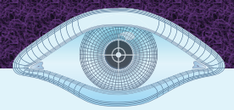
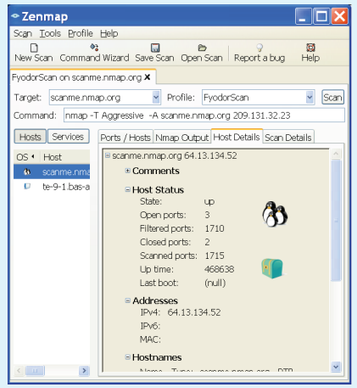


Official Nmap Project Guide to Network Discovery and Security Scanning

The Nmap Security Scanner is a free and open source utility used by millions of people for network discovery, administration, inventory, and security auditing. Nmap uses raw IP packets in novel ways to determine what hosts are available on a network, what services (application name and version) those hosts are offering, what operating systems they are running, what type of packet filters or firewalls are in use, and more. Nmap was named "Information Security Product of the Year" by *Linux Journal* and *Info World*. It was also used by hackers in seven movies, including *The Matrix Reloaded*, *Die Hard 4*, and *The Bourne Ultimatum*. Nmap runs on all major computer operating systems, plus the Amiga. A traditional command-line interface and the Zenmap GUI are included:

```
# nmap -sVC -O -T4 scanme.nmap.org

Starting Nmap ( http://nmap.org )
Interesting ports on scanme.nmap.org (64.13.134.52):
Not shown: 1710 filtered ports
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 4.3 (protocol 2.0)
53/tcp  open   domain
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.2.2 ((Fedora))
|_ HTML title: Go ahead and ScanMe!
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.20-1 (Fedora Core 5)
Uptime: 5.378 days
Nmap done: 1 IP address (1 host up) scanned in 51.818 s
```



About this book

Nmap Network Scanning is the official guide to the Nmap Security Scanner. From explaining port scanning basics for novices to detailing low-level packet crafting methods used by advanced hackers, this book suits all levels of security and networking professionals. A 42-page reference guide documents every Nmap feature and option, while the rest of the book demonstrates how to apply those features to quickly solve real-world tasks. Topics include:

- » Detecting and subverting firewalls and intrusion detection systems
- » Optimizing Nmap performance
- » Automating common networking tasks with the Nmap Scripting Engine

Visit *http://nmap.org/book* for updates and sample chapters.

About the author

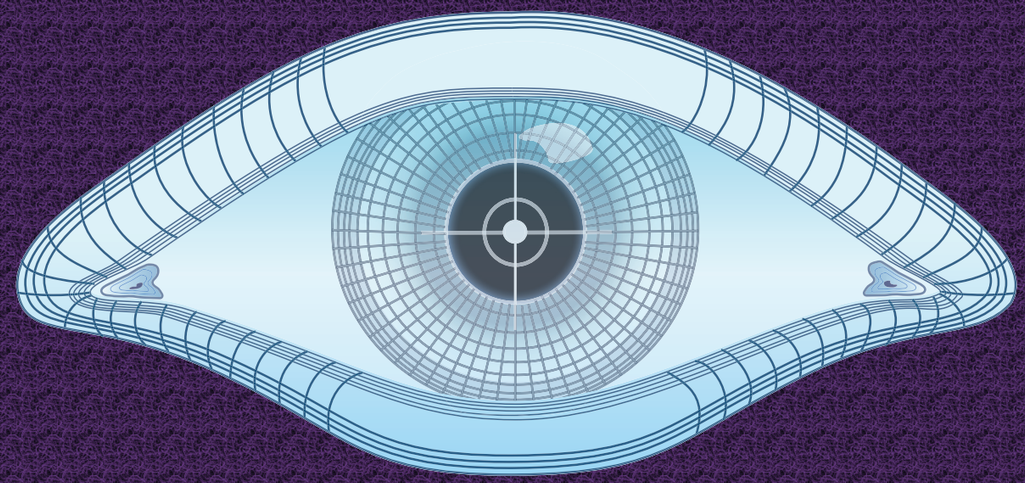
Gordon Lyon (also known by his nickname Fyodor) released Nmap in 1997 and continues to coordinate its development. He also maintains the *Insecure.Org*, *Nmap.Org*, *SecLists.Org*, and *SecTools.Org* security resource sites and has written seminal papers on OS detection and stealth port scanning. He is a founding member of the Honeynet Project, a popular speaker at security conferences, and co-author of the books "*Know Your Enemy: Honeynets*" and "*Stealing the Network: How to Own a Continent*". Gordon is President of Computer Professionals for Social Responsibility (CPSR), which has promoted free speech, security, and privacy since 1981.

Security / Networking $49.95 U.S.
ISBN 9780979958717
54995
9 780979 958717

NMAP NETWORK SCANNING

Fyodor

NMAP NETWORK SCANNING



Gordon "Fyodor" Lyon

Nmap.Org Insecure.Org