



zmap (1)

Contents

[NAME](#)

[SYNOPSIS](#)

[DESCRIPTION](#)

[OPTIONS](#)

[Basic options](#)

[Scan options](#)

[Network options](#)

[Advanced options](#)

[Additional options](#)

[EXAMPLES](#)

[WARNING](#)

[AUTHOR](#)

NAME

zmap – A fast Internet-wide scanner

SYNOPSIS

zmap [*OPTIONS* ...]

DESCRIPTION

ZMap is a network tool for scanning the entire Internet (or large samples).

OPTIONS

Basic options

-p, --target-port=port

TCP port number to scan (for SYN scans)

-o, --output-file=name

When using an output module that uses a file (such as the default), write results to this file. Use - for stdout.

-b, --blacklist-file=path

File of subnets to exclude, in CIDR notation (e.g. 192.168.0.0/16), one-per line. It is recommended you use this to exclude RFC 1918 addresses, multicast, IANA reserved space, and other IANA special-purpose addresses. An example blacklist file is provided in **conf/blacklist.conf** for this purpose.

-w, --whitelist-file=path

File of subnets to constrain scan to, in CIDR notation, e.g. 192.168.0.0/16

Scan options

-n, --max-targets=n

Cap number of targets to probe (as a number or a percentage of the address space)

-N, --max-results=n

Cap number of results to return

-t, --max-runtime=secs

Cap length of time for sending packets

-r, --rate=pps

Set send rate in packets/sec

-B, --bandwidth=bps

Set send rate in bits/second (supports suffixes G, M and K). This overrides the **--rate** flag.

-c, --cooldown-time=secs

How long to continue receiving after sending last probe (default=8)

-e, --seed=n

Seed used to select address permutation. Specify the same seed in order to scan the same sample repeatedly.

-T, --sender-threads=n

Threads used to send packets (default=1)

-P, --probes=n

Number of probes to send to each IP (default=1)

-d, --dryrun

Print out each packet to stdout instead of sending it. (May be useful for debugging.)

Network options

-s, --source-port=port|range

Source port(s) for scan packets

-S, --source-ip=ip|range

Source address(es) for scan packets

-G, --gateway-mac=addr

Specify gateway MAC address. All packets will be sent to this Ethernet address.

-i, --interface=name

Specify network interface to use.

-X, --vpn

If using ZMap through a VPN, use this option. Instead of sending raw Ethernet frames, ZMap will send IP packets. When using this option, it is generally also necessary to provide the interface (through the **-i** flag).

Advanced options

-M, --probe-module=name

Select probe module (default=tcp_synscan)

-O, --output-module=name

Select output module (default=simple_file)

-f, --output-fields=fields

Fields that should be output in result set; see **--list-output-fields**

--probe-args=args

Arguments to pass to probe module

--output-args=args

Arguments to pass to output module

--list-output-modules

List available output modules

--list-probe-modules

List available probe modules

--list-output-fields

List all fields that can be output (using **--output-fields**) by selected probe module

Additional options

-C, --config=filename

Read a configuration file, which can specify any of these options (default=/etc/zmap/zmap.conf)

-q, --quiet

Do not print status updates

-g, --summary

Print configuration and summary at end of scan

-v, --verbosity=n

Level of log detail (0-5) (default=3)

-h, --help

Print help and exit

-V, --version

Print version and exit

EXAMPLES

Scan the whole Internet for hosts with port 443 open (results discarded):

zmap -p 443

Find 5 HTTP servers (port 80), scanning at 10 Mb/s, print the results to stdout:

```
zmap -N 5 -B 10M -p 80 -o -
```

WARNING

By default, ZMap attempts to scan at the line speed of your Ethernet interface and can easily use 1 Gbit/second of bandwidth. If your network is not able to support sending packets this quickly, your local network may become congested, causing connectivity problems for you and those around you. Use the `-B` (`--bandwidth`) option to set ZMap's maximum bandwidth to an appropriate limit for your network and upstream connection.

AUTHOR

Zakir Durumeric, Eric Wustrow, J. Alex Halderman (<https://www.zmap.io>)

