

Forum: [Hack Forums](#)

Thread: [Port scan the entire internet in 5-10 minutes \(masscan tool\)](#)

Hackers - November 1, 2025, 2:32 pm

MASSCAN: Mass IP port scanner

Scan the internet in 5~ minutes

I know there are a number of people here who use nmap, but there are other tools that may be faster for your purposes if you are scanning in bulk for anything in particular, across your high number of personal servers.

Quote: "TCP port scanner, spews SYN packets asynchronously, scanning entire Internet in under 5 minutes."

You can check out the masscan repo here:

Use only within all local, national, or international laws, regulations, and terms of service or other agreements for personal use, in agreement with all subsequent terms or conditions of use defined in the masscan repository, your personal machine or server, ISP requirements, and in full compliance with any other required or implied rules.

<https://github.com/robertdavidgraham/masscan>

current:

<https://github.com/robertdavidgraham/masscan/tree/b99d433505f942fb384516553442c15322efc472>

AI Quote: A high-throughput port scanner engineered for Internet-scale discovery. From a single machine it can probe the public address space in under five minutes, transmitting on the order of 10 million packets per second.

Command syntax and output follow familiar port-scanner conventions (think nmap), so typical flags and workflow feel natural. The tool is optimized for wide, distributed scanning of many hosts rather than deep, slow inspection of a single target.

Under the hood it performs asynchronous packet transmission (similar in approach to scanrand, unicornscan, and ZMap) and accepts arbitrary port and address ranges for maximum flexibility.

Important safety note: the scanner implements its own lightweight TCP/IP handling. Running anything beyond simple stateless port probes can interfere with your system's network stack. To avoid conflicts you should either bind probes to an alternate source IP with --src-ip, or fix source ports with --src-port and then block those ports at the host firewall (pf/iptables) so the kernel doesn't attempt to use them for normal connections.

To be legendary,
do legendary things.

RITARI - November 2, 2025, 5:02 am

Nmap is better when you want more detailed results such as service/version enumeration or OS detection. Masscan is useful for very large ranges due to its speed.

Hackers - November 2, 2025, 5:22 am

(Nov 2, 2025 06:02 AM)RITARI Wrote: [\[CITE\]](#) Nmap is better when you want more detailed results such as service/version enumeration or OS detection. Masscan is useful for very large ranges due to its speed.

yeah that's 100% true, Masscan is not going to have the vuln scripts to follow up with or other deeper scans.

InspectorGadget - November 2, 2025, 6:54 am

Don't forget the multiple 10 gigabit networked servers you'll need to do this in 10 minutes lol.

I found the cost of using 10g uplinks was too much, so i use 1g uplinks across 4 servers. Takes 12 hours but thats good enough for me.

Hackers - November 2, 2025, 7:30 am

(Nov 2, 2025 07:54 AM)InspectorGadget Wrote: [\[CITE\]](#) Don't forget the multiple 10 gigabit networked servers you'll need to do this in 10 minutes lol.

I found the cost of using 10g uplinks was too much, so i use 1g uplinks across 4 servers. Takes 12 hours but thats good enough for me.

Yeah absolutely, it's a little gimicky in the sense that you do need the hardware as well, and the networking / bandwidth in general.

I think the point is the speed at which it can check all. It does make a point of noting that people should specifically prepare their server for this in a way that doesn't let it interfere with other server networking. This tool is designed for much larger operations than most people, including me really need tbh

InspectorGadget - November 2, 2025, 7:32 am

(Nov 2, 2025 08:30 AM)nodes Wrote: [\[CITE\]](#) Yeah absolutely, it's a little gimicky in the sense that you do need the hardware as well, and the networking / bandwidth in general.

I think the point is the speed at which it can check all. It does make a point of noting that people should specifically prepare their server for this in a way that doesn't let it interfere with other server networking. This tool is designed for much larger operations than most people, including me really need tbh

Yeah 100%, it's the GOAT in terms of scanning at a mass scale.