

[Download](#)[Reference Guide](#)[Book](#)[Docs](#)[Zenmap GUI](#)[In the Movies](#)[Nmap Network Scanning](#) / Chapter 15. Nmap Reference Guide[◀ Prev](#)[Next ▶](#)

Chapter 15. Nmap Reference Guide

Table of Contents

[Description](#)[Options Summary](#)[Target Specification](#)[Host Discovery](#)[Port Scanning Basics](#)[Port Scanning Techniques](#)[Port Specification and Scan Order](#)[Service and Version Detection](#)[OS Detection](#)[Nmap Scripting Engine \(NSE\)](#)[Timing and Performance](#)[Firewall/IDS Evasion and Spoofing](#)[Output](#)[Miscellaneous Options](#)[Runtime Interaction](#)[Examples](#)[Nmap Book](#)[Bugs](#)[Authors](#)[Legal Notices](#)[Nmap Copyright and Licensing](#)[Creative Commons License for this Nmap Guide](#)[Source Code Availability and Community Contributions](#)[No Warranty](#)[Inappropriate Usage](#)[Third-Party Software and Funding Notices](#)[United States Export Control](#)

Name

nmap — Network exploration tool and security / port scanner

Synopsis

```
nmap [ <Scan Type> ... ] [ <Options> ] { <target specification> }
```

Description

**Note**

This document describes the very latest version of Nmap available from <https://nmap.org/download.html> or <https://nmap.org/dist/?C=M&O=D>. Please ensure you are using the latest version before reporting that a feature doesn't work as described.

Nmap (“Network Mapper”) is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

The output from Nmap is a list of scanned targets, with supplemental information on each depending on the options used. Key among that information is the “interesting ports table”. That table lists the port number and protocol, service name, and state. The state is either open, filtered, closed, or unfiltered. Open means that an application on the target machine is listening for connections/packets on that port. Filtered means that a firewall, filter, or other network obstacle is blocking the port so that Nmap cannot tell whether it is open or closed. Closed ports have no application listening on them, though they could open up at any time. Ports are classified as unfiltered when they are responsive to Nmap's probes, but Nmap cannot determine whether they are open or closed. Nmap reports the state combinations open|filtered and closed|filtered when it cannot determine which of the two states describe a port. The port table may also include software version details when version detection has been requested. When an IP protocol scan is requested (-s0), Nmap provides information on supported IP protocols rather than listening ports.

In addition to the interesting ports table, Nmap can provide further information on targets, including reverse DNS names, operating system guesses, device types, and MAC addresses.

A typical Nmap scan is shown in [Example 15.1](#). The only Nmap arguments used in this example are -A, to enable OS and version detection, script scanning, and traceroute; -T4 for faster execution; and then the hostname.

Example 15.1. A representative Nmap scan

```
# nmap -A -T4 scanme.nmap.org

Nmap scan report for scanme.nmap.org (74.207.244.221)
Host is up (0.029s latency).
rDNS record for 74.207.244.221: li86-221.members.linode.com
Not shown: 995 closed ports
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 5.3p1 Debian 3ubuntu7 (protocol 2.0)
|_ ssh-hostkey: 1024 8d:60:f1:7c:ca:b7:3d:0a:d6:67:54:9d:69:d9:b9:dd (DSA)
|_ 2048 79:f8:09:ac:d4:e2:32:42:10:49:d3:bd:20:82:85:ec (RSA)
80/tcp    open  http         Apache httpd 2.2.14 ((Ubuntu))
|_ http-title: Go ahead and ScanMe!
646/tcp   filtered ldp
1720/tcp  filtered H.323/Q.931
9929/tcp  open  nping-echo   Nping echo
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6.39
OS details: Linux 2.6.39
Network Distance: 11 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:kernel

TRACEROUTE (using port 53/tcp)
HOP RTT      ADDRESS
[Cut first 10 hops for brevity]
```

```
11 17.65 ms li86-221.members.linode.com (74.207.244.221)

Nmap done: 1 IP address (1 host up) scanned in 14.40 seconds
```

The newest version of Nmap can be obtained from <https://nmap.org>. The newest version of this man page is available at <https://nmap.org/book/man.html>. It is also included as a chapter of [Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning](#).

Site Search



Nmap Security Scanner

Ref Guide

Install Guide

Docs

Download

Nmap OEM

Npcap packet capture

User's Guide

API docs

Download

Npcap OEM

Security Lists

Nmap Announce

Nmap Dev

Full Disclosure

Open Source Security

BreachExchange

Security Tools

Vuln scanners

Password audit

Web scanners

Wireless

Exploitation

About

About/Contact

Privacy

Advertising

Nmap Public Source License

