Zmap 2.1.1 Cheatsheet (ingenieriainformatica.uniovi.es)

Fast internet-wide scanner

https://zmap.io/

GENERAL USAGE

```
zmap [OPTION]... [SUBNETS]…
```

```
operario@kali:~$ sudo zmap -p 80 88.151.16.0/24 -o asturias.txt
Oct 29 18:33:29.149 [WARN] blacklist: ZMap is currently using the default blacklist located at /etc/zmap/blacklist.
conf. By default, this blacklist excludes locally scoped networks (e.g. 10.0.0.0/8, 127.0.0.1/8, and 192.168.0.0/16
). If you are trying to scan local networks, you can change the default blacklist by editing the default ZMap confi
guration at /etc/zmap/zmap.conf.
Oct 29 18:33:29.153 [INFO] zmap: output module: csv
 0:00 0%; send: 10 0 p/s (261 p/s avg); recv: 0 0 p/s (0 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 0.00%
 0:01 13%; send: 256 done (6.23 Kp/s avg); recv: 17 16 p/s (16 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 6.64%
 0:02 26%; send: 256 done (6.23 Kp/s avg); recv: 76 56 p/s (36 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 29.69%
 0:03 38%; send: 256 done (6.23 Kp/s avg); recv: 76 0 p/s (24 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 29.69%
 0:04 51%; send: 256 done (6.23 Kp/s avg); recv: 76 0 p/s (18 p/s avg); drops: 0 p/s (0 p/s avg); hitrate: 29.69%
 0:05 64% (3s left); send: 256 done (6.23 Kp/s avg); recv: 76 0 p/s (14 p/s avg); drops: 0 p/s (0 p/s avg); hitrate
: 29.69%
 0:06 77% (2s left); send: 256 done (6.23 Kp/s avg); recv: 76 0 p/s (12 p/s avg); drops: 0 p/s (0 p/s avg); hitrate
: 29.69%
 0:07 89% (1s left); send: 256 done (6.23 Kp/s avg); recv: 76 0 p/s (10 p/s avg); drops: 0 p/s (0 p/s avg); hitrate
: 29.69%
Oct 29 18:33:37.339 [INFO] zmap: completed
```

NOTES

Probe-module (tcp_synscan): Probe module that sends a TCP SYN packet to a specific port. Possible classifications are: synack and rst. A SYN-ACK packet is considered a success and a reset packet is considered a failed response.
Output-module (csv): By default, ZMap prints out unique, successfulIP addresses (e.g., SYN-ACK from a TCP SYN scan) in ASCII form (e.g., 192.168.1.5) to stdout or the specified output file. Internally this is handled by the "csv" output module and is
equivalent to running zmap --output-module=csv --output-fields=saddr --output-filter="success = 1 && repeat = 0".

OPTIONS

BASIC ARGUMENTS

-b, --blacklist-file=path: File of subnets to exclude, in CIDR notation, e.g. 192.168.0.0/16

-o, --output-file=name: Output file

-p, --target-port=port: port number to scan (for TCP and UDP scans)

-w, --whitelist-file=path: File of subnets to constrain scan to, in CIDR notation, e.g. 192.168.0.0/16

SCAN OPTIONS

--retries=n: Max number of times to try to send packet if send fails (default=`10')

--shard=n: Set which shard this scan is (0 indexed) (default=`0')

--shards=N: Set the total number of shards (default=`1')

-B, --bandwidth=bps: Set send rate in bits/second (supports suffixes G, M and K)

-c, --cooldown-time=secs: How long to continue receiving after sending last probe (default=`8')

-d, --dryrun: Don't actually send packets

-e, --seed=n: Seed used to select address permutation

-N, --max-results=n: Cap number of results to return

-n, --max-targets=n: Cap number of targets to probe (as a number or a percentage of the address space)

-P, --probes=n: Number of probes to send to each IP (default=`1')

-r, --rate=pps: Set send rate in packets/sec

-t, --max-runtime=ses: Cap length of time for sending packets

ADDITIONAL OPTIONS

--cores=STRING: Comma-separated list of cores to pin to

--ignore-invalid-hosts: Ignore invalid hosts in whitelist/blacklist file

--max-sendto-failures=n: Maximum NIC sendto failures before scan is aborted (default=`-1')

--min-hitrate=n: Minimum hitrate that scan can hit before scan is aborted (default=`0.0')

NETWORK OPTIONS

--source-mac=addr: Source MAC address

-G, --gateway-mac=addr: Specify gateway MAC address

-i, --interface=name: Specify network interface to use

-S, --source-ip=ip|range: Source address(es) for scan packets

-s, --source-port=port|range: Source port(s) for scan packets

-X, --vpn: Sends IP packets instead of Ethernet (for VPNs)

PROBE MODULES

--list-probe-modules: List available probe modules

--probe-args=args: Arguments to pass to probe module

-M, --probe-module=name: Select probe module (default=`tcp_synscan')

DATA OUTPUT

--list-output-fields: List all fields that can be output by selected probe module

--list-output-modules: List available output modules

--output-args=args: Arguments to pass to output module

--output-filter=filter: Specify a filter over the response fields to limit what responses get sent to the output module

-f, --output-fields=fields: Fields that should be output in result set

-O, --output-module=name: Select output module (default=`default')

LOGGING AND METADATA

--disable-syslog: Disables logging messages to syslog

--notes=notes: Inject user-specified notes into scan metadata

--user-metadata=json: Inject user-specified JSON metadata into scan metadata

-L, --log-directory=directory: Write log entries to a timestamped file in this directory

-C, --config=filename: Read a configuration file, which can specify any of these options (default=`/etc/zmap/zmap.conf')	**-l, --log-file=name**: Write log entries to file
-h, --help: Print help and exit	**-m, --metadata-file=name**: Output file for scan metadata (JSON)
-T, --sender-threads=n: Threads used to send packets (default=`1')	**-q, --quiet**: Do not print status updates
-V, --version: Print version and exit	**-u, --status-updates-file=name**: Write scan progress updates to CSV file
EXAMPLES	**-v, --verbosity=n**: Level of log detail (0-5) (default=`3')
zmap -p 80 (scan the Internet for hosts on tcp/80 and output to stdout)	**by José Manuel Redondo López**
zmap -N 5 -B 10M -p 80 (find 5 HTTP servers, scanning at 10 Mb/s)	
zmap -p 80 10.0.0.0/8 192.168.0.0/16 -o (scan both subnets on tcp/80)	
zmap -p 80 1.2.3.4 10.0.0.3 (scan 1.2.3.4, 10.0.0.3 on tcp/80)	