[Skip to main content](https://lms.alnafi.com/xblock/block-v1:alnafi+DCCS102+2025_DCCS+type@vertical+block@afbe6245afe54fa983f57806032591fa?exam_access=&recheck_access=1&show_bookmark=0&show_title=0&view=student_view#main)

**Who is Masscan for?**

Masscan is useful for red teamers doing offensive research (like penetration testing) as well as blue teamers and IT managers doing defensive research (like finding attack vectors within their network).

Masscan is also useful for both beginners and advanced users. It isn't difficult to use and provides valuable functionality for researchers performing larger investigations.

**Installation**

Now we'll cover Linux and macOS installation procedures for Masscan.

**Installing Masscan on Linux**

The quickest way to install Masscan on Linux is to download the source code and compile the software. The tool may already exist in pentesting distros like Kali Linux, but we haven't verified that.

It's always important to use some type of sandboxing environment when installing new software. You could opt for a virtual machine (VM), container, or remote test server. We used Ubuntu 20.04 for this review and any commands used here should apply to Debian-based distros (and with a few minor tweaks, to other distros as well).

The first step is to install some necessary software:

sudo apt update

sudo apt upgrade

sudo apt install git gcc make libpcap-dev

Next, we clone the [official repo](https://github.com/robertdavidgraham/masscan?rel=nofollow,noopener,noreferrer&target=_blank) and compile the software:

git clone https://github.com/robertdavidgraham/masscan

cd masscan

make

You might get 1 or 2 warnings during the compilation, but if the software compiled successfully, you will see an output like the:



**Installing Masscan on MacOS**

Installing Masscan on MacOS is even easier. Simply use this command:

brew install masscan

And that's it!

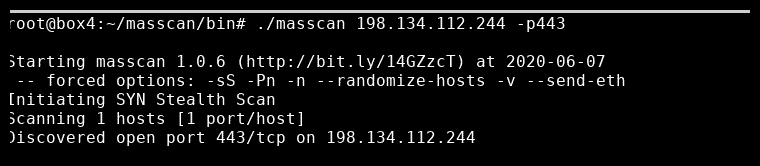
**How to use it? Masscan examples**

We'll now attempt to run a few basic commands to see Masscan in action. Firewalls or proxies may block IPs that aggressively do port scans, and we'll use this hindsight to run our tests.

**Single IP port scan**

Our first test is a single IP and single port scan of a malvertising IP we're tracking.

./masscan 198.134.112.244 -p443



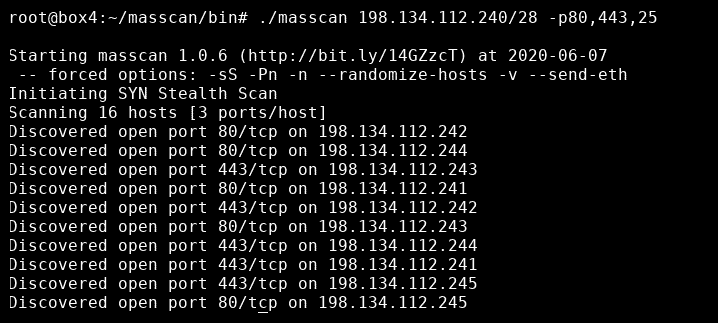
The tool confirmed that port 443 is indeed open at the chosen IP.

**Advanced port scan against multiple ports**

An advanced scan can be executed to analyze multiple ports or a range of ports on an IP subnet. We'll share examples for both and the output for a multi-port analysis.

./masscan 198.134.112.240/28 -p80,443,25 #multiple ports

./masscan 198.134.112.240/28 -p1000-9999 #range of ports



The scanner tells us how many hosts (16) were found, and then displays which ports are open on which IP addresses.

**Scanning the top ports**

This is another interesting feature: Masscan users can scan the [most popular ports](https://securitytrails.com/blog/top-scanned-ports) by using the 'top-ports' option from the Nmap command with Masscan.

The syntax is simple, just add "--top-ports X", replacing the X with several popular ports, for example, 10 or 100, which are the most popular ones used by security researchers.

So the full syntax would look like this:

masscan 192.168.1.105 ‐‐top-ports 10

This saves you time, as you're focused on the most important ports from Nmap scan stats.

**Scanning a subnet**

Now let's use Masscan to its full potential, by running a scan on a bigger subnet and at a faster rate, looking for the top 100 Nmap ports.

./masscan 198.134.112.0/20 --top-ports 100 --rate 100000 > output.txt

We piped the results of this scan to a file so that we could store the results of the scan. The results show that 4096 hosts were found, and among them, we found many interesting details. Besides the usual ports of 80/443, some of the IP addresses had open ports such as 21, 23, 53, 111, 427, and 514.

An important thing to note about Masscan is that all scans run by default in "SYN Stealth Scan" mode. The Nmap website explains this:

"SYN scan is the default and most popular scan option for good reason. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by intrusive firewalls. SYN scan is relatively unobtrusive and stealthy since it never completes TCP connections. It also works against any compliant TCP stack rather than depending on idiosyncrasies of specific platforms as Nmap's FIN/NULL/Xmas, Maimon and idle scans do. It also allows clear, reliable differentiation between open, closed, and filtered states."

This feature would explain why port scanners can scan through so many IP addresses without getting banned by basic firewalls. However, with more advanced protection software, we suspect that even this type of scanning can be blocked.

**Exclude targets from your scan**

Sometimes you need to reduce the number of hosts that are going to be scanned. To skip some of them, the 'exclude targets' option can be of help.

Masscan enables you to create an exclude file, so you can use the --exclude file parameter for any of your scans. The syntax would look like this:

masscan 192.168.1.105 ‐‐top-ports 10 ‐‐excludefile exclude-list.txt

Once you run the scan, a warning will be seen at the beginning of the scan:

exclude-list.txt: excluding 1 range from file

**Scanning the entire Internet with Masscan**

As we said before, Masscan was built with speed in mind. It's prepared to run massive amounts of port scans across networks. Therefore, here you have a few examples of how to scan the entire Internet, for one specific port, or all of the 65535 ports for each host.

Important note: Keep in mind that this may yield a vast amount of results, and most importantly, you might be probing IP addresses related to government servers, honeypots, and digital traps that you probably never want to get involved with.

How can I scan the Internet for one specific port?

Just use this syntax, at full speed (10 million p/s).

masscan 0.0.0.0/0 -p22 --rate 10000000 #see footnote below [1]

This will trigger a massive scan across the whole internet, against port 22.

How can I scan the Internet for all the existing ports?

masscan 0.0.0.0/0 -p0-65535 --rate 10000000 #see footnote below [1]

[1] The ability to transmit up to 10M packets per second requires the purchase of a commercial product. The standard scan ability is around 1.5-2 million packets per second, according to the documentation.

**Tweaking Masscan output**

The output above isn't very useful in its current format, but Masscan offers 5 output options that are more practical for analyzing the data elsewhere:

1. XML: -oX <filename> for XML files

Further tests

The --help command becomes handy to get a full picture of Masscan’s full potential, where you can find a wide range of options for advanced scanning techniques, as you see below:

