os-db, change GCD=<7 to GCD=1–5. The "<7" value was meant to encompass small multiples of 1 when a GCD of 1 was observed.

NMAP IS A POWERFUL TOOL
USE CAREFULLY AND RESPONSIBLY

WHY FREE SOFTWARE?

For many computer users, and even many programmers, the experience of using software at least partly unpleasant. For them, using a computer means having to type in a CD key; it means paying for dubious upgrades; it means having 14 days left to register; it means spyware and adware; it means the computer doing things without your consent or knowledge. When you have to ask permission to reinstall a program, it's natural to ask, "Whose computer is this, anyway?"

The winning alternative is free software—software that you can use, study, modify, and share. Free software is good for users, who don't have to put up with proprietary tricks anymore; and it is especially good for developers, who now have control over the code that runs on their computers.

Nmap's COPYING file has this to say:

> Source is provided to this software because we believe users have a right to know exactly what a program is going to do before they run it. This also allows you to audit the software for security holes (none have been found so far). Source code also allows you to port Nmap to new platforms, fix bugs, and add new features.

In computer security there are white hats and black hats—good guys and bad guys. Just so in the wider world of software development. Some programmers get paid to write DRM systems and others get paid to enhance open-source tools. You can do good for yourself without doing harm to others.

HOWTO get started in free software development

Step 1. Stop using Windows and Mac OS X.

To be a free software hacker you need to use a free OS. To be taken seriously you will need day-to-day experience with the environment used by the programmers you want to work with. Download a free Unix: GNU/Linux, FreeBSD, NetBSD, OpenBSD. Pick a side in vi versus Emacs. Start reading some source code—that's what it's there for.

Step 2. Find some software you care about.

Find a project you are interested in and join the mailing list. Take a tour through the source code. If no existing project interests you, start your own. Even packaging up 100 lines of Perl and putting it on the web will give you useful skills.

Step 3. Write a patch.

Fix a bug or write a new feature and send the code to the mailing list. Be prepared to revise it. When it is accepted, reflect on how your code will have perhaps thousands of users after the next release.

Congratulations, you are now a bona fide free software programmer. Remember, though, that if you plan to make a living at this, you have to be more than just bona fide—you have to be good enough that someone will want to pay you. So keep enhancing your skills through practice with your own and others' projects, and start reading some serious programming books.

Google Summer of Code

If you are already a good programmer, you could be writing free software—and getting paid for it—as early as this summer.

http://code.google.com/soc/

Google will pay $4,500 to 1,000 students to code for an open-source project over the summer. You can apply to as many projects as you wish. The application period is from March 23 to April 3, so don't delay.

Happy Hacking!