# Port Scanning

NMAP

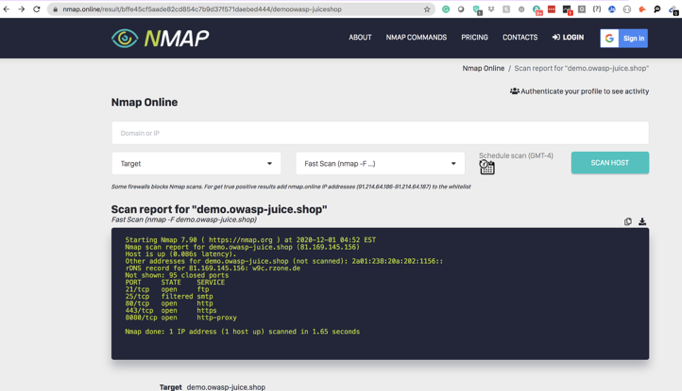
Nmap ("Network Mapper") is a free and open source ([license](https://nmap.org/npsl/)) utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. 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.

Nmap is ...

* **Flexible**: Supports dozens of advanced techniques for mapping out networks filled with IP filters, firewalls, routers, and other obstacles. This includes many [port scanning](https://nmap.org/book/man-port-scanning-techniques.html) mechanisms (both TCP & UDP), [OS detection](https://nmap.org/book/osdetect.html), [version detection](https://nmap.org/book/vscan.html), ping sweeps, and more. See the [documentation page](https://nmap.org/docs.html).
* **Powerful**: Nmap has been used to scan huge networks of literally hundreds of thousands of machines.
* **Portable**: Most operating systems are supported, including Linux, Microsoft Windows, FreeBSD, OpenBSD, Solaris, IRIX, Mac OS X, HP-UX, NetBSD, Sun OS, Amiga, and more.
* **Easy**: While Nmap offers a rich set of advanced features for power users, you can start out as simply as "nmap -v -A *targethost*". Both traditional command line and graphical (GUI) versions are available to suit your preference. Binaries are available for those who do not wish to compile Nmap from source.
* **Free**: The primary goals of the Nmap Project is to help make the Internet a little more secure and to provide administrators/auditors/hackers with an advanced tool for exploring their networks. Nmap is available for [free download](https://nmap.org/download.html), and also comes with full source code that you may modify and redistribute under the terms of the [license](https://nmap.org/data/COPYING).
* **Well Documented**: Significant effort has been put into comprehensive and up-to-date man pages, whitepapers, tutorials, and even a whole book! Find them in multiple languages [here](https://nmap.org/docs.html).
* **Supported**: While Nmap comes with no warranty, it is well supported by a vibrant community of developers and users. Most of this interaction occurs on the [Nmap mailing lists](https://nmap.org/#lists). Most bug reports and questions should be sent to the [nmap-dev list](https://seclists.org/nmap-dev), but only after you read the [guidelines](https://nmap.org/book/man-bugs.html). We recommend that all users subscribe to the low-traffic [nmap-hackers](https://seclists.org/nmap-hackers) announcement list. You can also find Nmap on [Facebook](http://facebook.com/nmap) and [Twitter](http://twitter.com/nmap). For real-time chat, join the #nmap channel on [Freenode](http://freenode.net/) or [EFNet](http://www.efnet.org/).
* **Acclaimed**: Nmap has won numerous awards, including "Information Security Product of the Year" by Linux Journal, Info World and Codetalker Digest. It has been featured in hundreds of magazine articles, several movies, dozens of books, and one comic book series. Visit the [press page](https://nmap.org/nmap_inthenews.html) for further details.
* **Popular**: Thousands of people download Nmap every day, and it is included with many operating systems (Redhat Linux, Debian Linux, Gentoo, FreeBSD, OpenBSD, etc). It is among the top ten (out of 30,000) programs at the Freshmeat.Net repository. This is important because it lends Nmap its vibrant development and user support communities.

<https://nmap.org/>

## https://nmap.online/



‘demo.owasp-juice.shop

With OS detection

Starting Nmap 7.90 ( https://nmap.org ) at 2020-12-01 05:02 EST

Nmap scan report for demo.owasp-juice.shop (81.169.145.156)

Host is up (0.086s latency).

Other addresses for demo.owasp-juice.shop (not scanned): 2a01:238:20a:202:1156::

rDNS record for 81.169.145.156: w9c.rzone.de

Not shown: 995 closed ports

PORT STATE SERVICE VERSION

21/tcp open ftp ftpd.bin round-robin file server 3.4.0r14

|\_ftp-anon: Anonymous FTP login allowed (FTP code 230)

| ftp-syst:

| STAT:

| Server status:

| Transfer mode: ASCII

| List mode: UNIX

| Current number of users: 29

| Maximum number of users: 250

| Idle timeout: 300 seconds

| Hostname: desiderata

|\_End of server status.

25/tcp filtered smtp

80/tcp open http-proxy F5 BIG-IP load balancer http proxy

|\_http-cors: HEAD GET POST PUT DELETE PATCH

| http-robots.txt: 1 disallowed entry

|\_/ftp

| http-server-header:

| BigIP

|\_ Cowboy

|\_http-title: OWASP Juice Shop

443/tcp open ssl/ssl Apache httpd (SSL-only mode)

|\_http-cors: HEAD GET POST PUT DELETE PATCH

| http-robots.txt: 1 disallowed entry

|\_/ftp

|\_http-server-header: Apache/2.4.43 (Unix)

|\_http-title: OWASP Juice Shop

| ssl-cert: Subject: commonName=\*.owasp-juice.shop

| Subject Alternative Name: DNS:\*.owasp-juice.shop, DNS:owasp-juice.shop

| Not valid before: 2020-09-30T00:00:00

|\_Not valid after: 2021-10-14T12:00:00

8080/tcp open http-proxy F5 BIG-IP load balancer http proxy

|\_http-cors: HEAD GET POST PUT DELETE PATCH

| http-robots.txt: 1 disallowed entry

|\_/ftp

| http-server-header:

| BigIP

|\_ Cowboy

|\_http-title: OWASP Juice Shop

Device type: load balancer

Running (JUST GUESSING): F5 Networks TMOS 11.6.X (87%)

OS CPE: cpe:/o:f5:tmos:11.6

Aggressive OS guesses: F5 BIG-IP Local Traffic Manager load balancer (TMOS 11.6) (87%)

No exact OS matches for host (test conditions non-ideal).

Network Distance: 14 hops

Service Info: Device: load balancer

TRACEROUTE (using port 8888/tcp)

HOP RTT ADDRESS

1 0.94 ms 91.214.64.185

2 10.65 ms 45.11.82.1

3 0.20 ms 208.91.107.205

4 0.22 ms border2.ae6.dedipath-1-3-10-12.nyj004.pnap.net (64.74.240.241)

5 1.03 ms core4.be1-bbnet1.nym007.pnap.net (216.52.95.29)

6 15.93 ms bbr2.ae4.inapvox-lag.nym007.pnap.net (64.95.158.217)

7 0.88 ms bbr1.ae7.nym007.pnap.net (64.95.158.73)

8 85.77 ms bbr1.ae103.inapbb-nym-lon-3.lon.pnap.net (64.95.159.22)

9 66.62 ms 173.231.129.66

10 ...

11 83.62 ms ae-4.bb-b.bs.kae.de.oneandone.net (212.227.120.49)

12 83.12 ms 212.227.112.119

13 86.44 ms 110.po19.fiddlersriddle.as6724.net (193.141.3.141)

14 85.88 ms w9c.rzone.de (81.169.145.156)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .

Nmap done: 1 IP address (1 host up) scanned in 28.43 seconds