Scanning the **whole internet** is a massive task — and **Masscan** is one of the few tools fast enough to attempt it. But with great power comes great risk and responsibility.

**🚨 ⚠️ Disclaimer (VERY IMPORTANT):**

* Scanning the entire internet without **permission** or legitimate purpose can trigger **legal action**, get you **banned**, or alert **national security systems**.
* Only scan **your own assets** or use **test ranges (like Hack The Box, TryHackMe, etc.)** for learning.
* This explanation is purely **educational**.

**🧠 What is Masscan?**

**Masscan** is the fastest port scanner – it can scan the **entire internet (IPv4)** in minutes.

* Written in C
* Asynchronous
* Can scan **10 million packets/second**
* But… it’s **very noisy** and can be **easily detected**.

**⚙️ Step 1: Install Masscan**

**🐧 On Linux:**

sudo apt install git build-essential

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

cd masscan

make

**🪟 On Windows:**

* Use precompiled binaries or compile using MSVC.

**🛠️ Step 2: Basic Syntax**

sudo masscan -p80 0.0.0.0/0 --rate=1000

**🔍 Breakdown:**

* -p80 → scan **port 80**
* 0.0.0.0/0 → entire **IPv4 address space**
* --rate=1000 → packets per second (be very conservative or you’ll crash your network)

**🧪 Example: Scan Port 443 on the Entire Internet**

sudo masscan -p443 0.0.0.0/0 --rate=10000 -oX output.xml

* -oX output.xml → save output in XML format for further analysis.

**🧠 Recommended Practice Range Instead:**

Use **Scanme** (allowed by Nmap team):

masscan -p80 scanme.nmap.org --rate=100

**🧰 Advanced Flags:**

| **Flag** | **Meaning** |
| --- | --- |
| -p1-65535 | Scan all TCP ports |
| --rate=100000 | Increase packets/sec (only if network supports it) |
| --source-port 4444 | Set a source port (can bypass basic firewalls) |
| --banners | Try to grab banner info (limited compared to Nmap) |
| --exclude | Exclude ranges like AWS/GCP/etc. |

**💾 Output Formats:**

* -oG file.gnmap → Grepable format
* -oX file.xml → XML (good for parsing)
* -oJ file.json → JSON output (requires patch/fork)

**🧪 Sample Use Case (CTF Style):**

Let’s say you want to **scan a range for open SSH** (port 22):

masscan 10.10.0.0/16 -p22 --rate=5000 -oG found\_ssh.txt

Then, feed it into **Nmap** for deeper scanning:

cat found\_ssh.txt | awk '/open/ {print $2}' > ips.txt

nmap -sV -iL ips.txt -p22

**🔐 Warning: Avoid Scanning These**

Never scan:

* Government IPs
* Cloud providers (AWS, Azure, GCP)
* Major websites (Google, Facebook, etc.)

You may:

* Get IP banned
* Receive cease and desist
* Trigger ISP/network alerts

**📚 Want to Practice Legally?**

Use ranges like:

* [Hack The Box](https://www.hackthebox.com/)
* [TryHackMe](https://tryhackme.com/)
* [RangeForce](https://www.rangeforce.com/)
* [OverTheWire](https://overthewire.org/)
* Your own virtual lab